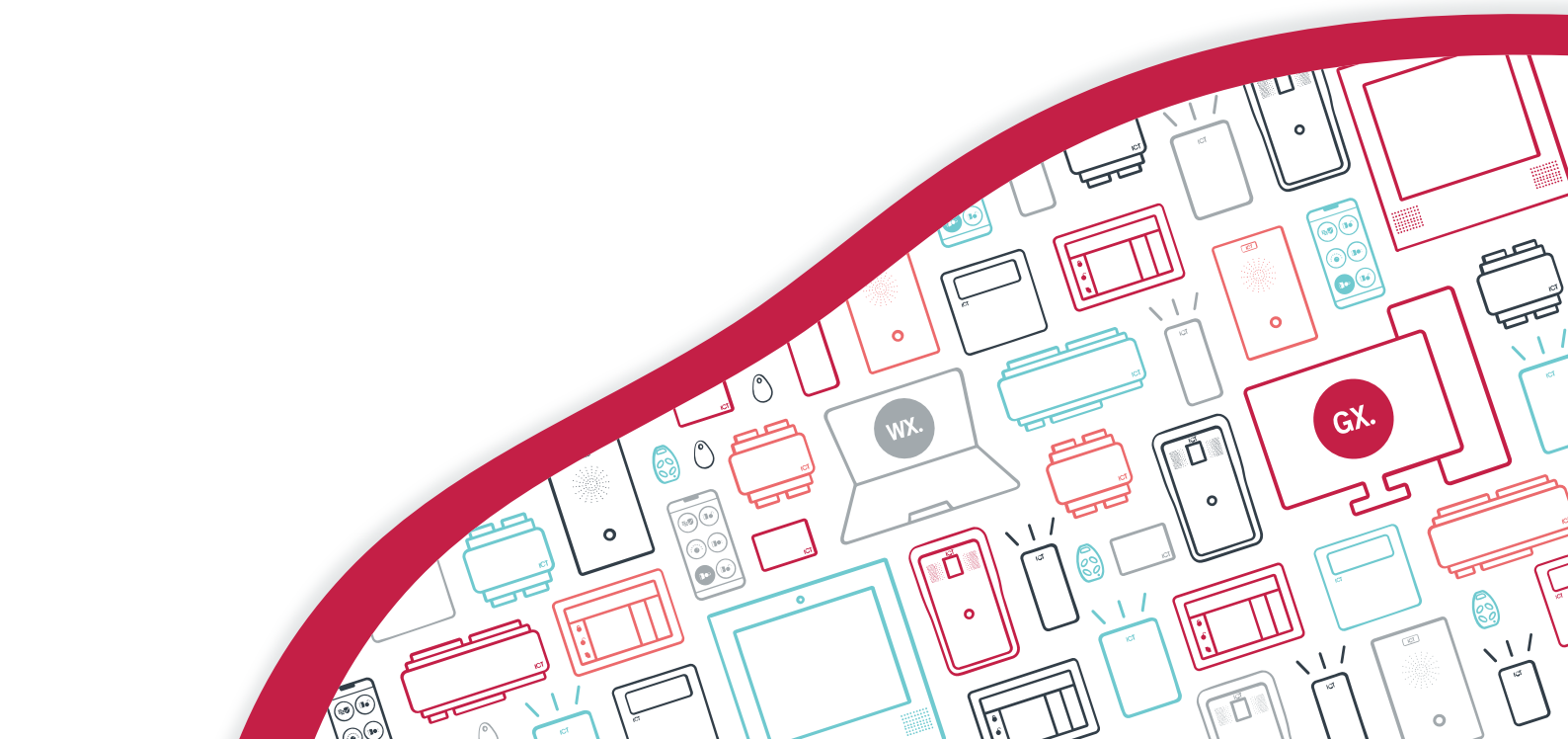
PRT-GX-SRVR

Protege GX Setup Guide



Last Published: 23-Dec-24 2:01 PM

Contents

Introduction

This document is a step-by-step guide to setting up your Protege GX system and quick reference for programming common features.

This guide includes instructions for configuring:

- Controllers, expander modules and other hardware
- Access control and user management
- Intruder detection, trouble monitoring and offsite reporting
- System monitoring and reports
- Common advanced features

We also provide a printable checklist (see next page) to help you ensure that everything is complete before you leave site.

We assume that you have installed and licensed the Protege GX software and completed security configuration and initial setup - you can use the **Installation Checklist** in the Protege GX Installation Manual to make sure everything is ready. If you don't have the hardware yet, don't worry: it is easy to pre-program the whole system and connect everything up once you get on site.

As every Protege GX system has unique requirements, not every feature and setting you need can be covered here. Always confirm the client's requirements before you begin. For more help with the system, see:

- Protege GX Operator Reference Manual (click **About | Help** in the software)
- Protege Troubleshooting Guide
- Application notes for specific features and integrations (available on our website)

If all else fails, ICT Technical Support is always happy to help.

Site Setup Checklist

The following checklist indicates what is required to set up a 'standard' Protege GX site. You can print these pages for easy reference as you work through the setup guide.

Installation

- ☐ Complete all setup steps in the Protege GX Installation Manual

Before You Start Programming

- ☐ Take a backup of the current configuration (navigate to **Global | Global settings** and click **Backup now**)

Controller and Module Hardware

- ☐ Add controllers (see page 8)
- ☐ Bring controllers online (see page 8)
- ☐ Set controller time (see page 11)
- ☐ Enable onboard reader expander (see page 12)
- ☐ Bring expander modules online (see page 12)
- ☐ Configure input settings (see page 13)
- ☐ Deactivate input and output events (see page 13)

Schedules

- ☐ Create holiday groups (see page 15)
- ☐ Create schedules (see page 15)

Access Control

- ☐ Bring card readers online (see page 16)
- ☐ Program doors (see page 17)
- ☐ Program latch unlocking (see page 18)

Intruder Detection

- ☐ Configure keypads (see page 20)
- ☐ Create areas (see page 20)
- ☐ Program arming/disarming (see page 21)
- ☐ Program inputs to activate alarms (see page 22)
- ☐ Walk test inputs (see page 22)

Trouble Monitoring

- ☐ Create system area (see page 23)
- ☐ Program trouble inputs to activate alarms (see page 23)
- ☐ Arm system area

User Management

- ☐ Create groups (see page 24)
- ☐ Create access levels (see page 24)
- ☐ Create user records (see page 24)

Offsite Reporting

- ☐ Create primary reporting service (see page 27)
- ☐ Create backup reporting service
- ☐ Start primary service
- ☐ Assign reporting service to areas (see page 29)
- ☐ Send central station report to monitoring station (see page 29)

Monitoring and Reports

- ☐ Create status pages or floor plans (see page 30)
- ☐ Create event reports (see page 31)
- ☐ Create user reports (see page 32)
- ☐ Export programming for site documentation (see page 33)

Software Management

- ☐ Create roles (see page 35)
- ☐ Create operators (see page 35)

Before You Leave Site

- ☐ Log out of keypad
- ☐ Check heath status (**Sites | Controllers**)
- ☐ Check system area for trouble input alarms
- ☐ Arm areas and lock doors
- ☐ Inform central monitoring station that you are leaving site

Controllers and Module Hardware

This section covers the required steps for programming controllers and expanders, bringing them online and configuring them.

You can complete most of the programming in this guide without controllers or modules connected. If you do not have hardware available, simply skip the steps related to bringing controllers online and addressing expanders and complete them when the modules are connected.

Adding a Controller

The easiest way to add a controller and its related modules is through the controller wizard. This allows you to automatically add programming for the controller, expander modules, inputs, outputs, trouble inputs, doors and other features of the site. You can add more expander records later as required.

1. Navigate to **Sites | Controllers**.
2. Click **Add**.
3. Select **Use the controller wizard**.
4. Enter a **Name** for the controller. You can select **Prepend controller name to added records** to help distinguish the records that belong to this controller.
5. Set the **Type** of controller you wish to add.
6. If the controller will be used for access control, you can set the **Inputs** to 0. The inputs will be provided by the corresponding reader expander record.
7. Set the **Type** and number of keypads and expanders that will be connected to the controller.

   If you are using the controller's onboard reader expander, add one extra reader expander to represent it.
8. Under **Options**, you can select some additional default settings for your site:
   - **Create "Installer" menu group**: Creates a menu group with all permissions enabled. Typically only one is needed per system, so you can disable this setting if you already have one.
   - **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 default Report ID mapping for inputs. We recommend the Large mapping for most sites, but you can change this later if required.
9. The default settings in the **Doors** section will automatically program two doors per reader expander, create trouble inputs and program their locks and alarm beepers. Edit these settings if required.
10. Click **Add now**.

Bringing a Controller Online

Before you attempt to bring the controller online, consult the site's IT team about the architecture of the network and reserve the IP addresses and ports that you need. ICT Technical Support is not able to help you resolve networking issues.

If you need more help with bringing controllers online, see:

- Protege Troubleshooting Guide
- Application Note 193: Troubleshooting Controller Connectivity
- Protege GX Integrated System Controller Configuration Guide

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**.

Setting the Controller Time

You must set the appropriate time zone and daylight savings settings for the controller to ensure that schedules and event records operate correctly.

The recommended method for keeping the controller's time accurate is to synchronize all controllers to the same time server. There may be a preferred time server that is used on the local network - discuss with the site's IT team. Alternatively, use the NTP Pool Project to find online time servers in your region.

If the controller is in a region with daylight savings, first program a daylight savings record:

1. Navigate to **Programming | Daylight savings**.
2. In the toolbar, select the **Controller** you are programming.
3. Add a new record with a descriptive name (e.g. NZ Daylight Savings).
4. Enter the start and end days for daylight savings time in this region.
5. If all controllers will be in the same region, in the **Options** tab select **Apply to all controllers**.
6. Click **Save**.

To set up the time server:

1. If you are using an online time server, ping it to get an IP address:
   - Identify an appropriate pool to use as a time server (e.g. 0.oceania.pool.ntp.org).
   - Open a command prompt (press Windows, type **cmd** and press Enter).
   - Enter `ping` followed by the pool name. For example:

     ```
     ping 0.oceania.pool.ntp.org
     ```
   - Press Enter. The response should include the IP address.
   - Repeat with another pool to get a secondary time server for backup.

   It is recommended that you get a different IP address each time you set up a new site. This ensures that not all of your sites are reliant on a single time server.
2. Navigate to **Sites | Controllers**.
3. Enter the following settings in the **Time update** tab:
   - Enable **Automatically synchronize with an internet time server**.
   - Enter the IP address for the **Primary SNTP time server** and **Secondary SNTP time server**.
   - Set the **Time zone**.
4. Click **Save**.

If not using a time server, set the controller's time based on the server time:

1. Navigate to **Sites | Controllers**.
2. Right click on the controller and select **Set controller date time**.

Addressing Modules

After you have programmed all of the modules required for your site, you can address them and bring them online.

Addressing the Onboard Reader Expander

1. Navigate to **Sites | Controllers | Configuration**.
2. Set **Register as reader expander** to 1.
3. Set the **Onboard reader lock outputs** to Controller relay 3/4 outputs.
4. Click **Save**.

Addressing Keypads

1. Power cycle the keypad.
2. When the keypad displays version information, press **[X]**, then **[ENTER]**.
3. Enter the new address. This must be a number between 1 and 255.
4. Press **[ENTER]** to save the setting.

Addressing Expanders

1. Connect all modules to the RS-485 network and wait until they boot up.
2. Navigate to **Sites | Controllers**.
3. Right click on the controller record and select **Module addressing**.
4. The module addressing window will display the modules that the controller can detect. Identify each module using the serial number (visible on the product sticker), or click the **Find** button to command the module to rapidly flash its LEDs (DIN rail modules only).

   The onboard reader expander will be displayed with the same serial number as the controller and the address selected above.
5. Set the **Address** of each module as required.
6. Click **Update all**.
7. Click **Refresh**. All modules should now be registered and online.
8. Click **Close**.

Configuring Inputs

The default input configuration is:

- **Alarm input speed**: 500ms (10ms for REX inputs)
- **Restore input speed**: 500ms (10ms for REX inputs)
- **Input end of line (EOL)**: 1k alarm, 1k tamper
- **Contact type**: Normally closed

If your inputs have different wiring or timing requirements, navigate to **Programming | Inputs** and update these settings.

Reducing Unnecessary Events

By default the Protege GX system produces a large number of events that are typically not required (such as motion detection in disarmed areas). On busy sites this can quickly fill up the events database.

To reduce the number of unnecessary events, you can turn off events for inputs and outputs.

1. Navigate to **Programming | Inputs**.
2. Press Ctrl + A to select all inputs.
3. In the **Options** tab, disable **Log to event buffer**. This prevents logging of open, close, tamper and short events. The controller will still generate events for alarms, REX and other effects of the input changes.
4. Click **Save**.
5. If there are any inputs that require a high level of auditing, select them and re-enable **Log to event buffer**.
6. Navigate to **Programming | Outputs**.
7. Press Ctrl + A to select all outputs.
8. In the **Options** tab, disable **Log output events**. This prevents logging of on and off events.
9. Click **Save**.

Naming Conventions

It is recommended that you use a consistent naming convention for all hardware and other records throughout the site. It may be beneficial to name records such as inputs, outputs and doors at this stage to ensure that all are named consistently and avoid programming errors later on.

The name fields available in Protege GX are:

- **Name**: Used in the English version of Protege GX. A useful name contains the device's physical location, network address and function.
- **Name (second language)**: Used in the second language version of Protege GX.
- **Keypad display name**: The name displayed on the keypad and in reports to the central monitoring station. The keypad can only display the first 16 characters of the name. You can use the down arrow next to the **Name** field to automatically populate this field.

Schedules

To create schedules for controlling user access, doors or areas, you must first create a holiday group for the days when normal hours do not apply. Then you can create schedules with different periods for weekdays, weekends and holidays.

To create a holiday group:

1. Navigate to **Sites | Holiday groups**.
2. Click **Add**. Give the holiday group a descriptive name (e.g. National Holidays).
3. In the **Holidays** tab, click **Add**.
4. Enter the **Name**, **Start date** and **End date** for the holiday.
5. If the holiday recurs on the same day or days every year, click **Repeat**.
6. Repeat to program every required holiday. You can program multiple years in advance.
7. Click **Save**.

To program a schedule:

1. Navigate to **Sites | Schedules**.
2. Click **Add**. Give the schedule a descriptive name (e.g. Working Hours 9-5).
3. First, program the period for weekdays.
   - Set the **Start time**, **End time** and days for **Period 1** (e.g. 9:00am - 5:00pm, Monday to Friday).
   - Set the **Holiday mode** to Disabled on holiday.
4. Program the period for weekends:
   - Set the **Start time**, **End time** and days for **Period 2** (e.g. 9:00am - 5:00pm, Saturday and Sunday).
   - Set the **Holiday mode** to Disabled on holiday.
5. Program the period for holidays.
   - Set the **Start time** and **End time** for **Period 3**. Select all days of the week.
   - Set the **Holiday mode** to Enabled on holiday.

   If the schedule is always invalid on a holiday, this is not required.
6. In the **Holiday groups** tab, click **Add**.
7. Select one or more holiday groups and click **OK**.
8. Click **Save**.

See Application Note 262: Configuring Schedules in Protege GX for more information and tips for creating different types of schedules (e.g. overnight schedules). For an example of advanced schedule programming, see Qualified Schedules.

Access Control

This section covers configuration of reader expanders, card readers and doors for standard access control.

Reader Expanders

Navigate to **Expanders | Reader expanders** to see the reader expanders created by the controller wizard. The instructions for configuring card readers differ depending on whether they are ICT RS-485, OSDP or Wiegand readers.

ICT RS-485 Readers

For a typical configuration with entry or entry/exit readers:

1. Select a reader expander. Update the name to describe the doors controlled by this expander (e.g. CTRL1 RD2 - Front Door & Factory Door).
2. Set the **Offline operation**. We recommend First 10 users plus cache for most doors.
3. In the **Reader 1** tab, set the **Reader 1 format** and **Reader 1 secondary format** to the types of cards your site uses.

   If you are using custom credential types, select Custom credential (see page 41).
4. If users can control areas from these card readers, set the **Reader 1 arming mode**. Scroll down and enable **Disarm area for door on access**.
5. Repeat in the **Reader 2** tab.
6. Return to the **General** tab. Set the **Port 1 network type** and **Port 2 network type** to ICT RS485.
7. Click **Save**.
8. Right click on the reader expander and select **Update module**.
9. Badge a card at the card reader and ensure that the reader beeps multiple times (access granted or denied).

OSDP Readers

For more detailed information, see Application Note 254: Configuring OSDP Readers in Protege.

For a typical configuration with entry or entry/exit readers:

1. Select a reader expander. Update the name to describe the doors controlled by this expander (e.g. CTRL1 RD2 - Front Door & Factory Door).
2. Set the **Offline operation**. We recommend First 10 users plus cache for most doors.
3. Set the **Port 1 network type** and **Port 2 network type** to OSDP.
4. Click **Save**.
5. Navigate to **Expanders | Smart readers**. The software has automatically created two smart readers per reader port to represent entry and exit OSDP readers.
6. Select a smart reader record. The **Expander address** and **Expander port** shows where the OSDP reader is connected.
   - If the OSDP reader will be used, give it a descriptive name including the door it will control (e.g. CTRL1 RD2 Front Door Entry).
   - If the OSDP reader will not be used (e.g. the door does not have an exit reader), delete the smart reader record.

7. The **Configured address** must be the OSDP address of the card reader + 1. By default this is 1 for entry and 2 for exit. Update the address if required.
8. In the **Reader** tab, set the **Reader one format** and **Reader one secondary format** to the types of cards your site uses.

   If you are using custom credential types, select Custom credential (see page 41).

9. Set the **Reader one location** to Entry or Exit.
10. Select the **Reader one door**.
11. If users can control areas from this card reader, set the **Reader one arming mode**. Scroll down and enable **Disarm area for door on access**.
12. Click **Save**.
13. Repeat for any other smart reader records.
14. Return to **Expanders | Reader expanders**. Right click on the reader expander and select **Update module**.
15. Validate that the OSDP readers are functioning correctly before enabling secure channel. Badge a card at each reader and ensure that you get the expected access granted or denied events.

    If you do not have a status page yet (see page 30), you can view events by running an event search (**Events | Event search**).

16. If the card readers support installation mode, right click on the reader expander and select **Activate OSDP install mode**.

    If the card readers do not support installation mode, do not activate installation mode on the reader expander. See Application Note 254: Configuring OSDP Readers in Protege for alternative instructions.

Wiegand Readers

For a typical configuration with entry or entry/exit readers:

1. Select a reader expander. Update the name to describe the doors controlled by this expander (e.g. CTRL1 RD2 - Front Door & Factory Door).
2. Set the **Offline operation**. We recommend First 10 users plus cache for most doors.
3. Set the **Port 1 network type** and **Port 2 network type** to Wiegand.
4. If the reader port has both entry and exit readers connected (multiplexing), enable **Multiple reader input port 1/2**.
5. In the **Reader 1** tab, set the **Reader 1 format** and **Reader 1 secondary format** to the type of cards your site uses.

   If you are using custom credential types, select Custom credential (see page 41) .

6. If users can control areas from these card readers, set the **Reader 1 arming mode**. Scroll down and enable **Disarm area for door on access**.
7. Repeat in the **Reader 2** tab.
8. Click **Save**.
9. Right click on the reader expander and select **Update module**.
10. Badge a card at the card reader and ensure that the reader beeps multiple times (access granted or denied).

Doors

To set up doors with standard door types:

1. Navigate to **Programming | Doors**.
2. Select a door and give it a descriptive name (e.g. CTRL1 RD1 DR1 Front Door).
3. Set the **Door type** to determine which credentials the door will accept (Card, PIN only, Card and PIN, Card or PIN).
4. If you have already programmed the areas, set the **Area inside door** and **Area outside door**. If not, you can program these later.
5. The controller wizard programs the lock output, alarm outputs, door input and REX input by default. Review the **Outputs** and **Inputs** tabs to ensure that these are correct and add any other hardware required.
6. In the **Advanced options** tab, set the **Door extended access time**. This determines how long the door unlocks for access by people with mobility restrictions.
7. Click **Save**.

If your system uses custom credentials, see Custom Wiegand Credentials for specific instructions.

Latch Unlocking

By default, when a user accesses a door it unlocks temporarily, then relocks again. There are several options for latch unlocking doors, i.e. unlocking them until they are locked again.

To toggle the door lock when a user badges their card:

1. In the **Outputs** tab, set the **Lock activation time** to 0.
2. Click **Save**.

To unlock the door on a schedule:

1. In the **General** tab, set the **Unlock schedule**.
2. Click **Save**.

To unlock the door on schedule, but only after the first person has unlocked the door for the day (late to open or snow day function):

1. In the **General** tab, set the **Unlock schedule**.
2. In the **Options** tab, enable **Schedule operates late to open**.
3. Click **Save**.

To unlock the door when the inside area is disarmed:

1. In the **General** tab, set the **Area inside door**.
2. In the **Options** tab, enable **Door lock follows inside area**.
3. Enable **Area disarmed or schedule valid unlock door**.
4. Click **Save**.

To unlock the door when a schedule is valid **and** the inside area is disarmed:

1. In the **General** tab, set the **Area inside door**.
2. Set the **Unlock schedule**.
3. In the **Options** tab, enable **Door lock follows inside area**.
4. Enable **Area disarmed and schedule valid unlock door**.
5. Click **Save**.

You can also use a door control programmable function to latch unlock the door based on an output's status (see page 40).

You may wish to prevent door left open alarms and warnings while the door is latch unlocked so that users can prop the door open. See the **Alarm options** tab for various methods for disabling the alarms.

Intruder Detection

This section covers keypad configuration, adding areas and programming and walk testing inputs.

Keypads

1. Navigate to **Expanders | Keypads**.
2. Select the keypad and give it a descriptive name (e.g. CTRL1 KP1 Reception Keypad).
3. Set the keypad's default display.
   - Enter custom text in **Default display line one/two**. Each line has a maximum of 16 characters.

     Tip: To display the current time on the keypad use the code &t (12 hour format) or &m (24 hour format).
   - On the **Options 1** tab, select the messages and notifications you wish to display on the keypad screen.
4. By default the keypad can control all areas on the controller. To narrow this down, in the **Configuration** tab select an **Area group for this keypad**.
5. In the **Options 1** tab, enable **Lock keypad on excess attempts**.
6. Click **Save**.

For more information about configuring keypads, see Application Note 338: Programming Protege Keypads.

Areas

1. Navigate to **Programming | Areas**.
2. Add a new area with a descriptive name (e.g. Reception Area).
3. In the **Configuration** tab, program the following timings:
   - **Entry time**: Entry delay period for disarming the area (seconds).
   - **Exit time**: Warning period when the area is arming (seconds).
   - **Alarm 1 time**: Period that the siren will activate for during an alarm (minutes).
4. If a reporting service has already been programmed, add it under **Reporting services**. If not, you can add this later (see page 29).

   The **Reporting ID** will be generated automatically when you save the area.
5. In the **Outputs** tab, select the outputs or output groups used for signaling the area status.
   Most areas use the following outputs:
   - **Bell output**: Typically the controller's bell output.
   - **Exit delay output**: Typically the keypad or reader beeper.
   - **Entry delay output**: Typically the keypad or reader beeper.
   - **Disarmed output** or **Ready output**: Typically the keypad's green LED.
   - **Armed output**: Typically the keypad's red LED or a pulsed reader LED.

   You can also adjust the pulse on/off times (in milliseconds) to pulse the outputs.
6. In the **Options (2)** tab, select the types of arming that should be available for this area.
   - **Enable stay arming**: Arm the perimeter inputs only.
   - **Enable force arming**: Arm even when some inputs are open.
   - **Enable instant arming**: Arm no exit delay. All inputs are treated as instant inputs (no entry delay).
7. Click **Save**.

Arming and Disarming Areas

There are several options for arming and disarming areas besides using the keypad.

Automatic Arming/Disarming

To arm and/or disarm the area on a schedule:

1. In **Sites | Schedules**, create a schedule that becomes valid when you want the area to disarm, and becomes invalid when you want the area to arm (e.g. a 9-5 schedule).
2. Return to **Programming | Areas**. In the **Configuration** tab, set the **Arm/Disarm schedule**.
3. Enable **Disarm area when schedule starts** and/or **Arm area when schedule ends**.
4. In the **Options (2)** tab, ensure that **Enable force arming** is selected.
5. Click **Save**.
6. When you assign inputs to this area (see next page), ensure that they have a force input type. Alternatively, enable **Use unattended brute force arming** in the area's **Options (1)** tab.

To automatically rearm the area after a set time:

1. In the **Configuration** tab, set the **Rearm area time** to determine how long the area will remain disarmed before rearming.
2. In the **Options (1)** tab, select **Re-arm enabled**.
3. In the **Options (2)** tab, ensure that **Enable force arming** is selected.
4. If the area will be disarmed by schedule during the day but should rearm automatically out-of-hours, add the following additional settings:
   - In the **Options (2)** tab, enable **Disable rearm on schedule**.
   - In the **Configuration** tab, scroll down and expand the **Commands** section. Enter the following command:
     `ReArmLevelTrigger = true`
5. Click **Save**.
6. When you assign inputs to this area (see next page), ensure that they have a force input type. Alternatively, enable **Use unattended brute force arming** in the area's **Options (1)** tab.
7. Arm and then disarm the area to start the timer.

Arm/Disarm on Door Access

It is convenient for users to automatically disarm an area when they gain access to the door that leads into it. You can also enable them to arm the area by badging twice or three times at the entry reader.

1. Navigate to **Expanders | Reader expanders** and select the relevant reader expander.
2. In the **Reader 1** or **Reader 2** tab, set the **Reader 1/2 arming mode** to determine how users can arm the area.
3. Scroll down and enable **Disarm area for door on access** to allow users to disarm the area.
4. Click **Save**.
5. Navigate to **Programming | Doors** and select the relevant door.
6. Ideally the **Door type** should be Card or PIN only.
7. Set the **Area inside door** and **Area outside door**.
8. Click **Save**.
9. When you create an access level, ensure that **Enable multi-badge arming** is enabled or disabled appropriately (enabled by default).

For arming and disarming via a key switch, see Area Follows Input (Key Switch).

Inputs

To add inputs into areas:

1. Navigate to **Programming | Inputs** and select each input. You can use Ctrl + Click to select multiple inputs and give them the same settings.
2. In the **Areas and input types** tab, assign the first area and input type. You can use the default input types or click the ellipsis **[...]** button to create a new one.
   - Instant: Triggers the alarm instantly.
   - Instant Force: As above, but can be force armed.
   - Delay: Triggers the entry delay.
   - Delay Force: As above, but can be force armed.
   - Delay Follow: Triggers the alarm instantly, unless the entry delay has already started.
   - Delay Follow Force: As above, but can be force armed.
3. If the input sits in multiple areas (e.g. a door contact), assign a second area and input type.
4. Click **Save**.
5. Once you have finished programming, disarm and rearm all affected areas to implement the changes.

Walk Test

The walk test function allows you to test the functionality of all of the inputs in the area. Inputs activated during the walk test do not generate alarms and are not reported to the central monitoring station.

To walk test the area:

1. Right click on the area (in **Programming | Areas** or on a floor plan or status page) and click **Walk test enable**.
2. Walk through the area and test inputs such as door sensors and PIRs. The system will log an event for each input activated:
   `Input Activated during Walk Test of Area`
3. Right click on the area and click **Walk test disable**. The system will log an event for each input that was not activated during the walk test:
   `Input did Not Activate during Walk Test of Area`
4. Review the events using an event search or report.

Trouble Monitoring

This section covers how to monitor system troubles using trouble inputs.

System Area

Trouble inputs are typically monitored by a system area that is always armed. Best practice is to create one system area per controller.

1. Navigate to **Programming | Areas**.
2. Add a new area with a descriptive name (e.g. CTRL1 System Area).
3. In the **Configuration** tab, update the timing settings:
   - **Exit time**: 0
   - **Rearm area time**: 1
4. If a reporting service has already been programmed, add it under **Reporting services**. If not, you can add this later (see page 29).

   The **Reporting ID** will be generated automatically when you save the area.
5. In the **Outputs** tab, set the **Bell output** to the controller's bell or another alarm output.
6. In the **Options (1)** tab, select **Re-arm enabled**.
7. Click **Save**.

Trouble Inputs

Now you can assign trouble inputs to the system area.

1. Navigate to **Programming | Trouble inputs**.
2. In the toolbar, set the **Controller** to the controller you are programming.
3. Use Ctrl+A to select all trouble inputs.
4. In the **Areas and input types** tab, set **Area 1** to the new system area.
5. Set **Input type 1** to Trouble silent.
6. Click **Save**.
7. Navigate to **Programming | Areas**.
8. Right click on the system area and click **Arm**.

User Management

This section covers how to create access levels and user records to grant people access.

Groups

First, you must create area groups to grant access to areas.

1. Navigate to **Groups | Area groups**.
2. Add a new area group with a descriptive name (e.g. Office Staff).
3. Click **Add** and select the areas that will be included in the group.
4. Click **Save**.

Optionally, you can also create door groups in **Groups | Door groups**.

If the site uses keypads, you must create a menu group to grant access to keypad menus:

1. Navigate to **Groups | Menu groups**.
2. Add a new menu group with a descriptive name (e.g. Office Staff).
3. Select the menus that the user will have access to.
   - For most users this is **Area (1)** (arming and disarming areas) and **User (2)** (changing their own PIN code).
   - Security guards and technicians may also have the **View (5)** menu (view/control device status and alarm memory).
4. Set whether the user is permitted to stay, force or instant arm areas.
5. In the **Options** tab, select **User can acknowledge alarm memory** if required.
6. Click **Save**.

Access Levels

1. Navigate to **Users | Access levels**.
2. Add a new access level with a descriptive name (e.g. Office Staff).
3. Set the **Operating schedule** to determine when access is permitted.
4. If your site allows areas to be disarmed from card readers, ensure **Enable multi-badge arming** is enabled or disabled appropriately for this group of users.
5. In the **Doors** or **Door groups** tab, add the doors that the user will have access to.
6. In the **Menu groups** tab, add the user's menu group for keypads.
7. In the **Arming area groups** and **Disarming area groups** tabs, add the area groups that the user will have access to.

   If an area is in the **Disarming area groups** tab, the user is also allowed to arm that area.
8. Click **Save**.

Users

1. Navigate to **Users | Users**.
2. Add a user. Enter their **First name** and **Last name**.
3. Enter a **PIN** (4-6 digits is recommended), or click a numbered button to automatically generate one.

4. If your site uses standard access cards, enter the user's **Facility number** and **Card number**.
5. If your site uses custom credentials, scroll down to the **Credentials** section. Enter the user's **Credential**. For access cards, this is typically a facility number and card number separated by a colon (e.g. 100:4035).
6. Optionally, set the **User expiry date/time**.
7. In the **Access levels** tab, click **Add**.
8. Select one or more access levels and click **OK**.
9. In the **Options** tab, there are some common settings you may need to enable:
   - **Treat user PIN plus 1 as duress**: The user can activate the silent duress alarm by adding 1 to the last digit of their PIN code.
   - **User has super rights and can override antipassback**: The user can ignore lockdown and antipassback restrictions.
   - **User operates extended door access function**: The user unlocks doors for a longer time (for people with mobility issues).
10. Click **Save**.
11. Test the user by badging their card at a reader.

Importing Users from a CSV

This is a one-off import, e.g. from a previous access control system. For continuous imports, use the ICT Data Sync Service.

1. Use a spreadsheet program such as Microsoft Excel or Google Sheets to create a spreadsheet of users. Alternatively, export one from another database. This should look similar to the following:

First Name	Last Name	PIN	Facility Number	Card Number	Access Level	Expiry (Start)	Expiry (End)
Alice	Taylor	1234	1	540	Office	02/12/2026 08:00:00	
Matthew	Harrison	2345	1	541	Warehouse Day Shift	02/12/2026 08:00:00	31/05/2027 18:00:00
...	...	...	...	...	...	...	...

   - Not all columns are required.
   - Access levels that already exist in Protege GX will be assigned to the users. Access levels that do not exist yet will be created automatically.
   - Start and end expiry dates must be in the format dd/MM/yyyy HH:mm:ss or MM/dd/yyyy HH:mm:ss.
   - Your file can have up to 5 header rows.
2. Save the spreadsheet in CSV (comma separated values) format.
   - In Microsoft Excel, select **Save As** and set the format to **CSV UTF-8 (Comma delimited)**.
   - In Google Sheets, select **File > Download > Comma Separated Values**.
3. To confirm this is in the correct format, open it with a text editor such as Notepad. It should look similar to the following:

```
First Name,Last Name,PIN,Facility Number,Card Number,Access Level,Expiry
(Start),Expiry (End)
Alice,Taylor,1234,1,540,Office,2/12/2026 8:00,
Matthew,Harrison,2345,1,541,Warehouse Day Shift,2/12/2026 8:00,31/05/2027
18:00
```

4. In Protege GX, navigate to **Sites | Import users**.
5. Click **Browse** and select the CSV file.

6. Click **Next**.
7. Set the number of header rows in the file (e.g. if your spreadsheet has one header row, select 1).
8. Select the **Text delimiter** (typically double quotes).
9. Click **Next**.
10. Review the preview table to ensure that the rows and columns have been configured correctly.
11. Select each column header, then select the data type that it corresponds to. In the table above, column 1 corresponds to **First name**, column 2 to **Last name**, and so on. If there is irrelevant data, select **Skip** for that column.
12. If you are importing the first and last names separately, set the **User display name auto format** to determine the format of the display name.
13. Click **Next**.

    If there are some users with expiry dates and some without, the wizard will warn you that the column has invalid data. Click **Yes** to allow the wizard to import some users without an expiry date.

14. If your data did not include cards, PINs or access levels you can assign them on this screen.
15. Click **Next**.
16. Click **Finish**.
17. Navigate to **Users | Users** to view the new user records created by the import tool. You can now program any additional settings required.
18. Navigate to **Users | Access levels** to program any new access levels created by the import tool.

Offsite Reporting

This section covers setting up IP or Contact ID reporting to a central monitoring station.

For more information about reporting and the available report mappings, see:

- Application Note 316: Contact ID Reporting in Protege GX and Protege WX
- Application Note 317: SIA L2 Reporting in Protege GX and Protege WX

Report IP

Before you begin, you will need the following information from your monitoring station:

- Client code
- Reporting protocol
- Username and password (if using CSV reporting)
- Encryption level and encryption key
- Poll time
- Primary and secondary IP addresses / host names and port numbers
- Expected message acknowledgment (ack) time
- Offline polling codes and frequency

To program a primary Report IP service:

1. Navigate to **Programming | Services**.
2. In the toolbar, select the **Controller**.
3. Add a new service with a descriptive name (e.g. ArmorIP over Ethernet).
4. Set the **Service type** to Report IP.
5. Set the **Service mode** to 1 - Start with controller OS.
6. In the **General** tab, enter the following details:
   - Client code
   - Reporting protocol
   - Encryption level
   - Encryption key
   - Poll time (in seconds)
7. If you are using a SIMS II input mapping, set **CID map settings** to SIMS II. If not, do not change this setting.
8. Enter the settings for the primary communication channel:
   - **IP address / Host name** for the receiver
   - **IP port number** for the receiver
   - **Adaptor** for the controller. Select Cable for ethernet, USB ethernet for a cellular modem.
9. Enter the settings for the secondary communication channel. This will be used if the first channel fails.
10. In the **Options** tab, select the types of events that the service will report:
    - Report open (area disarming)
    - Report close (area arming)
    - Report alarms
    - Report tampers
    - Report restore
    - Report bypass

11. Click **Save**.
12. Right click on the service and click **Start service**.

You should program a backup service that will be started when the primary service fails to communicate. This is programmed the same way as the regular service, but typically uses a different communication method (e.g. cellular modem instead of wired ethernet).

1. Program another service following the instructions above.
2. In the **General** tab, under **Primary channel settings**, select **Enable offline polling**.
3. Enter the Contact ID codes for reporting a polling failure and the polling details.
4. Repeat under **Secondary channel settings**.
5. In the **Options** tab, enable **Service operates as backup**.
6. Click **Save**.
7. Select the primary service. In the **General** tab, set the **Backup service** to the new service.
8. Click **Save**.

Contact ID

Before you begin, you will need the following information from your monitoring station:

- Client code
- All phone numbers associated with the monitoring station (primary numbers, backups, night numbers)
- Number of messages per call
- Expected handshake time and dial time
- Background polling codes and frequency

First you must program all phone numbers for the monitoring station and the internal PABX number (if needed):

1. Navigate to **Programming | Phone numbers**.
2. Add a new phone number with a descriptive name (e.g. ABC Monitoring Day Number).
3. Enter the **Phone number**.
4. If the number is only used at specific times of day, select an **Operating schedule**. Set the **Secondary phone number** that will be used when the schedule is invalid.
5. Click **Save**.

To program the Contact ID service:

1. Navigate to **Programming | Services**.
2. Add a new service with a descriptive name (e.g. Contact ID over Landline).
3. Set the **Service type** to ContactID.
4. Set the **Service mode** to 1 - Start with controller OS.
5. In the **General** tab, enter the **Client code** provided by the monitoring station.
6. Select the phone numbers created above. The service will attempt to use **Phone number 1**, then **Phone backup**, then **Phone number 2**.
7. In the **Options** tab, select the types of events that the service will report:
   - Report open (area disarming)
   - Report close (area arming)
   - Report alarms
   - Report tampers

- Report restore
- Report bypass

8. If the service is a backup, enable **Service operates as backup**.
9. In the **Settings** tab, if you are using a SIMS II input mapping, set **CID mapping** to SIMS II. If not, do not change this setting.
10. Adjust the reporting settings if required.
11. If this is a backup service, select **Enable background monitoring** and enter the polling details and report codes.
12. Click **Save**.
13. If this is a primary service, right click on the service and click **Start service**.
14. If this is a backup service, select the primary service.
    In the **General** tab, set the **Backup service**. Click **Save**.

Assigning Services to Areas

The service must be assigned to the areas it will monitor, including the system area.

1. Navigate to **Programming | Areas** and select each area.
2. In the **Configuration** tab, scroll down to **Reporting services**.
3. Add the primary reporting service.
4. In some cases, such as buildings with multiple tenancies, each area has its own client code. If required, set the **Client code** as provided by the monitoring station.
5. Click **Save**.

Central Station Report

The central station report contains the names, reporting codes and IDs for all inputs, trouble inputs, areas and users monitored by a service. You can export it in CSV and HTML formats to send to your central monitoring station.

1. Navigate to **Reports | Central station report**.
2. Select the **Reporting service**.
3. Set the **Output directory** where the file will be saved.
4. If you are using a specific reporting map, enable **Reset area, input and trouble input ID's** to apply it to all records associated with this service. Select the appropriate **Report map type** to reset all Reporting IDs to use that mapping.

   Select None to reset the Reporting IDs to a sequential mapping, which may be more efficient in scenarios with large numbers of inputs.
5. Click **Generate**.
6. Click **Open** to view the report.

You can now send the report to your central monitoring station.

Monitoring and Reports

This section covers status pages for site monitoring as well as reports on events, users and site programming.

Some common features are not covered in this document:

- Floor plans for site monitoring and control - see Application Note 340: Programming Floor Plans in Protege GX
- Software and email notifications on event - see Application Note 332: Setting Up Event Notifications in Protege GX
- Push notifications to the Protege Mobile App - see Application Note 201: Protege GX Push Notification Setup

Status Page

We will create a couple of simple status pages as examples. You can create as many additional status pages as required, such as a system monitoring page to display system area and trouble input status.

These examples use the default All Events report, but you can create custom event reports to filter the events that will be displayed on the status page (see next page).

All Events Status Page

1. Navigate to **Monitoring | Setup | Status page editor**.
2. Click **Add**.
3. Give the status page a descriptive name (e.g. All Events).
4. Select the first default layout (a single big square).
5. Click **OK**.
6. Set the **Type** to Event windows.
7. Set the **Record** to All Events.
8. Click **Save**.
9. Navigate to **Monitoring | Status page view** to view the new status page.

Door and Area Monitoring Status Page

To create status lists:

1. Navigate to **Monitoring | Setup | Status lists**.
2. Add a new status list with a descriptive name (e.g. CTRL1 Doors).
3. Click **Add**.
4. Select the doors to add to the status list, then click **OK**.
5. Click **Save**.
6. Add another status list (e.g. CTRL1 Areas).
7. Click **Add**.
8. Set the **Device type** to Area.
9. Select the areas to add to the status list, then click **OK**.
10. Click **Save**.

To create the status page:

1. Navigate to **Monitoring | Setup | Status page editor**.
2. Click **Add**.
3. Enter a descriptive name (e.g. Office Status).
4. Select the layout with four equal squares.
5. Click **OK**.
6. In the top left square, select the following:
   - **Type**: Event windows
   - **Record**: All Events, or another event report of your choice.
   - **Columns**: 2
   - **Rows**: 1
7. In the bottom left square, select the following:
   - **Type**: Status list
   - **Record**: The door status list created above
   - **Columns**: 1
   - **Rows**: 1
8. In the bottom right square, select the following:
   - **Type**: Status list
   - **Record**: The area status list created above
   - **Columns**: 1
   - **Rows**: 1
9. Click **Save**.
10. Navigate to **Monitoring | Status page view** to view the new status page.

Event Reports

Event reports are repeatable reports that can be run regularly. To run a one-off report, use the event search in **Events | Event search**.

First create an event filter that includes the events that will be in the report.

1. Navigate to **Events | Event filters**.
2. Add a new event filter with a descriptive name (e.g. Door Alarm Events).
3. In the **Event types** tab, disable **Include all event types**.
4. Click **Add**.
5. Locate the events you want to display in the report and drag and drop them into the event type box. You can find events using the categories or use the **Keyword** box to search for event keywords (e.g. 'forced', 'left open').

   You can drag and drop an entire event category to include all events of that type.

6. By default the filter includes events from all records. If you wish to restrict the report to specific records (e.g. alarms from specific doors, access from specific users), select them in the **Records** tab:
   - Under **Record filter**, click **Add**.
   - Select the **Device type** to filter by.
   - Select the records that you want to see events for, and click **OK**.
   - If required, add records to **Record filter 2**. Only events that include a record from both lists will be

included in the report (e.g. a specific user disarmed a specific area).

7. Click **Save**.

Next, create the event report:

1. Navigate to **Reports | Setup | Event**.
2. Add a new event report with a descriptive name (e.g. Door Alarm Events).
3. Enter the **Title** for the report. This will be used in printed and exported reports.
4. Under **Event filters**, select the default All Events filter and click **Delete**.
5. Click **Add**.
6. Select the **Event filter** created above.
7. Enable **Access all record groups**, or select the specific record groups you wish to include in this report.
8. Click **OK**.
9. The **Columns** tab shows the columns that will be included in this report by default. You may wish to remove some of these (e.g. remove the **Alarm priority** column if you are not using this feature) and add others that are relevant to your report.
10. Click **Save**.

To run the report:

1. Navigate to **Reports | Event**.
2. In the toolbar, select the **Event report**.
3. Click **Execute**.
4. Set the **Time period** that the report will cover.
5. Click **OK** to run the report.
6. Adjust the columns, sorting and grouping of the event data, then if required use the **Print** button to print or export the report.

   Only the data that is currently displayed will be printed/exported.

You can also automatically export and email event reports at fixed times. For instructions, see Application Note 243: Exporting and Emailing Reports in Protege GX.

User Reports

User reports are repeatable reports that can be run regularly. To run a one-off report, use the user search in **Users | User search**.

To create a user report:

1. Navigate to **Reports | Setup | User**.
2. Add a new user report with a descriptive name (e.g. Night Shift Report).
3. Select the **Report type** for this report:
   - **All users**: All users currently programmed in this site.
   - **All users who have access to the selected doors**: All users with access levels that grant access to the selected doors.
   - **All users included in the following access levels**: All users with the selected access levels assigned.
   - **All users by events**: All user records included in any events from the selected event filter, within the specified time period.
   - **All users by record group**: All users in the selected record group.

- **Users by event type/doors**: All users who have triggered events at the selected doors within the specified time period.
- **Cards about to expire**: Any user records which are set to expire within the selected period.
- **Last users through door(s)**: The last users (and the time of access) who accessed the selected door(s).
- **All users not in events**: Any users not included in any events from the selected event filter, within the specified time period.
- **All current visitors**: All visitors currently signed in (requires visitor management system).
- **All overdue visitors**: All visitors still signed in after their expected signout time (requires visitor management system).
- **All visitors by date**: All visitors who signed in within a specific period (requires visitor management system).
- **Record modified history report**: All user records which have been modified in the selected time frame, grouped by user. It includes the settings that were modified, the old and new values and the operator.
- **All users by access levels**: Users with the specified access levels, grouped by access level. Access level expiry times are displayed. Users who have been disabled or have expired access levels are not included.
- **All access levels by users**: Users with the specified access levels, grouped by user. Access level expiry times are displayed. Users who have been disabled or have expired access levels are not included.

4. Enter a **Title** that will be displayed on printed and exported reports.
5. Depending on the type of report, you may need to select additional parameters, such as access levels or doors.
6. In the **Columns** tab, set the columns that will be displayed in this report. Click **Add** and select the required columns. Common requirements are:
   - First name and Last name or Display name
   - Facility/Card number or credential types
   - Access level
   - Expiry date
   - Disable user
7. Click **Save**.

To run the report:

1. Navigate to **Reports | User**.
2. In the toolbar, select the **User report**.
3. Click **Execute**.
4. Adjust the columns, sorting and grouping of the user information, then if required use the **Print** button to print or export the report.

   Only the data that is currently displayed will be printed/exported.

You can also automatically export and email event reports at fixed times. For instructions, see Application Note 243: Exporting and Emailing Reports in Protege GX.

Exporting Programming for Site Documentation

Protege GX allows you to export data about many types of programmed records such as doors, areas, inputs, outputs, users and access levels. This is convenient for creating 'as-built' site documentation to provide to the customer.

For example, to export the programmed inputs:

1. Navigate to **Programming | Inputs**.
2. If you only need to export some inputs, select the **Controller** in the toolbar and use Shift+Click or Control+Click to select the required inputs.

3. Click **Export** in the toolbar.
4. Set the **Export type** to Selected records or All records.
5. Set the **Destination** to File to export a CSV file.
6. Select the **Columns** (settings) you wish to include in the report. For inputs, this would commonly be:
   - Name and Keypad display name
   - Module type, Module address and Module input
   - Areas and input types
   - Input end of line and Contact type
   - Reporting ID
7. Click **OK**.
8. Select where to save the CSV file and click **Save**.

Software Management

This section covers operator management. See the Protege GX Installation Manual for cybersecurity and database configuration.

Operators

First, create a role to control the operator's access:

1. Navigate to **Global | Roles**.
2. Add a new role with a descriptive name (e.g. Human Resources).
3. Select a **Preset**. The available presets are:
   - **Administrator** or **Installer**: Can perform all actions in the system without any restrictions.
   - **End user**: Can perform most actions related to user access and scheduling. Can view status pages and floor plans and run event reports.
   - **Guard**: Can view status pages and floor plans and run event reports.
4. In the **Tables** tab, adjust any permissions that need to be changed from the defaults.
5. Click **Save**.

See Application Note 191: Programming Operator Roles in Protege GX for more detailed instructions and examples.

Then create an operator and assign the role to them:

1. Navigate to **Global | Operators**.
2. Add a new operator with a descriptive name (e.g. Janet Li - Human Resources).
3. Enter the operator's **Username** and **Password**.

   Ensure that you use a secure password that is difficult to guess.
4. Select the **Role**.
5. Set the operator's **Time zone**.
6. Click **Save**.

Advanced Features

This section covers a number of advanced Protege GX features which may be useful on your site. It is not intended to be comprehensive but should provide you with a toolbox for achieving more complex functionality.

We also include some example instructions for common scenarios, such as changing a door type based on area status and key switch arming.

Virtual Outputs

Virtual outputs are any programmed outputs that do not correspond to a physical output on the hardware. They can turn on and off in response to triggers such as inputs, areas and schedules and use that status drive other functions, unlocking huge potential for automation and other advanced solutions.

You can add a virtual output to any existing module at any address that does not have a physical output associated with it. For example, a two-door controller only has 8 outputs, so addresses 9-255 are available for controlling virtual outputs.

To create a single virtual output:

1. Navigate to **Programming | Outputs**.
2. In the toolbar, select the **Controller** you are programming.
3. Click **Add**.
4. Select **No** so that the output is not inverted.
5. Give the output a descriptive name, including the output's address, purpose and the term Virtual or VO (e.g. CP1.9 Reception Area Armed VO).
6. Set the **Module type** and **Module address** to any existing module.
7. Set the **Module output** to an address above the normal range for that module (typically from 9 onwards).
8. Click **Save**.

Alternatively, you can use a virtual output expander to add multiple virtual outputs in a batch:

1. Navigate to **Expanders | Output expanders**.
2. In the toolbar, select the **Controller** that will control these outputs.
3. Add a new output expander with a descriptive name (e.g. CTRL1 PX32 (Virtual)).
4. Enable **Virtual module**.
5. Set the **Physical address** to a value above existing physical expanders (e.g. 32).
6. Click **Save**.
7. Disable **Add trouble inputs** and click **Add now**.
8. Navigate to **Programming | Outputs** to view the outputs created for this output expander. It is recommended that you rename them so that they include the term Virtual or VO in their names.

Qualified Schedules

When a schedule is qualified by an output, it will only be valid when the periods are valid and the output is in the correct state.

For example, to create a schedule that is only valid when an output is on:

1. Navigate to **Sites | Schedules**.
2. Click **Add**. Give the schedule a descriptive name (e.g. Automation Schedule - Valid when lights are on).

3. In **Period 1**, select all days of the week. The **Graphics view** should show that the schedule is valid at all times.
4. In the **Options** tab, select **Validate schedule if qualify output on**.
5. Select the **Qualify output** that will control this schedule.
6. Click **Save**.

Automation Area

Inputs can be used to control outputs, output groups and areas, enabling you to create automated responses to sensor input. This functionality requires a custom input type and an automation area to connect the inputs with the input type. It is recommended to create one automation area per controller.

1. Navigate to **Programming | Areas**.
2. Add a new area with the name CTRL1 Automation Area.
3. Set the **Exit time** to 0.
4. Click **Save**.
5. Right click on the area and select **Arm 24 hrs**.

Output Follows Input

There are two methods for controlling outputs using inputs:

- The input type method enables many inputs to control the same output (many to one) or output group (many to many).
- The input method enables each input to control a different output (one to one) or output group (one to many).

For both methods, we will need to create an input type and program the relevant inputs.

Input Type Method: Many to One/Many

In this setup, each input controls the same output or output group.

1. Create an automation area if there isn't one already (see above).
2. To control multiple outputs at once, create an output group in **Groups | Output groups**.
3. Navigate to **Programming | Input types**.
4. Add a new input type with a descriptive name (e.g. Lighting Control).
5. Select an **Operating schedule** if the automation will only operate at specific times.
6. Set the **Control output time** to determine how long the output will remain on when activated.
7. Select a **Control output** or **Control output group** that these inputs will control.
8. Do not enable any settings in the **Options (1)** tab.
9. In the **Options (2)** tab, set how the output will be controlled:
   - **Activate control output on alarm**: When the input opens, the output turns on.
   - **Activate control output on restore**: When the input closes, the output turns on.
   - **Deactivate control output on alarm**: When the input opens, the output turns off.
   - **Deactivate control output on restore**: When the input closes, the output turns off.
   - **Toggle control output state on alarm**: When the input opens, the output changes state between off and on.
   - **Input retriggers output time**: If the input opens/closes again while the output is still on, it will reset the timer.
10. Click **Save**.

11. Navigate to **Programming | Inputs**.
12. Use **Ctrl+Click** to select the inputs that will control the output.
13. In the **Areas and input types** tab, set **Area 4** to the automation area and **Input type 4** to the new input type.
14. Click **Save**.

Input Method: One to One/Many

In this setup, each input activates a different output or output group.

1. Create an automation area if there isn't one already (see previous page).
2. To control multiple outputs at once, create an output group in **Groups | Output groups**.
3. Navigate to **Programming | Input types**.
4. Add a new input type with a descriptive name.
5. Select an **Operating schedule** if the automation will only operate at specific times.
6. Do not enable any settings in the **Options (1)** or **Options (2)** tabs.
7. In the **Options (3)** tab, set how the output will be controlled:
   - **Use input type output time**: When enabled, all output activations will use the **Control output time** in the input type (**General** tab). When disabled, outputs will activate for the **Activation time** in the output.
   - **Activate input control output on alarm**: When the input opens, the output turns on.
   - **Activate input control output on restore**: When the input closes, the output turns on.
   - **Deactivate input control output on alarm**: When the input opens, the output turns off.
   - **Deactivate input control output on restore**: When the input closes, the output turns off.
   - **Toggle input output state**: When the input opens, the output changes state between off and on.
8. Click **Save**.
9. Navigate to **Programming | Inputs**.
10. Select an input and set the **Control output** or **Control output group**.
11. In the **Areas and input types** tab, set **Area 4** to the automation area and **Input type 4** to the new input type.
12. Click **Save**.
13. Navigate to **Programming | Areas** and arm the automation area.

Example: Motion-Activated Lights

As an example, we will program lighting circuits to turn on when motion is detected by a PIR. The lights will switch on for half an hour whenever motion is detected, and if motion is detected again the timer will reset so that they remain on longer.

1. Create an output group containing the lighting circuits.
2. Add an input type with the following settings:
   - **Control output time**: 1800 seconds (half an hour)
   - **Control output group**: Lighting output group
   - **Activate control output on alarm**
   - **Input retriggers output time**
3. Program the PIR inputs with the control area and input type.

Area Follows Input (Key Switch)

Inputs may also be used to arm and disarm areas. In this example we will program a key switch for arming and disarming a specific area.

1. Create an automation area if there isn't one already (see page 37).
2. Navigate to **Programming | Input types**.
3. Add a new input type with a descriptive name (e.g. Warehouse Key Switch).
4. Select the **Control area** that this input type will control.
5. Do not enable any settings in the **Options (1)** tab.
6. In the **Options (2)** tab, set how the area will be controlled:
   - **Disarm control area on input restore**: When the input closes, the area is disarmed.
   - **Arm control area on input alarm**: When the input opens, the area is armed.
   - **Toggle control area on input alarm**: When the input opens, the area changes state.
7. Click **Save**.
8. Navigate to **Programming | Inputs** and select the key switch input.
9. In the **Areas and input types** tab, set **Area 4** to the automation area and **Input type 4** to the new input type.
10. Click **Save**.

Changing Door Type based on Area Status

In this example, we will program an exterior door that accepts card and PIN when the inside area is armed and card only when the inside area is disarmed. The basic logic is:

- The area activates an armed output when it is armed
- When the armed output is on, a qualified schedule is valid
- When the schedule is valid, the door uses the primary door type
- When the schedule is invalid, the door uses the secondary door type

To program the automation:

1. Create virtual outputs if you do not have them already (see page 36). Select one of the virtual outputs and give it a descriptive name (e.g. Reception Area Armed VO).
2. Navigate to **Programming | Areas** and select the area inside the door.
3. In the **Outputs** tab, set the Armed output to your virtual output.
4. Click **Save**.
5. Navigate to **Sites | Schedules**.
6. Add a new schedule with a descriptive name (e.g. Reception Area Armed).
7. In **Period 1**, select all days of the week. Ensure the **Graphics view** shows that the schedule is valid at all times.
8. In the **Options** tab, select **Validate schedule if qualify output on**.
9. Set the **Qualify output** to the armed output.
10. Click **Save**.
11. Navigate to **Programming | Door types**.
12. Add a new door type with a descriptive name (e.g. Card and PIN when Reception Armed, Card when Disarmed).
13. Set the **Operating schedule** to the new schedule.
14. Set the **Secondary door type** to Card.
15. Set the **Entry reading mode** to Card and PIN.
16. Click **Save**.
17. Navigate to **Programming | Doors** and select the relevant door.

18. Set the **Door type** to the new primary door type.
19. Click **Save**.

Door Control Programmable Functions (Lockdown/Emergency Egress)

Door control programmable functions can be used to lock or unlock doors, start or clear lockdown and start or clear emergency egress (fire unlock) based on the state of an output.

This example covers how to create panic buttons that enable and disable lockdown on a group of doors. The process for activating emergency egress is almost exactly the same. For more detailed instructions, see Application Note 208: Emergency Egress and Lockdown Programming.

1. In **Groups | Door groups**, create the group of doors that will be locked down.
2. Create a virtual output to control this function (see page 36). Give it a descriptive name (e.g. Lockdown Control VO).
3. Program the input type for activating this output and assign it to the panic button inputs (see page 37). You will need these settings in the **Options (2)** tab:
   - **Activate control output on alarm**
   - **Deactivate control output on restore**
4. Navigate to **Automation | Programmable functions**.
5. In the toolbar, select the **Controller** you are programming.

   It is possible to lock down doors from multiple controllers using a single programmable function, but one controller must be the 'owner' of the function.
6. It is best practice to create two programmable functions: one to activate the lockdown and a second one to clear it. This allows you to clear lockdown on specific doors as needed with manual commands.
   Add a new programmable function with a descriptive name (e.g. Activate Lockdown).
7. Set the **Type** to Door Control.
8. In the **Door control** tab, set the following:
   - **Door function mode**: Follow pulse on output
   - **Door control mode**: Select one of the lockdown modes
   - **Output to check**: The virtual output created above
   - **Door group to control**: The door group created above
9. Click **Save**.
10. Add another programmable function with a descriptive name (e.g. Deactivate Lockdown).
11. Set the **Type** to Door control.
12. In the **Door control** tab, set the following:
    - **Door function mode**: Inverted follow pulse off output
    - **Door control mode**: Select the same lockdown mode as above
    - **Output to check**: The virtual output created above
    - **Door group to control**: The door group created above
13. Click **Save**.
14. Right click on each programmable function and click **Start**.

To create an emergency egress function instead, create the same two programmable functions but set the **Door control mode** to Fire control door unlock.

Many regions require mechanical fire unlock systems instead of controller-level functions. Ensure that you meet local regulations and safety requirements.

Custom Wiegand Credentials

Credential types allow you to use custom Wiegand credentials that are not included in the standard Protege GX options.

For more information about custom credential types, including alternative credentials such as license plates, see Application Note 276: Configuring Credential Types in Protege GX.

To program the credential type:

1. Navigate to **Sites | Credential types**.
2. Add a new credential type with a descriptive name (e.g. Wiegand 42 bit).
3. Set the **Format** to Wiegand.
4. Enter the **Wiegand or TLV format**. If you do not know what this should be, see Application Note 276: Configuring Credential Types in Protege GX or contact ICT Technical Support.
5. Click **Save**.

You must program the reader expanders and/or smart readers to accept custom credentials:

- **Wiegand and ICT RS-485 Readers**: In **Expanders | Reader expanders | Reader 1/2**, ensure that the **Reader 1/2 format** is set to Custom credential for each door.
- **OSDP Readers**: In **Expanders | Smart readers | Reader one**, ensure that the **Reader one format** is set to Custom credential (for both the entry and exit readers).

Create a door type that uses this custom credential type:

1. Navigate to **Programming | Door types** and add a new door type with a descriptive name (e.g. Wiegand 42 bit card).
2. Set the **Entry reading mode** to Custom.
3. Under **Entry credential types**, click **Add**.
4. Select the new credential type and any other credentials needed at this door, then click **OK**.
5. Repeat for the **Exit credential type**.
6. Click **Save**.

For each door:

1. Navigate to **Programming | Doors** and select the door.
2. Set the **Door type** to your new door type.
3. Click **Save**.

Monitoring a Power Supply

Protege power supplies can monitor their output voltage, core voltage and current and display these values in Protege GX.

The analog channels on the power supply represent the following information:

Channel Number	Function
1	V2 Voltage
2	V1 Voltage
3	Core Voltage
4	Current

To monitor the power supply:

1. Navigate to **Expanders | Analog expanders** and select the power supply.
2. In the **Channel 1** tab, configure the following settings for the core voltage channel:
   - **Enable channel**: Enabled
   - To update the value at regular intervals disable **Send ADC value in diff mode** and set the **Channel 1 update time**, OR
   - To update the value whenever it changes by a defined amount enable **Send ADC value in diff mode** and set the **Channel 1 diff comparison value**.
3. Click the ellipsis **[...]** beside **Channel 1 data value** to open a breakout window with data value programming.
4. Create a new data value with a descriptive name (e.g. CTRL1 PSU1 V2 Voltage). Click **Save**.
5. Close the breakout window and set the **Channel 1 data value** to the new data value.
6. Repeat the above for Channel 2 (V1 Voltage), Channel 3 (Core Voltage) and Channel 4 (Current).
7. Click **Save**. Wait for the programming to be downloaded to the controller, then right click on the analog expander record and click **Update module**.
8. Navigate to **Automation | Variables**.
9. Create a new variable with a descriptive name (e.g. CTRL1 PSU1 V2 Voltage Variable)
10. Set the **Scale** to 0.01.
11. Set the **Data value** to the corresponding data value programmed above.
12. Click **Save**.
13. Repeat to create variables for V1 Voltage, Core Voltage and Current.
14. You can display the variables on a status page or floor plan.
    - **Status page**: Add the variables to a status list.
    - **Floor plan**: Add the variables to the floor plan from the **Devices** menu.

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