Integrated Control Technology

Protege Troubleshooting Guide

Protege GX / Protege WX / Protege X

Last Published: 01-Nov-24 9:54 AM

Contents

Introduction

This document is a quick reference guide to help you troubleshoot commonly-encountered issues on Protege GX, Protege WX and Protege X sites. It provides concise information so you can identify and resolve issues related to:

- LED indicators
- Card readers
- Trouble inputs
- Health status messages
- Networking
- Reporting services
- Door, keypad and area access

This guide is intended for reference only, so it assumes some familiarity with Protege systems. For more information about your system, click the **Help** button in the software or see the documentation on the ICT website.

If all else fails, contact ICT Technical Support: https://ict.co/about/contact-us/

LED Indicators

Protege modules include handy LED indicators to help you identify issues with the system at the cabinet. This section provides a quick reference guide for the meaning of each LED indicator color and pattern.

Module Status Indicators

Power Indicator

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

Status Indicator

State	Description
Fast flash (green)	Module attempting registration with controller
Slow flash (green)	Module successfully registered with controller
Flashing (red)	Module communications activity

The status indicator will flash an error code when the fault indicator is on (see below).

Fault Indicator

State	Description
Continuous slow flash (red)	Module is in boot mode awaiting firmware update
Constantly on (red)	Module is in error state and will flash an error code with the status indicator

Error Codes

Flash	Error Description
1	**Unknown Error Code** The error code returned by the system controller could not be understood by the module.
2	**Firmware Version** The firmware version on the module is not compatible with the system controller. To clear this error, update the module using the module update feature in the controller's web interface.
3	**Address Too High** The module address is above the maximum number available on the system controller. To clear this error change the address to one within the range set on the system controller, restart the module by disconnecting the power.
4	**Address In Use** The address is already in use by another module. To clear this error set the address to one that is not currently occupied. Use the view network status command to list the attached devices, or the network update command to refresh the registered device list.

5	**Controller Secured Registration Not Allowed** The controller is not accepting any module registrations. To allow module registrations use the network secure command to change the setting to not secured.
6	**Serial Number Fault** The serial number in the device is not valid. Return the unit to the distributor for replacement.
7	**Locked Device** The module or system controller is a locked device and cannot communicate on the network. Return the unit to the distributor for replacement.

Controller Status Indicators

Controller Status Indicator

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

Fault Indicator

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

Ethernet Link Indicator

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

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

Input/Output Indicators

Input Indicators

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

Output Indicators

State	Description
Constantly on (red)	Output is ON
Constantly off	Output is OFF

Relay Indicators

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

Bell Indicator

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

Reader Indicators

Reader 1/Reader 2 Indicators

State	Description
Short Flash (red)	A short **flash** (<250 Milliseconds) on the reader 1/reader 2 indicators 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.

Power Supply Indicators

V1 Output/V2 Output Indicators

State	Description
On (green)	12VDC output operating OK
Flashing (red)	12VDC output failure

Battery Indicator

State	Description (with mains power connected - power indicator on)
Flashing (red)	Backup battery is disconnected
On (red)	Backup battery failed its dynamic battery test
On (green)	Last backup battery dynamic test successful
State	**Description (with mains power disconnected - power indicator off)**

Flashing (red)	Mains has failed and the PSU is drawing power from the battery. State is Battery Low
Flashing (green)	Mains has failed and the PSU is drawing power from the battery. State is Battery Restore

Temp Indicator

State	Description
On (red)	Core temperature exceeded. **Over Temp Shutdown Activated**
Flashing (red)	Core temperature within 10°C of Over Temp Shutdown
On (green)	Core temperature OK

Output Current Indicator

State	Description
Constantly on	Output current exceeded. **Over Current Shutdown Activated**
Continuous flash	Output current exceeded maximum, approaching Over Current Shutdown
Constantly on (all indicators)	Maximum output current level reached
Constantly on (partial)	Indicated output current level reached

Cellular Modem Indicator

State	Description
Off	Incorrect input voltage applied and/or no controller connection
On	Communicating with controller. Not registered on the cellular network
Blinking (1s / 1s)	Registered on the cellular network (i.e. communicating with a cell tower) This does not indicate that an internet connection has been established or that data can be sent.

Card Readers

The table below outlines issues that commonly occur with card readers and the most likely solutions.

Issue	Possible Cause	Solution
The card reader is flashing blue and green	The card reader is configured for ICT RS-485 or OSDP operation, but is not connected or not wired correctly.	Ensure that the reader is wired correctly according to the installation manual.
	The card reader is configured for ICT RS-485 or OSDP operation, but the reader expander port is not configured correctly.	Check the **Port 1/2 network type** in the reader expander programming. Set the network type to ICT RS-485 or OSDP as required, save and perform a module update. Alternatively, set the reader's output format to Wiegand. See the ICT Card Reader Configuration Guide.
	The card reader is configured for OSDP operation, but there is an encryption mismatch between the reader and reader expander (e.g. secure channel is enabled on the reader, but not the expander).	Put the card reader into installation mode to clear the encryption key. Activate installation mode in the reader expander to re-establish secure channel.
	There are communication issues between the card reader and the reader expander.	Ensure that the wiring meets the minimum required wiring standards in the installation manual. If there is a very long cable run between the card reader and reader expander or a particularly noisy environment, it may be helpful to insert a 330 ohm resistor across NA/NB at each end to reduce signal reflection.
When I badge a card, the reader gives one short beep.	The card reader is configured for Wiegand operation but is not connected or not wired correctly.	Ensure that the reader is wired correctly according to the installation manual.
	The card reader output format and reader expander port network type do not match.	Check the **Port 1/2 network type** in the reader expander programming. Set the network type to the same as the card reader configuration, save and perform a module update.
	The card does not match the expected format.	In the reader expander programming, set the **Reader 1/2 format** and **Reader 1/2 secondary format** to the correct formats for the cards you are using. Save, then perform a module update. If you are using OSDP readers, check the **Reader one format** in the smart reader. In Protege GX these settings may not be available when the readers are set to ICT RS-485. To work around this issue, temporarily set the **Port 1/2 network type** to Wiegand, update the reader formats, then set the network type back to ICT RS-485.

Issue	Possible Cause	Solution
When I badge a card, the reader does not respond.	The card technology and reader technology do not match (for example, 13.56MHz readers cannot read 125kHz cards).	Use a card that matches the technology of the reader.
	Either the card or the card reader has encryption which the other does not recognize.	Use a card with the correct encryption for the card reader, or configure the encryption keys in the card reader. Contact ICT Technical Support for more information.
The card reader beeps multiple times, but there are no events.	The controller is offline or events are otherwise not being displayed.	See Troubleshooting Controller Connections.
Access is denied.	There is an issue with user access.	See Door Access Denied.

Trouble Inputs

Trouble inputs are used to monitor the status and condition of the system. Each trouble input represents a specific issue such as a power failure, communications fault or tamper. Typically an open trouble input will raise a silent alarm in the programmed area and display a trouble message on the keypad.

You can view the status of trouble inputs by the following methods:

- On a status page or floor plan in Protege GX.
- Under **Monitoring | Status Lists | Trouble Inputs** in Protege WX.
- In **Controller Records | Trouble Inputs** in Protege X.
- In the Installer menu on a keypad. Navigate to **Menu > 4. Install > 1. View > 2. Trouble Input**.

This section provides a quick reference for the trouble inputs on each module, what causes them to open and how to resolve the issue and close the trouble input. It also contains a guide to the trouble messages displayed on the keypad.

Controller Trouble Inputs

Input Number	Description	Cause	Solution
2	12V Supply Failure	Opens when the controller is no longer receiving power from the RS-485 network. The controller can remain powered long enough to report the fault before shutting down.	Restore power to the controller.
4	Real Time Clock Not Set	Not used.	
5	Service Report Test	Opens automatically at a specific time to test the connection between the controller and the central monitoring station.	Closes automatically after one minute.
6	Contact ID Reporting Failure or Service Report Failure to Communicate	Opens when a Contact ID or SIA service fails to communicate with the central monitoring station.	Resolve the connection issue or stop the reporting service.
7	Phone Line Fault Modem model only	Opens when the phone line is disconnected.	Reconnect the phone line or stop the reporting service.
8	Auxiliary Failure	Opens when output auxiliary power fails. This can occur when the controller loses 12V power.	Closes when output auxiliary power is restored.
9	Bell Cut/Tamper	Opens when the controller loses connection to the bell output across the B+ and B- terminals, or when auxiliary power to the B+ and B- terminals fails.	Closes when the bell is reconnected or power is restored.

Input Number	Description	Cause	Solution
11	Bell Current Overload	Opens when the bell output draws too much current. See the controller installation manual for the electronic shutdown threshold.	Closes when the current returns to normal levels.
13	Module Communication Fault	Opens when the controller loses communication with any module on the RS-485 module network for at least 5 minutes. The Module Communication Fault trouble input for the specific module that has gone offline will also open.	Closes immediately when all modules are back online. To avoid triggering this trouble input for modules that are not physically connected, enable the **Virtual module** option in the expander programming.
14	Module Network Security	Not used.	
20	Report IP Reporting Failure	Opens when a Report IP service fails to communicate with the central monitoring station.	Resolve the connection issue or stop the Report IP service.
22	Modbus Communication Fault	Opens when a Modbus service fails to communicate with the Modbus client.	Resolve the connection issue.
23	Protege System Remote Access	Not used.	
24	Installer Logged In	Opens when a user with the **Installer menu group** option enabled (in the menu group programming) logs in to a keypad.	Log out of the keypad.
29	System restarted	Opens for one second after the controller restarts. A health status message will also be generated.	Closes automatically after one second.
30	PoE Connection Lost Legacy PoE model only	Opens when power over ethernet is lost and the controller starts drawing from the battery.	Closes when power over ethernet is restored.
31	Output Over-Current Failure Legacy PoE model only	Opens when too much output current is being drawn by the system. If more current is drawn, the output supply will be shut down. See the PoE controller installation manual for the output over-current thresholds.	Closes when the output current draw returns to normal levels.
32	3G Modem Link Lost Legacy 3G modem model only	Opens when the onboard 3G modem fails to communicate with the central monitoring station.	Closes when the connection issue is resolved or the reporting service is stopped.

Input Number	Description	Cause	Solution
33	Controller Group Link Lost or Cross-Controller Communication Fault	Opens when the controller attempts to control a resource that is hosted on another controller (e.g. an output, door or area), but fails to communicate. Protege GX only.	Resolve the network issue between the two controllers or remove cross controller programming to close the trouble input.

Reader Expander Trouble Inputs

Input Number	Description	Cause	Solution
12	Reader 1 Tamper / Missing	Opens when the controller or reader expander loses connection with a card reader on reader port 1 for at least 2 minutes.	Closes when the card reader comes back online. Check the wiring of the card reader. For OSDP readers, make sure that the number of smart readers programmed is the same as the number of readers physically connected.
13	Reader 2 Tamper / Missing	Opens when the controller or reader expander loses connection with a card reader on reader port 2 for at least 2 minutes.	Closes when the card reader comes back online. Check the wiring of the card reader. For OSDP readers, make sure that the number of smart readers programmed is the same as the number of readers physically connected.
14	Door 1 Lockout or Door 1 Too Many Attempts	Opens when an unknown credential or PIN is received at the door on reader port 1 too many times in a row. The default number of attempts is 3.	Badge a valid credential or enter a valid PIN at the door.
15	Door 2 Lockout or Door 2 Too Many Attempts	Opens when an unknown credential or PIN is received at the door on reader port 2 too many times in a row. The default number of attempts is 3.	Badge a valid credential or enter a valid PIN at the door.
16	Module Offline or Module Communication Fault	Opens when the controller loses communication with this module for at least 5 minutes. The Module Communication Fault trouble input for the controller will also open.	Closes immediately when the module is back online. To avoid triggering this trouble input for modules that are not physically connected, enable the **Virtual module** option in the expander programming.

Door Trouble Inputs

Input Number	Description	Cause	Solution
1	Door Forced Open	Opens when the door is forced open.	Close the door. See the **Alarm options** tab for settings to disable the door forced alarm.
2	Door Left Open	Opens when the door is left open for the **Door left open alarm time**.	Close the door. See the **Alarm options** tab for settings to disable the door left open alarm.
3	OSDP Tamper Switch / Power Loss	Opens when an OSDP reader is removed from the wall or loses power.	Close the OSDP reader's tamper switch or restore power to the reader.
8	Door Duress	Opens when the door receives a duress PIN, regardless of whether access is granted or denied.	Enter a standard, non-duress PIN at the door.

Power Supply Trouble Inputs

Input Number	Description	Cause	Solution
1	Module Tamper	Opens when the tamper switch (TP) is opened. This is typically used for the cabinet door tamper.	Close the tamper switch.
2	Mains Failure	Opens when the mains power input is lost and the power supply starts drawing from the battery.	Closes when the mains power input is restored.
3	Battery Low / Missing	Opens when the power supply loses connection to the backup battery or detects that the capacity is low. See the power supply installation manual for the battery low and restore thresholds.	Reconnect the battery or reconnect the mains power so that the battery can charge.
4	Output Voltage Low	Opens when the output voltage drops below 10.6V.	Closes when the output voltage returns to normal levels.
5	Output Over-Current Failure	Opens when too much output current is being drawn by the system. If more current is drawn, the output supply will be shut down. See the power supply installation manual for the output over-current thresholds.	Closes when the output current draw returns to normal levels.

Input Number	Description	Cause	Solution
6	Core Temperature Over-Temp Failure	Opens when the core temperature of the power supply rises to near-unsafe levels. If the temperature rises higher, the power supply will shut down the mains input and supply output power from the battery. See the power supply installation manual for the core temperature thresholds.	Closes when the core temperature returns to normal levels.
8	Module Offline or Module Communication Fault	Opens when the controller loses communication with this module for at least 5 minutes. The Module Communication Fault trouble input for the controller will also open.	Closes immediately when the module is back online. To avoid triggering this trouble input for modules that are not physically connected, enable the **Virtual module** option in the expander programming.

Output Expander Trouble Inputs

Input Number	Description	Cause	Solution
8	Module Offline	Opens when the controller loses communication with this module for at least 5 minutes. The Module Communication Fault trouble input for the controller will also open.	Closes immediately when the module is back online. To avoid triggering this trouble input for modules that are not physically connected, enable the Virtual module option in the expander programming.

Keypad Trouble Inputs

Input Number	Description	Cause	Solution
1	Module Tamper	Opens when the keypad's tamper switch opens, i.e. when the keypad is removed from the wall.	Closes when the tamper switch closes.
2	Power Supply Low Voltage PRT-KLCD only	Opens when the supplied voltage drops below 8.8V.	Closes when the supplied voltage reaches 11.1V.
3	User Panic	Opens when someone presses the 1 and 3 keys together for 3 seconds.	Enter any other code into the keypad.
4	User Duress	Opens when someone enters a duress PIN.	Enter a standard, non-duress PIN code.

Input Number	Description	Cause	Solution
7	Too Many Attempts	Opens when too many incorrect PINs have been entered at the keypad in a row. Only occurs when the **Lock keypad on excess attempts** option is enabled.	Closes automatically after the programmed time.
8	Module Offline	Opens when the controller loses communication with this module for at least 5 minutes. The Module Communication Fault trouble input for the controller will also open.	Closes immediately when the module is back online. To avoid triggering this trouble input for modules that are not physically connected, enable the Virtual module option in the expander programming.

Trouble Messages on the Keypad

If you do not have access to the Protege system or installer menu, you can diagnose system issues using a keypad connected to the RS-485 module network.

To view trouble messages on the keypad, either:

- Log in and navigate to **Menu > 5. View > 2. Trouble View**.
- Navigate to **Menu > 2. Trouble View** without logging in (if offline operation is enabled).

Press **Enter** to acknowledge the trouble message and remove it from the list on the keypad (the trouble input will remain open). An event will be logged in the software to indicate who has acknowledged the trouble message. For example:

```
User John Smith Acknowledged Trouble 1 - General AC failure At Reception Keypad
```

The keypad message for each trouble input is determined by the **Trouble group** and **Trouble group options** settings. The table below shows which messages correspond to each trouble input, based on the default settings.

Trouble Message	Trouble Group	Trouble Group Options	Trouble Inputs
AC Fail The system or a component has lost AC and is operating on battery backup.	1 - General	AC failure	Controller 1: 12V Supply Failure Power Supply 1: Mains Failure
Battery The system or a component of it has a battery problem. Call service tech.	1 - General	Battery	Power Supply 3: Battery Low / Missing
Reporting Panel could not send an event to the monitoring station. Call service tech.	1 - General	Reporting	Controller 6: ContactID Reporting Failure Keypad 2: Power Supply Low Voltage Power Supply 4: Output Voltage Low
Phone Line The telephone line is faulty or it has been disconnected. Call service.	1 - General	Phone line	Controller 7: Phone Line Fault

Trouble Message	Trouble Group	Trouble Group Options	Trouble Inputs
Power Problem The panel has registered a problem with the power supply, call service.	1 - General	Power	Controller 8: Auxiliary Fuse / Supply Fault Power Supply 4: Output Voltage Low Power Supply 5: Output Over-Current Failure Power Supply 6: Core Temperature Over-Temp Failure
Bell PGM A Bell/Siren is faulty or it is in tamper, verify fault or call service.	1 - General	Bell	Controller 9: Bell Siren 1 Tamper / Cut Controller 11: Bell Siren 1 Current Overload
System System Trouble has occurred. Press [ENTER] to view current system troubles.	2 - System		
Module Tamper The enclosure that houses a system device is open, call service tech.	2 - System	Module tamper	Keypad 1: Module Tamper Power Supply 1: Module Tamper Reader Expander 12: Reader 1 Tamper / Missing Reader Expander 13: Reader 2 Tamper / Missing
Module Loss A module has gone offline or a network error has occurred.	2 - System	Module loss	Controller 13: Module Communication Fault Keypad 8: Module Communication Fault Reader Expander 16: Module Communication Fault Power Supply 8: Module Communication Fault Output Expander 8: Module Communication Fault Input Expander 16: Module Communication Fault
Hardware A hardware problem on the panel or module exists, call service tech.	2 - System	Hardware fault	Controller 20: ReportIP Reporting Failure Controller 22: ModBUS Communication Failure Controller 24: Installer Logged In Controller 29: System Restarted Controller 33: Cross-Controller Communication Fault
Access Control Access Trouble has occurred, press [ENTER] to view current access troubles.	3 - Access		
Door Force A door that was secure has been forced open, verify the door or call service.	3 - Access	Forced door	Door 1: Door Forced Open

Trouble Message	Trouble Group	Trouble Group Options	Trouble Inputs
Door Ajar A door that was opened has been left open, verify the door or call service.	3 - Access	Door left open	Door 2: Door Left Open
Attempts A user has exceeded the no. times an invalid card/code can be presented.	3 - Access	Number attempts	Reader Expander 14: Door 1 Too Many Attempts Reader Expander 15: Door 2 Too Many Attempts

Health Status Messages

The controller's health status is a useful tool for diagnosing issues with modules and configuration.

You can view the current health status:

- On the homepage of the controller web interface
- In Protege GX, by right clicking on a controller record and selecting **Get health status**.
- In Protege X, on the **Controller Records | Controllers** page.

Category	Message	Cause	Solution
Controller status	The controller has restarted	The controller has rebooted since the last time this message was cleared. This can be caused by the controller losing power or restarting due to an error.	This message is for information only. In Protege GX, select the message and click **Clear** to remove it.
	Encryption is turned off	Controller encryption has not been initialized. Communications between the controller and Protege GX server are insecure. Protege GX only.	In **Sites | Controllers | Configuration**, click **Initialize**.
Module status	Expander is offline	The controller has lost communication with the expander module for at least five minutes.	If the controller has recently restarted, it may take up to five minutes for all modules to come back online. Check the physical connection between the controller and the expander module. Ensure that the expander module is addressed correctly. To prevent this message from appearing for modules that are not physically connected, enable the **Virtual module** option in the expander programming.
Record not functioning	Area has its Tamper Area disarmed	The area does not have its 24 hour (tamper) portion enabled. This prevents it from monitoring trouble inputs, tampers, shorts or 24 hour panic inputs.	Use the **Arm 24hrs** command to enable the 24hr portion of the area.
	Function is stopped	The programmable function is stopped and will not operate.	If the programmable function should be operating, use the **Start** command to start it. If it does not need to operate, no action is required.
	Service is stopped.	The service is stopped and will not operate. This will prevent central station reporting or other features from functioning.	If the service should be operating, use the **Start** command to start it. If it does not need to operate, no action is required.

Category	Message	Cause	Solution
Configuration updates	Area requires rearming due to input changes	The inputs assigned to the area or their input types have been changed, but the changes will not come into effect until the area is rearmed.	If you have added an input to the area or edited its input type, disarm and rearm the area. If you have removed an input from the area, you must disarm both the main and 24hr portions of the area, then rearm.
	Expander requires a module update/restart	The expander module programming has been changed. Some types of changes will not come into effect until the module has been updated.	Use the **Update module** command to update the module's configuration. To prevent this message from appearing for modules that are not physically connected, enable the **Virtual module** option in the expander programming.
Configuration errors	Access Level has too many Menu Groups assigned	The access level has more than one menu group assigned.	Remove all but one menu group from the access level. You may need to create a new menu group with all of the required settings.
	Access Level has too many Output Groups assigned	The access level has more than one output group assigned.	Remove all but one output group from the access level. You may need to create a new output group that contains all of the required outputs.
	Elevator car is assigned to multiple reader expanders	The elevator car is assigned to more than one reader expander.	Ensure that only one reader expander has this elevator car as the **Reader 1/2 elevator** (reader expander programming).
	Elevator car has contending Inputs	Two or more floors assigned to this elevator car have the same **Input**.	Correct the elevator programming so that all floors have different inputs assigned.
	Elevator car has contending Outputs	Two or more floors assigned to this elevator car have the same **Output**.	Correct the elevator programming so that all floors have different outputs assigned.
	Expander has its Physical Address set too high	The expander module's **Physical address** is above the maximum address that can be stored by the controller. It will not function correctly.	Change the **Physical address** of the module to a lower number and readdress the module.
	Input has an Area but no Input Type assigned	The input is missing an input type in one of the areas assigned to it. It will not raise alarms or perform any control functions.	Add an input type in the **Areas and input types** tab.

Defaulting Controllers

This section covers how to temporarily reset a controller to a known IP address, as well as how to default a controller to factory settings.

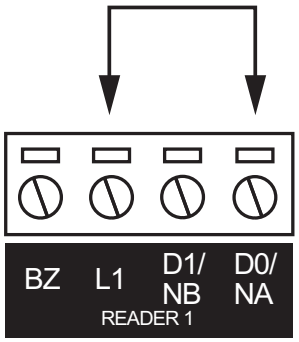
Temporarily Defaulting the IP Address

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 will also temporarily disable HTTPS security, which may help resolve some connection issues.

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.

Defaulting the IP Address of a Two Door Controller

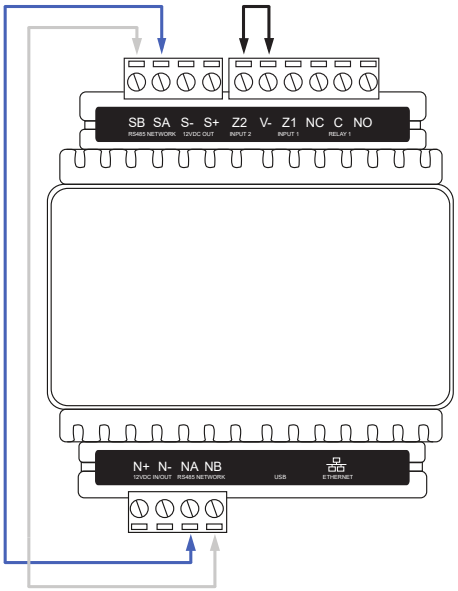
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



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

Defaulting the IP Address of a Single Door Controller

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 **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 2** to ground.



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

Accessing the Controller

5. 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
   - **Use HTTPS**: Disabled
6. Connect to the controller by entering http://192.168.111.222 into the address bar of your web browser, and view or change the IP address and other network settings as required.

   Remember to change the subnet of your PC or laptop to match the subnet of the controller.
7. Remove the wire link(s) and power cycle the controller again.
   The controller will now use the configured network settings.

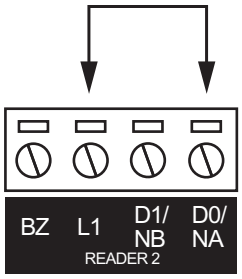
Defaulting a Controller

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

Defaulting a Two-Door Controller

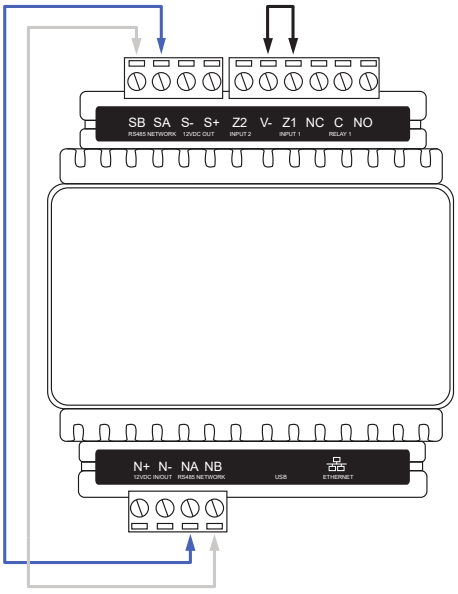
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.
5. Remove the wire link **before making any changes to the controller's configuration**.

Defaulting a Single-Door Controller

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 **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 1** to ground.



5. Power up the controller. Wait for the status indicator to begin flashing steadily.
6. Remove the wire links **before making any changes to the controller's configuration**.

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

Before making any changes to the controller's configuration or upgrading the firmware, **remove the wire link used to default the 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.

Protege GX Networking

This section provides some basic networking steps and troubleshooting to help you get your controllers online with Protege GX.

Always communicate with the person or team responsible for the network before starting to connect controllers.

Networking Local Controllers

The basic steps for bringing a defaulted Protege GX controller online in a local network are:

1. Find out the details of the Protege GX server and the network it is connected to. In most cases you will need:
   - The server's IP address or domain name
   - A fixed IP address that the controller can use
   - Subnet mask
   - Default gateway
   - DNS server (if using the domain name)
2. If you are setting up the server for the first time, allow the following services through the relevant firewalls:
   - GXSV.exe
   - GXEvtSvr.exe
3. If the controller was recently defaulted, **remove the default link**.
4. Use an ethernet cable to connect the controller to a laptop.
5. On the laptop, open **Settings** and navigate to **Network & internet > Ethernet**. Temporarily change the **IPv4 address** to 192.168.x.x (e.g. 192.168.1.1).
6. Browse to the controller's web interface. The default IP address is https://192.168.1.2.
7. Set a secure administrator password and log in.
8. On the **Settings** pages, enter the following settings:
   - Event Server 1 (the server IP address or domain name)
   - IP Address (of the controller)
   - Subnet Mask
   - Default Gateway
   - DNS server (if using a domain name)
9. Make a note of the controller's **Serial Number**.
10. Save and click **Restart**.
11. Once the controller has restarted, connect it to the network.
12. In Protege GX, navigate to **Sites | Controllers** and add or select the controller record.
13. Enter the following details:
    - Serial number
    - IP address (of the controller)
    - Download server
14. Save the record. After a few seconds, the controller should come online.
15. Once the controller is online and receiving downloads, navigate to the **Configuration** tab and click **Initialize controller encryption**.

Networking Remote Controllers

Consider a situation where the Protege GX server (in Building A) must communicate with both controllers on the same network (Controller A1 and Controller A2) and controllers on a remote network (Controller B1 and Controller B2 in Building B).

Set up the local controllers following the steps in Networking Local Controllers.

For the remote connections, you will need the following details:

- External static IP address of Building A
- External static IP address of Building B
- Unique static IP addresses for each controller on the network
- Subnet mask and default gateway for the router in Building B
- Unique ports that may be used for downloads and control for Controller B1 and Controller B2. The controllers in Building A can use the default ports.

  For example, the ports could be:

Controller	Event Port	Download Port	Control Port
Controller A1	22000	21000	21001
Controller A2	22000	21000	21001
Controller B1	22000	21002	21003
Controller B2	22000	21004	21005

First, program the controller records on the Protege GX server:

1. Add Controller B1:
   - Enter the **Serial number**.
   - Set the **IP address** to the external IP address of Building B.
   - Set the **Download port** to 21002.
   - Select the **Download server**.
   - Set the **Control and status request port** to 21003.
2. Add Controller B2:
   - Enter the **Serial number**.
   - Set the **IP address** to the external IP address of Building B.
   - Set the **Download port** to 21004.
   - Select the **Download server**.
   - Set the **Control and status request port** to 21005.

   Leave the event server port set to 22000.

Set up Controller B1 in the web interface:

1. Set **Event Server 1** to the external IP address of Building A.
2. Set the **Event Port**, **Download Port** and **Control Port** as per the table above.
3. Enter the controller's **IP Address**.
4. Enter the **Subnet Mask** and **Default Gateway** for the network.

Set up Controller B2 in the same way, using the unique ports for that controller.

The Building B router needs port forwarding rules to direct incoming downloads and controls to each controller:

1. Incoming messages on port 21002 are sent to Controller B1, port 21002.
2. Incoming messages on port 21003 are sent to Controller B1, port 21003.

3. Incoming messages on port 21004 are sent to Controller B2, port 21004.
4. Incoming messages on port 21005 are sent to Controller B2, port 21005.

Once each controller is online and receiving downloads, navigate to the **Configuration** tab and click **Initialize controller encryption**.

Networking with a Cellular Modem

The PRT-4G-USB cellular modem can be used to connect a controller to Protege GX in place of a traditional ethernet network.

For more information about using the cellular modem, see the Protege DIN Rail Cellular Modem Configuration Guide.

1. Ensure that the SIM you intend to use allows inbound connections and has been validated for use with the cellular modem. For more information, see the Prerequisites section of the Protege DIN Rail Cellular Modem Configuration Guide.
2. Before you begin, you will need:
   - An external static IP address or hostname for the Protege GX event server.
   - The APN, username and password for the cellular network
3. Insert the SIM into the cellular modem's Micro-SIM slot.
4. If the controller was recently defaulted, **remove the default link**.
5. Use an ethernet cable to connect the controller to a laptop.
6. On the laptop, open **Settings** and navigate to **Network & internet > Ethernet**. Temporarily change the **IPv4 address** to 192.168.x.x (e.g. 192.168.1.1).
7. Browse to the controller's web interface. The default IP address is https://192.168.1.2.
8. Set a secure administrator password and log in.
9. On the **Settings | General** page:
   - Set **Event Server 1** to the external IP address or hostname of the Protege GX event server.
   - Set the **Primary Adaptor** to USB Ethernet.
10. In **Settings | Adaptor - USB Ethernet**, set the following:
    - Cellular APN
    - Cellular Username
    - Cellular Password
11. Make a note of the controller's **Serial Number**.
12. Save and click **Restart**.
13. Log in to the controller again. In **Settings | Adaptor - USB Ethernet**, ensure that the cellular modem has connected to the network provider. Note the **IP Address** assigned by the provider.
14. In Protege GX, navigate to **Sites | Controllers** and add a new controller record.
15. Enter the following details:
    - Serial number
    - IP address (as provided by the cellular network)
    - Enable **Dynamic IP address update**
    - Download server
16. Save the record. After a few seconds, the controller should come online.
17. Once the controller is online and receiving downloads, navigate to the **Configuration** tab and click **Initialize controller encryption**.

Troubleshooting Controller Connections

For more detailed troubleshooting steps, see Application Note 193: Troubleshooting Protege GX Controller Connectivity.

Can't browse to web interface:

1. It is not possible to browse to the web interface over a cellular network connection. Use a local ethernet connection instead.
2. Add **https://** to the start of the IP address. If this fails, add **http://** to the start of the IP address.
3. Try the previous IP address. You may need to restart the controller to update the network settings.
4. Check that your computer is on the same network as the controller. If necessary, change the computer's IP address temporarily.
5. If you do not know the current network settings, connect a keypad to the controller. Log in with an installer PIN (**0000**) and navigate to **Menu > 4. Install > 2. IP config > 1. View/Edit IP**. Scroll up to view the IP address, subnet mask and gateway.
6. Connect a default link on reader port 1 and power cycle to temporarily set the controller's address to 192.168.111.222.

Not receiving events, controller status is offline:

1. Check that the controller is connected to the network.
2. Check that the Protege GX event service is running.
3. Check that GXEvtSvr.exe is allowed through the firewall.
4. If the controller is remote, ensure that all required port forwarding rules are enabled on the server network's router.
5. Check that the **Event Server 1** IP address in the controller is correct. If using a domain name, confirm that you have the correct **DNS Server** set.
6. In **Sites | Controllers**:
   - Check that the **Serial number** matches this controller.
   - Check that the **IP address** matches this controller.
7. In **Global | Event server**:
   - Check that the **Computer name** is correct. If you change this, restart the event service.
   - Check that the **Port** matches the **Event Port** in the controller.

Not receiving events, controller status is online:

1. Your selected event report may be filtering out relevant events. Try running the default All Events report to see whether the expected events are being received.
2. Check that the Save Events action still exists in **Events | Actions**. If it does not exist, create a new action with these settings:
   - **Type**: Save to database
   - **Event filter**: All events
3. Check whether the server's hard drive is full. If it is, contact ICT technical support.
4. If you are using SQL Express, the server may have reached the 10GB limit. Check this in SQL Server Management Studio:
   - Right click on the ProtegeGX database.
   - Select **Reports > Standard Reports > Disk Usage**
   - Repeat for the ProtegeGXEvents database and add the totals.

   If the server has reached the limit, contact ICT technical support.

5. Your event server may have reached the 2.1 billion Event ID limit and is unable to save new events. If this occurs:
   - **Immediately** open the Windows Services Manager and locate the Protege GX Event Service.
   - Right click and select **Properties**. Set the **Startup type** to Disabled.
   - Click **Apply**.
   - Click **Stop**. While the event service is stopped, controllers will save incoming events to prevent them from being lost (up to 50,000 events per controller).
   - Contact ICT Technical Support as soon as possible for assistance with backing up your events database and creating a new one.

Not receiving downloads / manual commands, last download status is failed:

After each change, send a force download to the controller to see whether the issue is resolved.

1. Ensure that the controller is online with the event server first.
2. Open the Windows Services Manager and check the Protege GX Download Service.
   - If it is not running, start it.
   - If it is running, restart it.
3. If the controller is remote, ensure that all required port forwarding rules are enabled on the remote network's router.
4. Check that the firewall does not block outbound communications from GXSV2.exe (typically outbound communications are allowed by default).
5. In **Sites | Controllers**:
   - Check that the **Download port** and **Control and status request port** match those in the controller web interface.
   - Ensure that there is a **Download server** set.
6. In **Global | Download server**, ensure that the **Computer name** is correct. If you change this, restart the download service.
7. Check the **Download server diagnostic window**. If the controller is receiving download traffic but the download does not complete successfully (the 'Saving Packet to File' message never appears), the controller may be encrypted while the server is not. The controller may appear online in this scenario.

   The only way to resolve this issue is by defaulting the controller, then restoring the connection settings. If downloads are now successful, re-enable encryption.

   Defaulting the controller should be a last resort on a live site, as this will delete the existing programming and leave the controller inoperable until the downloads are functional again. Check all other possible causes of download issues before defaulting the controller.

Reporting Services

These troubleshooting steps will help you resolve issues with reports not being received by the central monitoring station.

No reports are being received at all:

1. Ensure that the service has been downloaded to the controller.
2. Start the service.
3. Ensure that all of the information provided by the central monitoring station has been programmed correctly.
   For phone line reporting, check:
   - All phone numbers
   - Schedules assigned to the phone numbers
   - **Client code** in the service

   For IP reporting, check:
   - **Client code** in the service
   - **Reporting protocol**, **Encryption level** and **Encryption key**
   - All IP addresses and port numbers
4. For IP services, ensure that the **Adaptor** is correct. Select Cable for the ethernet network or USB ethernet for a cellular modem.
5. Ensure that the required reporting options are enabled in the **Options** tab.
6. If the service is not a backup service, disable **Service operates as backup**.
7. Ensure that the service is assigned to an area (**Configuration** tab).
8. For IP reporting over ethernet:
   - Log in to the controller's web interface. In **Settings | Adaptor - Onboard Ethernet**, ensure that the **Default Gateway** matches the gateway of the network.
   - Ensure that the IP port used for reporting is open for outbound and inbound traffic. The port must be open on the network the controller is connected to, not the server network.
9. For IP reporting over 4G, log in to the controller's web interface. In **Settings | Adaptor - USB Ethernet** (Protege GX) or **System | Settings | Adaptor USB Ethernet** (Protege WX), confirm that the cellular modem is online with the mobile network provider.

Area arming/disarming reports are not being received:

1. Ensure that the **Report open** and **Report close** options are enabled in the service programming (**Options** tab).
2. Ensure that the service is assigned to the area (**Configuration** tab).
3. Ensure that the **Client code** for the area is correct (**Configuration** tab).
   - To use a unique client code for this area, enter it here.
   - To use the same client code as the service, set to FFFF.
4. Ensure that the **Reporting options** are enabled in the area programming (**Options (1)** tab).

Input or trouble input reports are not being received:

1. Ensure that **Report alarms**, **Report tampers**, **Report restore** and **Report bypass** options are enabled in the service (**Options** tab).
2. Ensure that the input or trouble input has an input type and area assigned.
3. Ensure that the service is assigned to the area (**Configuration** tab).
4. Ensure that **Generate alarms** and/or **Generate 24hr alarms** are enabled in the input type (**Options (1)** tab).

5. Ensure that the **Reporting options** are enabled in the input type (**Options (1)** tab).
6. Ensure that the area is armed and/or has its 24hr area enabled.

Enabling service logging:

To help you determine where the reporting service is failing, you can enable logging in the service.

- For a phone line service, enable **Log modem events to event buffer** in the **Options** tab.
- For an IP service, enable the various logging options in the **Options** tab.

Generate a report and monitor the live events. This should show you whether the controller is failing to send the event or whether it is not getting a response from the central monitoring station.

Once you have resolved the issue, always disable the logging settings as they generate a very large number of events.

Access

This section covers configuration issues which may cause access to be denied to a user.

Door Access Denied

If the card readers are online and responding correctly but the user is still denied access to the door, you will hear a long beep after the user presents their card or PIN. First, ensure that all programming changes have been downloaded to the controller. If access is still denied, there is an issue with the programming of the user or access level record. The event log can help you identify where the issue has occurred.

The table below describes a number of common events which can help with troubleshooting user access. The causes for access to be denied are ordered from lowest to highest priority.

Event Example	Causes
Read Control Error RD1 Port Port 1 Error Door Is Not Valid Or Not Programmed For Port	There is no door programmed for this reader port. • For Wiegand or ICT RS-485 readers, check the **Reader 1/2 door** in the reader expander programming, **Reader 1/2** tab. • For OSDP readers, check the **Reader one door** in the smart reader programming, **Reader** tab.
Read Raw Data (1:1) At Entry Reader On Door Office Door (RD1 Port 1)	The controller does not recognize this card number. Possible causes: • The card has not been assigned to a user. Right click on the event to assign the card. • The user record has not been downloaded to this controller. Ensure that the user has an access level assigned and that the access level includes a door or area from this controller. Wait for the download to complete. • If the card read was received at a smart reader, the credential may not match one of the **Reader credential match types**.
User INVALID USER PIN Not Valid RD1 Using Port Port 1 In Keypad Input	The controller does not recognize this PIN code. Possible causes: • The PIN has not been assigned to a user. • The user record has not been downloaded to this controller. Ensure that the user has an access level assigned and that the access level includes a door or area from this controller. Wait for the download to complete. • The PIN does not match another credential entered by the user (e.g. when the door is using card + PIN operation, and the user enters the incorrect PIN).
Door Office Door Invalid Credential Supplied By Brett Lamb	The door requires multiple credentials, and the second credential supplied does not match the first.
User Brett Lamb Record Disabled At RD1 Using Port Port 1	Possible causes: • The user record has been disabled. • The user's credential has been disabled.
User Brett Lamb Record Expired At RD1 Using Port Port 1	Possible causes: • The user record has expired. • The user's access level has expired.

Event Example	Causes
User Brett Lamb Schedule Not Valid At Office Door Using Any Access Level	All of the user's access levels are currently invalid due to schedules. Possible causes: • The **Schedule** set on the access level in the user programming is not valid. • The **Operating schedule** set in the access level programming is not valid.
User Brett Lamb Door Not Allowed Office Door Using Any Access Level	The user does not have this door in any of their access levels, or the door is not valid due to a schedule. Check the access level's doors and door groups.
User Brett Lamb Access Denied By Door Lockdown At Office Door	The door is in lockdown state and does not allow access in this direction.
User Brett Lamb Denied By Invalid Door Type At Office Door Using Door Type Door Type (DTUnknown)	The door type is not set or incorrectly programmed. Possible causes: • There is no **Door type** set in the door programming. • The user's access level has **Use access level door type** enabled, but there is no **Access level door type** set in the door type.
User Brett Lamb Denied By Door Type Schedule At Office Door Using Door Type Door Type	The **Operating schedule** for the door type is invalid, but the **Secondary door type** is missing or not programmed correctly.
User Brett Lamb Entry Antipassback Failure At Door Office Door Area Office Required Area Reception	The door type is configured for hard antipassback and the user has committed an antipassback violation. Access is denied. • The first area listed in the event is the last known area that the user entered. The second area listed is the required area to access this door. In this example, Brett Lamb needs to be in the Reception area to enter the Office Door. However, he was last recorded entering the Office area. Therefore he is denied access. • Right click on the event to reset the user's antipassback status.
User Brett Lamb Soft Antipassback Failure At Office Door Area Office User Area Reset to Office	The door type is configured for soft antipassback and the user has committed an antipassback violation. Access is granted. • The area listed in the event is the area that the user is currently entering. The system automatically resets the user's area to this new area. In this example, Brett Lamb is incorrectly attempting to enter the Office area. The system grants access and resets his current area to the Office area.
User Brett Lamb Denied Entry At Office Door By Area Status Office Using Access Level Staff	The user is prevented from accessing the door because the area behind the door is armed. Possible causes: • By default, the user is not allowed access if they are not able to disarm the area. Ensure that this area is included in the user's disarming area groups. • If the **Deny entry if inside/outside area is armed** option is enabled in the door programming, **Advanced options** tab, access will be denied even if the user can disarm the area.

Event Example	Causes
User Brett Lamb Denied Entry At Office Door By Area Count Office Using Access Level Staff	The area which the user is attempting to enter has user counting enabled (area programming, **Options (1)** tab) and currently contains the maximum number of people.
User Brett Lamb Entry Denied By Interlock Office Door	The door has an interlock door group assigned (door programming, **General** tab) and one or more of the doors in the group are open/unlocked. To allow access, close and lock all other doors in the interlock group.
User Brett Lamb Denied Entry At Office Door By Entry Mode Error...	The user has presented a type of credential which is not allowed by the door type. The second part of the event gives more details about the error, for example: • Door programmed for card only operation using PIN input The door type requires a card, but the user has entered a PIN. • Door programmed for PIN only operation using card input The door type requires a PIN, but the user has badged a card. • Door waiting for PIN mode using card input The door type requires card and PIN. The user badged their card, then badged again instead of entering a PIN. • Door waiting for bio mode using card input The door type requires a biometric credential or credential type, but the user badged a card.
User 'Brett Lamb' Denied Access At Door 'Office Door' Because User Is Not a Dual Access Master/Provider	The door is configured for dual authentication (door type programming, **Options** tab) but the user is not a dual access master or dual access provider (user programming, **Options** tab).

Keypad Login Denied

The table below indicates issues that may block a user from logging in to a keypad.

Event Example	Keypad Message	Causes
Trouble Input KP 1 Too Many Attempts Opened	Keypad 001 is locked out.	An incorrect/unknown PIN has been entered too many times. The keypad will unlock after the **Lockout keypad time** expires.
User INVALID USER Invalid PIN Code At KP 1	Incorrect code please try again	Possible causes: • The user has entered the wrong PIN code. • The user record has not been downloaded to this controller. Ensure that the user has access to at least one record on this controller and wait for the download to complete.
User Jane Smith Disabled At KP 1	User not valid record disabled	The user record is disabled.
User Jane Smith Record Expired On KP 1	User not valid record expired	Possible causes: • The user record has expired. • The user's access level has expired.

Event Example	Keypad Message	Causes
User Jane Smith Schedule Not Valid At KP 1	Invalid Schedule please try again	Possible causes: • The **Schedule** set on the access level in the user programming is not valid. • The **Operating schedule** set in the access level programming is not valid.
User Jane Smith Menu Group Schedule Not Valid At KP 1 Using Staff Access Level	Invalid Menu please try again	Possible causes: • The user has no menu group in their access level • The **Operating schedule** of the menu group is not valid and there is no **Secondary menu group** to fall back to. • This keypad is not included in the **Keypad groups** for the user's menu group.
User Jane Smith Menu Options Not Valid At KP 1 Using Staff Access Level	Invalid Menu, please try again	Possible causes: • The user's menu group doesn't grant access to any menus. Check the **Secondary menu group** if there is one. • The **Menu group for this keypad** doesn't grant access to any menus. • The user's menu group and the **Menu group for this keypad** don't have any menus in common.

Another issue that may occur is that the user can log in, but the menu they are looking for is not available. Possible causes are:

- The menu is disabled in the menu group or secondary menu group.
- Some menus are no longer used in Protege systems:
  - Time (6)
  - System (8)
  - Advanced installer (4, 8)
  - Extended time menus (6, 2-4)
- In Protege WX, only users with **User Can Edit User Setting from Keypad** enabled can edit other user records in the **2. Users** menu. By default, the user can only edit their own PIN code.

Area Arming/Disarming Failure

Arming/Disarming from Keypad

The table below indicates issues that may prevent a user from arming or disarming an area from the keypad once they have successfully logged in.

Issue	Keypad Message	Causes
No areas are displayed in the Areas menu	No Keypad Area Group defined	The user has access to the area menu, but cannot arm/disarm any areas available from this keypad. Check the area groups in the access level.
	No current area access on keypad	The user does not currently have access to any areas included in the **Area group for this keypad**.
	No access to the PRIMARY Area	The user does not have access to the **Area this LCD belongs to** for the keypad.
Only some areas are displayed in the Areas menu		Possible causes: • Areas are restricted by the area groups in the access level. • Areas that are included in the **Arming area groups** but not the **Disarming area groups** will only be displayed when they are currently disarmed (i.e. available to arm). • Areas are restricted by the **Area group for this keypad**. • Not all areas are available on this controller.
The area detects open or tampered inputs.	Input 1 is OPEN	Close or bypass the inputs to allow arming. Alternatively, enable **Exit alley input do not test it** in the input type to allow an input to remain open during arming.
The area begins arming, then fails	Trouble fault failed to ARM	The **Do not arm if trouble condition** setting is enabled in the area and there is a trouble input open in the system. Acknowledge or resolve all trouble messages on the keypad to arm (see page 17).
	Area can not be armed. There are 5 User(s) in area. Press [Disarm] to halt arming.	The **Prevent arming on count not zero** setting is enabled in the area and there are still users in the area. Ensure that all users have left and badged at the exit reader. If the user count is incorrect, badge at the exit reader until the count goes to zero.
	Too many bypassed input (s)	The number of bypassed inputs exceeds the **Maximum bypass input count** for this area. Close and remove the bypasses from some inputs.
Disarming fails	Interlock Active please wait...	The area has an **Interlock area group** programmed and at least one area in that group is currently disarmed. All areas in the group must be armed to allow this area to disarm.
Disarming is delayed	Office in DISARM delay Office in CODE delay	**Vault control area** and/or **Dual code vault control** are enabled in the area programming. Wait for the disarm delay to expire, then log out and get a second user to log in and disarm the area.
Cannot press Right to arm/disarm the area group	Area group is not assigned	There is no **Area group for this keypad** selected in the keypad programming.
	No access to AREA Groups	Possible causes: • **Area group control allowed** is disabled in the menu group. • **Allow area group selection access** is disabled in the keypad.
Cannot press Left to arm/disarm 24hr area	No access to TAMPER Control	Possible causes: • **Tamper area control allowed** is disabled in the menu group. • **Allow 24hr area access** is disabled in the keypad.

Issue	Keypad Message	Causes
Cannot stay arm the area	STAY Arming not allowed	Possible causes: • **Stay arming** is disabled in the menu group. • **Enable stay arming** is disabled in the area.
Cannot force arm the area	FORCE Arming not allowed	Possible causes: • **Force arming** is disabled in the menu group. • **Enable force arming** is disabled in the area.
Some inputs cannot be force armed	Input 1 is OPEN	**Force input** is disabled in the input type.
Cannot instant arm the area by pressing the arm key again	Area is already armed or arming	Possible causes: • **Instant arming** is disabled in the menu group. • **Enable instant arming** is disabled in the area.

Unattended Arming/Disarming

The table below indicates issues that may prevent the area from being armed or disarmed remotely - for example, by an operator, schedule or programmable function.

Keep in mind that unattended automatic arming methods use force arming, so any issue that can prevent force arming will prevent the area from arming by schedule, automatic rearm or programmable function.

Issue	Event	Causes
The manual command has no effect		The `NoRemoteArm` or `NoRemoteDisarm` command is set in the area.
The area does not arm/disarm on schedule		Possible causes: • The periods and holidays of the **Arm/Disarm schedule** are not correct. • **Disarm area when schedule starts** or **Arm area when schedule ends** is not enabled.
The arming attempt fails	Area Office Arming Failure By Operator/Schedule/SYSTEM USER	Possible causes: • The area is already armed or in delay • If you are force arming, **Enable force arming** is disabled in the area • If you are stay arming, **Enable stay arming** is disabled in the area. • If you are instant arming, **Enable instant arming** is disabled in the area.

Issue	Event	Causes
Arming begins, but fails	Area Office Arming Failure By Operator/Schedule/SYSTEM USER Area Office Arming Cancelled By Operator/Schedule/SYSTEM USER	Possible causes: • The area received a disarm command before arming was complete. • The area contains open or tampered inputs. Close or bypass the inputs to allow arming. Alternatively, enable **Exit alley input do not test it** in the input type to allow an input to remain open during arming. • If you are force arming, open inputs need the **Force input** option enabled in the input type. Alternatively, enable **Use unattended brute force arming** in the area. • The number of bypassed inputs exceeds the **Maximum bypass input count** for this area. Close and remove the bypasses from some inputs. • The **Do not arm if trouble condition** setting is enabled in the area and there is a trouble input open in the system. Clear all trouble messages from the keypad to arm (see page 17). • The **Prevent arming on count not zero** setting is enabled in the area and there are still users in the area. Ensure that all users have left and badged at the exit reader. If the user count is incorrect, badge at the exit reader until the count goes to zero.
Disarming fails	Area Office Disarm Denied By Interlock For Operator/Schedule/SYSTEM USER	There is an **Interlock door group** programmed in the area and at least one area in that group is currently disarmed. All other areas in the group must be armed to allow disarming of this area.

Replacing System Components

This section outlines how to replace system components in case of an upgrade, issue or hardware failure. It is recommended that you carry out these procedures during periods of low activity or scheduled system maintenance.

If you need assistance with these processes, contact ICT Technical Support.

Replacing the Protege GX Server

See the Protege GX Installation Manual for instructions on backing up and restoring databases and encryption certificates.

1. Contact ICT Customer Services to tell them that your server hardware profile will be changing.
2. Stop the Protege GX services. While the services are stopped, the controllers will save incoming events (up to 50,000 per controller).
3. Back up the programming and event databases. If the database is encrypted, export the encryption certificates.
4. Uninstall Protege GX from the old server.
5. Disconnect the old server from the network. Connect the new server with the same IP address and/or hostname.

   If the IP address or hostname of the server changes, you may need to update the event server settings in the controllers.
6. Install Protege GX on the new server and activate the license.

   Ensure that the new Protege GX installation is the same version or higher.
7. Stop the Protege GX services. Restore the encryption certificates and databases to the new SQL Server instance.
8. If you are restoring a database from an older version to a later version, uninstall and reinstall Protege GX to upgrade the database.
9. Start the Protege GX Data Service.
10. In Protege GX, navigate to **Global | Download server** and update the **Computer name**.
11. Update the **Computer name** in **Global | Event server**.
12. Restart the Protege GX Event Service. You should start receiving events from controllers.
13. Start the Protege GX Download Service.

Replacing Controllers

To replace a Protege GX controller:

1. Disconnect the old controller from the ethernet network, RS-485 module network and other hardware.
2. In Protege GX, navigate to **Sites | Controllers**. Replace the **Serial number** of the old controller with that of the new one.
3. In the **Configuration** tab, click **Disable controller encryption**.
4. If the new controller has been used on a different server, default the new controller (see page 23).
5. Log in to the new controller's web interface. In **Settings**, enter the same IP settings, event server and ports as those of the old controller, then restart the controller.
6. Connect the new controller to the networks and hardware.
7. In Protege GX, right click on the controller record and select **Force download**. The controller should receive the download and come online.
8. Once the controller is online, in the **Configuration** tab click **Enable controller encryption**.

To replace a Protege X controller:

1. Contact ICT Customer Services with the new controller's serial number to register it for use with Protege X.
2. Disconnect the old controller from the ethernet network, RS-485 module network and other hardware.
3. In Protege X, navigate to **Controller Records | Controllers**. Click **Unpair**.
4. Enter the **Serial Number** of the new controller.
5. Log in to the new controller's web interface. In **System | Settings**, update the IP settings if required and select **Enable Cloud**. Restart the controller.
6. Connect the new controller to the networks and hardware.
7. In Protege X, click **Pair & Sync**. When you receive the "Controller Download Complete" message, the controller is ready to operate normally.

To replace a Protege WX controller:

1. Take a backup of the old controller's programming in **System | Backup**, or retrieve a previous backup.
2. Disconnect the old controller from the ethernet network, RS-485 module network and other hardware.
3. Log in to the new controller and register it in **System | Licensing**.
4. Restore the backup in **System | Backup**.
5. In **System | Settings**, enter the same IP settings as those of the old controller, then restart the controller.
6. Connect the new controller to the networks and hardware.

Replacing Expanders

1. Disconnect the old expander from the RS-485 module network and any inputs, outputs or card readers.
2. Connect the new expander to the module network and hardware.
3. Set the new expander's address to the same as that of the old expander.
   - In Protege GX, navigate to **Sites | Controllers**, right click the controller and select **Module addressing**.
   - In Protege X, navigate to **Controller Records | Controllers** to find the **Module Addressing** section.
   - In Protege WX, use the **Expanders Wizard**.
   - To address a keypad, power cycle it and then press **[X]**, **[Enter]**. Enter the new address and press **[Enter]** to save.

Sometimes the old expander can remain in the module addressing window even after being physically disconnected. To free up the address, module update the expander record. This will fail, but the address should become available.

4. Module update the new expander. The expander should start operating as normal using the programming from the original expander.

Replacing Card Readers

1. Disconnect the old card reader from the reader port.
2. Connect the new card reader.
3. If the reader needs any custom config, apply it within two minutes of the reader starting up using the Protege Config App or config card.
4. Wiegand and RS-485 readers should connect automatically.

   For OSDP readers, put the card reader into installation mode, then send an **OSDP install mode** command to the reader expander.

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