PRT-CTRL-DIN

Protege GX DIN Rail Integrated System Controller

Installation Manual

Last Published: 25-May-21 4:27 PM

Contents

Introduction

The Protege GX DIN Rail Integrated System Controller is the central processing unit responsible for the control of security, access control and building automation in the Protege GX system. It communicates with all system modules, stores all configuration and transaction information, processes all system communication, and reports alarms and system activity to a monitoring station or remote computer.

Protege GX is an enterprise level integrated access control, intrusion detection and building automation solution with a feature set that is easy to operate, simple to integrate and effortless to extend.

Flexible module network architecture allows large numbers of modules to be connected to the RS-485 module network. Up to 250 modules can be connected to the Protege system in any combination to the network, over a distance of up to 900M (3000ft). Further span can be achieved with the use of a network repeater module.

The current features of the controller include:

- Internal industry standard 10/100 ethernet
- 32 Bit advanced RISC processor with 2Gb total memory
- Encrypted module network using RS-485 communication
- NIST Certified AES 128, 192 and 256 Bit Encryption
- Factory loaded HTTPS certificate
- OSDP configurable RS-485
- 8 high security monitored inputs
- Built-in offsite communications dialer (ContactID or SIA)
- Industry standard DIN rail mounting

Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- UL 681 - Installation and Classification of Burglar and Holdup Systems
- UL 827 - Central-Station Alarm Services
- CAN/ULC-S301, Central and Monitoring Station Burglar Alarm Systems
- CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults
- CAN/ULC-S561, Installation and Services for Fire Signal Receiving Centres and Systems
- The National Electrical Code, ANSI/NFPA 70
- The Canadian Electrical Code, Part I, CSA C22.1
- AS/NZS 2201.1 Intruder Alarm Systems
- The Local Authority Having Jurisdiction (AHJ)

Grounding Requirements

An effectively grounded product is one that is intentionally connected to earth ground through a ground connection or connections of sufficiently low impedance and having sufficient current-carrying capacity to prevent elevated voltages which may result in undue hazard to connected equipment or to persons.

Grounding of the Protege system is done for three basic reasons:

1. Safety
2. Component protection
3. Noise reduction

Safety Grounding

The object of safety grounding is to ensure that all metalwork is at the same ground (or earth) potential. Impedance between the Protege system and the building scheme ground must conform to the requirements of national and local industrial safety regulations or electrical codes. These will vary based on country, type of distribution system and other factors. The integrity of all ground connections should be checked periodically.

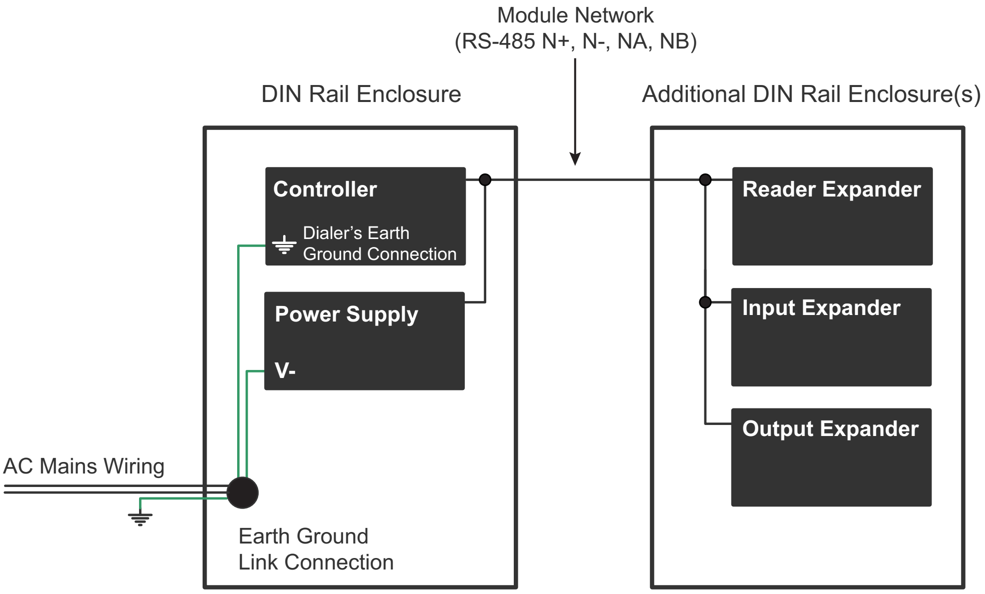
General safety dictates that all metal parts are connected to earth with separate copper wire or wires of the appropriate gauge.

Earth Ground Connection

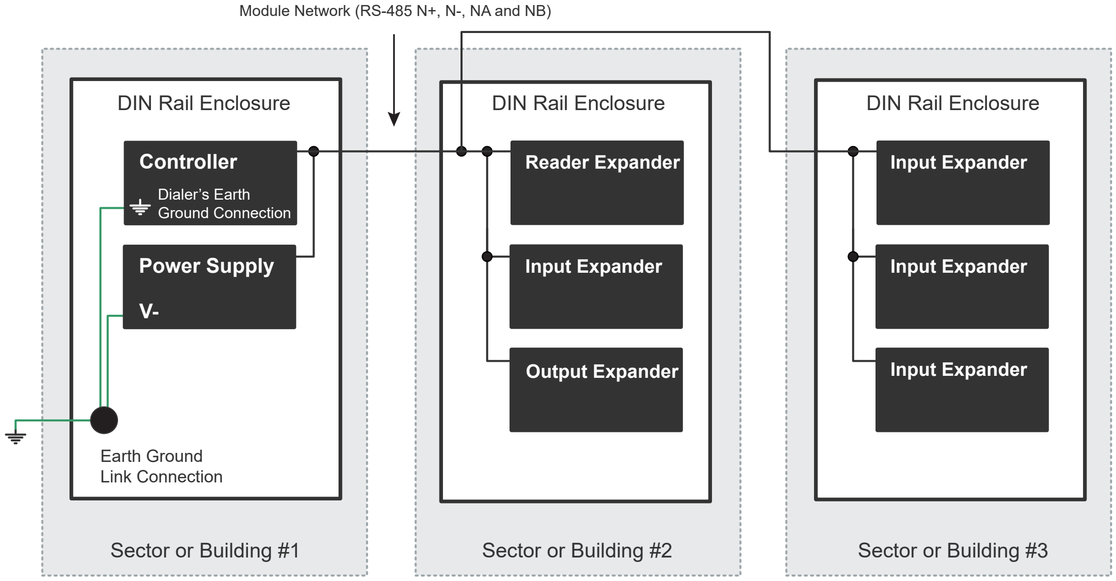
The DIN rail enclosure and the DIN rail modules must be grounded to a suitable single-point earth ground connection in the installation. A minimum 14AWG solid copper wire (or thicker, in accordance with local authorities) shall be used from the Protege system's earth connection points.

The DIN rail enclosure includes an earth ground single-point link connection via the metallic enclosure. This single-point link is the Protege system's earth ground. All modules that have earth ground connections and that are installed in the same enclosure shall be connected to this single point. A single-point earth ground connection avoids the creation of ground loops in the system and provides a single reference point to earth ground.

DIN Rail Ground Connections (one or more cabinets installed in the same room)



DIN Rail Ground Connections (multiple cabinets in different rooms, sectors, or buildings)



Note that the DIN rail enclosure earth terminal is connected to the power supply V- terminal.

There must be only **one** single earth grounding point per system.

Mounting

Protege DIN rail modules are designed to mount on standard DIN rail either in dedicated DIN cabinets or on generic DIN rail mounting strip.

When installing a DIN rail module, ensure that there is adequate clearance around all sides of the device and that air flow to the vents of the unit is not restricted. It is recommended that you install the module in a location that will facilitate easy access for wiring. It is also recommended that the module is installed in an electrical room, communication equipment room, secure cabinet, or in an accessible area of the ceiling.

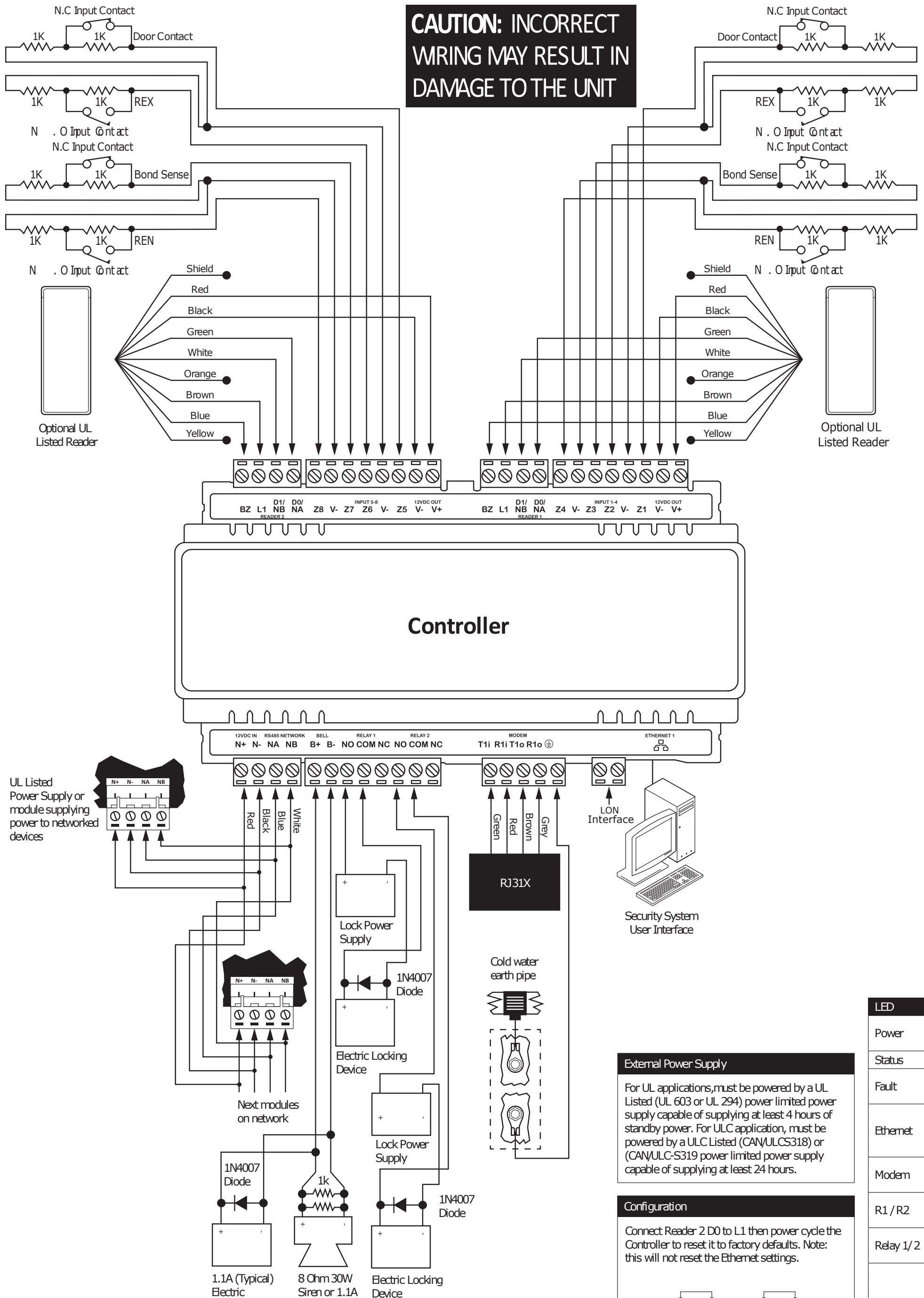
1. Position the DIN rail module with the labeling in the correct orientation.
2. Hook the mounting tabs (opposite the tab clip) under the edge of the DIN rail.
3. Push the DIN rail module against the mount until the tab clips over the rail.

Removal

A Protege DIN rail module can be removed from the DIN rail mount using the following steps:

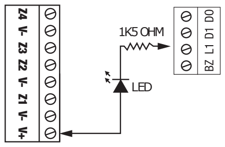
1. Insert a flat blade screwdriver into the hole in the module tab clip.
2. Lever the tab outwards and rotate the unit off the DIN rail mount.

Wiring Diagram



Programmable Outputs (L1 & BZ)

If not used for Reader functions the Reader outputs (L1 & BZ) can be used as general purpose ouputs. They are Open Collector Outputs & switch to 0V. The outputs can be used to activate relays, sounders and lights.



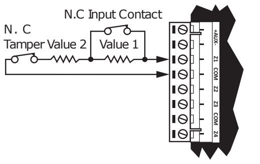
Wiring

EARTH GND WIRING: Minimum 14AWG solid copper wire.
INPUT WIRING: maximum distance of 300m (1000ft) from the Controller when using 22 AWG
AUX WIRING: Min 22AWG Max 16AWG. (Depends on length and Current consumption). For wire/cable size, a maximum of 5% voltage drop at the terminals of the powered device has to be observed.
ETHERNET WIRING: CAT5e / CAT6 max 100m (330 ft)
MODULE NETWORK WIRING: Recommended Belden 9842 or equivalent. (24AWG twisted pair with characteristic impedance of 120ohm or CAT5e / CAT6 are also supported for Data Transmission when using ground in the same cable. Do not use extra wires to power devices.) max 900m (3000ft).

Typical Input Circuits

EOL Resistor Input Configuration

Value 1	Value 2	Monitored Status
No Resistor	No Resistor	Open, Closed
1k	1k	Open, Closed, Tamper, Short
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



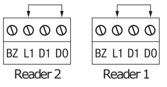
LED	Description	
Power	Green	Power is applied
	Off	Low or no power is applied
Status	Flashing green	Normal operation
Fault	Red	A fault has occurred
	Off	Normal operation
Ethernet	Green	Ethernet connection present
	Off	No Ethernet connection detected
	Fast green flash	Active Ethernet data
Modem	Green	The modem has control of the telephone line
	Off	Modem not active
R1 / R2	Short red flash	Data received but format is incorrect
	Long red flash	Correctly formatted data received
Relay 1/ 2	Red	Relay is closed
	Off	Relay is open
Bell	Green	Bell is turned on
	Off	Bell is connected and turned off
	1 green flash	Bell is turned on, and the circuit is in over-current protection
	2 green flashes	Bell is turned off, and the circuit is cut, damaged or tampered
Input1-8	Off	The Input is not programmed
	Red	Input is in the OPEN state
	Green	Input is in the CLOSED state
	Flashing red	Input is in the TAMPERED state
	Flashing green	Input is in the SHORTED state

External Power Supply

For UL applications,must be powered by a UL Listed (UL 603 or UL 294) power limited power supply capable of supplying at least 4 hours of standby power. For ULC application, must be powered by a ULC Listed (CAN/ULCS318) or (CAN/ULC-S319 power limited power supply capable of supplying at least 24 hours.

Configuration

Connect Reader 2 D0 to L1 then power cycle the Controller to reset it to factory defaults. Note: this will not reset the Ethernet settings.



Connect Reader 1 D0 to L1 then power cycle the Controller to force it to use 192.168.111.222 as it's IP address.

Input Options

The onboard reader ports use inputs 1 – 8 as door contact, REX, bond sense and REN inputs respectively. Any of these inputs that are not configured for use with the Onboard Reader may be used as general purpose inputs. Refer to the Controller Installation Manual for instructions on programming the onboard reader.

Connections

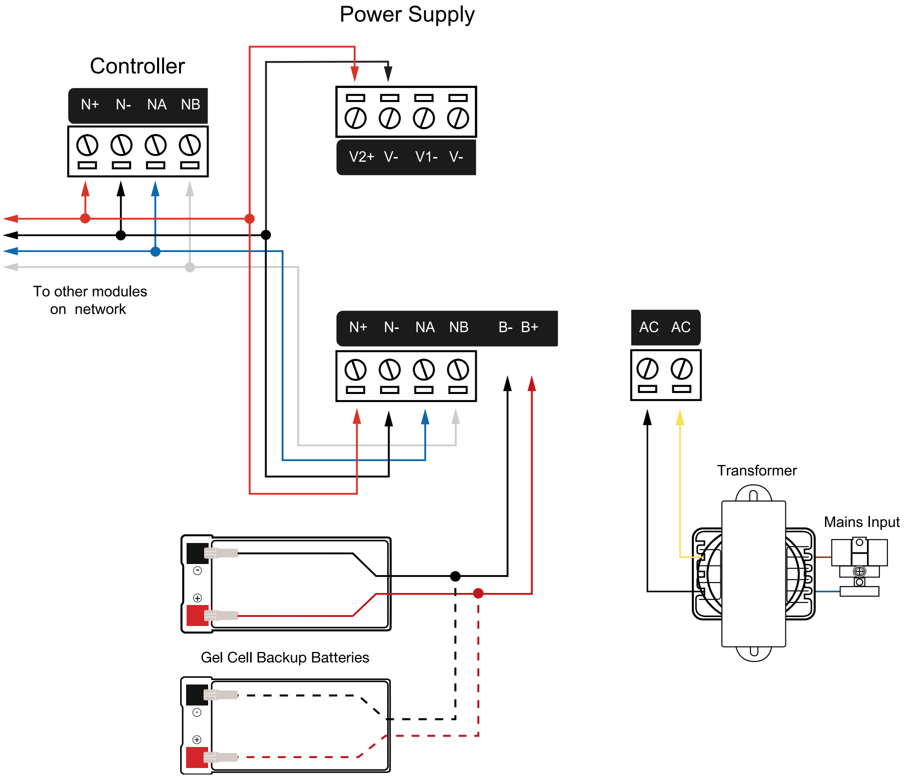
Power Requirements

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 any clean 12V DC supply is suitable for this purpose.

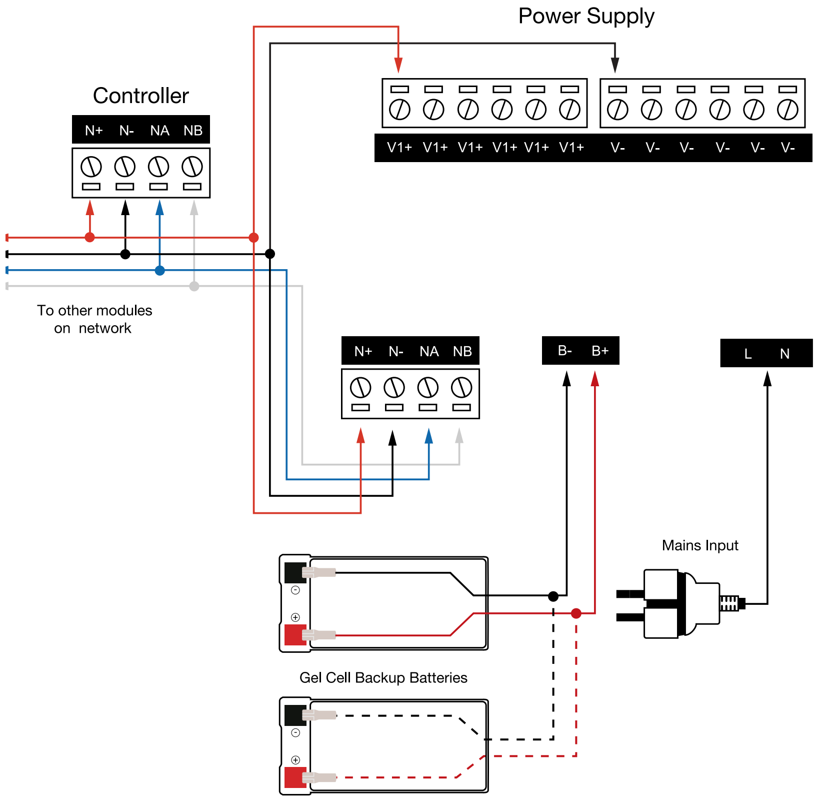
Termination of wiring to the module while power is applied or the battery is connected may cause serious damage to the unit and will VOID ALL WARRANTIES OR GUARANTEES.
Power the unit only after all wiring, configuration and jumper settings are completed.

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 2A Power Supply Connection:



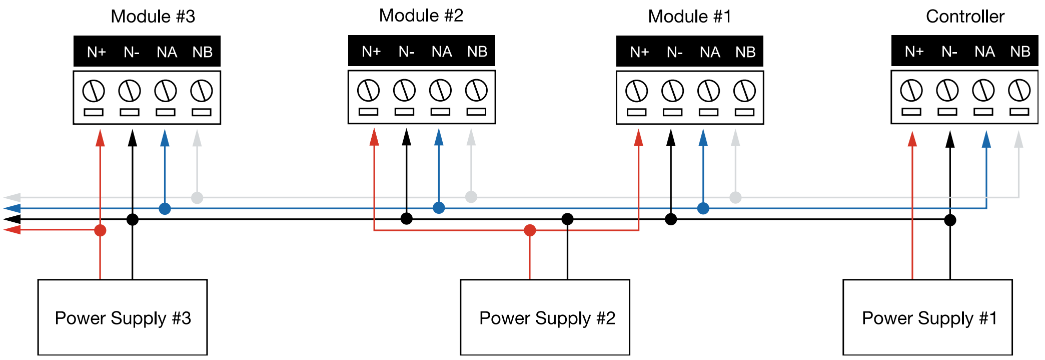
Example 4A Power Supply Connection:


Power Supply
V1+ V1+ V1+ V1+ V1+ V1+ V- V- V- V- V- V-
Controller
N+ N- NA NB
To other modules on network
N+ N- NA NB
B- B+
L N
Mains Input
Gel Cell Backup Batteries

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.

To comply with EN 50131-1 only one battery can be connected and monitored per system. If more capacity is required a single larger battery must be used.

Example Multiple PSU Connection:



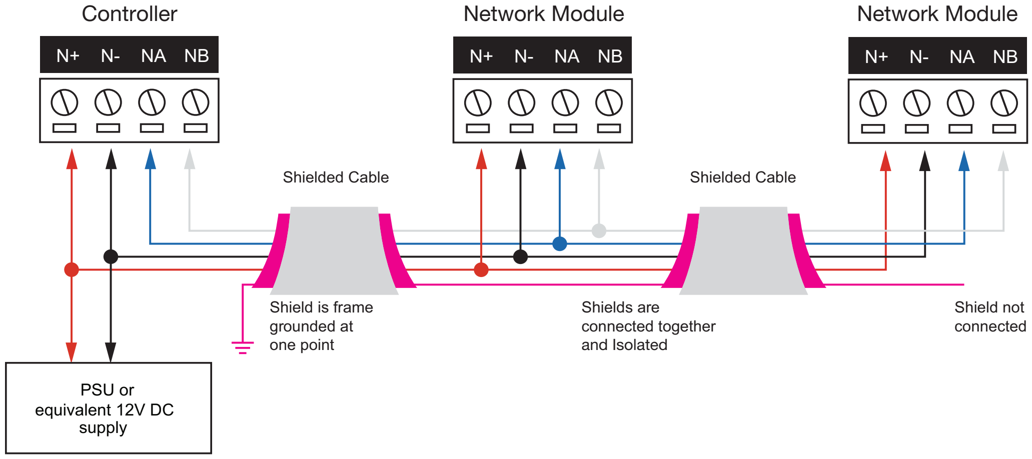
When using multiple power supplies it is important to ensure that all ground connections (V-) are connected between all power supplies and that no power connections (V+) are connected between any power supplies.

Auxiliary Outputs

The auxiliary outputs (V- V+) of the controller can be used to supply other equipment. Note that there is no onboard regulation or isolation for these outputs; they are a fused feed-through from the N+ N- input terminals. When using these outputs to supply other devices, be sure not to exceed the rating of the internal fuses as outlined in the Technical Specifications.

Encrypted Module Network

The controller incorporates encrypted RS-485 communications technology. Connection of the communications should be performed according to the following diagram.


Controller
N+
N-
NA
NB
Network Module
N+
N-
NA
NB
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
PSU or equivalent 12V DC supply

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.

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 unit or the device supplying network power. Make sure that the power supply can supply enough current for the peak load drawn by **all modules** connected to the 12V supply, including the controller itself.

Module Wiring

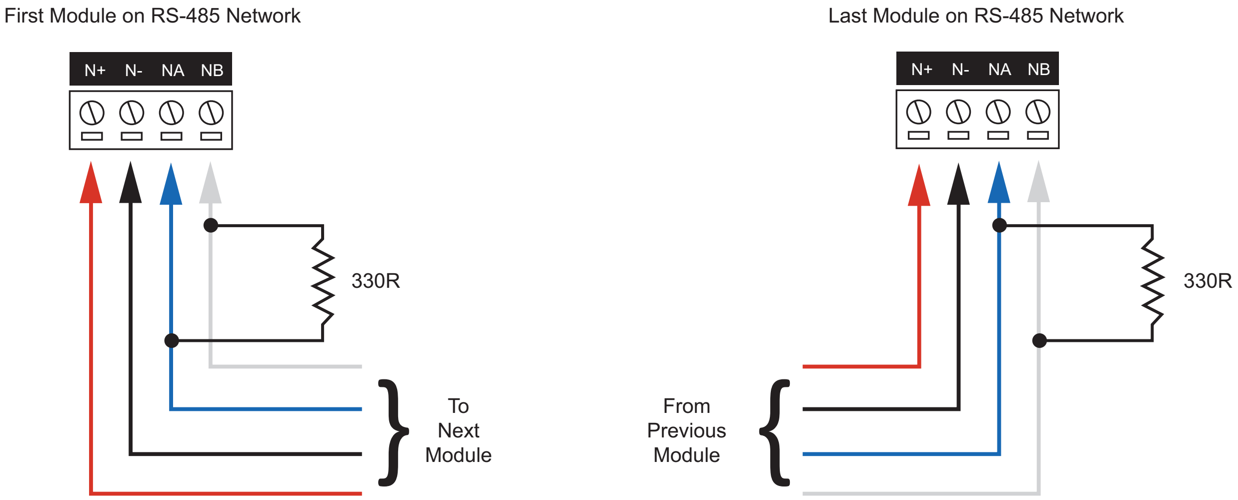
The recommended module network wiring specifications are:

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

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

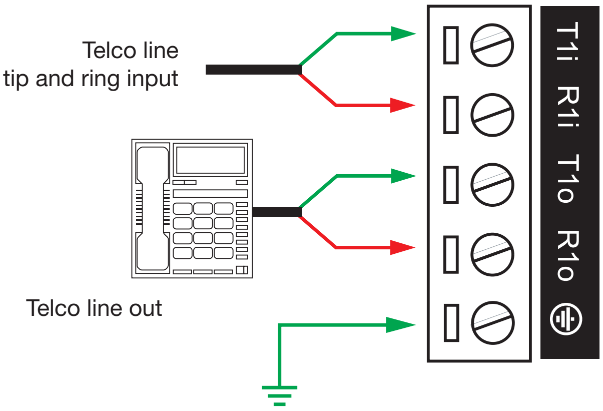
End of Line (EOL) Resistors

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.



Telephone Dialer

The controller provides the ability to communicate alarms and upload information to remote systems using the onboard 2400bps modem. The telephone line can be connected directly to the controller using the onboard telephone connection terminals.



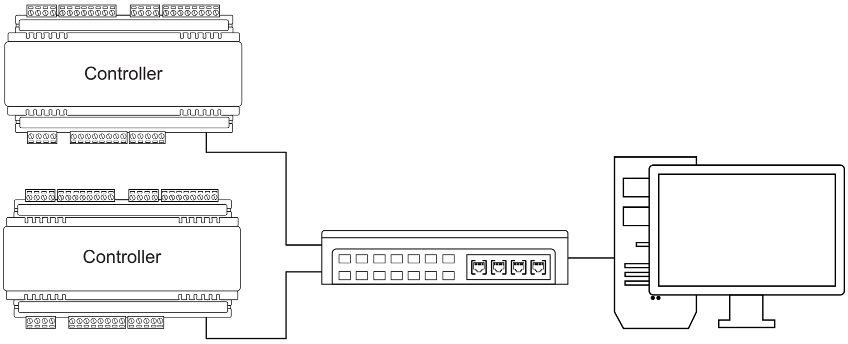
Ethernet 10/100 Network Interface

The communication between the Protege system and the controller uses a 10/100 ethernet network operating the TCP/IP protocol suite. The IP address of the controller can be configured using an LCD keypad terminal or via the built-in web interface. The default IP address is set to a static 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.

Installing the module 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 module.

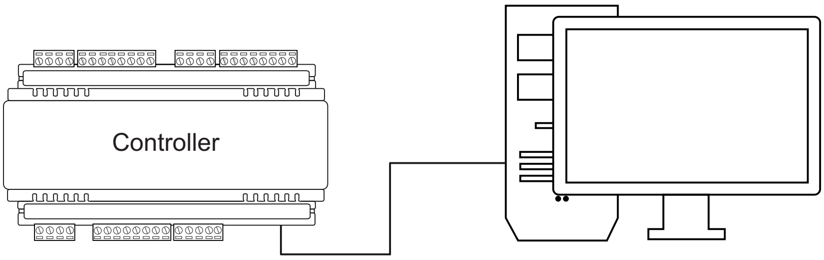
When installing an ethernet connection the module should be interfaced using a standard segment (<100m in length) and should be connected to a suitable ethernet hub or switch:

Ethernet 10/100 Switch hub Connection:



Temporary direct connections can be used for onsite programming by using a standard ethernet cable.

Ethernet 10/100 Direct Connection:



- All network equipment such as hubs/routers/gateways used with the controller must comply with the UL and ULC standard requirements associated with a signal receiving center.
- The controller must be installed in the same room as the network equipment that provides it the network connection.

Door Access Control

The controller provides access control functionality onboard without the requirement for additional hardware. The controller allows the connection of 2 Wiegand devices to control 2 doors (entry or exit only) or 1 door (entry and exit), or it can be configured in multiplex mode to allow 4 Wiegand devices controlling 2 doors with entry and exit readers. Alternatively, the reader ports can be independently configured to connect RS485-based readers.

The recommended cable types for RS-485 are:

- Belden 9842 or equivalent
- 24 AWG twisted pair with characteristic impedance of 120ohm

The recommended cable types for Wiegand are:

- 22 AWG alpha 5196, 5198, 18 AWG alpha 5386, 5388

Important:

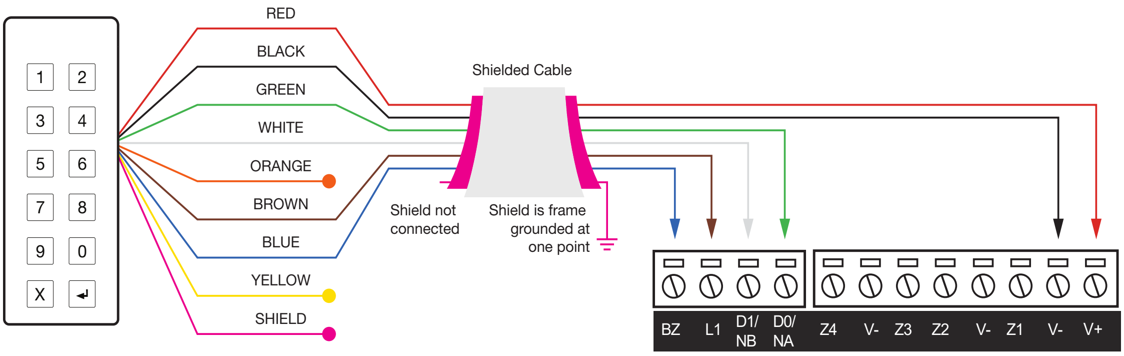
- The card reader must be connected to the module port using a shielded cable.
- Do not connect the shield to an AUX-, 0V or V- connection on the module.
- Do not join the shield and black wires at the reading device.
- Do not connect the shield to any shield used for isolated communication.
- The shield connection must only be connected at one end of the cable in the metallic enclosure (frame grounded).

UL ULC

All UL listed ICT readers are shipped with single LED mode set as default and are fully compatible with the Protege system, such as tSec Standard Readers, tSec Mini Readers, etc.

Wiegand Reader Connection

The controller allows the connection of 2 magnetic clock and data reading devices or 4 Wiegand reading devices and the ability to control 2 doors (entry or exit only) or 1 door (entry and exit). The following diagrams show the connection of a standard Wiegand reader with the controller controlling an access door and an entry/exit door.

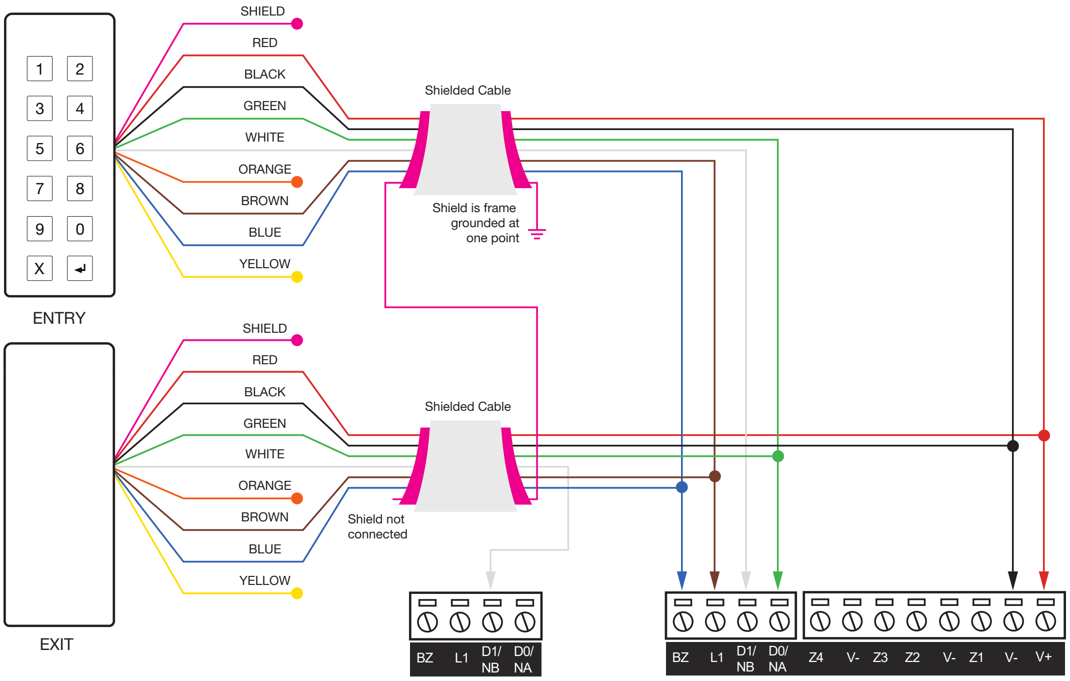


Multiple Wiegand Reader Connection

Multiple reader mode allows the connection of 4 Wiegand reading devices controlling 2 doors each with entry/exit readers.

In multiple reader 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.

The reader that is multiplexed into the alternate reader port will operate as the **exit** reader, and the normal reader connection shall operate as the **entry** reader.



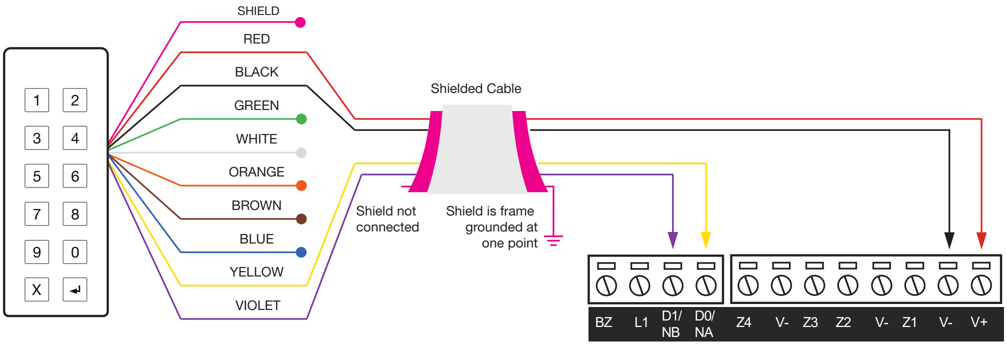
RS-485 Reader Locations

As two RS-485 readers can be connected to the same RS-485 reader port, configuration of the **green** and **orange** wires uniquely identifies the reader, and determines which is the entry reader and which is the exit reader.

Location	Configuration
Entry	Green and orange wires **not** connected.
Exit	Green and orange wires connected together.

RS-485 Reader Connection (Entry Only)

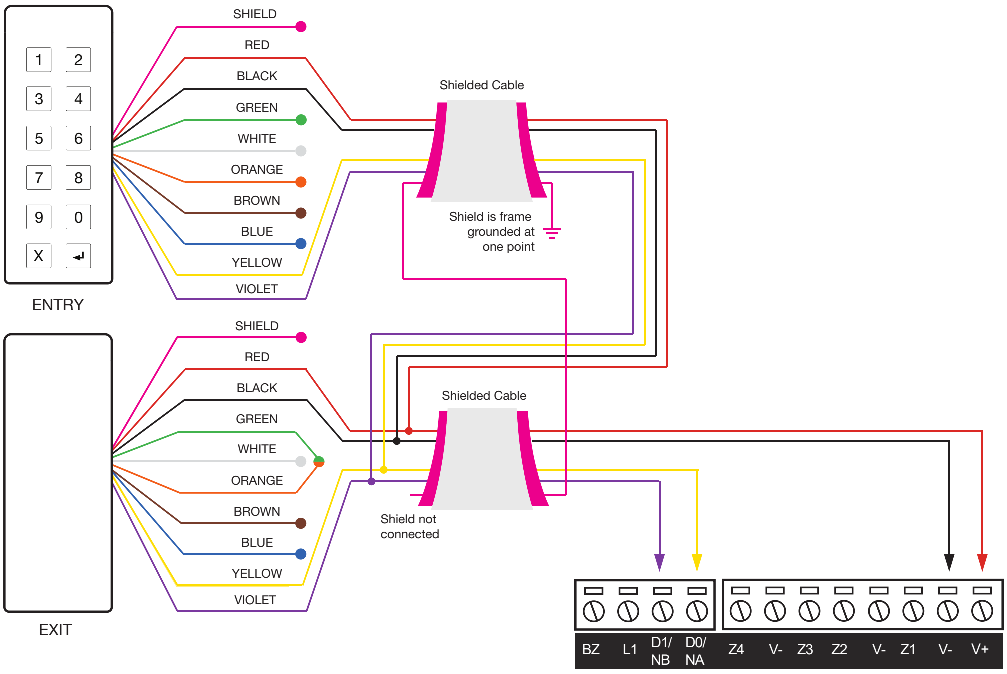
The following diagram shows the connection of a single RS-485 reader connected in entry only mode.



When the green and orange wires are not connected together, the reader defaults to an entry reader.

RS-485 Reader Connection (Entry/Exit)

The following diagram shows the connection of two RS-485 readers connected to provide an entry/exit configuration.



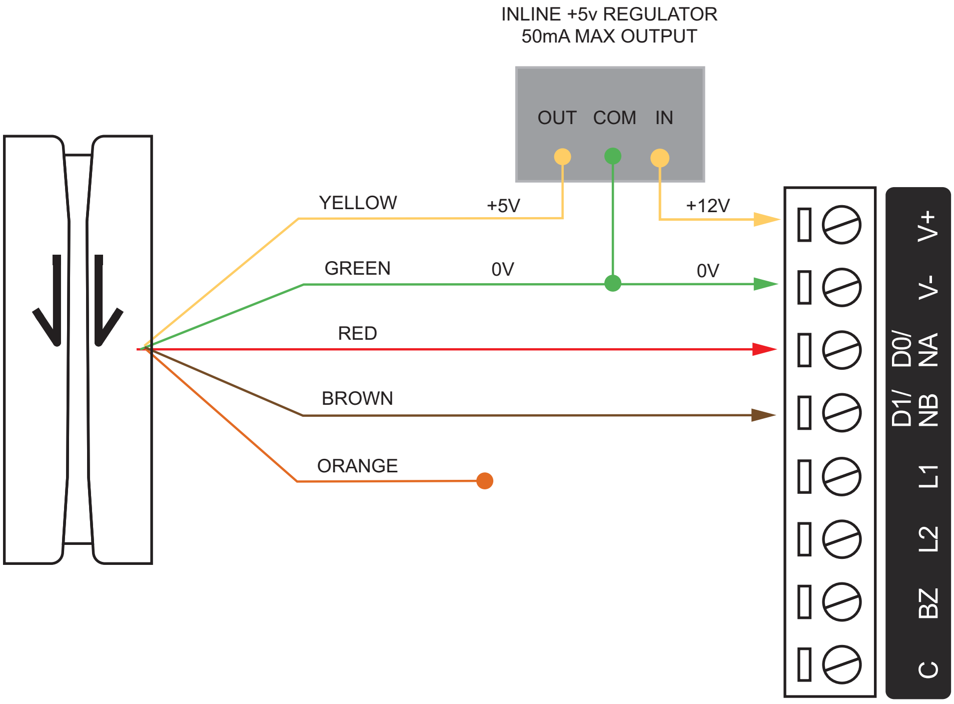
The exit reader has the **green** and **orange** wires connected together.

A 330 ohm EOL (End of Line) resistor may be required to be inserted between the NA and NB terminals of the reader and a second 330 ohm EOL resistor must then be inserted between the source NA and NB terminals at the other end of the wiring.

Magnetic Reader Connection

The controller allows the connection of standard magnetic track 2 format cards and provision is made in the software for a large number of formats. Formats include BIN number for ATM access control and first 4, 5 and 6 card numbers.

Magnetic Card Reader Interface:

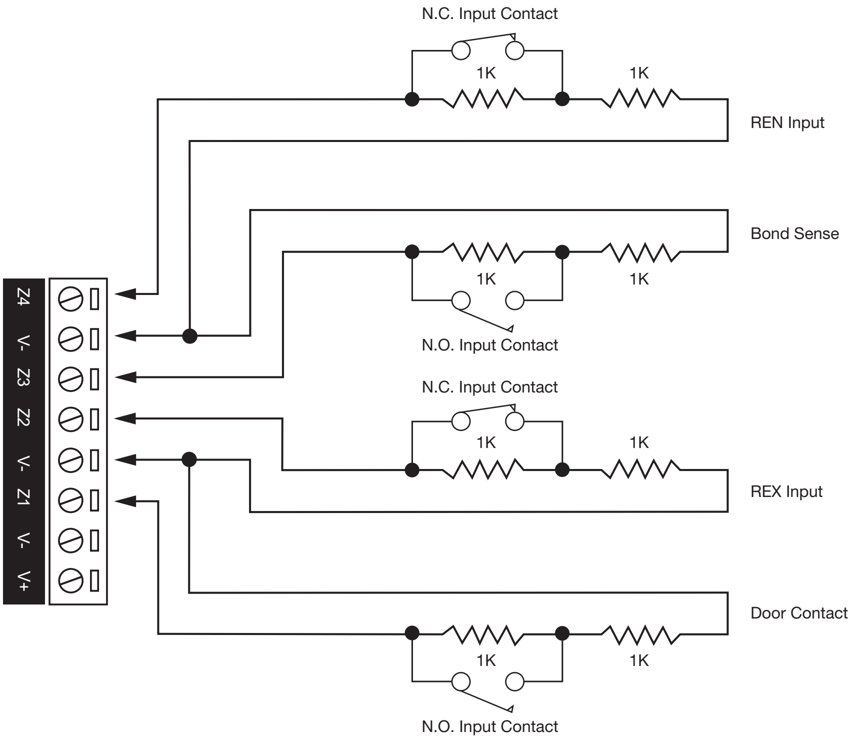


Magnetic card readers are typically operated by 5 volts. Before connecting the magnetic card reader to the controller, ensure that the supply voltage is correct and if required insert the inline 5 Volt regulator as shown in the diagram above.

UL ULC The magnetic reader connection has not been evaluated for UL/ULC applications.

Door Contact Connection

The module allows the connection of up to 4 contacts for monitoring and controlling access control doors. Each input can be used for either the door function that is automatically assigned or as a normal input on the system. The following example shows the connection of a normally closed door position monitoring contact to monitor the open, closed, forced and alarm conditions of the door.



Inputs 1-4 and 5-8 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.

UL ULC

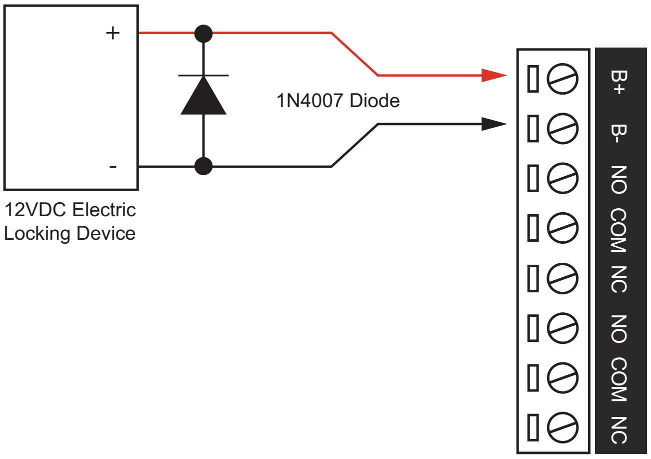
When inputs are configured as bond sense and/or general purpose inputs (access control and burglar installations), remaining inputs cannot be used for fire.

Lock Output Connection

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. The door lock monitoring can be disabled if it is not required.

The lock output is shared with the bell/siren function as shown in the diagram below. You can select another output for the lock control (Relay 1 (CP001:03) or Relay 2 (CP001:04)) if the bell/siren function is required.

To use the lock outputs in conjunction with the onboard reader module, the lock output for the door associated with the reader port must be configured to be the desired lock output on the controller. This is not configured by default.



When using a door with an entry and exit reader, the lock output should be connected to the Bell (CP001:01), and the swap lock option for the second reader input should be enabled to allow the reader LEDs to display the correct status.

The bell output current must not exceed 1.6A or electronic shutdown will be engaged. Ensure the devices connected to the outputs are within the limits as described in the Technical Specifications.

Programming the Onboard Reader

The onboard reader is programmed in exactly the same way as any other reader module. It can be thought of as if it were a normal reader expander module on a separate circuit board. By default the onboard reader is disabled. To enable it, configure the address at which you want it to register using the Protege user interface. Note that any physical reader expander module that is connected with the same address will be treated as a duplicate and will fail to register, so care should be taken to ensure the address is unique.

The onboard reader uses inputs 1-4 and 5-8 as its door contact, REX, bond sense and REN inputs respectively. Any inputs that are not configured for used with the onboard reader may be used as general purpose inputs. If you wish to use an access control input as a general input, you will need to disable the associated function input in the door programming section of the Protege user interface.

UL ULC REX and REN devices must be listed to UL 294 for UL installations and CAN/ULC-S319 for ULC installations, and be compatible with the system.

The default settings are shown in the following table:

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

Inputs

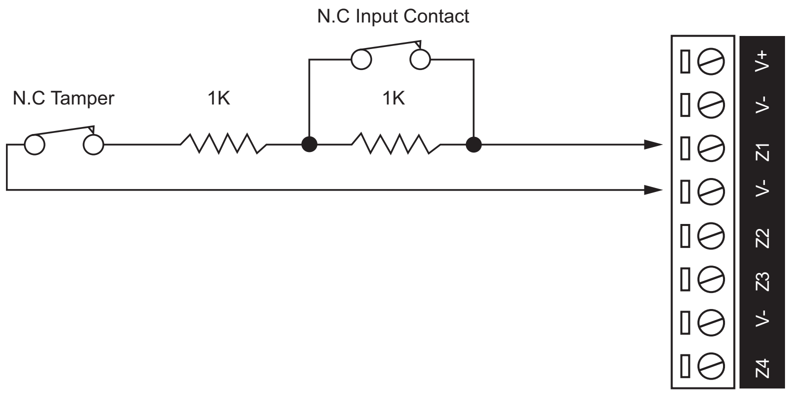
The controller has 8 onboard inputs for monitoring the state of devices such as magnetic contacts, motion detectors and temperature sensors. Devices connected to the inputs can be installed to a maximum distance of 300m (1000ft) from the module when using 22 AWG wire.

- Magnetic contacts shall be listed to UL 634 to comply with UL installation standards and ULC/ORD-C634 to comply with ULC installation standards.
- Motion detectors and temperature sensors shall be listed to UL 639 to comply with UL installation standards and ULC-S306 to comply with ULC installation standards.
- The controller has been evaluated for UL 294, UL 1076, UL 1610, UL 1635, CAN/ULC-S304, CAN/ULC-S319 and CAN/ULC-S559.

Inputs can be programmed using the Protege software. Inputs CP001:01 to CP001:08 represent the controller's onboard inputs. Additional inputs are supported through the use of expansion modules.

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 changes between open and closed and generates a tamper alarm condition when a wire fault (short circuit) or a cut wire (tampered) in the line occurs. Inputs default to require the EOL resistor configuration.

EOL Resistor Input Configuration

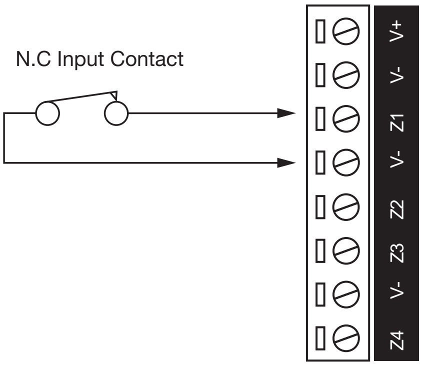


Inputs 1-4 and 5-8 can operate as either general purpose inputs or as onboard reader inputs. If used as general purpose inputs you must ensure that they are not defined in the onboard reader set up.

Each input can use a different input configuration. To program a large number of inputs with the same configuration, use the multiple selection feature within the Protege software.

When using the 'No Resistor' configuration the controller only monitors the opened and closed state of the connected input device, generating the alarm (open) and restore (closed/sealed) conditions.

No EOL Resistor Input Configuration



EOL Resistor Value Options

When using the EOL resistor configuration, the EOL resistor option must be configured based on the site requirements. Note these resistor options are supported on the controller but not all resistor options are supported on all Protege field modules.

Value 1	Value 2	Monitored Status
No Resistor	No Resistor	Open, Closed
1K	1K	Open, Closed, Tamper, Short
6K8	2K2	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
5K6	5K6	Open, Closed, Tamper, Short
No Resistor	5K6	Open, Closed

The 5k6 Value 1 and Value 2 have not been evaluated by UL, cUL, ULC.

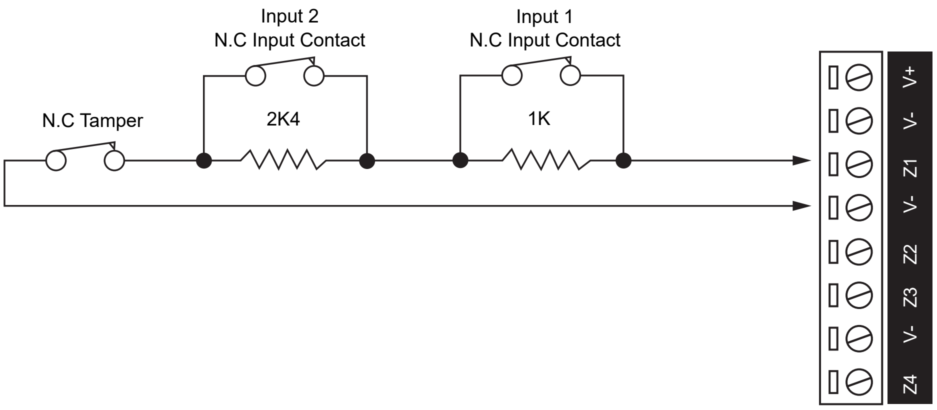
Duplex Inputs

The controller is able to support up to 16 inputs when duplex mode is enabled.

To enable this feature, check the **Duplex Inputs** option in **Sites | Controllers | Options**.

In addition, you will need to manually add additional inputs with addresses 9-16 in **Programming | Inputs**.

Duplex Input Configuration



The following table indicates the position and resistor configuration corresponding to each input address:

Input Address	Position	Resistor
1	Z1	1K
2	Z1	2K4
3	Z2	1K
4	Z2	2K4
5	Z3	1K
6	Z3	2K4
7	Z4	1K
8	Z4	2K4
9	Z5	1K
10	Z5	2K4
11	Z6	1K
12	Z6	2K4
13	Z7	1K
14	Z7	2K4
15	Z8	1K
16	Z8	2K4

Enabling duplex inputs will not change the programming of any existing inputs. These must be reprogrammed or rewired to match the new addressing scheme.

Trouble Inputs

Each controller can monitor up to 64 local 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 table details the trouble inputs that are configured in the controller and the trouble type and group that they activate.

Input Number	Description	Type	Group
CP001:01	Reserved	-	-
CP001:02	12V Supply Failure	Power Fault	General
CP001:03	Reserved	-	-
CP001:04	Real Time Clock Not Set	RTC/Clock Loss	General
CP001:05	Service Report Test	-	-
CP001:06	Service Report Failure to Communicate	Reporting Failure	General
CP001:07	Phone Line Fault	Phone Line Lost	General
CP001:08	Auxiliary Failure	Power Fault	General
CP001:09	Bell Cut/Tamper	Bell/Output Fault	General
CP001:10	Reserved	-	-
CP001:11	Bell Current Overload	Bell/Output Fault	General
CP001:12	Reserved	-	-
CP001:13	Module Communication	Module Loss	System
CP001:14	Module Network Security	Module Security	System
CP001:15	Reserved	-	-
CP001:16	Reserved	-	-
CP001:17	Reserved	-	-
CP001:18	Reserved	-	-
CP001:19	Reserved	-	-
CP001:20	Ethernet Link Lost	Hardware Fault	System
CP001:21	Reserved	-	-
CP001:22	ModBUS Communication Fault	Hardware Fault	System
CP001:23	Protege System Remote Access	Hardware Fault	System
CP001:24	Installer Logged In	Hardware Fault	System
CP001:25	Reserved	-	-
CP001:26	Reserved	-	-
CP001:27	Reserved	-	-
CP001:28	Reserved	-	-
CP001:29	System restarted	Hardware Fault	System
CP001:32	3G Modem Link Lost	Hardware Fault	System
CP001:33	Controller Group Link Lost	Hardware Fault	System
| | | |	| |	|	|
CP001:64	Reserved	-	-

CP001:33 Controller Group Link Lost is not evaluated by UL, cUL, ULC.

Outputs

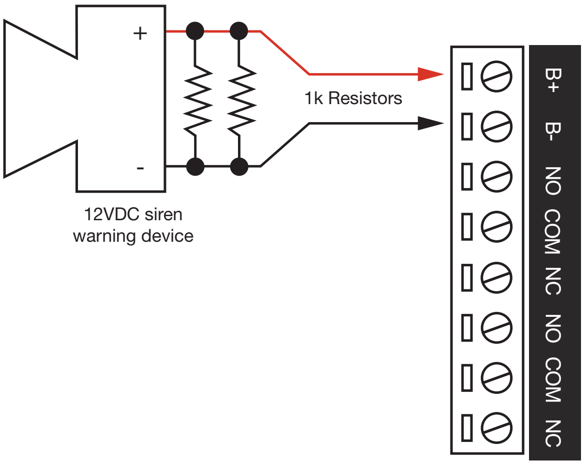
The controller has 7 onboard outputs. These outputs are used to activate bell sirens, lighting circuits, door locks, relay accessory products and other automation points. The first output on the controller has a special hardware design that allows it to monitor for fault conditions and is ideally suited to driving sirens or warning devices.

Bell/Siren Output

Not investigated by UL/ULC for local burglary applications.

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.

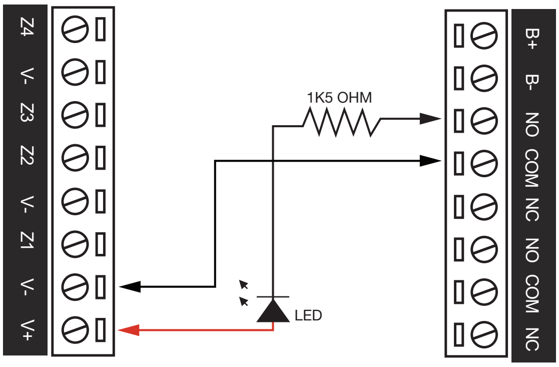


If the load on the bell terminals returns to normal, the controller reinstates power to the bell terminals on the next transition of the output.

When the bell output is not used, the appropriate trouble input will be activated. This can be avoided by connecting a 1K resistor (provided in the accessory bag) 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

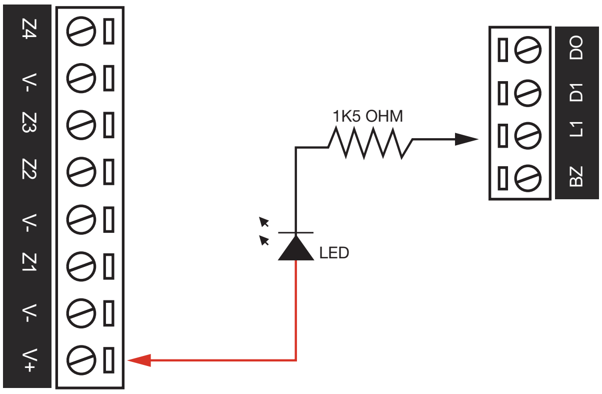
The relay outputs (CP001:03 and CP001:04) on the controller are Form C relays with normally open and normally closed contacts. These outputs can be used to activate larger relays, sounders and lights, etc.



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.



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

Configuration

Configuring a Controller via the Web Interface

The controller's built-in web interface allows you to configure specific settings in order to get the controller online with a Protege GX server. These settings include:

- IP addressing – IP address, subnet mask, gateway and DNS settings
- Event server addresses
- Event, control and download port settings

In addition, you can update the controller firmware and/or the firmware of connected expander modules from this interface, and control operator access to the controller.

When the controller is connected to the computer's network, the web interface can be accessed by entering its current IP address into the address bar of a browser, then logging in with valid credentials for that controller.

Protege controllers come equipped with a factory loaded HTTPS certificate, ensuring a secure encrypted web connection. This means HTTPS must be used when accessing the web interface (e.g. https://192.168.1.2). The factory loaded HTTPS certificate is a self-signed certificate, so when connecting to the controller's web interface a certificate warning may be displayed, but your connection is still secure.
For older controllers not equipped with a default certificate, HTTP must be used to connect to the interface.

Logging In for the First Time

When using Safari, ensure that private browsing mode is disabled. This applies to all versions of Safari: Mac, iPad and iPhone. If private browsing mode is enabled an error message prompts you to disable it.

To log in to the controller for the first time, open a web browser and enter the default IP address of **192.168.1.2** with the prefix https:// (e.g. https://192.168.1.2).

If you cannot access the controller with this URL, remove the https:// prefix and try again (e.g. 192.168.1.2).

If you are presented with a security warning when accessing the HTTPS web page, use the advanced options to proceed to the controller web page.

Once you connect to the controller's web interface you will be prompted to create the admin operator, which is the default login for accessing the web interface.

Creating the Admin Operator

The controller's factory default settings do not contain a default operator. When a controller is first connected or has been factory defaulted you will be prompted to **Create Admin Operator**. The admin operator must be added before the controller can be accessed and configured through the web interface.

Earlier versions of the controller firmware have a preconfigured admin operator. If you are not prompted to create a new operator you can log in using the default username admin with the password admin.

1. **Add a Username** for the admin operator. This does not need to be 'admin'.
2. **Choose a Password** for the admin operator. The password cannot be blank or 'admin'.
3. **Verify Password**.

A very secure password is recommended for the admin operator (see Creating a Secure Password).

Creating a Secure Password

When creating or changing the admin operator password it is **highly recommended** that you create a very secure password.

As a guideline, a secure password should include these features:

- Minimum 8 characters in length
- Combination of upper and lower case letters
- Combination of numbers and letters
- Inclusion of special characters

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.

1. Log in to the controller web interface and navigate to **Settings**.
2. Enter the required settings:
   - **Use DHCP**: When the option is enabled, the controller will use DHCP to dynamically allocate an IP address instead of using a static IP address.

     To use this feature, there must be a DHCP server on the network you are attempting to connect to.
   - **IP Address**: This is the IP address that the controller is currently using. 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 **192.168.1.254**.

     Set this field to **0.0.0.0** to prevent any external communication.
3. Click **Save**.
4. Click **Restart** to restart the controller and implement the changes.

Programming the IP address, subnet mask, and default gateway requires knowledge of the network and subnet that the system is connected to. You should always consult the network or system administrator before programming these values.

Setting Up Integrated DDNS

DDNS (Dynamic Domain Name Server) is a method which allows you to create a static hostname even when the external IP address of the controller is not fixed. The controller contains an integrated DDNS client which automatically updates the DDNS provider whenever the IP address changes.

Controllers currently support two DDNS providers: Duck DNS (free provider) and No-IP (free accounts available, paid plans for further services).

In order to set up DDNS, the controller must be port forwarded so that it is externally accessible.

Setting Up Duck DNS

Duck DNS can be used for HTTPS certification via third-party certificates.

1. Browse to Duck DNS and create a free account by signing in with Google or another existing account. Take note of the **Token** that is generated when you create your account.
2. Create a new **subdomain**. The full hostname will have the form [subdomain].duckdns.org.
3. The **Current IP** field should automatically populate with the external IP address of your network. Ensure that this is the controller's externally accessible IP address.
4. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
5. Navigate to the **System Settings** and select the **Enable DDNS** checkbox.
6. Enter the **Hostname** [subdomain].duckdns.org and **DDNS Server** duckdns.org.
7. Leave the **DDNS Username** blank. For the **DDNS Password**, enter the **Token** generated by your Duck DNS account.
8. **Save** your settings.
9. Confirm that the controller is externally accessible by browsing to the hostname on another PC.

   If the controller's external port is not the default port, you will need to append the port number to the URL (e.g. controller.duckdns.org:1000).

Setting Up No-IP

The free No-IP Dynamic DNS service does not support third-party certification. This is only supported with the additional Plus Managed DNS service.

1. Browse to No-IP and create a **Dynamic DNS** account (free or paid as required).

   Free Dynamic DNS hostnames provided by No-IP require confirmation every 30 days, whereas paid accounts do not.

2. Create a new **Hostname** and select a **Domain**.
3. Ensure that the **IP Address** matches the controller's externally accessible IP address.
4. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
5. Navigate to the **System Settings** and select the **Enable DDNS** checkbox.
6. Enter the **Hostname** and **DDNS Server**.
7. Enter the **Username** and **Password** that you used to sign up to No-IP.
8. **Save** your settings.
9. Confirm that the controller is externally accessible by browsing to the hostname on another PC.

If the controller's external port is not the default port, you will need to append the port number to the URL (e.g. controller.ddns.org:1000).

Setting Up an HTTPS Connection

Protege controllers have HTTPS connection enabled by default with a pre-loaded certificate. However, an alternative certificate can be installed if preferred. Installing a third-party certificate on the controller will remove the security warning which you may see in your browser when accessing a controller with a factory certificate.

For older controllers not equipped with a default certificate, ICT strongly recommends that all live Protege sites establish an HTTPS connection between the controller web interface and the web browser. This is especially important if the controller can be accessed on-site via a router, or externally via the internet.

If the controller is factory defaulted, any user-created HTTPS certificates are removed and the default certificate is reloaded. Custom certificates will need to be reinstalled.

Two different connection methods are available, each of which can be configured directly within the web interface:

- Validating and installing a third-party certificate obtained from a certificate authority.
- Installing a self-signed certificate (recommended for testing only).

For configuration and version requirements refer to AN-314: HTTPS Connection to the Protege GX Controller, available from the ICT website.

Connectivity Requirements for HTTPS

To acquire a third-party certificate for HTTPS connection to the controller's web interface, the controller must be accessible over the internet. This section discusses some of these requirements so that the system can be properly prepared for HTTPS implementation.

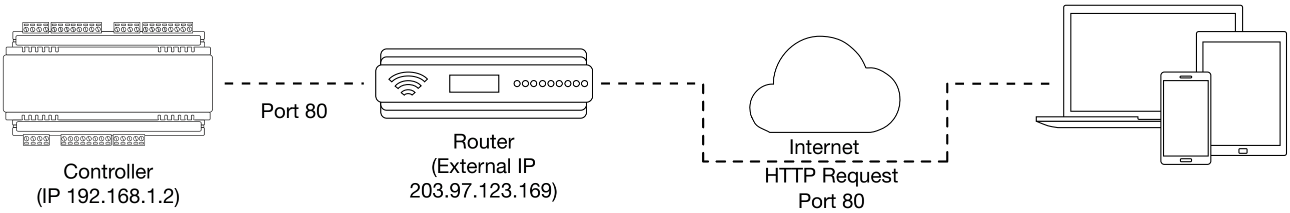
Operating on an active network requires knowledge of the configuration and structure of the network. Always consult the network or system administrator before you begin.

For detailed networking information, see the Protege GX Network Administrator Guide.

Port Forwarding Requirements

In order for the controller to be accessible externally, port forwarding must be configured at the router. Port forwarding is a method of mapping an IP address and port on a local subnet to an external port, so that the networked device is accessible over the internet.

In particular, validating a third-party certificate generally requires the controller to be accessible via **external port 80**. This is the default port for HTTP requests. This external port must be set up to forward traffic to an internal port on the controller that accepts HTTP requests. By default this is **internal port 80**; however, if required this can be changed in the **System Settings**.



Once this port has been forwarded, the controller will be accessible via the external IP address of the network. In this example, typing 203.97.123.169 into an external web browser will open the controller's web interface.

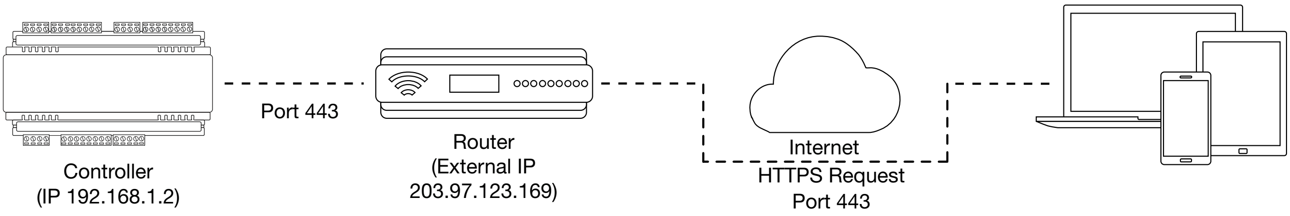
External access via HTTP is only required in order to validate and install your certificate. Once the certificate has been installed, HTTP access will be disabled because the more secure HTTPS connection is available. Therefore it will no longer be necessary to forward external port 80 to the controller.

Port forwarding is configured from the router's utility interface, which can be accessed by browsing to the router's IP address. Different routers have different interfaces, so it is recommended that you consult the documentation for your router.

Optional Port Forwarding

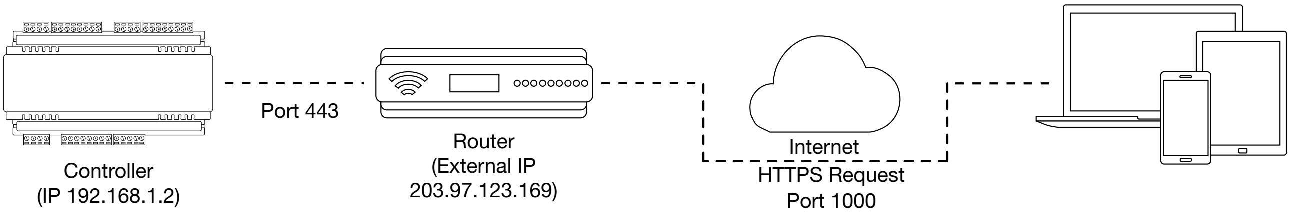
After you have installed a certificate and established an HTTPS connection to the controller, you may wish to continue accessing the controller over the internet. To achieve this, the controller must be accessible via its HTTPS port. The default HTTPS port is **internal port 443**, but this can be changed if necessary in the **System Settings** (available once **Use HTTPS** is enabled).

The easiest method is to configure the router to forward all traffic from **external port 443** (the default HTTPS port) to the controller's internal HTTPS port, as in the image below.



In this case, all traffic directed to the external HTTPS IP address will be forwarded to the controller. The controller's web interface could be accessed by typing https://203.97.123.169 into an external web browser.

However, it is possible to grant external access by forwarding any external port to the controller's HTTPS port. This is especially useful if external port 443 is not available on your network.



In this case, any traffic directed to **external port 1000** will be forwarded to the controller's HTTPS port. The controller's web interface can be accessed simply by appending the external port number onto the end of the URL: e.g. https://203.97.123.169:1000.

Note: If the controller does not have a factory loaded certificate, it will not be accessible via HTTPS until an HTTPS certificate has been installed, regardless of whether port forwarding has been configured.

Controller Default Gateway

In order for the controller to send and receive external communications via the router, its default gateway needs to be set to the router's **internal** IP address.

1. Log in to the controller's web interface and navigate to **System Settings**.
2. In the **Default Gateway** field, enter the IP address of the router.
3. **Save** the configuration and **Restart** the controller.

Note: The default gateway must be set to the router's internal IP address that identifies it on the local internal network, not the external IP address used to connect over the internet.

Mapping an IP Address to a Domain

In order to achieve third-party HTTPS certification, it is necessary to map the controller's externally accessible IP address to a domain. The domain name becomes the **hostname** for the controller: a fixed, human readable point of access to the device.

Domain names can be purchased from Domain Name Registrars and assigned to a **static IP address**, usually for an annual fee. For example, the IP address 203.97.123.169 could be assigned the domain name controller.com, and would then be accessible by typing that domain name into a browser address bar.

However, typically routers are assigned a **dynamic IP address**. This IP address is not static: internet service providers may reassign the address whenever the router is reset or even more frequently. A fixed domain name would have to be constantly monitored and updated, as the IP address it is mapped to will change unpredictably. If necessary, a **static IP address** may be purchased from your internet service provider.

Alternatively, you may use a **Dynamic Domain Name Server (DDNS)**, which allows a dynamic IP address to be mapped to a static domain name. Generally a DDNS service will provide a client application which runs on the web server PC and automatically updates the domain's IP address mapping whenever the external IP address changes. Controllers also have an **integrated DDNS client** which supports several free DDNS providers.

Third-Party Certificate

This method uses a certificate generated by a recognized third-party certificate authority (CA) to encrypt the HTTPS connection. Unlike the self-signed certificate method, third-party certificates generally require an annual fee; however, they are trusted by web browsers.

The process has five main stages:

1. The installer generates a private/public encryption key pair and certificate signing request for their domain.
2. The installer purchases a certificate and submits the certificate signing request to the certificate authority.
3. The certificate authority provides a validation file which is loaded onto the controller.
4. The certificate authority validates the domain and provides the certificate.
5. Finally, the installer converts the certificate format (if necessary) and installs the certificate onto the controller.

Requirements for Third-Party Certificates

- The controller must be exposed to the internet via external port 80.
- The controller must be externally accessible via a hostname.

  Either static IP or DDNS (see page 33) can be used to assign this hostname.

- The operator must renew the certificate whenever it expires.
- Different certificate authorities may have different requirements. For example, some CAs do not require manual validation of domain names, allowing you to skip the certificate authentication stage. It is recommended that you carefully note all requirements for your chosen CA before beginning.

IT support should be consulted when obtaining and loading a third-party certificate. ICT Technical Support cannot assist with this process.

Creating a Private Key and Certificate Signing Request

To begin, it is necessary to generate the private/public encryption key pair which will be the basis for the HTTPS encryption. The public key will be integrated into a certificate signing request which will be submitted to the CA.

The following instructions will use the free OpenSSL utility. The latest version of OpenSSL for Windows can be downloaded from this page.

1. Download and install the OpenSSL utility.
2. Navigate to the installation directory, open the **bin** folder, locate the **openssl** executable and run it as an administrator. This will open the OpenSSL command prompt.
3. To **generate the key pair**, enter the following command, replacing `[name]` with your desired filenames:

   ```
   req -newkey rsa:2048 -keyout [name].key -out [name].csr
   ```

   This generates a new 2048-bit private key (.key file) and certificate signing request (.csr file). The files should appear in the current OpenSSL directory.
4. Enter a **passphrase** for the private key. This is a phrase used to encrypt the private key to protect it against anyone with access to your local system. It will be required whenever the private key is used.

   > Note that passphrase characters will not be displayed in the console. Only alphanumeric characters are supported for the passphrase.

5. Enter your **location and identity information** as requested. These details will be incorporated into your certificate and publicly viewable from the web browser.

   > Ensure that the **Common Name** is the same as the **Domain Name** which is being used for the controller.

   Some details are optional. Confirm with your CA which fields are required.
6. **Save** both files in a safe, known location, as both are required for the following steps. It is especially important that the private key is not publicly accessible.

Purchasing a Certificate

Below are very basic instructions for purchasing a third-party certificate from a CA. Every CA will have different processes and requirements - this is only intended to be a rough guide to what is required for implementation on a controller.

1. Begin the process of generating a certificate from a recognized CA such as:
   - **GoDaddy**: https://nz.godaddy.com/web-security/ssl-certificate
   - **Network Solutions**: https://www.networksolutions.com/
   - **RapidSSL**: https://www.rapidsslonline.com/

   > It is important that you select **File-Based or HTTP-based Validation** (or equivalent) when asked to choose an authentication/validation method. You will require a .txt file to upload to the controller.

2. When prompted, upload the text of your **Certificate Signing Request** (.csr).
3. Follow the CA's instructions to complete the request. You should be prompted to download a **.txt** validation file.

   > **DO NOT** change the name or contents of this file.

Authenticating the Certificate

The .txt file that you received in the previous steps must be uploaded to a known directory on your domain (in this case, the controller) so that it can be viewed by the CA. This verifies that you are the owner of the domain in question.

1. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
2. Navigate to the **System Settings**. If not already enabled, enable the **Use HTTPS** option.
3. Enter an appropriate **HTTPS Port**. The default is port 443, which is commonly used for this purpose. You should retain the default port unless you are required to use another port by your system administrator.
4. Click **Load Validation File** and browse to the .txt validation file to load it onto the controller.
5. Scroll up the page to the **Controller Hostname** field. Enter your controller's Domain Name.

6. Confirm that the file is publicly accessible by using another machine to navigate to [domainname]/.wellknown/pki-validation/[filename].txt. You should be able to view the content of your validation file.

Once the CA has verified that your domain is accessible, you will be sent the signed certificate. Wait times can vary between providers, but will typically take from one hour to several hours.

Converting the Certificate Format

The controller requires a file with the .pfx extension. Your CA may have provided a different file type, potentially several files such as a certificate (e.g. .cer, .crt or .pem) and an intermediate certificate. These must be combined with the private key generated with your certificate request to create a .pfx file. The following instructions will use the OpenSSL utility installed above.

1. Navigate to the installation directory, open the **bin** folder, locate the **openssl** executable and run it as an administrator. This will open the OpenSSL command prompt.
2. **Export** your certificate as a .pfx file using the following command, replacing `[name]` with your filenames:

   ```
   pkcs12 -export -out [name].pfx -inkey [name].key -in [name].[cer/crt/pem]
   ```

   If you have been provided with an intermediate certificate, append to the end of the command:

   ```
   -certfile [intermediatename].cer
   ```

   > Replace `[cer/crt/pem]` with the extension on your certificate file as required.

3. Enter the **passphrase** for the private key (set above) to continue.

   > Note that passphrase characters will not be displayed in the console.

4. Enter an **export password** when requested. This will be required when installing the certificate on the controller.
5. This process will generate a [name].pfx file in the current OpenSSL directory. This is your third-party certificate. Store this file in a safe, known location.

Installing the Certificate on the Controller

1. Access the controller's web interface and log in. Navigate to the **System Settings**.
2. Scroll to the **Certificate File** section. Click **Install Certificate** and browse to the .pfx certificate file to install it on the controller.
3. Enter the **export password** that you created when generating the certificate file.
4. Click **Save**, then **restart the controller** using the button on the top right to implement the new settings.

   > Once the restart process is complete, the controller will restart but the web page will not automatically refresh.

5. Browse to the controller web page by adding the prefix https:// to the beginning of the IP address or URL.

A lock or similar icon in the browser toolbar should indicate that the connection is secure. Click on this icon to see details about the certificate, including the information you entered in the certificate signing request.

Self-Signed Certificate

Self-signed certificates do not require the certificate to be validated by an authority, or for the controller to be accessible over the internet. They can also be created for free. However, self-signed certificates are not considered secure by web browsers, which will generate warnings whenever the web interface is accessed. This method is fine for testing and development but is **not recommended** for live sites.

Requirements for Self-Signed Certificates

- There is no requirement for the controller to be externally accessible.
- The operator must manually renew the certificate whenever it expires.

Generating a Self-Signed Certificate with OpenSSL

The following instructions will use the free OpenSSL utility. The latest version of OpenSSL for Windows can be downloaded from this page.

1. Download and install the OpenSSL utility.
2. Navigate to the installation directory, open the **bin** folder, locate the **openssl** executable and run it as an administrator. This will open the OpenSSL command prompt.
3. To **generate** your certificate, enter the following command, replacing `[name]` with your desired filenames:

   ```
   req -new -newkey rsa:2048 -x509 -sha256 -days 365 -out [name].crt -keyout
   [name].key
   ```

   This generates a new key pair (.cer certificate and .key private key) with 2048-bit encryption that will expire after 365 days. The files should appear in the current OpenSSL directory.
4. Enter a **passphrase** for the private key. This is a phrase used to encrypt the private key to protect it against anyone with access to your local system. It will be required whenever the private key is used.

   Note that passphrase characters will not be displayed in the console. Only alphanumeric characters are supported for the passphrase.
5. Enter your **location and identity information** as requested. These details will be incorporated into your certificate and publicly viewable from the web browser.

   Ensure that the **Common Name** is the same as the **Domain Name** which is being used for the controller, if any.
6. To **export** your certificate, enter the following command, replacing `[name]` with your desired filename:

   ```
   pkcs12 -export -out [name].pfx -inkey [name].key -in [name].crt
   ```
7. Enter the **passphrase** assigned above when prompted.
8. Create an **export password** when prompted. This will be required when installing the certificate on the controller.

   This process will generate a [name].pfx file in the current OpenSSL directory. This is your self-signed certificate. Store this file in a safe, known location.

Installing the Self-Signed Certificate to the Controller

1. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
2. Navigate to the **System Settings**. If not already enabled, enable the **Use HTTPS** option.
3. Enter an appropriate **HTTPS Port**. The default is port 443, which is commonly used for this purpose. You should retain the default port unless you are required to use another port by your system administrator.
4. Click **Install Certificate** and browse to the .pfx certificate file to install it on the controller.

   No .txt validation file is required for this method, as the connection is not validated by a third party.
5. Enter the **export password** that you created when generating the certificate file.
6. Click **Save**, then **restart the controller** using the button on the top right to implement the new settings.

   Once the restart process is complete, the controller will restart but the web page will not automatically refresh.
7. Browse to the controller web page by adding the prefix https:// to the beginning of the IP address or URL.

When using a self-signed certificate, you will likely be presented with a security warning if you attempt to access the HTTPS web page. The connection is still encrypted, but the browser has flagged the certificate as untrustworthy as it lacks third-party validation.

Signing In

To access the system after the initial setup you need to sign in with a valid operator username and password.

1. Open a web browser and enter the controller's IP address, with the prefix https:// (e.g. https://192.168.1.2).

   If you cannot access the controller with this URL, remove the https:// prefix (e.g. 192.168.1.2).

2. If you are presented with a security warning when accessing the HTTPS web page, use the advanced options to proceed to the controller web page.
3. The **Sign In** window is displayed.
4. Enter your operator **Username** and **Password**.
5. Click **Sign In**.

Repeatedly entering incorrect passwords at the sign in window forces a login stand down. Three consecutive incorrect attempts will result in the sign in process being locked for 5 seconds. If another three attempts fail, the sign in process is locked for 60 seconds between all subsequent attempts until a valid login is made. It is not possible to configure the length of time for the login stand down.

Home Page

Controller Status

- **Health**: Displays the health status of the controller.
- **Voltage**: Shows the voltage passing through the controller.
- **Memory Usage**: Shows the current memory usage of the controller, along with a breakdown of what that memory is being used for.
- **Status**: Displays the current serial number of the controller.

Operator Details

- **Logged on as**: Shows the username of the current operator.
- **Logged on at**: Shows the time and date this operator logged in.

Options

- **Display Theme**: Switch between the dark (dark background, white text) and light (white background, dark text) display themes for the web interface.
- **Display Color**: Select the display color used for the web interface. This selection will persist whenever this operator logs in to the controller with the same web browser.
- **Logout**: Log out and return to the login screen.
- **Change Password**: Change the password used by this operator.

System Settings

This page can be saved or refreshed using the toolbar buttons in the top right. The **Restart** button can be used to reboot the controller, which is required to apply any changes to the fields marked with an asterisk *****.

- **Name**: Equivalent to the **Panel Name** in the Protege GX software. This name is currently not configurable via the controller web interface.
- **Serial Number**: The serial number of the controller.
- **HTTP Port***: The default port is 80. This can be changed to any network port that is not occupied.

  IMPORTANT: If this field is set to no value (which is converted to an invalid 0 value), the controller will no longer be accessible via the web interface and will require defaulting the IP address in order to connect.

- **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. The **Dynamic IP Address Update** option must also be enabled for this controller in Protege GX (**Sites | Controllers | General**).

  When DHCP is enabled, the IP information below will not be updated and so will continue to display the last static IP configuration.

- **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 **192.168.1.254**. Set this to **0.0.0.0** to prevent any external communication.
- **DNS Server***: The IP address of the DNS server being used by the controller. This is required if a DNS name is being used to connect to the event server below.
- **Event Server 1***: The IP address or DNS name of the event server.
- **Event Server 2/3***: Alternative paths to the event server (optional).
- **Event Port***: The default port is **22000**. This must match the port defined in **Global | Event Server** in the Protege GX software.
- **Download Port***: The default port is **21000**. This must match the port defined in **Sites | Controllers | General** in the Protege GX software.
- **Control Port***: The default port is **21001**. This must match the port defined in **Sites | Controllers | General** in the Protege GX software.

Hostname

- **Hostname**: If the controller is accessible via an external hostname it can be entered here.

  This is only required if the DDNS or HTTPS options (below) are being used.

Dynamic DNS

- **Enable DDNS**: The controller has an in-built DDNS (Dynamic Domain Name Server) application, which allows it to dynamically connect to an external hostname even if its external IP address is not static. Check this checkbox and enter the required details to activate DDNS.
- **DDNS Server**: Enter the name of the DDNS server which is being used. Currently Duck DNS (www.duckdns.org) and No-IP (www.noip.com) are supported DDNS providers.
- **DDNS Username/Password**: Enter the required credentials for your DDNS provider.
  - **Duck DNS**: The username should be left blank. The password is the **Token** generated by your Duck DNS account.
  - **No-IP**: The username and password are the credentials used to log in to your No-IP account.

HTTPS

Protege controllers have HTTPS connection enabled by default with a pre-loaded certificate. However, an alternative certificate can be installed if preferred.

For older controllers not equipped with a default certificate, ICT strongly recommends that all live Protege sites establish an HTTPS connection between the controller web interface and the web browser. This is especially important if the controller can be accessed onsite via a router, or externally via the internet.

If the controller is factory defaulted, any user-created HTTPS certificates are removed and the default certificate is reloaded. Custom certificates will need to be reinstalled.

- **Use HTTPS**: ICT controllers come preconfigured with a pre-loaded certificate and HTTPS enabled by default, however an alternate certificate can be installed if preferred.
- **HTTPS Port***: The default port is **443**. This can be changed to any port that is not occupied.
- **Use HTTPS Certificate**: This option will be illuminated when Use HTTPS is selected, to signify that HTTPS is enabled. The HTTPS certificate can be the default factory certificate, a third-party certificate obtained from a Certificate Authority, or a self-signed certificate.
  - **Load Validation File**: Click to browse and upload a validation file (.txt format) provided by the Certificate Authority. This will be used by the CA to validate your domain name. Validating the domain this way requires your controller to be externally accessible via a hostname on external port 80.

    This step is not required when installing a self-signed certificate.
  - **Install Certificate**: Click to browse and upload an HTTPS certificate in .pfx format. If the file is secured with an export password you will be prompted to enter it. **Restart the controller** to implement or update HTTPS.

Operators

Operators can be created, deleted and saved using the toolbar buttons at the top right. Note that these are operators for the controller's web interface and do not correspond to operators in the Protege GX software.

- **Name**: A name for the operator record in the web interface.

Configuration

- **Username/Password**: The operator's login credentials for the controller's web interface.
- **Change Password**: Click this button to change the password of the operator. It is recommended that you give each operator a secure password (see below).
- **Default Language**: Select a default language for the operator. This language will be displayed when the operator uses the web interface.

Operator Timeout

- **Enable Operator Timeout**: When this option is enabled, the operator will be automatically logged out of the web interface after a defined period of inactivity.
- **Operator Timeout**: Set the length of time in minutes before the operator will be automatically logged out.

Application Software

Controller Software

- **Current Version**: Displays the current firmware version of this controller. Click on this field to display further version information.

Update Application Software

- **BIN File**: This section is used to update the firmware of the controller. Click **Upload** to browse to the firmware file (.bin format) supplied by ICT, and open the file to install the new firmware on the controller.

  This process will take approximately 10 minutes and the controller will not be able to perform its normal functions during this period. It is recommended that firmware updates are performed when the site is closed for maintenance or at times of low activity.

Updating Modules with RS-485 Readers Connected

Important: Prior to starting a firmware update on any module with readers connected (wired) to its reader ports in RS-485, it is strongly recommended to physically disconnect the readers from the ports. This applies to all controllers and reader expanders with RS-485 readers physically connected to their reader ports. When a reader sends data to a reader port it can potentially stop the firmware update and leave the module stuck in boot mode. Physically disconnecting the readers alleviates the possibility of the firmware update failing due to the expander/controller receiving a packet on the RS-485 line while the update is in progress.

Update Module Firmware

- **Module**: This section is used to update the firmware of any module connected to the controller. Select the connected module that requires a firmware update from the dropdown.
- **BIN File**: Click **Upload Firmware** to browse to the firmware file (.bin format) supplied by ICT, and open the file to install the new firmware on the selected module.

Warning: Updating module firmware will put the entire network into maintenance mode, preventing normal activity for the duration of the update process. Module firmware **must not** be updated remotely.

Force Update

In situations where a module becomes stuck in the bootloader mode and the application is not running, it may become necessary to perform a force update.

This hidden feature in the Update Module Firmware section of the web interface provides the ability to update module firmware on an inoperable module where it is not possible through the regular update process.

Clicking **Module** will expand the hidden section, making the **Force Update** panel available.

1. Select the **Force Update - Module**, carefully selecting the module type and model.
2. Select the **Force Update - Address**, which is the configured **Physical Address** of the module.
3. The **Skip Verification** option will bypass the firmware check and allow firmware that does not match the module type of the module to be loaded.

   This option should only be selected at the direction of ICT Technical Support .

4. Click **Upload Firmware** to browse to the firmware file (.bin format) supplied by ICT, and open the file to install the firmware on the selected module.

Note: The maximum address that can be selected for force update is 32. If the module has an address greater than 32 it cannot be upgraded via this method. You will need to contact ICT Technical Support for assistance.

Configuring a Controller via the Protege GX Software

To add a controller to the Protege GX system, navigate to **Sites | Controllers** and click **Add**. Several options are available, allowing you to define which records will be created alongside your controller.

- **Use the Controller Wizard**: The controller wizard allows you to specify the inputs, outputs, doors and expander modules that are required by your site. Some additional options can also be configured. The selected default records are automatically added to the database with the controller.
- **Just add a Controller**: Only the controller record itself is added to the database. All other records must be programmed separately.
- **Add new controller based on an existing controller**: The controller record and all connected programming are duplicated from an existing controller. This includes devices such as expander modules, inputs, outputs and doors.

  It may be convenient to create a 'template' controller record as a base for adding new controllers.

Once the controller record has been created, bring it online by entering the **Serial Number**, **IP Address**, **Download Port**, **Download Server** and **Control and Status Request Port** in the **General** tab. If the controller does not come online, you will need to troubleshoot the connection (see page 55).

Adding a Controller with Default Records

When you select **Use the Controller Wizard**, the **Add Controller** configuration window is displayed. This allows you to automatically add default records (inputs, outputs, expander modules, doors) alongside the controller. The records have default names and settings, and can be renamed, edited or deleted as required.

General

- **Name**: The name of the controller in the Protege GX software.
- **Count**: The number of controllers that will be added with the same default records. If more than one controller is added the subsequent controllers will be assigned default names that can be edited later.
- **Prepend Controller name to added records**: When this option is enabled, all new records generated by the wizard will include the controller name at the start of the record name. For example, if the controller is named Office, the first output on the controller will have the name Office CP1 Bell 1.

Controller

- **Type**: The model code of the controller that is being added to the system. This is displayed on the upper right of the controller face.
- **Inputs**: The number of onboard inputs that will be created for the controller. This is set automatically based on the **Type** of controller selected.

  Not all controller inputs may be required if the onboard reader expander is being used, as the inputs can be assigned to the reader expander record.
- **Outputs**: The number of onboard outputs that will be created for the controller. This is set automatically based on the **Type** of controller selected.

  This number includes only the bell and relay outputs (outputs 1, 3 and 4). Reader outputs are assigned to the onboard reader expander record (even if not used for connected readers).

  Controller output 2 only exists on legacy hardware. This address is skipped when the wizard automatically adds the default records.
- **Add Trouble Inputs**: Enable this option to automatically add the trouble inputs associated with the controller.

Keypads, Input Expanders, Reader Expanders, Output Expanders and Analog Expanders

Enter the **Type** and number of each expander module that should be added to this controller. The number of inputs and outputs required should be set automatically. Enable **Add Trouble Inputs** to include the trouble inputs for each module.

If the controller's onboard reader expander is being used it should be included in the number of reader expanders so that the relevant programming can be created.

Options

- **Create "Installer" Menu Group**: Creates a menu group with every menu enabled for use by site installers.
- **Create Floor Plan**: Creates a floor plan including all inputs and outputs on the controller. This is useful for small sites with only a few inputs and outputs. For larger sites it is generally better to create the floor plans manually.
- **CID Report Map**: The Contact ID report map that will be used for assigning the **Reporting ID** to each input. The options are:
  - **Standard**: Suitable for small burglary and access control installations.
  - **Large**: Suitable for intrusion detection installations with a large number of input expanders.
  - **SIMS II**: A variant of the Contact ID format which can send a much larger number of inputs. For this mapping to function correctly the service must also be configured for SIMS II by setting the **Cid Mapping** option for a Contact ID service, or the **CID Map Settings** option for a Report IP service.

  For more information, see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.

Doors

- **Doors**: Automatically creates the defined number of door records. Typically this should be 2 doors per reader expander.
- **Assign to Reader Expanders**: Automatically assigns the doors to reader expander ports, in order of creation.
- **Add Door Trouble Inputs**: Creates the relevant trouble inputs for each door record.
- **Assign Reader Lock Output to Door Configuration**: Automatically sets the **Lock Output** for each door to the relay output on the associated reader expander.
- **Assign Reader Beeper to Door Alarm Configuration**: Automatically sets the **Pre Alarm Output**, **Left Open Alarm Output** and **Door Forced Output** for each door to the beeper output on the associated reader expander.

Adding a Controller Based on an Existing Controller

When you select **Copy an existing Controller**, the **Copy Controller** configuration window is displayed. This allows you to select the controller to copy, and configure some options.

The copied records include inputs, outputs, doors, areas and groups associated with that controller.

The new controller record will have a blank **Serial Number**, **IP Address** and **Download Server**.

- **Site (Copy From)**: Defines the site that the programming will be copied from.
- **Controller (Copy From)**: Defines the controller that the programming will be copied from.
- **New Controller Name**: The name of the new controller in the Protege GX software.
- **Name (Second Language)**: The name of the new controller in the second language.
- **Prepend Controller name to all record names**: When this option is enabled, all new records generated by the copy process will include the new controller's name at the start of the record name. This means all new records will have the same name as those on the original controller, with the new controller's name added.

> If the original records included the controller's name, this name will still be included in the new records (i.e. will not be replaced by the new name).

- **Copy Access Levels**: When this option is enabled the access levels of the original controller are copied for the new controller. The new access levels are assigned the equivalent doors, areas and other records from the new controller, but are not assigned to any users.
- **Copy Global Records**: When this option is enabled, site-wide records such as schedules and function codes will be copied for use with the new controller.

Configuring a Controller

Once added, the controller needs to be configured to define settings including the serial number and communication parameters.

Controllers | General

General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (Second Language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Record Group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

Communications

- **Serial Number**: The serial number of the controller. This can be obtained from the configuration page of the built-in web interface, or the label on the side of the controller.
- **IP Address**: The IP address of the controller. The default IP address is 192.168.1.2, which can be changed via the built-in web interface.

  In general the IP address should be the same here and in the controller web interface. Alternatively, if the controller is external to the server network you may need to enter the external IP address of the router which is forwarding traffic to the controller.

  > Programming the IP address, subnet mask, and default gateway requires knowledge of the network and subnet that the system is connected to. You should always consult the network or system administrator before programming these values.

- **Dynamic IP Address Update**: When this option is enabled the software automatically detects the IP address of the controller from incoming messages and updates the **IP Address** field automatically. Use this for situations where the controller's IP address may change unexpectedly, or when the controller is configured to use DHCP.
- **Username / Password**: If the single record download service is in use, you must enter a username and password for the controller so that the service can make a connection. These must match an operator in the controller's web interface.
- **Download Port**: The TCP/IP port that is used by the download service to send programming downloads to the controller. By default, this is port 21000.
- **Single Record Download Port**: The TCP/IP port that will be used by the single record download service (if in use) to send programming downloads to the controller. This should match the **HTTPS Port** of the controller. By default, this is port 443.
- **Download Server**: Defines the download server which will send downloads to the controller. If this field is <not set> the controller will not receive any downloads.

- **Control and Status Request Port**: This field specifies the port that will be used to send manual commands and status requests to the controller over TCP/IP. By default, this is port 21001.
- **Last Known IP Address**: Shows the last IP address that the controller used to communicate with the server (read only).
- **Last Downloaded**: Shows the date and time of the last download to the controller (read only).

Display

- **Panel Name**: The name used to identify the controller to IP reporting services.

Diagnostic Windows

- **Open Download Server Diagnostic Window**: Opens a window listing transactions between the controller and the download server. This can be useful for checking whether recent programming changes have been downloaded successfully.
- **Open Event Server Diagnostic Window**: Opens a window showing the current status of the event server. This can be useful for diagnosing controller connection issues.

Commands

- This field is used to send programming commands to the device. It should only be used when specifically advised by ICT documentation or technical support.

Download Binary Blob

- **Set the download binary blob from a file**: This feature allows you to select a binary blob file and download it to the controller. This is required for some specific transitions and integrations.

  Do not use this feature unless specifically advised by ICT.

- **Database Data Length (bytes)**: The size of the file that has been selected for download.

Record History

Each record displays its programming history, including the time and date it was created, the time and date it was last modified and the operator who last modified it.

Controllers | Configuration

Configuration

- **Test Report Time (HH:MM)**: The controller periodically tests the reporting service by opening the predefined Service Report Test trouble input. This field sets the time of day the trouble input will be opened.

  When the **Test Report Time is Periodic** option is enabled in the **Options** tab, 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**: The time of day when the controller will update the users and other offline parameters on legacy intelligent expander modules. The **Enable Automatic Offline Download** option must be enabled. This option is not used for DIN rail modules.
- **AC Restore Delay Time**: The time, in seconds, that the AC Failure trouble input will remain open after an AC failure before restoring. This setting is only relevant to legacy hardware which is supplied by an AC power source.
- **AC Fail Time**: The time, in seconds, that the AC mains voltage must have failed before the AC failure trouble input will be opened. This setting is only relevant to legacy hardware which is supplied by an AC power source.

- **Module UDP Port**: Some modules, such as the Protege Module Network Repeater, can communicate with the controller over an ethernet connection using the UDP protocol. This field defines the UDP port that will be used for these communications. The default port is 9450. If this port is changed at the controller it must also be updated at all relevant modules.

  From controller firmware version 2.08.886 module UDP/TCP communications are disabled by default. You can re-enable communications by entering the following commands in the **Commands** field (**General** tab): `EnableModuleUDP = true` and `EnableModuleTCP = true`.

- **Modem Country**: This option affects the number of dial attempts made by phone line reporting services, and may override the **Dial Attempts** setting in the reporting service. It is recommended to test the number of dial attempts to ensure that you comply with regional requirements.
- **Modem Backup Phone Number**: If ethernet communication fails, the controller's onboard modem will dial this number to report events. The **Module Backup if IP Fails** option must be enabled (**Options** tab).
- **Default Language**: The default language displayed on the keypad for users who have no language selected and for any events generated by a serial printer service (see **Programming | Services | Serial Printer**).
- **Download Retry Delay**: This is a legacy option that has no effect.
- **Register as Reader Expander**: The module address assigned to the controller's onboard reader expander. You can program the onboard reader expander by creating a record with the same address in **Expanders | Reader Expanders**.

  This address must not be the same as that of any physical reader expander.

- **Onboard Reader Lock Outputs**: This option determines which outputs on the controller are mapped to the onboard reader expander's lock outputs. This should generally be set to Controller Relay 3/4 Outputs, which maps controller outputs 3 and 4 to reader expander outputs 1 and 2. If the controller is not being used for door control this option may be set to None.
- **Touch Screen UDP Port**: The UDP port that a Protege Touchscreen will communicate over.

  From controller firmware version 2.08.886 touchscreen communications are disabled by default. You can re-enable communications by entering the following command in the **Commands** field (**General** tab): `EnableTLCDCommsUDP = true`.

- **Maximum Packet Size**: The maximum packet size that can be downloaded to the controller.
- **Controller Offline Grace Time (Minutes)**: If a controller drops offline there is a fixed grace period of 1 minute before Protege GX begins indicating that the controller is offline. This option allows you to extend this grace period by a number of minutes. This should be used in situations where the controller periodically drops offline and comes online again, allowing you to avoid unnecessary alerts.

Encryption

- **Initialize Controller Encryption**: Enables encryption of the messages sent between the controller and the Protege GX server. Selecting this option initiates a one-off process that randomly generates a 256 bit AES encryption key. Using an RSA algorithm, this key is exchanged and stored in both the controller and the Protege GX database.
- **Disable Controller Encryption**: Instructs the software to stop using encryption. To prevent encryption from being disabled accidentally or maliciously, this option will not change the encryption setting in the controller itself. You must hardware default the controller to fully disable encryption and allow communications.
- **Encryption Enabled**: Read only field that indicates whether encryption is enabled.

HTTPS Public Key

- **HTTPS Public Key**: If the single record download service is in use this field displays the public key of the controller's HTTPS certificate. This is automatically populated when the single record download service connects to the controller for the first time. If the certificate is changed or the controller is defaulted you must delete the information in this field to allow the single record download service to reconnect.

Version 3 Settings

This section displays settings which were used in software version 3 and earlier. These settings do not require configuration in version 4 or later.

Controllers | Options

Options

- **Test Report Time is Periodic:** When this option is enabled the **Test Report Time** set in the **Configuration** tab will be treated as a frequency rather than a time of day. For example, a Test Report Time of 12:00 AM will cause the Service Report Test trouble input to be opened every 12 hours if this option is enabled, or every day at 12AM if this option is disabled.
- **Weekly Test Report**: When this option is enabled the test report is sent once a week based on the day of the week selected. The Service Report Test trouble input will be opened at the time specified in the **Test Report Time** field in the **Configuration** tab. When this option is disabled the trouble input will be opened once a day.
- **Day of the Week**: Defines the day of the week that the weekly test report is sent.
- **Troubles Require Acknowledge**: System troubles are displayed in the trouble view menu of the keypad (**[Menu] [5] [2]**). Normally if the trouble condition ends (i.e. the trouble input closes) the trouble is no longer included in this list; however, with this option enabled the trouble condition remains in the list until it is acknowledged by an authorized user.

  Users must have **Acknowledge System Troubles** enabled in **Users | Users | Options** and access to the **View (5)** menu from their menu group.

- **Generate Input Restore On Test Report Input**: When this option is enabled the controller will generate a restore event for the Service Report Test trouble input closing after the regular test report. This occurs one minute after the Service Report Test trouble input has been activated.
- **Report Short Duration Module Communication Failure**: When this option is enabled the controller will always generate trouble events for any module communications failure, without allowing any grace period for the module to come back online.
- **Advance UL Operation**: When this option is enabled the Protege GX system runs in UL compliance mode.

  This setting has the following effects:

  - Adds a 10 second grace period following a failed poll before a module is reported as offline.

    Each module sends a poll message to the controller every 250 seconds. The module will be reported as offline if no poll has been received for the duration of this poll time plus the 10 second grace period.

  - Suppresses reporting of all alarms and/or reportable events to a monitoring station within the first two minutes of the controller powering up. The system will continue to send poll messages as usual.
  - Reports 'Input Tamper' events as 'Input Open' events when the area that the input is assigned to is armed. If the area is disarmed an 'Input Tamper' message will be sent.
  - Limits the **Dial Attempts** for reporting services to a maximum of 8.

  This setting must be used in conjunction with the other configuration requirements in the controller installation manual.

- **Duplex Inputs**: With this option enabled the controller can support twice the number of inputs, wired in duplex configuration. For more information, see the relevant controller installation manual.

Misc Options

- **Enable Automatic Offline Download**: When this option is enabled the controller will automatically update the users and other offline parameters on legacy intelligent expander modules at the **Automatic Offline Time** (**Configuration** tab). This option is not used for DIN rail modules.

- **Modem Backup if IP Fails**: When this option is enabled the controller will dial out through the onboard modem if it cannot connect to the software via ethernet to report events. The **Modem Backup Phone Number** must be set in the **Configuration** tab.
- **Backup Only Alarm Events**: With this option enabled, when the controller has lost ethernet connection it will only report alarms and other reportable events over the phone line. All stored events will be reported when the ethernet link is restored.
- **Invert Controller Tamper Input**: When this option is enabled the controller will invert the module tamper input allowing a normally open tamper switch to be used. This setting is only relevant to older hardware which includes an onboard tamper input.
- **Log All Access Level Events**: This is a legacy option that has no effect.
- **Do Not Wait for Dial Tone When Modem Dials Out**: When this option is enabled, modem dialing occurs even when no dial tone is detected.

Controllers | Time Update

When using a time server the time provided is always in UTC (Coordinated Universal Time), which has no time zone and is not subject to any daylight saving time rules. This means that you must correctly configure the time server, the time zone that the controller is operating in, and the daylight savings settings for the time to be synchronized correctly. Failure to configure any of these will result in the time being inaccurate.
Daylight savings settings can be configured in **Programming | Daylight Savings**.

- **Automatically Synchronize with an Internet Time Server**: Select this option to automatically synchronize the controller's internal clock with an internet time server.
- **Primary SNTP Time Server**: The IP address of the primary SNTP time server that the controller will use to update its time.
- **Secondary SNTP Time Server**: The IP address of the secondary (backup) SNTP time server that the controller will use to update its time. This time server will be used if the controller cannot connect to the primary server.
- **Time Zone**: The current time zone that the controller is stationed in. Each time zone is described via its offset from GMT and relevant regions.

Controllers | Custom Reader Format

This tab allows you to define a custom reader format (Wiegand or Magnetic) which is available for use by reader expanders connected to the controller. To use this format, set the **Reader Format** (**Expanders | Reader Expanders | Reader 1/2**) to Custom Format.

See **Sites | Credential Types** for alternative options for configuring custom credentials.

Custom Reader Configuration

- **Custom Reader Type**: Defines the reader type. The data can be output as Wiegand (D0 and D1) or Magnetic Data (Clock and Data).
- **Bit Length**: The total number of bits that are sent by the card reader for each credential.
- **Site Code Start**: The index where the site/facility code data starts in the transmitted credential data. The count starts at zero.
- **Site Code End**: The index where the site/facility code data ends in the transmitted credential data. The count starts at zero.
- **Card Number Start**: The index where the card number data starts in the transmitted credential data. The count starts at zero.
- **Card Number End**: The index where the card number data ends in the transmitted credential data. The count starts at zero.
- **Data Format**: This field describes how to handle the site/facility code and card number received from the reader. If the size of the site/facility code is smaller than 16 bits and the size of the card number is smaller than 16 bits, set the data format to 16 Bit Data. Otherwise use 32 Bit Data.

Parity Options (1-4)

There can be up to 4 blocks of parity calculated over the received data.

All parity options that are not in use must be set to 255.

- **Parity Type**: The method of calculating the parity for the block. This is either even or odd parity.
- **Parity Location**: The position of the parity bit in the received data. The count starts at zero.
- **Parity Start**: The index where the parity block starts in the received data. The count starts at zero.
- **Parity End**: The index where the parity block ends in the received data. The count starts at zero.

Bit Options (1-4)

All bit options that are not in use must be set to 255.

- **Set Bit**: The index of a set bit (a logical '1') in the received data. The count starts at zero.
- **Clear Bit**: The index of a clear bit (a logical '0') in the received data. The count starts at zero.

Card Data Options

- **Card Data AES Encryption Key**: Salto SALLIS and Aperio cards can be encoded with site/card information via the ICT Encoder Client. This field defines the decryption key so that Protege GX can decrypt data from these cards.

  For more information, see Application Note 147: Protege GX Aperio Integration or Application Note 148: Protege GX Salto SALLIS Integration.

  This field sets the Card Data AES Encryption Key for all reader ports associated with this controller.

Manual Controller Commands

Right clicking on a controller record (**Sites | Controllers**) displays a menu with manual commands for that controller.

Set Controller Date Time

If you are not using a time update server to synchronize the controller time (see **Sites | Controllers | Time Update**) you can update the time and date manually using this command. To manually update the time on a controller:

1. Right click on the controller record in **Sites | Controllers**.
2. The **Time** field displays the current date and time at the server. If you need to change these, enter new values in the field or click on the clock icon to use the time and date picker.
3. Click **Set Controller Date Time** to send the entered time to the controller.

Update Modules

Programming changes that alter the way hardware will operate require a module update to download the hardware-specific settings. A module update command causes the module to restart.

Use this option to perform a module update on the controller and all connected modules.

Warning: Sending this command will cause the controller and every connected module to temporarily go offline as they restart. This option should **not** be used in an active system.

To update only a specific module (such as a keypad or reader expander), right click on the specific record in the **Expanders** programming and click **Update Module**.

Force Download

In normal operation the download service checks each controller for changes in order by Database ID. If any changes are detected the services downloads the changes to that controller, then continues on to the next controller.

An operator can use the **Force Download** command to increase the priority of a specific controller, so that it will be next in line after the previous controller has been completed. In addition, the download service will download to the controller even if no changes are detected.

Get Health Status

The **Get Health Status** function sends a command to the controller to retrieve its current health status. The health status window will open, displaying any notices or issues relating to the controller or its module network.

The **Clear** button can be used to clear some notices which do not require action (e.g. 'The Controller has been restarted').

The health status window is static. Resolving or clearing notices will not cause the status to update until the **Get Health Status** command is sent again.

Module Addressing

The **Module Addressing** command is used to view the hardware that is connected to the system network, and to set the addresses of modules. Selecting this option opens a window showing the details of all modules that are currently connected, as well as those that have registered previously but are currently offline.

By default, Protege modules are shipped from the factory with an address of 254. This is outside the range that the controller will accept, so the address must be set by the installer. For some modules, such as keypads, the network address can be set in the module itself (see the relevant installation manual). For most Protege modules the address is set in the **Module Addressing** window.

The address of the controller's onboard reader expander is set by the **Register as Reader Expander** setting in **Sites | Controllers | Configuration**.

Setting Module Network Addresses

1. Ensure the controller is correctly powered and is communicating with the Protege GX software.
2. Connect the module(s) that require addressing to the module network. Make sure the power light on each module is on and that the status indicator 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 indicator will begin flashing an error code.
   - If the module has been previously addressed and is not a duplicate then it will succeed in registering and the status indicator will begin flashing at 1 second intervals.
4. Once all modules have completed the registration process (successful or not), open the Protege GX software and navigate to **Sites | Controllers**.
5. Right click on the controller record and select **Module Addressing** to open the module addressing window. This window displays all of the modules that are connected to the controller with the following information:
   - The module type (e.g. controller, keypad, etc.)
   - The serial number
   - Current firmware version and build number
   - The current module address
   - Whether the module address can be changed (for example, the controller's address cannot be changed)
   - Whether the module has successfully registered with the controller
   - Whether the module is currently online

   The controller's onboard reader expander will appear on this list as a reader expander with the same serial number as the controller. The address of this reader expander must be set in the **Register as Reader Expander** field (**Configuration** tab).
6. Before assigning addresses to modules you may need to identify specific physical modules:
   - For DIN rail modules, click the **Find** button to activate identification mode for the specified length of time. In identification mode the status and fault indicators flash in an alternating pattern, allowing you to identify the specific module.
   - For all modules, compare the **Serial** column with the serial number of each module (found on the module label).
7. For each module set the network address in the **Address** column. The new addresses will be displayed in **bold**, indicating that they have not yet been updated in the modules.
8. Push the addresses to the modules either by clicking **Update** for each individual module or by clicking **Update All**. Allow approximately 5 seconds for the module to re-register with the controller at the new address.
9. Click **Refresh**. The new addresses should change from bold to normal font and the newly addressed modules should be online.
   - If the address has not changed, check that the module has finished attempting to register with the controller.
   - If the address has changed but the module is not registered or online, check the address is in the valid address range and that it is not a duplicate of another module address.

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

Legacy Protege PCB modules cannot be addressed by this process. They must be addressed using DIP switches as described in the relevant installation manual.

Maximum Module Addresses

The Protege controller has a set limit on the number of modules of each type that it can support. This applies to both physical and virtual modules. The maximum addresses available for each type of module are outlined in the table below:

Module Type	Maximum Address
Keypad	200
Input Expander	248
Reader Expander	64
Output Expander	32
Analog Expander	32
Smart Reader	248

Any module with an address higher than these limits will not come online to the controller. A message will be generated in the controller's health status.

Update Firmware

Use the **Update Firmware** option to update the firmware of one or more controllers.

1. Click on the ellipsis **[...]** button and browse to the .bin firmware file. Click **Open**.
2. Check the boxes of the controller(s) that you wish to update.
3. Click **Update**.

This process will take approximately 10 minutes per controller and it is recommended 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 its normal function while firmware is being updated.

A popup message may appear in the user interface with the message 'Update Interrupted'. This is expected behavior and does not indicate that the update has failed.

Updating Modules with RS-485 Readers Connected

Important: Prior to starting a firmware update on any module with readers connected (wired) to its reader ports in RS-485, it is strongly recommended to physically disconnect the readers from the ports. This applies to all controllers and reader expanders with RS-485 readers physically connected to their reader ports. When a reader sends data to a reader port it can potentially stop the firmware update and leave the module stuck in boot mode. Physically disconnecting the readers alleviates the possibility of the firmware update failing due to the expander/controller receiving a packet on the RS-485 line while the update is in progress.

Troubleshooting Controller Connectivity

The following section provides useful troubleshooting steps for situations where the controller and server are not communicating.

For a demonstration, see Bringing a Protege GX Controller Online on the ICT YouTube channel.

Communication Requirements

For the server and controller to communicate, the following are required:

1. The controller must be physically networked to the server, or connected over the web.
2. The Protege GX services must be running.
3. The server must have the correct IP address for the controller.
4. The server must have the correct controller serial number to properly identify incoming messages from it.
5. The controller must have the event server IP address and port set correctly (port 22000 by default).
6. The controller must be contactable on the download and control ports (ports 21000 and 21001 by default).
7. Protege GX must have the correct computer name configured for the download and event servers.
8. The Protege GX software and databases must have the same database version.
9. Encryption must either be disabled at both ends or enabled at both ends with the correct encryption key.

Check that the Services are Running

The simplest and first thing to check is that the Protege GX services are running.

1. Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
2. Scroll down to the Protege GX services. Ensure that the following services are running:
   - Protege GX Data Service
   - Protege GX Download Service
   - Protege GX Event Service
   - Protege GX Update Service
3. If any service is not running, right click on it and click **Start**.

If any services will not start there may be another issue with your installation. For example, the database version may be incompatible (see page 58).

Confirm Controller IP Address

For the server to be able to contact the controller it must have the correct IP address programmed and be able to reach that IP address.

1. In Protege GX, navigate to **Sites | Controllers**.
2. In the **General** tab, highlight and copy (CTRL + C) the **IP Address**.
3. Paste (CTRL +V) the IP address into the address bar of a web browser on the server, with the prefix https:// (e.g. https://192.168.1.2).

   You may be presented with a certificate security warning on connection.
4. If you cannot connect, remove the https:// prefix and try again (e.g. 192.168.1.2) as your controller may not be configured for HTTPS.
5. If the controller is reachable using this IP address you should be presented with a simple login screen.
6. Log in to the controller using admin credentials.

If you are unable to web browse to the controller you may not have the correct IP address. If the IP address is unknown you will need to view/change it from a keypad or default the controller's IP address (see below).

If you do have the correct IP address then it is likely that you have a network problem. Ensure that the server and controller are on the same subnet, or have correct port forwarding configured at the router.

From firmware version 2.08.911 controller ping is disabled by default. If the controller is receiving downloads you can allow ping by adding the command `EnablePing = true` in the controller commands.

Unknown Controller IP Address

If the currently configured IP address is unknown:

- It can be viewed and/or changed using a Protege keypad. For more information, see Setting the IP Address from a Keypad (page 62).
- It can be temporarily set to 192.168.111.222 so that you can connect to the web interface to view and/or change it. For more information, see Temporarily Defaulting the IP Address (page 63).

Confirm Controller Serial Number

Incoming messages from the controller to the server are identified by the controller's serial number.

1. In the controller web interface, navigate to the **Settings** page.
2. Highlight and copy the **Serial Number**.
3. In Protege GX, navigate to **Sites | Controllers | General**.
4. Paste into the **Serial Number** field.

Duplicate IP Address or Serial Number

Although the software warns you, it is possible to save two controllers with the same IP or serial number. In this case, the controller created first takes priority.

- Confirm you haven't created a controller with a duplicate IP address or serial number. Check all of your sites.
- If you have created a site for templates, these should be left with zero IP addresses and serial numbers.

If you have two controllers with the same IP address or serial number anywhere on your server, there will be communication problems with at least one of them.

Confirm the Event Server is Functioning

To confirm the event server is functioning and listening on the correct port for incoming events, open the event server diagnostic window.

1. In Protege GX, navigate to **Sites | Controllers | General** and expand the **Diagnostic Windows** group.
2. Select **Open Event Server Diagnostic Window**. You should see a message that reads 'Listening on Port : 22000'.

   The default event server port is **22000**, but this can be changed in **Global | Event Servers**.

3. If the event server diagnostic window shows messages about an unknown serial number, events are being received from a controller with the serial number listed in the message. This also means the event server is accepting incoming events.
4. In the controller web interface, ensure that the **Event Port** matches the port set in Protege GX.
5. If you change the event port you must **save** and **restart the controller** using the icons in the upper right before your changes will take effect.

If the event server diagnostic window contains no text there is a problem with the configuration of the event server. This means the Event Server is **not** accepting incoming events. This can sometimes be resolved by restarting the Protege GX Event Service:

1. Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
2. Locate the Protege GX Event Service. Right click on the service and select **Restart**.

Confirm Event Server IP Address

For messages to get from the controller to the server, the controller must have the correct IP address for the event server.

1. On the server computer, open a command prompt. Enter the command `ipconfig` and press **[Enter]**.
2. You will be presented with the status and details of the server on various sub networks. Locate and copy the **IPv4 Address** for the sub network that the controller is connected to.

   For more complex networks it may be preferable to open a command prompt on a machine the controller is directly connected to and use the `ping` command to ascertain the external IP address of the server.

3. In the controller web interface, on the **Settings** page, check that **Event Server 1** has the correct IP address. Paste in the address located above if it does not match.

   There are three spaces for entering the event server IP. This is for situations where controllers have multiple paths to the server. In most cases the second and third event server IP addresses should be left as all zeros or all 255s.

Confirm Ports

Next, ensure that the download and control ports set on the server match those set in the controller interface.

1. In Protege GX, navigate to **Sites | Controllers | General** and check these values:
   - **Download Port** (default 21000)
   - **Control and Status Request Port** (default 21001)
2. In the controller web interface, on the **Settings** page, ensure that the **Download Port** and **Control Port** match those defined in the software.

3. If you have changed any settings on the controller, save your changes and restart the controller for the changes to take effect.

Check Computer Name

The download and event servers must have a correct computer name that matches the server machine. This usually only changes when you have restored a database from a different PC.

IMPORTANT: The computer name must be no longer than **15 characters**, or downloads will fail.

1. On the server computer, open **Control Panel > All Control Panel Items > System** to view computer information.
2. Copy the **Computer Name**.
3. In Protege GX, navigate to **Global | Download Server** and check that the **Computer Name** matches the name of the server machine. If not, paste in the name copied earlier.
4. Navigate to **Global | Event Server** and again check and correct the **Computer Name**.
5. If you have changed the computer name for either server, you must restart the corresponding service.

   Open the **Services** snap-in by:

   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
6. Locate the Protege GX services. Right click on the download service and/or event service and click **Restart**.

Repair Database Compatibility

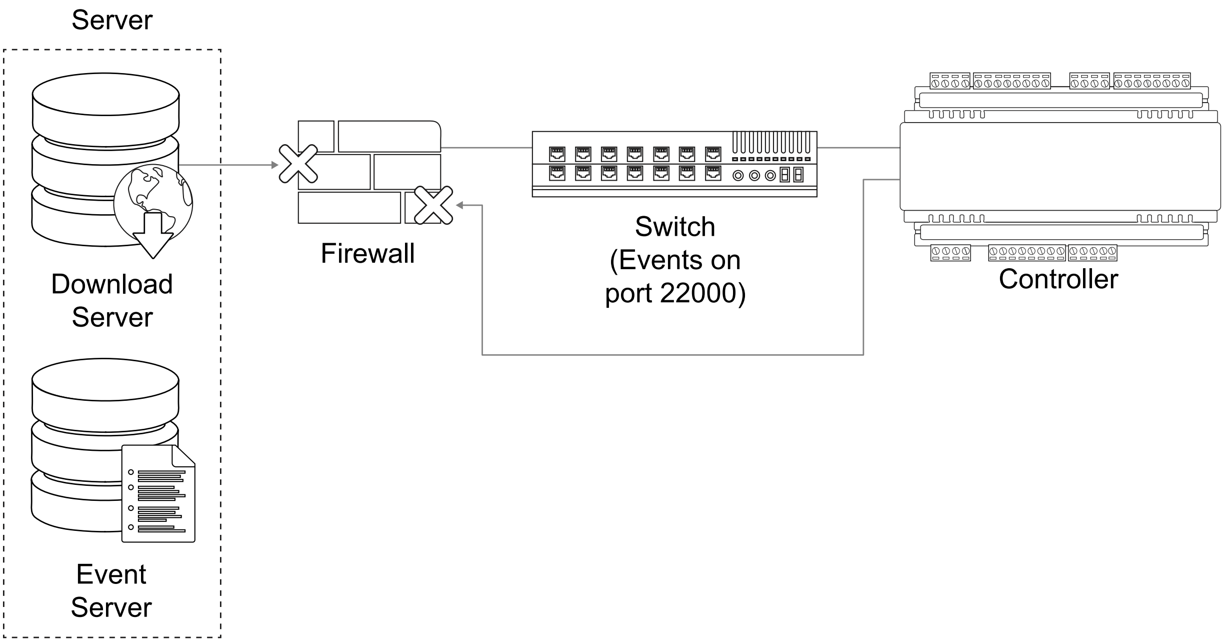
If you have restored a database from an older version of Protege GX, there may be a mismatch between the software and database versions. In this case the Protege GX Data Service will fail to start, the download and event server diagnostic windows will both remain blank, and no downloads will be passed to the controller.

To resolve this issue you must **uninstall and reinstall** Protege GX. This will prompt a database upgrade.

A backup taken from a newer version of Protege GX cannot be restored to an older version.

Windows Firewall

When the controller and server are on the same local network the only place a firewall can be blocking messages is on the server machine itself. This is called the Windows Firewall.



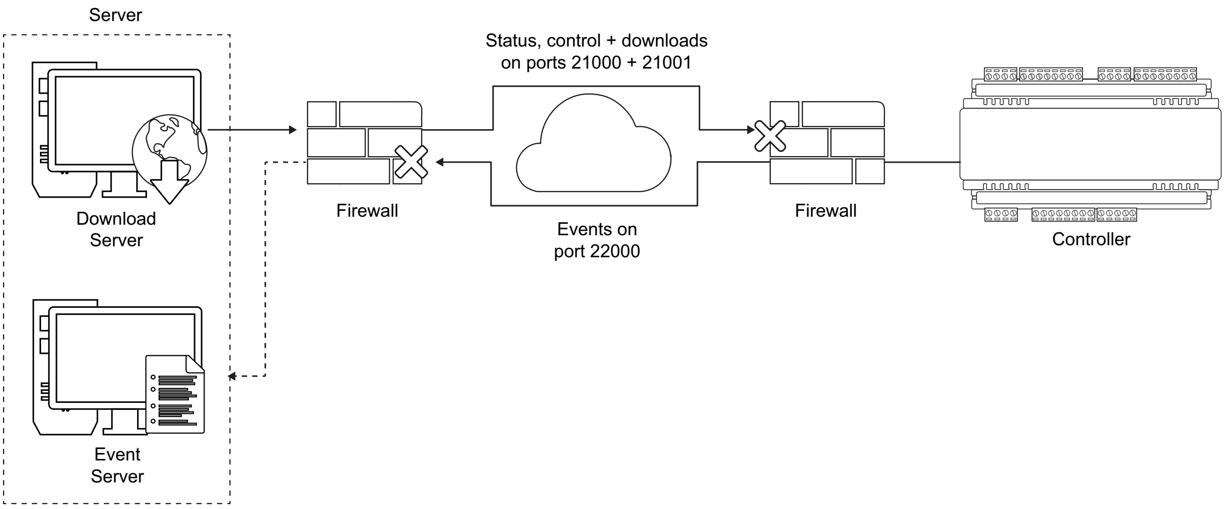
1. Open the Windows Firewall settings at **Control Panel > All Control Panel Items > Windows Firewall**. If the firewall is on, it is shown in green.
2. To eliminate the Windows Firewall as a cause of communication problems, turn it off temporarily by clicking **Turn Windows Defender on or off** at the left of the screen. Disable the firewall for each network location.

   Check whether this resolves the issue. If so, you can turn the Firewall back on and allow the Protege GX services through the Firewall.
3. Click the **Allow an app or feature through Windows Defender Firewall** link on the left of the screen.
4. Select **Allow another app...** to add a program as an exception.
5. Click Browse, then navigate to the Protege GX installation directory.
   By default, this is C:\Program Files (x86)\Integrated Control Technology\Protege GX.
6. Add the following executables, one by one:
   - GXSV.exe
   - GXSV2.exe
   - GXSV3.exe
   - GXPI.exe
   - GXEvtSvr.exe
   - GXDVR1.exe
   - GXDVR2.exe

   This allows the Protege GX services access through the Firewall.

Multiple Firewalls

On corporate networks there can be multiple firewalls.



To ensure these are configured correctly, provide the Protege GX Network Administrators Guide to the appropriate IT staff member. This document is included in the software installation pack.

Encryption

Both Server and Controller Encryption Enabled

Encryption relies on a shared key that both the sender and receiver of a message know. The message is encrypted using the key, then decrypted by the receiver using the same key. If the message is intercepted, it will make no sense to anyone without the encryption key.

Server Enabled, Controller Disabled

If for some reason the receiver loses the key, it is unable to decrypt incoming messages. In this case, the message is rejected.

Server Disabled, Controller Enabled

If the sender loses the key, the message is sent in plain text. The receiver, expecting to receive encrypted events, will also reject the message as it may be of a malicious nature.

Server and Controller with Different Encryption Keys

If the sender and receiver have different keys, the message can still not be decrypted by the receiver. This also results in the receiver rejecting incoming messages.

Each time encryption is enabled at the server, a new encryption key is generated. Each controller has a unique key, independent from all other controllers. If encryption for a controller is disabled then enabled again, the key is changed. If encryption for a controller is disabled at the server, the controller must be defaulted. It is not possible to re-enable encryption without first defaulting the controller.

Both Server and Controller Encryption Disabled

If encryption is disabled at both the sender and receiver, received messages are accepted. The downside with this scenario is that anyone 'listening' between the sender and receiver can also receive the messages.

Disabling Encryption

Defaulting the controller is the only way to remove the encryption key. This is by design and intended as a security feature. It means that physical access to the controller must be gained before encryption can be disabled.

If you are unsure of the state of encryption of either the server or controller, disable encryption at the server, then default the controller. This ensures that neither is encrypted and rules this out as a cause of communications problems. Encryption should then be re-enabled once communications are established.

1. Disable encryption at the server.
   Navigate to **Sites | Controllers | Configuration** tab and click **Disable Controller Encryption**.
   The software warns you prior to disabling encryption.
2. Default the controller (see Defaulting a Controller).

Telnet

To confirm a network path exists from the server to the controller and the correct ports are open, you can telnet to the controller on the download port (by default port 21000).

1. If the Telnet feature is not turned on, open the **Control Panel > All Control Panel Items > Programs and Features**.
2. Click **Turn Windows features on or off**. Locate the **Telnet Client**, check the box next to it and click **OK**.
3. Open a command prompt and attempt to telnet to the controller.
   For example, enter the command `telnet 192.168.1.2 21000`
   - If the controller can accept the connection, a clear screen appears with a cursor blinking in the top left corner.
   - If there is no connection, a message will advise there is still a problem between the server and controller. If you can web browse to the controller, it is likely a firewall is blocking the connection somewhere.

Finally, to confirm the event server is able to accept connections, configure a laptop with the same IP settings as the controller.

1. Remove the ethernet plug from the controller and plug into your laptop.
2. Try to telnet to the server IP address on the event server port (22000 by default):
   ```
   telnet 192.168.1.100 22000
   ```
   - If the server is able to accept connections, the clear screen and blinking cursor appear.
   - If the server is not reachable, a message will advise there is still a problem, indicating a firewall is blocking port 22000 to the server.

Hardware Configuration

Setting the IP Address from a Keypad

If the current IP address of the controller is not known it can be viewed and changed using a Protege keypad.

1. Connect the keypad to the module network.
2. Log in to the keypad using any valid installer code. The default installer code is 000000.

   If the default code has been overridden and you do not know the new codes you will need to default the controller (see Defaulting the Controller in this document) to reset the code.

   Note that this will erase **all** existing programming as well as setting up the default installer code.

3. Once logged in select **Menu 4** (Install Menu) then **Menu 2** (IP Menu) and view or edit the IP address, network mask, and gateway as required.

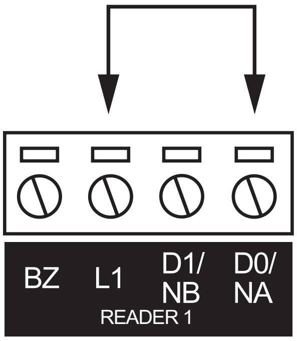
Once the settings have been changed you must save the settings by pressing the **[Arm]** key. You will be prompted to confirm the changes by pressing **[Enter]**. You must then restart the controller, either through the menu **[4], [2], [2]** or by cycling the power, for the settings to take effect.

Temporarily Defaulting the IP Address

If the currently configured IP address is unknown it can be temporarily set to 192.168.111.222 so that you can connect to the web interface to view and/or change it.

This defaults 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 configured IP address is used.

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.

Accessing the Controller

1. When the controller starts up it will use the following temporary settings:
   - IP address : 192.168.111.222
   - Subnet Mask : 255.255.255.0
   - Gateway : 192.168.111.254
   - DHCP : disabled
2. Connect to the controller by entering https://192.168.111.222 into the address bar of your web browser, and view or change the IP address as required.

   Remember to change the subnet of your PC or laptop to match the subnet of the controller.
3. Remove the wire link(s) and power cycle the controller again.

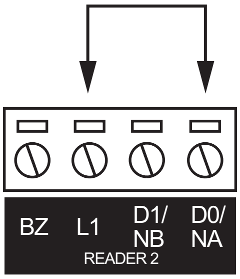
   You can now connect to the controller using the configured IP address.

Defaulting a Controller

The controller can be factory defaulted, which resets all internal data and event information. This allows you to remove all programming and start afresh.

Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.
5. Remove the wire link.

The system will now be defaulted with all programming and **System Settings** returned to factory configuration, including resetting the IP address and all network configuration, and removing all operator records.

- Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2.

  Earlier versions of the controller firmware do not reset the IP address. If the controller is not available on 192.168.1.2 you will be able to connect to it via its previous IP address.

- Any configured system settings (e.g. **Default Gateway**, **Event Server**) are reset to their default values.
- Any custom HTTPS certificates are removed and the default certificate is reinstalled.

  Earlier versions of the controller do not have a default HTTPS certificate installed. If the controller is not available via HTTPS, connect to it via HTTP.

- All operator records are removed and the admin operator must be recreated.
- All other programming is removed.

After Defaulting a Controller

After defaulting a controller a number of essential steps will need to be performed to resume normal operation. Not all of the following steps will necessarily be required, depending on your site configuration:

1. Connect to the controller's web interface using HTTPS, unless it is an older controller with no default certificate loaded, then it will connect using HTTP.
2. Recreate the admin operator and log in to the controller's web interface.

   If you are not prompted to create the admin operator, the default username is admin with the password admin.

3. Reset the controller's IP address to its previous value.
4. Reconfigure any additional network settings.
5. Reinstall previously installed custom HTTPS certificates.
6. Restore any other system settings as required by your site configuration.

LED Indicators

Protege DIN rail modules feature comprehensive diagnostic indicators that can aid the installer in diagnosing faults and conditions. In some cases an indicator may have multiple meanings depending on the status indicator display at the time.

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	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 flash (red)	A SHORT flash (<250 milliseconds) will show that data was received but was not in the correct format
Long flash (red)	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 flash (green)	Bell is ON, the circuit is in over current protection
Two flashes (green)	Bell is OFF, the circuit to the siren/bell is cut, damaged or tampered

Relay Indicators

The relay indicators show the status of the lock output relays.

State	Description
Constantly on (red)	Relay output is ON
Constantly off	Relay output is OFF

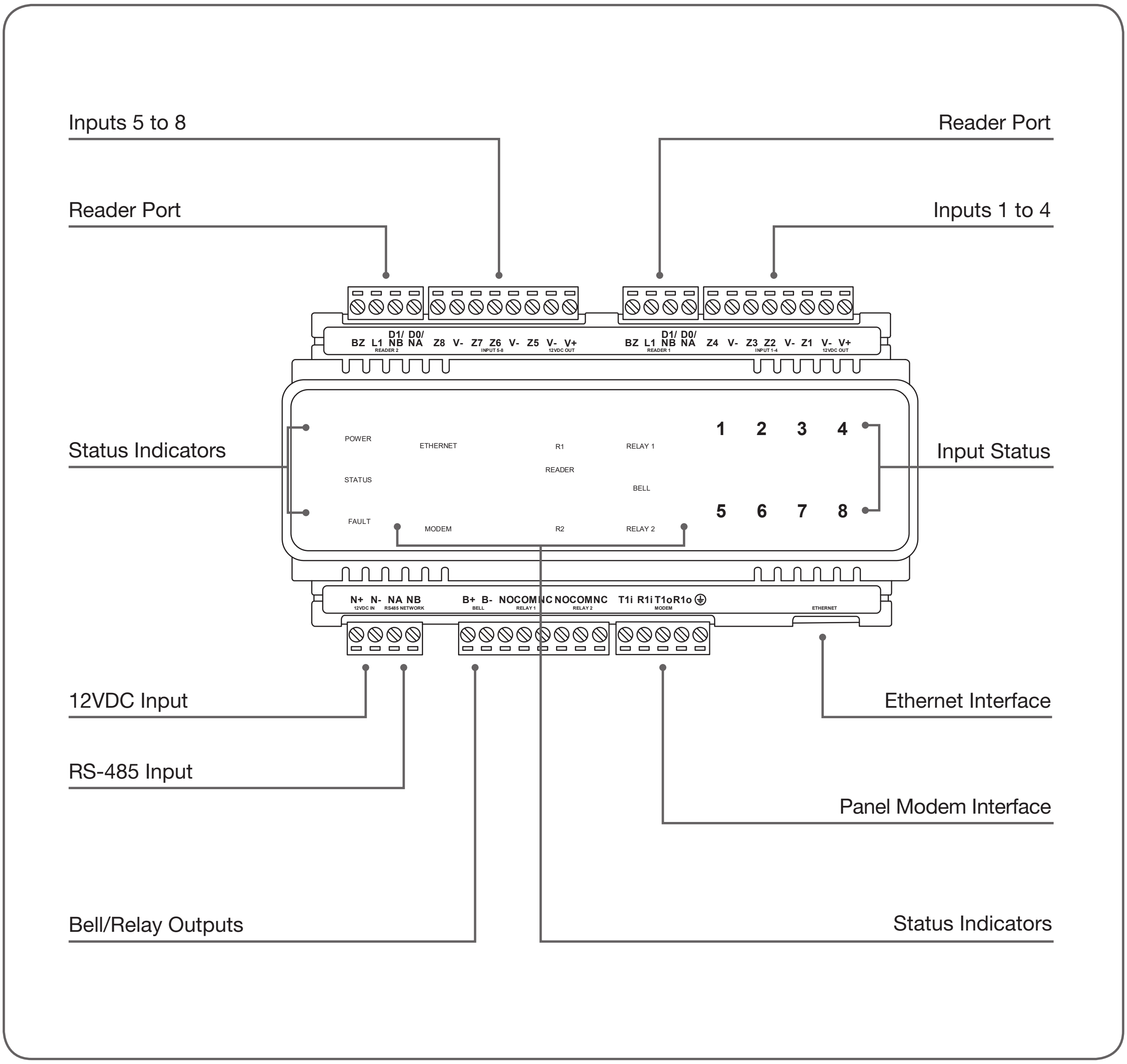
Input Indicators

Whenever an input on the module is programmed with an input type and area, the input status will be displayed on the front panel indicator corresponding to the physical input number. This allows for easy test verification of inputs without the need to view the inputs from the keypad or the Protege software.

State	Description
Constantly off	Input is not programmed
Constantly on (red)	Input is in an open state
Constantly on (green)	Input is in a closed state
Continuous flash (red)	Input is in a tamper state
Continuous flash (green)	Input is in a short state

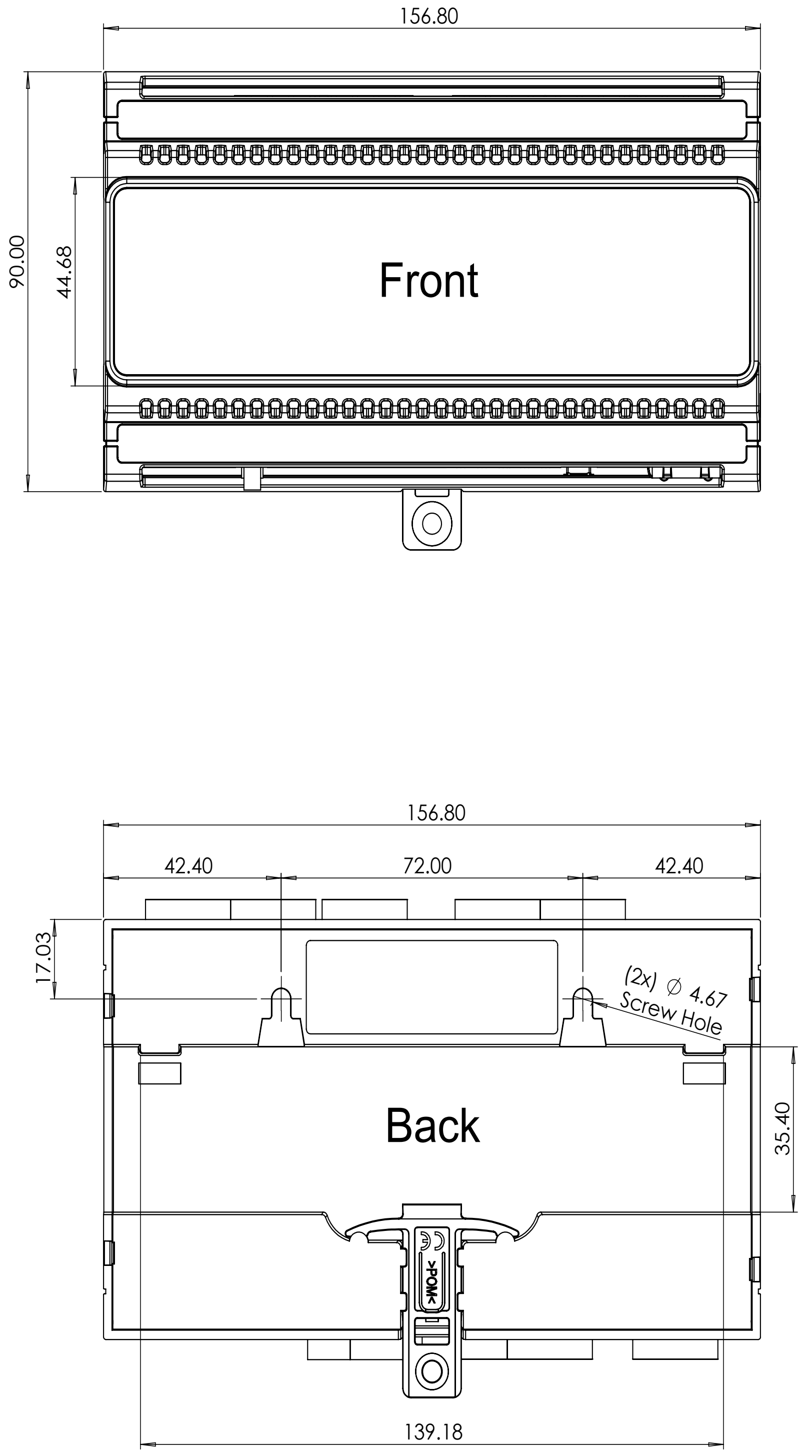
Mechanical Diagram

The mechanical diagram shown below outlines the essential details needed to help ensure the correct installation of the controller.



Mechanical Layout

The mechanical layout shown below outlines the essential details needed to help ensure correct installation and mounting. All measurements are shown in millimeters.



Technical Specifications

The following specifications are important and vital to the correct operation of this product. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Ordering Information	
PRT-CTRL-DIN	Protege GX DIN Rail Integrated System Controller
Power Supply	
Operating Voltage	11-14V DC
Operating Current	120mA (typical)
DC Output (Auxiliary)	10.45-13.85VDC 0.7A (typical) electronic shutdown at 1.1A
Bell DC Output (Continuous)	10.4-13.45VDC 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	
Communication (Ethernet)	10/100Mbps Ethernet communication link
Communication (RS-485)	3 RS-485 communication interface ports, 1 for module communication and 2 for reader communication
Communication (Modem)	2400bps modem communication
Readers	
Readers	2 reader ports that can be independently configured for either Wiegand (up to 1024 bits configurable) or RS-485, allowing connection of up to 4 readers providing entry/exit control for two doors **
	RS-485 reader port connections support configuration for OSDP protocol
Inputs	
Inputs (System Inputs)	8 high security monitored inputs
Outputs	4 50mA (max) open collector outputs for reader LED and beeper or general functions
Outputs	
Relay Outputs	2 Form C relays - 7A N.O/N.C. at 30 VAC/DC resistive/inductive
Dimensions	
Dimensions (L x W x H)	156 x 90 x 60mm (6.14 x 3.54 x 2.36")
Weight	330g (11.64oz)
Operating Conditions	
Operating Temperature	UL/ULC 0° to 49°C (32° to 120°F) : EU EN -10° to 55°C (14° to 131°F)
Storage Temperature	-10˚ to 85˚C (14˚ to 185˚F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)

Mean Time Between Failures (MTBF)	560,421 hours (calculated using RFD 2000 (UTE C 80-810) Standard)

* The total combined current refers to the current that will be drawn from the external power supply to supply the expander and any devices connected to its outputs. The auxiliary outputs are directly connected via thermal resettable fuses to the N+ N- input terminals, and the maximum current is governed by the trip level of these fuses. The Bell output is connected in the same way.

** Each reader port supports either Wiegand or RS-485 reader operation, but not both at the same time. If combining reader technologies, they must be connected on separate ports.

The ICT implementation of OSDP conforms to a subset of the OSDP functionality. For specifications and reader configuration, refer to AN-254 Configuring OSDP Readers, available from the ICT website.

The size of conductor used for the supply of power to the unit should be adequate to prevent voltage drop at the terminals of no more than 5% of the rated supply voltage.

Integrated Control Technology continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting our website (www.ict.co) for the latest documentation and product information.

Current and Validation Example

The example shown below refers to the specifications needed to help ensure the correct installation of a Protege controller. Specifications should be validated to ensure that individual maximum currents and total combined current are not exceeded.

Example

External Devices Connected to Panel
4 EDGE PIR Motion Detectors (Inputs 1-4) connected on AUX1 Output
4 EDGE PIR Motion Detectors (Inputs 5-8) connected on AUX2 Output
1 30W Siren (1.1A (1100mA) @ 13.8VDC)

Current Consumption	
Total Combined Current before shutdown	3.4A (3400mA)
Operating Current	120mA (Typical)
DC Output (AUX1)	4 EDGE PIR Motion Detectors @ 15mA each (Total 60mA)
DC Output (AUX2)	4 EDGE PIR Motion Detectors @ 15mA each (Total 60mA)
Siren on Bell Output	1.1A (1100mA)
Total Consumption	1.34A (1340mA)

Validation		
Is the total DC Output (AUX1) current less or equal to 1.1A (1100mA)?	Yes, it is 60mA	✓
Is the total DC Output (AUX2) current less or equal to 1.1A (1100mA)?	Yes, it is 60mA	✓
Is the Bell current output less or equal to 1.1A (1100mA)?	Yes, it is 1.1A (1100mA)	✓
Is the total combined current less or equal to 3.4A (3400mA)?	Yes, it is 1.34A (1340mA)	✓

New Zealand and Australia

General Product Statement

The RCM compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.

Intruder Detection Maintenance Routine

Integrated Control Technology recommends regular maintenance of the Protege system, including Protege controllers, expander modules and other connected devices.

Peripheral Devices

This section outlines specific routine maintenance procedures for Protege controllers and expander modules which are used for intruder detection. It does not include specific instructions for peripheral devices connected to the Protege system, such as motion detectors, smoke detectors and warning devices. Although many of these peripheral devices will be operated as part of the maintenance procedures described below, this may not meet the routine maintenance procedures recommended for those devices.

As a minimum, we recommend that you follow the AS/NZS 2201.1-2007 standards relating to:

- Detection devices for internal use (AS/NZS 2201.3 Part 3)
- Audible and visible alarm and warning devices

Testing Frequency

The maintenance procedures outlined below meet the requirements of AS/NZS 2201.1-2007, which specifies that testing of the intruder detection system must be carried out at least once a year. However, the testing frequency of detection devices, alarm warning devices and reporting operations should be determined according to the needs of the particular installation and local body regulations.

For some clients or sites it may be prudent to perform more frequent testing to ensure the integrity of the system. For example:

- Sites which require a higher rate of security or are heavily affected by environmental conditions may choose to have testing carried out more frequently.
- Very large sites with hundreds of detection devices may prefer to arrange multiple testing rounds per year, with a percentage of the devices tested in each round.

In contrast, sites where automated testing functions have been implemented may find that annual maintenance visits are adequate.

Recommended Routine Maintenance Procedures

Preliminary Procedures

Task	Frequency	Description
Notify the alarm monitoring company (place account 'on test')	As required prior to start of maintenance routine	If the system is monitored, the monitoring company must be notified before any testing begins (commonly referred to as placing the system 'on test'). In most circumstances you must be authorized to perform this task. The monitoring company may request a Technician or 'voice' code to identify you and the company that you represent.
Notify personnel on the premises	As required prior to start of maintenance routine	Prior to any test that may have an impact on personnel such as testing inputs or warning devices, ensure that all affected staff members are given any necessary notification, warning or instructions.

On Site Maintenance Procedures

Task	Frequency	Description
Check the equipment schedule and/or maintenance sheets	Once per year	Check the installation, location and siting of all equipment and devices against the 'as-built' documentation. Record and report any discrepancies.
Check wiring and cable protection	Once per year	Visually inspect all wiring and cable protection systems (conduits, trunking, etc.). Record any damage or deterioration.
Check for dust, moisture and vermin	Once per year	Check all equipment enclosures for dust, moisture, condensation and vermin. If excessive moisture or foreign matter is present, clear this out of the enclosure and take steps to prevent future accumulation.
Check the power supply	Once per year	Check that all power supplies are properly connected to a mains outlet and are operational.
Test the power supply DC output voltage	Once per year	Disconnect the backup batteries and test the DC voltages across the V+ and V- output terminals on all power supplies. The recommended voltage range is **12.4 - 14.0 VDC**.
Test expander module DC output voltage	Once per year	Test DC voltage across the V+ and V- output terminals on Protege controllers, input expanders and output expanders. The recommended voltage range is **10.4 - 14.0 VDC**.
Check battery connections	Once per year	Check that all power supplies have batteries fitted and connected correctly to the B+ and B- terminals, and that the batteries and connections show no visible signs of corrosion.
Test battery charge voltage	Once per year	Test the DC voltage across the B+ and B- terminals of all power supplies. The recommended voltage range is **13.4 - 13.8 VDC**. Note: When the mains power is restored following an AC fail condition, the battery charge voltage may fluctuate between **10.0 - 13.8 VDC** while the battery is recharging.

Task	Frequency	Description
Replace battery	Once per 3-5 years, or as specified by the battery manufacturer	Replace each power supply battery as required with another of equivalent or better specifications. Record the installation date of the new battery in the system maintenance records and in a clearly visible location within the equipment enclosure or on the battery itself.
Check keypad keys	Once per year	Check the operation of every key on the keypad, that all keys are clearly legible and that the keypad backlighting is operational.
Check keypad display	Once per year	Check the operation of the keypad display to ensure that all characters display correctly on the screen and that the backlight is operational and at the correct brightness.
Test the primary reporting service	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Ensure that the system is 'on test'. • Perform an operation that triggers reporting. • Check that the system reports successfully.
Test the backup reporting service	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Disable the primary reporting service. • Perform an operation that triggers a reportable alarm. • Check that the system correctly reports alarm to the backup reporting service after failing to communicate with the primary service. • Re-enable the primary reporting service.
Test system inputs and areas programmed to report	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Consult the maintenance sheets for a list of all inputs to be tested. • Activate each input by causing it to switch from the closed state to open (alarm) and back to closed. • Check the system event log for associated open/close events. • Check off each input on the maintenance sheet after successful testing and report any discrepancies. • Return all alarm areas to their pre-test states. • Obtain an activity report of all input opens/closes and area alarms/restores from the monitoring station. • Compare the monitoring station report with the system event log for the period to ensure that all tested inputs and areas reported correctly. Record and report any discrepancies. Special testing equipment and procedures may be required for smoke, heat, seismic glass-break and other detectors.

Task	Frequency	Description
Test warning device outputs	As agreed between monitoring company and client, but not less than once per year May be performed alongside Input Testing (above)	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. Test the operation of each audible and visible warning device. - Consult the maintenance sheets for a list of all outputs to be tested. - Arm any relevant areas. - Activate each warning device, either by user operation or by triggering an alarm which should cause activation. - Check that each warning device works as specified. Record and report any discrepancies. - Reset/Restore alarm areas to their previous state.

Software Maintenance Procedures

Task	Frequency	Description
Back up programming database	Recommended monthly	Backups of the programming database should be performed on a regular basis. It is vital that backups be stored offsite for disaster recovery. See the Operator Reference Manual for instructions on how to backup your database.
Back up events database	Recommended monthly	Backups or exports of recorded events should be performed on a regular basis. Verify that the backup file has been created. See the Operator Reference Manual for instructions on how to backup your database.

Follow-up Procedures

Task	Frequency	Description
Perform necessary system modifications	As required	Complete any modifications to the system resulting from the maintenance procedures. Record these in the maintenance sheets and report.
Obtain client sign off	At the conclusion of each maintenance visit	Obtain the signature of the client or the client's representative on the maintenance record.

European Standards

CE Statement

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED)2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules, of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directive(s).

WEEE

Information on Disposal for Users of Waste Electrical & Electronic Equipment

This symbol on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, please take this product(s) to designated collection points where it will be accepted free of charge.

Alternatively, in some countries you may be able to return your products to your local retailer upon purchase of an equivalent new product.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Please contact your local authority for further details of your nearest designated collection point.

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

For business users in the European Union

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.

Information on Disposal in other Countries outside the European Union

This symbol is only valid in the European Union. If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

EN50131 Standards

This component meets the requirements and conditions for full compliance with EN50131 series of standards for equipment classification.

EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013

This component meets the requirements and conditions for full compliance with EN50131-3 (2010) 8.10.1 and EN50131-1 (2006) 8.10 when connected to a compliant ARC (Alarm Reporting Centre).

Security Grade 4
Environmental Class II
Equipment Class: Fixed
Readers Environmental Class: IVA, IK07
SP1 (PSTN – voice protocol)
SP2 (PSTN – digital protocol),
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)

Tests EMC (operational) according to EN 55032:2015
Radiated disturbance EN 55032:2015
Power frequency Magnetic field immunity tests (EN 61000-4-8)

EN50131

In order to comply with EN 50131-1 the following points should be noted:

- Ensure for Grade 3 or 4 compliant systems, the minimum PIN length is set for 6 digits.
- To comply with EN 50131-1 Engineer access must first be authorized by a user, therefore Installer codes will only be accepted when the system is unset. If additional restriction is required then Engineer access may be time limited to the first 30 seconds after the system is unset.
- Reporting delay –Violation off the entry path during the entry delay countdown will trigger a warning alarm. The warning alarm should not cause a main alarm signal and is not reported at this time. It can be signaled locally, visually and or by internal siren type. If the area is not disarmed within 30 seconds, the entry delay has expired or another instant input is violated, the main alarm will be triggered and reported.
- To comply with EN 50131-1 neither Internals Only on Part Set Input Alarm nor Internals Only on Part Set Tamper Alarm should be selected.
- To comply with EN 50131-1 Single Button Setting should not be selected.
- To comply with EN 50131-1 only one battery can be connected and monitored per system. If more capacity is required a single larger battery must be used.

Anti Masking

To comply with EN 50131-1 Grade 3 or 4 for Anti Masking, detectors with a separate or independent mask signal should be used and the mask output should be connected to another input.

I.e. Use 2 inputs per detector. One input for alarm/tamper and one input for masking.

To comply with EN 50131-1:

- Do not fit more than 10 unpowered detectors per input,
- Do not fit more than one non-latching powered detector per input,
- Do not mix unpowered detectors and non-latching powered detectors on an input.

To comply with EN 50131-1 the Entry Timer should not be programmed to more than 45 seconds.

To comply with EN 50131-1 the Bell Cut-Off Time should be programmed between 02 and 15 minutes.

EN 50131-1 requires that detector activation LEDs shall only be enabled during Walk Test. This is most conveniently achieved by using detectors with a Remote LED Disable input.

To comply with EN 50131-1, EN 60839-11 Security Grade 4 and AS/NZS2201.1 class 4&5 Vibration Detection for PreTamper Alarm, protection is provided by a DSC SS-102 Shockgard Seismic vibration sensor mounted within the system enclosure. Alarm output is provided by a pair of non-latching, N.C. (normally closed), relay contacts, opening for a minimum of 1 second on detection of an alarm connected in series with the 24Hr tamper input (TP) on the PSU (or any other system input designated/programmed as a 24Hr Tamper Alarm).

This relay is normally energized to give fail-safe operation in the event of a power loss. Indication of detection is provided by a LED situated on the front cover. The vibration sensor is fully protected from tampering by a N.C. micro switch operated by removal of the cover.

Enclosure EN-DIN-24has been tested and certified to EN50131.

By design, the enclosures for all Integrated Control Technology products, EN-DIN-11, EN-DIN-12, EN-DIN-24-ATTACK and EN-DIN-31, comply with the EN 50131 standards. Tamper protection against removal of the cover as well as removal from mounting is provided by tamper switch.

Warning: Enclosures supplied by 3rd parties may not be EN50131-compliant, and should not be claimed as such.

UK PD 6662:2017 and BS 8243

Protege systems conform to PD 6662:2017 and BS 8243 at the security grade and notification option applicable to the system.

UL and ULC Installation Requirements

Only UL / ULC listed compatible products are intended to be connected to a UL / ULC listed control system.

UL/ULC Installation Cabinet Options

ULC Central Station Fire Monitoring, UL/ULC Central Station Alarm Installations

Cabinet Model	UL/ULC Installation Listings
EN-DIN-24-ATTACK	UL1610, UL1635, UL1076, ULC-S304, ULC-S559

ULC Fire Monitoring

Cabinet Model	ULC Installation Listings
EN-DIN-12	ULC-S559
EN-DIN-31	
EN-DIN-24	
EN-DIN-24-ATTACK	
EN-DIN-11V	

Electronic Access Control System Installations

Cabinet Model	UL/ULC Installation Listings
EN-DIN-12	UL294, UL1076, ULC-ORD-C1076-86, CAN/ULC-S319
EN-DIN-31	
EN-DIN-24	
EN-DIN-24-ATTACK	

All cabinet installations of this type must be located **inside the Protected Area**.

Not to be mounted on the exterior of a vault, safe or stockroom.

All cabinet internal covers and lids/doors must be connected to the cabinet's main ground point for electrical safety and static discharge protection.

Central Station Signal Receiver Compatibility List

- IP Receiver via Ethernet Port: ArmorIP Internet Monitoring Receiver. Internet monitoring software and interconnected with a (DAXW/C) central station automation system software and compatible receiving equipment.
- CID Receiver via Onboard Modem: Any UL and ULC listed receiver that uses the Contact ID protocol.

UL Operation Mode

UL operation mode should be enabled in Protege GX system settings. Select **Sites | Controllers | Options** and then select **Advance UL Operation** for the Protege GX system to operate in UL compliance mode.

This setting has the following effects:

- Adds a 10 second grace period following a failed poll before a module is reported as offline.

  Each module sends a poll message to the controller every 250 seconds. The module will be reported as offline if no poll has been received for the duration of this poll time plus the 10 second grace period.

- Suppresses reporting of all alarms and/or reportable events to a monitoring station within the first two minutes of the controller powering up. The system will continue to send poll messages as usual.
- Reports 'Input Tamper' events as 'Input Open' events when the area that the input is assigned to is armed. If the area is disarmed an 'Input Tamper' message will be sent.
- Limits the **Dial Attempts** for reporting services to a maximum of 8.

This setting must be used in conjunction with the other configuration requirements as noted in this section.

ULC Compliance Requirements

CAN/ULC-S304

- **Auto Arming**

  Control units that support auto arming shall provide an audible signal throughout the protected area not less than 10 min prior to the auto arming taking place. The control unit shall allow authorized users to cancel the auto arming sequence and transmit such cancelation to the signal receiving center with the identification of the authorized user that canceled the action.

  The following options must be enabled in the Protege system when using the Auto Arming feature. When the defer warning time is programmed to 10 minutes, the output group will be activated 10 minutes before the system performs the Auto Arming in the associated Area.

  - The **Defer Output or Output Group** must be programmed. Refer to the section Areas | Outputs in the Operator Reference Manual for programming instructions.
  - The **Defer Warning Time** must be programmed to not less than 10 minutes. Refer to the section Areas | Configuration in the Operator Reference Manual.
  - The **Defer Automatic Arming** option must be enabled. Refer to the section Areas | Options (2) in the Operator Reference Manual.
- **Arming Signal**

  A bell or visual indicator used as an arming acknowledgment signal must be listed to a ULC security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- **Double EOL Input Configuration**

  Only double EOL Input Configuration shall be used. Refer to the Inputs section of this manual and the section Inputs | Options in the Operator Reference Manual.
- **Multiplex System and Poll Time**

  The Protege controller is compatible with the ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

  In the Protege system, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:

  - The **Log Polling Message** option must be enabled. Refer to the section Report IP | Options in the Operator Reference Manual.
  - The **Poll Time** must be programmed to 40 seconds. Refer to the Report IP | General section in the Operator Reference Manual.
- **Central Station Signal Receiver**

The common equipment of each signal receiving center control unit shall be limited to 1000 alarm systems.

- **Number of attempts**

  In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

  In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dial Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Operator Reference Manual.

- **Check-In Time**

  DACT communication channel check-in time is not to exceed 24 hrs.

- **Trouble Input Service Test Report**
  - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.

- **Primary Communication Channel**

  The first attempt to send a status change signal shall utilize the primary communication channel.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system, and the CID service must be set as the backup service. The following options are required:
  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section Contact ID in the Operator Reference Manual.
  - The **Report IP Service** must be enabled as the primary communication channel and the **Service Mode** must be configured to start with the operating system. The **Reporting Protocol** must be set to ArmorIP, and the **Backup Service** must be configured to use the Contact ID Service.
  - Refer to the section Report IP in the Operator Reference Manual.
  - All ULC S304 P3 applications must transmit signals simultaneously over both the Contact ID Reporting Service and the Report ID Service. This will occur automatically with the above programming.

- **Status Change Signal**

  An attempt to send a status change signal shall utilize both primary and secondary communication channels.

- **Local Annunciation if Signal Reporting Failure**

  Failure of the primary communication channel or secondary communication channel shall result in a trouble signal being transmitted to the signal receiving center within 240 seconds of the detection of the fault. Failure of either communication channel shall be annunciated locally within 180 seconds of the fault.

  The following options must be enabled in the Protege system:
  - The **Ethernet Link Failure** trouble input must be programmed.
  - The **Trouble Input Area** must be armed. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.
  - The **Log Modem Events to Event Buffer** option must be selected in the Contact ID Reporting Service.

- **Network and Domain Access**

  Neither the subscriber control unit nor the signal receiving center receiver shall be susceptible to security breaches in general-purpose operating systems.

  Network access policies should be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

- **Ethernet Connections**

  All ethernet network connections shall be installed within the same room as the equipment.

- **Encryption**

For active communications channel security, encryption shall be enabled at all times.

The ArmorIP-E (UDP) protocol must be used and the Encryption Type must be set to AES-256.

The following options must be enabled for the Report IP service in the Protege system.

  - The **Reporting Protocol** must be set to ArmorIP (UDP) Encrypted. The AES key must be set as specified by monitoring station.
  - Refer to the section Report IP | General in the Operator Reference Manual.

- **Server Configuration**

  Where a server is employed for control over network addressing, encryption or re-transmission, such shall be designed to remain in the "on state" at all times.

  Communicators are not suitable for active communication channel security and medium or high risk applications unless such can be "online" at all times, have a minimum 128 bit encryption scheme, have encryption enabled, network and domain security implemented.

  Network access policies shall be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

- **Internet Service Provider (ISP)**

  The Internet Service Provider (ISP) providing service shall meet the following requirements:

  - redundant servers/systems
  - back-up power
  - routers with firewalls enabled and
  - methods to identify and protect against "Denial of Service" attacks (i.e. via "spoofing")

- **Information Technology Equipment, Products or Components of Products**

  Products or components of products, which perform communications functions only, shall comply with the requirements applicable to communications equipment as specified in CAN/CSA-C22.2 No. 60950-1, Information Technology Equipment Safety - Part 1: General Requirements. Where network interfaces, such as the following, are internal to the subscriber control unit or receiver, compliance to CAN/CSA-C22.2 No. 60950-1 is adequate. Such components include, but are not limited to:

  - A) Hubs;
  - B) Routers;
  - C) Network interface devices;
  - D) Third-party communications service providers;
  - E) Digital subscriber line (DSL) modems; and
  - F) Cable modems.

- **Backup Power Requirements**

  Power for network equipment such as hubs, switchers, routers, servers, modems, etc., shall be backed up or powered by an uninterruptible power supply (UPS), stand-by battery or the control unit, capable of facilitating 24h standby, compliant with Clauses 16.1.2 and 16.4.1 of CAN/ULC-S304.

  For communications equipment employed at the protected premises or signal receiving center and intended to facilitate packet switched communications, as defined in CAN/ULC-S304, 24h back-up power is required.

- **Compromise Attempt Events**

  ArmorIP detects the reception of any invalid packet on the programmed port as a potential system **compromise attempt**. Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event under the Live Panel Events.

  The event is sent with the following details:

  - **Account Code** as defined in the Serial Receiver settings
  - **Event Code** 0x163
  - **Group Code** as defined in the Serial Receiver settings
  - **Point Code** as defined in the Serial Receiver settings

  Refer to the section Global Settings | Serial Receiver in the ArmorIP Version 3 Internet Monitoring Application User Manual.

For UL and ULC installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.

- **Power Supply Mains Power Connection**

  If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

  The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S319

- The Protege controller and reader expander module are intended to be mounted within the enclosure (refer to UL/ULC Installation Cabinet Options), installed inside the protected premise, and are CAN/ULC-S319 Listed for Class I applications only.
- Exit devices and wiring must be installed within the protected area.
- For the Protege controller and reader expander module, all RS-485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgment signal must be listed to a ULC security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Fail secure locking mechanisms shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to ULC-S533 and CAN/ULC-S104.
- Must be installed with CAN/ULC-S319 listed portal locking device(s) for ULC installations.
- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S559

- **Signal Reporting**

  Any fault of an active communication system shall be annunciated and recorded at the signal receiving center within 180 s of the occurrence of the fault.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system. The following options are required:

  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section Contact ID in the Operator Reference Manual.
  - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
  - Refer to the section Report IP in the Operator Reference Manual.
  - The **Trouble Area** must be armed. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.

  In the ArmorIP Internet Monitoring Software the **Poll Time** must be set to 40 seconds and the **Grace Time** must be set to 20 seconds. Refer to the section Poll/Grace Time in the ArmorIP Version 3 Internet Monitoring Application User Manual.

- **Central Station Signal Receiver**

  The maximum number of signal transmitting units connected to any transmission channel shall conform to the manufacturer's recommendations. The ArmorIP Receiver supports up to 10000 simultaneous connections.

  Refer to the section Internet Connections Requirements in the ArmorIP Receiver Installation Manual for further details.

- **Number of attempts**

In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dialing Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Operator Reference Manual.

- **Check-In Time**

  DACT communication channel check-in time is not to exceed 24 hrs.

- **Trouble Input Service Test Report**
  - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.

- **Ethernet Connections**

  All ethernet network connections shall be installed within the same room as the equipment.

- **External Wiring**

  All wiring extending outside of the enclosure must be protected by conduit.

- **Power Supply Mains Power Connection**

  If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

  The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

- **Arming Signal**

  A bell or visual indicator used as an arming acknowledgment signal must be listed to a ULC security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.

- **Keypad Wiring**

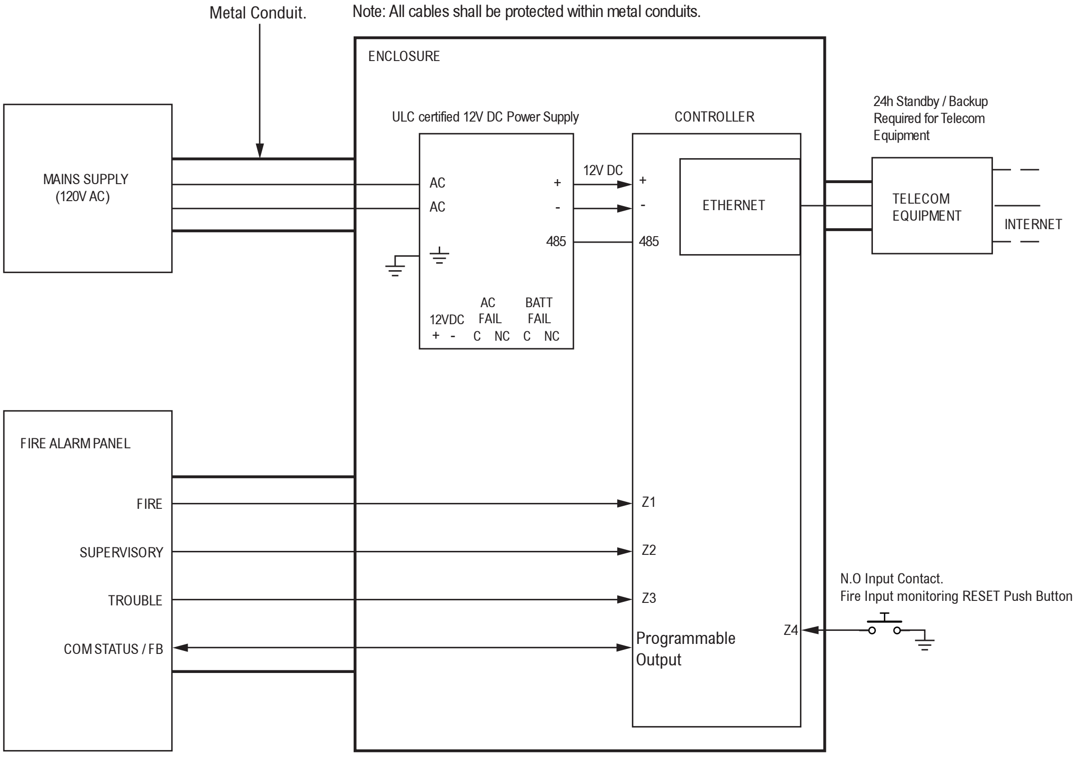
  The RS-485 connection to the keypad must be wired such that the shorts and other faults on the RS-485 line connection of the keypad will not cause the controller to malfunction.

- **Fire Areas**

  Fire areas shall be separated from burglar areas through area partitioning.

  NOTE: Any available dry relay contact on the Protege controller or output expander may be used for the FACP system, provided the selected output is programmed as the Report OK output.

CAN/ULC-S559
CONTROLLER
ACTIVE COMMUNICATION



* The AC FAIL output on the Power Supply MUST be programmed to follow the AC Trouble Input as follows:
AC FAIL = OPEN on fail

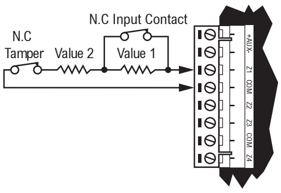
* Fire areas shall be separated from burglar areas through area partitioning.

* Fire Inputs Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output

* Fire Input Z4 N.O Push Button to be used as monitoring reset switch.

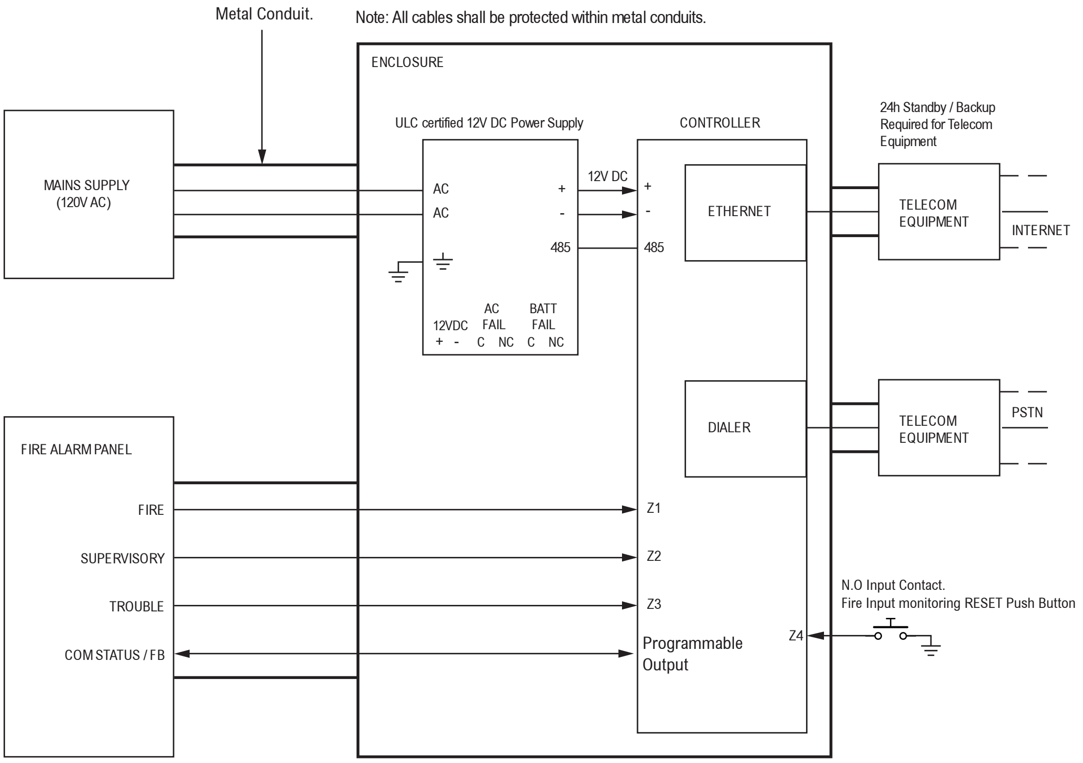
Typical Input Circuits

EOL Resitor Input Configuration		
Value 1	Value 2	Monitored Status
1K	1K	Open, Close, Tamper, Short
6K8	2K2	Open, Close, Tamper, Short
10K	10K	Open, Close, Tamper, Short
2K2	2K2	Open, Close, Tamper, Short
4K7	2K2	Open, Close, Tamper, Short
4K7	4K7	Open, Close, Tamper, Short



*EOL resistor must be installed at the Fire Alarm Control Panel Output.

CAN/ULC-S559
CONTROLLER
PASSIVE COMMUNICATION



Note: All cables shall be protected within metal conduits.

* The AC FAIL output on the Power Supply MUST be programmed to follow the AC Trouble Input as follows:
AC FAIL = OPEN on fail

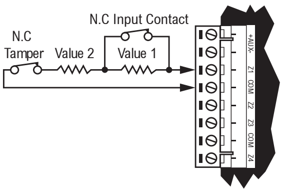
* Fire areas shall be separated from burglar areas through area partitioning.

* Fire Inputs Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output

* Fire Input Z4 N.O Push Button to be used as monitoring reset switch.

Typical Input Circuits

EOL Resitor Input Configuration		
Value 1	Value 2	Monitored Status
1K	1K	Open, Close, Tamper, Short
6K8	2K2	Open, Close, Tamper, Short
10K	10K	Open, Close, Tamper, Short
2K2	2K2	Open, Close, Tamper, Short
4K7	2K2	Open, Close, Tamper, Short
4K7	4K7	Open, Close, Tamper, Short



*EOL resistor must be installed at the Fire Alarm Control Panel Output.

Fire area inputs must be programmed as follows:

- FACP Fire Alarm Signal input type must be programmed as Fire.
- Supervisory Trouble Signal input type must be programmed as 24 HR Silent.
- Trouble Signal input type must be programmed as 24 HR Silent.

Please refer to the section Inputs | Areas and Input Types in the Operator Reference Manual.

- All fire area inputs must be placed into an area and this area must be armed. Please refer to the section Inputs | Areas and Input Types in the Operator Reference Manual.
- COM Status

FACP system with a COM STATUS input must have this input connected to one of the dry relay contacts of the Relay1 or Relay2 outputs of the Protege controller and the selected output must be programmed as the Report OK output in the Contact ID Service.

Note: Any available dry relay contact on the Protege controller or output expander may be used for the FACP system, provided the selected output is programmed as the Report OK output.

Please refer to section Contact ID | Settings in the Operator Reference Manual.

- Fire inputs Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output.

UL Compliance Requirements

UL1610

- A local alarm sounding device, alarm housing, and control unit shall comply with the mercantile requirements in the Standard for Police Station Connected Burglar Alarm Units and Systems, UL365.
- A bell or visual indicator used as an arming acknowledgement signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Exit and entry delay must not exceed 60 seconds. To program the entry and exit delay time, refer to the section Areas | Configuration in the Operator Reference Manual.
- All ethernet network connections shall be installed within the same room as the equipment.
- Signals between the premises control unit and the receiving equipment, when not carried by wireless means, shall be protected by the following method:
  - Onboard modem telco connection must be dedicated to the Protege controller.
  - Ethernet connection to the Internet Service Provider (ISP) with a fixed IP Address must be dedicated to the Protege controller.
- To comply with the dual signal line transmission system requirement, both transmission lines (onboard modem and IP reporting) must be enabled. Signals shall be sent simultaneously to both, Report IP Service and Contact ID Reporting Service.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system. The following options are required:
  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section Contact ID in the Operator Reference Manual.
  - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
  - Refer to the section Report IP in the Operator Reference Manual.
- When more than one means of signal transmission is used, loss of communication with the receiving system shall be annunciated at the receiver within 200 seconds. If a fault is detected on any of the signal transmission means, at least one of the signal transmission channels shall send a signal to the central-station to report the fault within 200 seconds.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system.

  The Protege controller is compatible with the ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

  In the Protege system, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:
  - The **Poll Time** must be programmed to 40 seconds. Refer to the Report IP | General section in the Operator Reference Manual
  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section Contact ID in the Operator Reference Manual

  - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
  - Refer to the section Report IP in the Operator Reference Manual.
  - The **Trouble Input Area** must be armed in 24h mode. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.

  In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

  In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The following options are required:

  - The **Dial Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Operator Reference Manual.
- DACT communication channel check-in time is not to exceed 24 hrs.
- Trouble Zone Service Test Report
  - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - ArmorIP detects the reception of any invalid packet on the programmed port as a potential system **compromise attempt**. Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event under the Live Panel Events.

    The event is sent with the following details:

    - **Account Code** as defined in the Serial Receiver settings
    - **Event Code** 0x163
    - **Group Code** as defined in the Serial Receiver settings
    - **Point Code** as defined in the Serial Receiver settings

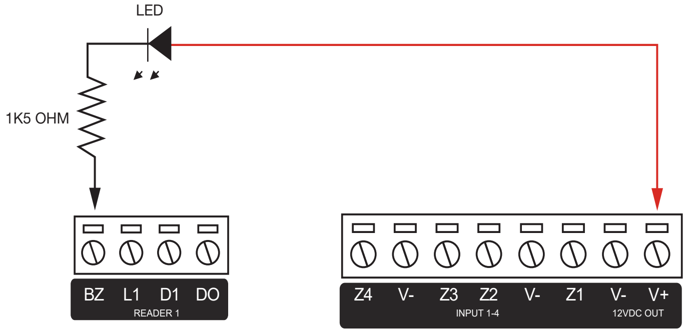
    Refer to the section Global Settings | Serial Receiver in the ArmorIP Version 3 Internet Monitoring Application User Manual.

    For UL and ULC installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.
- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

UL294

- The Protege controller and reader expander module are intended to be mounted within the enclosure (refer to UL/ULC Installation Cabinet Options), installed inside the protected premise, and are UL 294 Listed for Attack Class I applications only.
- Exit devices and wiring must be installed within the protected area.
- For the Protege controller and reader expander module, all RS485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgment signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to UL10B or UL10C.
- Must be installed with UL 1034 listed electronic locks for UL installations.

- AC power on shall be indicated by an external panel mount LED (Lumex SSI-LXH312GD-150) and fitted into a dedicated 4mm hole in the cabinet to provide external visibility. This shall be wired between 12V and a PGM output that is programmed to follow the AC trouble input as shown below:



- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

FCC Compliance Statements

FCC PART 15, WARNINGS: INFORMATION TO USER

This equipment complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Changes or modifications not authorized by the party responsible for compliance could void the user's authority to operate this product.

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

IMPORTANT INFORMATION

This equipment complies with Part 68 of the FCC Rules and the requirements adopted by the ACTA. Inside the cover of this equipment is a label that contains, among other information, a product identifier in the format US: AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

FCC REGISTRATION NUMBER:	US: 48DMM00BPRTCTRLDI
RINGER EQUIVALENCE NUMBER:	0.0
USOC Jack:	RJ-31X

Telephone Connection Requirements

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See this document for details.

Ringer Equivalence Number (REN)

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US: AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Incidence of Harm

If this equipment (Protege controller) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

Changes in Telephone Company Equipment or Facilities

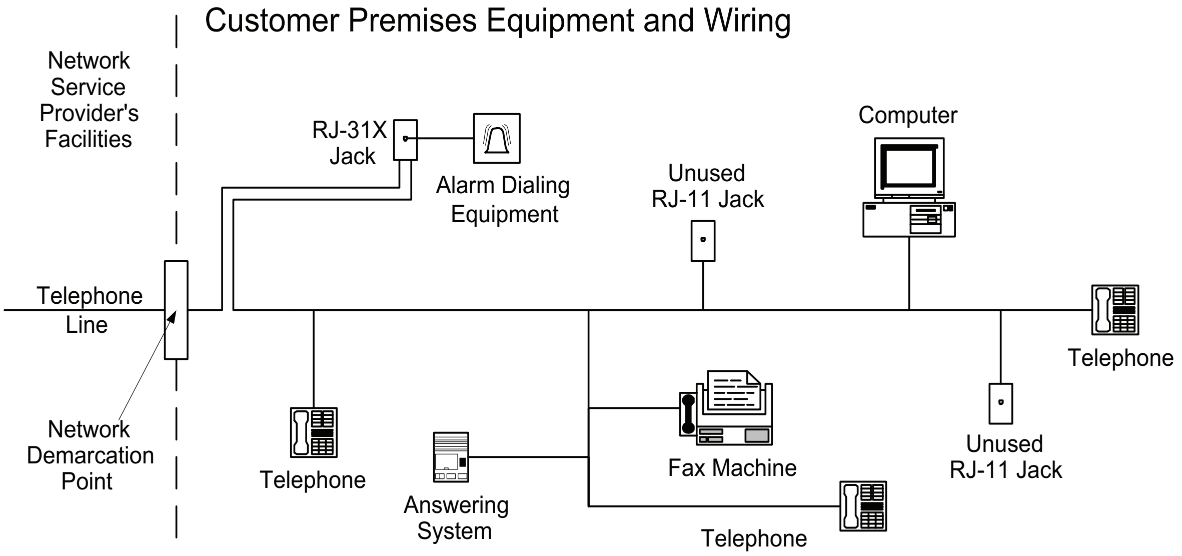
The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

Equipment Maintenance Facility

If trouble is experienced with this equipment (Protege controller), for repair or warranty information please contact Integrated Control Technology. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved. This equipment is of a type that is not intended to be repaired by the end user.

Additional Information

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information. Alarm dialing equipment must be able to seize the telephone line and place a call in an emergency situation. It must be able to do this even if other equipment (telephone, answering system, computer modem, etc.) already has the telephone line in use. To do so, alarm dialing equipment must be connected to a properly installed RJ-31X jack that is electrically in series with and ahead of all other equipment attached to the same telephone line. Proper installation is depicted in the figure below. If you have any questions concerning these instructions, you should consult your telephone company or a qualified installer about installing the RJ-31X jack and alarm dialing equipment for you.



Industry Canada Statement

This class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (A)/NMB-3(A)

This product meets the applicable Industry Canada technical specifications. The Ringer Equivalence Number (REN) for this terminal equipment is 0.0. The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 0.0. Le présent materiel est conforme aux spécifications techniques applicables d'Industrie Canada. L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Controller REGISTRATION NUMBER	IC: 10012A-PRTCTRLDIN
Controller NUMÉRO D'ENREGISTREMENT	IC: 10012A-PRTCTRLDIN

Disclaimer and Warranty

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 ICT policy of enhanced development, design and specifications are subject to change without notice.

For warranty information, see our Standard Product Warranty.

Submitted to UL 20-Apr-21

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.

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 ICT policy of enhanced development, design and specifications are subject to change without notice.