



**PRT-GX-SRVR**

# Protege GX

End User Guide



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

Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

Last Published: 30-May-24 2:33 PM

# Contents

<b>Understanding your Protege GX System</b>	<b>5</b>
Before You Begin	5
Logging In	5
Creating a Secure Password	6
Changing Operator Password	6
<b>The Protege GX User Interface</b>	<b>7</b>
Home Page	7
Navigating the User Interface	7
Main Menu	7
System Navigator	7
Status Bar	8
Programming Window	8
Toolbar	9
Selecting Multiple Records	9
Using the Find Tool	9
Opening Multiple Windows	10
History, Usage and Events Tabs	10
<b>Managing Users</b>	<b>12</b>
Adding a User	12
Setting Start and Expiry Dates (Optional)	12
Creating an Access Level	12
Adding Doors to an Access Level	13
Adding Areas to an Access Level	13
Adding a Menu Group to an Access Level	13
Deleting Users	14
Disabling Users	14
Managing Users with Offline Wireless Locks	14
<b>Configuring Schedules and Holidays</b>	<b>16</b>
Creating Holiday Groups	16
Creating and Editing Schedules	16
Using a Schedule to Automatically Unlock a Door	17
Using a Schedule to Control User Access	17
Schedules and Multiple Time Spans	17
Different Hours for Weekends	18
Different Hours on a Holiday	18

Multiple Periods in a Single Day .....	18
Overlapping Periods .....	18
Overnight Schedules .....	18
Rules for Schedules and Holidays .....	18
Updating Offline Locks .....	18
<b>Working with Reports .....</b>	<b>19</b>
Event Reports .....	19
Viewing an Event Report .....	19
Event Search .....	19
Creating a User Report .....	20
Running a User Report .....	21
Print Preview Window .....	21
<b>Monitoring Menu .....</b>	<b>23</b>
Status Page View .....	23
Floor Plan View .....	23
<b>Using a Keypad to Arm/Disarm your System .....</b>	<b>24</b>
Status Indicators .....	24
Audible Feedback .....	25
Keypad Functions .....	26
Logging in to the Keypad .....	26
Logging Off .....	27
Arming Your System .....	27
Stay Arming an Area .....	27
Force Arming an Area .....	28
Disarming Your System .....	28
Entering a Duress Code .....	28
Acknowledging an Alarm .....	29
<b>Using Card Readers .....</b>	<b>30</b>
Presenting Cards .....	30
Card Types .....	30
Entry Mode .....	30
Arming and Disarming from a Card Reader .....	31
Using Offline Locks .....	31

# Understanding your Protege GX System

---

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

Designed with the end user in mind, Protege GX offers an intuitive and user friendly interface with graphical floor plans and highly customizable status pages for controlling and monitoring the system.

Customizable alarm and event filters enable you to sort and categorize the event and alarm data that is shown, and display information relevant to your site and setup.

The system can include a number of components:

- The **database server** or 'server' which stores the system data and provides the centralized connection to the rest of the system. Depending on your site, the server will typically be located in a control room with restricted access, and in most circumstances there is no reason for anyone but your security professional or property manager to require physical access to the server.
- **Protege GX client** computers and the **web client** interface which provide the user interface for authorized operators to access the system to add and update records and view status and event information.
- The **Protege GX controller** which is the central processing unit of the system. The controller will be mounted in an out of the way area such as a utility room or cupboard, and in most circumstances there is no reason for anyone but your security professional or property manager to require physical access to this unit.
- Various **detection sensors** (referred to as **inputs**) such as motion detectors or door contacts which are connected to the controller. If your system is armed and a sensor is activated, the input is 'opened' and sends a signal to the controller to trigger an alarm. A siren or other alarm device is activated, and the controller automatically transmits these details to your monitoring station or guardhouse. Entering your access code and disarming the system will turn off the alarm.
- One or more **keypads** which are used to arm/disarm the system and display the current status. Each keypad will typically be located in a convenient location inside your premises, close to the entry/exit door.
- One or more **card readers** and/or **wireless locks** that provide access control for the doors in your building. These may be operated using access cards, mobile phones, PIN codes or other types of credentials
  - Card readers are used on all sites. They are wired to the security system, allowing them to instantly check a user's current access permissions and grant or deny access.
  - Some sites such as apartment buildings (condominiums) may use offline wireless locks. These are not actively connected to the security system: instead, each user's card or mobile phone carries the access permissions they need ('data on card'). The data is updated whenever the user presents their card or phone at a wired update point reader located at the front door or another key location.

## Before You Begin

The flexibility of the Protege system allows an integrator to program functionality and system behavior to suit the needs of the site. This guide is aimed at explaining the most common settings.

**Your system may behave differently depending on how your integrator has programmed it.** Check with your installer for further operating instructions.

## Logging In

1. Double click the Protege GX icon on your desktop or browse to the program from the Windows Start Menu. The Login window is displayed.
2. Enter your details as supplied by your system administrator or Protege GX integrator:
  - **Username:** Your Protege GX operator username.
  - **Password:** Your Protege GX operator password.

- **Language:** Defines the language of the user interface.  
The two language options available are defined by your installation.
- **Server:** Enter the name or IP address of the Protege GX server that you are connecting to, or select a previously used server from the dropdown list. If connecting to a server on the local machine this field can be blank.  
You can use the **Clear** button to delete the currently selected server from the dropdown.

3. **Use Windows Authentication:** If your installation is using Active Directory integration, select this option to log in using your Windows account.

If using Windows authentication you do not need to enter user details. In the **Server** field enter the computer name or IP address of the Protege GX server. If connecting to the server from outside the network domain you must enter a valid Fully Qualified Domain Name.

4. Click **Log in**.

When logging in for the first time you will be prompted to add a new site and controller. You must complete this process before closing the client application, otherwise important default records will not be created.

The default operator logon is admin with a blank password. For security purposes it is strongly recommended that the admin password is immediately changed to a strong password.

## Creating a Secure Password

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

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

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

Passwords must comply with password policy requirements.

## Changing Operator Password

1. To change your operator password, click the **Change Password** button from the Home page.
2. This opens the **Change Password** window.
3. Complete the **Old Password**, **New Password** and **Confirm New Password fields** respectively.
4. Click **Ok**.

# The Protege GX User Interface

---

This section provides a guide to the sections and features of the Protege GX user interface.

Your operator security level determines the functions available to you when logged on. Access to view and edit some record types may have been restricted by your site administrator.

## Home Page

The **Home page** is displayed when you first log in.

From here you can:

- View **Operator details** about the operator currently logged in.
- Change the **Current site** that you wish to view (if you have multiple sites).
- Set the **Display theme** (light or dark) and the **Display color** for the operator.
- **Log out** to close Protege GX and return to the logon screen.
- Use the **Change password** function to change your operator password.

This option cannot be accessed when using Windows Authentication.

The main menu at the top of the screen provides access to all available functions for working in the system. You can return to the home page at any time by navigating to **Global | Home** from the main menu.

## Navigating the User Interface

There are two methods for navigating the user interface: the main menu and the system navigator.

### Main Menu

The main menu is located across the top of the screen and provides access to all the pages in the software.

Menu items are organized in logical groups relevant to their functions. For example, the **Monitoring** menu accesses functions for monitoring the site (e.g. status pages, floor plans, cameras), while the **Users** menu allows you to program users and related items such as access levels.

To open a specific programming window click on the relevant main menu item to expand it, then select the desired item from the dropdown menu to open the programming window.

Some menus and pages may not be available without the relevant license or sufficient operator permissions.

### System Navigator

The system navigator provides a quick way of accessing specific devices and programmed records.

You can open the system navigator by clicking the hamburger icon  at the top left of the window. The back arrow closes the system navigator.

The navigation bar opens on the left side of the screen, displaying the available categories. Records are arranged in a relational order, so you can locate records by expanding the relevant categories.

The system navigator will only display records for the **Site** currently selected on the home page.

To navigate the system:

- Click the arrow beside a category to view the records included in that category. For example, expand the **Controllers** category to view the controllers on the site.

- Click the arrow beside a record to view the categories associated with that record. For example, expand a specific controller record to view categories for the expander modules, inputs and outputs that might be connected to the controller.
- Left click a category or record to open the programming window for that item. For example, click on a specific area record to open the **Programming | Areas** programming window and highlight that record.
- Right click a record to open the context menu for that item, as well as the programming window. For example, right click a specific area record to open the area manual commands menu, allowing you to arm and disarm the area.

Trouble inputs that have a module type of Door (DR) are not displayed in the system navigator. This is a known limitation of the navigator categories. To view all trouble inputs, including those assigned to door records, click on any **Trouble Inputs** category to open the programming window.

## Status Bar

The status bar is located at the bottom of the screen and indicates communication status, alarm status and current login details.

- **Person icon:** Click this icon to display the operator who is currently logged in, and the server name.
- **Server icon:** This icon displays the current status of connected controllers. The possible statuses are:
  - **OK:** No issues with any controller.
  - **Controllers offline:** The number of controllers that are offline is shown in a red flag.
  - **Health status issues:** The number of health status issues that controllers are currently reporting.

To view a controller's health status navigate to **Sites | Controllers**, right click on the controller record and click **Get health status**.

- **Bell icon:** This icon displays the number of operator alarms that have not yet been acknowledged. Click on the icon to open the Alarms status page, which allows you to view and acknowledge any alarms.

Some third-party integrations also display icons in the status bar indicating the connection status of the integration.

## Programming Window

The programming window is where you program items in the system. It is divided into three parts:

- **Toolbar:** The programming toolbar at the top of the window provides buttons for various functions, such as adding, saving, searching, exporting and deleting records.
- **Record list:** The record list on the left of the window displays the records that can be programmed. The columns show key details about each record, such as the **Controller**, **Database ID** and **Last modified** date.

A number of features help you find the records you need:

- In the toolbar you can select the **Site** and **Controller** to view records for.
- Records can be sorted by any column, such as by name or Database ID. Click on any column header once to sort the records in a descending order, and again to sort in an ascending order.
- The **Find** button lets you filter the displayed records by any field. For example, you might filter door records to find doors with Entry in the name. For more information, see [Using the Find Tool](#) (next page).

In addition, you can right click on some records to open a context menu with manual commands. For example, this allows you to lock or unlock a door.

- **Programming tabs:** The programming pane to the right of the window is where you configure the settings. Available options are grouped into tabs, displayed along the top of the programming pane. For example, door programming has **Inputs** and **Outputs** tabs for configuring settings relating to inputs and outputs respectively. Each tab is in turn divided into several sections. Click on the header of a section to expand or hide the options within that section.



## Toolbar

The programming toolbar is displayed any time a programming window is opened. It contains useful buttons relevant to the selected feature. The most common buttons are described below.

Button	Function
Programming mode	Select whether you are programming in local (this controller only) or global (cross controller) mode. Only available for doors and programmable functions.
Controller	Select the controller to display records for.
Site	Select the site to display records for.
Add	Create a new record with default settings.
Save	Save any changes to the current record. After a record is saved, the changes may be downloaded to the controller.
Find	Open the find tool to filter the record list. For more information, see <a href="#">Using the Find Tool</a> (below).
Refresh	Refresh the current record to view any updates.
Export	Export the records displayed in the record list, including the information from specified columns. You can export the data to a CSV file or to the clipboard.
Copy	Copy the configuration from a specified record onto the current record. This function does not create a copy of the currently selected record. Instead, it overwrites the currently selected record with settings from another record.
Delete	Delete the record from the programming database. This will also delete any records that are dependent on this record. For example, if you delete an input expander, the inputs connected to it will also be deleted.
Breakout	Open the current programming window in a new breakout window. For more information, see <a href="#">Opening Multiple Windows</a> (next page).

## Selecting Multiple Records

In Protege GX you can select multiple records from the record list. This makes it convenient to apply programming changes to a number of records simultaneously.

- To select multiple records in a continuous span, click on the first record you wish to select, then hold **Shift** and click on the final record in the span.
- To select multiple discontinuous records, click on the first record you wish to select, then hold **Control** and click on each additional record to include.
- To select all records in the record list, press **Control + A**.

Once you have selected multiple records you can program all of them collectively. For example, you might want to set the same schedule on a number of access levels. Use **Control + Click** to select the required access levels, then set the **Operating schedule** and click **Save**.

You can also export selected records. Click **Export** in the toolbar and set the **Export type** to Selected records.

## Using the Find Tool

The find tool provides a convenient method for locating records from a list. It works by filtering the record list to include only records with specified field properties. For example, you might want to find all users with a specific access level assigned, or all doors with a certain feature enabled.

Effective use of the find tool is vital for managing large Protege GX systems. To use the find tool:

1. Navigate to the relevant programming window and click the **Find** button in the toolbar. The find tool opens.
2. Select the **Field** you will use to filter the record list. For example, in user programming you might filter based on the **Last name, Record group** or **Access level**.
3. In the **Values** section, set the terms of the filter. The values available depend on the type of field selected:
  - For text fields you can either include or exclude a segment of text (**Label**).
  - For dropdown fields you can choose which options will be included or excluded by the filter.
  - For checkbox fields you can filter for either **Active** (checkbox enabled) or **Inactive** (checkbox disabled).
  - For numeric fields you can set minimum and maximum values, and either include or exclude records within that range.

You may need to expand the window by clicking and dragging from the bottom right corner.

4. Click **OK**. The record list will now display all records which match the criteria you entered.
5. To clear the filter and view all records, click **Refresh** in the toolbar.

## Opening Multiple Windows

Protege GX provides the ability to view and work on multiple application windows (breakout windows) on a single client login. This allows you to program efficiently, as well as view multiple graphical floor plans or status pages at once when monitoring a building.

Breakout windows include the toolbar, record list and programming tabs, but do not include the main menu. Therefore, you can view and program records in breakout windows, but only navigate in the main window.

### Detach (Breakout) Button

The **Detach** button (or Breakout button) in the toolbar opens a new breakout window containing the programming page you are currently viewing. This allows you to keep the current window open while navigating to a new programming page.

This feature is especially useful for monitoring the system using status pages or floor plans. Open the desired status page or floor plan, then click **Detach** to open it in a new window. You can place one or more breakout windows on a second monitor to keep an eye on the entire system at once.

### Ellipsis Button

Many fields in Protege GX programming windows provide an **ellipsis button [...]** to the right of the field. Clicking the ellipsis button opens a new breakout window containing the records that can be programmed in that field. This is convenient for editing or creating related records as you work.

For example, when programming an access level you may need to create a new schedule. Click the ellipsis **[...]** to the right of the **Operating schedule** field. The schedule programming opens in a breakout window, allowing you to program and save the new schedule. You can then close the breakout window and immediately set the **Operating schedule** in the access level programming.

## History, Usage and Events Tabs

The History, Usage and Events tabs are available on most programming pages in the system. They help you keep track of important features and activity for each individual record.

- **History tab:** Shows the audit history of the record, allowing you to view when the record was created and modified, and by which operators. Each time the record is saved the change details are saved to this tab. To view the full information on what has been changed, highlight an entry in the history list and click **Details**.
- **Usage tab:** Shows where the record is currently being used in the software. For example, for a door record you might be able to see where the door is used in door groups, access levels and programmable functions. This is useful for determining which other records will be affected if you make a modification to the record. It is recommended that you check this tab before you delete a record, to ensure that it is not being used anywhere else in the system.

- **Events tab:** Shows recent events associated with the record. For example, for a door record you would see the most recent access granted, door opened and door forced events.  
Click **Load events** to load the events. The **Run as report** button opens a breakout window containing an event report for that record, which can be exported, printed or emailed as required. Alternatively, use the **Copy to clipboard** button to copy the events so you can paste them into a CSV file.

# Managing Users

---

A **user** is a person that requires access to the facility being controlled by the system. Each user has unique credentials, such as access cards and PIN codes, which they can use to unlock doors and disarm the alarm system.

**Access levels** are used to control what users can do, where they can go, and when they can do these things.

There are several methods for creating users. This guide describes the steps for adding users from the Users menu. For instructions on using alternative methods, talk to your installer.

Each site will have its own unique requirements for user records, so consult with your installer or system administrator about which options are used in your system.

## Adding a User

1. Navigate to **Users | Users**, then click **Add**.
2. Enter a **First Name** and **Last Name** for the user. The system will automatically fill in the **Display Name**.
3. Depending on your site configuration, you may need to select a **Record Group** for the user. This determines which Protege GX operators can view and edit this user record.
4. Enter a **PIN Code**. This is the number the user must enter when logging in to a keypad or accessing a door that requires PIN credentials.
5. Enter the user's credential(s) by typing the relevant facility and card numbers into the available fields. Each user can have up to 8 card numbers assigned. Multiple card numbers allow the same user to have multiple credentials (such as cards, fobs, mobile credentials and wireless remotes), without the need to program duplicate user records.
6. Select the **Access Levels** tab to add the required access level(s) to the user. When the user performs an action, the system checks the access level(s) to ensure the user has the relevant permissions to perform the requested action.

For more information, see [Creating an Access Level](#) (below).

7. Click **Add**, select the relevant access level(s), and click **OK**.
8. Click the **Save** button in the toolbar to save the new user. Now the user can use their assigned credentials and PIN to gain access to doors, and arm and disarm the system from a keypad.

## Setting Start and Expiry Dates (Optional)

Each user can be assigned access for a defined period by checking the **Start** and/or **End** options (in the **General** tab) and setting a date and time.

This allows you to issue and send out cards prior to access being enabled, such as for employees who have not started yet. You can also set credentials to automatically expire, for example when a contractor is due to finish on a set date.

## Creating an Access Level

1. Navigate to **Users | Access Levels**, then click **Add**.
2. Enter a **Name** for the access level.
3. Set the **Operating Schedule**. This determines what times the user has access to the doors, areas and other parts of the access level. By default this is set to *Always*, which grants access at all times. For example, you may wish to limit employee access to only the days when they work.
4. Click **Save**.

Now you can add the parts of the site which the user is permitted to access. The most common requirements are doors, areas and menu groups.

## Adding Doors to an Access Level

Doors and door groups define which doors a user has access to, and the schedule that determines when. Most likely your installer has already programmed the doors required for your site.

Door groups are typically used on sites that have a large number of controlled doors. For smaller sites, it is common to use individual doors. Depending on how your installer has set up your system, you may or may not have door groups.

### To Add Doors to an Access Level:

---

1. Select the **Doors** or **Door Groups** tab and click **Add**.
2. Choose the relevant doors or door group and click **OK**.
3. Set the **Schedule** to be applied. By default, the schedule is set to *Always*, meaning access to the selected doors is permitted at all times. You can assign a schedule to restrict access to the door(s) to the period set in that schedule. For example, you may limit access to an office so it can only be entered during office hours.
4. Save your changes.

## Adding Areas to an Access Level

Area groups are assigned to an access level and are used to control the areas that a user can arm and disarm.

### To Add an Area Group to an Access Level:

---

1. Select the **Arming Area Groups** or **Disarming Area Groups** tab and click **Add**.

**Note:** If a user is allowed to disarm an area, they are also allowed to arm it.

2. Choose the relevant area group and click **OK**.
3. Set the **Schedule** to be used. By default, the schedule is set to *Always*, meaning users can arm/disarm areas within that group at all times. You can assign a schedule to restrict arming and disarming to the period set in the schedule. For example, you may not wish an employee to be able to disarm an area outside of their normal working hours.
4. Save your changes.

For information on programming area groups, refer to the Protege GX Operator Reference Manual or ask your installer.

## Adding a Menu Group to an Access Level

Menu groups determine what the user can do on a keypad. Typically most users are permitted to arm/disarm areas, but menu functions used for troubleshooting and controlling the system are only available to installers.

### To Add a Menu Group to an Access Level:

---

1. Select the **Menu Groups** tab and click **Add**.
2. Select the relevant menu group and click **OK**.

You can only add one menu group to each access level.

3. Save your changes.

## Deleting Users

You can easily delete user records that are no longer required.

Simply select the record(s) to be deleted, then click the **Delete** button on the toolbar.

## Disabling Users

The **Disable User** setting (found under the **Options** tab) removes access immediately while still retaining the user record and its details. This is ideal for removing access temporarily, such as when staff are away on extended leave, or removing access while still retaining the user information.

## Managing Users with Offline Wireless Locks

There are some key differences in user management between standard systems and systems with offline wireless locks.

Because offline wireless locks are not actively connected to the rest of the system, when you add a user or update their settings you must load those settings onto the user's credential. You can do this using either a **desktop encoder** connected to the computer or an **update point reader** at the front door or another key location in the building.

Any features that are connected to other parts of the security system (e.g. disarming an area based on door access) are not available on offline locks. Some access control settings also may not work as expected.

### Adding an Access Level

---

1. Navigate to **Users | Access levels** and click **Add**.
2. In the **Doors** or **Door groups** tab, add the doors and groups that the user will have access to.
3. Program the **Schedule** for each door and door group.
4. Click **Save**.

### Adding a New User

---

1. Navigate to **Users | Users** and click **Add**.
2. Program the user settings as normal:
  - Name
  - Access levels
  - Expiry dates under **User expiry date/time** (optional)
3. The **Update period** (**General** tab) determines how frequently the user has to renew their access data by presenting their card to an update point reader. If this period expires, the user will not be able to access any offline locks until they update their card again.
4. Select **Enable office unlock** (**General** tab) to allow the user to toggle the lock when the door is in office mode (see page 31).
5. Before the user can use their card or mobile credential at an offline lock, you must initialize it to download the access data. There are two methods for initializing a credential:

#### Using a desktop encoder (cards only):

- Save the user record.
- In the **General** tab, scroll down to the **Credentials** section and select the ICT Wireless Locking credential type.
- Set the **Start** and **End** expiry dates if needed.
- Place the card on the desktop encoder.

- Click **Program card**. Protege GX will encode the card, download the access data and save the facility and card number to the user record.

#### Using an update point reader (cards and mobile credentials):

- In the **General** tab, scroll down to the **Credentials** section and select the ICT Wireless Locking credential type.
- Under **Credential**, enter the facility and card number of the user's card or mobile credential, separated by a colon (e.g. 10636:7482).
- Set the **Start** and **End** expiry dates if needed.
- Click **Save**.
- Wait for the programming to be downloaded to the controller.
- Badge the card or mobile device at an update point reader to encode the card and download the access data.

The user can now use their card or mobile phone to access offline wireless locks.

## Updating Users

---

When you update user settings such as access levels or schedules, the user must badge their card at an update point reader before the new settings will be available.

## Disabling Users

---

To disable a user record, you can:

- Set the **User expiry date/time** or credential **End** date to an invalid date (e.g. yesterday).
- Remove or edit the access levels that grant access to wireless locks.

The **Disable user** setting in **Users | Users | Options** does not work with offline locks.

## Disabling Users

---

When you delete a user record or credential, it is added to the **blocklist** which is loaded onto all user credentials. As users travel through the system they update the blocklist stored on each wireless lock. This reduces the chance that a deleted credential will be able to gain unauthorized access.

Credentials on the blocklist cannot be reassigned to another user until they have expired. As a rule of thumb, after blocklisting a credential you should set it aside for twice the **Update period** (e.g. 60 days) before reassigning it to another user.

Do not delete large numbers of user records or credentials at once (e.g. over 100). Instead, disable records using the methods above, then delete user records over a longer period of time.

# Configuring Schedules and Holidays

---

Schedules are defined timeframes that enable a function or access level to operate only within certain specified periods. They can be used to control when a user can gain access, unlock doors automatically, arm or disarm areas at certain times, turn devices on and off or change the way they behave at certain times of day. Schedules are central to automating access control and intrusion detection within the Protege system.

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

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

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

This section provides some useful programming tips for programming schedules effectively.

## Creating Holiday Groups

Before creating a schedule, it is convenient to program one or more holiday groups that apply to it. These should include national, local and other holidays which might cause your site to operate differently - for example, a retail business might have shorter (or longer) hours on a public holiday.

There is no need to program weekends as holiday groups.

1. Navigate to **Sites | Holiday Groups** and click **Add**.
2. Enter a **Name** for the holiday group.
3. Select the **Holidays** tab and **Add** holidays to the group.
  - Enable the **Repeat** option for holidays that occur on the same day every year.
  - For holiday periods that span multiple days (such as Christmas Day and Boxing Day), define the start (first day) and end (last day) dates.
  - For holidays that fall on a different day each year (such as Easter), these need to be programmed for each annual occurrence as the dates do not repeat. However, by adding multiple entries you can program many years in advance.
4. Click **Save**. Once you have programmed your holiday group(s), they can be applied to your schedules.

## Creating and Editing Schedules

1. Navigate to **Sites | Schedules**.
2. Click **Add** and enter a **Name** for the schedule, or select the schedule that you wish to edit.
3. Each schedule has multiple periods that can be programmed, which can be used for different days of the week or holidays. For each period, enter the start and end times that you wish the schedule to operate, and tick the boxes for the required days of the week.

For more information, see [Schedules and Multiple Time Spans](#) (next page).

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

4. For each period, select the **Holiday Mode** to define how the schedule will operate during a holiday period. Choose from:



- **Disabled on Holiday:** When selected, the period will **not** make the schedule valid on a holiday. In other words, if a door is programmed to unlock by this schedule, it will not unlock on a holiday when this option is selected. This is the default mode of operation for schedules
  - **Enabled on Holiday:** When selected, the period will only ever make the schedule valid **on** a holiday. For example, a user might have different access hours on a holiday compared to a normal day.
  - **Ignore Holiday:** When selected, the period will make the schedule valid **regardless** of whether the day is a holiday or not. For example, the manager might be able to access the building at all times, holiday or not.
5. Select the **Holiday Groups** tab. Click **Add** and select the holiday groups you wish to apply to the schedule.
- This tells the schedule which days are holidays, but it does not tell the schedule what to do if it is a holiday. This is defined by the **Holiday Mode** above.
6. Click **Save** to finish creating your schedule.

## Using a Schedule to Automatically Unlock a Door

Assigning an unlock schedule to a door will determine when that door will unlock. For example, if you have an office entry door that you need to unlock at 8am and lock again at 5pm, you would create a schedule for the opening hours, then assign that schedule to the door.

1. Navigate to **Programming | Doors**.
2. Choose the door you wish to control and set the **Unlock Schedule**.
3. Save your changes.  
In many cases, you'll also need to prevent the door from unlocking if nobody turns up for work. A simple way to achieve this is using the Schedule Operates Late to Open feature.
4. Select the **Options** tab and enable the **Schedule Operates Late to Open** option and save your changes.  
This prevents the door from unlocking until the first user accesses the door.

There are many other door options that can be programmed, but these are outside the scope of this guide. For further assistance, and before making changes, we recommend you talk to your installer.

## Using a Schedule to Control User Access

Schedules are used to control **when** a user can do something. Assigning an operating schedule to an access level determines when the access level is valid and when users can access the options programmed within the access level.

1. Navigate to **Users | Access Levels**.
2. Select the access level you wish to add the schedule to, and set the **Operating Schedule**.
3. Save your changes.

You can also assign a schedule to the doors within an access level to restrict access to the hours defined, and/or to the area groups to restrict arming/disarming to a specific period. This provides more flexibility by allowing you to define access at a more granular level. For example, you may wish to restrict access to one group of doors to scheduled office hours, but permit access to another group outside these hours.

There are many other uses for schedules. For further assistance, we recommend you talk to your installer.

## Schedules and Multiple Time Spans

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

Below are some examples of when you might use this.

## Different Hours for Weekends

Premises may need to open for shorter (or longer) hours on a weekend.

To set this up, simply add a second period with shorter hours and select the relevant day(s).

## Different Hours on a Holiday

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

To set this up, simply set up another period with the required days and times, and set the **Holiday mode** to Enabled on holiday.

## Multiple Periods in a Single Day

Sometimes multiple periods are required in a single day. Consider a movie theater where there are multiple session times, so the doors must be unlocked during certain periods.

Set as many separate periods for the same day(s) as required.

## Overlapping Periods

Where periods overlap, the schedule will take the sum of all periods.

## Overnight Schedules

Where a schedule is required to operate overnight, enter a start time, but leave the end time as **12:00 AM**. This results in the period being valid from the start time until midnight.

Now program a second period to start at midnight and continue until the end of the shift. By extending the days that the period is valid, we can create an overnight Monday to Friday shift.

The graphics view is useful for providing a visual representation of when the schedule is valid.

## Rules for Schedules and Holidays

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

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

1. The holiday must be programmed in a holiday group.
2. That holiday group must be applied to the schedule in the **Holiday groups** tab.
3. The **Holiday mode** for the schedule period must be set to Disabled on holiday.

## Updating Offline Locks

Because offline locks are not connected to the system, any changes to their configuration must be transferred to the lock by an authorized installer or administrator using the Protege config app. This includes changes to:

- Door settings
- Schedules for user access or automatic unlocking
- Holiday groups
- Door groups for user access

Keep in mind that features that relate to other parts of the security system (e.g. disarming an area based on door access) are not available on offline locks.

Contact your installer if you need to update the schedules or any other settings on your offline wireless locks.

# Working with Reports

---

Use the Reports menu to view a range of system reports.

Powerful filtering and flexible reporting options are standard within the Protege GX application, enabling you to easily obtain detailed and relevant event and user information. All reports allow the information returned to be further filtered, sorted, printed, emailed, and exported to a range of file formats.

## Event Reports

Event reports enable an operator to view what is happening within the system with ease. Events are categorized for easy identification and details can be readily accessed.

By default, there are three preconfigured event reports already set up:

- All Events
- All Alarms
- All Acknowledged Alarms

Your system administrator may have created custom reports for your specific site.

## Viewing an Event Report

1. Navigate to **Reports | Event**.
2. Select an event report to run from the list available and click **Execute**.
3. Enter details of the period you want to list events for and click **Ok**.

A list of events is returned and displayed in a list spanning from the latest event to the oldest.

4. This list can be sorted and filtered to display a subset of events rather than showing them all at once. You can also adjust the list to show and hide certain columns, or to resize the columns that are displayed:
  - **Resize columns** by hovering your mouse over the edge of the column header until it forms a double-headed arrow then dragging the column to the required size. You can also use the right click menu to automatically resize your columns for the best fit.
  - **Reorder columns** by dragging and dropping a column header to a new position in the grid.
  - **Remove columns** by dragging them down from the column header section into the list. When a red delete icon appears over the column header, release the mouse to remove the column.
5. If more than 200 events are returned, use the **Previous** and **Next** buttons to navigate between results that span multiple pages.
6. Use the **Print** button to open the print preview window where you can print, export, or email the results.
7. Use the grid view to further sort, group, and filter the results that are displayed.

## Event Search

The event search provides a simple way of viewing what is happening in the system.

An event search generates a 'one-off' temporary report that can be printed or exported but cannot be saved.

1. Navigate to **Events | Event Search**.
2. Select the time period you wish to include events from.
  - Choose a period from the available list or enter a specific start date and time.
  - If required, select a specific end date and time.
3. You can choose to **Include All Event Types** or disable this option and select specific event types.

4. If the option to **Include All Event Types** has been disabled, you will need to define the event types to include.
  - Click **Add** to open the **Select Event Types** window.
  - Select the relevant event type(s) and click **Ok**.
5. Click the **Records** tab to create up to two (optional) record filters that enable you to further restrict the results returned.
6. Click **Add** to open the **Select Devices** window.
  - Select the **Device Type** and **Controller**, then select the **Devices** from those available.
  - Repeat to create a second record filter if required.
7. Click **Find** to start the search.
8. A temporary report is generated and displayed in a separate window. You can adjust the list to resize or reorder the columns that are displayed:
  - **Resize columns** by hovering your mouse over the edge of the column header until it forms a double-headed arrow then dragging the column to the required size. You can also use the right click menu to automatically resize your columns for the best fit.
  - **Reorder columns** by dragging and dropping a column header to a new position in the grid.
  - **Remove columns** by dragging them down from the column header section into the list. When a red delete icon appears over the column header, release the mouse to remove the column.
9. If more than 200 events are returned, use the **Previous** and **Next** buttons to navigate between results that span multiple pages.
10. Use the **Print** button to open the print preview window where you can print, export, or email the results.
11. Use the grid view to further sort, group, and filter the results that are displayed.

## Creating a User Report

User reports contain detailed information about the users in your system. By creating user reports for the information you need, you can quickly identify important details such as which users have access to selected doors, have triggered defined events, or have cards due to expire.

1. From the main menu, select **Reports | Setup | User**.
2. Click the **Add** button and enter a name for the report.
3. Select the **Report Type** to run from those listed. Choose from:
  - All Users
  - All Users who have Access to the selected Doors
  - All Users included in the following Access Levels
  - All Users by Events
  - All Users by Record Group
  - Users by Event Type/Doors
  - Cards About to Expire
  - Last Users through the Door(s)
  - All Users not in Events
  - All Current Visitors
  - All Overdue Visitors
  - All Visitors by Date
  - Recorded Modified History Report

As the report type is selected the screen is updated, enabling you to define the additional options relevant to that report type (such as doors, access levels, event types, and so on).

4. Enter any **Sorting** criteria you require:

- **Sort Column:** Determines which column the results will be sorted by.
  - **Sort Direction:** Determines if the returned data is sorted in ascending or descending order.
  - **Group by:** Groups the returned data by the column defined.
5. Click the **Columns** tab to choose the columns to include in the report. By default, only the last and first names are included.
  6. Click **Add** to open the **User Fields** window. Select the columns to include then click **OK**.
  7. The columns are added in alphabetical order. To change the order, select an item and use the **Move Up** and **Move Down** buttons until you have the sequence you require.
  8. Click the **Email** tab to enter details of who and when the report should be emailed to.
  9.
    - **Operators:** Add the operator(s) to send the report to.
    - **Email Report:** Select to enable email. Note that the operator must have an email address defined under their operator settings and the SMTP server must be defined under the Global settings or the email will fail to send.
    - **Report Format:** Defines the format of the file format if the report that will be sent. Choose from PDF, CSV, Text, or XLS.
    - **Time:** Defines the time and day(s) that the report will be sent.
    - **Current Server Time:** Defines the current local time of the server or the current local time where the Protege GX services are running.
  10. Click **Save** to save the report.

## Running a User Report

1. Navigate to **Reports | User**.
2. Select a user report to run from the list available and click **Execute**.
3. A list of users is returned and displayed using the grid view.  
You can adjust the list to show and hide certain columns, or to resize the columns that are displayed:
  - **Resize columns** by hovering your mouse over the edge of the column header until it forms a double-headed arrow then dragging the column to the required size. You can also use the right click menu to automatically resize your columns for the best fit.
  - **Reorder columns** by dragging and dropping a column header to a new position in the grid.
  - **Remove columns** by dragging them down from the column header section into the list. When a red delete icon appears over the column header, release the mouse to remove the column.
4. Use the **Print** button to open the Print Preview window where you can print, export, or email the results.
5. Use the Grid View to further sort, group, and filter the results that are displayed.

## Print Preview Window

Once you have generated a report, use the **Print** button in the toolbar to open the Print Preview window. This window will only display results that are currently visible in the report, so you can filter, group and order as required and then easily export the results.

The print preview will only display the current 'page' of the report (i.e. 200 results). Multiple exports may be required for large reports.

Use the options on the toolbar to preview, print, export and/or email the results.

Button	Function
Search	Opens a basic find tool, allowing you to search the preview file for specific terms.
Open	Allows you to open a previously saved report preview file (.prnx format).

Button	Function
Save	Saves the current report preview file in .prnx format to temporarily store reports to open again within Protege GX. To export a report in a more widely used format use the <b>Export</b> option.
Print	Opens a print dialogue, allowing you to select a printer, printing preferences, page range and number of copies before printing. It is not possible to print reports in landscape orientation directly to a printer. For landscape orientation it is necessary to export the report to PDF, which can then be sent to the printer.
Quick print	Prints the report to your default printer with default settings.
Page setup	Displays the page setup dialog, where you can specify printer settings such as paper size, page orientation and margins.
Scale	Scales the content of the report on the page. This allows you to scale the width of the report to a number of pages. For example, a scale of 100% means that the width of the report spans a single page. With a scale of 200% the report will be scaled up to span two pages wide.
Zoom out	Zooms out one step.
Zoom	Changes the zoom level to one of the predefined sizes.
Zoom in	Zooms in one step.
First page	Skips to the first page of the report.
Previous page	Navigates back one page in the report.
Next page	Navigates forward one page in the report.
Last page	Skips to the last page of the report .
Export	Exports the report to one of a number of available formats: PDF, HTML, MHT, RTF, XLS, XLSX, CSV, Text, Image or XPS. The main button automatically exports to PDF; you can click the arrow to the right of the button to select a different format. Each format requires you to configure options specific to that format. Ticking the <b>Open after export</b> box at the top of the window will cause the exported file to open when the export is complete. You can also set up a regular file export of specific reports in the <b>Reports   Setup</b> programming. Exported CSVs may contain blank columns. This is a known issue.
Send via email	Saves the report in a specified format, then opens a new message with the report attached using your computer's default email program. You can also set up a regular email export of specific reports in the <b>Reports   Setup</b> programming.

# Monitoring Menu

---

Functions for monitoring your site are found here. From this menu you can create and view floor plans and status pages, create status lists and web links, and configure standalone cameras and DVR integrations.

## Status Page View

Status pages provide an intuitive and efficient overview of your system and each page is fully customizable to include the information you want, with content relevant to your site. A status page can include devices as such as doors, areas, inputs and outputs, live event lists, camera feeds and floor plans.

### To View a Status Page

---

1. From the main menu, select **Monitoring | Status Page View**.
2. The default status page is shown. Select an alternative status page from the dropdown list if required.
3. The screen updates automatically to display the page selected.
4. Right clicking a device such as a door or area on the status page opens a menu where you can manually control the device. For example, you can use this to unlock a door, activate an input or arm an area.

## Floor Plan View

Floor plans enable you to view and control doors, outputs, inputs, cameras, areas, trouble inputs, elevators and variables from a floor plan in real time. Objects on a floor plan are updated dynamically both on the graphical display and in the status pane to the right of the floor plan.

### To View a Floor Plan

---

1. Navigate to **Monitoring | Floor Plan View**.
2. The default floor plan is shown. Select an alternative floor plan from the dropdown list if required.
3. The floor plan consists of the following components:
  - A graphical representation of the floor plan.
  - A status list that dynamically updates to display the real time status of the devices used on the floor plan.
  - An event window displaying a list of floor plan events, and optionally other custom event tabs.
4. Right-clicking a device from the floor plan opens a menu where you can manually control the device by selecting the required action from the menu.

# Using a Keypad to Arm/Disarm your System

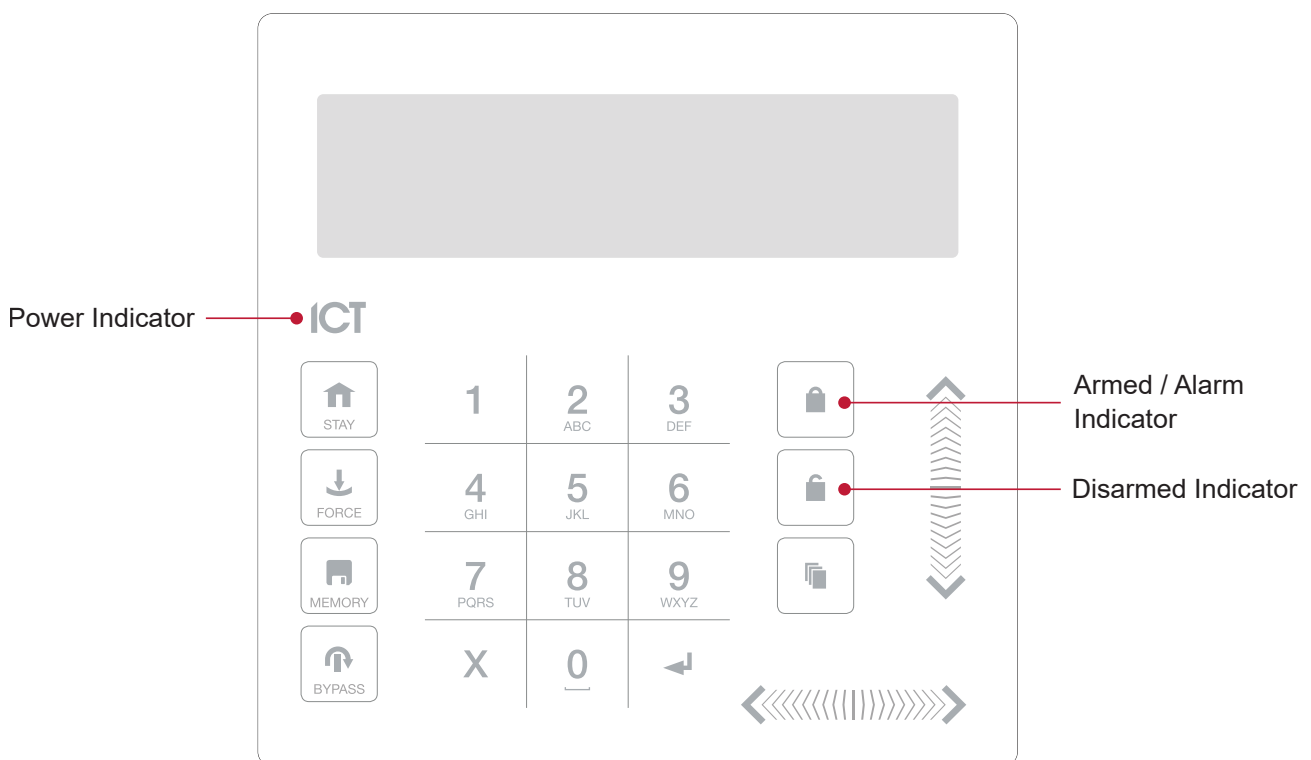
Keypads are typically located near an entrance or door to allow areas within the system to be armed and disarmed.

The following instructions provide an overview of the keypad and how it is used to arm and disarm your system. There are a number of keypad features that are only available when the option has been enabled by your installer. Your installation company or security professional can provide you with further information on these features.

For further information, see the user manual for your keypad model.

## Status Indicators

The keypad features three status indicator lights showing the condition of the Protege system.



### Power Indicator

When the power indicator **on**, the system is powered and operating normally. If there is a complete power failure this indicator will be **off**.

### Armed / Alarm Indicator

When the armed/alarm indicator is **flashing** the system is in alarm and you need to enter your user code to silence the alarm. When **on**, the system is armed.

This indicator is programmable and may not function as described here. Verify the operation with your installation company or security professional.

### Disarmed Indicator

When the disarmed indicator is **on** the system is disarmed. Alternatively, when the disarmed indicator is **on** the system may be ready to arm (all inputs are secure). Enter your user code to arm.



This indicator is programmable and may not function as described here. Verify the operation with your installation company or security professional.

## Confidentiality Mode

Keypads include a confidentiality mode where all lights (Power, Disarm, Arm and LCD backlight) will turn off when the keypad is not in use. Confidentiality mode may be enabled by your installer.

## Audible Feedback

When a key is pressed, a short audible tone is generated. Other tones are generated when certain functions are performed.

### Confirmation Tone










When an operation has been successfully completed, the keypad generates a sequence of four audible tones.

### Rejection Tone

When the system times out or when an operation is incorrectly entered, the keypad generates an audible tone for three seconds.

If required, audible tones can be silenced by pressing and holding the **[CLEAR]** key for 3 seconds. This option must be enabled by your security professional or system administrator.

# Keypad Functions

Key	Function
0-9	The primary function of the numeric keys is to enter user codes. When controlling devices the <b>[1]</b> key turns the device on, the <b>[2]</b> turns the device off, and in the on state the <b>[3]</b> key latches the device.
	The <b>[ARM]</b> key is used to start the arming process for an area.
	The <b>[DISARM]</b> key is used to silence alarms, disarm the area, and cancel an arming sequence.
	The <b>[MENU]</b> key is used to access the menu and can be followed by menu shortcut selection key(s) that represent a menu item. When the <b>[MENU]</b> key is held for 2 seconds, the keypad will recognize it as the <b>[FUNCTION]</b> key, which can be programmed to unlock a door.
	The <b>[STAY]</b> key is used to initiate the stay arming process for an area.
	The <b>[FORCE]</b> key is used to force arm an area.
	The <b>[MEMORY]</b> key will take a user directly to the memory view menu.
	The <b>[BYPASS]</b> key can be pressed when an area is breached during an arming process to bypass the displayed input.
	The <b>[CLEAR]</b> key will log off the user currently logged in to the keypad. When pressed while not logged in the display will be refreshed.
	The <b>[ENTER]</b> key is used to confirm an action on the keypad, acknowledge memory and alarm information, and move to the next programming screen.
ARROW KEYS	The arrow keys are used to scroll the menu, move the focus of a program window to the next screen, and move the cursor when programming or editing values.

## Logging in to the Keypad

### Single Credential Login

1. To log in, enter your **PIN** code and press **[ENTER]**.

Once a valid PIN is entered you will be presented with a welcome screen, area status or available menu.

### Dual Credential Login

You may need to enter dual credentials to log in to the keypad, if this has been configured by your installer.

1. To log in using dual credential authentication, enter your **User ID** credential code and press **[ENTER]**.
2. When prompted, enter your **PIN** code and press **[ENTER]**.

Once a valid PIN is entered you will be presented with a welcome screen, area status or available menu.

If the **Lock Keypad On Excess Attempts** option has been enabled on your system, entering an invalid login three times will lock the keypad for a short period, preventing further login attempts by any user. The lockout time is defined under the keypad programming.

## Logging Off

You are automatically logged out after a short period of inactivity, or if the **[CLEAR]** key is pressed while you are logged in.

The period of inactivity is defined by the installer. Even if the system has been programmed to automatically log you out, it is good security practice to get into that habit of logging out when you walk away from the keypad. This prevents unknown parties from using your login to disarm the area.

## Arming Your System

When leaving your building, you will need to arm (or activate) the areas within your system. You may have a single area or multiple areas that can be armed independently.

1. Enter your **[USER CODE]** and press **[ENTER]** to login to the system.
2. A greeting is displayed. Press any key to continue or wait for the greeting to time out.
3. An area and status will be displayed. If you have access to more than one area, use the up and down keys to scroll through the available areas and locate the area you wish to arm.
4. Press the **[ARM]** key to start the arming process.
5. The system checks that all inputs (such as motion detectors and door latches) are closed before beginning to arm the area. If you attempt to arm the system while an input is open, the keypad will emit a beep and display a warning message onscreen. You will either need to close the input before you can proceed with arming the system, or you can choose to **bypass** the input.  
Bypassing an input tells the system to temporarily ignore that input until the next time the system is armed. For example, you may wish to disarm a sensor in a room where you're making repairs or renovations, or keep a window open to allow fresh air in.
6. To bypass an open input, press **[BYPASS]**. A prompt appears advising that the system has a number of bypassed inputs. Press **[ARM]** to confirm the action or **[DISARM]** to halt the arming process and return the area to the disarmed state.
7. The area will begin the exit delay. This provides you with enough time to exit the area before the system arms completely. The keypad and/or card reader will beep during the exit delay period.
8. Press **[CLEAR]** to log out. Leave the area before the exit delay finishes and the area is armed.

## Stay Arming an Area

Stay arming is an option that must be enabled by your installer.

Stay arming allows you to remain in an area while it is partially armed. Selecting this mode only arms the exterior sensors and not the interior ones, allowing you to freely move around inside without setting the alarm off. For example, if you are working late, you can arm a portion of the building to protect the windows and doors without arming other inputs.

1. Enter your **[USER CODE]** and press **[ENTER]** to log into the system.
2. A greeting is displayed. Press any key to continue or wait a few seconds for the greeting to timeout.
3. Press the **[STAY]** key to start the stay arming process.
4. The system checks that the exterior sensors in the area are closed while bypassing the interior sensors.

5. If all the exterior inputs are closed, the area goes into exit delay. Once the exit delay time has elapsed, the area is stay armed.

## Force Arming an Area

Force arming is an option that must be enabled by your installer.

Force Arming allows you to arm the system without waiting for all the inputs in the system to close. It is commonly used when a motion detector is monitoring the space where the keypad is located. If the motion detector has been programmed as a force input, the system will allow you to arm the area even if the input is open. When you leave the range of the motion detector, the input will close and the system will start to monitor it.

1. Enter your **[USER CODE]** and press **[ENTER]** to log into the system.
2. A greeting is displayed. Press any key to continue or wait a few seconds for the greeting to timeout.
3. Press the **[FORCE]** key to start the force arming process.
4. The system checks that the inputs in the area are closed, automatically skipping any open inputs that can be force armed.
5. If all the inputs are closed, the area goes into exit delay. Once the exit delay time has elapsed, the area is force armed.

## Disarming Your System

Upon entering the premises, you will need to disarm (or deactivate) the system.

Entry points, such as the front door, are programmed with an entry delay time. When an entry point is opened, the keypad will emit a continuous audible tone until you disarm the system. Your system will not generate an alarm until this timer elapses.

1. Enter your **[USER CODE]** and press **[ENTER]** to login to the system.
2. A greeting is displayed. Press any key to continue, or wait a few seconds for the greeting to time out.
3. An area and status will be displayed. If you have access to more than one area, use the up and down keys to scroll through the available areas and locate the area you wish to disarm.
4. Press the **[DISARM]** key to disarm the area.

If an alarm has been triggered while your system was armed, a message is displayed onscreen. To acknowledge an alarm, simply press **[ENTER]** and continue with the disarming process.

## Entering a Duress Code

If you are forced to arm or disarm your system or unlock a door, you can enter a **duress code**, which will complete the action and immediately transmit a silent alert message to the monitoring station.

Depending on how your system has been configured, you may have one of two common types of duress code:

- A designated user duress code which applies generally to the whole site.
- A specific duress code which is equal to your regular user code plus one. For example, if your pin was 1234, the duress code would be 1235.

Note that the +1 counter applies to the last digit only. This means if the user pin is 1239, the pin to trigger a duress code would be 1230.

Duress code functions must be enabled before they can be used. Your installer can confirm which of these options have been configured and provide you with further operating instructions.

## Acknowledging an Alarm

Alarms are stored in memory until they have been acknowledged.

- To acknowledge an alarm, simply press **[ENTER]** and continue with the disarming process.
- If you proceed with disarming without acknowledging the alarm, you can view it later by pressing **[MENU]** + **[MEMORY]** and **[ENTER]** then using the arrow keys to view the details. Press **[ENTER]** to acknowledge and clear the alarm from memory.

# Using Card Readers

---

Proximity readers work by constantly emitting a short range radio frequency (RF) field. When an access card comes within range of this field, an integrated chip within the card transmits a card number back to the reader. The reader sends these details to the security system, which grants or denies you access based on your permissions.

Many card readers also have Bluetooth® and NFC capabilities, allowing users to gain access with mobile credentials using the Protege Mobile App.

## Presenting Cards

It can help if you think of a card reader as a security guard. When requesting access, the reader needs to be shown your credentials, much like a security guard might inspect an ID card. To gain access to an area via a door with an access card reader, you simply present your access card to the reader.

If you are using the Protege Mobile App, you can unlock doors with your phone using either Bluetooth® or NFC. To unlock a door, log in to the app and keep it open or minimized on your phone, then present your phone to the card reader. To unlock the door at greater distances, increase the **Bluetooth Range** or use the **Shake to Unlock** feature.

## Card Types

There are a number of options for modern proximity cards - 125kHz, MIFARE and DESFire. While there is little visible difference between the various card types, what happens behind the scenes is quite different.

Historically, card based access control systems were built around a card with a magnetic stripe that required a swipe action through a magnetic card reader to gain access to a door. These cards had a number of disadvantages, including a high wear rate and very low security.

Newer proximity technology allows cards to be read without physically contacting the reader, and apart from the frequency that is used to transmit data, there are key differences in security and the card read range.

- 125kHz cards offer a good read range (around 10cm) and a short read time, which means you can effectively present, swipe, or wave your card in the general direction of the reader to get a successful read.
- MIFARE has a slightly reduced read range (around 7cm) and a longer read time, which means that generally a MIFARE card cannot be simply swiped or waved at a card reader, but must be presented.
- DESFire is the highest standard of card security currently available, however it has a further reduced read range of 1-2cm. This means that a DESFire card must be firmly presented to the reader and held in place until access is granted. Waving or swiping a DESFire card will not result in a successful read.

Discuss with your installer which access card technology is being used on your site.

## Entry Mode

Your installer will have programmed the doors in your system with an entry mode that controls how a door operates. These include:

- **Card Only:** A card badge is all that is required to unlock the door.
- **Card and PIN:** Both a card badge and PIN entry is required to unlock the door.
- **Card or PIN:** Either a card badge or a PIN entry can be used to unlock the door.
- **PIN Only:** A PIN entry is all that is required to unlock the door.

The mode used may vary according to your system requirements and may also be scheduled based on the time of day, allowing different security credentials to be used. For example, a door may be programmed to require card only access between standard office hours of 8am and 5pm, but require both card and PIN outside these hours for added security.

## Arming and Disarming from a Card Reader

Depending on how your system has been programmed, you may be able to disarm the area behind a door simply by badging your card to unlock the door. This removes the inconvenience of needing to disarm the area using a keypad after you enter.

Commonly, systems are configured to allow you to arm the area behind a door from a card reader also. There are a few common options:

- Badge at the reader twice to arm the area.
- Badge at the reader three times to arm the area.
- Hold a button and badge at the reader to arm the area.

Your installer can confirm whether these options are enabled.

## Using Offline Locks

Offline wireless locks operate differently from the wired card readers in the system. Instead of sending your credential to the system for validation, offline locks use the access data stored on your card or mobile phone to validate your access permissions.

**Update point readers** at key locations such as the front door are used to update and renew the data stored on your credential. You must present your credential to the update point reader regularly, as the data will expire after a period of time (typically every 30 days). The reader will rapidly flash purple while it is updating your data, then flash green and beep when it unlocks the door.

Be patient while the update point reader updates the card. Do not remove the card until the reader stops flashing purple.

Wireless locks have various operating modes:

- **Standard:** When you gain access, the door unlocks temporarily.
- **Unlock on schedule:** The door unlocks based on a specific schedule (e.g. working hours).
- **Office unlock:** Any authorized user can unlock the door temporarily, but specific users (e.g. managers) can unlock the door indefinitely by holding down the inside handle and presenting a credential to the reader. Repeat the process to relock the door.
- **Toggle:** Whenever any authorized user accesses the door, the lock will toggle on/off.
- **Exit leaves door unlocked:** When someone exits the door using the inside handle, it will remain unlocked. Depending on the settings, it will either lock again after a set length of time or remain unlocked until someone badges a card.

Each lock can use different modes based on different schedules (e.g. office unlock mode during office hours, then standard mode after hours).

In addition, with some lock models you can use the inside thumbturn or key to activate **privacy mode**. This will deny access to anyone trying to unlock the door from the outside unless they have a key or super user rights.

Designers & manufacturers of integrated electronic access control, security and automation products.  
Designed & manufactured by Integrated Control Technology Ltd.  
Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

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