PRT-GX-SRVR

# Protege GX System Management Suite

## Operator Reference Manual

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 2003-2025. All rights reserved.

Last Published: 18-Dec-25 3:12 PM

# Contents


Protege GX Operator Reference ..... 15
The Protege GX User Interface ..... 16
Logging In ..... 16
Home Page ..... 16
Supported Screen Resolutions ..... 16
Changing the Operator Password ..... 17
Creating a Secure Password ..... 17
Navigating the User Interface ..... 18
Main Menu ..... 18
System Navigator ..... 18
Status Bar ..... 18
Programming Window ..... 20
Toolbar ..... 20
Selecting Multiple Records ..... 21
Using the Find Tool ..... 21
Opening Multiple Windows ..... 22
History, Usage and Events Tabs ..... 22
Reports Window ..... 22
Programming Tips and Troubleshooting ..... 23
Additional Resources ..... 23
Naming Conventions ..... 23
Cross Controller Operations ..... 24
Guide to Common Event Types ..... 25
User Access Events ..... 25
Reporting Events ..... 27
Database Backup and Restore ..... 29
Database Compatibility ..... 29
Creating Database Backups ..... 29
Restoring Database Backups ..... 31
Backing up and Restoring with Transparent Data Encryption ..... 31
Backing up and Restoring with Encrypted Columns ..... 32
Viewing Controller Health Status ..... 34
Troubleshooting Controller Connectivity ..... 35
Communication Requirements ..... 35
Check that the Services are Running ..... 35

Confirm Controller IP Address ..... 35
Confirm Controller Serial Number ..... 37
Duplicate IP Address or Serial Number ..... 38
Confirm the Event Server is Functioning ..... 38
Confirm Ports ..... 39
Check Computer Name ..... 39
Repair Database Compatibility ..... 39
Windows Firewall ..... 39
Encryption ..... 41
Telnet ..... 45
Global Menu ..... 46
Home ..... 46
Global settings ..... 47
Global settings | General ..... 47
Global settings | Email settings ..... 48
Global settings | Display ..... 49
Global settings | Sound ..... 49
Sites ..... 51
Sites | General ..... 51
Sites | Display ..... 51
Sites | Active Directory ..... 52
Sites | Site defaults ..... 53
Sites | User photos export ..... 55
Sites | Biometrics ..... 55
Sites | Salto ..... 56
Sites | Cencon ..... 57
Sites | Key cabinets ..... 57
Sites | Portal ..... 58
Sites | Offline wireless locks ..... 58
Operators ..... 60
Operators | General ..... 60
Roles ..... 62
Roles | General ..... 62
Roles | Tables ..... 62
Roles | Sites ..... 63
Roles | Security levels ..... 63
Roles | Display ..... 63

Role Presets and Tables ..... 63
Download server ..... 69
Download server | General ..... 69
Event server ..... 70
Event server | General ..... 70
Modem ..... 71
Color maps ..... 71
Color maps | General ..... 71
Color Maps Device tabs ..... 71
Floor plan symbols ..... 73
Floor plan symbols | General ..... 73
Event types ..... 75
Event types | General ..... 75
Sites Menu ..... 76
Schedules ..... 76
Schedules | Configuration ..... 76
Schedules | Options ..... 77
Schedules | Holiday groups ..... 77
Edge Triggering ..... 77
Configuring Schedules and Holidays ..... 78
Calendar actions ..... 80
Viewing Calendar Actions ..... 80
Creating a Calendar Action ..... 80
Holiday groups ..... 82
Holiday groups | General ..... 82
Holiday Groups | Holidays ..... 82
Controllers ..... 83
Controllers | General ..... 83
Controllers | Configuration ..... 84
Controllers | Options ..... 89
Controllers | Time update ..... 90
Controllers | Custom reader format ..... 90
Manual Controller Commands ..... 91
Adding a Controller ..... 94
Cross controller groups ..... 97
Cross controller groups | General ..... 97
Biometric readers ..... 99

Biometric readers | General ..... 99
Security levels ..... 100
Security levels | General ..... 100
Security levels | Tables ..... 100
Security levels | Manual commands ..... 104
Record groups ..... 105
Record groups | General ..... 105
Record groups | Custom data ..... 105
Credential types ..... 106
Credential types | General ..... 106
Card profiles ..... 109
Card profiles | General ..... 109
Function codes ..... 110
Function codes | General ..... 110
Jobs ..... 112
User import job step ..... 112
Import users ..... 112
Importing Users from a CSV ..... 112
Batch add users ..... 112
Batch Adding Users ..... 113
Users Menu ..... 114
Users ..... 114
Users | General ..... 114
Users | Access levels ..... 118
Users | Options ..... 118
Users | Photo ..... 121
Users | Extended ..... 121
Users | Attendance ..... 122
Users | Area groups ..... 122
Users | Biometrics ..... 122
Users | Salto ..... 123
Users | Salto doors / door groups ..... 124
Users | Cencon locks ..... 124
Users | Accommodation ..... 124
Users | Visitor ..... 124
Users | Portal ..... 125
Manual User Commands ..... 125

User search ..... 126
Running a User Search ..... 126
Access levels ..... 128
Access Levels | General ..... 128
Access levels | Doors ..... 130
Access levels | Door groups ..... 130
Access levels | Floors ..... 130
Access levels | Floor groups ..... 130
Access levels | Elevator groups ..... 130
Access levels | Menu groups ..... 131
Access levels | Arming area groups ..... 131
Access levels | Disarming area groups ..... 131
Access levels | Outputs ..... 131
Access levels | Output groups ..... 131
Access levels | Salto doors / door groups ..... 132
Access levels | Cencon locks / lock groups ..... 132
Access levels | Keys / Key groups ..... 132
Access levels | Integration options ..... 132
Custom fields ..... 133
Custom fields | General ..... 133
Custom fields | Drop down items ..... 133
Custom field tabs ..... 134
Custom field tabs | General ..... 134
Card template editor ..... 135
Card Template Editor Menus ..... 135
Card Template Editor Toolbar ..... 138
Events Menu ..... 139
Event search ..... 139
Running an Event Search ..... 139
Event filters ..... 140
Event filters | General ..... 140
Event filters | Event types ..... 140
Event filters | Records ..... 140
Alarms ..... 141
Alarms | General ..... 141
Actions ..... 143
Actions | General ..... 143

Email Field Variables ..... 145
Alarm priorities ..... 147
Alarm priorities | General ..... 147
Alarm routing ..... 148
Alarm routing | General ..... 148
Alarm routing | Workstation groups ..... 148
Workstations ..... 149
Workstations | General ..... 149
Workstation groups ..... 151
Workstation groups | General ..... 151
Workstation groups | Workstations ..... 151
Reports Menu ..... 152
Setting up Reports ..... 152
Reports | Setup | Event ..... 152
Reports | Setup | Muster ..... 155
Reports | Setup | Attendance ..... 157
Reports | Setup | User ..... 162
Reports | Setup | Shift type ..... 164
Setting up Regular Report Emails ..... 165
Setting up Regular Report File Exports ..... 165
Viewing Reports ..... 167
Running a Report ..... 167
Working with the Grid View ..... 167
Print Preview Window ..... 170
Central Station Report ..... 172
Operator Permission Report ..... 172
Monitoring Menu ..... 173
Status page view ..... 173
Status Page Interactions ..... 173
Alarms Status Page ..... 173
Floor plan view ..... 174
Floor Plan Sections ..... 174
Monitoring | Setup ..... 175
Floor plan editor ..... 175
Floor plan editor (batch) ..... 179
Add bulk floor plans ..... 180
Status page editor ..... 182

Status page editor (batch) ..... 183
Status lists ..... 184
Web links ..... 185
DVRs ..... 186
Cameras ..... 187
PTZ commands ..... 189
Intercoms ..... 190
Salto Menu ..... 191
Salto | Doors ..... 191
Salto | Doors | General ..... 191
Salto | Door groups ..... 194
Salto | Door groups | General ..... 194
Salto | Door groups | Doors ..... 194
Salto | Calendars ..... 195
Salto| Calendars | General ..... 195
Salto | Calendars | Dates ..... 195
Salto Log ..... 196
Manual Salto Door/Door Group Commands ..... 196
Cencon Menu ..... 197
Cencon lock groups ..... 197
Cencon lock groups | General ..... 197
Cencon transaction logs ..... 197
Programming Menu ..... 198
Doors ..... 198
Doors | General ..... 198
Doors | Outputs ..... 201
Doors | Function outputs ..... 203
Doors | Inputs ..... 204
Doors | Options ..... 206
Doors | Advanced options ..... 207
Doors | Alarm options ..... 209
Doors | Function codes ..... 210
Doors | Offline wireless lock settings ..... 210
Manual Door Commands ..... 211
Inputs ..... 213
Inputs | General ..... 213
Inputs | Areas and input types ..... 215

Inputs | Options ..... 215
Manual Input Commands ..... 216
Door types ..... 217
Door types | General ..... 217
Door types | Options ..... 219
Input types ..... 221
Input types | General ..... 221
Input types | Options (1) ..... 223
Input types | Options (2) ..... 225
Input types | Options (3) ..... 226
Input types | Options (4) ..... 227
Areas ..... 229
Areas | General ..... 229
Areas | Configuration ..... 229
Areas | Outputs ..... 232
Areas | Options (1) ..... 235
Areas | Options (2) ..... 238
Area Manual Commands ..... 240
Outputs ..... 242
Outputs | General ..... 242
Outputs | Options ..... 243
Manual Output Commands ..... 244
Trouble inputs ..... 245
Trouble inputs | General ..... 245
Trouble inputs | Areas and input types ..... 246
Trouble inputs | Options ..... 247
Elevator cars ..... 248
Elevator cars | General ..... 248
Elevator cars | Schedules and areas ..... 249
Manual Elevator Car (Floor) Commands ..... 250
Floors ..... 251
Floors | General ..... 251
Daylight savings ..... 252
Daylight savings | General ..... 252
Daylight savings | Options ..... 252
Phone numbers ..... 253
Phone numbers | General ..... 253

Services ..... 254
Setting up Reporting Services ..... 254
Services | Service Type ..... 254
Contact ID ..... 256
Serial printer ..... 259
SIA ..... 261
Automation and control ..... 263
Modbus ..... 265
C-Bus ..... 266
Report IP ..... 267
Intercom ..... 270
Link me ..... 272
VizIP ..... 273
Apartments ..... 274
Apartments | General ..... 274
Apartments | Options ..... 274
Apartments | Keypads ..... 276
Apartments | Inputs ..... 277
Apartments | Areas ..... 278
Apartments | Users ..... 279
Manual Apartment Commands ..... 281
Batch add apartments ..... 282
Groups Menu ..... 283
Door groups ..... 283
Door groups | General ..... 283
Area groups ..... 284
Area groups | General ..... 284
Keypad groups ..... 285
Keypad groups | General ..... 285
Menu groups ..... 286
Menu groups | General ..... 286
Menu groups | Options ..... 287
Output groups ..... 288
Output groups | General ..... 288
Elevator groups ..... 289
Elevator groups | General ..... 289
Floor groups ..... 290

Floor groups | General ..... 290
Expanders Menu ..... 291
Module Updates ..... 291
Virtual Modules ..... 291
Keypads ..... 292
Keypads | General ..... 292
Keypads | Configuration ..... 293
Keypads | Options 1 ..... 294
Keypads | Options 2 ..... 295
Manual Keypad Commands ..... 296
Analog expanders ..... 297
Analog expanders | General ..... 297
Analog expanders | Channel 1-4 ..... 297
Monitoring Power Supply Voltage and Current ..... 298
Input expanders ..... 300
Input expanders | General ..... 300
Output expanders ..... 302
Output expanders | General ..... 302
Reader expanders ..... 303
Reader Expanders | General ..... 303
Reader expanders | Reader 1/2 ..... 305
Reader expanders | Reader 1/2 options ..... 309
Reader expanders | Reader 1/2 PIMs ..... 310
Manual Reader Expander Commands ..... 311
Smart readers ..... 312
Smart readers | General ..... 312
Smart readers | Reader ..... 313
Visitor Menu ..... 316
Templates ..... 316
Templates | General ..... 316
Templates | Pages ..... 317
Templates | Email ..... 317
Templates | Display ..... 317
Pages ..... 318
Pages | General ..... 318
Pages | Custom fields ..... 318
Workstations ..... 319

Workstations | General ..... 319
Cards ..... 320
Cards | General ..... 320
Images ..... 321
Images | General ..... 321
Automation Menu ..... 322
Automation ..... 322
Automation | General ..... 322
Automation | Options ..... 323
Programmable functions ..... 324
Starting and Stopping Programmable Functions ..... 324
Programmable functions | General ..... 324
Logic control ..... 326
Area control ..... 328
Roof top heat pack ..... 329
Floor temping ..... 333
Value compare ..... 335
Ripple output ..... 336
Door control ..... 337
Virtual door ..... 339
Input follows output ..... 341
Elevator control ..... 342
Register counter ..... 343
Average ..... 344
Variable output compare ..... 345
Data values ..... 346
Data values | General ..... 346
Variables ..... 347
Variables | General ..... 347
Variables | Log ..... 347
About Menu ..... 348
Help ..... 348
License ..... 348
License | Information ..... 348
License | Site details ..... 348
Registering and Updating Your Software License ..... 348
Viewing Version Information ..... 349

# Protege GX Operator Reference

Welcome to the Protege GX Operator Reference, documentation designed to give you the information you need when programming and maintaining Protege GX. This PDF manual provides a full reference for the Protege GX system, and can be printed or viewed on a PC or tablet. The documentation is also available as a help system within Protege GX itself.

There are multiple ways to use this documentation:

- **Introduction to Protege GX**: The first two sections provide information on how to navigate the Protege GX user interface (see next page), as well as general programming and troubleshooting tips (see page 23).
- **Programming Page Reference**: The second part of the documentation includes full reference information for every page in the software. You can use the table of contents (see page 3) or the **Bookmarks** pane of your PDF viewer to navigate through the documentation, which is organized in the same structure as the main menu of Protege GX.

  For example, if you need to find information about the **Options** tab in the doors programming, expand the Programming menu and locate Doors | Options.
- **Programming Field Reference**: Almost every field in the software is described in this documentation. To quickly find information about a particular field in the software, press Control + F and type the name of the field into the search bar, then press Enter.

  For example, you might search for **Always check unlock schedule** to learn about what that option does.

This documentation is intended for operators who will be using and programming the software. For instructions on installing the Protege GX software please refer to the separate Protege GX Installation Manual. The Protege GX End User Guide provides an introduction to key features for end users such as building managers, HR personnel and security guards.

Please consider the environment before printing this documentation.

# 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.

## 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.

## 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.

### Supported Screen Resolutions

The Protege GX user interface supports the following standard screen resolutions:

- 1280 x 1024
- 1400 x 1050
- 1600 x 1200
- 1680 x 1050
- 1920 x 1080

Selecting alternative screen resolutions may produce unexpected display results.

## Changing the Operator Password

1. To change your operator password, click the **Change password** button from the Home page. This opens the **Change password** window.
2. Enter the existing operator password in the **Old password** field.
3. Enter a **New password**, then repeat the same password in the **Confirm new password** field.

   It is recommended that you create a very secure password, especially for the admin operator. For more information, see Creating a Secure Password (below).
4. Click **OK**.

To reset another operator's password, navigate to **Global | Operators** and click the ellipsis **[...]** button beside the **Password** field.

## 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.

# 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 | Standard download server systems only.<br>Select whether you are programming in local (this controller only) or global (cross controller) mode. Only available for doors and programmable functions. |
| Cross controller group | Enterprise download server systems only.<br>Displays which cross controller group this record belongs to. The record can only use inputs, outputs and other resources from the same cross controller group. Enable the **Local** checkbox to restrict programming to only resources on the same controller.<br>This is not displayed when the host controller is standalone and does not belong to a cross controller group. |
| Controller | Display only records associated with one controller. |
| 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 Using the Find Tool (next page). |
| 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. |

| Button | Function |
|---|---|
| Copy | Copy the configuration from a specified record onto the current record.<br>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 Opening Multiple Windows (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.

# Reports Window

The reports window is displayed whenever you run a report (such as a user report or event report) or a search (user search or event search). The report grid view has a variety of functions for sorting, grouping and filtering event data, ensuring you can view and export exactly the information you need.

For more information, see Viewing Reports (page 167).

# Programming Tips and Troubleshooting

This section contains useful programming tips, information on where to find additional resources, and troubleshooting information.

## Additional Resources

There are a number of additional resources available to you when using the Protege GX system, whether you are just learning the system or looking for advanced programming tips.

- **Application notes** describe specific applications of the system, such as how to program a particular feature or integration. They typically include step-by-step programming instructions.

  This documentation includes references to application notes which contain more detailed information about particular features.

  Application notes are available on the ICT website: www.ict.co/Application-Notes.
- The **ICT Knowledge Base** is designed to answer the most common technical questions that operators have about Protege systems. It provides troubleshooting and programming tips to help you resolve issues.

  Visit the ICT Knowledge Base here.
- **Videos** on the ICTNZ YouTube Channel provide visual and audible demonstrations. These include software and hardware tutorials, tips for techs, solution showcases and free webinars. New videos are added frequently.
- **Training** is available both in person with our skilled technical trainers and online. Online modules can be reviewed at any time to refresh your memory. Contact ICT for more information and to register for courses.
- If all else fails you can contact the **ICT Technical Support** team by email or phone, or log a support ticket. See www.ict.co/Contact-Us for the best ways to get in touch.

## Naming Conventions

Before programming a site it is important to define a naming convention that will be used throughout the system. The more consistent the naming convention the easier it will be to maintain the site, as records can always be identified easily and accurately.

Descriptive record names are helpful for searching for specific records using the find tool (see page 21). It is recommended that you give similar records a common naming element so you can find them easily.

A good naming convention is also important to help installers and technicians quickly and accurately identify physical devices, whether they are using the software or a keypad on site. A useful name contains information about the device's physical location, network address and function.

There are three naming fields available for devices:

- **Name**: This is the name which appears throughout the English version of the Protege GX software, and in event logs. It should identify the key features of the record such as its function within the system, its module address and the controller it is connected to.
- **Name (second language)**: The name which appears in the second language version of the software and event logs. If the site does not use a second language, this field can be used for additional information about the record.
- **Keypad display name**: The name which is displayed on the keypad (for areas, doors, inputs etc.) and in reports to an IP monitoring station. This name should be recognizable to end users. For example, if the end user is arming an area and there are some inputs open, they should be able to easily identify which inputs they need to check on before leaving the premises.

  The keypad can only display the first 16 characters of the name.

### Example

Below is an example of a naming convention for inputs. These are inputs 1-4 connected to reader expander 1 on controller 1:

| Name | Keypad Display Name |
|---|---|
| CTRL1 Office Door Reed RD1.1 | Office Door |
| CTRL1 Office Door REX RD1.2 | Office Door REX |
| CTRL1 Office Door Bond RD1.3 | Office Door Lock |
| CTRL1 Office PIR RD1.4 | Office PIR |

## Cross Controller Operations

Normally in the Protege GX system each controller operates independently of other controllers, with its own network of expanders, inputs and outputs. With cross controller operations a number of controllers communicate with each other, enabling them to act as a system and share hardware resources. For example, this allows you to:

- Assign inputs from two different controllers to a single area
- Create output groups that span multiple sections of the building
- Lock down all doors on site from a single panic button
- Use one reporting service for alarms from multiple controllers

The method for programming cross controller operations differs depending on the type of download server used by your system.

- **Standard Protege GX Download Server**: Create programming links between controllers to connect them together. In the background, the system will create an implicit cross controller group containing the linked controllers and initiate cross controller operations. For example, assign an input from one controller to a door on another controller to add them both to a cross controller group.
- **Protege GX Enterprise Download Server**: Create explicit cross controller groups in **Sites | Cross controller groups**. Once the cross controller groups have been created, you can assign inputs, outputs and other records freely among the controllers in the group. The user interface will prevent you from linking controllers that do not belong to the same cross controller group. For more information, see Cross controller groups (page 97).

For complete information about this feature, see Application Note 180: Protege GX Cross Controller Operations.

You can link up to 64 controllers in a cross controller group. Any controllers beyond 64 will not be able to communicate with each other. Protege GX will generate a health status message when a cross controller group exceeds 64 controllers.

# Guide to Common Event Types

Protege GX features extensive event reporting, with hundreds of unique descriptions for different occurrences. As well as providing data for reports and audits, understanding Protege GX events is very useful for troubleshooting. This section provides a guide for some common event types.

## User Access Events

When a user is denied access to enter or exit a door, it is important to know why this has occurred. The event log is a valuable resource for determining what is restricting the user's access.

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

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

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

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

## Reporting Events

When an area is armed or disarmed or an input is open, closed, bypassed or tampered, the system typically logs a reporting event alongside the normal events. These events correspond to Contact ID reporting codes, indicating the information that would be sent to the monitoring station using standard Contact ID reporting.

The relevant events are:

- Report In <AREA_NAME> Using Input <ZONE_NAME> Special Code [<CUSTOM_REPORT_CODE>] Flags [<REPORT_FLAGS_A>]
- Report In <AREA_NAME> Using Trouble Input <TROUBLE_ZONE_NAME> Special Code [<CUSTOM_REPORT_CODE>] Flags [<REPORT_FLAGS_A>]
- Report In <AREA_NAME> User <USER_NAME> Report <AREA_REPORT_TYPE> Flags [<REPORT_FLAGS_A>]

The definitions of the different parameters in these events are as follows:

| Parameter | Definition/Notes |
|---|---|
| Report in <AREA_NAME> | The name of the area where the event occurred.<br>• For input / trouble input events, this is the area that the input is programmed in.<br>• For area events, this is the area that was armed/disarmed. |

| Parameter | Definition/Notes |
|---|---|
| <ZONE_NAME> or <TROUBLE_ZONE_NAME> | The name of the input or trouble input which triggered the event. |
| <USER_NAME> | The name of the user who armed/disarmed the area.<br>• If the area was not armed/disarmed by a user, the event is attributed to SYSTEM USER. This refers to Protege GX operators, programmable functions, schedules and other methods of arming/disarming. |
| Special Code [<CUSTOM_REPORT_CODE>] | Based on the Contact ID event code for inputs, which describes which kind of input is causing the event.<br>• The event code can be set as the **Custom reporting code** in **Programming \| Input types \| General**. By default this is set to None.<br>• For example, for a panic button the **Custom reporting code** might be set to 12 - Panic alarm.<br>• Trouble inputs use preset event codes based on the type of trouble condition they report. These are outlined in the relevant module installation manuals. |
| Report <AREA_REPORT_TYPE> | Based on the Contact ID event code for areas, which describes the method or type of arming/disarming. For example:<br>• User indicates that the area was disarmed locally by a user.<br>• Remote indicates that the area was disarmed remotely by the software or an automatic function.<br>• Partial indicates that the area was force armed.<br>• Stay indicates that the area was stay armed. |
| Flags [<REPORT_FLAGS_A>] | The <REPORT_FLAGS_A> parameter is made up of two terms.<br>• The first term is based on the Contact ID event qualifier. This is either:<br>- [NEW] for new incidents (e.g. input opens)<br>- [RESTORE] for the end of the incident (e.g. input closes).<br>• The second term is based on the Contact ID event code and describes what has happened to the input. The options are:<br>- [ALARM] for input alarms and restores.<br>- [TAMPER] for input tampers/shorts and restores.<br>- [Bypass] for input bypasses and restores.<br>• For example, when an input is tampered it will display the flags [NEW+TAMPER]. When the tamper is restored it will display [RESTORE+TAMPER].<br>• Area reports always display the flags [NEW+ALARM] |

# Database Backup and Restore

It is recommended that you create backups of both Protege GX databases regularly. This ensures programming and events are not lost when a database is corrupted or destroyed. You can set up regular backups of both databases within Protege GX, or back up manually within Microsoft SQL Server Management Studio (SSMS). In addition, the events database can perform differential backups, allowing it to regularly purge old events so that the database does not become full.

The database restore process must be carried out in SSMS, with the Protege GX services stopped. Restoring a database allows you to recover lost programming and events when necessary.

Because the Protege GX server and databases are completely separate, any database can be restored to any server installation. This allows you to restore databases to a testing server, create preprogrammed databases that contain default configuration, and review past events in a separate installation.

## Database Compatibility

When you back up or restore a database, you should take note of the **database version**. The software version number (see **About | Version**) indicates the database version as indicated below:

| 4 | 3 | 264 | 39 |
|---|---|---|---|
| **Major Release** | **Minor Release** | **Database Version** | **Software Build** |

Backups made by the Protege GX software always include the database version number in the filename. This is a good practice to follow when making your own backups.

When restoring a database, you must ensure that the database version of the backup file is compatible with that of the software, as outlined below:

| Database Version | | Software Version | |
|---|---|---|---|
| 265 | > | 264 | ✖ |
| 264 | = | 264 | ✔ |
| 264 | < | 265 | ✔ |

- If the database version is newer than the software version it is not possible to restore the database. **Upgrade the software before restoring.**
- If the version numbers match the restore should be successful.
- If the database version is older than the software version the database can be restored but must be upgraded to match the software version. **Restore the database, then uninstall and reinstall the server software to upgrade the database version.**

  Do not use the **Repair** option in the installer to upgrade the database, as the data service will fail to start. Always uninstall and reinstall Protege GX.

If the database version and software version do not match, **the data service will not start**.

## Creating Database Backups

There are multiple methods of backing up the Protege GX databases, both within the Protege GX software and in SQL Server Management Studio (SSMS). Within the software, you can also configure regular backups of the main database, and regular differential backups and purges of the events database.

## Taking Backups in Protege GX

In Protege GX, navigate to **Global | Global settings**. The following options are available for backing up the databases.

When setting a backup path, ensure that the selected directory already exists on the server machine. Do not select a directory that denies SQL Server write access, such as Program Files, Program Data, Users, Windows, etc.

**To back up the main database once:**

1. Enter a **Backup path**.
2. Click **Backup now**.

The database version number will be appended to the filename.

**To back up the main database every night at midnight:**

1. Enter a **Backup path**.
2. Enable **Backup main database every night**.
3. You may also enable **Append day of week to backup file name**.

New backup files will overwrite existing backups with the same name. If more than one week of stored backups is required, consider changing the backup path regularly.

**To back up the events database once:**

1. Set the **Select a backup option** field to Local Path, Network Path or FTP.
2. Enter the **Events DB backup path**. If you selected FTP above, you must enter the relevant FTP settings such as **IP address** and **Port number**.
3. Click **Backup now**.

**To create a regular differential backup of the events database and purge old events:**

1. Set the **Select a backup option** field to Local Path, Network Path or FTP.
2. Enter the **Events DB backup path**. If you selected FTP above, you must enter the relevant FTP settings such as **IP address** and **Port number**.
3. Enter the **Purge events older than** and **Purge start time** details to determine how long events will be kept in the database before they are purged.
4. Enable **Generate differential events backup**.

For more information, see Application Note 279: Creating and Restoring Differential Backups in Protege GX.

## Taking Backups in SSMS

The following procedure allows you to take a backup of either database in SQL Server Management Studio (SSMS). The instructions may differ slightly depending on the version of SSMS you are using.

1. Open SSMS and connect to the Protege GX server.
2. Expand the **Databases** node. Right click the ProtegeGX or ProtegeGXEvents database and select **Tasks > Back Up...**.
3. If a backup has been created previously, the file will be displayed in the **Destination** field. To use this file click the **Media Options** tab and select whether you will append the current backup to the existing file or overwrite the existing file.

   To back up to a different file click **Remove**. Then click **Add...** to enter the name and location of the new backup file. Click **OK**.

The backup file must be in the .bak format. It is recommended that you add the database version number to the filename.

4. Click **OK** to perform the backup.

## Restoring Database Backups

This section demonstrates how to restore programming backups using SQL Server Management Studio (SSMS).

These instructions assume you are using the Simple database recovery model to restore a full backup. To restore to a specific point in time with the Full recovery model, see the Microsoft Help.

Before you restore a database, back up your current database so you can return to a known point if there are any issues.

1. If you are restoring a database with Transparent Data Encryption to a different server, you first need to load the encryption certificate onto the new server.
   See Backing up and Restoring with Transparent Data Encryption for instructions.
2. Check the database version you are restoring against the current version of the software (**About | Version**).
   If the database version is higher than the third number of the software version, do not proceed (see page 29).
3. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
4. Locate the Protege GX Update Service. Right click on the service and click **Stop**. This will also stop the other Protege GX services.
5. Open SSMS and connect to the Protege GX instance.
6. Expand the **Databases** node. Right click the ProtegeGX or ProtegeGXEvents database and select **Tasks > Restore > Database...**.
7. Set the **Source** to **Device**, then click the ellipsis **[...]** button.
8. Click **Add** to browse to the backup file (.bak) that you will restore. Click **OK**.
9. The **Restore Plan** section will show the backup set(s) that are available to restore. If there is more than one, use the backup date to determine which one should be restored, then check the **Restore** checkbox beside the selected backup set.
10. In the **Options** tab, enable **Overwrite the existing database**.
11. Click **OK** to start the restore process.
12. If the database version you restored is earlier than the current version of the software, you must **uninstall and reinstall** Protege GX to upgrade the database.
13. In the **Services** snap-in, right click on the Protege GX data service and click **Start**. If the data service starts, the database restoration was successful.

    Starting the data service also starts the event service and update service; however, the download service must be started manually. It is recommended that you check the configuration before starting the download service, as this will begin downloading programming to the controllers.

## Backing up and Restoring with Transparent Data Encryption

When a database has Transparent Data Encryption (TDE) enabled, any backups from that database are also encrypted. If you need to restore the database to another server you must first create a Database Master Key (DMK) and add the backed up certificate to the new server.

Before you begin, you will need the certificate, private key and the password used to encrypt the private key. If you do not have backups of these you can export them from the original server.

1. On the original server, click **New Query** and enter the following query:

```
BACKUP CERTIFICATE TDECertificate TO FILE = 'c:\storedcerts\TDE
Certificate'
    WITH PRIVATE KEY ( FILE = 'c:\storedkeys\TDE Key' ,
    ENCRYPTION BY PASSWORD = '<UseAStrongPasswordHere>' );
GO
```

2. Click **Execute**. SQL Server will export the certificate and private key files to the specified locations.

> You must back up the certificate, private key and the password used to encrypt the private key in a secure location. If these are lost, it will not be possible to restore database backups to another server.

3. Transfer the files to the new server.

You will then need to create a Database Master Key and certificate on the new server.

1. Open SQL Server Management Studio (SSMS) and connect to the Protege GX instance as an admin user.
2. Click **New Query**.
3. Enter the following query:

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
GO
CREATE CERTIFICATE TDECertificate
    FROM FILE = 'c:\storedcerts\TDE Certificate.cer'
    WITH PRIVATE KEY (FILE = 'c:\storedkeys\TDE Key.pvk',
    DECRYPTION BY PASSWORD = '<EnterPrivateKeyPasswordHere>');
GO
```

4. Click **Execute**. The certificate will be uploaded to the server and encrypted using the Database Master Key.
5. Restore the database backups as normal, following the instructions in Restoring Database Backups.

# Backing up and Restoring with Encrypted Columns

Some features in Protege GX use encrypted database columns to keep your data secure:

- PIN encryption
- ICT wireless locking

We recommend that you back up the Data Service Encryption Certificate to ensure that it is not lost if the Protege GX server goes down. In addition, when you restore the Protege GX database to another server or secondary download server you must import the certificate to allow the new server to access the encrypted columns.

## Backing up the Certificate

The certificate is created on the machine where the data service is installed, which may not be the same machine as the SQL server installation.

1. To open the Certificate Manager tool as an administrator, press the **Windows + R** keys, then type **certlm.msc** into the search bar and press **Control + Shift + Enter**.
2. Under **Certificates - Local Computer**, open **Personal**, then **Certificates**.
3. In the window displaying the certificates, scroll across to the **Friendly Name** column and locate the certificate called Data Service Encryption Certificate.

4. Right click the certificate and select **All Tasks > Export**.
5. The **Certificate Export Wizard** will open. Click **Next**.
6. Select **Yes, export the private key**, then click **Next**.

   The private key is the critical component in decryption. If you do not export the private key, when the certificate is imported it will not be able to decrypt the encrypted data.

7. Select the following **Export File Format** options:
   - **Include all certificates in the certification path if possible**
   - **Enable certificate privacy**

   The **Delete the private key if the export is successful** option **must be disabled**.

   Then click **Next**.
8. On the **Security** page, select **Password**. Enter and confirm a strong password.

   Save this password to a password manager or other secure location.

9. Set **Encryption** to AES256-SHA256, then click **Next**.
10. Specify an export **File name** and path, then click **Next**.
11. Click **Finish** to complete the certificate export.

When the export is complete, confirm that the certificate backup .pfx file has been exported to the file path as specified. The file should be stored securely in a separate location to ensure that it is available if required.

You must back up the certificate and the password used to encrypt the private key in a secure location. If these are lost, it will not be possible to restore database backups to another server.

## Restoring the Certificate

1. Ensure that the .pfx backup file is accessible from the local PC.
2. Stop all Protege GX services before initiating the import.
3. To open the Certificate Manager tool as an administrator, press the **Windows + R** keys, then type **certlm.msc** into the search bar and press **Control + Shift + Enter**.
4. The tool directory will display Certificates - Local Computer.
5. Open the **Personal** folder.
6. Right click the **Certificates** sub-folder and navigate to **All Tasks**, then select **Import**.
7. The **Certificate Import Wizard** will open. Click **Next**.
8. Click **Browse...** and locate the .pfx backup file to import, then click **Next**.

   You will need to change the file type dropdown to Personal Information Exchange (*.pfx;*.p12).

9. Enter the **Password** that was created during the export process.
10. Import Options:
    - **Mark this key as exportable. This will allow you to back up or transport your keys at a later time**.
      - This option must be selected if you want to be able to export/backup the private key with this certificate in the future. This option is slightly less secure.
      - The key is more secure if this option is not selected, however you will not be able to export the private key with the certificate in the future if you lose your current .pfx backup file.
    - Ensure that **Include all extended properties** is selected.
11. Click **Next**.
12. Ensure the **Certificate store** is set to Personal, then click **Next**.
13. Click **Finish** to complete the certificate import.

14. Close the Certificate Manager tool.
15. Restore the Protege GX database in SQL Server as normal.
16. Restart the Protege GX services.

# Viewing Controller Health Status

The **Get health status** function provides details of the overall status of the system and can be useful in identifying any problem areas that need to be addressed.

## To View Health Status:

1. Navigate to **Sites | Controllers**.
2. Right click on the controller and choose **Get health status**.
3. The **Controller status** window appears, indicating any areas that need addressing.

   If the health status request fails, there may be an issue with the controller's connection to the server. See further below.

# Troubleshooting Controller Connectivity

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

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

## Communication Requirements

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

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

## Check that the Services are Running

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

1. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
2. Scroll down to the Protege GX services. Ensure that the following services are running:
   - Protege GX Data Service
   - Protege GX Download Service
   - Protege GX Event Service
   - Protege GX Update Service
3. If any service is not running, right click on it and click **Start**.

If any services will not start there may be another issue with your installation. For example, the database version may be incompatible (see page 39).

## Confirm Controller IP Address

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

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

   You may be presented with a certificate security warning on connection.

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

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

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

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

## Setting the IP Address from a Keypad

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

1. Connect the keypad to the module network.
2. Log in to the keypad using any valid installer code. The default installer code is 000000.
   If the default code has been overridden and you do not know the new codes you will need to default the controller (see Defaulting the Controller in this document) to reset the code.

   Note that this will erase **all** existing programming as well as setting up the default installer code.
3. Once logged in select **Menu 4** (Install Menu) then **Menu 2** (IP Menu) and view or edit the IP address, network mask, and gateway as required.

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

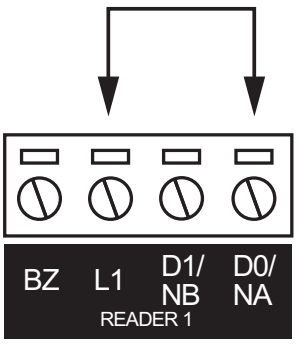
## Defaulting the IP Address

If the currently configured IP address is unknown it can be temporarily set to 192.168.111.222 so that you can connect to the web interface to view and/or change it. This will also temporarily disable HTTPS security, which may help resolve some connection issues.

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

### Defaulting a 2 Door Controller's IP Address

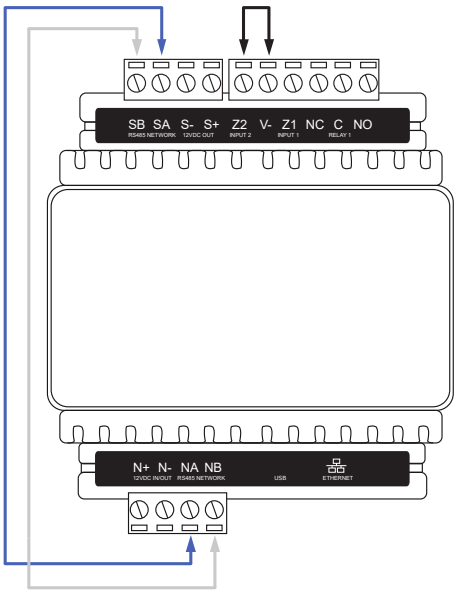
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.




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

## Defaulting a 1 Door Controller's IP Address

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 2** to ground.




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

## Accessing the Controller

6. When the controller starts up it will use the following temporary settings:
   - **IP Address**: 192.168.111.222
   - **Subnet Mask**: 255.255.255.0
   - **Gateway**: 192.168.111.254
   - **DHCP**: Disabled
   - **Use HTTPS**: Disabled
7. Connect to the controller by entering http://192.168.111.222 into the address bar of your web browser, and view or change the IP address and other network settings as required.

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

# Confirm Controller Serial Number

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

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

## Duplicate IP Address or Serial Number

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

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

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

## Confirm the Event Server is Functioning

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

1. In Protege GX, navigate to **Sites | Controllers | General** and expand the **Diagnostic windows** section.
2. Select **Open event server diagnostic window**. You should see a message that reads 'Listening on Port : 22000'.

   The default event server port is **22000**, but this can be changed in **Global | Event servers**.
3. If the event server diagnostic window shows messages about an unknown serial number, events are being received from a controller with the serial number listed in the message. This also means the event server is accepting incoming events.
4. In the controller web interface, ensure that the **Event Port** matches the port set in Protege GX.
5. If you change the event port you must **save** and **restart the controller** using the icons in the upper right before your changes will take effect.

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

1. Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
2. Locate the Protege GX Event Service. Right click on the service and select **Restart**.

### Confirm Event Server IP Address

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

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

   For more complex networks it may be preferable to open a command prompt on a machine the controller is directly connected to and use the `ping` command to ascertain the external IP address of the server.
3. In the controller web interface, on the **System Settings** page, check that **Event Server 1** has the correct IP address. Paste in the address located above if it does not match.

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

## Confirm Ports

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

1. In Protege GX, navigate to **Sites | Controllers | General** and check these values:
   - **Download port** (default 21000)
   - **Control and status request port** (default 21001)
2. In the controller web interface, on the **System Settings** page, ensure that the **Download Port** and **Control Port** match those defined in the software.
3. If you have changed any settings on the controller, save your changes and restart the controller for the changes to take effect.

## Check Computer Name

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

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

1. On the server computer, open **Control Panel > All Control Panel Items > System** to view computer information.
2. Copy the **Computer Name**.
3. In Protege GX, navigate to **Global | Download server** and check that the **Computer name** matches the name of the server machine. If not, paste in the name copied earlier.
4. Navigate to **Global | Event server** and again check and correct the **Computer name**.
5. If you have changed the computer name for either server, you must restart the corresponding service.
   Open **Services** as an administrator:
   - Press the **Windows + R** keys.
   - Type **services.msc** into the search bar.
   - Press **Control + Shift + Enter**.
6. Locate the Protege GX services. Right click on the download service and/or event service and click **Restart**.

## Repair Database Compatibility

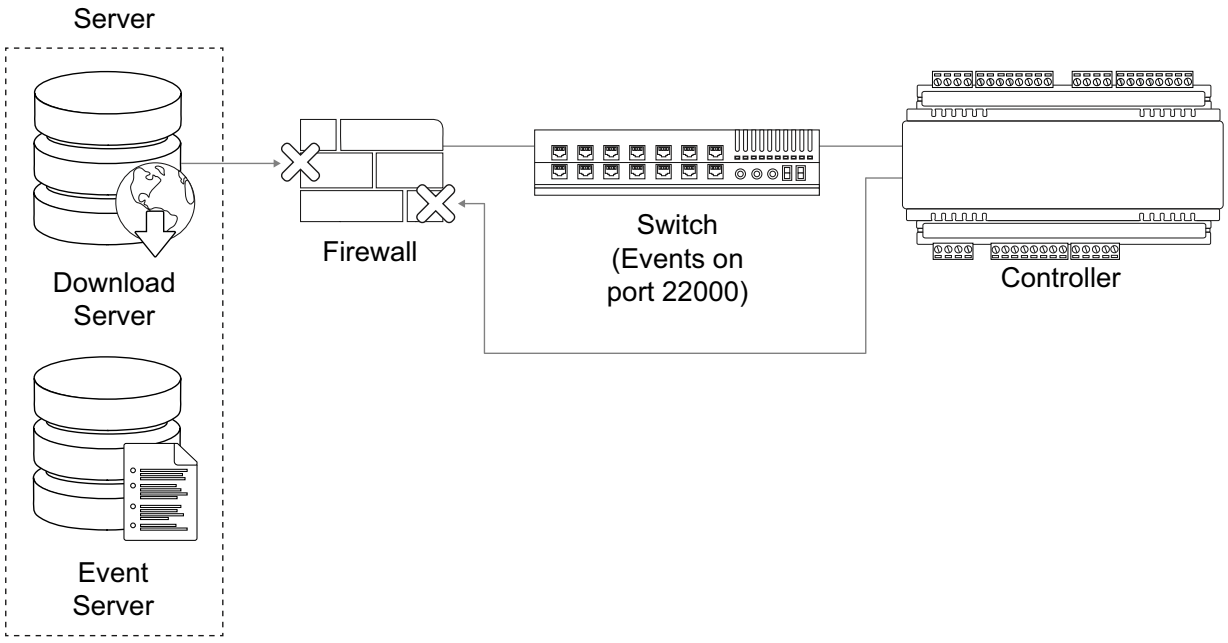
If you have restored a database from an older version of Protege GX, there may be a mismatch between the software and database versions. In this case the Protege GX Data Service will fail to start, the download and event server diagnostic windows will both remain blank, and no downloads will be passed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

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

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

## Windows Firewall

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




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

   Check whether this resolves the issue. If so, you can turn the Firewall back on and allow the Protege GX services through the Firewall.
3. Click the **Allow an app or feature through Windows Defender Firewall** link on the left of the screen.

   Third-party antivirus or firewall software may prevent modification of Windows Firewall rules. If this is the case, refer to the third-party manufacturer for details on allowing programs through the firewall.
4. Select **Allow another app...** to add a program as an exception.
5. Click **Browse...**, then navigate to the Protege GX installation directory.

   The default installation directory is C:\Program Files (x86)\Integrated Control Technology\Protege GX.
6. Select (double click or select and **Open**) the executable that you want to allow, then click **Add**.

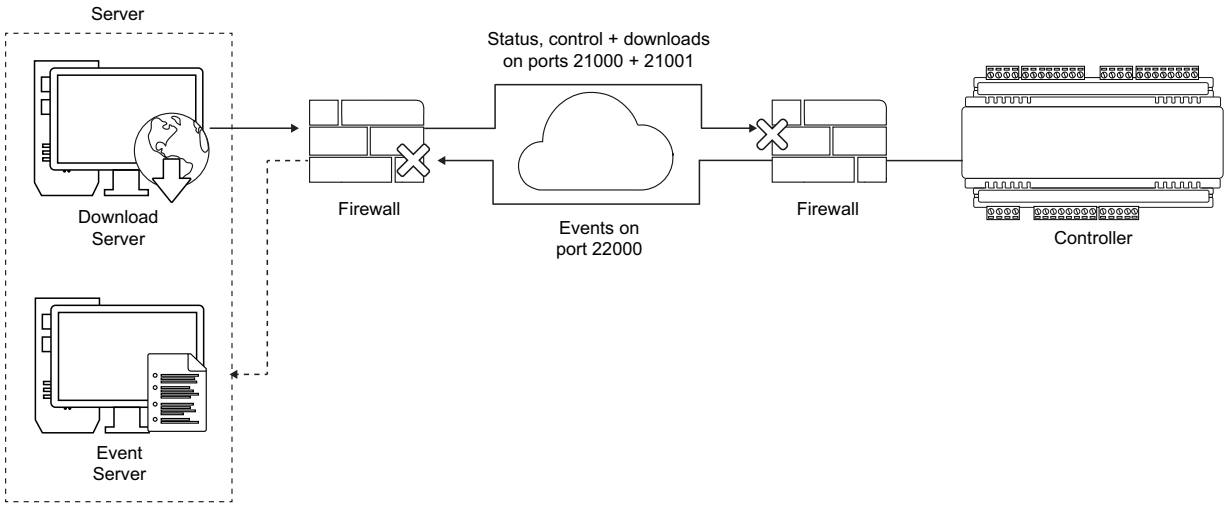
   Add the following Protege GX executables, one by one:
   - GXSV.exe
   - GXSV2.exe
   - GXSV3.exe
   - GXPI.exe
   - GXEvtSvr.exe
   - GXDVR1.exe
   - GXDVR2.exe

   This allows the necessary Protege GX services access through the Windows firewall.

   The above process will only allow access through your primary network connection. If you have multiple networks connected you will need to manually allow access (tick the checkbox in the network column) for each additional network that the Protege GX executable requires access through.

## Multiple Firewalls

On corporate networks there can be multiple firewalls.

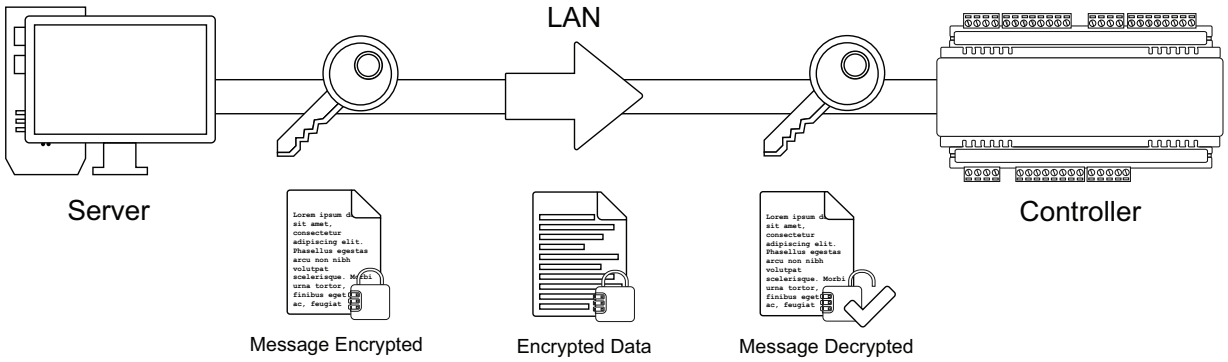



To ensure these are configured correctly, provide the Protege GX Network Administrators Guide to the appropriate IT staff member. This document is included in the software installation pack.

# Encryption

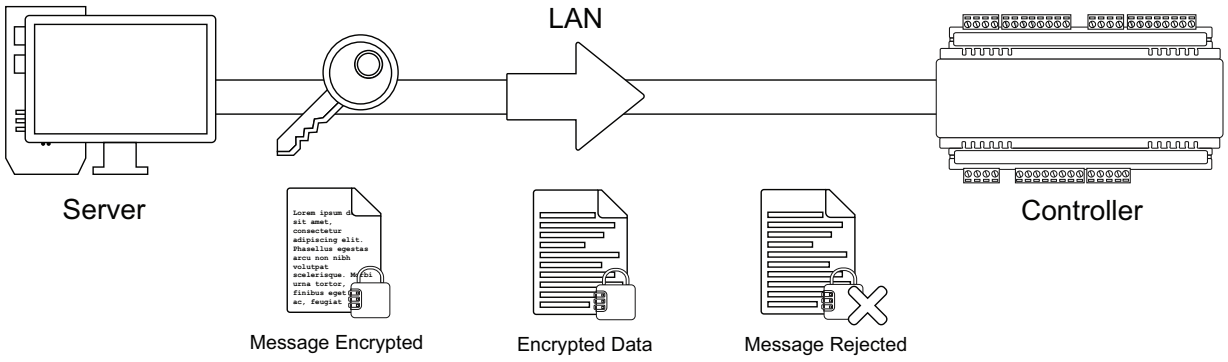
## Both Server and Controller Encryption Enabled

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



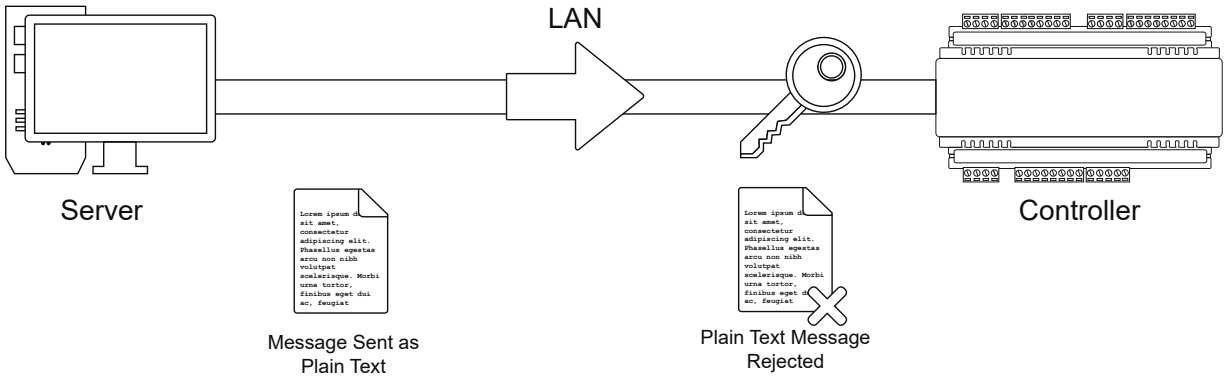

## Server Enabled, Controller Disabled

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



## Server Disabled, Controller Enabled

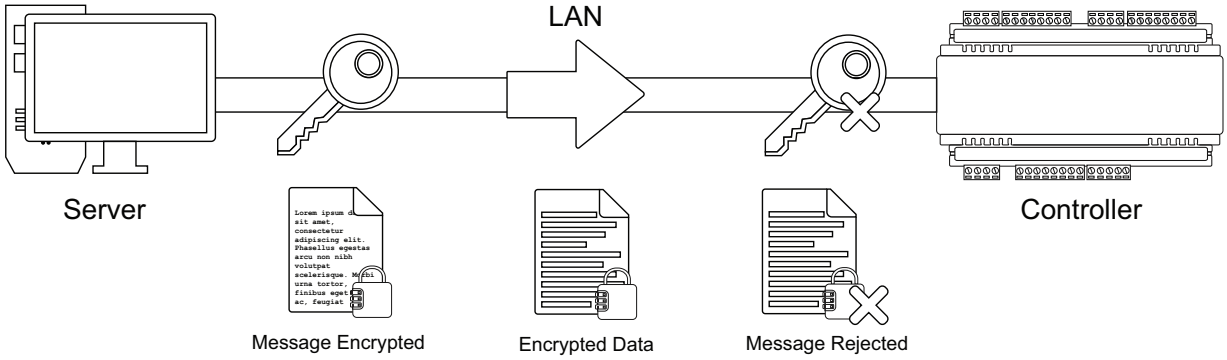
If the sender loses the key the message is sent in plain text. The receiver, expecting to receive encrypted events, will also reject the message as it may be of a malicious nature.




## Server and Controller with Different Encryption Keys

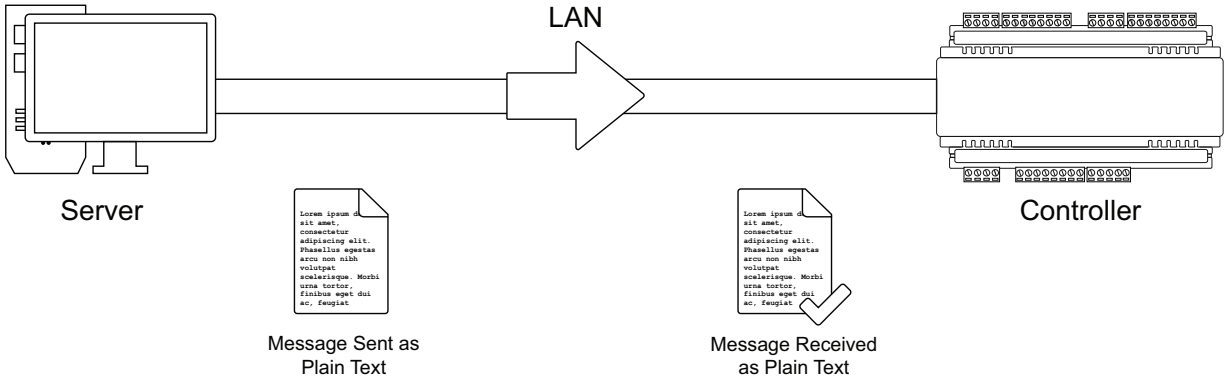
If the sender and receiver have different keys the message cannot be decrypted by the receiver. This also results in the receiver rejecting incoming messages.

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




## Both Server and Controller Encryption Disabled

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



# Disabling Encryption

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

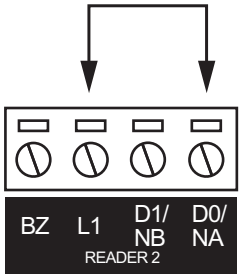
If you are unsure of the state of encryption of either the server or controller, disable encryption at the server, then default the controller. This ensures that neither is encrypted and rules this out as a cause of communications problems. Encryption should then be re-enabled once communications are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

## Disabling Encryption at the Server

If the controller is defaulted, encryption must be disabled at the server before communications can be established. Navigate to **Sites | Controllers | Configuration** and click **Disable controller encryption**. The software warns you prior to disabling encryption.

## Defaulting a Two Door Controller

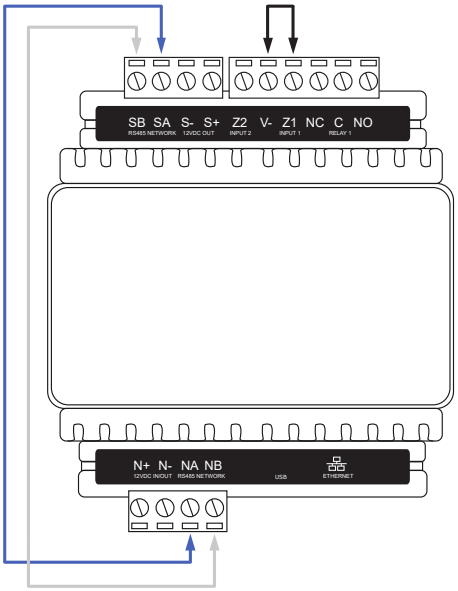
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.




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

## Defaulting a One Door Controller

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 1** to ground.




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

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

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

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

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

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

- All encryption keys used for secure sessions and pairing are deleted. This includes:
  - OSDP secure channel encryption keys for the controller **and** connected reader expanders
  - Protege wireless lock encryption keys
  - Pairing with Protege GX extended services
  - Pairing with Protege X
- All operator records are removed and the admin operator must be recreated.
- All other programming is removed.

## After Defaulting a Controller

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

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

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

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

3. Reset the controller's IP address to its previous value.

4. Reconfigure any additional network settings.
5. Reinstall previously installed custom HTTPS certificates.
6. If you were using OSDP secure channel, put **all** OSDP card readers connected to the controller **and** its reader expanders into installation mode. Initiate installation mode on the controller and all connected reader expanders to re-establish the secure channel.

## Telnet

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

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

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

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

# Global Menu

Settings that apply to the operation of the entire Protege GX system are grouped under the **Global** menu for easy access.

## Home

The Home page is displayed when you first log in and allows you to view operator details and change your operator password.

### Operator details

- **Logged on as**: Displays the name of the operator currently logged on.
- **Logged on at**: Displays the date and time you logged on.

### Options

- **Current site**: Displays the site which is currently being viewed. Records associated with this site will be displayed by default on programming pages and in the system navigator.
- **Display theme**: Choose between two display themes for the Protege GX interface: Light (white background, dark gray text) and Dark (dark gray background, light text). The display theme is saved for each individual operator on each workstation.
- **Change display color**: Choose which color theme will be displayed for menus, headings and other UI elements. The display color is saved for each individual operator on each workstation.
- **Log out**: Closes the Protege GX session, logging you out and returning you to the logon screen.
- **Change password**: Opens a window enabling you to change your operator password.

# Global settings

The global settings page is used to configure settings that apply to the entire Protege GX system.

## Global settings | General

### Main database

- **Main database version**: Version number of the current database (read only).
- **Save field changes to audit log**: This is a legacy option that has no effect.
- **User display name auto format**: Determines the default Protege GX display name for new user records. When you enter a new user's first and last names, the **Name** field will be filled automatically based on the format selected here. The options are:
  - **Do not format display name**
  - **Short format** (first initial, last name)
  - **Reverse short format** (last name, first initial)
  - **Long format** (first name, last name)
  - **Reverse long format** (last name, first name)

  This field only applies to new users created through the **Users | Users** programming. It does not affect the display names of existing users. This setting does not apply to users created through the web client, as the web client will always provide the display name in long format by default.
- **Encrypt user PINs**: Enable this option to permanently encrypt user PIN codes in the Protege GX database. This has the following effects:
  - Operators can no longer view user PINs.
  - User PINs can only be generated randomly (no manual entry).
  - Randomly generated PINs are single-use. When the user next logs in to a keypad they will be prompted to change their PIN.

  **Warning**: PIN encryption is permanent and can only be reversed by restoring a previous database backup.

  For more information, see Application Note 306: User PIN Encryption and Advanced PIN Management in Protege GX.

### Event database

- **Purge events older than**: Select the maximum length of time that events will be kept in the events database before they are deleted (purged). The default is 1 year, but busier sites may require the database to be purged more frequently to ensure there is always storage available for new events.
- **Purge start time**: Determines the time each day when old events will be deleted (purged) from the database.
- **Save operator events to event database**: When this option is enabled an event will be created every time a record is added, modified or deleted by an operator.

  This option is enabled by default but can be disabled to reduce the number of events being saved to the events database.
- **Save failed operator login events to event database**: When this option is enabled an event will be created every time there is a failed attempt to log in to the software. This allows you to detect and report on potential security issues, such as attackers attempting to guess an operator's password.
- **Generate differential events backup**: When this option is enabled a differential backup of the event database will be created every time events are purged. This backup will contain only the events that have been purged, so that they can be restored for review at a later date.

The backups will be created as .bak files in the directory specified in the **Backup path** (under **Main database backup** below). Each filename will be suffixed with the day of the week that the backup occurred. If a backup file with that name already exists the recently purged events will be appended to the existing file.

For more information, see Application Note 279: Differential Backups in Protege GX.

### Main database backup

- **Backup main database every night**: Select this option to automatically back up the programming database each day at midnight. New backups will overwrite existing backups with the same name.
- **Append day of week to backup file name**: Optional setting that appends the day of the week to the main database backup filename. This allows the system to maintain a week of programming backups.
- **Backup path**: The directory where main database backups will be created. If this field is left blank, backups will be created in the default location for SQL Server.

  When setting a backup path, ensure that the selected directory already exists on the server machine. Do not select a directory that denies SQL Server write access, such as Program Files, Program Data, Users, Windows, etc.

- **Backup now**: Click to perform an immediate backup of the programming database. The .bak file will be generated in the directory specified by the **Backup path**, and will include the current Protege GX database version in the filename.

### Events database backup

- **Select a backup option**: Events database backups can be saved to the local disk, a network drive or an FTP location. If you select FTP, you will be prompted to enter the following details:
  - IP address
  - Port number
  - Certificate path (if authentication is required)
  - Username
  - Password
- **Events DB backup path**: The directory where backups of the events database will be saved. This includes differential backups (see **Generate differential events backup** above).

  When setting a backup path, ensure that the selected directory already exists on the server machine. Do not select a directory that denies SQL Server write access, such as Program Files, Program Data, Users, Windows, etc.

- **Backup now**: Click to perform an immediate backup of the events database. The .bak file will be generated in the directory specified by the **Events DB backup path**, and will include the current Protege GX database version in the filename.

### Record history

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

## Global settings | Email settings

### Email SMTP settings

- **SMTP mail server**: The address of the outgoing SMTP email server.
  The tested and supported SMTP servers are:
  - Microsoft Exchange Server 2016
  - Gmail (requires an app password - see this help page)
  - Yahoo

The SMTP server may require some configuration to allow it to receive and relay emails from Protege GX.

- **SMTP port**: The port used for outgoing mail connections.
- **Use SSL**: When this option is enabled, Protege GX will use TLS 1.2 to transmit emails to the SMTP server. Both the host OS and the SMTP server must support TLS 1.2, and the **SMTP port** above must be changed to a TLS-enabled port (e.g. 587, 2525).

  When this option is disabled, no encryption will be used.
- **SMTP login**: The username to log in to the SMTP mail server. For Gmail accounts this is the email address that you used to generate the app password.
- **SMTP password**: The password for the SMTP mail server. For Gmail accounts this is your app password.
- **SMTP timeout**: Defines how long (in seconds) before the connection to the SMTP mail server times out.
- **Sender email address**: The email address used when sending outgoing mail.
- **Sender display name**: The display name used when sending outgoing mail. If a display name is not entered, the sender email address is used.
- **Test email address**: Enter an email address for test notifications.
- **Test email settings**: Sends a test email to the address specified above.

  The test email is sent from the client machine which is currently in use. To validate the email settings from the Protege GX server, ensure that you are testing using the server machine. This is important for scheduled report emails and other automated emails.

# Global settings | Display

## Status symbol colors

- **Color map**: Defines the color map used to represent the state of devices (such as doors and areas) on floor plans and status pages. These can be defined under **Global | Color maps**.

## Photo display settings

- **Reset display size**: Resets the setting below to 300 pixels wide x 400 pixels high.
- **Pixels**: Sets the default width and height of photos for new user records across all sites. To apply this default, navigate to **Global | Sites | Display**, enter 0 in one of the **Pixels** fields, then click **Save**. This setting does not automatically override the site settings or affect existing user records and photos.

## Display clock time

- **Display date and time in full screen mode**: Select this option to display the date and time in the lower right of the status bar when the Protege GX interface is in full screen mode. You can enter full screen mode by clicking the expand button at the top right.

# Global settings | Sound

## Alarm sounds

- **Alarm sound**: Sets the default notification sound played on operator workstations when an alarm pops up. Choose from the Default Windows sound, a Wave file of your choice, or No sound.
- **Wave file path**: If you are using a wave file for the **Alarm sound**, click the ellipsis button **[...]** to browse to and select the .wav file.

  This wave file must be located in a shared network folder that clients have access to. If the file is not accessible in the same location on all client machines, no sound will be played when an alarm is triggered.

## Sounds

This section enables you to add custom alarm sounds that can be assigned to specific types of alarms. This helps personnel to quickly distinguish between different types of alerts and respond appropriately.

1. Click **Add** to add a custom sound. This must be a wave file with a maximum size of 3 MB.
2. Set a descriptive **Name** for the sound and click **Ok**.
3. Navigate to **Events | Alarms** and assign the custom sound as the **Alarm sound** for the relevant alarm records.
   Any alarm that does not have a custom alarm sound assigned will use the default notification **Alarm sound** setting above.

Sounds added to this section and assigned to an alarm record will be automatically synchronized to each client machine when an operator logs in.

# Sites

Sites are divisions of the Protege GX system which can be used to allow more than one complete security system to reside on the same server.

- Only global records are shared between sites, i.e. programming in the **Global** menu.
- Most types of records are not shared between sites. For example, users on one site cannot access doors and areas on another site, and sites cannot share hardware resources such as inputs and outputs.
- Protege GX operators may be able to access records on multiple sites, or one site only. For more information, see Roles (page 62).

Sites are commonly used when a single Protege GX server is used to run security systems for several different customers. This allows the customers to be kept completely separate from each other while sharing server resources and global settings.

It is not recommended to create a new site record for every location or branch of the same system, as user records are not shared between sites. Instead, use record groups to organize the records which belong to each location.

Use the sites menu to create and configure your site(s). This includes display settings and options related to certain integrations. When you add a new site, the **Add controller** wizard will open automatically, prompting you to add a controller to your new site.

The System site must not be modified.

## Sites | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Alarm status page**: Determines the default status page displayed when clicking the **View alarms** icon in the status bar.
- **Show controller stability bar graph**: When this option is enabled the **Sites | Controllers** record list for the site displays a Connection stability column for each controller. This column uses a bar to represent the stability of the connection, where red blocks represent offline time and green blocks represent online time. This is useful for monitoring the connection when the controller seems to be dropping offline periodically.

### Address

Contact details for the site and/or organization for operator reference.

### Record history

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

## Sites | Display

### Floor plan events tabs

- **Event window 1-6**: Select up to six event reports that will be displayed as additional tabs in the event window when viewing a floor plan.
- **Default floor plan**: The default floor plan that is first displayed when opening the floor plan view for this site.

- **Default status page**: The default status page that is first displayed when opening the status page view for this site.

### User window

- **Display predefined custom fields in users**: Select this option to display the **Users | Users | Extended** tab, which includes a range of predefined custom fields.
- **Display users in groups**: Select this option to view user records in group (or tree) view by default in the **Users | Users** menu. In this view the users are grouped by **Record group**. When this option is disabled user records are displayed in list view by default.
- **Display only one card slot**: Select this option to only display one **Facility/Card number** field for each user. This prevents more than one card from being added to a user through the Protege GX software.

  This setting cannot be enabled if one or more users already have more than one card assigned. You can run a user search (**Users | User search**) with the Facility/Card number column to see which users have excess cards assigned.

  This feature cannot be used with the Suprema integration, as biometric credentials use the second card slot.

  The SOAP service ignores the card number restriction.
- **Display first name and last name columns in users**: Select this option to display columns for **First name** and **Last name** in the **Users | Users** page. You can then sort the users list by first or last name by clicking the column header.

### Default user expiry date/time

These settings allow you to specify default start and/or expiry parameters for all new user records. They are applied when new users are added, and do not affect existing user records.

- **Start**: The default start date/time for all new user records. New users will not be able to gain access before this time and date.
- **End**: The default expiry date/time for all new user records. User records will expire after this time and date and users will not be able to gain access.

These settings can be overridden by the settings for individual users in **Users | Users | General**.

### Photo display settings

- **Reset display size**: Resets the setting below to 300 pixels wide x 400 pixels high.
- **Pixels**: Sets the default width and height of photos for new user records. This does not affect existing user records or photos.

  To use the default settings from **Global | Global settings | Display**, set either the width or height to 0 and click **Save**.

### Calendar actions display

- **Hide old calendar actions**: Select this option to automatically clear calendar actions from the system once they become invalid (**Sites | Calendar actions**).

## Sites | Active Directory

These settings allow you to synchronize Protege GX users with Windows Active Directory for enhanced user management. For synchronizing Protege GX operators with Active Directory, see the options in **Global | Operators | General**.

Active Directory integration is a separately licensed feature. For more information, see Application Note 288: Using Active Directory in Protege GX.

### Active Directory user import settings

- **Import users from Active Directory**: Select this option to import user details from Active Directory to the Protege GX database.
- **Active Directory domain**: Defines the Windows Active Directory domain being used.
- **Windows group**: The Windows group containing the users to import.

  Only one selected Windows security group can be synchronized with this integration.

- **Synchronization period (minutes)**: Defines the frequency of synchronizing users with Active Directory.
- **Disable users if AD users are disabled**: Disables Protege GX user access if the Active Directory account is disabled.
- **Disable users if AD users are deleted**: Disables Protege GX user access if the Active Directory account is deleted.

## Sites | Site defaults

### User card inactivity defaults

- **Disable inactive user card**: If this option is enabled, new users added to the system will automatically have a default **Inactivity period** applied to their credentials. If the user does not use the credential within that period it will be disabled.

  When you change this default setting, you can choose whether to apply the new default to all existing users. Updating existing users may take some time on large sites.

- **Default card inactivity period**: Set the number of days, hours or minutes that the credential must be inactive before it is disabled.

### User inactivity defaults

- **Disable inactive users**: If this option is enabled, new users added to the system will automatically have a default **Disable period** applied to their credentials. If the user is completely inactive for that period the record will be disabled.

  When you change this default setting, you can choose whether to apply the new default to all existing users. Updating existing users may take some time on large sites.

- **Default user inactivity period**: Set the number of days, hours or minutes that the user must be inactive before the record is disabled.
- **Delete inactive users**: If this option is enabled, new users added to the system will automatically have a default **Delete period** applied to their credentials. If the user is completely inactive for that period the record will be deleted.

  When you change this default setting, you can choose whether to apply the new default to all existing users. Updating existing users may take some time on large sites.

- **Default inactivity user deletion period:** Set the number of days, hours or minutes that the user must be inactive before the record is deleted.

### Site security enhancement

For more information, see Application Note 275: Configuring Site Security Enhancements in Protege GX.

- **Require dual credential for keypad access**: With this option enabled, users must enter both a User ID and a PIN to gain access to a keypad. Each user record will include a User ID credential type, which must be a unique numeric ID from 1-10 digits in length.

  In addition, no operator will be able to view user PINs, regardless of whether the **Show PIN numbers for users** option is enabled (**Global | Operators**).

- **Autopopulate User ID credential value**: This feature enables the system to generate User ID numbers for users automatically. When the option is first enabled all users who do not have an existing User ID are automatically assigned a unique ID (based on their Database ID). After that point any new users created will automatically be assigned a unique 8-digit User ID. User IDs can always be manually edited, even after being autopopulated. This is convenient on larger sites where it may be difficult to ensure that every new user is assigned a unique ID.
- **Allow PIN duplication**: Enabling this feature allows the creation of identical PINs among user records for the site. Each user will be required to enter a unique User ID to identify themselves as well as a PIN, allowing the system to accurately identify the user logging in to the keypad and maintaining the integrity of site security.

  The PIN only and Card or PIN door types are not compatible with duplicate PINs, as there is no way to uniquely identify the user who is requesting access.

- **Default PIN length**: The default length of PIN codes when automatically generated by the system, from 4 to 8 digits.

  For example, if this is set to 6 the system will generate new PINs with 6 digits first. Once those are depleted it will then generate PINs with higher numbers of digits, then PINs with fewer digits.
- **Minimum PIN length**: The minimum number of digits (options between 1-8) permitted for PINs. The higher the PIN length the higher the security level, since PIN complexity increases with a greater number of digits.
- **Maximum sequential digits**: The maximum number of sequential digits permitted for PINs, between 2 and 4 digits. For example, selecting 4 will allow a numerical sequence of 1234 or 4321, but not 12345.
- **Maximum repetitive digits**: The maximum number of repeated digits permitted for PINs, between 2 and 4 digits. For example, selecting 4 will allow a PIN of 0000, but not 00000.
- **PIN expiry time**: User PINs will expire after the length of time defined in this field. When the user attempts to log in to a keypad after this time they will be prompted to enter and confirm a new PIN. This is a sitewide setting and can be overridden by the **PIN expiry** settings for individual users (**Users | Users | General**).

  When PIN expiry is enabled any PIN created through the user interface will immediately expire on first use. The user must set their own permanent PIN using a keypad. This ensures that only the user knows their PIN.

  When you change this default setting, you can choose whether to apply the new default to all existing users. Updating existing users may take some time on large sites.

- **New PIN to be generated by system**: When this option is enabled, any permanent PIN must be generated by the system (other than a temporary single-use PIN created by the operator). A user can request a new PIN when logging in at a keypad. If an expired PIN is used to log in at a keypad the system will automatically present the user with a new PIN.

  This option is only available when a **PIN expiry time** is set.

## Photo ID

- **Save badge number and date after card printing**: When this option is enabled, after a Photo ID card is printed the **Badge number** (beginning from 1) and **Date of badge production** will be automatically saved to the user record in the **Extended** tab. The **Badge type** will be set to Printed.

  For this option to function, the **Display predefined custom fields in users** option must be enabled in the **Display** tab.

## Integration

- **Enable Milestone bidirectional integration**: Enable the bidirectional integration with Milestone XProtect. For more information, see Application Note 358: Milestone XProtect Bidirectional Integration with Protege GX.

## Wireless locking integration

- **Enable offline wireless locks**: Enable this setting to use Protege offline wireless locks in your Protege GX system. This will allow you to program, initialize and update offline wireless locks.

Enabling this feature cannot be reversed. **Take a backup before enabling wireless locks.**

For more information and programming instructions, see the Protege Offline Wireless Lock Configuration Guide.

# Sites | User photos export

User photos stored in Protege GX can be periodically exported to a directory on the server machine. This feature can be used to share images captured within Protege GX with third-party systems such as HR or badge printing systems.

## General

- **Enabled**: Activates the photo export process.
- **Export folder**: The disk location where the user photo files will be saved.
- **Export photo format**: The image format the photo files are saved as. Select from: .jpg, .png, .bmp, .gif, .tif or .wdp.
- **Export file name custom field**: The exported images will be named numerically (1, 2, 3, etc). The custom field selected here will be prefixed to the filename, allowing users to be grouped or specifically identified.

## Schedule type

- **Start manually**: The user photos export is operated manually using the **Export user photos now** button.
- **One time**: The user photos export will run once. After selecting this option you will need to specify the start date and time in the **Start time** field.
- **Recurring**: The user photos export will run on a recurring basis. After selecting this option you will need to set the occurrence (daily, weekly or monthly) and frequency (day(s) and time) the export will occur. You may also want to specify a **Duration** (start and/or end date) for the export schedule.
- **Next run time**: Displays when the user photos export will run next (read only).

## Last Run Time

- **Export user photos now**: Click this button to manually export user photos.
- **Last run time**: Displays the date and time of the most recent user photos export (read only).
- **Last run status**: Indicates whether the most recent user photos export succeeded or failed.

# Sites | Biometrics

Suprema and Princeton Identity biometric integrations are separately licensed features. For more information, see Application Note 264: Suprema Biometric Integration in Protege GX and/or Application Note 297: Princeton Identity Biometric Integration with Protege GX.

## Suprema biometrics

- **Enable Suprema integration**: Select this option to enable Suprema biometric integration for this site.
- **Default facility number**: The default facility number used for biometric credentials for this site. When a biometric credential is enrolled, a card number will be automatically generated and assigned to the user alongside this facility number as their second credential.

  Ensure that this number is not the same as the facility number for any cards used on site. The default number of 100 is recommended.

- **Default enrollment reader**: Defines which biometric reader will be used as the default enrollment device for new biometric credentials. Biometric readers can be programmed in **Sites | Biometric readers**. This option can be overridden for specific users (**Users | Users | Biometrics**).

### Princeton biometrics

- **Enable Princeton integration**: Select this option is enable Princeton Identity biometric integration for this site.
- **Default facility number**: The default facility number used for biometric credentials for this site. When a biometric credential is enrolled, a card number will be automatically generated and assigned to the user alongside this facility number as their second credential.

  Ensure that this number is not the same as the facility number for any cards used on site. The default number of 100 is recommended.

- **Default enrollment reader**: Defines which biometric reader will be used as the default enrollment device for new biometric credentials. Biometric readers can be programmed in **Sites | Biometric readers**. This option can be overridden for specific users (**Users | Users | Biometrics**).
- **IP address**: The IP address of the Princeton Identity Server (IDS).
- **IP port**: The IP port of the Princeton Identity Server. The default port is 8843.
- **Username**: The username required to log in to the Princeton Identity Server.
- **Password**: The password required to log in to the Princeton Identity Server.
- **Credential type**: When Princeton integration is enabled a default PrincetonIris credential type will be created and assigned to the site configuration here. This credential type contains the programming required to enroll and use Princeton biometric credentials. It can be viewed in **Sites | Credential types**.

## Sites | Salto

The parameters entered here must match the settings in the Salto SHIP interface programming. In this integration, Salto cards for users are encoded directly within Protege GX, using a desktop encoder. To obtain the required encoder.ini file, contact ICT Technical Support.

Salto SHIP integration is a separately licensed feature. For more information, see Application Note 188: Salto SHIP RW Pro Access Integration with Protege GX or Application Note 335: Salto SHIP ProAccess SPACE Integration with Protege GX.

This tab is not used for Salto SALLIS integration.

### Salto options

- **Enable Salto (SHIP) integration**: Select this option to enable Salto SHIP integration for this site.
- **Enable logging**: Enables the Salto error log, which logs all data sent to the Salto system. The error log can be accessed in Protege GX via **Salto | Salto error log**.

  This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.

- **IP address**: The IP address of the SHIP server.
- **IP port**: The port used to communicate with the SHIP server.
- **Default Salto encoder ID**: If there are multiple Salto encoders connected to the PC being used to encode Salto credentials, by default Protege GX will use the first encoder that was configured. If a different encoder should be used, specify its ID here.
- **Mifare A key**: The Salto Mifare A key string for encoding Salto cards. This field can be left empty - the value from the encoder.ini file will be used.
- **Mifare B key**: The Salto Mifare B key string for encoding Salto cards. This field can be left empty - the value from the encoder.ini file will be used.
- **Master key**: The Salto master key string for encoding Salto cards. This field can be left empty - the value from the encoder.ini file will be used.

### MIFARE 1K/4K sector selection

To encode cards from the Protege GX interface you must select the card sectors that are allocated to Salto. The allocated sectors are site specific and can be viewed in the encoder.ini file located in the C:\Program Files (x86)\Integrated Control Technology\Protege GX folder.

Sector 14 should be left for use by the ICT MIFARE format.

## Sites | Cencon

Cencon integration allows you to monitor and manage Cencon locks from within Protege GX. This allows you to manage Cencon users, create logical lock groups, view a Cencon lock's status, and monitor Cencon events.

Cencon integration is a separately licensed feature. For more information, see Application Note 160: Configuring Cencon Integration.

### Cencon Options

- **Enable Cencon integration**: Select this option to enable Cencon integration for this site.
- **CenTran input transaction path**: The directory where Protege GX will send outgoing Cencon transactions.

  For the integration to function correctly, ensure this directory can be accessed by both the Protege GX and CenTran services.
- **CenTran output transaction path**: The directory where Protege GX will receive incoming Cencon transactions.

  For the integration to function correctly, ensure this directory can be accessed by both the Protege GX and CenTran services.
- **Dispatcher ID**: The Dispatcher ID identifies the source of the transaction in the CenTran programming. If this field is blank the default Dispatcher ID will be used.
- **Branch name**: The name of the Cencon Branch that Protege GX manages.
- **Cencon command timeout (seconds)**: Defines how long (in seconds) Protege GX waits for a response from Cencon after sending a transaction file.

  This value should not be changed unless advised by ICT Technical Support.
- **Cencon synchronization interval (minutes)**: Defines how frequently (in minutes) a synchronization between Protege GX and Cencon occurs.

  This value should not be changed unless advised by ICT Technical Support.
- **Log all Cencon transactions**: When this option is enabled, Protege GX logs all Cencon transactions in the Cencon Transaction Log (**Cencon | Transaction logs**). When disabled, Protege GX only logs error transactions.

  This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Synchronize**: When this button is activated Protege GX will attempt to synchronize with the Cencon database.

## Sites | Key cabinets

Key cabinet integrations enable you to monitor and manage access to keyboxes and keys from within Protege GX.

The KeyWatcher and KeySecure integrations are separately licensed features. For more information, see Application Note 220: KeyWatcher Touch Integration in Protege GX or Application Note 331: KeySecure Integration with Protege GX.

### Integration options

- **Enable integration**: Select this option to enable key cabinet integration for this site.
- **Integration type**: Select either KeyWatcher - Morse Watchmans or KeySecure - CIC Technology.

- **Enable logging**: The log file for the integration service is stored in the installation directory. Enable this option to log all available messages. Disable this option to log error messages only.

  This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.

- **Third party user ID digit length**: For KeyWatcher integrations, this is the length of the **KeyWatcher ID** that will be automatically assigned to each user who has a valid access level assigned that includes KeyWatcher keys or key groups (**Users | Users | General**). All KeyWatcher IDs must contain this number of digits.

  This setting must match the **User ID Digit Length** field assigned in the KeyWatcher True Touch client software. Any changes to this field must be matched in the KeyWatcher software.

# Sites | Portal

Tenancy portal sync allows you to automatically sync Protege GX users to the Protege tenancy portal and create Protege mobile app and SIP accounts for them. This enables visitors to directly call tenants from an entry station.

For more information and setup instructions, see the Protege Tenancy Portal User Guide.

## General options

- **Enable portal synchronization**: Enable this setting to allow users to be synchronized to the tenancy portal.

  When the tenancy portal sync is enabled, user PINs will always be returned in plain text when the SOAP service gets a user record. This overrides settings which normally mask the PINs, such as **Show PIN numbers for users** and **Encrypt user PINs**, and affects **all** operators using the web client and other SOAP applications.

- **Enable touchless elevator sync**: This option is reserved for future development.

## Credentials

- **Username**: The username for your tenancy portal account.
- **Password**: The password for your tenancy portal account.

# Sites | Offline wireless locks

This section is only available when the wireless locking integration is enabled (**Global | Sites | Site defaults**).

This tab enables you to configure the default settings for offline wireless locks and users, as well as some general options for the operation of the offline system.

## General options

- **Collect event log when updating locks**: With this option enabled, when the Protege Config App updates an offline lock it will also collect the lock's archived event log, including events that have been retrieved by cards in the past. The events are uploaded to Protege GX the next time the app is badged at an update point reader. This may be time consuming if there are a large number of events to retrieve.
- **Enable lock reinitializing**: When this option is enabled, you can right click on an offline door record and select **Reinitialize** to remove the lock pairing without deleting the programming. You can then either default and reinitialize the existing lock, or initialize a new lock.

## Offline wireless lock options

These settings determine the default configuration of any new offline wireless locks that are added to the system in **Programming | Doors**. When you change the settings and save, you can either update all existing door records or leave them as they are.

- **Enable lock event log**: Enable this option to allow the offline lock to store events in its internal memory. You can determine what types of events are recorded using the settings below.
- **Enable card event log**: Enable this option to allow the offline lock to transfer events to access cards and mobile devices when access is granted. The events will be uploaded to the system when the credential is badged at an update point reader. This option can be disabled when cards do not have enough storage to collect events.

  If this option is disabled, events can still be retrieved from the lock using the Protege Config App.
- **Log access granted events**: Enable this option to allow the offline lock to log access granted events.
- **Log door open/close events**: Enable this option to allow the offline lock to log door open and close events. This should typically remain disabled, as the additional events can fill up the card's event log quickly.
- **Log access denied events**: Enable this option to allow the offline lock to log access denied events.
- **Log exit events**: Enable this option to allow the offline lock to log exit (REX) events.
- **Deny access when card storage is full**: With this option enabled, the lock will deny access if there is no space on the user's card to store events. The user must badge their card at an update point reader to upload their events before they can gain access. When this option is disabled, access will be granted even if there is no space for new events on the card.

  Use this setting with caution, as cards with low storage space can fill up with events quickly in normal operation.
- **Enable beeper**: With this option enabled, the lock will signal with the beeper as well as the LED. This may impact the lock's battery life.
- **Flash when unlocked by key**: With this option enabled, the reader will flash blue three times when the door is unlocked with a key. This occurs when the door latch is fully retracted (not when the deadbolt is retracted).
- **Allow emergency opening**: Enable this option to allow operators to send the **Emergency open** manual command to the door. An authorized config app user can retrieve the command from an update point reader and use it to unlock the door once. This allows a building manager to open the door when the owner or tenant locks themselves out, but does not grant them permanent access.
- **Exit leaves door unlocked time period**: When the lock is in Exit leaves door unlocked or Exit leaves door unlocked + toggle mode (**Programming | Door types | Options**), by default when someone exits the door will remain unlocked until a user badges a credential to relock it. With this option enabled, the door will automatically lock when the defined period expires. It can still be manually relocked by badging a credential.
- **Blocklist creation**: This setting determines whether offline lock credentials are added to the blocklist when a credential or user record is deleted.
  - **Automatic** (default setting): Credentials are automatically added to the blocklist when deleted.
  - **Prompt**: When the operator deletes a credential or user record, they can select whether the credential is added to the blocklist or not. If the user is deleted automatically due to inactivity, their credentials will not be added to the blocklist.
  - **Disabled**: No credentials are added to the blocklist.

## User settings

- **Update period**: The update period determines how frequently the user must update their credential at an update point reader. If they do not update their credential within this period, the access data will expire and they will not be able to access offline locks until they renew the data at the update point reader.
- **Enable office unlock**: When the **Lock operating mode** is set to Office unlock (**Programming | Door types | Options**), users with this option enabled can latch unlock the door by holding down the inside handle and badging a credential at the same time. They can relock the door using the same method.

# Operators

An operator is a person who uses Protege GX and is responsible for programming and maintaining the system and monitoring the site.

Some fields in the default Admin operator record cannot be edited.

## Operators | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.

  This does not need to be the same as the operator's username (below).

- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Username**: The username that the operator uses to log in to Protege GX.
- **Password**: The operator's password for logging in to the software. You can reset an operator's password by clicking the ellipsis **[...]** button.

  Operators can also change their own passwords from the Home page.
- **Role**: Select the appropriate role to determine what the operator can see and do in the software. Roles can be configured in **Global | Roles**.

  Click the ellipsis **[...]** button to open a role access window, which shows which database tables the operator has read access, write access and manual command permissions for. You can print the report by clicking the **Print** icon in the toolbar, filter results by typing terms in the second header row, and group results by dragging columns into the bar above the table.
- **Time zone**: The time zone where the operator is based. This determines the event log times shown on status pages and floor plans. If the operator uses the same time zone as the Protege GX server, select Use server time zone.
- **Use Windows Authentication**: Select this option to use Windows Authentication/Active Directory and enable the operator to connect using their Windows user credentials. This bypasses the need to enter a username and password when logging into Protege GX, making the log in process more secure.

  To connect this operator to an Active Directory user, enable this option then click the ellipsis **[...]** beside the **Username** field. Select a **Domain** and locate the **Active Directory user** that corresponds to this operator.

  This feature requires the **Enable Windows Authentication on Data Service / Client Communications** option to be enabled during installation. For more information, see Application Note 288: Using Active Directory in Protege GX.

- **Show PIN numbers for users**: Enables the operator to view user PINs.
- **Show Salto keys**: Enables the operator to view Salto key information.

### Email

- **Email**: The email address of the operator. This can be used by Protege GX for automatic email on event and other functions.

  Automated email features in Protege GX require an SMTP mail server to be configured in **Global | Global settings | Email settings**.

- **Default report language**: The default language used when a scheduled report is emailed to the operator. Select from the first or second language (as determined by the software installation).

## Operator Timeout

- **Enable operator timeout**: Select this option to automatically log the operator out after a period of inactivity.
- **Operator timeout in seconds**: Defines the inactivity period (in seconds). If the operator is not active during this time, there will be a 30 second warning, after which the client will close.

## Record history

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

# Roles

Roles define the level of access that operators have to the Protege GX system. Each role is based on a preset (administrator, installer, end user or guard) and can be further customized to precisely control which sections of the system an operator can view and edit. More complex roles also use security levels, which allow for finer-grained control over access to menus, manual commands, sites and record groups.

The default Administrator role cannot be edited. This ensures that the admin operator has full system access.

Changes to roles will not take effect until the affected operators have restarted their client sessions.

For more information and programming examples, see Application Note 191: Programming Operator Roles in Protege GX and Application Note 247: Using Record Groups in Protege GX.

## Roles | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Preset**: Select this option to choose one of the four role presets:
    - **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.

  Role presets provide a quick means of providing operator access. Unless role permissions are specifically edited, all permissions will be inherited from the preset. For more information, see Role Presets and Tables (next page).

### Record history

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

## Roles | Tables

The **Tables** tab determines role's permissions to menus and other features within the software. This allows you to customize access based on the role assigned to an operator. For example, operators in an HR role may be given access to tables containing staff data and denied access to other tables.

For each table, select one of the following options:

- Inherit from preset to retain the default permissions from the selected role preset.
- Deny to prevent access to the data contained in the table. This hides any functions and menu options for that table from the operator.
- Grant full access to grant full read/write permission.
- Grant read only access to grant access to view but not to update data in the table. The operator will be able to view the relevant settings but the options for updating them are disabled.

See Role Presets and Tables for a full breakdown of the permissions that are granted/denied by each preset and table.

# Roles | Sites

The **Sites** tab determines the sites that the role has access to. Access permissions within specific sites can be further customized in the **Security levels** tab.

- **Has access to all sites**: Check this box to grant the role access to all sites in the system.
- **Sites**: Check the **Active** checkbox beside each site to grant the role access to that site (based on the permissions granted in the **Tables** tab), or disable it to deny access. If they are denied access to a site, operators will be able to see that the other site exists, but not view or edit any of its records.

# Roles | Security levels

The **Security levels** tab allows you to further specify the operator's permissions using security levels, as well as restrict access to particular record groups. Security levels are programmed in **Sites | Security levels**. The permissions granted in a security level will override those granted in the role's **Tables** tab.

If there are no record groups selected, the operator will be able to access all record groups. If any record groups are added, the operator will only be able to access records from the specified groups.

Multiple record groups with the same security level can be included, but record groups with different security levels are not supported. If this is required it is recommended that you add a separate operator record.

Click the **Add** button to assign a security level. Select the following options:

- **Site**: The site which the desired security level is relevant to.
- **Security level**: The security level that will grant the required permissions for this site.
- **Access all record groups**: Enable this option to grant access based on the permissions in the security level to all record groups (or select specific record groups from the **Name** field below).
- **Name**: Select the specific record group(s) which this security level will apply to. The operator will only have access to these record groups, using the permissions in the selected security level.

# Roles | Display

## Alarm notification settings

- **Pop up while alarms present**: When this option is enabled the operator will receive a popup notification when specific alarm events occur. Alarms can be created in the **Events | Alarms** programming.
- **Popup frequency**: The time between popup notification reminders. When an alarm popup is displayed to the operator, the computer will play an audible notification tone each time this period elapses without the alarm being acknowledged.

  In addition, an operator can click on the mute icon in the upper right of the popup window and dismiss the alarm for the duration of the popup frequency.
- **Operator can disable until next logon**: When this option is enabled the operator can disable an alarm popup window until they next log on by clicking the mute icon in the upper right of the popup window.
- **Operator can put alarm popup to sleep for X minutes**: When this option is enabled the operator can disable an alarm popup window for a defined number of minutes by clicking the mute icon in the upper right.

## Camera options

- **Allow camera popup**: When this option is enabled the operator can receive camera window popups displaying live footage when specific events occur. These popups can be configured by creating an action (**Events | Actions**) with the **Type** set to Popup camera window, or via the **Auto camera popup** settings in **Programming | Doors | General**.

# Role Presets and Tables

This reference table contains the following information:

- What permissions are granted/denied by each role table.
- The default permissions for the End User and Guard presets. The Administrator and Installer presets have full access to everything by default.

= Read and edit access by default

= Read only access by default

= Access denied by default

All roles have access to the **Visitor** and **About** menus by default.

| Table | Permissions | End User | Guard |
|---|---|---|---|
| **Global tables** | | | |
| Sites | • Global \| Sites | | |
| Operators | • Global \| Operators<br>• Reports \| Central station report<br>• Reports \| Operator permission report<br>Requires access to **User reports**. | | |
| Roles | • Global \| Roles | | |
| Event servers | • Global \| Event server | | |
| Download servers | • Global \| Download server | | |
| Device states | Not used. | | |
| Event logs | • Salto \| Salto log<br>Requires access to **Salto programming windows**. | | |
| System | • Global \| Global settings<br>• Global \| Color maps<br>Not available for End User or Guard presets.<br>• Global \| Floor plan symbols<br>Not available for End User or Guard presets.<br>• Global \| Event types<br>Not available for End User or Guard presets. | | |
| Modems | • Global \| Modem (not used) | | |
| Event types | Not used. | | |
| **Site tables** | | | |
| Access levels | • Users \| Access levels | | |
| Alarms | • Events \| Alarms | | |
| Card template editor | • Users \| Card template editor | | |

| Table | Permissions | End User | Guard |
|---|---|---|---|
| Custom fields | • Users \| Custom fields<br>• Users \| Custom field tabs | ✓ | ✗ |
| Door groups | • Groups \| Door groups | ✗ | ✗ |
| Holidays | • Sites \| Holiday groups | ✓ | ✗ |
| Jobs | Not used. | | |
| Record groups | • Sites \| Record groups | ✓ | ✗ |
| Schedules | • Sites \| Schedules | ✓ | ✗ |
| Calendar actions | • Sites \| Calendar actions | ✗ | ✗ |
| Security levels | • Sites \| Security levels | ✗ | ✗ |
| Users | • Sites \| Import users<br>• Sites \| Batch add users<br>• Users \| Users<br>The End User and Guard presets do not have access to edit user PIN codes without **Generate PINs** enabled in the security level. | ✓ | ✗ |
| Credential types | • Sites \| Credential types | ✓ | ✗ |
| Card profiles | • Sites \| Card profiles | ✓ | ✗ |
| Cross controller groups | • Sites \| Cross controller groups | ✗ | ✗ |

| Table | Permissions | End User | Guard |
|---|---|---|---|
| Controller programming windows | • Sites \| Controllers<br>Grants access to perform all controller manual commands except for setting the date/time (see **Manual commands**).<br>• Programming \| Doors<br>• Programming \| Inputs<br>• Programming \| Door types<br>• Programming \| Input types<br>• Programming \| Areas<br>• Programming \| Outputs<br>• Programming \| Trouble inputs<br>• Programming \| Elevator cars<br>• Programming \| Floors<br>• Programming \| Phone numbers<br>• Programming \| Services<br>• Groups \| Area groups<br>• Groups \| Keypad groups<br>• Groups \| Menu groups<br>• Groups \| Output groups<br>• Groups \| Elevator groups<br>• Groups \| Floor groups<br>• Expanders \| Keypads<br>• Expanders \| Analog expanders<br>• Expanders \| Input expanders<br>• Expanders \| Output expanders<br>• Expanders \| Reader expanders<br>• Automation \| Automation<br>• Automation \| Programmable functions<br>• Automation \| Data values<br>• Automation \| Variables | ✗ | ✗ |
| | • Programming \| Daylight savings<br>The End User preset has access to edit daylight savings records by default. | ✓ | ✗ |
| Salto programming windows | • Salto \| Doors<br>• Salto \| Door groups<br>• Salto \| Calendars<br>• Salto \| Salto log<br>Requires access to **Event logs**. | ✗ | ✗ |
| Smart readers | • Expanders \| Smart readers | ✗ | ✗ |
| Apartments | • Programming \| Apartments<br>• Programming \| Batch add apartments<br>Requires access to **Controller programming windows**. | ✗ | ✗ |

| Table | Permissions | End User | Guard |
|---|---|---|---|
| Function codes | • Sites \| Function codes | ✗ | ✗ |
| **Site monitoring and control** | | | |
| Floor plans | • Monitoring \| Floor plan view<br>• Monitoring \| Setup \| Floor plan editor<br>• Monitoring \| Setup \| Floor plan editor (batch)<br>• Monitoring \| Setup \| Add bulk floor plans | ✓ | ✓ |
| Status pages | • Monitoring \| Status page view<br>The role must also have access to view the status lists, event reports and other objects on the status page.<br>• Monitoring \| Setup \| Status page editor<br>• Monitoring \| Setup \| Status page editor (batch)<br>• Monitoring \| Setup \| Status lists<br>• Monitoring \| Setup \| Web links | ✓ | ✓ |
| Cameras | • Monitoring \| Setup \| DVRs<br>• Monitoring \| Setup \| Cameras<br>• Monitoring \| Setup \| PTZ commands | ✗ | ✗ |
| Manual commands | Grants access to perform manual commands on devices.<br>Grants access to set the controller date/time. | ✗ | ✓ |
| Acknowledge alarm | Grants access to acknowledge alarms. | ✗ | ✓ |
| Intercoms | • Monitoring \| Setup \| Intercoms | ✗ | ✗ |
| **Site reports** | | | |
| Event reports | • Events \| Event search<br>• Events \| Event filters<br>• Reports \| Setup \| Event | ✗ | ✗ |
| | • Reports \| Event<br>The Guard and End User presets have access to run event reports by default.<br>• Reports \| Central station report | ✓ | ✓ |
| Muster reports | • Reports \| Muster<br>• Reports \| Central station report<br>• Reports \| Setup \| Muster | ✗ | ✗ |
| Attendance reports | • Reports \| Attendance<br>• Reports \| Central station report<br>• Reports \| Setup \| Attendance<br>• Reports \| Setup \| Shift type | ✗ | ✗ |

| Table | Permissions | End User | Guard |
|---|---|---|---|
| User reports | • Sites \| Jobs (not used)<br>• Sites \| User import job step (not used)<br>• Users \| User search<br>• Reports \| Users<br>• Reports \| Central station report<br>• Reports \| Setup \| User | | |

# Download server

The download server manages communication from the Protege GX user interface to the controller. It may also manage synchronization with integrated third-party servers and devices.

Typically only the standard Protege GX Download Service is required. However, there are some additional features that can be implemented to reduce download times on very large installations.

- The single record download service (installed separately) reduces download times by sending to controllers only the record(s) that have been added, changed or deleted. For more information, see Application Note 309: Single Record Downloads in Protege GX.
- Multiple standard download servers can be used to handle separate groups of controllers. For more information, see Application Note 290: Setting up a Secondary Protege GX Download Server.

If the settings for the download server are changed you may be required to restart the Protege GX Download Service.

## Download server | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Computer name**: The name of the computer hosting the download server.

  The maximum length for the computer name is 15 characters.

- **Maximum number of concurrent downloads**: Defines the maximum number of connections to the controller when downloading. The default of 4 is acceptable for most systems and increasing it beyond this number will not necessarily improve download speeds.

  The server can only download to one controller at a time (unaffected by this setting).

- **Version**: Displays the current version details of the download server (read only).
- **Version date**: Displays the date the download server was last updated (read only).
- **Last notification time**: Displays the date the download server last generated a notification (read only).
- **Download server type**: The options are:
  - Standard: The Protege GX Download Service
  - Single record: The Protege GX Single Record Download Service
- **Download server parent**: If the **Download server type** is Single record it is possible to select a standard download server as the parent. This restricts the single record download server to only download to controllers which are managed by the standard download server. If no parent is selected the single record download server downloads to all controllers.

### Record history

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

# Event server

The event server manages communication from the controller to the Protege GX user interface.

If the settings for the event server are changed you may be required to restart the Protege GX Event Service.

## Event server | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Computer name**: The name of the computer hosting the event server.

  The maximum length for the computer name is 15 characters.

- **Port**: The IP port through which events will be sent from the controller to the software. By default, this is port 22000.
- **Number of communication threads**: The number of threads dedicated to decoding events and status messages. The default of 8 is acceptable for most systems.

  When set to **Automatic**, the event server will use twice the number of processor threads.

- **Number of database threads**: The number of threads that are used for saving events to the database. The default of 1 is acceptable for most systems.

  The number of threads is a licensed feature in SQL server.

- **Watch dog**: Automatically resets communications if the event server has not received events from a controller within 90 seconds.
- **Version**: Displays the current version details of the event server (read only).
- **Version date**: Displays the date the event server was last updated (read only).
- **Last notification time**: Displays the date the event server last generated a notification, such as an operator alarm (read only).

### Record history

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

# Modem

This programming page refers to legacy features and is no longer used in Protege GX.

# Color maps

Color maps allow you to customize the colors used to represent the state of objects (such as doors or outputs) on a floor plan or status page. For example, you could configure a color map so that unlocked doors were displayed as blue rather than the default green to aid operators with red-green color blindness.

You can select the color map that will be used for the entire system in **Global | Global settings | Display**. If no color map is set the default colors will be used.

Any changes to color map settings require Protege GX to be closed any reopened before the new settings will be applied to objects displayed in the user interface.

## Color maps | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

## Color Maps Device tabs

The following status icons may have a custom color applied. The available colors are gray, red, orange, yellow and green.

### Color Maps | Doors

- Door offline
- Door closed and locked
- Door closed and unlocked
- Door forced open
- Door open and unlocked
- Door left open, door sense not sealed
- Door left open, bond sense not sealed

### Color Maps | Inputs

- Input offline
- Input closed
- Input open
- Input tamper
- Input short circuit

## Color Maps | Outputs

- Output offline
- Output on
- Output off

## Color Maps | Areas

- Area offline
- Area disarmed
- Area armed
- Area entry delay
- Area (other statuses)

## Color Maps | Elevators

- Elevator offline
- Elevator locked
- Elevator unlocked

# Floor plan symbols

Floor plan symbols are custom symbols that represent the various objects (such as doors and areas) and their states when displayed on a floor plan.

## Creating a Floor Plan Symbol

1. In **Global | Floor plan symbols**, click **Add**. Enter a **Name**.
2. Select the **Type** of device that you want this floor plan symbol to represent. Only one device type can be selected per record.
3. For each state field, click the ellipsis **[...]** button to add an image.
   - If the image is already stored on the network, select the ellipsis **[...]** beside **Path** to browse to the image. The image must be accessible from the server machine.
   - If the image does not yet exist set the **Image source** field to capture a new image. You can capture an image from a connected webcam, or from a Topaz signature pad.
   - When complete, click **Next**.
4. In the next window you may crop the image if required:
   - Adjust the dotted rectangle's size and position to include the section of the image you wish to keep. Check the **Aspect** option to fix the aspect ratio of the rectangle.
   - To crop the image, check the **Crop** checkbox.
   - Click **Ok**.
5. Repeat the above for all state fields then **Save** the floor plan symbol.
6. Once a floor plan symbol is created you can select this record as a **Device style** when you add a device to a floor plan (**Monitoring | Setup | Floor plan editor**).

# Floor plan symbols | General

## General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Type**: Select the type of device to add symbols for. Each floor plan symbol record can only hold symbols for a single device type (any other images loaded will not be available in the floor plan editor).

## Door States

- Door offline
- Door closed and locked
- Door closed and unlocked
- Door forced open
- Door open and unlocked
- Door left open, door sense not sealed
- Door left open, bond sense not sealed

## Input States

- Input offline
- Input closed

- Input open
- Input tamper
- Input short circuit

## Output States

- Output offline
- Output on
- Output off

## Area States

- Area offline
- Area disarmed
- Area armed
- Area entry delay
- Area (other statuses)

## Elevator States

- Elevator offline
- Elevator locked
- Elevator unlocked

## Record history

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

# Event types

The event types page provides a full list of the events that can be generated by the system, allowing you to search for specific events and identify their Database IDs as necessary. You can also define the display color used for events in the event window, making it easy to quickly identify specific events.

To bring any custom event colors into effect you must save the changes, close the Protege GX client and restart the Protege GX services. When the client is reopened the custom colors will be displayed on status pages and floor plans.

## Event types | General

### General

- **Name**: The event description in English, as it appears in event searches and reports. This field is read only.
- **Name (Second Language)**: The event description in the second language installed with the software. This field is read only.

### Display Colors

- **Customize Display Colors**: Enable this option to allow you to customize the background and text color of the event type.
- **Background Color**: The background color of this event type in the event log. Enter an RGB code, or click the ellipsis **[...]** button to open a color picker.
- **Text Color**: The text color of this event type in the event log. Enter an RGB code, or click the ellipsis **[...]** button to open a color picker.

# Sites Menu

The sites menu contains records used for setting up the site, such as controllers, schedules and credential types.

Sites are divisions of the Protege GX system which can be used to allow more than one complete security system to reside on the same server. For more information, see Sites (page 51).

## Schedules

Schedules in Protege GX are central to automating both access control and intrusion detection. Access levels, areas, doors and other records can be configured to follow a schedule, allowing them to automatically change state when a schedule becomes valid or invalid.

Each schedule can be programmed with up to 8 periods including different times and days of the week, programmed to cover a wide range of operational scenarios. A schedule can be programmed with a holiday group, allowing it to be valid for different hours on public holidays. A schedule can also follow the state of an output, providing more complex automation.

For a demonstration, see Programming a New Schedule in Protege GX on the ICT YouTube channel.

### Schedules | Configuration

#### General

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

#### Record history

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

#### Time periods and groups

- **Periods**: You can configure up to 8 time periods in each schedule to define when the schedule is valid and invalid. Set a **Start time** and **End time** for each period using the time picker. Then check the days of the week the period will apply to and set the **Holiday mode** for the period.

  To create a 24/7 schedule, set both the **Start time** and **End time** to 12:00 AM and check every day of the week. Set the **Holiday mode** to Ignore holiday.

- **Holiday mode**: Defines how the schedule will operate during a holiday (as defined in the **Holiday groups** tab). For each individual time period, choose from:
  - **Disabled on holiday**: When this option is selected this period will not operate on a holiday and the schedule will not become valid during this period on a holiday. For example, if a door is programmed to unlock during this period, it will not unlock on a holiday.
  - **Enabled on holiday**: When this option is selected this period will only operate on a holiday and not on normal days. For example, an area might be programmed to disarm for shorter periods on public holidays but longer periods on other days.

- **Ignore holiday**: When this option is selected the period will operate regardless of whether the day is a holiday or not.

- **Salto**: These fields allow you to configure specific periods that will be used for holidays and special days in the Salto SHIP integration. If the H (Holiday), S1 (Special 1) or S2 (Special 2) boxes are checked this period will be used on those days, as defined in the relevant Salto calendar (see **Salto | Calendars**).

  The Salto calendar used by the schedule is set in the user programming: **Users | Users | Salto**.

### Graphics view

The graphics view provides a visual representation of the schedule periods. Each day of the week is represented by a 24 hour timeline indicating the times when the schedule is valid (solid bar) and invalid (empty). Note that all periods are combined on this view, regardless of their holiday mode.

The graphics view is read-only. Period times cannot be adjusted from this section of the screen.

## Schedules | Options

### Qualify output

- **Validate schedule if qualify output on**: When this option is enabled the schedule can only become valid when the **Qualify output** (below) is on.
- **Validate schedule if qualify output off**: When this option is enabled the schedule can only become valid when the **Qualify output** (below) is off.
- **Qualify output**: This field allows you to assign an output which will qualify the schedule. This means that the schedule will only become valid when both the period and the qualify output are in a valid state. The state required for the output is defined by the options above.

  The feature has many applications for integrating access control, intruder detection and automation. For example, you could use an area's **Disarmed output** as the qualify output so that the schedule only becomes valid when the area is disarmed. The schedule could then be used to control other areas, access levels, door types and other features within the system.

  For an advanced programming example using a qualified schedule, see Application Note 307: Programming a Man Down Switch in Protege GX.

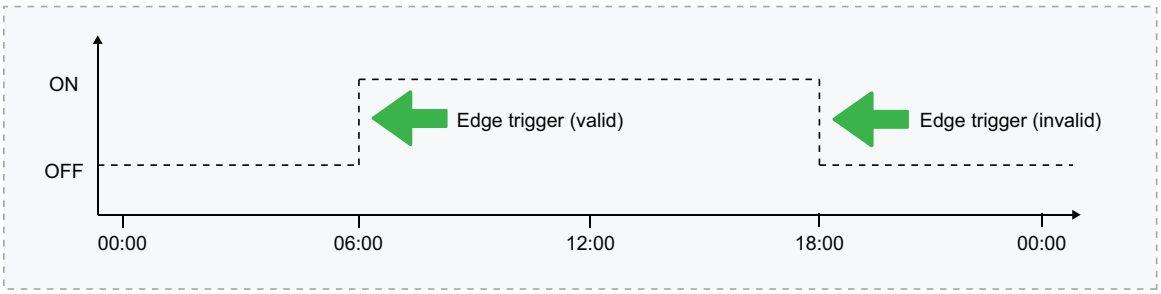
## Schedules | Holiday groups

Holiday groups allow a schedule to operate differently on holidays than normal days. This tab allows you to select which holiday groups will apply to a particular schedule by clicking **Add** and selecting items from the list.

Holiday groups can be programmed in **Sites | Holiday groups**.

## Edge Triggering

Objects that are programmed to change when a schedule changes are **edge triggered**. This means that by default they are only checked and changed when the schedule changes state.



For example, if a door is programmed to unlock by a schedule at 6:00am, it will only unlock at the point that the schedule becomes valid. If you assigned this schedule as the door's unlock schedule at 10:00am, that door will not unlock until 6:00am the following morning. This is because the trigger that unlocks the door only occurs when the schedule changes from invalid to valid.

In summary:

- Devices that are controlled by a schedule will be edge triggered by default.
- Edge triggering allows full manual control of the devices in between times.
- Edge triggering is only processed at the start and end of a period.
- If you program a device to follow a schedule, control will not take place until the next 'start' time passes.
- If you configure the device to always follow the schedule, the device state will immediately start following the schedule (for example, using the **Always check unlock schedule** in **Programming | Doors | Options**).
- When a device is configured to always follow the schedule, manual control of the device is no longer possible.

# 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.

## 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.

### 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.

### Overlapping Periods

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

## 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.

# Calendar actions

Calendar actions allow you to create door and output actions that override schedules for a specified duration. These actions can be set as one-offs or set to recur every day, week, month or year.

Output actions can be used to control other records such as areas, access levels and door types using the **Qualify output** feature (see page 77) or programmable functions.

For more information on the application of this function, refer to Application Note 179: Configuring Calendar Actions in Protege GX.

## Viewing Calendar Actions

1. Navigate to **Sites | Calendar actions**. This will display a calendar showing past and future calendar actions.
2. Use the navigation buttons to select the most useful calendar view:
   - **Today**: Displays the calendar actions occurring on the current day.
   - **Next 7 days**: Displays the calendar actions occurring over the next 7 days.
   - **Work week**: Displays the calendar actions occurring during a selected work week.
   - **Week**: Displays the calendar actions occurring during a selected week.
   - **Month**: Displays the calendar actions occurring during a selected month.
   - **Schedule view**: Displays calendar actions in a schedule view.
   - **List**: Displays calendar actions in a list.
3. Use the arrow keys or the scroll wheel on your mouse to navigate through the calendar. Move between weeks or months using the arrows in the upper left, or navigate with the calendar bar on the left side.

## Creating a Calendar Action

To create a calendar action, navigate to **Sites | Calendar actions**.

1. Select the day (and time where practical) when the calendar action should begin.
2. Click **New appointment**.
3. Enter the required details (see below).
4. Click **Save and close**.

You can open a calendar action to edit or delete at any time by double clicking it in the calendar view.

### General

- **Description**: The name or description of the calendar action.
- **Record group**: The record group that the calendar action belongs to.
- **Start/End Time**: Set the period when the calendar action will operate.

  The start and end times may be overridden by the recurrence options described below.
- **All day event**: With this option enabled the calendar action will operate for the entire day, from midnight to midnight.
- **List of devices**: Calendar actions can affect both doors and outputs, overriding any schedules or other factors which would normally control them. Click **Add** to add devices to the action. Select the **Device type**, then activate the required device(s) and click **OK**.

  Doors have the following action options:
  - **Lock**: The door is locked for the duration.
  - **Unlock latched**: The door is unlocked (but latched, i.e. closed) for the duration.

- **Extended lock time**: For the duration, whenever the door is unlocked by access the lock output will be activated for the time specified in the **Extended time** field (in seconds) rather than the normal **Lock activation time** (**Programming | Doors | Outputs**).

Outputs may be switched on or off by the calendar action. This may be used alongside programmable functions and schedules to control other parts of the system, such as area arming.

## Recurrence

Click the **Recurrence** button to open the Activity Recurrence window. As the recurrence options are configured, a field at the bottom of the window describes the pattern of recurrence.

- **Activity time**: Set the start time, end time and/or the duration of the calendar action. These settings override those in the **General** programming.
- **Recurrence pattern**: Set how often the calendar action will recur, based on daily, weekly, monthly or yearly recurrence. Each frequency include further options to more precisely when the event will recur.
- **Range of recurrence**: Set the start date when the calendar action will become enabled. You can set no end date, a specific end date, or a fixed number of occurrences.

# Holiday groups

Holiday groups are used to disable (or enable) schedule periods during a holiday. Holiday groups can be assigned to schedules in **Sites | Schedules | Holiday groups**.

For more information, see Configuring Schedules and Holidays (page 78).

## Holiday groups | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

## Holiday Groups | Holidays

Click **Add** to add holidays to the group.

- **Name**: The name of the holiday.
- **Repeat**: When this option is enabled the holiday will recur on an annual basis.

  Keep in mind that some holidays recur on the same day every year (e.g. Christmas), while others occur on different days (e.g. Easter). It is useful to program holidays several years in advance.

- **Start date**: The first day of the holiday.
- **End date**: The final day of the holiday.

  To create a single-day holiday, select the same end date as the start date. For example, to create a 24 hour holiday period for new years' day you would set both the start and end date to January 1st.

# Controllers

The Protege GX controller is the central processing unit of the Protege GX system. The controller communicates with all system modules, stores all configuration and transaction information, processes all system communication, and reports alarms and events to the Protege GX server.

## Controllers | General

### General

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

  Some record types, such as outputs, inputs, trouble inputs and expander modules, inherit the record group assigned to the controller.

### Communications

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

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

  Programming the IP address, subnet mask, and default gateway requires knowledge of the network and subnet that the system is connected to. You should always consult the network or system administrator before programming these values.
- **Dynamic IP address update**: When this option is enabled the software automatically detects the IP address of the controller from incoming messages and updates the **IP address** field automatically. Use this for situations where the controller's IP address may change unexpectedly, or when the controller is configured to use DHCP.
- **Username / Password**: If the single record download service is in use, you must enter a username and password for the controller so that the service can make a connection. These must match an operator in the controller's web interface.

  Ensure that the **Username** is entered in all lowercase letters, otherwise the connection will fail.

  These fields are not required when the single record download service is not in use.
- **Download port**: The TCP/IP port that is used by the download service to send programming downloads to the controller. By default, this is port 21000.
- **Single record download port**: The TCP/IP port that will be used by the single record download service (if in use) to send programming downloads to the controller. This should match the **HTTPS Port** of the controller. By default, this is port 443.
- **Download server**: Defines the download server which will send downloads to the controller. If this field is <not set> the controller will not receive any downloads.
- **Control and status request port**: This field specifies the port that will be used to send manual commands and status requests to the controller over TCP/IP. By default, this is port 21001.

- **Last known IP address**: Shows the last IP address that the controller used to communicate with the server (read only).
- **Last downloaded**: Shows the date and time of the last download to the controller (read only).

### Display

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

### Diagnostic windows

- **Open download server diagnostic window**: Opens a window listing transactions between the controller and the download server. This can be useful for checking whether recent programming changes have been downloaded successfully.

  This window is not used for the enterprise download server. Navigate to **Global | Diagnostics | Downloads** instead.

- **Open event server diagnostic window**: Opens a window showing the current status of the event server. This can be useful for diagnosing controller connection issues.

### Commands

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

### Download binary blob

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

  Do not use this feature unless specifically advised by ICT.

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

### Record history

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

## Controllers | Configuration

### Configuration

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

  When the **Test report time is periodic** option is enabled in the **Options** tab, the time programmed will be used as a period between reports in hours and minutes. Otherwise it is treated as a time of day.

- **Automatic offline time**: The time of day when the controller will update the users and other offline parameters on legacy intelligent expander modules. The **Enable automatic offline download** option must be enabled. This option is not used for DIN rail modules.
- **AC restore delay time**: The time, in seconds, that the AC Failure trouble input will remain open after an AC failure before restoring. This setting is only relevant to legacy hardware which is supplied by an AC power source.
- **AC fail time**: The time, in seconds, that the AC mains voltage must have failed before the AC failure trouble input will be opened. This setting is only relevant to legacy hardware which is supplied by an AC power source.

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

  After changing this port you must restart the controller for the setting to take effect.

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

- **Modem country**: This option affects the number of dial attempts made by phone line reporting services, and may override the **Dial attempts** setting in the reporting service. It is recommended to test the number of dial attempts to ensure that you comply with regional requirements.

  This setting is only supported by controller models with onboard modem dialers.

- **Modem backup phone number**: If ethernet communication fails, the controller's onboard modem will dial this number to report events. The **Module backup if IP fails** option must be enabled (**Options** tab).

  This setting is only supported by controller models with onboard modem dialers.

- **Default language**: The default language displayed on the keypad for users who have no language selected and for any events generated by a serial printer service (see **Programming | Services | Serial printer**).
- **Download retry delay**: This field allows you to set a minimum delay period (in seconds) between downloads to this controller. After the download server has completed a download it will not attempt to download to this controller again until the delay has elapsed, except in the following circumstances where the download server will send the download as soon as possible without waiting for the delay period:
  - When a **Force download** command is sent
  - When changes are made to hardware devices that are hosted by the controller (e.g. expanders, inputs, outputs)
  - When the single record download service triggers a full download

  The minimum retry delay is 10 seconds.

- **Register as reader expander**: The module address assigned to the controller's onboard reader expander. You can program the onboard reader expander by creating a record with the same address in **Expanders | Reader expanders**.

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

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

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

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

### Encryption

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

### HTTPS public key

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

### Version 3 settings

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

## Controllers | Configuration (Integrations)

The following integration settings are available on the **Configuration** tab.

### Elevator HLI

**Elevator HLI type**: Defines the elevator system that the controller is integrating with using an HLI (High Level Interface). Different options are available depending on which elevator system is selected. Choose from:

- **KONE**: For more information, see Application Note 170: Protege GX KONE HLI Integration.
  - **Network adaptor**: Only Cable is supported for this integration.
  - **Primary port**: The TCP/IP port for communication with the primary KONE group controller.
  - **Secondary port**: The TCP/IP port used for communications with the secondary (backup) KONE group controller.
  - **Primary IP address**: The IP address of the primary KONE group controller.
  - **Secondary IP address:** The IP address of the secondary (backup) KONE group controller.
  - **Default DOP source floor group**: This floor group contains all of the floors which have a KONE DOP that can be used to call elevators. This defines all of the floors that an elevator can depart from (i.e. source floors). This option applies when the KONE system is online with the controller.

    This option does not account for the **Schedule** setting in the floor group programming.
  - **Default DOP destination floor group**: This floor group contains all of the floors which can be freely accessed at all times from a KONE DOP. This defines floors that an elevator can travel to (i.e. destination floors). This option applies when the KONE system is online with the controller.

    This option does not account for the **Schedule** setting in the floor group programming. Floor groups with schedules can be applied to individual DOP records in **Programming | Doors | General**.
  - **Default COP destination floor group:** This floor group contains all of the floors which can be freely accessed at all times from a KONE COP. This defines floors that an elevator can travel to (i.e. destination floors). This option applies when the KONE system is online with the controller.

    This option does not account for the **Schedule** setting in the floor group programming. Floor groups with schedules can be applied to individual COP records in **Programming | Doors | General**.

- **Default DOP disconnection source floor group:** This floor group contains all of the floors with a KONE DOP that can be used to call elevators while the KONE system is disconnected from the controller. This defines all of the floors that an elevator can depart from during a communication failure (i.e. source floors).
- **Default DOP disconnection destination floor group:** This floor group contains all of the floors which can be freely accessed from a KONE DOP while the KONE system is disconnected from the controller. This defines floors that an elevator can travel to during a communication failure (i.e. destination floors).
- **Default COP disconnection destination floor group:** This floor group contains all of the floors which can be freely accessed from a KONE COP while the KONE system is disconnected from the controller. This defines floors that an elevator can travel to during a communication failure (i.e. destination floors).
- **Enable elevator call functionality**: Enables the KONE Remote Call Giving Interface (RCGIF) functionality. Using this interface, a user can badge their card to summon an elevator which will automatically take them to the **Elevator destination floor** set in their access level (**Users | Access levels | General**).
  - **RCGIF primary port**: The TCP/IP port on which the primary RCGIF KONE controller is listening.
  - **RCGIF secondary port**: The TCP/IP port on which the secondary (backup) RCGIF KONE controller is listening.
  - **RCGIF primary IP**: The IP address of the primary RCGIF KONE controller.
  - **RCGIF secondary IP**: The IP address of the secondary (backup) RCGIF KONE controller.
- **Elevator HLI debug:** When this option is enabled, all HLI packets sent and received via ethernet are viewable using a telnet terminal. This should be used for troubleshooting only, and disabled during normal operation.

  To view HLI packets, set up a serial printer service in **Programming | Services** and open a telnet session to the configured port. When packets are exchanged between the Protege GX controller and the KONE controller the data received will be echoed to the telnet window.

  Although some of the information is displayed in plain English, much of the data requires a low level understanding of the KONE protocol.

- **ThyssenKrupp**: For more information, see Application Note 169: Protege GX ThyssenKrupp HLI Integration.
  - **Network adaptor**: Only Cable is supported for this integration.
- **OTIS**: For more information, see Application Note 174: Protege GX Otis Compass HLI Integration.
  - **Network adaptor**: Only Cable is supported for this integration.
  - **Lowest basement floor**: The lowest physical underground floor accessible by an elevator. For example, if there are five underground floors the value should be 5. If there are no underground floors, set to 0.

    What is considered an underground floor is determined by the elevator system configuration.
- **Schindler**: For more information, see Application Note 196: Protege GX Schindler HLI Integration.
  - **Network adaptor**: Only Cable is supported for this integration.
  - **Port system primary IP**: The primary IP address of the Schindler server.
  - **Port system secondary IP**: The secondary IP address of the Schindler server (backwards compatible configuration).
  - **Online database port**: The TCP port of the Schindler online database interface.
  - **Call interface port**: The TCP port of the Schindler call interface.
  - **Life reporting interface port**: The TCP port of the Schindler life reporting interface.
  - **Lowest basement floor**: The lowest physical underground floor accessible by an elevator. For example, if there are five underground floors the value should be 5. If there are no underground floors, set to 0.

    What is considered an underground floor is determined by the elevator system configuration.
  - **Default floor group**: The floor group containing all accessible floors and the schedules used to control when each floor can be freely accessed.

    This floor group can be created in **Groups | Floor groups**.
  - **Enable call interface**: Enables the Schindler call interface.

- **Enable life reporting interface**: Enables the Schindler life reporting interface.
- **Enable elevator HLI debug:** When this option is enabled, system debug messages will be logged in the event log for troubleshooting.

  This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.

- **Site code formats**: Defines the facility numbers and formats of user credentials which will be sent to the Schindler system. Site code formats are only necessary if Schindler readers and credentials are being used for this integration
  - **Site code**: The site code or facility number of the user credentials that will be formatted.
  - **Format**: All credentials that match the **Site code** defined above will be converted to this format and sent on to the Schindler system.
  - **Sub format**: Set to 0 by default. Only relevant when the **Format** is set to Unknown Wiegand.

  For a list of supported Schindler formats, see Application Note 196: Protege GX Schindler HLI Integration.

- **MCE**: For more information, see Application Note 241: Protege GX MCE Elevator Integration.
  - **Network adaptor**: Only Cable is supported for this integration.
  - **MCE sentry IP**: The IP address of the MCE Sentry interface that the controller is connected to.
  - **MCE sentry port**: The TCP port that the controller and MCE Sentry interface will use to communicate.
  - **Default floor group**: A floor group including all floors accessible by the MCE system, as well as their unlock schedules. This is used as the MCE system's building security map.
  - **Enable elevator HLI debug:** When this option is enabled, system debug messages will be logged in the event log for troubleshooting.

    This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.

**Restart HLI**: Restarts the elevator HLI service.

## Input expander integration

**Integration type**: Defines the input expander integration the controller is used for. Choose from:

- **Redwall**: For more information, see Application Note 181: Protege GX Redwall Integration.
  - **Port**: The UDP port the controller uses to receive Redwall event codes.
  - **Module integration port**: The port used for communication between the Redwall scanner and the Protege GX controller when the scanner is acting as a Protege input expander.
  - **Enable Redwall debug**: When this option is enabled, system debug messages will be logged in the event log for troubleshooting.

    This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.

- **Inovonics**: For more information, see Application Note 183: Protege GX Inovonics Integration.
  - **Port:** Defines the TCP port that the controller uses to receive Inovonics event codes. This must be set to port 80.
  - **Module integration port:** Defines the UDP port that the integration uses to listen for replies to requests from Protege GX. This must be set to port 9452.
  - **Inovonics IP address:** The IP address of the Inovonics ACG unit the Protege GX controller is connected to.
  - **Inovonics password:** The password used by the controller when it attempts to access information from the Inovonics ACG. The controller must log in as an administrator, so ensure that the password entered is the administrator password used for the ACG.

### VingCard VisiOnline integration

VingCard VisiOnline integration is a separately licensed feature. For more information, see Application Note 215: Protege GX VingCard VisiOnline Integration.

- **Enable integration**: Select this option to enable VingCard VisiOnline integration for this controller.
- **IP address**: The IP address of the VingCard server.
- **Restart integration**: Click to restart VingCard Visionline integration.
- **Port**: The TCP port of the VingCard server. This is set to 443 by default.
- **Username**: The username of the account to be used to connect to the VingCard server.
- **Password**: The password of the account to be used to connect to the VingCard server.
- **VingCard Visionline encoder**: The name of the encoder to be used to program cards within the VingCard server.
- **Enable integration debug**: When this option is enabled, system debug messages will be logged in the event log for troubleshooting.

  This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.

## Controllers | Options

### Options

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

  Users must have **Acknowledge system troubles** enabled in **Users | Users | Options** and access to the **View (5)** menu from their menu group.
- **Generate input restore on test report input**: When this option is enabled the controller will generate a restore event for the Service Report Test trouble input closing after the regular test report. This occurs one minute after the Service Report Test trouble input has been activated.
- **Report short duration module communication failure**: When this option is enabled the controller will always generate trouble events for any module communications failure, without allowing any grace period for the module to come back online.
- **Advance UL operation**: When this option is enabled the Protege GX system runs in UL compliance mode.

  This setting has the following effects:
  - Adds a 10 second grace period following a failed poll before a module is reported as offline.

    Each module sends a poll message to the controller every 250 seconds. The module will be reported as offline if no poll has been received for the duration of this poll time plus the 10 second grace period.
  - Suppresses reporting of all alarms and/or reportable events to a monitoring station within the first two minutes of the controller powering up. The system will continue to send poll messages as usual.

- Reports 'Input Tamper' events as 'Input Open' events when the area that the input is assigned to is armed. If the area is disarmed an 'Input Tamper' message will be sent.
- Limits the **Dial attempts** for reporting services to a maximum of 8.

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

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

### Misc options

- **Enable automatic offline download**: When this option is enabled the controller will automatically update the users and other offline parameters on legacy intelligent expander modules at the **Automatic offline time** (**Configuration** tab). This option is not used for DIN rail modules.
- **Modem backup if IP fails**: When this option is enabled the controller will dial out through the onboard modem if it cannot connect to the software via ethernet to report events. The **Modem backup phone number** must be set in the **Configuration** tab.

This setting is only supported by controller models with onboard modem dialers.

- **Backup only alarm events**: With this option enabled, when the controller has lost ethernet connection it will only report alarms and other reportable events over the phone line. All stored events will be reported when the ethernet link is restored.

This setting is only supported by controller models with onboard modem dialers.

- **Invert controller tamper input**: When this option is enabled the controller will invert the module tamper input allowing a normally open tamper switch to be used. This setting is only relevant to older hardware which includes an onboard tamper input.
- **Log all access level events**: This is a legacy option that has no effect.
- **Do not wait for dial tone when modem dials out**: When this option is enabled, modem dialing occurs even when no dial tone is detected.

This setting is only supported by controller models with onboard modem dialers.

## Controllers | Time update

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

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

## Controllers | Custom reader format

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

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

### Custom reader configuration

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

### Parity 1-4 options

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

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

- **Parity type 1-4**: The method of calculating the parity for the block. This is either even or odd parity.
- **Parity location 1-4**: The position of the parity bit in the received data. The count starts at zero.
- **Parity start 1-4**: The index where the parity block starts in the received data. The count starts at zero.
- **Parity end 1-4**: The index where the parity block ends in the received data. The count starts at zero.

### Bit options

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

- **Set bit 1-4**: The index of a set bit (a logical '1') in the received data. The count starts at zero.
- **Clear bit 1-4**: The index of a clear bit (a logical '0') in the received data. The count starts at zero.

### Card data options

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

  For more information, see the relevant application note for your integration.

  This field sets the card data AES encryption key for all reader ports associated with this controller.

## Manual Controller Commands

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

### Set controller date time

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

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

## Update modules

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

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

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

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

## Force download

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

An operator can use the **Force download** command to increase the priority of a specific controller, so that it will be next in line after the previous controller has been completed. The **Download retry delay** period will be ignored so that the download is sent as soon as possible.

In addition, the download service will download to the controller even if no changes are detected.

## Get health status

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

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

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

## Module addressing

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

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

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

### Setting Module Network Addresses

1. Ensure the controller is correctly powered and is communicating with the Protege GX software.
2. Connect the module(s) that require addressing to the module network. Make sure the power light on each module is on and that the status indicator begins flashing rapidly.
3. Allow some time for the module(s) to attempt to register with the controller.

- If the module has the default address of 254 or has the same address as another module the fault indicator will begin flashing an error code.
- If the module has been previously addressed and is not a duplicate then it will succeed in registering and the status indicator will begin flashing at 1 second intervals.

4. Once all modules have completed the registration process (successful or not), open the Protege GX software and navigate to **Sites | Controllers**.
5. Right click on the controller record and select **Module addressing** to open the module addressing window. This window displays all of the modules that are connected to the controller with the following information:
   - The module type (e.g. controller, keypad, etc.)
   - The serial number
   - Current firmware version and build number
   - The current module address
   - Whether the module address can be changed (for example, the controller's address cannot be changed)
   - Whether the module has successfully registered with the controller
   - Whether the module is currently online

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

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

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

### Maximum Module Addresses

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

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

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

## Update firmware

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

### Before Upgrading Firmware

- This process will take approximately 10 minutes per controller and it is recommended that firmware updates are performed when the site is closed for maintenance or at times of low activity. The controller will not be able to perform its normal function while firmware is being updated.
- Ensure that the controller does not lose power during the firmware upgrade process.
- Ensure that there is a stable network connection between the controller and the Protege GX server before you begin upgrading the firmware. If the network connection is unstable, we recommend upgrading locally from the controller's web interface.
- Controllers do not support defaulting and firmware upgrade at the same time. Before you upgrade the controller firmware, ensure that the wire link used to default the controller is **not** connected.
- We strongly recommend having a technician on site during the firmware upgrade process to respond to any issues that might arise.

Losing power or network connection during the upgrade process or upgrading with a default link connected can cause the controller to become inoperable.

### Upgrading the Firmware

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

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

# Adding a Controller

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

- **Use the controller wizard**: The controller wizard allows you to specify the inputs, outputs, doors and expander modules that are required by your site. Some additional options can also be configured. The selected default records are automatically added to the database with the controller.
- **Just add a controller**: Only the controller record itself is added to the database. All other records must be programmed separately.

- **Add new controller based on an existing controller**: The controller record and all connected programming are duplicated from an existing controller. This includes devices such as expander modules, inputs, outputs and doors.

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

Once the controller record has been created, bring it online by entering the **Serial number**, **IP address**, **Download port**, **Download server** and **Control and status request port** in the **General** tab. If the controller does not come online you will need to troubleshoot the connection (see page 35).

## Adding a Controller with Default Records

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

### General

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

### Controller

- **Cross controller group**: If this controller will use cross controller operations to share resources with other controllers, select the **Cross controller group** it belongs to.

  Only available in systems that use the enterprise download server. For more information, see **Sites | Cross controller groups**.

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

  Not all controller inputs may be required if the onboard reader expander is being used, as the inputs can be assigned to the reader expander record.

- **Outputs**: The number of onboard outputs that will be created for the controller. This is set automatically based on the **Type** of controller selected.

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

  Controller output 2 only exists on legacy hardware. This address is skipped when the wizard automatically adds the default records.

- **Add trouble inputs**: Enable this option to automatically add the trouble inputs associated with the controller.

### Keypads, Input expanders, Reader expanders, Output expanders and Analog expanders

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

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

### Options

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

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

### Doors

- **Doors**: Automatically creates the defined number of door records. Typically this should be 2 doors per reader expander.
- **Assign to reader expanders**: Automatically assigns the doors to reader expander ports, in order of creation.
- **Add door trouble inputs**: Creates the relevant trouble inputs for each door record.
- **Assign reader lock output to door configuration**: Automatically sets the **Lock output** for each door to the relay output on the associated reader expander.
- **Assign reader beeper to door alarm configuration**: Automatically sets the **Pre alarm output**, **Left open alarm output** and **Door forced output** for each door to the beeper output on the associated reader expander.

## Adding a Controller Based on an Existing Controller

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

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

The new controller record will have a blank **Serial number**, **IP address** and **Download server**.

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

  If the original records included the controller's name, this name will still be included in the new records (i.e. will not be replaced by the new name).
- **Copy access levels**: When this option is enabled the access levels of the original controller are copied for the new controller. The new access levels are assigned the equivalent doors, areas and other records from the new controller, but are not assigned to any users.
- **Copy global records**: When this option is enabled, site-wide records such as schedules and function codes will be copied for use with the new controller.

# Cross controller groups

Cross controller groups allow you to group together controllers that can share resources such as inputs, outputs, doors, areas and services. For example, two controllers in the same group might share control of an area, or one controller might host a reporting service that is used by several others in the same cross controller group.

Any controllers that are not in a cross controller group are standalone controllers, and can only use the inputs, outputs and other resources connected to that controller.

In systems that use the Protege GX Enterprise Download Server, you can create explicit cross controller groups in **Sites | Cross controller groups**. This allows you to assign resources from one controller to other controllers in the same group. The user interface will prevent you from linking controllers that do not belong to the same cross controller group.

Systems that use the standard Protege GX Download Server do not use explicit cross controller groups, so the **Sites | Cross controller groups** page is not available. Instead, the system creates implicit cross controller groups based on existing programming. For more information, see Application Note 180: Protege GX Cross Controller Operations.

**Cross Controller Group Rules**

The programming rules for cross controller groups are:

- All controllers that use cross controller operations must be in a cross controller group.
- Controllers that do not use cross controller operations do not need to be in a cross controller group.
- Each controller can only be in one cross controller group.
- For best performance, we recommend a maximum of **48** controllers per cross controller group. There is a strict upper limit of 64 controllers per group.
- All controllers in the same group must be networked so they can communicate with each other. If the controllers cannot communicate, they will suffer performance issues.

In general, we recommend that cross controller groups should only be used when needed, as unnecessary cross controller operations can impact the performance of all controllers.

For complete information about this feature, see Application Note 180: Protege GX Cross Controller Operations.

## Cross controller groups | General

Only available in systems that use the Protege GX Enterprise Download Server.

### General

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

### Controllers

Click **Add** to assign controllers to the group. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

All controllers in the same cross controller group can share resources such as inputs, outputs, doors, areas and services.

## Record history

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

# Biometric readers

Protege GX can be integrated with biometric identification systems, allowing you to use biometric credentials such as fingerprints and facial recognition to grant access to doors.

Biometric reader integrations are a separately licensed feature. For more information, see Application Note 264: Suprema Biometrics Integration with Protege GX and Application Note 297: Princeton Biometric Integration with Protege GX.

## Biometric readers | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **IP address**: The IP address of the biometric reader.
- **IP port**: The port that will be used to communicate with the biometric reader.
- **Type**: The brand of biometric reader.
- **Secondary type**: The secondary or sub-type of biometric reader, where applicable. For the Suprema integration this indicates whether the Suprema system uses Biostar 1 (Version 1) or Biostar 2 (Version 2).
- **Automatically download users to this reader**: When enabled, the download server will download users to the reader automatically. Disable this option if you don't want users to be downloaded. For example, if the reader is only used for enrolling (capturing fingerprints) and is not attached to a door for access.

### Record history

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

# Security levels

Security levels define the access an operator has within the Protege GX system. You can add security levels to roles in **Global | Roles | Security levels** to more precisely control what individual operators can see or do, or limit operators to particular record groups. Permissions granted in a security level override those granted in the role.

For more information and programming examples, see Application Note 191: Programming Operator Roles in Protege GX and Application Note 247: Using Record Groups in Protege GX.

## Security levels | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

## Security levels | Tables

The Tables tab determines the permissions that each security level has for programming menus and other features in the system. The permissions granted or denied here can be used to override those assigned in the roles programming.

For each table, select one of the following options:

- Inherit from role to retain the permissions from the role that this security level is assigned to.
- Deny to prevent access to the data contained in the table. This hides any functions and menu options for that table from the operator.
- Grant full access to grant full read/write permissions to the table.
- Grant read only access to grant access to view but not to update data in the table. The operator will be able to view the relevant settings but the options for updating them are disabled.

## Security Level Table Reference

This reference table contains the following information:

- The menu items and other features that each security level table provides access to.
- The parent role table that each security level table inherits from.

| Table | Permissions | Parent Role Table |
|---|---|---|
| Access levels | • Users \| Access levels | Access levels |
| Actions | Not used - see **Event filters**. | |
| Alarm priorities | Not used - see **Event filters**. | |
| Alarms | Not used - enable **Alarms** in the role. | |
| Analog expanders | • Expanders \| Analog expanders | Controller programming windows |

| Table | Permissions | Parent Role Table |
|---|---|---|
| Apartments | • Programming \| Apartments<br>• Programming \| Batch add apartments | Apartments |
| Area groups | • Groups \| Area groups | Controller programming windows |
| Areas | • Programming \| Areas | Controller programming windows |
| Automation | • Automation \| Automation | Controller programming windows |
| Bit data values | Not used. | |
| Calendar actions | • Sites \| Calendar actions | Calendar actions |
| Cameras | • Monitoring \| Setup \| Cameras | Cameras |
| Card profiles | • Sites \| Card profiles | Card profiles |
| Cross controller groups | • Sites \| Cross controller groups | Cross controller groups |
| Controllers | • Sites \| Controllers<br>Grants access to perform all controller manual commands except for setting the date/time (see **Manual commands** tab). | Controller programming windows |
| Credential types | • Sites \| Credential types | Credential types |
| Custom fields | • Users \| Custom fields<br>• Users \| Custom field tabs | Custom fields |
| Data values | • Automation \| Data values | Controller programming windows |
| Daylight savings | • Programming \| Daylight savings | Controller programming windows |
| Door groups | • Groups \| Door groups | Controller programming windows |
| Door types | • Programming \| Door types | Controller programming windows |
| Doors | • Programming \| Doors | Controller programming windows |
| DVRs | • Monitoring \| Setup \| DVRs | Cameras |
| Elevator cars | • Programming \| Elevator cars | Controller programming windows |
| Elevator groups | • Groups \| Elevator groups | Controller programming windows |
| Event filters | • Events \| Event filters<br>• Events \| Actions<br>• Events \| Alarm priorities | Event reports |
| Event groups | Not used. | |

| Table | Permissions | Parent Role Table |
|---|---|---|
| Event logs | • Salto \| Salto log<br>Requires access to **Salto programming windows** in the role. | Event logs |
| Event reports | • Reports \| Event<br>• Reports \| Central station report<br>• Reports \| Setup \| Event | Event reports |
| Filters | Not used. | |
| Floor groups | • Groups \| Floor groups | Controller programming windows |
| Floor plans | • Monitoring \| Floor plan view<br>• Monitoring \| Setup \| Floor plan editor<br>• Monitoring \| Setup \| Floor plan editor (batch)<br>• Monitoring \| Setup \| Add bulk floor plans | Floor plans |
| Floors | • Programming \| Floors | Controller programming windows |
| Function codes | • Sites \| Function codes | Function codes |
| Generate PINs | Grants access to program user PIN codes. Also requires access to the **Users** table. | Users |
| Holidays | • Sites \| Holiday groups | Holidays |
| Input expanders | • Expanders \| Input expanders | Controller programming windows |
| Input types | • Programming \| Input types | Controller programming windows |
| Inputs | • Programming \| Inputs | Controller programming windows |
| Intercoms | • Monitoring \| Setup \| Intercoms | Intercoms |
| Jobs | Not used. | |
| Keypad groups | • Groups \| Keypad groups | Controller programming windows |
| Keypads | • Expanders \| Keypads | Controller programming windows |
| Menu groups | • Groups \| Menu groups | Controller programming windows |
| Modems | Not used. | |
| Muster reports | Not used - enable **Muster reports** in the role. | |
| Output expanders | • Expanders \| Output expanders | Controller programming windows |
| Output groups | • Groups \| Output groups | Controller programming windows |
| Outputs | • Programming \| Outputs | Controller programming windows |

| Table | Permissions | Parent Role Table |
|---|---|---|
| Phone numbers | • Programming \| Phone numbers | Controller programming windows |
| PhotoID | • Users \| Card template editor | Card template editor |
| Programmable functions | • Automation \| Programmable functions | Controller programming windows |
| PTZ setup | • Monitoring \| Setup \| PTZ commands<br>Requires access to cameras or DVRs. | Cameras |
| Reader expanders | • Expanders \| Reader expanders | Controller programming windows |
| Record groups | • Sites \| Record groups | Record groups |
| Record history | Not used. | |
| Salto calendars | Not used - enable **Salto programming windows** in the role. | |
| Salto door groups | Not used - enable **Salto programming windows** in the role. | |
| Salto doors | Not used - enable **Salto programming windows** in the role. | |
| Salto outputs | Not used - enable **Salto programming windows** in the role. | |
| Salto time periods | Not used - enable **Salto programming windows** in the role. | |
| Scheduled user imports | Not used. | |
| Schedules | • Sites \| Schedules | Schedules |
| Security levels | • Sites \| Security levels | Security levels |
| Services | • Programming \| Services | Controller programming windows |
| Smart readers | • Expanders \| Smart readers | Controller programming windows |
| Status definitions | Not used. | |
| Status lists | • Monitoring \| Setup \| Status lists | Available by default. |
| Status pages | • Monitoring \| Status page view<br>The role must also have access to view the status lists, event reports and other objects on the status page.<br>• Monitoring \| Setup \| Status page editor<br>• Monitoring \| Setup \| Status page editor (batch) | Status pages |
| Status table | Not used. | |
| Time and attendance | • Reports \| Attendance report<br>• Reports \| Central station report<br>• Reports \| Setup \| Attendance<br>• Reports \| Setup \| Shift types | Attendance reports |

| Table | Permissions | Parent Role Table |
|---|---|---|
| Trouble inputs | • Programming \| Trouble inputs | Controller programming windows |
| User reports | • Users \| User search<br>• Reports \| User<br>• Reports \| Central station report<br>• Reports \| Setup \| User | User reports |
| Variables | • Automation \| Variables | Controller programming windows |
| Web links | • Monitoring \| Web links | Status pages |
| Workstations | • Events \| Alarm routing<br>• Events \| Workstations<br>• Events \| Workstation groups | Available by default to Administrator and Installer presets. |

## Security levels | Manual commands

Manual commands enable an operator to manually control a device from within the Protege GX software: for example, right clicking on a door and unlocking it from a floor plan. These settings define the specific manual commands that are available to operators with this security level assigned.

For each command, choose from Inherit (from the role), Allow or Deny.

### Security Level Manual Command Reference

This reference table contains the following information:

- The menu items and other features that each manual command option refers to.
- The parent role table that each option inherits from.

| Setting | Permissions | Parent Role Table |
|---|---|---|
| Area control | All commands for areas (e.g. arming/disarming) | Manual commands |
| Door control | All commands for doors (e.g. locking/unlocking) | Manual commands |
| Elevator control | Locking and unlocking floors in elevators. | Manual commands |
| Keypad control commands | Module update command for keypads | Manual commands |
| Output control commands | Activating and deactivating outputs | Manual commands |
| Input control | Bypassing inputs and removing bypasses | Manual commands |
| Restart and stop services | Stopping and starting services | Manual commands |
| Reset user commands | Reset antipassback command for users | Manual commands |
| Update module commands | Module update command for all expander types | Manual commands |
| Variable control | Updating variables from a floor plan | Manual commands |
| Programmable function control | Stopping and starting programmable functions | Manual commands |
| Update controller time | Setting controller date/time | Manual commands |
| Change audit opening in the keys | Edit the **Audit on keys** setting for Salto locks and user records. | Salto programming windows |
| Allegion commands | Locking and unlocking Allegion doors | Manual commands |

# Record groups

Record groups enable a site to be divided into functional groups, which can be used to restrict operator access using roles and security levels. They also facilitate sorting, searching and reporting of large numbers of records. This is ideal for large systems where it may be practical to group records by building, branch or region.

Most record types in the Protege GX system allow you to assign a record group to each individual record. Other records such as outputs, inputs, trouble inputs and expander modules cannot be assigned an individual record group, and instead inherit the record group assigned to the controller.

For programming examples, see Application Note 247: Using Record Groups in Protege GX.

## Record groups | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Parent record Group**: Assign another record group which will act as the 'parent' to this one. Everything that is included in a child record group will be included in the parent record group, and multiple child groups can be assigned to a parent.

  This allows you to create a hierarchy of record groups. For example, a regional manager may be able to see records from multiple branches (each with their own record group), while the global manager can access records from every region.

### Record history

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

## Record groups | Custom data

### Custom data

- **Numeric data**: A number that identifies the record group. This information is included in the XML schema for record groups, and can be used to identify the record group in custom third-party integrations.
- **Text data**: A text string that identifies the record group. This information is included in the XML schema for record groups, and can be used to identify the record group in custom third-party integrations.

# Credential types

Credential types enable the Protege GX system to use a variety of custom data types - such as license plate, bar code, QR code, biometric or custom Wiegand credentials - to identify users. When data is sent to Protege GX from a third-party system (via either RS-485 or ethernet), a credential type can be used to interpret that data as a specific user credential.

For example, a third-party LPR (License Plate Recognition) system might send ASCII data to Protege GX, which will use the credential type programming to 'translate' that data into particular license plates.

Credential types can be applied to custom door types as the **Entry/Exit reading mode** (**Programming | Door types | General**). In addition, the **Reader format** must be set to Custom credential in the reader expander port or smart reader that is receiving the credential data. Specific credentials can be entered against user records under **Users | Users | General**.

For more information, see Application Note 276: Configuring Credential Types in Protege GX.

## Compliance types

Compliance types are a specific implementation of credential types which allow you to control access based on any custom compliance requirement that can be entered against a user. For example, access might be controlled based on health and safety induction, driver's license or current industry certification status.

Compliance types can provide hard or soft access failure, along with warning or expiry messages that must be acknowledged, allowing you to build up a record of compliance issues on site.

For more information and programming examples, see Application Note 286: Programming Compliance Types in Protege GX. Warning and expiry messages require a compatible ICT Touchscreen Card Reader.

# Credential types | General

## General

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

## Configuration

- **Format**: The data that is sent to the Protege GX controller by the third-party device. Supported formats include:
  - **Unicode**: The credential data sent to the controller uses two bytes to represent each character as per the Unicode standard.
  - **UTF8**: The credential data sent to the controller uses a variable number of bytes to represent each character as per the UTF-8 standard.
  - **ASCII**: The credential data sent to the controller uses a single byte to represent each character as per the ASCII standard.
  - **Numeric**: The credential data sent to the controller is a binary number composed of up to 8 bytes. The bytes are ordered using little endian.

- **Hexadecimal**: The credential data is sent to the controller as an array of binary numbers. When the specific credential is entered into the user programming for each user, the format used is hexadecimal with the numbers 0-9 and letters A-F representing each nibble of the credential.
- **Wiegand**: The credential data sent to the controller or reader expander is composed of a Wiegand bit stream.

  This bit stream can be encoded in numerous different ways and a format descriptor must be included in the **Wiegand or TLV format** field. For the Wiegand format the preceding, trailing and prefix character settings and case sensitive setting are ignored.
- **TLV**: This option is reserved for future development.
- **Compliance**: A special credential type that allows you to use custom requirements such as health and safety certificates, driver's licenses and industry qualifications as credentials. This credential type can be used with controllers and reader expanders. Compliance types have different settings from regular credential types.

Controllers support all credential type formats via either RS-485 or ethernet. Reader expanders only support Wiegand credential types.

- **Preceding characters**: The maximum number of characters that may be ignored at the start of the data packet received by the controller. If the credential is found before this number of characters is counted it will still be accepted.

  This setting is determined by the third-party device/application.
- **Trailing characters**: The maximum number of characters that may be ignored at the end of the data packet received by the controller. If there are fewer than this number of trailing characters after the credential is found the credential will still be accepted.

  For example, this field may be set to 1 to ensure that credentials will be accepted even if they are followed by a carriage return character.

  This setting is determined by the third-party device/application.
- **Prefix**: The characters that are required at the start of the credential data packet sent to the controller.

  This setting is determined by the third-party device/application.
- **Case sensitive**: Defines whether or not the data is case sensitive.

  This setting is determined by the third-party device/application.
- **Wireless locking**: Enable this setting to use this credential type with Protege offline wireless locks. For more information, see the Protege Offline Wireless Lock Configuration Guide.
- **Unique value**: When this option is enabled, duplicate credentials are not allowed (i.e. two users may not have the same credential). When disabled, duplicate credentials are permitted.

  If non-unique credential values are permitted, ensure that any door type using this credential type also requires a unique credential (e.g. card) for two-factor authentication so that Protege GX can accurately identify the user requesting access.
- **Credential limit per user**: This option allows you to restrict the number of credentials that can be added to each user through the Protege GX software. The credential limit is set to Unlimited by default, and can be restricted to a number from 1-10.

  The limit for compliance types is always 1 per user.

  It is not possible to set a credential limit if one or more users already have more than the maximum number of credentials. You can run a user search (**Users | User search**) with the Credential type column to see which users have excess credentials assigned.

  The SOAP service ignores the credential number restriction.

## User credential inactivity defaults

This section is not available for compliance types.

- **Disable inactive user credentials**: When this option is enabled, new users added to the system will automatically have a default **Inactivity period** applied to this credential type (**Users | Users | General**). If the user does not use the credential within that period it will be disabled.

  When you change this default setting, you can choose whether to apply the new default to all existing users. Updating existing users may take some time on large sites.

- **Default credential inactivity period**: Set the number of days, hours or minutes that the credential must be inactive before it is disabled.

  The maximum inactivity period is 365 days. If you enter a longer period the field will reset to the default period of 30 days.

## Compliance configuration

Different options are available when the **Format** above is set to Compliance.

- **Warning period**: The number of days before the compliance expires that the **Warning text** will be displayed to the user.
- **Warning text**: The message that will be displayed on the card reader screen to warn users that their compliance is about to expire. Users must acknowledge the warning before they will be granted access.

  Due to the size of the reader screen, compliance messages are restricted to 32 characters.

- **Expiry text**: The message that will be displayed on the card reader screen to inform users that their compliance has expired. If the compliance type is configured for soft failure, the user must acknowledge the expiry notice before they will be granted access.

  Due to the size of the reader screen, compliance messages are restricted to 32 characters.

- **Hard failure**: When this option is enabled the user will be denied access when their compliance has expired. When this option is disabled (soft failure), if a user's compliance has expired the expiry message will be displayed but access is still granted. The user must acknowledge the expiry notice before they will be granted access.

  It is also possible to configure soft failure for users who do not have the compliance at all, using the **Allow soft failure on missing compliances** option in **Programming | Door types | General**.

- **Never expires**: When this option is enabled the compliance type will be treated as if it never expires for any user, regardless of whether an expiry date has been set. Both the **Start date** and the **End date** in the user programming will be ignored.

## Commands

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

## Record history

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

# Card profiles

Card profiles are used in the ICT offline wireless locking system to determine how much storage is available on user cards for offline lock functions. One card profile is needed for every unique card technology and card size that is used on site. When a card is encoded at a desktop encoder or update reader, the matching card profile is used to create the wireless locking files.

This tab is only visible when **Enable offline wireless locks** is enabled in **Global | Sites | Site defaults**. For more information and programming instructions, see the Protege Offline Wireless Lock Configuration Guide.

## Card profiles | General

### General

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

### Storage

- **MIFARE Classic**: Displays the sectors available on the MIFARE card. Some sectors are permanently reserved and you can click on additional sectors to reserve them. Any sectors that are not reserved can be used for wireless locking data.
- **Card**: The bar shows the amount of space that is reserved, designated for each wireless locking function and available for other data. The total space used for wireless locking is displayed in the top right.

  Click **Edit** to adjust the amount of space available for each function.

  Total wireless locking storage cannot be changed after the cards have been encoded.

### Record history

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

# Function codes

This feature allows you to define a function - such as arming an area or activating an output - that can be activated by users from a card reader with a PIN pad. At the reader, the user can enter a specific digit (0-9) and press enter, followed by the door's credential sequence, to activate this function.

If you are using ICT readers with RGB LEDs and RS-485 wiring, you can also program unique acknowledgement LED colors to display whether the function has succeeded or failed.

Once you have created a function code you must assign it to specific doors so that it can be activated from the associated readers (**Programming | Doors | Function codes**).

For more information and programming examples, see Application Note 240: Function Codes in Protege GX.

## Function codes | General

### General

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

### Configuration

- **Digit**: The digit (0-9) that will be used to activate this function code. The user can press this number, the enter key, then enter the door's credential sequence to activate the function code.
- **Start of function LED color**: The color which the reader LED will display to indicate that the function code has been initiated. This can be used to prompt the user to enter their credentials.

  LED colors are only available for readers with RGB LEDs.
- **End of function success LED color**: The color which the reader LED will display to indicate that the function code has been completed successfully.

  LED colors are only available for readers with RGB LEDs.
- **End of function failure LED color**: The color which the reader LED will display to indicate that the function code has failed to complete. For example, this color will be displayed if the user fails to enter a correct credential sequence.

  LED colors are only available for readers with RGB LEDs.

### Actions

Click **Add** to add actions to the function code, with the following options:

- **Device type**: Select from door, area or output.
- **Name**: Select the required device.
- **Action**: The available actions correspond to those available as manual commands when right clicking on a device record. For more information on specific options, see the corresponding Manual Commands section in this manual.
- **Allow unauthorized**: When this option is enabled, no credentials will be required to activate the function code. By default, the credentials set in the door's door type are required to activate the function code.

If this option is enabled the event log will not indicate which user has activated the function code.

- **Schedule**: The function code can only be used when the selected schedule is valid. If the schedule is invalid the reader will indicate that the function code has failed (using the **End of function failure LED color** and a long beep). To allow the function code to be activated at any time, set the schedule to Always.
- **Timeout**: The length of time (in seconds) that the reader will wait for the user to enter their credentials after pressing the **[ENTER]** key. If no credentials are entered during this time the reader will indicate that the function code has failed (using the **End of function failure LED color** and a long beep).

## Record history

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

# Jobs

Jobs are a legacy feature that do not require configuration in Protege GX.

# User import job step

User import job steps are a legacy feature. The following alternatives are available:

- The user import feature under **Sites | Import users** provides a one-off import of users from a CSV file (see below).
- The ICT Data Sync Service allows you to configure recurring user imports, which can provide low level integration with third-party HR and booking systems.

  For more information, see the ICT Data Sync Service Integration Guide.

# Import users

It's not unusual to have hundreds of users that need to be loaded into the system. Entering the data manually can be tedious and time consuming, and data entry is often prone to human error. Protege GX enables you to use a standard CSV file to import user information from existing systems, such as HR or student enrollment systems. The columns within the spreadsheet can be mapped to fields within the Protege GX user tables, providing a great degree of flexibility.

The import users feature is useful for one-time initial imports of user records. For recurring imports, use the ICT Data Sync Service.

For a demonstration, see Importing Users via CSV in Protege GX on the ICT YouTube channel.

## Importing Users from a CSV

1. Navigate to **Sites | Import users** to launch the Import users wizard.
2. Browse to and select the CSV file you wish to import users from, then click **Next**.
3. Select the line to start importing data from and the text delimiter to use, then click **Next**.

   If your file contains a header row, ensure you start the import at line 2 so the header row is not imported.
4. Select each column in the panel on the left and map it to the associated field to import to on the right. The data in the top pane is updated as you make your selections.
5. Set your **User display name auto format** preference. This determines how the **Name** field will be populated. Click **Next** to continue.

   The Reverse short format (Smith, J) and Reverse long format (Smith, John) options are not available. If these are required, edit the CSV file so that the **Name** column has the correct format.
6. Assign the facility number, first card number, and access level if you have not already done so. You can also choose to generate PIN numbers automatically. Click **Next** to continue.
7. Click **Finish** to start the import process. The user records are imported and the wizard closes.

# Batch add users

By batch adding users you can automatically create a number of default user records with an assigned facility number and range of card numbers. These new records will be blank, ready for configuration as specific users.

## Batch Adding Users

1. Navigate to **Site | Batch add users**.
2. Enter the following details that will apply to all user records added in this batch:
   - **First/Last name**: You may wish to enter a placeholder first or last name so that it is easy to identify and search for the new user records.
   - **User display name auto format**: This setting determines how the **Name** field in the user record will be populated for display within Protege GX (based on the first and last name). The display name can be edited for each record later.
   - **Facility number**: The facility/site number that will be assigned for the first credential of all users added.
   - **Card number start/end**: Each added user will be assigned a card number, beginning from the start value and incrementing until the end value is reached. These values also determine the number of user records that will be created.
   - **Access level**: The access level that will be assigned to all users in this batch.
3. Click **OK**. The user records are now added and ready to be configured individually (**Users | Users**).
4. The **Add user results** popup confirms the number of user records created.

# Users Menu

The users menu contains the functions for working with and configuring users and defining the access they have within a site.

For demonstrations, see ICT Quick Tip: Adding a User in Protege GX and Creating and Managing Users in Protege GX on the ICT YouTube channel.

## Users

A user is a person programmed into the system with access control, alarm, biometric or photo identification credentials. The user can be assigned access to programmed doors and functions of the system.

You can view user records in either **List view** or **Tree view** (organized by record group) by clicking the icons in the toolbar. List view is the default, but you can set the default to tree view by enabling the **Display users in groups** option (**Global | Sites | Display**).

### Sorting and Filtering User Records

There are various tools available on the users page for sorting and filtering the user list to find the records you need:

- **Pagination**: You can set the **Number of records to display on page** at the bottom of the list and navigate between pages using the arrows. On large sites it can take a long time to load all of the records, so reduce the page size to load the pages faster.
- **Sorting**: You can sort the users list by clicking the column headers (e.g. click the **Name** header once to sort alphabetically, and a second time to reverse sort). You can also enable **First name** and **Last name** columns using the **Display first name and last name columns in users** in **Global | Sites | Display**.
- **Filtering**: There are two methods for filtering the user list:
  - The search bar at the top of the list allows you to quickly filter users by the **Name** field.
  - The **Find** tool in the toolbar can filter users by any setting. For more information, see Using the Find Tool (page 21).

## Users | General

### General

- **First name**: The first name of the user.
- **Last name**: The last name of the user.
- **Name**: The display name of the user as it appears on keypads and within the software. This field will be auto-filled based on the setting in **User display name auto format** (**Global | Global settings | General**).
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

  Record groups also determine how users will be grouped in the **Tree view** (activated from the toolbar).
- **Default language**: Defines the language that will be used when the user logs in to a keypad. This may be any supported language and is not limited by the Protege GX installation.
- **Email**: The email address of the user.

  This is used by the tenancy portal sync feature (see **Global | Sites | Portal**). The email address will be used to synchronize the user and create a mobile app account, enabling visitors to video call the user from the entry station. If the user already has a mobile app account, enter the email address associated with that account.

  For more information, see the Protege Tenancy Portal User Guide.

## PIN

See **Global | Sites | Site defaults** for default PIN settings.

- **PIN**: A user's PIN is used to log in to keypads and access doors (via card readers with PIN pads). Click on the **[4] [5] [6]** buttons to automatically generate a new random PIN of the selected length.

  The maximum PIN length accepted by keypads and readers is 8 digits. Any additional digits are ignored.

  Existing user PINs are only visible to operators with the **Show PIN numbers for users** option enabled (**Global | Operators**).

- **Reset PIN**: Click this button to generate a new random PIN with the number of digits specified by the **Default PIN length** field (**Global | Sites | Site defaults**).
- **Key Cabinet PIN**: This field is visible when the user has access to keys or key groups via their access level. The key cabinet PIN is based on the user's regular PIN, but truncated based on the requirements of the third-party system.

  For more information, see Application Note 220: KeyWatcher Touch Integration in Protege GX or Application Note 331: KeySecure Integration with Protege GX.

- **PIN expiry time**: Sets the length of time before the current PIN expires. The first time the user logs in to a keypad after their PIN expires they will be prompted to change their PIN. The user will not be able to use an expired PIN for door access.

## Card numbers

- **Program card**: This button is used to program cards for users for use with the Salto SHIP integration, using a USB desktop encoder (PRX-ENC-DT). Ensure that any required user settings are set in the **Salto** tab before encoding the card.
- **Facility/Card number**: Each user can have up to 8 standard credentials (cards, tags, biometric data) which can be used at any door with compatible readers. Each credential is made up of a facility number (first field, also known as a site code) and card number (second field), which each have a 10 digit limit.

  New credentials can be assigned to users by typing the facility and card numbers here. Alternatively, when you badge an unassigned card at a reader you can right click on the 'Read Raw Data' event and select either **Add new user** or **Add card to existing user** to automatically enter the credential details.

  Biometric credentials must be entered in the second row (labeled **Facility/Card number or biometric data**). If there is existing data in this row when a biometric credential is enrolled, the existing data will be moved down the list.

  **Note**: The Protege GX database cannot store user facility or card numbers of 2147483648 or above. Events referencing these cards will display no data. This is a known limitation.

- **Read card**: This feature is used with a compatible desktop encoder (such as PRX-ENC-DT). Rest a card on the encoder and click this button to automatically populate the **Facility/Card number** fields.

  The encoder must be able to read the card type being used. The ICT USB desktop encoder only supports ICT secured Mifare and DESFire cards.

- **Card disabled**: This setting allows a credential to be disabled without deleting the details. The credential can be re-enabled by unchecking the box. If a user has multiple credentials, the setting may be enabled or disabled where appropriate for each credential.
- **Card last used / modified**: Shows the date and time that the card was last granted access at a door or modified by an operator within the system (read only).

  The time last used is only updated when the credential is used to gain access to a door (i.e. **Reader 1/2 mode** is set to Access). It is not updated at readers in Elevator or Area modes. This is a known limitation.

- **Inactivity period**: When this option is enabled you can set an inactivity period in days, hours or minutes. If the

card is not used within this set period it will automatically be disabled.

You can set a **Default card inactivity period** in **Global | Sites | Site defaults**.

## User expiry date/time

You can set default expiry date/time settings for new users in **Global | Sites | Display**.

- **Start**: When this option is enabled the user will not be able to gain access before the time and date specified. For example, this could be used to automatically activate an employee who is due to start work on a specific date.
- **End**: When this option is enabled the user record will expire after the time and date specified and the user will not be able to gain access. For example, this could be used to automatically remove access from a contractor who is due to finish the job at a certain date.

## User disable/deletion

- **User last active**: Shows the date and time the user was last granted access to a door or keypad within the system (read only).

  This field is not updated when the user accesses a door record which represents a COP or DOP in an HLI elevator integration.

- **Disable period**: When this option is enabled you can set an inactivity period in days, hours or minutes. If there is no user activity during this period (i.e. they do not access any doors or keypads), the user record will be disabled (using the **Disable user** option in the **Options** tab).
- **Delete period**: When this option is enabled you can set an inactivity period in days, hours or minutes. If there is no user activity during this period (i.e. they do not access any doors or keypads), the user record will be deleted from the database.

You can set default inactivity settings under **User inactivity defaults** in **Global | Sites | Site defaults**.

## Areas

- **User area**: This field allows you to set an area that the user is associated with. This feature has several applications:
  - If the **Turn off the user area on login if user has access** option is enabled (**Options** tab), whenever the user logs in to a keypad that area will automatically be disarmed.
  - The **Disarm users area on valid card** option (**Expanders | Reader expanders | Reader 1/2**) allows the user to automatically disarm their user area when they badge at the corresponding reader. The **Arm users area** option (same location) allows the user to automatically force arm their user area when they badge twice at the reader.

  The same functionality is available for multiple areas in the **Area groups** tab. The user area should be included in **Users | Access levels | Disarming area groups**.

## Configuration

- **Reporting ID**: The code which will be used to identify this user in reports to monitoring stations. Contact ID, SIA, and Report IP reporting services use this code.

  The system will automatically generate a unique number for each new user. There is no need to edit these numbers unless there are specific reporting requirements.

## Wireless lock settings

This section is only available when the wireless locking integration is enabled (**Global | Sites | Site defaults**).

By default the settings in new user records match the defaults from **Global | Sites | Offline wireless locking**, but you can edit them as required.

- **Update period**: The update period determines how frequently the user must update their credential at an update point reader. If they do not update their credential within this period, the access data will expire and they will not be able to access offline locks until they renew the data at the update point reader.
- **Enable office unlock**: When the **Lock operating mode** is set to Office unlock (**Programming | Door types | Options**), users with this option enabled can latch unlock the door by holding down the inside handle and badging a credential at the same time. They can relock the door using the same method.

## Key cabinet integration

- **Third party user ID**: When a user is granted access to keys or key groups, a unique user ID is assigned for use with the key cabinet system. This can be edited if required.

  For more information, see Application Note 220: KeyWatcher Touch Integration in Protege GX or Application Note 331: KeySecure Integration with Protege GX.

## Cencon key

These options are only available when Cencon integration is enabled in **Global | Sites | Cencon**. For more information, see Application Note 160: Configuring Cencon Integration in Protege GX.

- **Cencon key ID**: When a Cencon key has been initialized this field will automatically display the Key ID.
- **Initialise key**: If the Cencon integration has been configured this button is used to assign a Cencon key to a user. When you click this button you will be prompted to place a key in the connected key box. If initialization is successful the user will be added to the Cencon database and the **Cencon key ID** field above will be filled automatically.

  After a key has been assigned, the same button will allow you to disable the user's key.

## Credentials

This section allows you to assign custom credentials to users. When a credential type has been created in **Sites | Credential types** it will be automatically added here, or you can use the **Add** and **Delete** buttons to manage the user's available credentials.

- **Credential type**: The custom credential type that the credential is associated with (e.g. license plate, custom card format, compliance type, etc.).
- **Disabled**: Check this box to disable the credential without deleting it.
- **Credential**: The specific credential data for the user (e.g. their license plate).
- **Start**: Only applicable to compliance types. When this option is enabled the user will not be able to gain access using this compliance before the date specified.
- **End**: Only applicable to compliance types. When this option is enabled the compliance will expire after the time and date specified and the user will not be able to use it to gain access.
- **Inactivity period**: When this option is enabled you can set an inactivity period in days, hours or minutes. If the credential is not used within this period it will automatically be disabled.

  You can set the **Default credential inactivity period** in **Sites | Credential types | General**.

  The maximum inactivity period is 365 days. If you enter a longer period the field will reset to the default period of 30 days.

- **Program card**: Only available in systems using offline wireless locks. To encode a card for offline locks, place it on a USB desktop encoder, select the relevant credential and click **Program card**. The encoder will encode the wireless locking files on the card and automatically record the facility and card numbers.

For sites with the **Require dual credential for keypad access** feature enabled in **Global | Sites | Site defaults**, each user will have a default User ID credential type and will require a valid User ID in the **Credential** field.

### VingCard Visionline

This is a separately licensed feature. For more information, see Application Note 215: Protege GX VingCard VisiOnline Integration.

- **Program staff card**: Press this button to encode a card for this user using the VingCard Encoder specified in the controller programming (**Sites | Controllers | Configuration**).

## Users | Access levels

This tab controls the access levels assigned to each user. Whenever the user performs an action (such as requesting access to a door or logging in to a keypad), the system checks their assigned access level(s) to determine whether they have the necessary permissions.

Click **Add** to select and assign an access level, or **Delete** to remove one. The **Graphic view** window displays timelines to indicate when the user has access to each door in the system, based on the schedules defined in the user, access level and door group programming.

The controller checks all access levels applied to a user. Generally if access is granted by one access level and denied by another, access will be granted.

- **Name**: Name of the access level assigned to the user.
- **Access level expires**: When this option is enabled the access level will expire based on the defined start and end dates. The user will only be able to use this access level between the expiry start and end dates.

  Multiple copies of the same access level can be assigned to a single user with different expiry times, allowing for periodic access. For example, a technician may only be able to access the building for a few days per month.
- **Expiry start**: This access level will not be valid for the user before this date and time.
- **Expiry end**: This access level will not be valid for the user after this date and time.
- **Schedule**: This schedule determines when the permissions provided by the access level are valid for this user. This is combined with any schedules set in the access level itself, as well as in door or floor groups.

  The user only has access if all relevant schedules are valid.

## Users | Options

### General options

- **Disable user**: When selected, the user record is disabled, preventing them from using any access permissions. The record is not deleted and can be re-enabled at any time.

  When a user is disabled a command is sent to the relevant controllers to update their internal databases. This means user records are disabled immediately without waiting for a controller download.
- **Show a greeting message to user**: When this option is enabled the user will be shown a greeting (e.g. 'Good Morning John Smith') on the keypad when they log in. Disabling this option instructs the keypad to proceed directly to the menu when the user logs in.

  This option is equivalent to the **Show user greeting** option in **Groups | Menu groups | Options**. The greeting will be displayed if either option is enabled.
- **Go directly to the menu on login (no area control)**: By default, when a user logs in to a keypad they will be presented with the area control menu, allowing them to arm and disarm available areas. When this option is enabled the user will be taken directly to the keypad's main menu instead. Users can still access area control from the main menu.

**User can acknowledge alarm memory**: When this option is enabled the user is able to acknowledge the alarm memory for available areas at the keypad. The alarm memory can be viewed by pressing **[Menu] [5] [1]** and records the last four alarm activations in each area.

This option is equivalent to the **User can acknowledge alarm memory** option in **Groups | Menu groups | Options**. Alarms can be acknowledged if either option is enabled.

- **Show alarm memory on login**: With this option enabled, if there have been any alarms in the keypad's primary area the keypad will display the alarm memory to the user as soon as they log in. With this option disabled the user must navigate to the View menu to acknowledge any alarms.

  This option is equivalent to the **Show user alarm memory on logon** option in **Groups | Menu groups | Options**. Alarms can be acknowledged if either option is enabled. The keypad's primary area is defined in the **Area this LCD belongs to** (**Expanders | Keypads | Configuration**).

- **Turn off the primary area if user has access on login**: With this option enabled, whenever the user logs in to the keypad the keypad's primary area will be disarmed. This will only work if the user has access to disarm that area - i.e. the area is included in the **Disarming area groups** tab of the access level.

  The keypad's primary area is defined in the **Area this LCD belongs to** (**Expanders | Keypads | Configuration**).

- **Turn off the user area on login if user has access**: With this option enabled, whenever the user logs in to the keypad the **User area** (set in the **General**) tab) will be disarmed.
- **Acknowledge system troubles**: When this option is enabled the user can acknowledge certain system trouble conditions using the keypad. System troubles can be viewed by pressing **[Menu] [5] [2]** on the keypad, and acknowledged by pressing **[Enter]**.
- **Treat user PIN plus 1 as duress**: When this option is enabled the user's PIN + 1 is treated as a duress code. When this special code is entered at a keypad or reader PIN pad access will be granted (or denied) as normal, but a User Duress (for keypads) or Door Duress (for reader PIN pads) trouble input will be opened. The trouble input will be closed when the normal user PIN is entered.

  To calculate the duress code, 1 is added to the last digit of the user PIN. For example, if the normal PIN is 1234 the duress code will be 1235. If the final digit is 9 then 0 as the final digit generates a duress code. User PINs must be longer than 3 digits for this feature to function correctly.

  If using a PCB controller with version 4.0 software or higher, enabling this option for one user enables it globally for all users.

## Advanced options

- **User has super rights and can override antipassback**: When this option is enabled the user is considered a 'super user' by the system. This grants the following permissions:
  - Override dual code requirements for doors and areas
  - Ignore antipassback rules
  - Unlock doors that have been locked down
  - Unlock wireless locks in privacy mode
- **User operates extended door access function**: With this option enabled, whenever this user is granted access to a door the lock will open for the **Door extended access time** (set in **Programming | Doors | Advanced options**) instead of the standard **Lock activation time**.

  This should be used to grant people with mobility issues additional time to access doors.
- **User loiter expiry count enabled**: When this option is enabled the user will be included in loiter area processing. This feature can be used to prevent users from remaining too long in transitional areas, such as corridors and carparks. When this option is disabled this user is not affected by loiter area programming.

  Loiter area programming must be configured correctly in the relevant area(s). For more information, see the **Area enabled in loiter mode** option in the **Programming | Areas | Options (1)** page.

- **User can edit user settings from keypad:** This is a legacy option that has no effect.

- **User is a duress user**: With this option enabled, when this user's PIN is entered at a keypad or reader PIN pad it will be processed as a duress code. Access will be access will be granted (or denied) as normal based on the duress user's access level, but a User Duress (for keypads) or Door Duress (for doors) trouble input will be opened. The trouble input will be closed when a normal user PIN is entered.

  This option should be used when the site requires duress codes that are common to multiple users.

  This option should not be applied to regular users. Use the **Treat user PIN plus 1 as duress** option to give each user a unique duress code.

- **Rearm area in stay mode**: Enabling this option allows the user to set areas to automatically rearm in stay mode. When the user disarms an area with the **User rearm in stay mode** option enabled (**Programming | Areas | Options 2**), the area will remain disarmed for a set period (the **Rearm area time** in **Programming | Areas | Configuration**), then automatically stay arm.

  This option is useful for people who work outside normal hours, allowing them to disarm the inside of the building and secure the perimeter.

## Dual custody options

- **Dual custody master**: When a door type has the **Requires dual authentication** option enabled (**Programming | Door types | Options**), two users must enter valid credentials for the door to unlock. By default, a **Dual custody master** must enter their credentials first to initiate dual authentication, followed by a dual custody provider or another master.
- **Dual custody provider**: When a door type has the **Requires dual authentication** option enabled (**Programming | Door types | Options**), two users must enter valid credentials for the door to unlock. By default, a **Dual custody provider** cannot initiate dual authentication, but can complete the process once a dual custody master has initiated it.

  When the **Dual card provider can initiate access** option is enabled in the door types programming, either a dual custody master or provider can initiate dual authentication.

## OTIS elevator HLI options

These options are only available when Otis HLI integration is enabled. For more information, see Application Note 174: Protege GX Otis Compass HLI Integration.

- **User is a VIP**: VIP users have non-stop priority service to their destination floor in dedicated elevator cars. This must be configured in the Otis system.
- **Enable Vertigo**: When vertigo is enabled the Otis system will select specific elevator cars for this user based on a particular characteristic (as configured in Otis). For example, passengers with vertigo will not be assigned to glass elevator cars.
- **Enable split group operation**: Enables contract special 1, as configured in the Otis system.
- **Enable Vertigo 2**: Following from **Enable Vertigo** above, this option further defines which type of elevator the user will be assigned, as configured in the Otis system. For example, elevators may be slowed for this passenger.
- **Enable cart service**: This feature minimizes cases of an elevator car arriving without the physical capacity required for a passenger and cart (e.g. in hotel/hospital service elevators).
- **Enable CIM override**: When CIM operation is enabled in the Otis system, the system prevents specified groups of users from sharing elevator cars or traveling to the same floors. Enable this option for users who need to access all elevator cars and floors, such as building managers.

## KONE elevator HLI options

These options are only available when KONE HLI integration is enabled. By default, all calls are normal call types. Use the options below to specify an alternative call type.

For more information, see Application Note 274: Protege GX KONE Destination 880 Integration and the operator documentation provided by KONE.

- **Enable normal call**
- **Enable handicap call**

- **Enable priority call**
- **Enable empty car call**
- **Enable space allocation call**

# Users | Photo

Photo ID is a separately licensed feature. For more information, see Application Note 149: Creating a Photo ID Template in Protege GX.

It is not possible to view user photos when multiselecting users. If multiple user records are selected the photo view will not be available, and this will persist even after the multiselect is cleared. You will need to navigate out of the Users | Users menu to refresh the photo view.

## Photo

- **Add photo...** Click this button to add a photo for the user.
  - If the image is already stored on the network, select the ellipsis **[...]** beside **Path** to browse to the image. The image must be accessible from the server machine.
  - If the image does not yet exist set the **Image source** field to capture a new image. You can capture an image from a connected webcam, or from a Topaz signature pad.
  - When complete, click **Next**.
- **Delete photo**: Delete the user photo from the database.
- **Photo settings**: By default, the photo size follows the setting in **Global | Sites | Display**. The settings here allow you to override this setting for individual users.
- **Print card**: Prints the Photo ID card based on the **Card template** selected below. There are several options for card printing. Hover over the arrow to see the available options:
  - **Print card**: Print the card without reading or writing the credential (smart card number, magstripe or ICT sector). You will be prompted to select the printer to use.
  - **Print & read**: Print the card and read the card number to the user's credential field.
  - **Print & process template**: Print the card and read or write the magstripe or ICT sector. The action taken depends on the settings in **Users | Card template editor | Card encoding**.
  - **Process Template Only**: Read or write the magstripe or ICT sector without printing the card. The action taken depends on the settings in **Users | Card template editor | Card encoding**.

  It is possible to batch print cards for a number of users at once. Run a user report with the desired users, then click **Batch print** to print cards for all users currently visible in the report.
- **Preview**: Displays a preview of the user card based on the **Card template** selected below.

## Photo ID

- **Card Template:** Defines the photo ID template to be used. Create a Photo ID template in **Users | Card Template Editor**.
- **Stretch Image to Fill**: This forces the image to stretch to the size defined in the **Photo Settings** above. With this option enabled the aspect ratio of the image is not maintained and some warping may occur.

# Users | Extended

This tab is only visible when the option to **Display predefined custom fields in users** is enabled in **Global | Sites | Display**, and allows you to enter additional user information. A number of preset fields are available.

For customized user fields use **Custom fields** and **Custom field tabs** (**Users** menu).

The available extended fields are:

- Badge number
- Badge type

- Service name
- Service number
- Employee function
- License number
- Union
- Site
- Date of badge production
- Expiration date of badge
- Custom fields 1-6
- Custom note fields 1-2
- Card number
- Card type
- Salary number

If the **Save badge number and date after card printing** option is enabled (**Global | Sites | Site defaults**), the **Badge number**, **Badge type** and **Date of badge production** fields will be automatically filled after a user card is printed. Other fields can be updated based on the settings in **Users | Card template editor | Card printing actions**.

In addition, fields on this tab can be included on a user card in barcode form. This allows you to interface with systems that use barcode scanners to identify users. For more information, see Card Template Editor Menus (page 135).

## Users | Attendance

This tab allows you to easily view the latest in and out (attendance) events for a user.

- **Load events**: Loads the most recent door entry and exit events for the user.
- **Add in/out event**: Allows you to add a new time and attendance event for the user (entry/exit from a specific door).

  When adding time and attendance events all times will be rounded down to the nearest hour.

- **Copy to clipboard**: Copies the selected event(s) to the clipboard as CSV data.

## Users | Area groups

The area groups tab has similar functionality to the **User area** field (**General** tab), allowing you to specify one or more area groups that the user is associated with. For example, this might be used to allow a user to quickly disarm a specific section of the building. This feature has several applications:

- If the **Turn off the user area on login if user has access** option is enabled (**Options** tab), whenever the user logs in to a keypad each area in the area group will be automatically disarmed.
- The **Disarm users area on valid card** option (**Expanders | Reader expanders | Reader 1/2**) allows the user to automatically disarm all areas in the area group when they badge at the corresponding reader. The **Arm users area** option (same location) allows the user to automatically force arm all areas in the area group when they badge twice at the reader.

The area groups assigned here should be included in the **Users | Access levels | Disarming area groups** tab.

## Users | Biometrics

The biometrics tab enables you to scan a user's biometric data at an enrollment reader. The credential will be entered in the second row of the user's card numbers, using the **Default facility number** set in **Global | Sites | Biometrics**. Both finger and face data can be registered to a single user record.

For instructions for enrolling biometric data, see the relevant application note for your integration:

- Application Note 264: Suprema Biometrics Integration with Protege GX
- Application Note 297: Princeton Identity Biometric Integration with Protege GX

This tab is only displayed when either the Suprema or Princeton biometrics integration is enabled in **Global | Sites | Biometrics**.

# Users | Salto

This tab enables configuration of the options related to Salto locks for this user.

This tab is only visible when the option to **Enable Salto (SHIP) integration** is checked in **Global | Sites | Salto**. For more information, see Application Note 188: Salto SHIP RW Pro Access Integration with Protege GX or Application Note 335: Salto SHIP ProAccess SPACE Integration with Protege GX.

## Salto options

- **Calendar**: A Salto calendar defines the days when the user's access permissions have different hours (such as holidays).

  Calendars can be programmed in **Salto | Calendars**. The schedule(s) assigned to the user's access level define the periods that are active on different days (see the **Salto** column of **Sites | Schedules | Configuration**).
- **Use extended opening time**: With this option enabled, whenever this user is granted access to a Salto door the lock will open for the **Increase open time** instead of the **Open Time** programmed in **Salto | Doors | General**. This should be used to grant people with mobility issues extended times to access doors.
- **Office**: When this option is enabled the user can set Salto doors to 'office mode' (latch unlock). Office mode is activated by presenting a Salto key while holding the inside handle down, and canceled by repeating the procedure.

  The door's **Open mode** must support office mode (**Salto | Doors**).
- **Use antipassback**: With this option enabled the user will be affected by any antipassback restrictions set on Salto doors.
- **Audit openings in the key**: With this option enabled the Salto system will generate an audit trail on the Salto credential itself when this user opens a Salto door. The **Audit on keys** option must also be selected in the **Salto | Doors | General** programming.
- **PIN**: When this option is enabled the user can use their PIN (**General** tab) to access keypad enabled Salto locks.
- **User can override privacy**: When this option is enabled the user can access a Salto door even when it has been set to privacy mode (locked from the inside).
- **User can override lockdown**: When this option is enabled the user can open a Salto door even when it has been closed by a lockdown (emergency close).
- **User can lockdown door**: When this option is enabled the user can initiate a lockdown on compatible Salto doors (with AMOK escutcheons). The lockdown is initiated by holding the card to the AMOK reader (lower inside handle) and canceled the same way.

## User and key expiration

A Salto key can be encoded and assigned to a user using the **Program card** function in the **General** tab.

- **Start**: When this option is enabled the user's Salto key will not become active until the date specified. They will not be able to gain access to Salto doors before this date.
- **End**: When this option is enabled the user's Salto key will expire after the date specified. They will not be able to gain access to Salto doors after this date.
- **Enable revalidation of key expiration**: When this option is enabled the Salto key will expire at the end of the **Update period**. Whenever the key is presented at a Ubox or online lock it is revalidated and the update period is renewed.
- **Update period**: Defines how long the Salto key will remain valid after it is updated at a Ubox or online lock. For example, for a short term residency you might set the key to expire every 48 hours unless revalidated.

- **Period**: Sets the **Update period** to days or hours.
- **Cancel key**: This button deactivates the user's Salto key.

### Key status

- **Key assigned**: The date the key was assigned (read only).
- **Valid until**: The date the key will expire (read only).

## Users | Salto doors / door groups

These tabs are only visible when the option to **Enable Salto (SHIP) integration** is enabled in **Global | Sites | Salto**. For more information, see Application Note 188: Salto SHIP RW Pro Access Integration with Protege GX or Application Note 335: Salto SHIP ProAccess SPACE Integration with Protege GX.

These tabs allow you to assign one or more Salto doors or door groups that the user is allowed to access. You can also set schedules on these doors to control when the user has access.

Salto doors can also be assigned to multiple users using access levels (**Users | Access levels | Salto doors / door groups**).

The maximum number of doors that Salto currently supports is 64,000 per database. A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

## Users | Cencon locks

This tab is only displayed when **Enable Cencon integration** is enabled in **Global | Sites | Cencon**. For more information, see Application Note 160: Configuring Cencon Integration with Protege GX.

This tab allows you to assign one or more Cencon locks that the user is allowed to access. Cencon locks and lock groups can also be assigned to users via access levels (**Users | Access levels | Cencon locks / lock groups**).

## Users | Accommodation

Accommodation is a legacy feature that is no longer available for use.

## Users | Visitor

This tab is only displayed when the VMS (Visitor Management System) has been licensed. For more information, see Application Note 287: Protege GX Visitor Management System.

### Receive visitor settings

- **User supports visitors**: When a visitor signs in to the VMS they must select which user they are visiting. Enabling this option allows this user to be available for selection by visitors.
- **Visitor access level**: The access level selected here will be automatically assigned to any visitor who selects this user. Set to None if visitors should not be assigned any access level.
- **Visitor notification mode**: Set this option to Email for the user to receive an email notification whenever a visitor signs in to visit them. Set to None for no notifications.

  Automated email features in Protege GX require an SMTP mail server to be configured in **Global | Global settings | Email settings**.

- **Notification email address**: The email address that visitor notifications for this user will be sent to.

### Visitor

- **User is a visitor**: Read only field that indicates whether this user is a visitor.
- **Expected departure**: When a visitor signs in to the VMS they must indicate how long they expect to remain on the premises. This field displays their estimated departure time, which can be updated by an operator if necessary.

  You can search for All overdue visitors by running a user report or user search.
- **Checked in**: The time that the visitor signed into the VMS (read only).
- **Checked out**: The time that the visitor signed out of the VMS (read only).
- **Visitor card disabled**: Read only field that indicates whether the visitor currently has an assigned credential. When a visitor record is 'disabled' (either by signing out of the VMS or by pressing the button below), their credential is deleted and this checkbox is checked.
- **Sign out visitor**: Click this button to immediately disable the visitor record.

## Users | Portal

This tab is used for the tenancy portal synchronization feature. For information and programming instructions, see the Protege Tenancy Portal User Guide.

### General options

- **Phone number**: The user's phone number will be synchronized to their tenancy and phonebook record.

  If the user has no **Email**, the phone number will be used as an alternative method to synchronize the user's tenancy details to the entry station directory, enabling visitors to voice call the user from the entry station.

  The phone number is only used in the directory if the user has no email address entered.

  Duplicate phone numbers are allowed so that multiple users from a tenancy can use the same directory contact number.
- **Tenancy name**: The name of the user's tenancy, generally corresponding to an apartment number or similar address. A tenancy with this name will be created in the tenancy portal with the user as a tenant.

  A tenancy name must be entered in order for the user to be synchronized to the tenancy portal.

## Manual User Commands

Right clicking on a user record (**Users | Users**) displays a menu with manual commands for that user.

### Reset antipassback

This command resets the antipassback status of a user. This will allow the user to enter or leave any area that they have been denied access to due to antipassback rules.

Antipassback functionality must be configured using the **Entry/Exit passback mode** in **Programming | Door types | General**.

# User search

The user search feature allows you to generate one-off temporary user reports that can be printed, exported or emailed. It is ideal for creating ad hoc reports that do not need to be repeated frequently.

User searches are equivalent to user reports, but the configuration cannot be saved. For more information, see Reports | Setup | User (page 162).

## Running a User Search

1. Navigate to **Users | User search**.
2. Select the **Report type**. Choose from:
   - **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.
3. Set the **Title** of the report, that will be displayed at the top of the page when the report is printed.
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. Set any additional options that are required based on the **Report type** selected. For example, you may need to specify a time period, or additional records such as doors or access levels.
6. In the **Columns** tab, click **Add** and **Delete** to select which columns will be included in the report. These correspond to fields in the Users programming. By default, only first and last names are included.
7. To change the order of the columns, select an item and use the **Move up** and **Move down** buttons until you have the sequence you require.
8. Click **Find** to start the search.

9. A temporary report is generated and displayed in a grid view. You can 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.

   You can use the grid view to further sort, group, and filter the results. For more information, see Working with the Grid View (page 167).
10. The **Save** icon allows you to save the current report layout so that it will be used for other searches or reports generated by this operator.
11. Click the **Print** icon to open the print preview window where you can print, export or email the results (see page 170).

# Access levels

Access levels are assigned to users to determine what access they have within the Protege GX site. A user's assigned access levels define which doors, areas, floors, elevator cars and keypad menus they are allowed to access, and when that access is valid.

You can set the **Number of records to display on page** at the bottom of the list and navigate between pages using the arrows. On large sites it can take a long time to load all of the records, so reduce the page size to load the pages faster.

For a demonstration, see Configuring a Basic Access Level in Protege GX on the ICT YouTube channel.

## Access Levels | General

### General

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

### Configuration

- **Operating schedule**: This schedule determines when the access level is valid. When the schedule is invalid, users will not be able to use any of the permissions that are granted by the access level.

  Most individual features of an access level can also be controlled on a specific schedule without affecting any of the other permissions.

- **Time to activate output**: If any of the **Activate output** options below are enabled the output/output group will be activated for the period (in seconds) set here.

  This setting overrides the **Activation time** in **Programming | Outputs | General**.

- **Reader access activates output**: When this option is enabled, all outputs assigned in the **Outputs** or **Output groups** tab will be activated when a user gains access at a card reader using this access level.

  The **Activate access level output** option must be enabled for any reader expander port where this feature will be used (**Expanders | Reader expanders | Reader 1/2**).

- **Keypad access activates output**: When this option is enabled, all outputs assigned in the **Outputs** or **Output groups** tab will be activated when a user logs in to a keypad using this access level.

  The **Activate access level output** option must be enabled for any keypad where this feature will be used (**Expanders | Keypads | Options 1**).

- **Activate output until access level expiry**: When this option is enabled, if an output is activated by the access level it will deactivate when the access level expires in the user record. This requires the user to use either the **Reader access activates output** or **Keypad access activates output** options above.

  This feature is useful for short-term access levels that are held by only a single user, such as in booking systems. For example, a user might be assigned access to a particular meeting room for an hour. When they first access the room all lights turn on (using **Reader access activates output** above). When the access level expires, the lights turn off.

- **Toggle access level output**: When this option is enabled the output state will be toggled whenever it is triggered by the access level. This also requires **Reader access activates output** or **Keypad access activates output** to be enabled.

  For example, if both **Toggle access level output** and **Reader access activates output** are activated, when a user badges their card at a reader for the first time the output will turn on. When they badge at the reader a second time the output will turn off.
- **Enable multi-badge arming**: With this option enabled, users with this access level can perform various functions (such as arming an area or toggling an output) by badging or entering their credentials multiple times at a card reader.

  Multi-badge functions are defined by the **Reader arming mode** setting in **Expanders | Reader expanders | Reader 1/2**.
- **Use access level door type**: With this option enabled, when a user uses this access level to gain access at a door they use alternative credentials instead of those set in the primary door type. These alternative credentials are set as the **Access level door type** in **Programming | Door types | General**.

  For example, this feature can be used to make it easier for security personnel to move around the site.

  **Important**: This option applies to all doors which are included in this access level. Ensure that all of these doors have a valid **Access level door type** assigned, otherwise users may be denied access due to an invalid door type.
- **Enable access to wireless lock config**: Enable this option to allow users to configure wireless locks using the Protege Config App. You also need to add the user's mobile credential to the ICT Wireless Locking credential type.

## Usage restriction

- **Enable usage restriction**: This feature allows you to limit the number of times that a user can access doors using this access level. After the user exceeds the **Usage limit** they will need to wait until the **Reset period** has passed before the limit is reset and they can use the access level to access doors again.
- **Usage limit**: Determines the number of times a user is granted access at affected doors before triggering the **Reset period**.
- **Reset period**: The length of time (in minutes, hours or days) a user will be denied access after reaching the **Usage limit** before the limit is reset.

  The **Reset period** begins when the user reaches the **Usage limit**, and will restart if the user makes any further attempts to gain access during this period.

## Commands

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

## Elevator HLI

- **Elevator destination floor**: If the KONE RCGIF (Remote Call Giving Interface) has been enabled, when a user badges at a DOP reader an elevator will be summoned to transport them to the floor defined here. For more information, see Application Note 170: Protege GX KONE HLI Integration.

  This option also allows you to set the home floor for an access level in the Schindler HLI integration. For more information, see Application Note 196: Protege GX Schindler HLI Integration.

## Record history

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

## Access levels | Doors

This tab defines the **Doors** the user has access to, the **Schedule** used, and the **Access direction** (entry, exit, or both) in which the user can pass through the door.

- By default, the **Schedule** is set to Always, meaning access to the defined door is permitted at all times. When a schedule is assigned the door will only be accessible when the schedule is valid. For example, you may wish to limit employee access to an office building to office hours.
- By default, the **Access direction** is set to Both (entry and exit). Some doors may be configured to permit access in one direction only.

## Access levels | Door groups

This tab defines the **Door groups** the user has access to, the **Schedule** used, and the **Access direction** (Entry, Exit, or Both) in which the user can pass through the doors.

- **Include all doors**: Select this option to assign all doors in the site to this access level.

  This option should be used with caution, as it provides unlimited access to all existing and new doors in the system. In many cases it is more secure to create a door group containing all current doors for this purpose.

- By default, the **Schedule** is set to Always, meaning access to the defined door group is permitted at all times. When a schedule is assigned the doors will only be accessible when the schedule is valid. For example, you may wish to limit employee access to an office building to office hours.
- By default, the **Access direction** is set to Both (entry and exit). Limiting the direction may be used, for example, to allow employees to exit a building but not enter it again after hours.

## Access levels | Floors

This tab defines the floors that the user has access to and the **Schedule** that is used.

- By default, the **Schedule** is set to Always, meaning access to the defined floors is permitted at all times. When a schedule is assigned the floor will only be accessible when the schedule is valid.

## Access levels | Floor groups

Defines the floor groups that the user has access to and the schedule that it used.

- **Include all floors**: Select this option to assign all floors in the site to this access level.

  This option should be used with caution, as it provides unlimited access to all existing and new floors in the system. In many cases it is more secure to create a floor group containing all current floors for this purpose.

- By default, the **Schedule** is set to Always, meaning access to the defined floor group is permitted at all times. When a schedule is assigned the floors will only be accessible when the schedule is valid.

## Access levels | Elevator groups

This tab defines the **Elevator groups** that the user has access to and the **Schedule** that is used.

- **Include all elevators**: Select this option to assign all elevators in the site to this access level.

  This option should be used with caution, as it provides unlimited access to all existing and new elevators in the system. In many cases it is more secure to create an elevator group containing all current elevators for this purpose.

- By default, the **Schedule** is set to Always, meaning access to the defined elevator group is permitted at all times. When a schedule is assigned the elevators will only be accessible when the schedule is valid.

## Access levels | Menu groups

This tab defines the menu group that the user has access to. Menu groups determine which menus the user has access to at a keypad, and can be programmed in **Groups | Menu groups**.

Only one menu group can be assigned to each access level.

## Access levels | Arming area groups

This tab defines the area groups that the user is allowed to arm.

If a user is permitted to disarm an area (**Disarming area groups** tab), they will automatically be permitted to arm the area as well; however, permission to arm an area (**Arming area groups** tab) does not grant permission to disarm that area.

- **Include all areas**: Select this option to permit arming of all areas in the site to this access level.
- By default, the **Schedule** is set to Always, meaning arming of the defined area group is permitted at all times. When a schedule is assigned the areas can only be armed when the schedule is valid.

## Access levels | Disarming area groups

This tab defines the area groups that the user is allowed to disarm.

If a user is permitted to disarm an area (**Disarming area groups** tab), they will automatically be permitted to arm the area as well; however, permission to arm an area (**Arming area groups** tab) does not grant permission to disarm that area.

- **Include all areas**: Select this option to permit disarming and arming of all areas in the site to this access level.
- By default, the **Schedule** is set to Always, meaning disarming of the defined area group is permitted at all times. When a schedule is assigned the areas can only be disarmed when the schedule is valid.

## Access levels | Outputs

This tab defines the outputs that are associated with this access level. These outputs can be automatically activated or toggled when users access readers or log in to keypads.

The following options must also be configured:

- To activate outputs when the user accesses a door:
  - **Reader access activates output** (**General** tab)
  - **Activate access level output** (**Expanders | Reader expanders | Reader 1/2**)
- To activate outputs when the user logs in to a keypad:
  - **Keypad access activates output** (**General** tab)
  - **Activate access level output** (**Expanders | Keypads | Options 1**)
- General options:
  - **Time to activate output** (**General** tab)
  - **Activate output until access level expiry** (**General** tab)
  - **Toggle access level output** (**General** tab)

For programming examples, see Application Note 204: Access Level Outputs in Protege GX.

## Access levels | Output groups

This tab allows you to assign an output group to this access level. The outputs in this group can be automatically activated or toggled when users access readers or log in to keypads.

The following options must also be configured:

- To activate outputs when the user accesses a door:
  - **Reader access activates output** (**General** tab)
  - **Activate access level output** (**Expanders | Reader expanders | Reader 1/2**)
- To activate outputs when the user logs in to a keypad:
  - **Keypad access activates output** (**General** tab)
  - **Activate access level output** (**Expanders | Keypads | Options 1**)
- General options:
  - **Time to activate output** (**General** tab)
  - **Activate output until access level expiry** (**General** tab)
  - **Toggle access level output** (**General** tab)

For programming examples, see Application Note 204: Access Level Outputs in Protege GX.

## Access levels | Salto doors / door groups

These tabs are only visible when the option to **Enable Salto (SHIP) integration** is enabled in **Global | Sites | Salto**. For more information, see Application Note 188: Salto SHIP RW Pro Access Integration with Protege GX or Application Note 335: Salto SHIP ProAccess SPACE Integration with Protege GX.

These tabs allow you to assign one or more individual Salto doors or door groups that users are allowed to access. Salto doors can also be assigned to individual users (**Users | Users | Salto doors / door groups**).

- By default, the **Schedule** is set to Always, meaning access to the defined Salto doors is permitted at all times. When a schedule is assigned the doors will only be accessible when the schedule is valid.

The maximum number of doors that Salto currently supports is 64,000 per database. A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

## Access levels | Cencon locks / lock groups

These tabs are only displayed when **Enable Cencon integration** is enabled in **Global | Sites | Cencon**. For more information, see Application Note 160: Configuring Cencon Integration with Protege GX.

These tabs allow you to assign one or more individual Cencon locks or lock groups that users are allowed to access. Cencon locks and lock groups can also be assigned to users via access levels (**Users | Access Levels | Cencon locks / lock groups**).

## Access levels | Keys / Key groups

These tabs are only available when key cabinet integration is enabled in **Global | Sites | Key cabinets**, and some keys or key groups have been synchronized to Protege GX. For more information, see Application Note 220: KeyWatcher Touch Integration in Protege GX or Application Note 331: KeySecure Integration with Protege GX.

These tabs allow you to assign one or more individual keys or key groups that users are allowed to access.

- By default, the **Schedule** is set to Always, meaning access to the defined keys is permitted at all times. When a schedule is assigned the keys will only be accessible when the schedule is valid.

## Access levels | Integration options

This tab is used for the KONE Office Flow integration. The Office Flow system determines what settings are available. If there are any settings you do not understand, discuss with your KONE representative.

For more information, see Application Note 361: Protege GX KONE Office Flow Integration.

# Custom fields

Custom fields are operator-defined fields that can be displayed in a user record. These can record a wide variety of data, such as text, numbers, dates, and drop drown selections.

In order to display and use custom fields you must create custom field tabs in **Users | Custom field tabs**.

## Custom fields | General

### General

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

### Configuration

- **Tab**: Defines the custom field tab where the custom field will appear in each user record. These can be created in **Users | Custom field tabs**.
- **Field type**: Defines the type of information that will be recorded in this custom field. Choose from:
  - Text
  - Numerical
  - Time
  - Date
  - Time and date
  - Option (single checkbox)
  - Link (on the user tab, you can click the **Link** button to automatically open the link)
  - Drop down box (options are defined in the **Drop down items** tab)
  - Image
- **Default value**: Optionally define a default value of the field. The required value will differ depending on the **Field type** (e.g. text, number, boolean operator).
- **Pixels**: Defines the pixel width and height when the **Field type** is set to Image.

If a custom field is changed to an Option field type after its initial creation, the option will be automatically enabled for all users (including apartment users). If you create a custom field and forget to set the field type to Option before saving, you should delete the custom field and re-add it correctly rather than changing the type.

### Record history

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

## Custom fields | Drop down items

This tab allows you to define the options that will appear in the drop down list when the **Field type** is set to Drop down box. Click **Add** to create a new drop down item.

- **Display text**: The description of the list item.
- **Value**: The ID index of the item. This determines the list order of items in the drop down.

# Custom field tabs

Custom field tabs are additional customizable tabs that appear under user records to display custom fields. You can assign custom fields to a custom field tab using the **Tab** option in **Users | Custom fields | General**.

## Custom field tabs | General

### General

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

### Record history

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

# Card template editor

Use the card template editor to create custom Photo ID templates and define the layout and information included on a user's card or label.

Photo ID is a separately licensed feature. For programming instructions, see Application Note 149: Creating a Photo ID Template in Protege GX.

## Card Template Editor Menus

### Card template properties

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.
- **Print both sides**: When this option is enabled, both sides of the card template will be printed. If this option is not enabled only the front of the card will be printed.

### Brushes

This section is used to set the color, visibility and opacity of lines, text and buttons on the card template.

1. Expand the **Brushes** section and select an item in the editor.
2. Select whether you are editing the **Background**, **Border** or **Foreground** color of the item. This will depend on the item being configured.
3. Set the colors for the item:
   - To set a solid color, click the **Solid** tab and select the color by using the color picker or entering RGB values.
   - To create a gradient, click the **Gradient** tab to display a slider bar beneath the color pickers. Click on each slider to set the color of each side individually, then adjust the sliders to achieve the desired effect.
   - To set no color (transparent), click the **Null** tab.
4. Set whether the item is **Visible** or **Hidden**.
5. Set the **Opacity** of the item.

### User fields

This section allows you to add user fields to the card template in various formats. For example, you might display each user's name and card expiry date (text), credential details, photo, and custom data such as badge number in a bar code form.

1. Expand the **User fields** section and click **Add** to add a new user field.
2. Set the **Field type**. The options are:
   - **User fields**: Standard fields available for any user, e.g. name, facility/card number, expiry date, etc.
   - **Photo holder**: The user photo as entered in the **Users | Users | Photo** tab.
   - **Extended fields**: The fields displayed on the user's **Extended** tab. **Display predefined custom fields in users** must be enabled in **Global | Sites | Display**.

     See the **Card printing actions** below to automatically populate some fields when the card is printed.

- **Custom fields**: Any custom fields defined in **Users | Users | Custom fields**.
- **Mask**: A black stripe used to isolate sections of the card where printing should be avoided. The mask is automatically placed in the default position for the type of mask required (e.g. a magnetic stripe mask is placed horizontally across the width of the card), but it can be moved and resized as necessary.
- **Bar code**: A bar code containing data from a relevant field from the **Extended** user tab. Select the required custom field, then choose the bar code format required for your system.

3. Drag and drop the required item(s) onto the card template. Then **Close** the popup window.
4. Move the user field by clicking and dragging, resize it using the squares in the corners, and rotate it using the circles in the corners.
5. For text fields, set formatting details such as **Font**, **Font size** and text style.

The **Data** field is read only and does not need to be configured.

## Lines

This section allows you to draw basic lines and shapes on the card template.

1. Expand the **Lines** section and click **Add**.
2. Your cursor will transform into a **+** shape. Click somewhere on the design field to create the first node of the line.
3. To create an additional node or corner, click once. The line can have as many corners as necessary, allowing you to create complex shapes.
4. To complete the line, double click.
5. Give the line a descriptive **Name**.
6. Once the line is complete you can:
   - Set the **Line width** in the **Lines** section
   - Set the color with the **Border** attribute in the **Brushes** menu
   - Move the line by clicking and dragging within the dotted box
   - Resize the line by clicking and dragging the squares at the corners
   - Rotate the line by clicking and dragging the circles at the corners
   - Move the line in front of or behind other elements using the **Front** and **Back** buttons in the toolbar.

## Text

This section allows you to add text labels to your card template (e.g. field descriptions, notes).

1. Expand the **Text** section and click **Add**.
2. Your cursor will transform into a **+** shape. Click and drag somewhere on the design field to create a text box.
3. Give the text a descriptive **Name**.
4. In the **Text** field, enter the required text.
5. Once the text is complete you can:
   - Set the **Font**, **Font size** and text style in the **Text** section
   - Set the color with the **Foreground** attribute in the **Brushes** menu
   - Move the text box by clicking and dragging within the dotted box
   - Resize the text box by clicking and dragging the squares at the corners
   - Rotate the text box by clicking and dragging the circles at the corners
   - Move the text box in front of or behind other elements using the **Front** and **Back** buttons in the toolbar.

## Images

You can add images such as company logos and background images to the card template.

1. Click **Add**, then enter a filepath or click the ellipsis **[...]** to browse to an image. The image can be in .bmp or .jpg file formats.

   Ensure that all images are located in a shared network folder that clients have access to. If the link to an image is broken or the client machine is not able to access it, the image will not appear in the Protege GX client.

2. Your cursor will transform into a **+** shape. Click and drag somewhere on the design field to add the image.
3. Give the image a descriptive **Name**.
4. Once the image has been completed you can:
   - Move the image by clicking and dragging within the dotted box
   - Resize the image by clicking and dragging the squares at the corners
   - Rotate the image by clicking and dragging the circles at the corners
   - Move the image in front of or behind other elements using the **Front** and **Back** buttons in the toolbar.

     You can use the **Back** button to create a background image.

## Card encoding

This section allows you to encode ICT secured MIFARE (diversified MIFARE) cards or print magstripes, if the card printer is capable of encoding cards. These processes take place if the operator selects **Print & process template** or **Process template only** when printing a user card from **Users | Users | Photo**.

- **ICT sector**: Enable this option to instruct the card printer to read or write cards with ICT secured MIFARE (diversified MIFARE) encoding.

  Contact ICT for more information about card encoding.

- **Process**: The process that will take place when the card is printed:
  - **Read**: When the card is printed the encoder reads the existing credential and enters it in the user's **Facility/Card number** field.
  - **Write**: When the card is printed the encoder writes the credential from the user's **Facility/Card number** field to the card. The facility and card number must match those included in the encoder.ini file.
- **Magnetic stripe**: With this option enabled, when the card is printed the printer can also write a magstripe based on user data. Ensure that you have included the appropriate mask in the **User fields** section above.
- **Track1-3**: Set the data that will be written to each track of the magstripe. The available fields are those from the **Users | Users | Extended** tab.

## Card printing actions

This section allows the template to modify the user record when the card is printed. This can be used with the fields in the **Users | Users | Extended** tab. For example, you could configure the card template to update the **Badge type** field with the type of card that is being printed.

The **Extended** tab is only visible when the option to **Display predefined custom fields in users** is enabled in **Global | Sites | Display**. See also the **Save badge number and date after card printing** option in **Global | Sites | Site defaults**.

The available actions are:

- **Update user field with print date**: The date of printing will be written to the specified user field.
- **Update user field with value**: A specific string or value will be written to the specified user field. The **Value** type depends on the type of user field selected (for example, the **Expiration date of badge** field requires a date input).
- **Copy value between user fields**: The data in one user field will be overwritten with information from another user field. The two fields must have the same type (e.g. both text or both date). User custom fields defined in **Users | Custom fields** can also be entered here.

## Card Template Editor Toolbar

The Toolbar provides functionality for controlling the layout and positioning of elements added to a card template.

| Button | Function |
|---|---|
| Redo | Enables you to reinstate (redo) the last action that was undone |
| Undo | Enables you to undo the last action |
| Copy | Copies the selected object(s) to the clipboard |
| Paste | Pastes the content from the clipboard into the design field |
| Delete | Removes the selected object from the design field |
| Snap | With this option enabled, when you draw, resize or move an object it will align or 'snap' to the nearest objects in the design field, even if the ruler is not visible. If your object does not move where you desire, turn this option off. |
| Angle | Aligns the selected object(s) to the nearest polar grid angle |
| Ruler | Select this option to toggle the ruler on or off |
| Front | Moves the selected object in front of other objects |
| Back | Moves the selected object behind other objects |
| Aln top | Aligns all selected objects to the top edge of the last object selected |
| Aln btm | Aligns all selected objects to the bottom edge of the last object selected |
| Aln lt | Aligns all selected objects to the left edge of the last object selected |
| Aln rt | Aligns all selected objects to the right edge of the last object selected |
| Lndscp | Toggles the layout of the card between landscape and portrait orientation |

# Events Menu

The events menu contains the functions used to create event filters, configure operator alarms, and create automatic actions which occur upon specific events.

## Event search

The event search feature allows you to generate one-off temporary user reports that can be printed, exported or emailed. This provides a simple way of viewing what is happening in the system.

Event searches are similar to event reports (see page 152), but the configuration cannot be saved and fewer customization options are available.

### Running an Event Search

1. Navigate to **Events | Event search**.
2. Select the time period for the events. Choose a period from the available list or enter a specific start 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, select the event type(s) to include.
   - Click **Add** to open the **Select event types** window.
   - The event types are sorted into categories (e.g. All area events). Select event types and categories by highlighting them and clicking **OK**, or by dragging and dropping them into the main window.
   - When all required event types have been added, click **OK**.

   It is currently not possible to multi-select events.
5. In the **Records** tab you can specify up to two record filters to narrow the search. For example, you might select a group of users and a door to search for user events relating to that particular door.
   - Click **Add** to open the **Select devices** window.
   - Select the **Device type** (and **Controller**, where applicable), then select the **Devices** from those available.
   - Create a second record filter if required.
6. Click **Find** to start the search.
7. A temporary report is generated and displayed in a grid view. You can 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.

   You can use the grid view to further sort, group and filter the results. For more information, see Working with the Grid View (page 167).
8. The **Save** icon allows you to save the current report layout so that it can be used for other searches or reports generated by this operator.
9. If more than 200 events are returned, use the **Previous** and **Next** buttons to navigate between results that span multiple pages.
10. Click the **Print** icon to open the print preview window where you can print, export or email the results (see page 170).

# Event filters

Event filters are used to sort and categorize event and alarm data. They can be used to determine which events will trigger alarms and other actions, as well as which events are included in reports and live status lists.

For more information and programming instructions, see Application Note 332: Setting Up Event Notifications in Protege GX.

## Event filters | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

## Event filters | Event types

- **Include all event types**: Enable this option to include all event types in the filter. This means any event type will be included (for example, in an event report), provided that it meets the conditions in the **Records** tab.

### Event types

Click **Add** to select the event types that will be included by the filter. The event types are sorted into categories (e.g. All Area Events). You can select event types and categories by highlighting them and clicking **OK**, or by dragging and dropping them into the main window.

## Event filters | Records

You can define up to two record filters to further narrow what the event filter will include.

- If any records are entered in these fields, the event filter will only include events involving those records.
- If no records are entered in these fields, the event filter will include events for all records.

Click **Add** to enter records for each field. Select a **Device type** (e.g. output, area) and **Controller** if required, then check the boxes for the relevant records and click **OK**.

# Alarms

Alarms are specific events that generate notifications for Protege GX operators. The alarm notifications must be acknowledged by an operator, either from the popup notification or on the predefined All Alarms status page.

This type of alarm is an operator alarm - i.e. an event that generates a notification to prompt action from an operator. This is different from area alarms that are generated on site and reported to the central monitoring station. Events which cause area alarms do not automatically generate operator alarms - they must be specifically configured.

When an operator receives an alarm notification they can right click on the event and acknowledge the alarm. Optionally, it is possible to leave a comment on the alarm. If desired, they can also temporarily dismiss the alarm by clicking the icon in the upper right of the popup window. Operator display settings for alarms can be modified under **Global | Roles | Display**.

For more information and programming instructions, see Application Note 332: Setting Up Event Notifications in Protege GX.

**Known issue:** If a second popup window (such as the find tool or area arming dialog) is opened while the alarms window is already open, it may appear behind the alarms window and render the alarms window unresponsive. If this occurs, you can close the second window by pressing **Escape**, or use **Windows + Left/Right/Up** to move the second window to another part of the screen. To avoid this issue, move the alarms window before opening any additional popup windows.

## Alarms | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Instructions**: The text entered here will be included in the alarm popup in the Instructions column. This is useful for entering brief instructions for the operator when they view the alarm. Instructions can also be sent to personnel using the email on event action (see **Events | Actions**).

  This field only supports 256 characters. Any characters past this limit will not be saved.
- **Instructions 2**: This field can be used to enter instructions in a second language. These will be displayed in the alarm event in the other language that was installed with the software.

  This field only supports 256 characters. Any characters past this limit will not be saved.
- **Event filter**: This event filter is used to determine which events will trigger the alarm notification.
- **Floor plan**: The floor plan associated with the alarm can be displayed by right clicking the event on a status page.
- **Alarm priority**: The priority assigned to the alarm determines the order in which the alarms are displayed in the notification popup and status page. Higher numbers will appear higher on the list. Alarm priorities can be created in **Events | Alarm priorities**.
- **Alarm routing list**: The alarm routing record associated with the alarm determines the 'path' the alarm will travel - i.e. which operator workstations will receive the alarm first, and which will be notified if the first do not acknowledge it. Alarm routing can be configured in **Events | Alarm routing**.

- **Alarm acknowledgement comments**: Set whether comments are required, optional or not permitted when operators acknowledge alarms. If Never is selected the alarm comment window will not be displayed.

  When multiple alarms are acknowledged at once, or the same event is included in multiple alarm records, alarms which require or allow comments will take priority over those that do not. For example, if Alarm A is set to Must and Alarm B is set to Never, when both alarms are acknowledged together the operator must enter a comment.

- **Alarm sound**: Set the custom sound that will be played when this alarm occurs. You can add custom alarm sounds in **Global | Global settings | Sound**.

  If this option is not set, the **Alarm sound** setting in **Global | Global settings | Sound** will be used.

## Camera options

- **Allow camera popup**: Enable this option to pop up a camera window alongside the alarm event popup. This will display the camera associated with the event (i.e. the **Camera** assigned to the specific door, area, input or output).

  The camera popup obeys alarm routing rules, allowing it to be routed to particular workstations. You can also restrict the camera popup for specific operators using the **Allow camera popup** setting in **Global | Roles | Display**.

## Record history

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

# Actions

Actions enable triggering a process that runs automatically when specific events occur. For example, you can send events by email to notify relevant people, trigger a camera or DVR to focus on the source of the event, or send events to integrated third-party systems.

The default preconfigured action is Save Events, which automatically saves all incoming events to the Protege GX database. This cannot be edited.

## Actions | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Type**: Select the type of action that will occur when a relevant event is recorded. Different configuration setting are available/relevant depending on which type is selected. Choose from:
  - **Save to database**: Saves a record of the event to the ProtegeGXEvents database. This option is only used for the preconfigured Save Events action.
  - **Send PTZ command**: Sends a PTZ command to a connected DVR. This causes a camera to move to a specific preset position. For example, when there is a door forced event you might want a nearby camera to focus on that door.
  - **Popup camera window**: A popup window displays live and archived camera feeds from a camera to operators.
  - **Run script**: This option is reserved for future development.
  - **Send email**: Sends an email about the event to one or more specified email addresses.
  - **Send event:** Sends the event to a set IP address in XML format. This can be used to create custom integrations with third-party systems.
  - **Custom DVR action**: Sends a custom command string to a connected DVR. This can be used to create custom integrations with DVR systems.
  - **Delete visitor card**: Automatically signs out the visitor who triggered the event. The visitor record will either be disabled or deleted based on the **Checkout mode** setting (**Visitor | Templates | General**). This can be used to automatically sign out visitors as they leave the building.

    For this action to function, the event filter must include user events.
  - **Send event to MSMQ**: Transmits the event to a queue using Microsoft Message Queuing (MSMQ) which can then be read by third-party systems.
  - **Send muster report by email**: Sends a muster report to a specific email address. This might be used in the event of a fire or lockdown to immediately ascertain which users are on site at the time of the emergency.
- **Event filter**: This event filter determines which events will trigger the action.
- **PTZ command**: If the type is set to Send PTZ command, this field determines the command that will be sent to the connected DVR.

  PTZ Commands can be programmed in **Monitoring | Setup | PTZ commands**.
- **Popup camera**: If the type is set to Popup camera window, this field defines which camera feed is used by the popup window. Choose from:

- Default camera associated with event
- Door entry camera
- Door exit camera
- Select camera from list

- **Camera**: If Select camera from list is selected above, set the specific camera that will be displayed in the popup window. Cameras can be programmed in **Monitoring | Setup | Cameras**.
- **Script**: This option is reserved for future development.

## Email settings

These settings are available when the type is set to Send email. Various field variables are available for use with the send email action, which allow you to include information about the specific event that has occurred (see next page).

For more information and programming instructions, see Application Note 332: Setting Up Event Notifications in Protege GX.

Automated email features in Protege GX require an SMTP mail server to be configured in **Global | Global settings | Email settings**.

- **Email address**: The address or addresses that the email will be sent to.

  You can add multiple email addresses in this field, separated by semicolons; however, this field is limited to 128 characters. If more addresses are required create a duplicate action.

- **Subject**: Defines the subject of the email.
- **Message**: Defines the message content of the email.

## IP settings

These settings are available when the type is set to Send event. The events will be sent in XML format.

- **IP address**: The IP address where the XML events will be sent.
- **IP port**: The port to which the XML events will be sent.

## Custom DVR command

These settings are available when the type is set to Custom DVR action.

- **DVR**: The DVR that the command will be sent to. DVRs can be programmed in **Monitoring | Setup | DVRs**.
- **Command string**: The string that will be sent to the DVR. This will be determined by the requirements of the third-party system.

## MSMQ

This setting is available when the type is set to Send event to MSMQ.

For more information, see Application Note 144: Configuring MSMQ Integration.

- **Message queue**: The name of the message queue that the event data will be sent to. It's a good idea to give the queue a name that relates to what it is being used for, such as 'ALARMS'.

## Email settings (Muster Report)

These settings are available when the type is set to Send muster report by email.

Automated email features in Protege GX require an SMTP mail server to be configured in **Global | Global settings | Email settings**.

- **Email address**: The address or addresses that the email will be sent to.

  You can add multiple email addresses in this field, separated by semicolons; however, this field is limited to 128 characters. If more addresses are required create a duplicate action.

- **Muster report**: The muster report that will be sent when the action is triggered. Muster reports can be created in **Reports | Setup | Muster**.

### Record history

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

## Email Field Variables

The send email action type provides support for a number of field variables which can be entered in the **Subject** or **Message** fields. When the email is sent, each placeholder will be substituted with specific information about the triggering event.

Field variables are case sensitive.

| Field Variable | Information |
|---|---|
| `<EVENTID>` or `<EVENT_ID>` | The Database ID of the logged event. |
| `<FIELDTIME>` or `<FIELD_TIME>` | The field time, or time the event was generated at the controller. |
| `<LOGGEDTIME>` or `<LOGGED_TIME>` | The logged time, or time the event was logged by the server. |
| `<DESCRIPTION>` | The description or full text of the event as it appears in the event log. |
| `<DESCRIPTION2>` | The description of the event in the second language. |
| `<DOORNAME>` or `<DOOR_NAME>` | The name of the door involved with the event. |
| `<USERNAME>` or `<USER_NAME>` | The name of the user involved with the event. |
| `<USERID>` or `<USER_ID>` | The Database ID of the user involved with the event. |
| `<FACILITYNUMBER>` or `<FACILITY_NUMBER>` | The facility number of the user credential involved with the event. |
| `<CARDNUMBER>` or `<CARD_NUMBER>` | The card number of the user credential involved with the event. |
| `<ALARM>` | A binary value that indicates whether the event is classed as an alarm.<br>• **0** = The event is not an alarm.<br>• **1** = The event is an alarm. |
| `<INSTRUCTIONS>` | The text of the **Instructions** field for alarms. |
| `<INSTRUCTIONS2>` | The text of the **Instructions 2** field for alarms (instructions in the second language). |

| Field Variable | Information |
| --- | --- |
| <ACKNOWLEDGED> | A binary value that indicates whether the event has been acknowledged. This only applies to alarms.<br>• **0** = The alarm has not been acknowledged.<br>• **1** = The alarm has been acknowledged. |
| <COMMENTS> | The text of any comments made by the operator who acknowledged the alarm. |

# Alarm priorities

Alarm priorities allow you to determine the order in which alarms are displayed within the alarm popup and event windows. Alarms with a higher priority will appear higher in the list.

Alarm priorities can also be used in alarm routing to ensure that high priority alarms are redirected to additional workstations if they are not acknowledged.

## Alarm priorities | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Priority**: The higher the priority, the higher an alarm will appear in any list of multiple alarms.

### Record history

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

# Alarm routing

Alarm routing records define which workstation groups receive alarms and in what order. This allows you to route an alarm to specific workstations rather than all workstations at once, and transfer the alarm to another workstation if it is not acknowledged within a defined timeframe.

To create an alarm routing record, you must first configure workstations and workstation groups. SIP settings do not need to be programmed for the workstation. Alarm routing records can be assigned to the **Alarm routing list** in the **Events | Alarms** programming.

## Alarm routing | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

## Alarm routing | Workstation groups

This tab lists the workstation groups that are available for alarm routing.

- **Name**: The name of each workstation group. These can be programmed in **Events | Workstation groups**.
- **Transfer after**: Defines the period (in seconds) that alarms will wait at this workstation group before being routed to the next group in the list.
- **Transfer priority**: Select an alarm priority that will be used for this workstation group. When set, only alarms with that priority will be routed to the group. Alarms with any other priority will be transferred to the next workstation group in the list. If this field is not set, all alarms will be routed to this workstation group.
- **Routing order**: Defines the sequence in which alarms will be routed. The workstation group that receives alarms first should be set to 1, the second group to 2, etc.
- **Active**: Enable this option to include the workstation group in the routing list.

# Workstations

Workstations identify specific Protege GX client computers on the network. It is not necessary to program a workstation record to run the Protege GX client, but they are used for some specific applications:

- Workstation records are used in workstation groups and alarm routing to send alarms to defined workstations (see **Events | Alarm routing**).
- Workstations are also used to configure Protege GX to act as a SIP client, enabling operators to hold calls with an intercom directly within the Protege GX interface using VoIP.

  VoIP capability is a separately licensed feature. A license is required for each intercom that is connected, and the intercom records must be programmed in **Monitoring | Setup | Intercoms**. For more information, see Application Note 339: Integrating SIP Intercoms with Protege GX Workstations.

- The Cencon integration requires each key box to be assigned to a workstation.

  For more information, see Application Note 160: Configuring Cencon Integration with Protege GX.

## Workstations | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Computer name**: The name of the Protege GX client computer on the network. This must be unique.

### SIP client

Some settings can only be configured on the workstation that you are currently using. Each workstation must also be registered with an extension in the SIP server.

- **Server address**: The domain name or IP address of the SIP server.
- **Account name**: The name of the SIP extension that has been allocated on the SIP PBX system for this workstation.
- **Account password**: The password of the SIP extension that has been allocated on the SIP PBX system for this workstation.
- **Realm**: The security domain this account is valid under. For example, for an Asterisk based PBX server you would enter Asterisk, while for a 3CX server you would enter 3CXPhoneSystem.
- **SIP port**: The UDP port that will be used for communications with the SIP PBX server.
- **Network interface**: The network interface card used for communications.
- **Microphone**: The microphone that is connected to the workstation. A microphone must be connected for the workstation to register as a SIP client.
- **Default microphone setting**: Defines the microphone level that will be used when the call window is launched.
- **Speakers**: The speakers that are connected to the workstation.
- **Default speaker setting**: Defines the speaker level that will be used when the call window is launched.

### Cencon key box

For more information on the Cencon integration, see Application Note 160: Configuring Cencon Integration with Protege GX.

- **Key box ID**: Each Cencon key box must be assigned to a Protege GX client workstation.

  Before attempting to assign a key box to a workstation, ensure that the key box is connected to the workstation via USB and that it is visible in the Centran Configuration Manager client's list.

## Record history

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

# Workstation groups

Workstation groups are used to define which workstations will receive alarms and in which order. For more information, see Alarm routing (page 148).

## Workstation groups | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

## Workstation groups | Workstations

This tab displays a list of programmed workstations. Enable the **Active** checkbox to include the necessary workstations in the workstation group.

# Reports Menu

Use the reports menu to create and view a range of reports. With Protege GX's flexible reporting options you can easily obtain detailed and relevant information as required. All reports can be filtered, grouped and sorted, then printed, emailed, or exported to a range of file formats.

The following reports are available in Protege GX:

- Event reports
- Muster reports (license required)
- Attendance reports (license required)
- User reports
- Central station reports (generates a reporting map for use by monitoring stations)
- Operator permission reports

## Setting up Reports

You can create and save event, muster, attendance and user reports under the **Reports | Setup** menu. Each report type has a variety of options that enable you to find the information you need. In addition, it is possible to set up regular file exports or emails of saved report configurations.

### Reports | Setup | Event

Event reports allow you to view what has happened or is currently happening within the system with ease. You can use event filters (**Events | Event filters**) and record groups to ensure that only relevant events are included in each report.

By default, there are three preconfigured event reports:

- All Events
- All Alarms
- All Acknowledged Alarms

Others can be created as required. Once an event report record has been created it can be run as a report, allowing the results to be reviewed, grouped and exported as required. Alternatively, you can include an event report on a status page or floor plan, providing a live view of events within the system.

### Event reports | General

#### General

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

### Configuration

- **Display**: Read only field that indicates the description that is displayed in the event report window.
- **Alarms**: Defines which types of events to include in the event report. Choose whether to include all events, all alarms, or only acknowledged alarms.

  Event reports with alarms can be included on a status page and used to acknowledge active alarms.
- **Number of events**: Defines the maximum number of events to include, allowing you to limit the number of events that will be included in the results.

### Integration

- **Sync to Milestone**: When the Milestone XProtect Bidirectional integration is enabled, use this setting to synchronize an event report to XProtect. This allows you to view live events from Protege GX in the XProtect interface.

  For more information, see Application Note 358: Milestone XProtect Bidirectional Integration with Protege GX.

### Event filters

Click **Add** to select one or more event filters. The following options are available in the popup window:

- **Event filter**: The event filter that will be used to filter the results of the event report. Event filters can be programmed in **Events | Event filters**.
- **Access all record groups**: The event filter will include records from all record groups. Otherwise, you must select one or more record groups to apply to the filter.

### Default event report filter

If a default report layout has been created for this report you can view the saved filters here. For more information, see Saving Report Layouts (page 170).

- **Edit in report view**: Clicking this button opens the event report in a breakout window, allowing you to run the report, configure filters, and save the default report layout.

### Record history

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

## Event reports | Columns

This tab allows you to define which columns will appear in the report. Almost any field in the system can be included in an event report, allowing operators to create highly customized reports with endless options for grouping and filtering.

To add a column to an event report, click **Add**. Select the **Table** (e.g. access levels, doors) and **Tab** (e.g. General, Options) to display the fields that are available for that particular tab.

### Columns

- **Record type**: The type of record that the column/field is drawn from.
- **Name**: The English name of the field in the software.
- **Second language name**: The second language name of the field in the software.
- **Customized name**: The operator can define an alternative English name for the field. This will appear in the column header of the report.
- **Customized second language name**: The operator can define an alternative second language name for the field. This will appear in the column header of the report when it is run in the second language installed with

the software.

Customized names are not automatically translated. Translations must be added manually.

# Reports | Setup | Muster

Muster reports allow you to keep track of which users are currently in a room, building or site. By monitoring the external (entry and exit) doors for a specific zone the muster report can generate a list of all users who have been active within a specified time and whether they currently are inside or outside that zone.

In addition to manually running the muster report you can also include it on a status page, providing regularly updated information about user status within the system.

Muster reports are especially useful in emergency situations where it is vital to know exactly which personnel are on site. You can configure an action to automatically email muster reports following specific events, such as a fire alarm activation (see page 143).

Muster reports are a separately licensed feature.

## Muster reports | General

### General

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

### Configuration

- **Period**: The time period which will be included in the muster report. For example, setting the period to 8 hours provides data about each user's most recent door access within in the previous 8 hours.
- **Report type**: The following types of muster report are available:
  - **Standard**: Users who have not been active in the selected **Period** will be excluded from the report.
  - **Detail / List**: Users who have not been active in the selected **Period** will be included in the report with an 'Unknown' status. There is no difference between the detail and list options.
- **Refresh rate**: The frequency at which the report data will be updated when the muster report is displayed on a status page. Unlike event reports, muster reports do not provide a 'live' list of events, but will update every 5 or 30 minutes.

  Actively running a report will always provide the most up to date information.
- **Time zone**: Determines what time zone the report will use to calculate the activity period. This should match the controller (field) time to ensure that the correct data is included in the report. The Use server time zone option will use the current time zone of the Protege GX server.

  For example, the controller may be located in Eastern Standard Time (EST) while the server is in Pacific Standard Time (PST). The operator runs a report at 3:15pm PST, which is equivalent to 6:15pm EST. If the **Time zone** for the report is set to PST and the **Period** is set to 30 minutes, the data in the report will begin at 5:45pm (field time) instead of 2:45pm (server time).

### Record history

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

## Muster reports | Doors

In this tab you can define the entry and exit doors (or chokepoints) that the muster report will report on. For example, to generate a report on all users who are currently inside a specific building you would track access on all external doors.

### Doors

Click **Add** to open the selection window and choose which doors to include.

- **Name**: The name of the door which the muster report will
- **Direction**: Determines which access types will be used to track user location.
  - **Both**: Both entry and exit access will be tracked for this door. This should be used for outer perimeter doors which serve as both entry and exit points. When a user enters a door they are identified as being on site (their **Status** is set to In). When they exit a door they are identified as off site (their **Status** is set to Out).
  - **Entry**: Only entry will be tracked for this door. This should be used for internal doors. When a user exits an internal door they are still on site in another area, so their **Status** will remain set to In.
  - **Exit**: Only exit will be tracked for this door. This should be used for external access points that are only used as exits. When a user exits one of these doors, their **Status** will be set to Out.

## Muster reports | Columns

This tab allows you to define which columns will appear in the report. As well as the default muster report columns, muster reports can also include a range of user fields and any custom field, allowing operators to create customized reports with additional options for grouping and filtering.

To add a column to a muster report, click **Add**. Select the **Table** (e.g. users) and **Tab** (e.g. General, Options) to display the fields that are available for that particular tab.

Muster reports displayed on status pages will only include the default columns.

### Columns

- **Record type**: The type of record that the column/field is drawn from.
- **Name**: The English name of the field in the software.
- **Second language name**: The second language name of the field in the software.
- **Customized name**: The operator can define an alternative English name for the field. This will appear in the column header of the report.
- **Customized second language name**: The operator can define an alternative second language name for the field. This will appear in the column header of the report when it is run in the second language installed with the software.

  Customized names are not automatically translated. Translations must be added manually.

# Reports | Setup | Attendance

Attendance reports make it easy to monitor user movements, assisting payroll and HR management. Using the entry and exit information that is already recorded as part of Protege GX's normal operation, attendance reports can track employee absenteeism, monitor start, finish and break times, and account for overtime.

Attendance reports are a separately licensed feature. For more information, see Application Note 308: Time and Attendance in Protege GX. For a programming example, see Application Note 163: Configuring Shift Reports in Protege GX.

## Attendance reports | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.
- **User source**: Determines how the report selects the users to be included. Choose from:
  - **User list**: The report will include all users individually selected in the **Users** tab.
  - **Access level**: The report will include users who have any access level(s) selected in the **Access levels** tab.
  - **Record group**: The report will include all users included in the **User record group** selection.
- **User record group**: If the **User source** is set to Record group, the report will include all users in this record group.
- **Report type**: Defines the type of attendance data that the report will generate. Choose from:
  - **Daily first in last out**: The report will use the first entry event and the last exit event each day to determine the user's attendance and hours worked. Any events between these times are ignored, meaning any time spent off site during the day is not deducted.
  - **Shift first in last out**: The report will use the first entry event and the last exit event each day, and any additional entry/exit events during the day. Protege GX then matches the various entry/exit events against the defined shift and break times to calculate the hours worked.
  - **Daily first and last user event**: The report will use the first and last user event each day to determine attendance and hours worked. Any events between these times are ignored, so that any time spent off site during the day is not deducted.
  - **Shift first and last user event**: The report will use the first and last user event each day, and any additional events during the day. Protege GX then matches the various entry/exit events against the defined shift and break times to calculate the hours worked.
  - **First scan in**: The report will show the earliest entry event for each user on each day.
  - **Last scan out**: The report will show the latest exit event for each user on each day.
  - **First scan in and last scan out**: The report will show the earliest entry event and the latest exit event for each user on each day.
  - **Late in**: The report will show the first entry time for each user on the days when the user was late to enter.

    This is calculated after the **Grace period** has been applied.
  - **Top 10 late in**: The report will show the 10 users with the highest number of late entries in the selected period.
  - **Late out**: The report will show the last exit time for each user on the days where the user was late to exit.

    This is calculated after the **Grace period** has been applied.

- **Early in**: The report will show the first entry time for each user for the days where the user was early to enter.

  This is calculated after the **Grace period** has been applied.

- **Early out**: The report will show the last exit time for each user for the days where the user was early to exit.

  This is calculated after the **Grace period** has been applied.

- **Absent**: The report will show the users with no time entry data for any of the days covered by the report.
- **Top 10 absent**: The report will show the 10 users with the highest number of days absent in the selected period.

- **Time zone**: Determines what time zone the report will use to calculate the relevant period. This should match the controller (field) time to ensure that the correct data is included in the report. The Use server time zone option will use the current time zone of the Protege GX server.

  For example, the controller may be located in the United States, while the server is located in Australia. On the morning of April 29th in Australia, it is the evening of April 28th in the US. With the time zone for the report set correctly, when the operator runs a report for the previous day it will generate data for April 27th (field time) instead of April 28th (server time).
- **Unscheduled days worked (excluding public holidays)**: When this option is enabled the report will only display entries for days that users worked that were outside the configured shift times (see the **Shift times** tab). Time worked on public holidays is excluded. This allows you to calculate any overtime worked on weekends or other days off.

  This option only functions correctly when the **Shift type** (**Shift times** tab) is set to Weekly (i.e. fixed). Unexpected results may be generated when the **Shift type** is set to Rotation.

- **Public holidays worked**: When this option is enabled the report will only display entries for days that users worked during public holidays (see the **Public holidays** tab). This allows you to calculate any overtime worked on public holidays.

  This option only functions correctly when the **Shift type** (**Shift times** tab) is set to Weekly (i.e. fixed). Unexpected results may be generated when the **Shift type** is set to Rotation.

- **Report print template**: This field defines the level of detail that will be included in the report, and the types of details that are required. Choose from:
  - **Summary**: The report displays a daily attendance summary for each user.
  - **Detail**: The report displays a detailed attendance breakdown for each user each day, including start, break and finish times, and the corresponding in and out calculations for each event. This template also allows the addition of extended custom user fields in the **User Fields** tab.
  - **Summary ICT**: The report is generated in a CSV format that provides a summary of each user's attendance and includes their employee code and pay code, to assist in payroll generation. This template also allows the addition of extended custom user fields in the **User fields** tab.
  - **Summary MYOB**: The report is generated in a CSV format that can be directly read into the MYOB program. It provides a summary of each user's attendance and includes fields for employee code and pay code to assist in payroll generation, and department and cost center fields for wage cost tracking.
    - The **Employee code** is set in the **User fields** tab.
    - The **Pay code** is set in the **Normal pay code** field on the **General** tab.
    - The **Department** and **Cost centre** columns provide fields in the CSV file that can be manually populated with details from MYOB.
  - **Action HRM**: The report is generated in a CSV format that can be directly read into the ActionHRM program. It provides a summary of each user's attendance, including the entry and exit times and total hours worked.

  For some **Report Type** options only the Summary print template is available.

- **Grace period**: This field defines the time (in hours and minutes) that a user may be late or early before suffering a time deduction. This prevents employees from being unnecessarily penalized for not clocking in exactly on time.

  For example, if the grace period is set to 5 minutes and a user badges in 3 minutes late the time will not be deducted from their total hours worked. However, if the user is 10 minutes late the entire 10 minutes will be deducted.
- **Normal pay code**: This field specifies the **Pay code** column that is used in the Summary ICT and Summary MYOB report print templates.

### Period

- **Period**: The period of time covered by the report. Choose from the previous day, week, two weeks or four weeks, or select Custom period to define a specific start and end date.
- **Starting**: Determines which day of the week the report will start from. For example, a report with a **Period** of Previous week starting on Monday will display data from 00:00am on Monday to 11:59pm Sunday.
- **Start date**: If the **Period** is set to Custom period, this field determines the date the attendance report will start from.
- **End date**: If the **Period** is set to Custom period, this field determines the date the attendance report will end on.
- **Prompt for date**: Instead of using the period defined in the above fields Protege GX will prompt the operator to enter a period each time the report is run.

### Record history

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

## Attendance reports | Shift times

### Shift type

- **Shift type**: There are two options for defining shifts in an attendance report: Weekly or Rotation. The weekly option is used for regular, repeating shifts which do not run overnight. The rotation option allows you to configure rotating shifts, multiple shifts per day and night shifts.
- **Rotation length**: The number of days in the shift rotation. For example, a hospital may assign shifts on a 10 day cycle.
- **Rotation start date**: The date on which the rotation will begin.

### Shift details

If the **Shift type** is set to Weekly, this section allows you to set which days of the week will be included in the shift, and the **Start time** and **End time** for each day.

If the **Shift type** is set to Rotation, this section allows you to configure and review which shifts will occur on which days of the rotation. To create a rotation:

1. Create any shift types required in **Reports | Setup | Shift types**.
2. Set the **Rotation length** and **Rotation start date** as above. The mini calendar at the bottom of the programming page will display a single cycle of the rotation beginning at the start date.
3. **Add** the required shift types to the list. Shifts may be included any number of times in a rotation.

   If required, you can create further shift types by clicking **Add**, then **Create shift type**.
4. Use the drop down to select the first shift type.
5. In the mini calendar, click on each date which includes that specific shift type. The days when the shift occurs will be marked with the shift type's color.

   If you need to remove a shift type from a day, set the dropdown to **No shift** and click on that day.

6. **Save** the record, then click **Calendar view** to review when the shift will occur on a yearly calendar.
7. Repeat the above for other shift types.

## Attendance reports | Break times

When the **Shift type** (**Shift times** tab) is set to Weekly this tab allows you to define the scheduled breaks which will occur on each day. These will be used with certain **Report type** settings.

You can enter up to 6 breaks for each day. Check the box beside each break to enable that break for every day on the weekly schedule.

- **Name**: A name for the break, e.g. 'Morning Tea'.
- **Start/End**: The start and end times for the break. These define the range of time in which the employee is allowed to take the break. For example, employees might be allowed 30 minutes for lunch, which can be taken any time between 12:00pm and 2:00pm.
- **Duration**: The length of the break in minutes. This will be used to calculate the employee's hours worked and time deductions.

  The duration of the break must be shorter than the space between the start and end times. For example, for a 10 minute break starting at 10:30am the end time should be at least 10:41am to allow for the full length of the break.
- **Calculation**: Determines how the break time will be used in attendance calculations. Exclude deducts the break duration from the hours worked, so the break is unpaid. Include does not deduct the break.

## Attendance reports | Users / Access levels

If the **User source** (in the **General** tab) is set to User list, you can add to the **Users** tab the specific users who will be included in this report.

If the **User source** is set to Access level, you can add to the **Access levels** tab the access levels that will be included in this report.

## Attendance reports | Allowed doors

This tab allows you to set which doors will be used for generating the attendance data. When a user enters a door they will be counted as on site or clocked in. When a user exits a door they will be counted as off site or clocked out. Therefore, typically the external doors of a site, building or workspace should be used.

- **Doors**: Click **Add** to select which doors will be used to determine when employees are working. These doors can be used to clock in and out of a shift or break. For example, if you are creating an attendance report for warehouse staff, you should ensure that you track the entry and exit doors to the warehouse.
- **Direction**: Set the direction that will be tracked for each door:
  - **Both**: Use for doors that serve as both clock in and clock out points.
  - **Entry**: Use for access points that are only used to clock in. This can be used for internal doors, to allow users to clock in when they are already inside the building.
  - **Exit**: Use for access points that are only used to clock out.

## Attendance reports | User fields

User custom fields and extended fields can be included in detailed reports to provide the data required by operators or third-party HR/payroll systems.

This tab is only available for some **Report types** (**General** tab). To reveal the **Extended** tab in the user programming, enable the **Display predefined custom fields in users** option in **Global | Sites | Display**.

### Default exported user fields

- **Employee code**: The Summary MYOB and Summary ICT Report Print Templates (**General** tab) identify users by a unique employee code. This field allows you to set the employee code to any extended user field (e.g. License number, Custom field 1).

### Additional exported user fields

To add additional extended or custom fields to the attendance report, click **Add** and select the appropriate fields.

## Attendance reports | Public holidays

This tab allows to you add public holidays to the attendance report. Holidays will not be included in attendance calculations, so employees will not be penalized for not attending work on a holiday.

You can also use the **Public holidays worked** option (**General** tab) to generate a report that includes only the shifts worked on public holidays, allowing you to calculate holiday pay.

### Public Holidays

- **Name**: The name of the holiday.
- **Repeat**: When this option is enabled the holiday will recur on an annual basis.

  Keep in mind that some holidays recur on the same day every year (e.g. Christmas), while others occur on different days (e.g. Easter). It is useful to program holidays several years in advance.

- **Start date**: The first day of the holiday.
- **End date**: The final day of the holiday.

  To create a single-day holiday, select the same end date as the start date. For example, to create a 24 hour holiday period for new years' day you would set both the start and end date to January 1st.

# Reports | Setup | User

User reports contain detailed information about the users in your system. You can quickly generate relevant data such as which users have access to selected doors, have triggered defined events, or have cards due to expire.

## User reports | General

### General

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

### Report Type

- **Report type**: The following report types are available for user reports. Additional columns can be added to any type of report in the **Columns** tab.
  - **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.
- **Title**: The title of the report will be displayed as a heading on printed and exported files.

### Sorting

The sorting criteria defined here will be implemented automatically in an exported report, but can be overridden when the report is executed manually.

- **Sort column**: Determines which column the results will be sorted by.
- **Sort direction**: Determines whether the returned data is sorted in ascending or descending order.
- **Group by**: Groups the returned data by the defined column.

### Specific Report Filters

Additional options are displayed according to the **Report type** selected. You may need to specify one or more of the following:

- Doors
- Access levels
- Record groups
- Time period
- Event filters
- Event types
- Expiry period for user records

### Default user report filter

If a default report layout has been created for this report, you can view the saved filters here. For more information, see Saving Report Layouts (page 170).

- **Edit in report view**: Clicking this button opens the event report in a breakout window, allowing you to run the report, configure filters, and save the default report layout.

### Record history

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

## User reports | Columns

This tab allows you to define which columns will appear in the report. Any user field can be added to the report, including extended fields (see **Users | Users | Extended**) and custom fields. This allows operators to create highly customized reports with many options for grouping and filtering.

Click **Add** to select which columns, i.e. user fields, will be included in the report. Use the **Move up** / **Move down** buttons to reorder the columns as required.

# Reports | Setup | Shift type

Industries such as law enforcement, security, healthcare and manufacturing often require operations to be run 24 hours a day, 7 days a week. This practice typically sees the day divided into shifts which often operate on a rotation.

Each shift type defines the start, end and break times for a single shift. Multiple shifts can be added to an attendance report and set on a rotation, so that time and attendance data can be calculated for each shift. For more information, see Attendance reports | Shift times (page 159).

For more information and a programming example, see Application Note 163: Configuring Shift Reports in Protege GX.

## Shift types | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Color**: The color used to identify the shift type in an attendance report. Set the color using the color picker, or enter the required RGB values manually.

### Record history

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

## Shift types | Time

### Shift times

- **Start/End time**: The start and end times of this shift type each time it occurs.
- **Include minutes before shift start**: Defines a grace period where users can badge in before the shift starts. Events during this period will be included in the attendance report for the shift.
- **Include minutes after shift end**: Defines a grace period where users can badge out after the shift ends. Events during this period will be included in the attendance report for the shift.

### Break times

You can enter up to 6 breaks for each shift. Check the box beside each break to enable that break for this shift.

- **Name**: A name for the break, e.g. 'Morning Tea'.
- **Start/End**: The start and end times for the break. These define the range of time in which the employee is allowed to take the break. For example, employees might be allowed 30 minutes for lunch, which can be taken any time between 12:00pm and 2:00pm.
- **Duration**: The length of the break in minutes. This will be used to calculate the employee's hours worked and time deductions.

  The duration of the break must be shorter than the space between the start and end times. For example, for a 10 minute break starting at 10:30am the end time should be at least 10:41am to allow for the full length of the break.
- **Calculation**: Determines how the break time will be used in attendance calculations. Exclude deducts the break duration from the hours worked, so the break is unpaid. Include does not deduct the break.

# Setting up Regular Report Emails

Each report setup programming page has an **Email** tab that can be used to configure regular automated report emails.

Automated email features in Protege GX require an SMTP mail server to be configured in **Global | Global settings | Email settings**.

## Operators

Add one or more Protege GX operators who will receive the report. Each operator must have an **Email address** defined in **Global | Operators | General**.

## Email Report

- **Email report**: Check this box to enable regular report emails.
- **Report format**: Defines the file format that the report will be sent in. Choose from PDF, CSV, Text, or XLS.
- **Time**: Defines the time of day the report will be sent, in the time zone of the Protege GX server.
- **Current server time**: Displays the current local time of the Protege GX server for reference.
- **Exclude report header and footer**: By default, most reports include a header and footer with additional details about the report (e.g. report name, date of export). However, this can cause blank columns to appear in exported or emailed reports in some formats, which may interfere with automated processes. Enable this option to remove the header and footer from the event reports, preventing this issue.

  This option is not available for attendance reports as they do not have headers or footers.
- **Number of events**: For event reports you can specify the number of events that will be exported and emailed. Very large reports will be broken into several files and sent as multiple emails.
- **Sunday-Saturday**: Defines the day(s) of the week the report will be sent.

## Time period

- **Period**: Only available for event reports. The period of time that the emailed report will cover. The options are:
  - Since report was last emailed: Includes all events from the last report email until now.
  - Since midnight: Includes all events from midnight until now.
  - Last 24 hours: Includes all events from the same time yesterday until now.
  - Last 48 hours: Includes all events from the same time two days ago until now.
  - Previous one week: Includes all events in the previous week, from Monday to Sunday (inclusive).
  - Previous two weeks: Includes all events in the previous fortnight, from Monday to Sunday (inclusive).
  - Previous calendar month: Includes all events in the previous month, from 1st - 30th/31st (inclusive).
- **Last run date**: Indicates when the last automatic report email was sent (read only).

# Setting up Regular Report File Exports

Each report setup programming page has a **File export** tab which can be used to configure scheduled or periodic automated file exports of the report.

## File report

- **Enable file export**: Check this box to enable the periodic report export.
- **Report format**: Defines the file format the report will be exported to. Choose from PDF, CSV, Text, or XLS.
- **Time**: By default, this field defines the time of day that the report will be exported. When **Export time is periodic** is enabled the minutes digits will be treated as a period.
- **Current server time**: Shows the current server time (read only field).

- **Export directory**: Defines the network location that the report will be exported to. Ensure this filepath is accessible on the Protege GX server.
- **Run report as operator**: For user reports you can specify the operator that will be used to run the report. This is important because different operators may have access to different user records.
- **Number of events**: For event reports you can specify the number of events that will be exported.
- **Append unique ID to filename**: When this option is enabled, a unique ID will be appended to the filename of each exported file. This allows you to run scheduled exports without concern that files will be overwritten.
- **Export time is periodic (minutes)**: When enabled, the **Time** programmed above will be used as a period between reports. The period is determined by the minute digits. For example, if the **Time** is set to 12:02 the report will be exported every two minutes.
- **Exclude report header and footer**: By default, most reports include a header and footer with additional details about the report (e.g. report name, date of export). However, this can cause blank columns to appear in exported or emailed reports in some formats, which may interfere with automated processes. Enable this option to remove the header and footer from the event reports, preventing this issue.

  This option is not available for attendance reports as they do not have headers or footers.
- **Days to export**: Select the days of the week the report will be exported. These options are automatically disabled if **Export time is periodic** is enabled.

## Time period

This section only applies to event reports.

- **Period**: Only available for event reports. The period of time that the exported report will cover. The options are:
  - Since report was last exported: Includes all events from the last report export until now.
  - Since midnight: Includes all events from midnight until now.
  - Last 24 hours: Includes all events from the same time yesterday until now.
  - Last 48 hours: Includes all events from the same time two days ago until now.
  - Previous one week: Includes all events in the previous week, from Monday to Sunday (inclusive).
  - Previous two weeks: Includes all events in the previous fortnight, from Monday to Sunday (inclusive).
  - Previous calendar month: Includes all events in the previous month, from 1st - 30th/31st (inclusive).
- **Last run date**: Indicates when the last automatic report export was completed (read only).

# Viewing Reports

Protege GX reports are easy to run and view, and have a number of powerful features which allow you to make the most of your archived events and user data. Create a custom report, group and filter by different columns on the fly, then print or export as you need.

The process for running and configuring reports is the same irrespective of what type of report is being run (with the exception of central station reports, which output a CSV file).

For a demonstration, see ICT Quick Tip: Viewing Event Reports in Protege GX on the ICT YouTube channel.

## Running a Report

1. Navigate to the setup programming for the report that you wish to run (e.g. **Reports | Setup | Event**) and create and save a new report record with the settings that you require. For more information, see Setting up Reports (page 152).

   The above is not required for operator permission reports.

2. From the **Reports** menu, select the type of report to run (e.g. **Reports | Event**).
3. From the toolbar, select the saved report you want to run, then click **Execute**.
4. For event reports you will be prompted to specify a **Time period**. You can set a **Start date** and **End date** manually, or select a predefined **Period** from the following options:
   - Today (since midnight), Yesterday, Day before yesterday: Events that occurred on the selected day, from midnight to midnight.
   - Last 1 hour, Last 12 hours, Last 1-21 days: Events that occurred between now and the selected start date/time. For example, the Last 1 day report begins 24 hours before the present time.
   - Last month, Last 2-6 months, Last year, Last 2 years: Events that occurred between now and the selected start date. For example, the Last month begins at midnight on the same day in the previous month and runs up to the present day (e.g. from 14th June - 14th July).
   - Last January-December: Events that occurred in the selected month. For example, the Last June report includes all events from 1st June to 30th June (inclusive). If the current month is selected, the report covers that month in the previous year.
5. For event reports you may further narrow your search by selecting a **Controller**.
6. For event reports you may enter a **Record name search** to include only records with the name specified.
7. The report will run and display the resulting records.

   For event reports you can use the toolbar icons to switch the display between **List view** (simple list of results) and **Grid view** (grid/table of results allowing more complex ordering and grouping operations).
8. If more than 200 results are returned, use the **Previous** and **Next** buttons in the toolbar to navigate between results that span multiple pages.
9. Sort, group and filter the results as required using the grid view (see below).
10. Use the **Print** button to open the print preview window, where you can print, export or email the results that are currently visible (see page 170).

    In addition, the **Batch print** button in user reports allows you to print photo ID cards for all users currently visible in the report. This requires a connected XPS card printer.

## Working with the Grid View

The grid view enables you to easily format, sort, group and filter report results.

### Adjusting the Column Display

The columns in the grid can be reorganized as necessary:

- **Resize columns** by hovering your mouse at the edge of the column header until it forms a double-headed arrow ↔. Then drag the column to the required size.

  The **Best fit** option enables you to automatically resize the columns when in grid view so they are the optimal width in order to display the data they contain.

  - To automatically resize a single column, hover your mouse at the edge of the column header until it forms a double-headed arrow ↔, then double click.
  - To automatically resize all of your columns, right click any column header and select **Best fit (all columns)**.
- **Reorder columns** by dragging and dropping a column header to a new position in the grid.
- **Remove columns** by dragging the column header downwards. When a red **x** icon appears over the column header release the mouse to remove the column.

  To retrieve columns that you have removed, right click on any header and select **Show column chooser** to display a list of available columns.

## Sorting by Column Data

A common requirement is to sort a large number of report results in a logical order. For example, you might want to sort a user report alphabetically by **Last name** or numerically by **Database ID**.

You can sort the results using the data in a particular column by simply clicking the column header in either list view or grid view. An arrow is displayed in the active column to show that the list is sorted by that column. The direction of the arrow (up or down) indicates whether the data is sorted in ascending or descending order. Click the column header again to toggle the order in which it is sorted.

Right clicking on a column header provides another method of selecting sorting options for the selected column:

- To sort a column, right click the column header and select either **Sort ascending** or **Sort descending**.
- To clear any sorting that is applied to the column, right click the column header and select **Clear sorting**.

## Grouping by Column

Grouping by columns allows you to organize a large number of events or records into a more readable form. For example, you may want to group a user report based of the users' access levels, or separate events based on which doors were involved.

Group data by dragging any column header above the others into the grouping box. This 'collapses' the report entries under headings based on the data in that column. You can expand each heading by clicking on it.

You can drag as many columns as you like into the grouping box, or remove the grouping by dragging a column back down to the normal level. The order of the columns in the grouping box creates a hierarchy which will separate the results into a tree structure.

Right clicking a column header provides another method of selecting grouping options. Simply right click the required column header and select **Group by this column**. To ungroup, right click the grouped column header and select **Ungroup**.

## Filtering the Report Results

There are several methods of filtering data in the returned report results:

- Using column headers.
- Using the filter row.
- Using the filter editor.

You can also edit filters you have added or clear filters you no longer require.

### Filtering Using Column Headers

Filter data by hovering your mouse over a column header until a small filter icon appears. Click the icon to select your filter criteria:

- **Blanks:** Only show results that have a blank entry (no data entered) in the selected column.
- **Non blanks**: Only show those events that do not have a blank entry in the selected column.
- **Results**: A list of the results that appear in that column is shown. Select one or more to filter the report by particular results.

  For example, select Office Staff in the access level column to show records for that access level only.

### Filtering Using the Filter Row

In any report the row directly below the header is the filter row. You can filter any column by typing a word, phrase or characters under the relevant column header.

For example, there might be several access levels that are used by warehouse staff: Warehouse Shift 1, Warehouse Shift 2 and Warehouse Supervisor. You can filter a user report for all three of these access levels by typing the common term 'Warehouse' into the filter row.

### The Filter Editor

The filter editor allows you to create complex filters to control which results are displayed. To open the filter editor window, right click a column header and select **Filter editor**.

You can add conditions (lines) to the filter editor by clicking the green **[+]** icon (or using the **Insert** key), and remove lines with the red **[x]** (or using the **Delete** key). Each term in each condition can be edited by clicking on the term and selecting an option from the dropdown, or by typing a relevant word or phrase.

## Using the Filter Editor

- **Condition Type**: To select the type of condition for the filter, click the red term at the top of the editor window. This type will apply to all of the conditions in the filter (or group): for example, if you select Or, the filter will have the structure A or B or C. The available conditions are:
  - **And**: All conditions in the filter must be met for a result to be included.
  - **Or**: One or more of the conditions in the filter must be met for a result to be included.
  - **NotAnd**: Only one of the conditions must be met for a result to be included. If more than one is met, it is excluded.
  - **NotOr**: None of the conditions must be met for a result to be included. If any of the conditions apply to an event, it is excluded.
  - **Add Condition**: Adds a new line/condition to the filter.
  - **Add Group**: Adds a new group of conditions to the filter. This group can have its own condition type, allowing you to create more complex conditions such as A and B and (C or D).
  - **Clear All**: Removes all conditions and groups from the filter.
- **Column**: The first entry in each condition. This determines which column the condition will apply to.
- **Operator**: The central entry (blue) in each condition. This defines a logical operator which will be used for that condition. The options available will depend on the column selected for the filter.
- **Value**: The term on the right of the condition, referring to the entries in the column being evaluated.
  - If the selected operator requires a value, click the grey link to enter or select it. For example, if the operator selected is **Equals** you need to enter or select the value that must be in this column for the filter condition to be met.
  - Some operators require or give you the option to enter more than one value. For example, if the selected operator is **Is between** you need to enter the two values between which the condition will be met.
  - If the selected operator is **Is any of** you can click the plus button to add more values.

When the filter is complete click **OK** to apply it to the report and close the filter editor, or **Apply** to apply the filter without closing the editor.

### Editing or Clearing Filters

It is easy to remove or edit filters that have been applied. Any filters that are currently applied are shown in a status bar at the bottom of the grid window.

### The Filter Status Bar

| Name | Description |
|---|---|
| Disable filter | Clear the checkbox to disable the current filter(s). Re-select to enable the current filter again. |
| Edit filter | Click on the edit button to display the filter editor for you to edit the currently applied filter(s). |
| Clear filter | Click on the clear button to permanently remove the filter. |

## Additional Grid View Features

A number of additional features are available in the right click (context) menu for the columns. To reveal these features, right click on the column and select the following:

- **Hide/Show group panel**: The group panel is displayed above the column headers, and is used when grouping columns. If you are not using grouping you can hide the group panel to provide more screen space for displaying results.
- **Hide/Show column chooser**: The column chooser displays the titles of any columns you have removed from the main report, allowing you to return them to the report as required.
- **Hide/Show search panel**: The search panel is a basic find tool, allowing you to search reports for specific results.

## Saving Report Layouts

Once you have configured the desired sorting, grouping and filter criteria in the grid view, you can save your layout for future use with this report.

Saved report layouts are only applied in the Protege GX client software. It is not possible to save report layouts in the web client.

### Saving Operator Report Layouts

Individual operators can save a report layout for each specific report, which will be applied automatically whenever that operator runs the report. This is available for all report types, as well as user searches and event searches.

To save a report layout, configure the grid view as desired, then click the **Save report layout** button in the toolbar. The next time that operator runs the report the saved report layout will be applied automatically.

### Saving Default Report Layouts

For event and user reports it is also possible to save a default report layout. This layout will be applied automatically when any operator runs that report.

To save a default report layout, configure the grid view as desired and click the **Save default report layout** button in the toolbar. Whenever any operator runs the report they can quickly apply this saved layout by clicking the **Load default report layout** button.

The filter set for this default report layout can be viewed on the report setup page. From there, click **Edit in report view** to run the report and save a new layout.

If both individual operator layouts and a sitewide default report layout are in use, whichever layout was last viewed by the operator will be used by default when the report is next generated.

# 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). |
| 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 **Export** option. |
| Print | Opens a print dialogue, allowing you to select a printer, printing preferences, page range and number of copies before printing.<br>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.<br>Ticking the **Open after export** box at the top of the window will cause the exported file to open when the export is complete.<br>You can also set up a regular file export of specific reports in the **Reports \| Setup** programming.<br>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.<br>You can also set up a regular email export of specific reports in the **Reports \| Setup** programming. |

# Central Station Report

You will typically need to supply your offsite monitoring station with a report map which specifies reporting codes for areas, inputs and users. These maps can be easily exported from within Protege GX for use with Contact ID and Report IP services.

The feature is not related to the other reporting options.

## Report Map Generator

Open the report map generator by navigating to **Reports | Central station report**.

- **Reporting service**: The service that the report map will be generated for.
- **Output directory**: The directory on the local network where the report map will be generated. The report map will be exported in both HTML and CSV formats.
- **Reset area, input and trouble input ID's**: By default, the report map will use the **Reporting ID** which has been programmed in each individual area, input and trouble input record. Enable this option if you want to reset the reporting IDs to follow a specific Contact ID mapping scheme.
- **Report map type**: If the **Reset area, input and trouble input ID's** option is enabled, select the Contact ID mapping scheme to use:
  - **Standard**: Suitable for small burglary and access control installations.
  - **Large**: Suitable for intrusion detection installations with a large number of input expanders.
  - **SIMS II**: A variant of the Contact ID format which can send a much larger number of inputs. For this mapping to function correctly the service must also be configured for SIMS II by setting the **Cid mapping** option for a Contact ID service or the **CID map settings** option for a Report IP service.
  - **None**: A sequential mapping: the first input will be mapped as 001, the second as 002 and so on. Inputs will be reported before trouble inputs. All IDs above the maximum reportable value (999) will be reported as 999.

  For more information, see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.
- **Generate**: Click this button to create the report. When the report is completed click **Open** to open the export folder.

# Operator Permission Report

The operator permission report allows you to view all of the operators in the system, along with the roles assigned to them, to easily see all operator permissions at a glance, and export, email or print them as required.

To run an operator permission report navigate to **Reports | Operator permission** and click **Execute**. There is no setup programming for this report type.

You can order, group and filter the results to display the information that is required. For more information, see Working with the Grid View (page 167).

# 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. Each status page is fully customizable, with up to 16 tiles which can be populated with event logs, device status information, floor plans, camera feeds or other items that require monitoring.

To open a status page navigate to **Monitoring | Status page view**. Select the status page you wish to view from the dropdown in the toolbar. It is convenient to use the **Breakout** button to break out the status page into a new window, so you can view it on a second monitor while continuing to program the system.

Status pages can be created in **Monitoring | Setup | Status page editor** (see page 182). The status page which will appear first when you open the status page view is set as the **Default status page** in **Global | Sites | Display**.

### Status Page Interactions

You can click on the vertical ellipsis ⋮ in the upper right of each tile for the following interactions:

- **Active**: When this checkbox is checked the tile will display an active or live view that updates continuously. Uncheck this box to freeze the current status of the tile.
- **Copy**: Click this button to copy the currently selected line(s). The information will be copied to the clipboard in CSV format, which can then be pasted into a text file or spreadsheet.
- **Update**: Click this button to update the status of the tile immediately based on information from the controller. This will not work if the **Active** option is unchecked.
- **Clear**: Click this button to clear the event window and only display new events.

You can right click on devices and some events to display a context menu for manual commands. For example:

- Right click on devices to open the manual commands for that device. For example, you can lock/unlock doors, arm/disarm areas, bypass inputs and switch outputs on/off.
- You can badge a new credential at a reader and right click on the 'Read Raw Data' event to assign it to a new or existing user.
- When an event occurs involving a record with an associated camera you can right click on the event to open a camera window with archived footage from the time of the event.
- When a user is denied access by antipassback you can right click on the event to reset the user's antipassback status.

### Alarms Status Page

The preconfigured alarms status page provides a live view of both active and acknowledged operator alarms in the system. To acknowledge an alarm, right click the event in the All Alarms section and click **Acknowledge**. The event will move to the All Acknowledged Alarms section.

For more information, see Alarms (page 141).

It is recommended that this default alarms status page is not edited or deleted, so that it is always available for acknowledging alarms.

# Floor plan view

Floor plans provide the ability to view and control doors, outputs, inputs, cameras, areas, trouble inputs, elevators and variables from a floor plan in real-time. Devices 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 open a floor plan navigate to **Monitoring | Floor plan view**. Select the floor plan you wish to view from the dropdown in the toolbar. It is convenient to use the **Breakout** button to break out the floor plan to a new window, so you can view it on a second monitor while continuing to program the system.

Floor plans can be created in **Monitoring | Setup | Floor plan editor** (see next page). The floor plan which will appear first when you open the floor plan view is set as the **Default floor plan** in **Global | Sites | Display**.

For more information on viewing and programming floor plans, see Application Note 340: Programming Floor Plans in Protege GX.

## Floor Plan Sections

The floor plan consists of the following sections:

- A graphical representation of the building or site, including interactive icons for devices. You can right click on any device icon on the image to open a context menu for manual commands (e.g. locking/unlocking doors, arming/disarming areas).

  The floor plan can also include buttons which are used to display a camera view or open another floor plan.
- A status list that dynamically updates to display the real-time status of the devices on the floor plan. You can right click on any device to open a context menu for manual commands.
- An event window displaying a live list of Floor plan events: events related to devices on the floor plan. You can right click on any event to run the floor plan events as a standard report, which can be exported, emailed or printed as normal.

  Up to six additional event reports can be displayed under separate tabs on this pane. This can be set as **Event window 1-6** in **Global | Sites | Display**.

# Monitoring | Setup

The setup submenu includes configuration pages for status pages and floor plans, as well as programming for camera and intercom integrations.

## Floor plan editor

Use the **Floor plan editor** to create and tailor floor plans to meet the specific needs of your system. Each floor plan can represent a section of the system, such as a single office floor or a specific device, or the system as a whole.

For more information on viewing and programming floor plans, see Application Note 340: Programming Floor Plans in Protege GX.

## Floor Plan Editor Menus

### Floor plan properties

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.
- **Background**: Click the ellipsis **[...]** button to set a background image for the floor plan. This should be in a file location that is accessible on the server machine, such as a shared network folder. The image can be in .bmp, .jpg or .png file formats.

  Ensure that all images are located in a shared network folder that clients have access to. If the link to an image is broken or the client machine is not able to access it, the image will not appear in the Protege GX client.
- **Width**: Defines the width of the floor plan (in pixels).
- **Height**: Defines the height of the floor plan (in pixels).
- **Color picker**: Sets the background color of the floor plan.
  - To set a solid color, click the **Solid** tab and select the color by using the color picker or entering RGB values.
  - To create a gradient, click the **Gradient** tab to display a slider bar beneath the color pickers. Click on each slider to set the color of each side individually, then adjust the sliders to achieve the desired effect.
  - To set no color (transparent), click the **Null** tab.
- Use the tabs above the color picker to set whether the color will be **Solid**, **Gradient** or **Null** (no color), then set the background color by using the color picker or entering RGB values.

### Brushes

The brushes section is used to set the color, visibility and opacity of lines, text and buttons on the floor plan.

1. Expand the **Brushes** section and select an item in the editor.
2. Select whether you are editing the **Background**, **Border** or **Foreground** color of the item. This will depend on the item being configured.
3. Set the colors for the item:
   - To set a solid color, click the **Solid** tab and select the color by using the color picker or entering RGB values.
   - To create a gradient, click the **Gradient** tab to display a slider bar beneath the color pickers. Click on each

slider to set the color of each side individually, then adjust the sliders to achieve the desired effect.
   - To set no color (transparent), click the **Null** tab.
4. Set whether the item is **Visible** or **Hidden**.
5. Set the **Opacity** of the item.

## Devices

This section is used to add representations of physical devices such as doors, areas, inputs and variables to the floor plan. When you view the floor plan each device icon will display its current status and can be right clicked to change the status.

1. Expand the **Devices** section and click **Add** to add a new device.
2. Set the **Device type** as required.
3. Set the **Device style** you wish to use. This determines the type of icon that will be used for this device on the floor plan.

   If you have created a floor plan symbol record (**Global | Floor plan symbols**) for a specific device type, when you add a device you can set the **Device style** to use your custom symbols.
4. Drag and drop the required device(s) onto the floor plan. Then **Close** the popup window.
5. Move the device by clicking and dragging, resize it using the squares in the corners, and rotate it using the circles in the corners.

The **Data** field does not need to be configured.

## Lines

Lines allow you to draw basic shapes on the floor plan, which can be used for walls and other features of the site.

1. Expand the **Lines** section and click **Add**.
2. Your cursor will transform into a **+** shape. Click somewhere on the design field to create the first node of the line.
3. To create an additional node or corner, click once. The line can have as many corners as necessary, allowing you to create complex shapes.
4. To complete the line, double click.
5. Give the line a descriptive **Name**.
6. Once the line is complete you can:
   - Set the **Line width** in the **Lines** section
   - Set the color with the **Border** attribute in the **Brushes** menu
   - Move the line by clicking and dragging within the dotted box
   - Resize the line by clicking and dragging the squares at the corners
   - Rotate the line by clicking and dragging the circles at the corners
   - Move the line in front of or behind other elements using the **Front** and **Back** buttons in the toolbar.

## Text

Text allows you to add text labels to your floor plan (e.g. area names, directions).

1. Expand the **Text** section and click **Add**.
2. Your cursor will transform into a **+** shape. Click and drag somewhere on the design field to create a text box.
3. Give the text a descriptive **Name**.
4. In the **Text** field, enter the required text.
5. Once the text is complete you can:

- Set the **Font**, **Font size** and text style in the **Text** section
- Set the color with the **Foreground** attribute in the **Brushes** menu
- Move the text box by clicking and dragging within the dotted box
- Resize the text box by clicking and dragging the squares at the corners
- Rotate the text box by clicking and dragging the circles at the corners
- Move the text box in front of or behind other elements using the **Front** and **Back** buttons in the toolbar.

## Images

In this section you can add pictures to your floor plan from files.

1. Click **Add**, then enter a filepath or click the ellipsis **[...]** to browse to an image. The image can be in .bmp or .jpg file formats.

   Ensure that all images are located in a shared network folder that clients have access to. If the link to an image is broken or the client machine is not able to access it, the image will not appear in the Protege GX client.

2. Your cursor will transform into a **+** shape. Click and drag somewhere on the design field to add the image.
3. Give the image a descriptive **Name**.
4. Once the image has been completed you can:
   - Move the image by clicking and dragging within the dotted box
   - Resize the image by clicking and dragging the squares at the corners
   - Rotate the image by clicking and dragging the circles at the corners
   - Move the image in front of or behind other elements using the **Front** and **Back** buttons in the toolbar.

     You can use the **Back** button to create a background image.

## Buttons

Operators can click buttons on the floor plan to perform specific actions. The types of actions available are:

- Launch a live camera feed to see the situation on the ground.
- Open another floor plan, enabling you to quickly navigate around a large site with multiple distinct sections. It is common to create a high-level 'map' of the site with buttons linking to separate floor plans for each zone or floor.

To create a button and link an action to it:

1. Create the record that the button will link to. This can be:
   - A camera (**Monitoring | Setup | Cameras**)
   - A floor plan (**Monitoring | Setup | Floor plans**)
2. Open the floor plan editor.
3. Expand the **Buttons** section and click **Add**.
4. Your cursor will transform into a **+** shape. Click and drag somewhere on the floor plan to create a button.
5. In the **Text** field, enter a label for the button.
6. Set formatting details such as **Font**, **Font size** and text style.
7. Expand the **Actions** section. Select a record for one or more of the action types.
8. Once the button has been completed, you can:
   - Set the colors with the **Background**, **Border** and **Foreground** attributes in the **Brushes** menu
   - Move the button by clicking and dragging within the dotted box
   - Resize the button by clicking and dragging the squares at the corners
   - Rotate the button by clicking and dragging the circles at the corners
   - Move the button in front of or behind other elements using the **Front** and **Back** buttons in the toolbar.

If the background color of a button is set to **Null**, you must click on the text label instead of the background to activate the button.

### Actions

Actions are required for use with buttons. To apply an action to a button, select the button and set one or more of the **Camera**, **Floor plan** and **Web link**.

## Floor Plan Editor Toolbar

The toolbar provides functionality for controlling the layout and positioning of elements added to a floor plan.

| Button | Function |
|---|---|
| Redo | Enables you to reinstate (redo) the last action that was undone. |
| Undo | Enables you to undo the last action. |
| Copy | Copies the selected object(s) to the clipboard. |
| Paste | Pastes the content from the clipboard into the design field. |
| Delete | Removes the selected object from the design field. |
| Snap | With this option enabled, when you draw, resize, or move an object it will align or 'snap' to the nearest objects in the design field even if the ruler is not visible. If your object does not move where you want, turn off this option. |
| Angle | Aligns the selected object(s) to the nearest polar grid angle. |
| Ruler | Select this option to toggle the ruler on or off. |
| Front | Moves the selected object in front of other objects. |
| Back | Moves selected object behind other objects. |
| Aln top | Aligns all selected objects to the top edge of the last object selected. |
| Aln btm | Aligns all selected objects to the bottom edge of the last object selected. |
| Aln lt | Aligns all selected objects to the left edge of the last object selected. |
| Aln rt | Aligns all selected objects to the right edge of the last object selected. |

# Floor plan editor (batch)

The batch floor plan editor allows you to edit specific features of floor plans in a normal programming window, which is convenient for batch changes or looking up record creation details.

## Floor plan editor (batch) | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.
- **Stretch mode**:
  - **Fill**: When enabled, the aspect ratio adjusts with the screen so that the floor plan is resized along with the window size.
  - **Uniform**: When enabled, the aspect ratio of the floor plan is retained when the window is resized.
- **Width**: Defines the width of the floor plan (in pixels).
- **Height**: Defines the height of the floor plan (in pixels).

### Record history

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

# Add bulk floor plans

The **Add bulk floor plans** feature enables you to quickly create a floor plan for each controller on a site, including all the devices (doors, inputs, outputs and/or areas) controlled by that controller.

This enables you to define a consistent background image that will be used by all floor plans, ensuring that all floor plans meet any branding or corporate style guidelines. The process also creates a placeholder image for each floor plan, which is stored outside of the Protege GX database. This allows you, or a graphic designer, to replace and update the floor layouts without opening Protege GX.

## Adding Multiple Floor Plans

1. Navigate to **Monitoring | Setup | Add bulk floor plans**. The **Add multiple floor plans** window opens.
2. Enter the required properties as described below.
3. Click **Add now** to create the floor plans.
4. In the location set as the **Image directory** you will find blank PNG images for each controller. You can edit or replace these images with representations of the layout for each floor plan.
5. In the floor plan editor (**Monitoring | Setup | Floor plan editor**), open each floor plan and finalize the positioning and design of the devices and other elements.

### Background template

- **Background image**: Defines the path and filename of an image that will be used as a background for all of the floor plans that are created. Ensure that you enter the full filename of an existing image to be used as the background.

  For best results, the dimensions of the image should already match the desired size and aspect ratio of the final floor plans in order to maintain the aspect ratio and avoid any distortion issues.

  Ensure that all images are located in a shared network folder that clients have access to. If the link to an image is broken or the client machine is not able to access it, the image will not appear in the Protege GX client.
- **Width**: Defines the width of the background (in pixels).
- **Height**: Defines the height of the background (in pixels).

### Floor plan image

- **Image directory**: Defines the location where the placeholder images will be created. This process will create a new blank PNG image for each controller. Note that this will overwrite any existing images with the same name at that location.

  Ensure that all images are located in a shared network folder that clients have access to. If the link to an image is broken or the client machine is not able to access it, the image will not appear in the Protege GX client.
- **Horizontal offset**: Sets the distance (in pixels) that the image will be offset horizontally from the left.
- **Vertical offset**: Sets the distance (in pixels) that the image will be offset vertically from the top.
- **Image width**: Defines the width of the images (in pixels).
- **Image height**: Defines the height of the images (in pixels).

### Buttons

The bulk add process also creates two buttons which will link to other floor plans - specifically, a 'home' and 'directory' floor plan. This makes it easy to navigate between floor plans when monitoring the system.

The home and directory floor plans must already have been created.

- **Home button text**: Defines the text (label) of the first button.
- **Floor plan**: Defines the 'home' floor plan that the button will link to.

- **Directory button text**: Defines the text (label) of the second button.
- **Floor plan**: Defines the 'directory' floor plan that the button will link to.

## Devices

- **Doors**: When enabled, includes each of the available doors on the floor plan for each controller.
- **Inputs**: When enabled, includes each of the available inputs on the floor plan for each controller.
- **Outputs**: When enabled, includes each of the available outputs on the floor plan for each controller.
- **Areas**: When enabled, includes each of the available areas on the floor plan for each controller.

# Status page editor

Status pages are a quick and efficient way to get an overview of your Protege system in one easy place. Each status page can include up to 16 tiles, each of which can display a single item or list.

## Creating a Status Page

1. Navigate to **Monitoring | Setup | Status page editor** and click **Add**. The **Add status page** window opens.
2. Enter a **Name** for your status page, select a default layout, and click **OK**. The programming window will display a number of tiles corresponding to the layout selected.
3. If you require a custom layout that is not available in the default options, you can:
   - Adjust the number of **Rows** and **Columns** of tiles that are included in the status page at the top of the editor window.
   - Adjust the number of **Rows** and **Columns** that each individual tile spans.
4. For each tile on the status page, set the **Type** to one of the available types:
   - **Status lists** that dynamically update to display the real time status of selected devices. These can be programmed in **Monitoring | Setup | Status lists**.
   - **Floor plans** that provide a visual representation of the site and the real time status of devices and objects in your system. These can be programmed in **Monitoring | Setup | Floor plan editor**.
   - **Cameras** from an integrated DVR/NVR system displaying live video feed. These can be programmed in **Monitoring | Cameras**.
   - **Event windows** that display a live view of the events in a particular event report. These can be programmed in **Reports | Setup | Event**.
   - **Variables** that return information on changeable data such as room temperature or humidity levels. These can be programmed in **Automation | Variables**.
   - **Web Pages** displaying the contents of a specific website or locally stored HTML page. These can be programmed in **Monitoring | Setup | Web pages**.
   - **Muster reports** that show a list of the most recent locations of users in the system. These can be programmed in **Reports | Setup | Muster**.

   If there is a tile that spans multiple rows or columns, ensure that adjacent tiles are left as <not set> to prevent content from overlapping on the status page.
5. Set the relevant **Record** for each tile (e.g. a status list or event report).
6. Once you have the configuration and layout you want, click **Save**.

# Status page editor (batch)

The batch status page editor allows you to make changes to status page names and layouts in a standard programming window.

## Status page editor (batch) | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.
- **Rows**: Defines the number of rows displayed on the status page.
- **Columns**: Defines the number of columns displayed on the status page.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

### Record history

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

# Status lists

Status lists can be used within a status page to provide a real-time display of the status of selected devices such as doors and areas. You can right click on a device in a status list to open the manual commands menu, allowing you to lock/unlock doors, arm/disarm areas, or open live camera views.

## Status lists | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Devices

Click **Add** to open the select devices window. Select the **Device type** (and **Controller**, where applicable) and check the boxes beside the desired records, then click **OK** to add the selected devices to the status list.

You can add the following device types:

- Doors
- Outputs
- Inputs
- Areas
- Trouble zones (i.e. trouble inputs)
- Elevators
- Variables

Other records may be available depending on which integrations are enabled for the site.

## Status Lists | Filters

Status filters allow you to display in the status list only devices which have a particular status (such as unlocked or disarmed).

### Status Filters

- **Area status filter**: Areas will only be displayed on the status list when they have the selected status. For example, you might want to create a status list which only shows areas that are currently disarmed.
- **Door status filter**: Doors will only be displayed on the status list when they have the selected status. For example, you might want to create a status list which only shows doors that are currently unlocked.

# Web links

Web links can be used on status pages to display a specific internal or external web page.

As well as displaying online websites, this feature can link to content such as a staff directory or policy and procedure information on a company intranet. Simply create an HTML page with the information you wish to display, save the file to a location on the Protege GX server or a shared network folder, then create a web link that links to that file.

## Web links | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **URL**: The address of the web page or directory location of the HTML page. Ensure that you include the https:// prefix for pages on the internet.

  If you are using a custom HTML page, the HTML file and any supporting files such as images or CSS files must be located in a folder that the Windows operator has permission to access. These files should be located on the Protege GX server or a shared network folder.
- **URL2**: An alternative web or directory address that will be used when Protege GX is being operated in the second language. The checkbox below must be enabled.
- **Use URL2 field for second language**: Select this option to enable the use of the **URL2** in the second language.

### Record history

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

# DVRs

Protege GX integrates with a number of third-party Video Management Systems (VMS) to provide integrated video surveillance. Cameras can be linked to particular devices in the system, providing live camera view and archived material based on events and triggers available in Protege GX. Most integrations also provide high level interfacing (HLI), allowing Protege GX to record HLI events such as 'Motion Detected'.

This programming page allows you to configure a connection to a DVR or NVR which is on the same network as the Protege GX server.

Integration with third-party video management systems requires appropriate licensing and typically installation of a dedicated integration service. For more information, see the relevant application note for each integration.

For a demonstration, see Configuring Video Management Systems in Protege GX on the ICT YouTube channel.

## DVRs | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **IP address**: The IP address of the DVR.
- **DVR port**: The port that Protege GX will use to communicate with the DVR. This is usually set in the relevant VMS integration service.
- **DVR type**: The type of DVR or integration that is being configured. If a VMS integration service is being used this field should be set to Custom, regardless of the brand of DVR that is being integrated.

### HLI

- **Monitor events from this DVR/NVR**: When enabled, HLI events from this DVR can be logged in Protege GX. Each integration has different HLI events available , such as 'DVR/NVR Offline' and 'Low Disk Space'.

  **Note**: To receive camera HLI events such as 'Motion Detected' the **Monitor events** option must also be enabled in **Monitoring | Setup | Cameras | General**.

- **Connect to this DVR/NVR on start up**: When this option is enabled, Protege GX will send a login request to the DVR when the client starts up. Otherwise, Protege GX will not connect to the DVR until it needs to request a camera list or footage.

  This option is only available when the **DVR Type** is set to Custom.

### Logon

- **Login required**: Select this option if the DVR requires credential details to log on.
- **Username/Password**: The credentials that Protege GX will use to log on to the DVR. Ensure this logon has the appropriate permissions to view camera footage and events within Protege GX.

### Record history

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

# Cameras

This programming page allows you to configure cameras to display live and archived video footage within Protege GX. You can configure standalone IP cameras or cameras that are associated with an integrated DVR or NVR (see **Monitoring | Setup | DVRs**).

Once cameras have been configured they can be monitored on status pages and associated with particular devices, allowing you to view live and archived camera footage from events.

## Cameras | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Type**: There are three camera types available:
  - **DVR**: Cameras that are connected to an integrated DVR or NVR.
  - **Direct camera**: Standalone IP cameras networked to Protege GX that provide direct URL access to either a static JPEG image feed or a streaming MJPEG feed. This option is used for RTSP protocol cameras.
  - **H.264 & motion JPEG stream camera**: Standalone IP cameras that provide direct URL access to an H.264 feed.
- **DVR**: The DVR record that the camera is associated with (if relevant). These can be programmed in **Monitoring | Setup | DVRs**.
- **DVR camera name**: Click the ellipsis **[...]** to open a list of cameras connected to the selected DVR. This list should be pulled from the integrated VMS. If no cameras appear on the list, check that the integration is configured correctly.
- **URL**: If the camera is not connected to a DVR enter its URL or IP address here. This is the link that you would use to log on to the camera's web interface.
- **Username/Password**: The credentials used to log on to the camera's web interface.

  This field is only available when the **Type** is set to Direct camera. For H.264 & Motion JPEG Stream Cameras, include the login username and password in the URL. e.g. http://username:password@192.168.1.2/video

### Display

- **Show sidebar controls in status page**: When this option is enabled, PTZ controls are displayed by default when the camera feed is viewed on a status page. When this option is disabled the control sidebar can be opened but will not be displayed by default.
- **Stretch image**: When this option is enabled the camera image will be stretched to fill the tile where it is displayed. This may not preserve the aspect ratio.
- **Floor plan**: The floor plan the camera belongs to. This allows you to right click on a camera event in the event log and open the floor plan associated with the camera.

### HLI

- **Monitor events**: When the camera is used as part of a VMS integration you can enable this option to log HLI events such as 'Motion Detected' from this camera. The operator can right click the event to open a camera with archived footage from the time of the event.

  This option requires the **Monitor events from this DVR** option to be enabled in **Monitoring | Setup | DVRs**.

## Record history

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

# PTZ commands

PTZ commands are command signals that can be sent to integrated PTZ cameras. PTZ commands can be sent in response to certain events, directing cameras to pan, tilt and zoom to focus on relevant areas.

For example, you might command a camera to focus on a nearby door whenever a door forced event occurs, ensuring that you will get direct footage of the event in progress.

Once a PTZ command has been programmed you must create an action that will control when that command should be sent. For more information, see Actions (page 143).

## PTZ commands | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Camera:** The camera that the PTZ command will control. These can be programmed in **Monitoring | Setup | Cameras**.
- **Command string**: The text that must be sent to the DVR to activate the PTZ movement. This is typically the name of a saved command in the integrated VMS. Refer to the relevant application note or your DVR documentation for information on the required command format.

### Record history

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

# Intercoms

Intercom records allow Protege GX to be integrated with VoIP compliant intercom systems. If a workstation has been configured as a SIP client in **Events | Workstations** operators can receive calls from the intercom, along with a relevant floor plan or camera feed.

In addition, intercoms can be linked to door records, allowing operators to call the intercom by right clicking on the door record in the software. For example, this allows guards to communicate with a visitor before granting them access remotely.

VoIP intercoms are a separately licensed feature. For more information and programming instructions, see Application Note 339: Integrating SIP Intercoms with Protege GX Workstations. This is a different feature to the intercom service that can be programmed in **Programming | Services**.

## Intercoms | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **URI:** Defines the URI (Uniform Resource Identifier) of the intercom.

### Graphics

- **Camera**: Defines the camera assigned to the intercom. A feed from this camera is displayed when a call is placed or received.
- **Floor plan**: The floor plan that will be launched when a call from the intercom is accepted.

### Record history

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

# Salto Menu

This menu allows you to program Salto doors, door groups and calendars, and view errors in the Salto error log.

Salto SHIP integration is a separately licensed feature. For more information, see see Application Note 188: Salto SHIP RW Pro Access Integration with Protege GX or Application Note 335: Salto SHIP ProAccess SPACE Integration with Protege GX. This programming menu is not used with the Salto SALLIS integration.

## Salto | Doors

Salto doors represent Salto SHIP wireless locks. Once you have programmed Salto door records they can be assigned to Salto door groups and access levels to grant access to users.

When offline Salto doors have been programmed in Protege GX and synchronized with the Salto SHIP server the hardware must be manually updated using a remote programming device. It is recommended that you complete all door programming before carrying out this update.

The maximum number of doors that Salto currently supports is 64,000 per database. A maximum of 96 doors (individual doors or doors within a group) can be assigned to a user. This rule applies to adding doors/door groups to a user directly or via an access level.

### Salto | Doors | General

#### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Salto display name**: The name of the record as it will be displayed in the Salto software. This is a read-only field, based on the **Name** set above. It is recommended to name Salto records in a way that will be recognizable in both Protege GX and Salto.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

#### Settings

- **Open time**: The duration (in seconds) that the Salto door will remain unlocked after access is granted. By default, this is set to 6 seconds.
- **Increase open time**: An alternative open time used for users who require extended access duration, such as people with mobility issues. This duration will be used for users with the **Use extended opening time** option enabled in **Users | Users | Salto**. By default, this is set to 20 seconds.

#### Antipassback

- **Enable antipassback**: When this option is enabled, antipassback will be enabled for this Salto door. If a user attempts to move through this Salto door in the same direction without exiting the door, access will be denied. This prevents users from passing their credentials back to another person to give them access to restricted areas.

  Antipassback should only be used with **Open mode** settings that require credentials at all times.

- **Direction**: If antipassback is enabled above, this field defines the direction of antipassback control. The options are From outside to inside (entry) and From inside to outside (exit).

## Audit options

- **Audit on keys**: When this option is enabled, offline Salto doors will generate an audit trail of access events on each user's card. These events are uploaded to the server whenever a user badges at an online lock.

  The **Audit openings in the key** option should be enabled for users in **Users | Users | Salto**. You can prevent operators from disabling this auditing in **Sites | Security Levels | Manual commands**.

## Open mode and periods

- **Open mode**: This field determines the operating mode for this electronic lock, i.e. how it can be accessed during different scheduled periods.
  - **Standard**: Users must badge an authorized Salto key to gain access.
  - **Office**: Users can set the door to office mode. Office mode is activated by presenting a Salto key while holding the inside handle down, and canceled by repeating the procedure. While in office mode the door is latch unlocked and can be accessed by any user without a credential.

    Only users with the **Office** option enabled can set a door to office mode (**Users | Users | Salto**).
  - **Toggle**: When this option is selected, users can activate and cancel office mode by badging their card, without holding down the inside handle.

    Only users with the **Office** option enabled can set a door to office mode (**Users | Users | Salto**).
  - **Automatic changes**: This option allows the door to operate under different modes at different times. The operation of this setting can be configured in the Salto software.
  - **Automatic open**: In this mode the door will automatically latch unlock when the **Open periods** schedule becomes valid. When the schedule is invalid the door will automatically lock and operate in standard mode.
  - **Automatic opening + office**: In this mode the door will automatically latch unlock when the schedule becomes valid. The door locks when the schedule becomes invalid, but users can still activate office mode by badging a card with the inside handle held down.
  - **Automatic opening + toggle**: In this mode the door will automatically latch unlock when the schedule becomes valid. The door locks when the schedule becomes invalid, but users can still activate office mode by badging a card.
  - **Key + PIN**: The door requires both a valid Salto key/card and a valid PIN to be entered at the keypad. This is valid at all times.

    The **PIN** option must be enabled in the **Users | Users | Salto** tab.
  - **Keypad only**: The door can be opened by entering a valid code at the keypad. This is valid at all times.
  - **Timed key + PIN**: This mode is the same as Key + PIN except a PIN is only required when the **Open periods** schedule is valid. Outside this period only a card is required for access.
  - **Timed keypad**: This mode is the same as Keypad except the code can only be used when the **Open periods** schedule is valid. Outside this period a card can be used for access.
  - **Timed office**: This option is similar to Office except office mode can be activated only when the **Open periods** schedule is valid. The door will automatically lock and operate in standard mode when the schedule period ends.
  - **Timed toggle**: This option is the same as Toggle except office mode can only be activated when the **Open periods** schedule is valid. The door will automatically lock and operate in standard mode when the schedule period ends.
  - **Exit leaves open**: When this option is selected the door operates in standard mode. However, when the inside handle is held down the door will latch unlock.

    The `EXIT_LEAVES_OPEN` option must also be enabled in the Salto software (**Advanced options**).

- **Toggle + exit leaves open:** This is a combination of the two modes. When a valid card is presented the door will begin to work in Toggle mode. Using the inner handle activates Exit Leaves Open mode.

  The `EXIT_LEAVES_OPEN` option must also be enabled in the Salto software (**Advanced options**).

- **Open periods**: The schedule that is associated with the Salto door. This is equivalent to a time periods record in the Salto software. The operation of this schedule will depend on the **Open mode** selected above.

## Cameras

- **Camera**: When a camera is assigned to a Salto door you can right click on any event involving that door in the event log to view archived camera footage from the event.

# Salto | Door groups

Salto door groups allow you to group Salto doors so that they can be more efficiently assigned to users and access levels. Within the Salto software, door groups are referred to as zones.

## Salto | Door groups | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Salto display name**: The name of the record as it will be displayed in the Salto software. This is a read-only field, based on the **Name** set above. It is recommended to name Salto records in a way that will be recognizable in both Protege GX and Salto.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

### Record history

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

## Salto | Door groups | Doors

### Salto doors

To add Salto doors to the group, click **Add**. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

# Salto | Calendars

Salto calendars are used to define specific days as holidays or special days for the purpose of Salto system operation.

In the schedule programming, you can set specific periods to operate on H (Holiday), S1 (Special 1) or S2 (Special 2) days as defined in the calendar (**Sites | Schedules | Configuration**, **Salto** column). Then the calendar can be applied to a user record (**Users | Users | Salto**), so that their access permissions will be modified on these specific days. Calendars can also be used to change Salto door schedules on specific days.

## Salto| Calendars | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Salto display name**: The name of the record as it will be displayed in the Salto software. This is a read-only field, based on the **Name** set above. It is recommended to name Salto records in a way that will be recognizable in both Protege GX and Salto.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

### Record history

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

## Salto | Calendars | Dates

Click **Add** to add dates to the calendar.

- **Name**: Describes the date (e.g. Christmas).
- **Date**: The date of the holiday or special day.
- **Type**: The type of day. Choose from Holiday, Special 1 or Special 2.

# Salto Log

When the **Enable Salto logging** option is enabled in the **Global | Sites | Salto** menu, the Salto error log shows events of all the data sent to the Salto system. This information is used for debugging.

Messages stored in the error log are generally logged in pairs, with one message showing the information sent to the Salto system and the other showing the reply from the Salto system.

Common events include:

- **GetInfo**: This message is logged once each time the download server starts, and displays the current SHIP version that the Salto system is running.
- **InsertOrUpdate**: This message indicates that Protege GX is updating the records within the Salto system.

# Manual Salto Door/Door Group Commands

Right clicking on a Salto door or Salto door group record displays a menu with manual commands for that record.

The available commands are:

- Open
- Emergency open
- Emergency close
- Cancel emergency

These commands are only relevant for online locks. Using these commands with offline locks causes Protege GX to return an error.

# Cencon Menu

The Cencon menu allows you to program Cencon lock groups and view the Cencon transaction log. Cencon locks assigned to the branch will be automatically added to Protege GX during synchronization.

This menu is only available when **Enable Cencon Integration** is selected in **Global | Sites | Cencon**.

Cencon integration is a separately licensed feature. For more information, see Application Note 160: Configuring Cencon Integration in Protege GX.

## Cencon lock groups

Cencon lock groups allow you to group connected Cencon locks so they can be more efficiently assigned to access levels for user access.

### Cencon lock groups | General

#### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

#### Include all locks

- **Include all locks**: Select this option to include all connected locks in the group.

#### Cencon locks

The locks that belong to this lock group. Click **Add** to open a list of the locks that have been programmed in the Cencon system. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

#### Record history

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

## Cencon transaction logs

When the **Log all Cencon transactions** option is enabled in **Global | Sites | Cencon**, communications between the Cencon database and Protege GX will be logged here. This allows you to view XML transactions in order to troubleshoot any issues.

# Programming Menu

Functions for programming records such as doors, areas, inputs, outputs, elevator cars, floors and services are found under the Programming menu.

## Doors

Doors in Protege GX are used to control user access, and monitor and control the flow of people into an area.

You can set the **Number of records to display on page** at the bottom of the list and navigate between pages using the arrows. On large sites it can take a long time to load all of the records, so reduce the page size to load the pages faster.

A number of options for doors, such as the credentials required for access and antipassback settings, are set in the door type (**Programming | Door types**).

## Doors | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

### Setup

- **Connection type**: This setting is only available when **Enable offline wireless locks** is enabled in **Global | Sites | Site defaults**. Set each door to either Wired (connected to a controller or reader expander) or Wireless offline.
- **Door type**: The door type assigned to a door controls the credentials required for access, as well as antipassback and dual authentication operation. Different door types can be scheduled for different times of day. For more information, see **Programming | Door types**.
- **Slave door**: You can assign another door as a slave door. When a user unlocks the primary door, the slave door will be unlocked as well if the user has access to it. This might be used to control two adjacent doors with a single reader port.

  By default, slave doors will only follow the primary door when it is unlocked by access with a valid credential. To enable slave door operation for REX, REN and manual commands, add `SlaveREX = true` in the **Commands** field for the primary door.

- **Area inside/outside door**: These fields allow you to set the areas that are inside and outside doors, enabling integration of the door's access control functions with area control and intrusion detection. Setting these areas allow you to use a range of features such as:
  - Unlock and lock doors automatically based on the area status (see the **Options** tab)
  - Prevent users from entering armed areas (see the **Advanced options** tab and **Expanders | Reader expanders | Reader 1/2**)

- Allow users to arm or disarm areas from the entry/exit reader (see **Expanders | Reader expanders | Reader 1/2)**
- Antipassback (see **Entry/Exit passback mode** in **Programming | Door types | General**)
- Loiter areas (see **Area enabled in loiter mode** in **Programming | Areas | Options (1)**)
- Area counting (see **Enable user counting** in **Programming | Areas | Options (1)**)

If there is no monitored area outside the door (i.e. the door is external) you can leave the outside area as <not set>.

- **Unlock schedule**: The unlock schedule can be used to latch unlock the door, allowing free access without a credential when the schedule is valid. By default, the unlocking function is edge triggered: the door will latch unlock when the schedule becomes valid and lock when the schedule becomes invalid, but can be overridden by user or operator commands. This behavior can be modified using the settings in the **Options** tab.

  For example, a retail shop could set an unlock schedule so that the door is unlocked for customers during their opening hours. Outside of these hours the door is locked but can be accessed by employees using their credentials.
- **Door pre-alarm delay time**: When a door is left open, after this period (in seconds) it will generate a pre-alarm. This pre-alarm generates an event and activates the **Pre alarm output / output group** (set in the **Outputs** tab), warning users that the left open alarm will soon be activated.

  This feature can be disabled under specific circumstances in the **Alarm options** tab.
- **Door left open alarm time**: When the door is left open, after this period (in seconds) it will activate the left open alarm. This alarm opens the Door Left Open trouble input and activates the **Left open alarm output / output group** (**Outputs** tab).

  The left open alarm timer begins when the door is first opened, not after the pre-alarm is activated. For example, with default settings the pre-alarm will be activated 30s after the door is opened, and the left open alarm will be activated 15s later (45s total).

  This feature can be disabled under specific circumstances in the **Alarm options** tab.
- **Support manual commands**: When this option is enabled, operators with the appropriate permissions can use manual commands to control the door. For example, a guard might be able to right click on a door icon on a floor plan to unlock the door.

  For more information, see Manual Door Commands (page 211).
- **Interlock door group**: When a door group is assigned to this field this door cannot be unlocked unless all of the doors assigned to the interlock door group are closed and locked. This ensures that only one door in the group can be opened at any given time.

  This feature is used to prevent a free path from being opened between safe and hazardous areas. For example, it could be applied to an entry point to a clean room or secure facility.

  For more information, see Application Note 206: Door Interlocking in Protege GX. For a demonstration, see Configuring Door Interlocking in Protege GX on the ICT YouTube channel.

## Commands

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

## Graphics

Cameras can be programmed in **Monitoring | Setup | Cameras**.

- **Camera (entry/exit)**: The camera that is monitoring the entry or exit side of the door respectively. You can view archived footage for door events by right clicking the event on a status page or floor plan.
- **Intercom (entry/exit)**: The intercom that is installed on the entry or exit side of the door respectively. You can place a call to this intercom by right clicking on the door record and clicking **Call intercom**.

Intercom records are programmed in **Monitoring | Setup | Intercoms**. The workstation must also be configured as a SIP client in **Events | Workstations**.

- **Floor plan**: The floor plan that the door belongs to. This allows you to right click on a door event in the event log and open the floor plan associated with the door.

## Auto camera popup

- **Auto camera popup on any door event**: When this option is enabled, a popup window will display live and archived camera footage whenever any door event is generated.
- **Auto camera popup on door forced event**: When this option is enabled, a popup window will display live and archived camera footage whenever a 'Door Forced' event is generated.
- **Camera**: The camera that is used for the auto camera popup. This does not need to be the same as the **Camera (entry)** or **Camera (exit)** set above.

## Elevator HLI

Different options are available depending on the type of Elevator HLI being configured. For more information, see the relevant elevator HLI application note.

- **Door used for elevator HLI**: When this option is enabled this door will be treated as part of the Elevator HLI integration. Generally the door record is used to represent either a Destination Operating Panel (DOP) located on a floor or a Car Operating Panel (COP) located in an elevator car.
- **Controller**: The controller that the door record is associated with. Only controllers with Elevator HLI enabled in **Sites | Controllers | Configuration** will be available for selection.
- **Elevator HLI type**: The type of Elevator HLI that the door will be used for (read only). This depends on the **Elevator HLI type** set in **Sites | Controllers | Configuration**.
- **KONE**: For more information, see Application Note 170: Protege GX KONE HLI Integration.
  - **Operator panel type**: Defines whether this door will be configured as a DOP (Destination Operating Panel) or a COP (Car Operating Panel).
  - **DOP/COP ID**: The unique ID of the DOP/COP which has been configured in the KONE system.
  - **Floor group**: The floor group that can be accessed from the DOP/COP. This allows specified floors to be unlocked on schedule for this DOP/COP.
  - **Floor**: For DOPs only. Defines which floor the DOP is located on.

    The combination of DOP ID and Floor must be unique.
  - **Elevator group**: For COPs only. Sets the internal elevator group number that has been configured in the KONE system.
  - **DOP sends elevator call**: This option enables the remote call giving interface for this DOP. With this option selected, when a user gains access to this DOP it will automatically send a call to transport the user to the **Elevator destination floor** set in their access level (**Users | Access levels | General**).

    The KONE Remote Call Giving Interface must enabled using **Enable elevator call functionality** in **Sites | Controllers | Configuration**.
- **Thyssenkrupp**: For more information, see Application Note 169: Protege GX ThyssenKrupp HLI Integration.
  - **Operator panel type**: Only the DOP option is supported by this integration. This represents floor based kiosks.
  - **DOP ID**: The unique ID of the kiosk which has been configured in the Thyssenkrupp system.
  - **Floor group**: The floor group that can be accessed from the kiosk. This allows specified floors to be unlocked on schedule for this kiosk.
  - **Floor**: Defines which floor the kiosk is located on.
  - **Group number**: The group number for this DOP that has been configured in the ThyssenKrupp system.

    The combination of DOP ID, Floor and Group number must be unique.
- **OTIS**: For more information, see Application Note 174: Protege GX Otis Compass HLI Integration.

- **Operator panel type**: Only the DOP option is supported by this integration. This represents floor based DECs (Destination Entry Computers).
- **DOP ID**: This information is provided by the Otis Compass elevator system and specifies the unique ID of the Otis Compass DEC. This needs to match the fourth octet of the DEC's IP address.
- **Floor group**: This floor group defines all of the floors that the DEC is able to access. When the schedules assigned to the floors in this group are valid the floors will be unlocked for free access.
- **Group number**: This information is provided by the Otis Compass elevator system and must match the third octet of the DEC's IP address.
- **DEC operation mode**: This defines the DEC operation mode (this must match the mode supplied by the Otis Compass elevator system). The following modes are supported:
  - **(1) Default floor**: The user presents their credentials to the card reader or enters a PIN at a DEC device. If the user's credentials are valid the security system sends the user's default floor to the DEC. If floor access is denied the DEC provides textual and/or audible feedback to the user informing them that the call request has been denied.

    The default floor is set as the **Elevator destination floor** in **Users | Access levels | General**.
  - **(3) User entry of destination floor**: Without the need for credentials, the user selects their destination floor. If the destination floor is free access the DEC forwards the call request to the DES. If the floor selected is not free access the user is prompted to present their credentials.
  - **(4) Default floor or user entry of destination floor**: The user presents their credentials and, if valid, their default floor is sent to the DEC. Within a defined timeframe the user is able to override the default floor selection and choose another destination floor.

    The default floor is set as the **Elevator destination floor** in **Users | Access levels | General**.

- **MCE**: For more information, see Application Note 241: Protege GX MCE Elevator Integration.
  - **Operator panel type**: Defines whether this door will be configured as a DOP (Destination Operating Panel) or a COP (Car Operating Panel).
  - **DOP/COP ID**: The unique ID of the DOP/COP which has been configured in the MCE system.
  - **Floor group**: The floor group that can be accessed from the DOP/COP. This allows specified floors to be unlocked on schedule for this DOP/COP.
  - **Floor**: For DOPs only. Defines which floor the kiosk is located on.
  - **Elevator car**: For COPs only. Sets the elevator car in the MCE system that the in-car reader is located in.
  - **DOP sends elevator call**: This option allows MCE turnstiles to send a call to the MCE interface. This option must be enabled for door records to act as a turnstile. It should be disabled for regular landing based kiosks.

### Record history

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

## Doors | Outputs

### Lock output

- **Lock output / output group**: The output or output group that controls the physical door lock. These are typically the relay outputs on the reader expander, but could be any output or output group in the system.
- **Lock activation time**: The unlock time in seconds, i.e. the time that the lock output will be activated for when the door is unlocked. If additional lock outputs are being used this controls the activation time of the first lock output.

  Setting the activation time to 0 will cause the door state to toggle between locked and unlock latched when unlocked by a user or operator. However, the REX and REN functions are disabled.

  The maximum lock activation time is 128 seconds.

- **Enable additional lock outputs**: When this option is enabled the additional lock outputs 2-6 will be available for use. These are typically used when more than one lock output controls the door lock or when additional functions such as an automatic door pump are required.

## Lock 2-6 output

When the **Enable additional lock outputs** option is enabled, up to 5 additional lock outputs can be programmed below. The standard lock output always activates first, and additional lock outputs may activate at the same time, or after a delay.

It is recommended that you test the timings of the additional lock outputs with any other locking/unlocking features used on site (such as extended unlock times or relocking functions) before implementation. As a general rule the lock outputs will always activate in the same order and deactivate in the same order.

- **Lock 2-6 output / output group**: The output or output group that controls the additional lock for the door.
- **Lock 2-6 activation time**: The duration (in seconds) that the additional lock output will remain activated when the door is unlocked.

  When used with an extended unlock time such as the **REX activation time** (**Inputs** tab), the **Door extended access time** (**Advanced options** tab) or an extended unlock calendar action, the activation times for all locks are extended (not just the first lock).

  The maximum lock activation time is 255 seconds.
- **Lock 2-6 delay before activation:** The delay (in seconds) between the activation of the first lock output and activation of this additional lock output. For example, if the delay for lock output 3 is set to 5 seconds, when access is granted the first lock output will activate immediately and lock output 3 will activate 5 seconds later.

  **Important**: All **Delay before activation** times must be completed before any other lock output is deactivated. This means that all outputs must be activated before any outputs are deactivated.

## Pre-alarm output

- **Pre alarm output / output group**: The door will generate a pre-alarm when a door is left open, to warn users that the door left open alarm will soon be activated. The pre alarm output or output group is activated when the **Door pre-alarm delay time** (**General** tab) is reached.

  This feature can be disabled under specific circumstances in the **Alarm options** tab.
- **Pre alarm pulse on/off time**: These fields are used to make the pre alarm output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

## Door left open output

- **Left open alarm output / output group**: When a door has been left open for too long, a door left open alarm will be generated to instruct users to close the door immediately. The left open alarm output or output group is activated when the **Door left open alarm time** (**General** tab) is reached.

  In addition, when the alarm is generated the Door Left Open trouble input is opened.

  This feature can be disabled under specific circumstances in the **Alarm options** tab.
- **Left open alarm pulse on/off time**: These fields are used to make the left open alarm output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

### Door forced open output

- **Forced open output / output group**: When a door is forced open without any access a door forced alarm will be generated. The forced open output or output group will be activated immediately.

  In addition, when the alarm is generated the Door Forced Open trouble input is opened.

  This feature can be disabled under specific circumstances in the **Alarm options** tab.

- **Forced open pulse on/off time**: These fields are used to make the forced open output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

## Doors | Function outputs

For more information and programming instructions, see Application Note 336: Programming Function Outputs in Protege GX and Protege WX.

### Function 1-3 output

- **Function 1-3 output / output group**: This output or output group will be activated when the door is unlocked. Up to three function outputs can be programmed for each door, operating independently. These can be used to activate additional mechanisms or logic when the door is unlocked, such as bypass shunts or automatic door pumps.

  By default, the function outputs are activated for the set activation time when the door is unlocked by any method. The options below can modify this behavior.

- **Function 1-3 activation time**: The duration (in seconds) that the function output will be activated for when the door is unlocked. When the activation time is set to 0, the function output will be activated indefinitely.

  When the door is latch unlocked, the function output will be activated until the door is locked again. After the door is locked the function output will remain on for the programmed activation time, then will be deactivated.

  The maximum function output activation time is 86400 seconds (24 hours).

  This setting overrides the **Activation time** set in the output programming.

- **Activate on access**: When this option is enabled the function output will only be activated when the door is unlocked by access. It will not be activated when the door is unlocked by other methods such as schedule, area or programmable function.

  This option can be combined with **Activate on REX/REN** below.

- **Activate on REX/REN**: When this option is enabled the function output will only be activated when the door is unlocked by REX or REN. It will not be activated when the door is unlocked by other methods such as schedule, area or programmable function.

  This option can be combined with **Activate on access** above.

- **Deactivate on door open**: When this option is enabled the function output will be deactivated immediately when the door is opened. If the door is not opened the output will still deactivate after the normal activation time.

  This feature does not operate while the door is latch unlocked.

- **Deactivate on door close**: When this option is enabled the function output will be deactivated immediately when the door is closed. If the door is not closed the output will still deactivate after the normal activation time.

  This feature does not operate while the door is latch unlocked.

- **Recycle time on access**: When this option is enabled, unlocking the door by access again when the function output is still on will reset the function output's activation time. This allows users to extend the time that the function output is activated.

  **Activate on access** must be enabled to use this feature. In addition, you must enter the command `RecycleDoorTimeOnAccess = true` in the **General** tab.

- **Recycle time on REX/REN**: When this option is enabled, unlocking the door by REX again when the function output is still on will reset the function output's activation time. This allows users to extend the time that the function output is activated.

  **Activate on REX/REN** must be enabled to use this feature. In addition, **Always allow REX** and **Recycle REX time** must be enabled in the **Inputs** tab.

# Doors | Inputs

## Door input options

- **Door position input**: This input is used to detect the position of the door. When this input is opened the door status will change to 'open', and when the input is closed the door status will change to 'closed'.

  This is also known as a door contact or reed input, as a reed switch is typically used for this function.

- **Invert door input**: When this option is enabled the operation of the door position input will be reversed. When the input is closed the door will be considered open. When the input is open the door will be considered closed.

  **Note**: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

## REX input options

- **REX input**: This input is used for the REX (request to exit) function. When a user activates this input it will generate a request to exit and unlock the door. When the door is unlocked by REX it uses the standard **Lock activation time**, unless the **REX time different to lock time** option has been enabled below.

  REX is generally used in situations where a door has entry readers but no exit readers. REX inputs are commonly buttons, so they typically have a normally open **Contact type** (**Programming | Inputs | Options**).

  The **Unlock door on REX** option must be enabled in the **Options** tab.

- **Invert REX input**: When this option is enabled the operation of the REX input will be reversed. When the input is closed (deactivated) a request to exit will be generated.

  **Note**: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

## Bond input options

- **Bond sense input**: This input is used to detect the position of the door lock. When this input is opened the door status will change to 'not locked', and when the input is closed the door status will be 'locked' (assuming the door position input is also closed).

  Door left open and forced alarms may be generated based on the position of the bond sense input.

  This feature can be used with any lock that has bond or lock sense monitoring. For example, a magnetic bond sense is a contact that indicates whether the magnetic bond between the electromagnet and the clamp is complete.

- **Invert bond input**: When this option is enabled the operation of the bond sense input will be reversed. When the input is closed the door will be considered not locked and vice versa.

  **Note**: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

## REN input options

- **REN input**: This input is used for the REN (request to enter) function. When the user activates the input it will generate a request to enter and unlock the door. The standard **Lock activation time** is used.

  REN is generally used for doors which allow free entry. Alternatively, a REN button may be placed in a guard station to allow guards to unlock a door remotely. REN inputs are commonly buttons, so they typically have a normally open **Contact type** (**Programming | Inputs | Options**).

  The **Unlock door on REN** option must be enabled in the **Options** tab.

- **Invert REN input**: When this option is enabled the operation of the REN input will be reversed. When the input is closed (deactivated) a request to enter will be generated.

  **Note**: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

## Beam input options

- **Beam sense input**: This input is used to ensure that automatic doors remain unlocked and open when there is something obstructing the path of the door. When the beam sense input is opened (while the door is already open) the door is unlocked and the lock is held open. When the input is closed the lock output(s) will remain on for the programmed **Lock activation time** (**Outputs** tab) before turning off again.

  This feature is typically used with automatic doors and gates which use a door pump as a lock output. This allows the door to begin opening again when it is about to collide with something.

  The beam input does not restart the pre-alarm and left open alarm timers.

- **Invert beam input**: When this option is enabled the operation of the beam sense input will be reversed. When the input is closed the beam function will be triggered.

  **Note**: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

## General options

- **Always allow REX**: When this option is enabled the door will process a request to exit even when the door is already open. This will activate the lock but will not reset the door forced or door open too long alarms. When this option is disabled the REX function will only operate when the door is closed.

  This option is useful when the lock output is controlling an automatic door opener. This allows the door to begin opening again if the REX is pushed while it is closing; however, some locks such as maglocks should remain locked while the door is open to prevent the door from 'bouncing' when it is closed.

- **Recycle door open time on REX**: When this option is enabled, users can press the REX input while the door is open to reset the time that it is allowed to be left open. If the pre-alarm has started, pressing the REX button will silence the pre-alarm; however, if the door left open alarm has already been activated, pressing the REX will not reset the timer.

  For example, if the **Door left open alarm time** is set to 45 seconds, pressing the REX button during this period will reset the timer, allowing the door to be open for an additional 45 seconds.

  The **Always allow REX** option must also be enabled.

- **Forced door sends door open**: When this option is enabled, when the door is forced open (i.e. opened without being unlocked) it will be processed as a 'door open' status. When this option is disabled the door forced status will be processed as normal.

This can be used in situations where the door might be opened without being controlled by the controller. For example, some doors have a physical key override to manually unlock the door, which would normally cause a door forced alarm.

- **Recycle REX time**: When this option is enabled, pressing the REX button while the door is unlocked by REX will reset the lock activation time so that the door will remain unlocked for longer.

  For example, if the **Lock activation time** is set to 5 seconds, pressing the REX button during this period will reset the timer, allowing the lock to remain open for another 5 seconds.

  This feature only applies when the door has been unlocked by REX. The **Always allow REX** option must also be enabled.

- **Maintain REX**: When this option is enabled the door will remain unlocked for as long as the REX button is held down. When the REX button is released the door will lock again after the **REX activation time**.

  Holding down the REX button will also prevent the door left open timer from starting, so the door can be held open indefinitely without activating an alarm.

- **Pulse reader beeper on REX**: When this option is enabled the readers associated with the door beep twice when the REX button is pressed. When this option is disabled there is no audible response from the request to exit function.
- **REX time different to lock time**: By default, the REX activation time is the same as the **Lock activation time** (**Outputs** tab). With this option enabled the **REX activation time** can be configured separately and will override the lock activation time when the REX button is pressed.

  For example, if the lock activation time is 5 seconds and the REX activation time is 10 seconds, when a user badges to enter a room the door will unlock for 5 seconds, but when they press the REX button to exit the door will unlock for 10 seconds.

- **REX activation time**: If the **REX time different to lock time** option is enabled above, this field sets the duration that the door lock will be activated when the REX button is pressed.

  The REX activation time cannot be set to 0.

# Doors | Options

## Door options

- **Always check unlock schedule**: Enabling this option causes the door to latch unlock when the **Unlock schedule** is valid, and lock when the schedule is invalid. While the schedule is valid, if the door is locked by another function it will immediately unlock again. This prevents the door from being manually locked when it should be unlocked.

  You can use this option together with **Schedule overrides latch** to also prevent the door from being latch unlocked when the schedule is invalid.

  Using the **Prevent unlock on schedule if inside area / outside area armed** options alongside this setting will prevent the door from unlocking while the schedule is valid, but does not relock the door when the area is armed. To achieve this use **Area disarmed and schedule valid unlock door** instead.

- **Enable open/close events on schedule**: By default, doors generate open and close events even while they are unlocked by schedule. As these events are typically not needed, you can disable this setting to suppress the events. This saves space in the events database.
- **Relock on door close**: With this option enabled the lock will relock as soon as the door closes. If the door is not closed the lock will still deactivate after the normal lock activation time.
- **Relock on door open**: With this option enabled the lock will relock as soon as the door opens. If the door is not opened the lock will still deactivate after the normal lock activation time.
- **Unlock door on REX**: When this option is enabled, opening the **REX input** (set in the **Inputs** tab) will unlock the door.

  When this option is disabled the door does not automatically unlock when the REX input is pressed, but temporarily enters a 'free egress' state, suppressing door forced alarms for the normal REX activation time. This allows the use of mortise locks with a free egress handle which mechanically unlocks the door.

- **Unlock door on REN**: When this option is enabled the **REN input** (set in the **Inputs** tab) can be used to unlock the door using the request to enter function. Disable this option to disable REN processing for this door.
- **Schedule operates late to open**: When this option is enabled the door will not latch unlock when the schedule is valid until a user or operator unlocks the door. This can be used to prevent the door from automatically unlocking on days when nobody arrives on site.

  This option overrides the **Always check unlock schedule** option above. For the door to lock when the schedule becomes invalid, also enable the **Schedule overrides latch** option below.

### Door options 2

- **Door lock follows inside/outside area**: Enable one of these options to select whether the **Area inside door** or **Area outside door** (**General** tab) will be used with the area control options below.
- **Prevent slave unlock on inside area**: If there is a **Slave door** set in the **General** tab, by default the slave door will always follow the state of the primary door when it unlocks on access. This option prevents the slave door from following the primary door when the slave door's inside area is armed, preventing false alarms. This option must be enabled in the slave door's programming.

  This feature does not work with the `SlaveREX = true` command. When the primary door is unlocked by REX, REN or manual commands the slave door will be unlocked regardless of area status.
- **Prevent unlock on schedule if inside / outside area armed**: When one of these options is enabled, if the unlock schedule becomes valid but the door's inside or outside area is still armed the door will not unlock. This can be used to prevent a door from unlocking on days when no one arrives to disarm the area.
- **Area disarmed and schedule valid unlock door**: When this option is enabled the door will automatically latch unlock when both the unlock schedule is valid and the relevant area is disarmed. When the schedule becomes invalid or the area is armed the door automatically locks.

  If the door is latch unlocked or locked by any other feature it will immediately be returned to the correct state.

  The relevant area is determined by the **Door lock follows inside area** or **Door lock follows outside area** options above.
- **Area disarmed or schedule valid unlock door**: When this option is enabled the door will automatically latch unlock when either the unlock schedule is valid or the relevant area is disarmed. When both the schedule is invalid and the area is armed the door automatically locks.

  If the door is latch unlocked or locked by any other feature it will immediately be returned to the correct state.

  The relevant area is determined by the **Door lock follows inside area** or **Door lock follows outside area** options above.
- **Enable access taken on REX/REN events**: With this option enabled, when a REX or REN is registered at the door the system will record whether the requested access was taken or not taken. For example, if the REX button is pressed and then the door is opened a 'Request to Exit Taken' event will be logged. If the door is not opened a 'Request to Exit Not Taken' event will be logged.
- **Schedule overrides latch**: With this option enabled, when the unlock schedule becomes invalid the door will automatically lock. In addition, if **Always check unlock schedule** is also enabled, if the door is latch unlocked by another function it will be immediately relocked by the schedule. This prevents the door from being latch unlocked when it should be locked.

## Doors | Advanced options

### Advanced options

- **Update user area when passback disabled**: By default, unless antipassback is enabled the system does not keep track of which area a user is in when they pass through the door. With this option enabled the controller will update the area the user is in even when antipassback is disabled on this door. This feature is useful on sites where some doors have antipassback enabled but others do not.

There is no connection to the **User area** option set in **Users | Users | General**.

- **Lock out REX when inside area armed**: When this option is enabled the door will deny any request to exit made when the inside area has been armed. This can be used to prevent people from exiting an armed area. Users can still exit with a valid credential.
- **Deny entry if inside area is armed**: When this option is enabled the door will deny entry to all users when the door's inside area is armed.

  This option overrides the **Disarm area for door on access** option in the **Expanders | Reader expanders | Reader 1/2** programming, so users will be locked out even if they have access to disarm the area.
- **Deny exit if outside area is armed**: When this option is enabled the door will deny exit to all users when the door's outside area is armed.

  This option overrides the **Disarm area for door on access** option in the **Expanders | Reader expanders | Reader 1/2** programming, so users will be locked out even if they have access to disarm the area.
- **Prompt user for access reason code**: With this option enabled, users who request access at the door must enter an access reason code at an associated keypad before the door will be unlocked.

  When the user badges their card the keypad will prompt them to enter an Area from 001-009, then press **[Enter]**. When they do, access will be granted and an event will be logged in the format: 'User Unlocked Door By Type [XX]'. The Type code in the event corresponds to the Area reason code minus 1, so that the codes Area 001-009 correspond to Type 00-08.

  Use of this feature requires the following settings in the **Expanders | Reader expanders | Reader 1/2** programming:
  - **Reader 1/2 keypad type**: LCD keypad
  - **Keypad to use for PINs reader 1/2**: Select a keypad adjacent to the door

  This feature is not supported with card and PIN operation.
- **Enable access taken on door unlock events**: With this option enabled, when a user is granted access at the door the system will record whether the requested access was taken or not. For example, if a card is badged and then the door is opened an 'Access Taken' event will be logged. If the door is not opened an 'Access Not Taken' event will be logged.

  When this option is not enabled the system will not indicate whether or not access was taken.

## Extended access time options

The antipassback options below apply when the door type associated with the door has antipassback settings configured (**Programming | Door types | General**).

- **Door extended access time**: The duration (in seconds) that the door will remain unlocked for users who require extended access times. This will override the **Lock activation time** for any users with the **User operates extended door access function** option enabled (**Users | Users | Options**).
- **Antipassback entry/exit user reset time**: If **Enable timed user antipassback reset** is enabled below, these fields define the period (in minutes) for resetting the antipassback status of all users who have entered or exited the door.
- **Reset antipassback status on schedule**: With this option enabled, the antipassback status of all users who have accessed this door will be reset whenever the **Antipassback reset schedule** below changes states (i.e. becomes valid or invalid).
- **Enable timed user antipassback reset**: With this option enabled, the antipassback status of all users who have accessed this door will be reset periodically. The period is set in the **Antipassback entry/exit user reset time** fields above.

  For example, if the entry reset time is set to 120 minutes, every 2 hours the system will reset the antipassback status of all users who have entered the door during this time.
- **Antipassback reset schedule**: If **Reset antipassback status on schedule** is enabled, this field defines the schedule used to reset antipassback status.

# Doors | Alarm options

To set the outputs used by the alarms below, see the **Outputs** tab.

## Pre-alarm options

- **Enable pre-alarm alarms**: The door pre-alarm is activated when the door has been left open for the **Door pre-alarm delay time**, activating an output to warn users that the left open alarm is about to be activated. Disable this option to disable the pre-alarm function for this door.
- **Disable during unlock schedule**: Enable this option to disable the door pre-alarm while the door has been latch unlocked by an unlock schedule.
- **Disable during manual commands**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by an operator using a manual command. The pre-alarm will still activate when the door has been unlocked (i.e. temporarily unlocked) by a manual command.
- **Disable during calendar actions**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by a calendar action.
- **Disable whilst unlocked by area**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by an area (e.g. using the **Area disarmed or schedule valid unlock door** option in the **Options** tab).
- **Disable whilst unlocked by programmable function**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by a programmable function.
- **Disable whilst unlocked by fire drop**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by a programmable function with the **Door control mode** 2 - Fire control door unlock.
- **Alarm operating schedule**: The door pre-alarm will be enabled when this schedule is valid and disabled when this schedule is invalid.

## Left open options

- **Enable left open alarms**: The door left open alarm is activated when the door has been left open for the **Door left open alarm time**, activating an output and opening the Door Left Open trouble input to report the alarm to the monitoring station. Disable this option to disable all left open alarm functions for this door.

  Disabling the left open alarm will not automatically disable the pre-alarm.

- **Disable during unlock schedule**: Enable this option to disable the left open alarm when the door has been unlocked by an unlock schedule.
- **Disable during manual commands**: Enable this option to disable the left open alarm when the door has been latch unlocked by an operator using a manual command. The pre-alarm will still activate when the door has been unlocked (i.e. temporarily unlocked) by a manual command.
- **Disable during calendar actions**: Enable this option to disable the left open alarm when the door has been latch unlocked by a calendar action.
- **Disable whilst unlocked by area**: Enable this option to disable the left open alarm when the door has been latch unlocked by an area (e.g. using the **Area disarmed or schedule valid unlock door** option in the **Options** tab).
- **Disable whilst unlocked by programmable function**: Enable this option to disable the left open alarm when the door has been latch unlocked by a programmable function.
- **Disable whilst unlocked by fire drop**: Enable this option to disable the left open alarm when the door has been latch unlocked by a programmable function with the **Door control mode** 2 - Fire control door unlock.
- **Alarm operating schedule**: The left open alarm will be enabled when this schedule is valid and disabled when this schedule is invalid.

## Forced open options

The door forced operation can also be delayed via commands. For more information, see Application Note 304: Delaying Door Forced Commands.

- **Enable forced open alarms**: The door forced alarm is activated when the door is forced, activating an output and opening the Door Forced Open trouble input to report the alarm to the monitoring station. Disable this option to disable all door forced alarm functions for this door (although the door will still have the 'Forced Open' status on a floor plan or status page).

  Alternatively, see the **Forced door sends door open** option (**Inputs** tab).

- **Alarm operating schedule**: The door forced alarm will be enabled when this schedule is valid and disabled when this schedule is invalid.

# Doors | Function codes

Function codes can be created in **Sites | Function codes**. For more information, see Application Note 240: Function Codes in Protege GX.

## Function Codes Options

Add a function code to the door by clicking **Add**. You can set the **Direction** of the function code to specify which reader(s) can be used to activate it: Entry, Exit or Entry/Exit.

The door must be assigned to the reader expander that the reader is connected to. Function codes will not operate correctly if the **Reader 1/2 door** is <not set>. For third-party and OSDP readers which require a smart reader record for configuration, in addition to the **Reader** tab of the smart reader record the door must also be assigned in the **Reader 1/2** tab of the reader port that the reader is physically connected to.

# Doors | Offline wireless lock settings

This section is only available when the wireless locking integration is enabled (**Global | Sites | Site defaults**).

By default the settings in new door records match the defaults from **Global | Sites | Offline wireless locks**, but you can edit them as required.

## Options

- **Enable lock event log**: Enable this option to allow the offline lock to store events in its internal memory. You can determine what types of events are recorded using the settings below.
- **Enable card event log**: Enable this option to allow the offline lock to transfer events to access cards and mobile devices when access is granted. The events will be uploaded to the system when the credential is badged at an update point reader. This option can be disabled when cards do not have enough storage to collect events.

  If this option is disabled, events can still be retrieved from the lock using the Protege Config App.

- **Log access granted events**: Enable this option to allow the offline lock to log access granted events.
- **Log door open/close events**: Enable this option to allow the offline lock to log door open and close events. This should typically remain disabled, as the additional events can fill up the card's event log quickly.
- **Log access denied events**: Enable this option to allow the offline lock to log access denied events.
- **Log exit events**: Enable this option to allow the offline lock to log exit (REX) events.
- **Deny access when card storage is full**: With this option enabled, the lock will deny access if there is no space on the user's card to store events. The user must badge their card at an update point reader to upload their events before they can gain access. When this option is disabled, access will be granted even if there is no space for new events on the card.

  Use this setting with caution, as cards with low storage space can fill up with events quickly in normal operation.

- **Enable beeper**: With this option enabled, the lock will signal with the beeper as well as the LED. This may impact the lock's battery life.

- **Flash when unlocked by key**: With this option enabled, the reader will flash blue three times when the door is unlocked with a key. This occurs when the door latch is fully retracted (not when the deadbolt is retracted).
- **Allow emergency opening**: Enable this option to allow operators to send the **Emergency open** manual command to the door. An authorized config app user can retrieve the command from an update point reader and use it to unlock the door once. This allows a building manager to open the door when the owner or tenant locks themselves out, but does not grant them permanent access.
- **Exit leaves door unlocked time period**: When the lock is in Exit leaves door unlocked or Exit leaves door unlocked + toggle mode (**Programming | Door types | Options**), by default when someone exits the door will remain unlocked until a user badges a credential to relock it. With this option enabled, the door will automatically lock when the defined period expires. It can still be manually relocked by badging a credential.
- **Schedule operates late to open**: When this option is enabled the door will not latch unlock on schedule until a user unlocks the door. This can be used to prevent the door from automatically unlocking on days when nobody arrives on site.

### Advanced options

- **Lock activation time**: Determines the length of time (in seconds) that the door will unlock for when a user is granted access. This does not apply in modes that toggle the lock.
- **Door extended access time**: When a user with **User operates extended door access function** enabled (**Users | Users | Options**) unlocks this door, it will be unlocked for this period instead of the standard lock activation time.

## Manual Door Commands

Right clicking a door record in **Programming | Doors** or a door icon on a floor plan or status page opens a menu with manual commands for that door.

### Door control

These commands allow you to control basic door functionality. The available commands are:

- **Lock**
- **Unlock** (temporarily activate the lock)
- **Unlock latched** (activate the lock and keep the door unlocked)

### Door lockdown

These commands allow you to lock down individual doors. Any lockdown command will lock the door regardless of any other function causing it to be unlocked. Some lockdown modes allow entry or exit with valid credentials or REX/REN, while others deny access. The available commands are:

- **Allow entry**
- **Allow exit**
- **Allow entry and exit**
- **Deny entry and exit**
- **Clear** (remove the lockdown from the door)

To implement automatic lockdown procedures across multiple doors, use **Door control** programmable functions (**Automation | Programmable functions**).

### View recent events

This command automatically runs an event search in a breakout window, showing all recent events for this door.

For sorting, grouping, filtering and exporting this report, see Viewing Reports (see page 167).

## Offline Wireless Lock Commands

Offline wireless locks are not actively connected to the system and so do not support the standard manual commands for wired doors. However, some commands are available to help with lock administration.

### Door control

- **Force update**: Changes the lock's status from **OK** to **Update required**, allowing you to update the programming with the config app. For example, this could be used to update the lock's internal clock if it is not following schedules correctly, or to collect the full event log using the config app.
- **Reinitialize**: If the **Enable lock reinitializing** setting is activated in **Global | Sites | Offline wireless locks**, you can use this command to change the lock's state to **Initialization required**. You must then default the wireless lock associated with this door record and either initialize it again or replace it with a new one.
- **Emergency open**: If the **Allow emergency opening** setting is enabled (**Offline wireless lock settings** tab), you can use this command to unlock the door once using the config app. Badge a config app at an update point reader to retrieve the command, move to the lock, then tap **Unlock** in the app to temporarily unlock the door.

  The command expires after one hour.

### View recent events

- **View recent**: Runs an event report for the most recent events from that lock.

# Inputs

Motion detectors, door contacts and other digital detection devices are connected to the system as inputs. Inputs can be programmed into areas and monitored to protect the area from unauthorized entry.

However, inputs are not limited to intrusion detection and door control: they can also be used for output control and automation. Because each input can be programmed into up to four different areas with different input types in each, a single unit can serve several purposes in the system.

For example, the traditional use of a PIR (infrared motion detector) is detecting intruders when an area is armed; however, the PIR is equally good at detecting motion from users during working hours. By programming the input into a control area (that is always armed) the same input can also be used to turn on lights when motion is detected, or automatically arm the area when there has been no movement for a specified period of time.

## Inputs | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.

### Address

- **Module type**: The type of module that the input is physically connected to (e.g. controller, input expander).
- **Module address**: The **Physical address** of the module that the input is connected to.
- **Module input**: The index of the input on the connected module. See the relevant module installation manual for wiring instructions.

### Configuration

- **Control output / output group**: You can set an output or output group that is controlled by this input ('output follows input' control), which has a wide variety of applications. For example, you could set up a key switch that will unlock a specific door (one-to-one control) or configure a group of lights to turn on when the REX button is pressed (one-to-many control).

  The relationship between the input state and the output state must be configured in the input type programming (**Programming | Input types | Options (3) | Control options**).

  Alternatively, you can set a **Control output / output group** in the input type programming, allowing many-to-one and many-to-many control (**Programming | Input types | General**).

  The control function is enabled when the area assigned to the input is armed, and disabled when the area is disarmed. If **Twenty four hour panic input** is enabled (**Programming | Input types | Options (1)**), the control function always operates as long as the 24hr portion of the area is armed.

- **Control automation**: This is a legacy option that has no effect.

  Automation control can be programmed in the input type configuration.

- **Support manual commands**: When this option is enabled an operator with the appropriate permissions can send manual commands to the input. For example, a guard might right click on an input on a floor plan and bypass it.

For more information, see Manual Input Commands (page 216).

- **Reporting ID**: The input's Reporting ID is the zone number which will represent that input to the monitoring station. Each newly created input will automatically be assigned the lowest available ID. Alternatively, you can manually assign an ID to each input, allowing a high amount of flexibility in input reporting. For example, if two inputs have the same Reporting ID they will both report as the same input.

  If an input has been assigned a number higher than the maximum that can be reported to a particular service, the highest possible number will be reported. Inputs and trouble inputs share the same range of zone numbers.

  You can view, reset and export Reporting IDs using the **Report map generator** (**Reports | Central station report**). For more information, see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.

- **Alarm input speed**: This setting determines how long an input must be open before the system will register that it has been opened (alarmed). For example, if this is set to 30 seconds the input must be open for 30 seconds before an 'Input Opened' event will be generated.

  The alarm input speed can be set between 0 seconds and 1 hour. Shorter times are useful for inputs which require a rapid response, such as REX buttons. Longer times can be used to prevent alarms from being triggered by small amounts of movement.

  If the alarm input speed is set to 0 seconds the restore input speed cannot be set below 100ms.

  A module update will be required whenever this setting is changed. If the controller is registered as a reader expander this option must be set in the programming for the controller input, not the reader expander input.

- **Restore input speed**: This setting determines how long an input must be closed before the system will register that is has been closed (restored). For example, if this time is set to 30 seconds the input must be closed for 30 seconds before an 'Input Closed' event will be generated.

  The restore input speed can be set between 0 seconds and 1 hour.

  If the alarm input speed is set to 0 seconds the restore input speed cannot be set below 100ms.

  A module update will be required whenever this setting is changed. If the controller is registered as a reader expander this option must be set in the programming for the controller input, not the reader expander input.

- **Enable input lockout**: When this option is enabled, the input will lock out after a certain number of activations (the **Input lockout count**) to reduce false alarms.

  The activation counter is incremented every time the input is opened while the area is armed (regardless of whether it causes an alarm). Once the counter reaches the limit, the input is locked out and further activations will not cause alarms. The lockout is reset when the area is disarmed and rearmed again.

- **Input lockout count**: If this input uses the **Enable input lockout** feature above, this setting defines the number of times the input can be opened before it is locked out.

## Commands

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

## Graphics

- **Camera**: Associating a camera with an input allows you to right click on any input event in an event window to open an archived camera feed from the time of the event.
- **Floor plan**: Associating a floor plan with an input allows you to right click on any input event in an event window to open the floor plan.

## Record history

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

# Inputs | Areas and input types

Much of an input's functionality is controlled by the areas and input types associated with it. The input type describes how the input will function in each area: for example, a door contact input might activate the entry delay in one area and instantly generate an alarm in another. Inputs can be programmed into up to four different areas, allowing the same input to be used for a variety of intrusion detection, control and automation functions in the system.

Changes to settings on this tab may require you to disarm and rearm the affected areas before they come into effect. You must rearm both the main and 24hr portions of the area. The controller will generate a health status message if rearming is required.

## Assigned areas

- **Area 1-4**: The area that monitors this input. Each input can be programmed into up to four different areas and perform different functions in each.
- **Input type 1-4**: The input type defines how the input will operate in a particular area. A wide variety of options and preconfigured input types are available for functions such as intrusion detection, tamper detection, smoke/fire detection and automation/control.

  For example, the preconfigured Instant input type will cause the area alarm to activate immediately when the input is opened, while the Delay input type will cause the area's entry delay to start. For more, see **Programming | Input types**.
- **KLES input LED 1-4**: If an Eclipse keypad is being used in this area, each input can be programmed with an index in this field. When a user is attempting to arm the area, if the input is open the LED number corresponding to this index will flash to indicate which input is preventing the area from arming.

  The input can be assigned an index from 1-19 in each area. The keypad will indicate inputs above 9 by flashing the 0 LED to represent the tens digit.

# Inputs | Options

## Options 1

- **Log to event buffer**: When this option is enabled (by default) the input will generate an event whenever it is opened, closed, tampered or shorted. Disable this option to prevent input events from being generated. The controller will still report alarms, restores and tampers to the monitoring station (as configured in the input type).

  It may be useful to disable event logging for inputs that are primarily used for automation or control to reduce their impact on event storage.
- **Test for trouble condition**: This is a legacy option that has no effect. Input trouble conditions (tamper and short) are generated and reported based on the settings in the input type (see **Generate 24hr alarms** and **Report tampers** in **Programming | Input types | Options (1)**).
- **Bypassing not allowed**: When this option is enabled the input cannot be bypassed (either temporarily or permanently) to arm an area. This should be used for high security inputs that should not be left open and unsupervised when an area is armed.

  This option will not prevent the area from being force armed when the input is open. To prevent this, ensure that the **Force input** option is disabled in the assigned input type (**Programming | Input Types | Options (1)**).
- **Latch bypassing not allowed**: When this option is enabled the input cannot be latch bypassed (i.e. bypassed permanently); however, it can be bypassed temporarily until the area is next disarmed.

  This option will not prevent the area from being force armed when the input is open. To prevent this, ensure that the **Force input** option is disabled in the assigned input type (**Programming | Input Types | Options (1)**).
- **Tamper follows bypass state**: With this option enabled (by default) you can bypass a tampered input to allow the area to arm. With this option disabled the tamper condition cannot be bypassed, so you will not be able to arm an area with a tampered input.

- **No bypass if any area armed**: When this option is enabled this input cannot be bypassed if any of the four areas assigned in the **Areas and input types** tab are armed.
- **Log input event when bypassed**: By default, if the input is bypassed the system will not log events when it changes state (e.g. opens or closes). With this option enabled events will be logged even while the input is bypassed.
- **Tamper input if module offline**: When this option is enabled if the expander module drops offline the controller will report that the input has a tamper condition. This only occurs if the module was previously registered and online with the controller.

### Options 2

- **Input end of line (EOL)**: The EOL resistor configuration used in the physical wiring for this input should be entered here. This determines whether the system can monitor the tamper and short conditions as well as open and closed. See the relevant installation manual for compatible EOL resistor configurations.

  A module update will be required whenever this setting is changed. If the controller is registered as a reader expander this option must be set in the programming for the controller input, not the reader expander input.

- **Contact type**: The contact type used in the physical wiring for this input should be entered here. Inputs can be wired Normally closed (default) or Normally open. This setting determines how the input will be processed by the system.

  For example, REX inputs (buttons) are typically wired with a normally open contact. With this field set to Normally open, when the button is not pressed the input will be marked as Closed/Off and when the button is pressed it will be marked as Open/On.

  A module update will be required whenever this setting is changed. If the controller is registered as a reader expander this option must be set in the programming for the controller input, not the reader expander input.

## Manual Input Commands

Right clicking an input record in **Programming | Inputs** or an input icon on a floor plan or status page opens a menu with manual commands for that input.

### Bypass

These commands allow you to bypass an input. This means the area can be armed even when that input is open or tampered, but the input will not be monitored and will not cause the area to go into alarm. The available commands are:

- **Remove** (remove any bypass from the input)
- **Permanently** (bypass the input permanently so it is always ignored by area arming)
- **Until next disarm** (bypass the input until an area assigned to the input is disarmed)

# Door types

Door types define how each door will operate, allowing you to define settings which can be applied to multiple doors. The credentials required for access (e.g. card, PIN, biometric) and antipassback settings are defined in the door type.

There are a number of preconfigured door types available that provide basic functionality. It is recommended that you do not edit these records, to ensure you have a known baseline to use for testing and troubleshooting. The following default records are available:

- Card
- Card and PIN
- Card or PIN
- PIN only

## Door types | General

### General

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

### General configuration

- **Operating schedule**: The operating schedule determines when this particular door type is active. When this schedule is valid the settings in this door type will be used for those doors. When the schedule is invalid the settings in the **Secondary door type** set below will be used instead.

  For example, you might configure a door type so that Card only access is allowed during working hours. Outside of working hours the door uses the secondary door type with Card and PIN access to improve security.
- **Secondary door type**: The door type that is used when the **Operating schedule** set above is invalid. All settings from this door type are used (including e.g. antipassback settings).
- **Fallback door type**: This door type provides a fallback set of credentials that can be used to gain access to a door at any time.

  For example, if a carpark gate is configured to grant access based on license plate recognition it is helpful to have a traditional card reader available in case users need to open the gate without a car.

  Only the entry/exit credentials from the fallback door type are used, not other settings such as antipassback.
- **Access level door type**: This alternative door type is used by users with the **Use access level door type** option selected in **Users | Access Levels | General**. The settings in the access level door type will be used instead of the primary door type.

  For example, this feature might be used to make it easier for managers or security personnel to move around a site.

- **Allow soft fail failure on missing compliances**: If the **Entry/Exit credential types** field(s) below include a compliance type, normally the user must have that compliance as a credential to gain access to the door. With this option enabled the user will not be denied access when they are missing a compliance. The **Message** set below will be displayed on a compatible reader display, and the user must acknowledge it before they will be granted access.

  For more information, see Application Note 286: Programming Compliance Types in Protege GX.

- **Message**: If the **Allow soft fail failure on missing compliances** option above is enabled, this message will be displayed on the card reader screen to warn users that they are missing a compliance.

  Due to the size of the reader screen, compliance messages are restricted to 32 characters.

## Entry / Exit

The options in these sections refer to door entry and exit settings respectively, and can be set independently for the entry and exit directions.

- **Entry/Exit passback is qualified with door opening**: By default, the user's current area is updated as soon as they are granted access to a door. With this option enabled the current area and antipassback status is not updated unless the user opens the door after being granted access.
- **Entry/Exit passback mode**: This field allows you to enable antipassback for this door type (in the entry and exit directions respectively). Enabling antipassback for a door allows it to monitor the areas that users are currently in, based on the **Area inside/outside door** (which must be set in **Programming | Doors | General**).

  If a user attempts to move through a door from the wrong area they are violating the antipassback rules. The option selected here determines what happens in that situation:
  - **Hard passback**: The user will be denied access until they enter the correct area or their antipassback status is reset.
  - **Soft passback**: The user will not be denied access but a 'Soft Passback Violation' event will be logged.

  User antipassback status can be reset manually by right clicking on a user record or automatically on a timer or schedule using the options in **Programming | Doors | Advanced options**.

  Antipassback has a number of applications. It is primarily used to prevent users from 'passing back' their access card or PIN to unauthorized persons, or to prevent people from 'tailgating' legitimate users. Antipassback can also improve the accuracy of area counting, muster reports and attendance reports, and allow you to manage loiter areas.

  Antipassback is global across the entire site. When a user passes through an antipassback controlled door the controller will update other controllers about the user's current area via cross controller operations. It may also be useful to enable the **Update user area when passback disabled** option in **Programming | Doors | Advanced options** for doors that are not using antipassback.

  For more information and programming examples, see Application Note 337: Configuring Antipassback in Protege GX. Antipassback is also supported for turnstiles and security gates in high level elevator integrations (see the relevant application note).

- **Entry/Exit reading mode**: The reading mode determines which credential or sequence of credentials the door will accept for entry or exit respectively. Even if users have valid permissions they will be denied access unless they have the correct type(s) of credential required by the door type.

  The default credentials available are: Card only, PIN only, Card and PIN, Card or PIN, Card and biometric, and Card or biometric. Selecting Custom opens the **Entry/Exit credential types** section, allowing you to enter a custom sequence of credentials.
- **Door entry/exit requires verification**: With this option enabled, users must gain verification from an operator before they can unlock the door. When a user enters their credentials to request access, operators will receive a popup window with a live camera feed. This allows an operator to visually confirm the user's identity and click an **Unlock** button to unlock the door.

  This option requires a **Camera (entry)** and/or **Camera (exit)** to be programmed for each door in **Programming | Doors | General**.

- **Alert operator but allow entry/exit**: With this option enabled, operators will receive a camera popup as above but the door will unlock without requiring operator action.

### Entry/Exit credential types

These sections are available when the **Entry/Exit reading mode** (respectively) are set to Custom. Click **Add** to create a custom list of credentials that will be accepted by this door type. This can include standard credentials (card, PIN, biometric), credential types and compliance types (both programmed in **Sites | Credential types**).

All credentials entered in this field must be entered to gain access at the door.

- **Sequence**: When this option is enabled the credentials must be entered at the door in the order they are included in the field below. When this option is not enabled the credentials can be entered in any order.

  Compliance types are not affected by this option and are always checked last in the sequence.

For more information and programming examples, see Application Note 276: Configuring Credential Types in Protege GX. For the use of Compliance Types, see Application Note 286: Programming Compliance Types in Protege GX

### Commands

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

### Record history

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

## Door types | Options

- **Door REX not allowed**: With this option enabled, REX (request to exit) operation will be disabled for any doors using this door type. This overrides the settings in the door programming.
- **Door REN not allowed**: With this option enabled, REN (request to enter) operation will be disabled for any doors using this door type. This overrides the settings in the door programming.
- **Requires dual authentication**: When this option is enabled any doors using this door type will require dual authentication (i.e. two separate user credentials) for access. To gain access, the following steps occur:
  - A user with **Dual custody master** enabled (**Users | Users | Options**) enters valid credentials.
  - The door activates the **Reader 1/2 dual authentication pending output** and waits for the second user. If the **Reader 1/2 Dual authentication wait time** is exceeded the access request times out.

    Both options can be configured in **Expanders | Reader expanders | Reader 1/2**.
  - A second user with **Dual custody master** or **Dual custody provider** enabled (**Users | Users | Options**) enters valid credentials.
  - Access is granted and the door unlocks.

  This feature is used for high security areas such as bank vaults or server rooms that require high levels of oversight. It can also be used to ensure there are always two people present in hazardous areas such as laboratories.
- **Dual card provider can initiate access**: When this option is enabled, a **Dual custody provider** can initiate the dual authentication sequence without the requirement for a **Dual custody master**. Any combination of provider and master can initiate and complete the credential sequence.

### Wireless locking options

- **Lock operating mode**: This setting determines how the wireless lock will operate when a user badges their credential or performs specific actions.

- **Standard**: When a user gains access at the reader the door will unlock for the **Lock activation time** (**Programming | Doors | Offline wireless locking**), then lock again. Motorized deadbolts that are unlocked from the inside will also relock after the lock activation time.
- **Office unlock**: A user with **Enable office unlock** can latch unlock the door by holding down the inside handle and badging at the reader. Once unlocked, the door will remain unlocked until the same process is repeated to lock it again.
- **Toggle**: When any user gains access at the reader, the lock will toggle (change from locked to unlocked or back again).
- **Exit leaves door unlocked**: The lock operates in standard mode, but when someone exits using the inside handle the door will remain unlocked. By default it will remain unlocked until someone badges their card to relock it. To automatically relock the door after a time period, enable **Exit leaves door unlocked time period** in **Programming | Doors | Offline wireless locking**.
- **Exit leaves door unlocked + toggle**: The door operates in toggle mode and will also remain unlocked when someone exits using the inside handle.

Mortise locks support all of the above settings. Deadbolt locks only support Standard and Toggle modes.

Wireless locks can change operating mode based on a schedule. When the **Operating schedule** is invalid, the lock will use the settings from the **Secondary door type** (**General** tab).

# Input types

Input types define how an input or trouble input will operate in a particular area. This covers a wide variety of applications: from alarm generation and reporting to trouble monitoring and output, area and automation control. Because each input can be programmed into up to four areas with a different input type in each, input types provide a flexible and efficient method of applying programming to one or more inputs.

There are a number of preconfigured input types available that provide basic functionality. It is recommended that you do not edit these records, to ensure you have a known baseline to use for testing and troubleshooting. You can also copy these defaults to provide a template for your own programming. The available records are:

- Instant: When the input is opened in an armed area the area goes into alarm immediately.
- Instant Force: The same as Instant but the input can be force armed.
- Delay: When the input is opened in an armed area the area begins the entry delay.
- Delay Follow: If the input is opened during the entry delay the alarm is not activated. If the input is opened when the area is armed and not in entry delay the area goes into alarm immediately.
- Delay Follow Force: The same as Delay Follow but the input can be force armed.
- Trouble Silent: Used for trouble inputs. If this input is opened while the 24hr portion of the area is armed a 24hr (tamper) alarm is generated. The bell output for the area is not activated.
- Trouble Bell: Used for trouble inputs. The same as Trouble Silent but the bell output for the area will be activated.
- Fire: Used for smoke detectors and other fire detection inputs. When this input is opened in an armed area the area goes into alarm and a 'Fire' code is sent to the monitoring station.

  It is recommended that fire detection inputs are programmed into a dedicated fire area that is always armed.
- Delay Force: The same as Delay but the input can be force armed.
- 24 Hour Alarm: Used for panic inputs. When this input is opened it generates an alarm even if the area is disarmed. A 'Panic' code is sent to the monitoring station.

## Input types | General

### General

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

### Configuration

- **Operating schedule**: This schedule determines when this particular input type is active. When this schedule is valid the settings for this input type will be used. When the schedule is invalid the settings from the **Secondary input type** will be used instead.
- **Secondary input type**: When the **Operating schedule** set above is invalid, inputs will use this secondary input type.
- **Keypad alarm display group**: When an input using this input type generates an alarm only the keypads in this keypad group will display the alarm information. For example, you might want trouble input alarms to appear only on specific keypads available to installers and maintenance staff rather than regular users.

  If this field is not set all keypads will display alarms from these inputs.

- **Control automation**: The automation that will be controlled by inputs with this input type. Automations can be used to control outputs, or can be connected to C-Bus groups for integrated building automation.

  The relationship between the input state and the automation state must be set in the **Options (3)** tab **Automation options** section.

  You must assign an area to the input and the area must be armed to enable the control function. This is typically a dedicated 'control area'.

  For more information and programming instructions, see Application Note 289: C-Bus Integration with Protege GX and Protege WX.

- **Custom reporting code**: When this input triggers an alarm the custom reporting code determines the event code reported to the central monitoring station. It is also included as a 'Special Code' in the Protege GX event log.

  This allows you to provide more information about the type of alarm being triggered (e.g. medical alarm, smoke alarm, etc.). If this field is set to None the standard burglary code will be used.

  The custom reporting codes available here are drawn from Contact ID standard event codes. For more information, see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.

- **Control output time**: Inputs with this input type will activate the **Control output / output group** (set below) for this period (in seconds). If this time is set to 0 the output will turn on indefinitely.

  By default this field only applies to the control output set in the input type, however if the **Use input type output time** option is enabled (**Options (3)** tab) this time also applies to the control output set in the input programming.

  This setting overrides the **Activation time** set in **Programming | Outputs | General** and the **Output time** set in **Groups | Output groups | General**.

- **Control output / output group**: This output or output group is controlled by inputs with this input type. The relationship between the input state and output state must be configured using the **Output activation options** (**Options (2)** tab).

  This allows 'output follows input' control in a many-to-one or many-to-many configuration. For example, you might configure a group of lights to turn on when motion is detected on one of several PIRs in the room. You can also set a **Control output / output group** in the input programming, allowing one-to-one or one-to-many control.

  The control function is enabled when the area assigned to the input is armed, and disabled when the area is disarmed. If **Twenty four hour panic input** is enabled (**Programming | Input types | Options (1)**), the control function always operates as long as the 24hr portion of the area is armed.

- **Control area**: This area can be force armed and/or disarmed by inputs with this input type. The relationship between the input state and the area state must be configured using the **Miscellaneous options** in the **Options (2)** tab.

  For example, this can be used to create key switches that will arm and disarm a specific area.

  The control area must have the **Enable force arming** option checked in **Programming | Areas | Options (2)**.

## Commands

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

## Record history

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

# Input types | Options (1)

## Alarm options

- **Generate alarms:** When this option is enabled, inputs using this input type will generate alarms. Alarms are generated when an input is opened in an armed area, causing the area to go into an alarm state. The bell output may be activated and the alarm may be saved to the area memory (depending on the settings in the **Options (2)** tab).

  Disabling this option will prevent inputs with this input type from generating alarms. The inputs will still generate open/close events. For example, input types that are used only for automation do not need to generate alarms.

  This feature is not related to the operator alarms that can be programmed in **Events | Alarms**.

- **Generate 24hr Alarms**: When this option is enabled, inputs using this input type will generate 24hr (tamper) alarms. 24hr alarms (sometimes called tamper alarms) are generated when an input is tampered or shorted in an area with the 24hr portion armed. 24hr alarms do not put the area into alarm state or (normally) activate the bell output (but see the settings in **Options (3)**).

  Trouble inputs also generate 24hr alarms when they are opened, however trouble input alarms do put the area into alarm and may activate the bell output as normal. This option should be enabled for any input type used by trouble inputs.

- **Entry delay input**: When this option is enabled, inputs using this input type will initiate the entry delay when they are opened in an armed area. Without this option enabled the area will go into alarm instantly without any entry delay.

  For example, this option could be enabled for inputs on external doors that are used to enter the building.

- **Entry delay follow input**: When this option is enabled, inputs using this input type will not generate alarms during the entry delay period, but will generate alarms if the area is not in entry delay. Without this option enabled inputs will generate alarms even during entry delay.

  This option should be used for inputs which cover the route between the entry and the disarming point. For example, a PIR in the entryway should not generate an alarm when someone enters through the door (beginning the entry delay), but should generate an alarm if someone is detected in the room without opening the door.

- **Exit delay input**: When this option is enabled, inputs with this input type will not generate alarms during the exit delay period. When this option is disabled the input will generate alarms even during exit delay.

  This option should be enabled for any inputs that users may trigger as they exit the building during arming. It may be disabled for other inputs to prevent people from re-entering parts of the building during the arming process.

- **Short exit on restore**: With this option enabled, an input with this input type can be used to shorten the exit delay timer for an area. When the input is restored (closed) during exit delay the exit delay will be reduced to 5 seconds.

  For example, you might enable this option for a door contact so the area arms 5 seconds after the door is closed.

- **Twenty four hour panic input**: When this option is enabled, inputs with this input type will generate alarms even when the assigned area is not armed. A 'panic' action code will be included in the central station report. This allows inputs to act as 'panic buttons' and generate alarms whenever they are opened regardless of the area status.

  This feature uses 24hr tamper monitoring to generate alarms when the main area is not armed. Therefore, the following are also required:

  - The **Generate 24hr alarms** option above must be enabled (however, **Generate alarms** may be disabled).
  - The 24hr portion of the assigned area must be armed.

  To provide more information about the alarm you should also set the **Custom reporting code** in the **General** tab to an appropriate code.

- **Fire input**: When this option is enabled, inputs using this input type will generate fire alarms when opened in an armed area. A 'fire' action code will be included in the central station report. It is recommended that you program any fire inputs in a dedicated fire area that is always armed.

  To provide more information about the alarm you should also set the **Custom reporting code** in the **General** tab to an appropriate code.

  Most smoke detectors use a normally open contact. Ensure that these inputs have the correct **Contact type** and **Input end of line** settings (**Programming | Inputs | Options** tab).

## Reporting options

- **Report alarms**: With this option enabled the controller will report all alarms generated by these inputs to the central monitoring station. In addition, a reporting event will be saved to the event log.

  The **Generate alarms** option must be enabled for this option to function. This feature is not related to the operator alarms that can be programmed in **Events | Alarms**.

- **Report tampers**: With this option enabled the controller will report all 24hr alarms (tamper alarms) generated by these inputs to the central monitoring station. This option should also be enabled to allow reporting of trouble input alarms. In addition, a reporting event will be saved to the event log.

  The **Generate 24hr alarms** option must be enabled for this option to function.

- **Report bypass**: With this option enabled the controller will report to the central monitoring station all instances where these inputs are bypassed to arm an area. It will also report when the bypass is removed. Reporting events will be saved to the event log.

  The **Report user bypass** option must also be enabled in **Programming | Areas | Options (1)**.

- **Report restores**: With this option enabled the controller will report all input restore events to the central monitoring station. This occurs when an input is closed again after generating either an alarm or a 24hr alarm. Reporting events will be saved to the event log.
- **Stay input**: When this option is enabled inputs with this input type will be monitored when the assigned area is stay armed. Inputs with this option disabled will not be monitored when the area is stay armed.

  For example, you may wish to stay arm an area to supervise the perimeter while people are still inside. In this case the **Stay input** option should be enabled for perimeter inputs such as door contacts, and disabled for internal PIRs and other inputs.
- **Force input**: When this option is enabled, inputs using this input type can be forced. This means that the assigned area can be force armed when these inputs are open without bypassing them. The inputs are still supervised and can still generate alarms if closed and opened again.

  If this option is disabled these inputs cannot be forced, however this can be overridden by the **Use unattended brute force arming** option in **Programming | Areas | Options (1)**.

  You may need to bypass inputs when they are force armed to generate bypass reports. Enter one of the following commands in the **General** tab:

  - `EnableForceBypass = true` (bypasses the input until the area is disarmed)
  - `ForceSendsBypass = true` (bypasses the input until it is closed)
- **Exit alley input do not test it**: Inputs with this option enabled will not be tested when the assigned area is arming. This means that the area can be armed even if these inputs are open and not bypassed.

  This should be used for inputs such as PIRs that overlook keypads and other arming points, which would otherwise need to be bypassed every time the area is armed. It should be used alongside the **Exit delay input** option.
- **Recycle input alarm on exit delay end**: By default, inputs with the **Exit delay input** feature do not generate alarms if they remain open after the exit delay ends. An alarm would only be generated if the input closes and opens again after arming. When this option is enabled any input that is still open at the end of the exit delay will be recycled (closed and opened again), generating an alarm.

  Use this feature for inputs that may be breached during exit delay, such as window or door contacts.

# Input types | Options (2)

## Miscellaneous options

- **Activate bell output**: With this option enabled, when an input or trouble input with this input type generates an alarm the bell output for the assigned area is activated. This may be disabled in cases where a silent alarm is required (e.g. duress inputs).

  For regular inputs this option does not normally apply to 24hr / tamper alarms, but the **24hr generates bell if armed** or **24hr always generates bell** settings (**Options (3)**) may be enabled as required.

- **Retrigger bell time**: When this option is enabled these inputs can retrigger the area's alarm/bell timer. If the alarm has already been activated when the input is opened the alarm timer will be reset to extend the time the bell output is activated.
- **Save to area memory**: When this option is enabled, alarms generated by these inputs will be saved to the area's alarm memory. The alarm memory can be viewed and acknowledged in the View menu of a keypad (**[Menu] [5] [1]**). Alarms in the memory are cleared the next time the area is armed.

  Disable this option to prevent alarms from being saved to the alarm memory.
- **Disarm control area on input restore**: When this option is enabled the **Control area** set in the **General** tab will be disarmed when any input with this input type is closed (restored).
- **Arm control area on input alarm**: When this option is enabled the **Control area** set in the **General** tab will be armed when any input with the input type is opened (alarmed).

  It is not necessary to activate the area alarm to perform the control function.

- **Toggle control area on input alarm**: When this option is enabled, whenever an input with this input type is opened the state of the **Control area** set in the **General** tab will be toggled. This means that each time the input is opened the area will switch from disarmed to armed, or vice versa.

  It is not necessary to activate the area alarm to perform the control function.

- **Allow force arming of tampered input**: By default, areas cannot be force armed if they contain an input which is in a tamper state. With this option enabled, areas can be force armed even if inputs with this input type are tampered.

  The **Force input** option must also be enabled in the **Options (1)** tab.

- **Activate entry output on bell time**: This is a legacy option that has no effect.
- **Test during hold up walk test**: A hold up walk test is a special walk test that can be enabled for an area in **Programming | Areas | Options (1)**. All inputs with this option enabled are required to be tested during the hold up walk test. This is useful when there are a small number of critical inputs that must be tested regularly, such as panic or duress buttons.

  For more information, see Application Note 197: Configuring a Hold Up Walk Test in Protege GX.

## Output activation options

- **Activate bypass output**: With this option enabled these inputs can activate the area's **Bypassed inputs output / output group**. This is activated when the area is armed with bypassed inputs in it, and deactivated when the area is disarmed.
- **Activate 24hr tamper output**: With this option enabled these inputs can activate the area's **Tamper alarm output / output group**. This is activated when an input generates a 24hr (tamper) alarm and deactivated when the area's 24hr portion is disarmed.
- **Activate memory output**: With this option enabled these inputs can activate the area's **Alarm memory output / output group**. This output is activated when an alarm occurs in an area and remains on until the area is disarmed.

  This feature can be used to indicate to users that there has been an alarm, preventing them from entering potentially insecure areas.

- **Activate control output on alarm**: With this option enabled the **Control output / output group** will be activated whenever an input with this input type is opened (alarmed).

  This option refers to the control output set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Activate control output on restore**: With this option enabled the **Control output / output group** will be activated whenever an input with this input type is closed (restored).

  This option refers to the control output set in the input type programming (**General** tab).

- **Deactivate control output on alarm**: With this option enabled the **Control output / output group** will be deactivated whenever an input with this input type is opened (alarmed).

  This option refers to the control output set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Deactivate control output on restore**: With this option enabled the **Control output / output group** will be deactivated whenever an input with this input type is closed (restored).

  This option refers to the control output set in the input type programming (**General** tab).

- **Toggle control output state on alarm**: With this option enabled the **Control output / output group** will be toggled whenever an input with this input type is opened (alarmed). This means that each time the input is opened the output will switch from off to on, or vice versa.

  This option refers to the control output set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Input retriggers output time**: When this option is enabled these inputs can be opened/closed a second time to restart the **Control output time** (**General** tab) so that the control output remains on for longer.

  For example, this can enable motion controlled lights to stay on for longer when a second person triggers the motion sensor.

  This feature also works with the **Control output / output group** set in the input programming. The **Use input type output time** option must be enabled in the **Options (3)** tab.

  This option only functions correctly when the area assigned to the input is armed.

# Input types | Options (3)

## Automation options

- **Activate automation on alarm**: With this option enabled the **Control automation** will be activated whenever an input with this input type is opened (alarmed).

  This option refers to the control automation set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Activate automation on restore**: With this option enabled the **Control automation** will be activated whenever an input with this input type is closed (restored).

  This option refers to the control automation set in the input type programming (**General** tab).

- **Deactivate automation on alarm**: With this option enabled the **Control automation** will be deactivated whenever an input with this input type is opened (alarmed).

  This option refers to the control automation set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Deactivate automation on restore**: With this option enabled the **Control automation** will be deactivated whenever an input with this input type is closed (restored).

  This option refers to the control automation set in the input type programming (**General** tab).

- **Toggle automation state**: With this option enabled the **Control automation** will be toggled whenever an input with this input type is opened (alarmed). This means that each time the input is opened the automation will switch from off to on, or vice versa.

  This option refers to the control automation set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **24hr generates bell if armed**: When this option is enabled, inputs with this input type can activate the area's bell output on a 24hr / tamper alarm, but only when the area is armed. The **Activate bell output** option must be enabled in the **Options (2)** tab.

  This option is not required for trouble inputs.

- **24hr always generates bell**: When this option is enabled, inputs with this input type will always activate the area's bell output on a 24hr / tamper alarm. The bell will be activated even if the area is not armed. The **Activate bell output** option must be enabled in the **Options (2)** tab.

  This option is not required for trouble inputs.

### Control options

- **Use input type output time**: This option allows the **Control output / output group** set in the input programming to use the **Control output time** set in the input type programming. When the control output is activated it will turn off after the period set in the input type.
- **Activate input control output on alarm**: With this option enabled the **Control output / output group** set in the input programming will be activated whenever an input with this input type is opened (alarmed).

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**). It is not necessary to activate the area alarm to perform the control function.

- **Activate input control output on restore**: With this option enabled the **Control output / output group** set in the input programming will be activated whenever an input with this input type is closed (restored).

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**).

- **Deactivate input control output on alarm**: With this option enabled the **Control output / output group** set in the input programming will be deactivated whenever an input with this input type is opened (alarmed).

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**). It is not necessary to activate the area alarm to perform the control function.

- **Deactivate input control output on restore**: With this option enabled the **Control output / output group** set in the input programming will be deactivated whenever an input with this input type is closed (restored).

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**).

- **Toggle input output state**: With this option enabled the **Control output / output group** set in the input programming will be toggled whenever an input with this input type is opened (alarmed). This means that each time the input is opened the output will switch from off to on, or vice versa.

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**). It is not necessary to activate the area alarm to perform the control function.

## Input types | Options (4)

### General options

- **Always log input event**: When this option is enabled, inputs with this input type will always generate events, regardless of whether the **Log to event buffer** option is disabled in the input programming (**Programming | Inputs | Options**).

- **Use alternate entry time**: With this option enabled, whenever an input with this input type initiates an entry delay it will use the **Alternate entry time** set in **Programming | Areas | Configuration**. For example, you might use this for the door contact on a rear entry or a garage door to allow the user more time to reach the keypad.

# Areas

Areas generally represent physical spaces in the Protege GX site, and are used for monitoring inputs and generating alarms when intruders are detected. These are sometimes known as alarm areas or partitions.

When an area is armed it begins monitoring the inputs assigned to it. If an input is opened the area will respond based on the input type assigned to the input - for example, by going into alarm or beginning the entry delay. Disarming the area will end monitoring and silence any alarms.

Areas also have a 24hr portion, which should be armed (enabled) at all times. This portion of the area is used to monitor tamper or short conditions and can also go into alarm (usually without activating the bell). Areas can also be integrated with access control by being assigned as the **Area inside / outside door** (**Programming | Doors | General**).

For some purposes it is useful to create areas that do not correspond to physical spaces and may not have physical alarm outputs, but are always armed so they can be used for monitoring and control. For example, a 'system area' allows you to monitor trouble inputs and report any system troubles at all times. A 'control area' or 'automation area' is generally used for output control and other automation functions, and does not generate alarms. Each input can be assigned to up to four areas, so they can perform a different function in each regardless of the other areas' status. For more information, see Inputs | Areas and input types (page 215).

## Areas | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

### Graphics

- **Camera**: Associating a camera with an area allows you to right click on any area event in an event window to open an archived camera feed from the time of the event.
- **Floor plan**: Associating a floor plan with an area allows you to right click on any area event in an event window to open the floor plan.

### Record history

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

## Areas | Configuration

### Timings

- **Entry time**: The duration of the area's entry delay, in seconds. If an entry delay input is triggered while the area is armed the area will go into entry delay. If the area is not disarmed before this period elapses the alarm will be activated.

  If this time is set to 0 the area will immediately go into alarm, regardless of the input that is activated.

For an input to begin the entry delay it must have **Entry delay input** enabled in the input type (**Programming | Input types | Options (1)**).

The remote notify delay feature allows you to delay offsite reporting of alarms which occur during the entry delay. For more information, see Application Note 312: Minimizing Offsite Reporting of False Alarms in Protege GX and Protege WX.

- **Alternate entry time**: An alternative duration for the area's entry delay, in seconds. This will be used if the entry delay is triggered by an input with the **Use alternate entry time** option enabled in the input type (**Programming | Input types | Options (4)**).

  This can be used to grant users a longer time to disarm the system when they enter through an alternative entrance, such as a garage or back door.
- **Exit time**: The duration of the area's exit delay, in seconds. Whenever the area is armed the exit delay will begin, giving users time to exit the area before it is armed. When the exit delay time elapses the area will be armed. If this time is set to 0 the area will arm immediately.

  During the exit delay, inputs with the **Exit delay input** option enabled (**Programming | Input types | Options (1)**) will not generate alarms. This should be used for any inputs that users may trigger as they exit the area (e.g. PIRs, door contacts).
- **Alarm 1 time**: The duration (in minutes) that the bell output will stay on when the area alarm is activated. The minimum alarm time is 1 minute.

  Some areas may have limitations on how long a bell or siren can be activated. Ensure you check your local regulations before setting this field.
- **SmartInput timer**: The smart input feature prevents false alarms in areas by counting multiple unique input activations before activating the alarm. When an input is opened the alarm will not activate unless one or more additional inputs open within the period defined here (in seconds).

  To use this feature check the **Enable smart inputs** option in the **Options (2)** tab. The number of inputs is defined by the **SmartInput count** below.
- **Rearm area time**: If the **Re-arm enabled** option is checked in the **Options (1)** tab, whenever this area is disarmed it will automatically rearm after the time defined here (in minutes). If this time is set to 0 the area will rearm after 1 minute.
- **Vault disarm delay**: If the **Vault control area** option is enabled in the **Options (2)** tab, whenever a user attempts to disarm the area from a keypad there will be an additional delay before the area is disarmed. This field defines the delay time (in minutes). If this time is set to 0 the area will be disarmed immediately.
- **Vault dual code delay**: If the **Dual code vault control** option is enabled in the **Options (2)** tab the area will require two user codes to disarm. This field defines the time limit (in seconds) in which a second user must log in to the keypad and disarm the area, after the vault disarm delay period has elapsed. If the second user does not enter a PIN within this time, the disarming process will expire.
- **Recent closing time**: This time (in seconds) defines how long after arming an area is considered to be 'recently closed'. If an alarm is generated in the area within this period (in seconds) a Recent Close message will be sent to the monitoring station along with the alarm message. This option will only function when the **Report alarms** option is enabled for the relevant input in **Programming | Input types | Options (1)**.

  The alarm will be activated regardless of whether the area has been recently armed or not.

## Schedule

- **Arm/Disarm schedule**: This schedule can be used to arm and disarm an area automatically. The function depends on the options selected below. See also **Always verify area schedule** in the **Options (2)** tab.
- **Disarm area when schedule starts**: When this option is enabled the area will automatically disarm when the **Arm/Disarm schedule** above becomes valid.

  Use this option with caution, as the area will be disarmed regardless of whether there are any authorized users present.

- **Arm area when schedule ends**: When this option is enabled the area will automatically arm when the **Arm/Disarm schedule** above becomes invalid. This can be used to ensure that the area is secured each day even if the users forget to arm it.

  This feature force arms the area, so the **Enable force arming** option must be enabled (**Options 2** tab).

## Setup

- **Child area**: A child area may be armed and disarmed automatically based on the state of one or more parent areas. The relationship between the child and parent area status is based on the options selected in the **Options (1)** tab.

  Since multiple parent areas can be applied to a single child area, this feature can be used to create a 'common area' that is dependent on a number of other areas.
- **Maximum bypass input count**: The maximum number of inputs that can be bypassed within the programmed area. If more than this number of inputs have been bypassed the area cannot be armed. When this field is set to 0 there is no limit on the number of bypassed inputs.
- **Max user count**: If the **Enable user counting** option is selected (**Options (1)** tab) this field allows you to set the maximum number of users who can be in the area at the same time. For example, if the user limit is set to 10 the 11th user who attempts to enter the area will be denied access.

  This feature is useful when there is a fire, security or health and safety code limiting the number of people allowed in a certain area, or to limit the number of users entering a carpark. You can set a **User count reached output** (**Outputs** tab) that will be activated when the area is at its maximum user count.

  This field must be set to a value above zero to enable area counting. If there is no limit on the number of users allowed in the area you can set this field to the maximum value (65535).
- **Client code**: This code represents the area in reports to the central monitoring station. This is typically a hexadecimal number but the format may depend on the receiver compatibility. If the client code for the area is left at the default value (FFFF) the area will use the **Client code** set in the reporting service (**Programming | Services | General**).

  It can be useful to set different client codes for each area in situations where a single Protege GX system contains multiple different tenancies, such as offices or apartments.
- **Interlock area group**: When an area has an interlock area group assigned it cannot be disarmed unless all other areas in the area group are armed. This can ensure that a high security area will not disarm until the areas surrounding it are secure.
- **SmartInput count**: The smart input feature prevents false alarms in areas by counting multiple unique input activations before activating the alarm. The alarm will not be activated until this number of unique inputs have opened within a certain time.

  To use this feature check the **Enable smart inputs** option in the **Options (2)** tab. The time period is set in the **SmartInput timer** field above.
- **Reporting ID**: The area's Reporting ID is the group number which will represent that specific area to the monitoring station. The next available ID will be automatically assigned when each area is created, or you can manually assign the required IDs. If an area has been assigned a number higher than the maximum that can be reported to a particular service the highest possible number will be reported.

  You can view, reset and export area Reporting IDs using the report map generator (**Reports | Central station report**). For more information, see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.
- **Lock door group on arming**: When this area is armed the doors in this door group will be automatically locked. This can be used to ensure that all entry doors for an area are locked when the area is armed, preventing users from accidentally entering an armed area.

## Reporting services

This field allows you to assign the reporting services that will send reports for this area and any inputs or trouble inputs programmed in it.

Services can be programmed in **Programming | Services**.

### Loiter

- **Loiter timer**: When the area has the **Area enabled in loiter mode** option selected (**Options (1)** tab) this field determines how long (in minutes) a user can remain in this area before they are moved into the **Loiter reset area**.

  When this field is set to 0 users will never be moved into the loiter reset area.
- **Loiter reset area**: When the area has the **Area enabled in loiter mode** option selected (**Options (1)** tab) the user will be 'moved' to the area defined here when the **Loiter timer** elapses. After the user has been moved to the loiter reset area antipassback rules can prevent them from exiting the physical area they are in until their antipassback status is reset.

### Defer warning

- **Defer warning keypad group**: When the area has the **Defer automatic arming** option enabled (**Options (2)** tab) the keypads in this group will beep once and display a warning message when the area is about to arm automatically. While the message is displayed users can log in to the keypad and use the **[DISARM]** key to prevent the area from arming automatically.

  The **Display defer area warning messages** option must also be enabled for each keypad in **Expanders | Keypads | Options 1**. Higher priority messages (e.g. alarms) may override the defer arming warning.
- **Defer warning time**: When the area has the **Defer automatic arming** option enabled (**Options (2)** tab), automatic arming will be delayed by the time defined here (in minutes). Use this setting to give users sufficient time to leave the area or log in to the keypad and cancel the arming.

### Commands

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

## Areas | Outputs

### Outputs

- **Bell output / output group**: This output or output group is activated when an alarm is generated in the area. The bell output will remain on for the **Alarm 1 Time** (**Configuration** tab) or until the area is disarmed.

  Whether the bell output is activated depends on the input type that generated the alarm. The **Activate bell output** option in **Programming | Input types | Options 2** must be enabled.
- **Bell pulse on/off time**: These fields are used to make the bell output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Exit delay output / output group**: This output or output group is activated during the area's exit delay period. It is deactivated when the exit delay is complete or if the area is disarmed again.

  Use this output, commonly a keypad or reader beeper, to warn users to leave the area before it is armed.
- **Exit delay pulse on/off time**: These fields are used to make the exit delay output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Entry delay output / output group**: This output or output group is activated during the area's entry delay period. It is deactivated when the entry delay times out (activating the alarm) or when the area is disarmed.

  Use this output, commonly a keypad or reader beeper, to warn users to disarm the area before the alarm is activated.
- **Entry delay pulse on/off time**: These fields are used to make the entry delay output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Disarmed output / output group**: This output or output group is activated when the area is disarmed. It is deactivated when the area begins arming.

  This feature can be used to give users a visual indication when the area is disarmed (e.g. the green LED on a keypad). This could also be used to activate any lock relays that are not controlled by readers, so internal doors unlock when the area is disarmed. Disarmed outputs may also drive further processes that are activated when an area is disarmed.
- **Disarmed pulse on/off time**: These fields are used to make the disarmed output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Armed output / output group**: This output or output group is activated when the area is successfully armed. It is deactivated when the area is disarmed.

  This feature can be used to give users a visual indication when the area is armed (e.g. the red LED on a keypad), preventing users from attempting to enter armed areas. Armed outputs are also useful for driving further processes that are activated when an area is armed.
- **Armed pulse on/off time**: These fields are used to make the armed output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Bypassed inputs output / output group**: This output or output group is activated when the area is armed with one or more bypassed inputs. It is deactivated when the area is disarmed.

  This output will only be activated by inputs with **Activate bypass output** enabled in the input type (**Programming | Input types | Options 2**).
- **Bypassed inputs pulse on/off time**: These fields are used to make the bypassed inputs output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Tamper alarm output / output group**: This output or output group is activated whenever a 24hr / tamper alarm is generated in the area. It is deactivated when the area's 24hr portion is disarmed (disabled). This feature can be used to alert personnel that an input has been tampered, without activating the area's bell output.

  This output will only be activated by inputs with **Activate 24hr tamper output** enabled in the input type (**Programming | Input types | Options 2**).

- **Tamper alarm pulse on/off time**: These fields are used to make the tamper alarm output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Alarm memory output / output group**: This output or output group is activated whenever an alarm is generated in the area. It is deactivated when the area is disarmed. This feature can be used to warn users when there has been an alarm, preventing them from entering a potentially insecure area.

  This output will only be activated by inputs with **Activate memory output** enabled in the input type (**Programming | Input types | Options 2**).

- **Alarm memory pulse on/off time**: These fields are used to make the alarm memory output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **User count reached output / output group**: This output or output group is activated when the user count in an area reaches the **Max user count** set in the **Configuration** tab. It is deactivated when the area no longer contains the maximum number of users. For example, this could be used in a carpark to activate a 'Carpark Full' sign when there are no more parks available.

  **Enable user counting** must be selected in the **Options 1** tab.

- **User count reached pulse on/off time**: These fields are used to make the user count reached output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Area defer arming started output / output group**: This output or output group is activated whenever the area defers automatic arming. It is deactivated when the **Defer warning time** (**Configuration** tab) expires and the area arms or when the arming is canceled at a keypad. Use this feature to notify users in the area that it is about to start arming.

  **Defer automatic arming** must be enabled in the **Options 2** tab.

- **Defer arming started pulse on/off time**: These fields are used to make the defer arming output or output group pulse on and off when activated.

The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Fail to arm output / output group**: This output or output group is activated for 5 seconds whenever the area fails to arm (for example, because there are inputs that have not been bypassed).
- **Ready output / output group**: This output or output group is activated when all of the inputs and trouble inputs programmed in the area are closed, signaling that the area is ready for arming. It is deactivated when the area is armed or when an input or trouble input is opened and the area is no longer ready to arm.

# Areas | Options (1)

## General options

- **Input restore on bell cut-off**: With this option enabled, when this area goes into alarm any inputs that are open enter a 'siren lockout' state. This means that if the inputs are restored (closed) or reopened it will not be reported to the monitoring station until the bell times out or is silenced.

  This option prevents the **Retrigger bell time** feature in **Programming | Input types | Options (2)** from functioning.

- **Re-arm enabled**: With this option enabled, whenever the area is disarmed it will be automatically rearmed after a certain time. The delay before rearming is set by the **Rearm area time** (**Configuration** tab). This function force arms the area, so **Enable force arming** must be selected (**Options (2)** tab).

  This feature should be used for areas that are used for system monitoring and control, which should never be disarmed. It can also be used to ensure bank vaults, automatic teller machines and similar are not disarmed for longer than the programmed time.

  When you enable rearming you must arm and disarm the area for the setting to take effect.

- **Arm child area**: When this option is enabled, whenever this area finishes arming the **Child area** (**Configuration** tab) will be armed.

  This option must be enabled in the parent area(s).

- **Arm child if all other areas are armed**: When this option is enabled the **Child area** (**Configuration** tab) will be armed whenever this area is armed, provided that all other parent areas are already armed. The **Arm child area** option above must also be enabled.

  For example, there may be three areas; A, B and C, where C is a child area of A and B. By default, C will be armed whenever either A OR B is armed. With this option enabled, area C will be armed when both A AND B are armed.

  This option must be enabled in the parent area(s).

- **Disarm child area**: When this option is enabled, whenever this area finishes disarming the **Child area** (**Configuration** tab) will be disarmed.

  This option must be enabled in the parent area(s).

- **Disarm child if all other areas are disarmed**: When this option is enabled the **Child area** (**Configuration** tab) will be disarmed whenever this area is disarmed, provided that all other parent areas are already disarmed.

  For example, there may be three areas; A, B and C, where C is a child area of A and B. By default, C will be disarmed whenever either A OR B is disarmed. With this option enabled in both A and B, C will be disarmed when both A AND B are disarmed.

  This option must be enabled in the parent area(s).

- **Use unattended brute force arming**: Typically an area cannot be force armed if there are open inputs with the **Force input** option disabled (**Programming | Input types | Options (1)**). Enabling this option allows you to 'brute force arm' the area using unattended or remote methods even if these inputs are open.

  Use this option to ensure that the area can always be force armed by the system (e.g. on schedule or automatic rearm), an operator or a user at a card reader. This will not allow users at a keypad to brute force arm the area.

  By default, when an area is brute force armed the status is set to Armed. To use Force Armed for the status, enter the `UnattendedForceArm = true` command.

- **Area enabled in loiter mode**: Loiter mode allows you to limit the amount of time that users spend in an area. This is commonly used in carparks, where users must transit the public parking area to reach their designated parking space.

  When a user enters the area the **Loiter timer** starts. If they stay in the area longer than the allotted time the system automatically moves the user into the **Loiter reset area** (a virtual 'holding area'). When the user attempts to leave the physical area the system detects that they are in the wrong area and denies exit due to the antipassback violation. The user cannot exit until their antipassback status has been reset (e.g. by an operator or by badging at a designated reader that provides exit from the loiter area).

  The following must be configured to complete loiter area programming:

  - **Loiter timer** (**Configuration** tab)
  - **Loiter reset area** (**Configuration** tab)
  - **Entry/Exit passback mode** set to Hard passback (**Programming | Door types | General**)
  - **Area inside/outside door** (**Programming | Doors | General**)
  - **User loiter expiry count enabled** (**Users | Users | Options**)

  For more information and programming examples, see Application Note 341: Programming Area Loiter Functionality in Protege GX.

## Reporting options

- **Report arming**: With this option enabled, whenever this area is armed a report will be sent to the monitoring station and saved to the event log. This report includes the user who initiated the arming. Disable this option when these reports are not required (e.g. for virtual control areas).
- **Report disarming**: With this option enabled, whenever this area is disarmed a report will be sent to the monitoring station and saved to the event log. This report includes the user who initiated the disarming. Disable this option when these reports are not required (e.g. for virtual control areas).
- **Report 24hr area disarming**: With this option enabled, whenever the 24hr portion of this area is disarmed (disabled) a report will be sent to the monitoring station and saved to the event log. This report includes the user who initiated the disarming. There is no equivalent report available for arming / enabling the 24hr portion of the area.
- **Report user bypass**: With this option enabled, whenever this area is armed it will report all bypassed inputs in the area. The reports will be sent to the monitoring station and saved to the event log. The **Report bypass** option must also be enabled for the relevant input(s) in **Programming | Input types | Options (1)**.
- **Enable user counting**: With this option enabled the system will count the number of users in the area. When a user enters the area the count is increased by one, and when they exit the count is decreased by one.

  This feature should only be used in areas serviced by doors that have both entry and exit readers, as REX and REN will not alter the user count. The **Area inside/outside door** must be set correctly in **Programming | Doors | General**. It is recommended that user counting is used alongside antipassback (see **Programming | Door types | General**) to ensure that user counts are accurate.

  A number of features are available with user counting:

  - **Max user count** (**Configuration** tab)

    This option must be set to a non-zero value for user counting to function.

  - **User count reached output / output group** (**Outputs** tab)
  - **Arm on user count at 0** (**Options (1)** tab)

- **Clear user count when armed** (**Options (1)** tab)
- **Prevent arming on count not zero** (**Options (2)** tab)

For more information, see Application Note 205: Area Counting in Protege GX. For advanced applications, see Application Note 278: Access Level Area Counting in Protege GX.

- **Arm on user count at 0**: When **Enable user counting** is selected above, this feature causes the area to automatically arm when the user count reaches zero. This feature ensures the area will be secured when the last user leaves, regardless of whether they have actively armed it. This is especially useful in large office environments where it is not practical for users to check whether there is anyone else in the area.

  It is recommended that this feature is used alongside antipassback settings to ensure that the user count is accurate. If not, the area may arm while there are still people inside.

- **Report entry alarm immediately**: When this option is enabled, if an entry input opens in an armed area a report will be sent to the monitoring station and the event log immediately, even though the area is in entry delay. A second report will be generated if the area goes into alarm. When this option is disabled an input opening that triggers entry delay will not be reported.

  This option applies to inputs with the **Entry delay input** and **Report alarms** options enabled in the input type (**Programming | Input types | Options (1)**).

- **Clear user count when armed**: When this option is enabled (by default) the user count for the area (see **Enable user counting** above) will be cleared / set to zero when the area is armed. When this option is disabled the user count will not be cleared.

## Hold up area walk test

- **Enable hold up walk test when disarming**: A hold up walk test is a special kind of walk test that allows specific inputs to be tested every time the area is disarmed. The inputs that must be tested have **Test during hold up walk test** enabled in the input type (**Programming | Input types | Options (2)**). This feature is used for regular testing of a small number of critical inputs, such as panic buttons.

  Whenever a user attempts to disarm the area from a keypad the hold up walk test begins automatically. All of the required inputs must be tested (opened) before the **Maximum test time** elapses. If the test times out before all the inputs have been tested the area will not be disarmed.

  During the test the keypad will beep regularly and display messages, including the name of each input as it is tested. After the first input has been opened the **Output / Output group to activate during test** (set below) will be activated. These are deactivated when the test is completed or times out.

  For programming instructions, see Application Note 197: Configuring a Hold Up Walk Test in Protege GX.

- **Maximum test time (seconds)**: The maximum duration (in seconds) that the hold up walk test will run. After this time the test times out and the area will not be disarmed. Ensure that the time is sufficient for testing all of the required inputs.
- **Contact ID group code for test starting**: This Contact ID event code is sent to the monitoring station when the hold up walk test starts.
- **Contact ID group code for input activation**: This Contact ID event code is sent to the monitoring station when each input is activated during the hold up walk test.
- **Contact ID group code for test passed**: This Contact ID event code is sent to the monitoring station when the hold up walk test is passed (i.e. all inputs have been activated successfully).
- **Contact ID group code for test canceled**: This Contact ID event code is sent to the monitoring station when the hold up walk test is manually canceled or times out.
- **Output / Output group to activate during test**: This output or output group is activated during the hold up walk test as soon as the first input has been activated. It is deactivated when the test is completed or times out. Use this to notify users that the test is active, prompting them to activate their inputs.

# Areas | Options (2)

## Advanced options

- **Enable stay arming**: When an area is stay armed only inputs with the **Stay input** option enabled (**Programming | Input types | Options (1)**) will be monitored. For example, this allows you to arm the perimeter of an area without arming the internal sensors, so that users can remain securely inside. With this option disabled the area cannot be stay armed.
- **Enable force arming**: When an area is force armed it is armed without testing the inputs. The area will be armed even if there are inputs open, provided that the inputs have the **Force input** option enabled (**Programming | Input types | Options (1)**). When this option is disabled the area cannot be force armed.

  See also **Use unattended brute force arming** below.
- **Enable instant arming**: When an area is instant armed it arms immediately with a 1 second exit delay. Also, all inputs that would normally initiate the entry delay instead trigger the alarm immediately (i.e. all inputs are treated as 'instant' inputs). When this option is disabled the area cannot be instant armed.

  Areas can be instant armed or instant force armed from the software, and instant stay armed or instant force armed from a keypad.
- **Do not arm if trouble condition**: When this option is enabled the area will be prevented from arming if there is any trouble input open in the system. This ensures that all trouble conditions are resolved before the area is armed.

  This is useful for high security areas which should not be vacated before all troubles are resolved.
- **Vault control area**: When this option is enabled the area will not disarm until the defined delay period elapses. The **Vault disarm delay** is set in the **Configuration** tab. This ensures that very high security areas such as bank vaults cannot be disarmed quickly in the case of a hold up.

  For more information and programming instructions, see Application Note 338: Programming Protege Keypads.
- **Dual code vault control**: When this option is enabled two separate users must log in to a keypad and press the disarm button in order to disarm the area. After the first user presses disarm, the vault disarm delay must expire before the second user can enter their code. The time allotted for the second user to disarm the area is the **Vault dual code delay** set in the **Configuration** tab.

  The **Vault control area** setting above must also be enabled.
- **Prevent arming on count not zero**: When user counting is enabled (**Options (1)** tab), this option prevents the area from arming when the user count is not zero. This ensures that the area cannot be armed (manually or automatically) when there are still users in the area.

  It is recommended that this feature is used alongside antipassback settings to ensure the user count is accurate. If there is an error in the user count it may become impossible to arm the area even after all users have left.
- **Always verify area schedule**: By default, the area only checks the **Arm/Disarm schedule** (**Configuration** tab) on edges, i.e. when the schedule becomes valid or invalid. This means the area can be disarmed or armed manually regardless of the status of the schedule.

  When this option is enabled the area will verify the schedule every minute. If the area is not in the armed/disarmed state required by the schedule it will change to the correct state.
- **Enable smart input**: By default, an area will go into alarm based on a single input activation. In smart input mode multiple unique inputs must be activated before the area will activate the alarm. This is useful for preventing false alarms.

  When an input is opened in the armed area a timer starts based on the **SmartInput timer** (**Configuration** tab). The area will count unique input activations (reactivating the same input will not increase the counter). If the number of activations reaches the **SmartInput count** (**Configuration** tab) the alarm will be activated. The same number of activations is required to initiate the entry delay.

The response of the area depends on the input type of the final input that is triggered. For example, if the first input would start the entry delay but the last causes an instant alarm the area will go into alarm instantly.

Smart inputs can be used alongside the remote notify delay feature to send confirmed alarm reports to the monitoring station. For more information, see Application Note 312: Minimizing Offsite Reporting of False Alarms in Protege GX and Protege WX.

- **Area can be reset**: When this option is enabled the area can be rearmed from a keypad without being disarmed first. This means that an area that goes into alarm can be reset (silencing the bell output) without being disarmed. Use this option for areas that should not be disarmed after an alarm.

## Arming options

- **Defer automatic arming**: When this option is enabled, whenever the area begins arming automatically by a schedule the arming can be deferred (delayed) for a defined period of time. Users will receive notice that the area is about to arm, allowing them to leave the area or log in to the keypad and press the disarm key to defer the automatic arming.

  The **Always verify area schedule** option (see above) **must be disabled** as it will override any defer arming.

  The following settings are available:
  - The **Defer warning time** (**Configuration** tab) determines how long the area will display the warning before beginning to arm.
  - You can give users a visual and/or audible indication that the area is about to arm using the **Defer warning keypad group** (**Configuration** tab) and **Area defer arming started output / output group** (**Outputs** tab).
  - When a user defers arming from the keypad, the **Rearm area time** (**Configuration** tab) defines how long the area will wait before attempting to arm again.
  - Alternatively, the `AskForDeferTime = true` command allows users to specify the number of hours that arming will be deferred for when they cancel the arming at the keypad.
  - The `ReArmAsDeferArea = true` command allows the area to defer automatic rearming, so that defer arming can be used alongside the **Re-arm enabled** feature (**Options (1)** tab).

  For more information and programming instructions, see Application Note 338: Programming Protege Keypads.

- **Always force arm using card reader**: When this option is enabled, whenever a user arms an area using a card reader the area will be force armed. If this option is disabled open inputs can prevent the area from being armed.

  Options for arming using a card reader can be found under **Reader arming mode** in **Expanders | Reader expanders | Reader 1/2**.

- **Disable exit output on stay arming**: When this option is enabled the **Exit delay output / output group** (**Outputs** tab) will not be activated when the area is stay armed. This is useful when there is no need to prompt users to leave the stay armed area.
- **Clear alarm memory after arming**: When this option is enabled (by default) the area's alarm memory is cleared every time the area is armed. When it is disabled alarms will remain in the alarm memory until a user acknowledges them at a keypad (**[MENU] [5] [1]**).
- **Enable late arm report**: When this option is enabled the system will generate a report for the monitoring station and event log whenever the area is armed later than expected. The report is generated if the area is still disarmed when the **Normal arm schedule** set below becomes invalid. This ensures that operators and monitoring stations are alerted to any anomalies.
- **Enable early disarm report**: When this option is enabled the system will generate a report for the monitoring station and event log whenever the area is disarmed earlier than expected. The report is generated if the area is disarmed before the **Normal disarm schedule** set below becomes valid. This ensures that operators and monitoring stations are alerted to any anomalies.

- **Disable rearm on schedule**: When this option is enabled, automatic rearming will be disabled when the area has been disarmed by the **Arm/Disarm schedule** (**Configuration** tab). Use this to ensure the area does not automatically rearm when it is supposed to be disarmed.

  The command `ReArmLevelTrigger = true` prevents the area from automatically rearming while the schedule is valid, regardless of how the area was disarmed.

- **User rearm in stay mode**: With this option enabled, when certain users disarm the area it will automatically rearm in stay mode after a period of time. Users must have the **Rearm area in stay mode** option enabled in **Users | Users | Options**. The area will remain disarmed for the length of time specified in the **Rearm time** setting (**Configuration** tab).

  This option is useful for allowing users to enter the building to temporarily disarm the area and remain inside while the perimeter is secured again.

  Stay arming must be enabled (above).

### Squawk options

Squawk operation is not supported on the controller's onboard reader expander outputs.

- **Bell squawk on arming start**: When this option is enabled the area's **Bell output** (**Outputs** tab) will squawk (sound briefly) when the area begins arming.
- **Bell squawk on arming complete**: When this option is enabled the area's **Bell output** (**Outputs** tab) will squawk (sound briefly) when the area successfully finishes arming.
- **Bell squawk only when unattended**: With this option enabled the bell output will only squawk when the area is armed or disarmed by an unattended method such as schedule, automated rearming or programmable function. It will not squawk when armed or disarmed from the keypad or card reader.

  One or more of the other **Squawk options** must also be enabled.

- **Bell squawk on disarm**: When this option is enabled the area's **Bell output** (**Outputs** tab) will squawk twice when the area is disarmed.
- **Bell squawk on successful report**: When this option is enabled the area's **Bell output** (**Outputs** tab) will squawk when a successful 'Area Armed' report has been sent and acknowledged by the reporting service.

### Schedule

- **Normal disarm schedule**: This schedule defines when the area is expected to be disarmed on any given day. Along with **Enable early disarm report** above this allows you to generate reports if the area is disarmed earlier than expected.

  For example, you might set the normal disarm schedule to 8:30-9:30am every weekday. This represents when you expect the area to be disarmed for the first time. If the area is disarmed at 7:00am (before this schedule becomes valid) an event will indicate that the area is 'Early to Disarm'.

- **Normal arm schedule**: This schedule defines when the area is expected to be armed on any given day. Along with **Enable late arm report** above this allows you to generate reports if the area is armed later than expected.

  For example, you might set the normal arm schedule to 4:30-5:30pm every weekday. This represents when you expect the area to be armed for the last time. If the area is still disarmed at 5:30pm (when the schedule becomes invalid) an event will indicate that the area is 'Late to Arm'.

## Area Manual Commands

Right clicking an area record in **Programming | Areas** or an area icon on a floor plan or status page opens a menu with manual commands for that area.

## Disarm

- **Disarm**: Disarms the main portion of the area. This disables supervision of inputs in the area.
- **Disarm 24 hrs**: Disarms the 24hr portion of the area. This disables tamper and trouble input monitoring in the area.

## Arm

- **Arm**: Arms both the main and the 24hr portions of the area. First the system tests all of the inputs in the area. If any are open or tampered they must be bypassed before the area will begin arming. Then the area's exit delay begins. When exit delay is complete the area reports a successful arming to the monitoring station and in the event log.

  Bypassed inputs are not monitored by the armed area.

- **Force arm**: Force arms the main portion of the area. An area can be force armed without bypassing any open inputs. These inputs will still be monitored by the force armed area.

  Force arming must be enabled in the **Options (2)** tab. Inputs cannot be force armed if the **Force input** option is disabled in the input type (**Programming | Input types | Options (1)**).

- **Arm stay**: Stay arms the main portion of the area. A stay armed area will monitor certain inputs ('stay inputs') but ignore others.

  Stay arming must be enabled in the **Options (2)** tab. Only inputs with the **Stay input** option enabled in the input type (**Programming | Input types | Options (1)**) will be monitored when the area is stay armed.

- **Arm instant**: Instant arms the main portion of the area. When an area is instant armed the exit delay time is reduced to 1 second. Also, all inputs that would normally initiate the entry delay instead trigger the alarm immediately (i.e. all inputs are treated as 'instant' inputs).

  Instant arming must be enabled in the **Options (2)** tab.

- **Force arm instant**: Force arms the main portion of the area with a one second exit delay. All inputs that would normally initiate the entry delay instead trigger the alarm immediately (i.e. all inputs are treated as 'instant' inputs).

  Force arming and instant arming must be enabled in the **Options (2)** tab.

- **Arm 24 hrs**: Arms the 24hr portion of the area to allow monitoring and reporting on tamper conditions and trouble inputs. There is no testing or exit delay.
- **Walk test enable**: Arms the area in walk test mode, which is used to test input function. During a walk test the inputs in the area do not generate any alarms and central station monitoring is suspended for the area. One event will be logged for each input activation (even if the input is activated multiple times). When the walk test ends an event will be logged for each input that was not activated.

  Arming of the area in walk test mode is not reported to the monitoring station.

- **Walk test disable**: Disarms the area to end the walk test. This is not reported to the monitoring station.
- **Silence alarm**: If the alarm is currently active, this command silences the alarm. This deactivates the **Bell output** and **Alarm memory output**. The area will remain armed.

# Outputs

Outputs generally represent physical devices connected to the Protege GX system, such as sirens, beepers, LED indicators and door lock relays. Any device that has a binary on-off state can be connected to Protege GX as an output. This means Protege GX can be used to control a wide range of devices, from lighting to HVAC.

However, outputs do not need to be physical: Protege GX can use virtual outputs to track binary states without the need for a physical device. This allows for advanced programming using schedules, input types, automations and programmable functions.

## Outputs | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.

### Address

- **Module type**: The type of module that the output is connected to (e.g. keypad, output expander).
- **Module address**: The **Physical address** of the module that the output is connected to.
- **Module output**: The index of the output on the connected module. See the relevant module installation manual for wiring instructions.

### Configuration

- **Activation schedule**: This schedule is used to automatically turn the output on and off. When the schedule becomes valid the output is activated. When the schedule becomes invalid the output is deactivated.

  By default, the activation schedule only controls the output when the schedule changes state (becomes valid or invalid). The output can still be controlled by other methods between these times. To ensure the output remains in the scheduled state enable **Always verify schedule** below.
- **Always verify schedule**: With this option enabled the output will verify the schedule every minute. If the output is not in the correct state it will be activated or deactivated to match the state of the schedule.
- **Activation time**: The duration (in seconds) that the output will stay on when it is activated. This applies to most methods of activation (e.g. manual activation, activation schedule, programmable function, automation). The output status will be shown as 'On Timed' on a status page.

  If the activation time is set to 0 the output will remain on continuously until it is deactivated by any method.

  Some methods of output activation (e.g. output group, input type, access level) have specific times which may override the activation time.
- **Activation retrigger**: With this option enabled, if an output is activated a second time when it is already 'On Timed' the activation time will restart. This allows outputs such as lights to stay on for longer when they are retriggered.
- **Support manual commands**: When this option is enabled, an operator with the appropriate permissions can send manual commands to the output. For example, an operator might right click on a lighting output on a floor plan to turn on the lights.

  For more information, see Manual Output Commands (page 244).

### Elevator HLI

This section is only relevant for the Schindler HLI Integration. For more information, see Application Note 196: Protege GX Schindler HLI Integration.

- **Output used for elevator HLI**: With this option enabled the output can be configured for use with elevator HLI. This should typically be used with virtual outputs.
- **Controller**: The controller used for Schindler integration.
- **Elevator HLI type**: Indicates the type of elevator HLI set at the controller (read only).
- **SOM activation mode**: This setting allows Protege GX outputs (typically virtual outputs) to activate Schindler Special Operating Modes (SOMs). These can be used for functions such as sending an express elevator or releasing trapped passengers.

  This field determines when the SOM will be controlled: either when the output turns on, when it turns off, or whenever it changes state. If you are using a single output to activate and deactivate an SOM, select the On change option.

  The name of the SOM to be activated should be set as the **Keypad display name** for the output.
- **Append output state to SOM message**: When this option is selected the state of the output is added to the end of the SOM message. Enable this option if the **SOM activation mode** above is set to On change.
- **SOM primary terminal ID**: The Schindler Terminal ID that the messages will be sent to when the controller is communicating via the primary IP address for the Schindler server.
- **SOM secondary terminal ID**: The Schindler Terminal ID that the messages will be sent to when the controller is communicating via the secondary IP address for the Schindler server.

### Commands

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

### Graphics

- **Floor plan**: Associating a floor plan with an output allows you to right click on any output event in an event window to open the floor plan.
- **Camera**: Associating a camera with an output allows you to right click on any output event in an event window to open an archived camera feed from the time of the event.

### Record history

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

## Outputs | Options

### General

- **Log output events**: When this option is enabled the output will generate an event whenever it is activated or deactivated. Disable this option to prevent output events from being generated.

  You may disable event logging for outputs that are primarily used for automation or control (such as virtual outputs) to reduce their impact on event storage.
- **Invert output**: When this option is enabled the output activation will be inverted. For example, if a light output is inverted deactivating the output will turn the light on and activating the output will turn the light off.

  A module update will be required whenever this setting is changed.

  If the output is on the controller the option must be enabled in both the controller output and the corresponding output on the onboard reader expander. Then it must be manually activated and deactivated before this change will take effect.

### Preset state

- **Preset controller power up**: With this option enabled the output will be set to a specific state when the controller is restarted or powered on for the first time. If not, the output will be reset to its last known state.
- **Output turns on when controller powers up**: This option defines the initial state of the output when the controller powers up. With this option enabled the output turns on. With this option disabled the output turns off.
- **Preset module power up**: With this option enabled the output will be set to a specific state when the module it is connected to is powered up. This will override the last known state of the output and the **Preset controller power up** setting above.

  A module update will be required whenever this setting is changed.

- **Output turns on when module powers up**: This option defines the initial state of the output when the connected module powers up. With this option enabled the output turns on. With this option disabled the output turns off.
- **Preset module offline**: With this option enabled the output will be set to a specific state when the connected module goes offline. For example, this could be used to turn on an indicator light or beeper when a module goes offline, or ensure that emergency lighting turns on if a connection is damaged.

  A module update will be required whenever this setting is changed.

- **Output turns on when module offline**: This option defines the state of the output when the connected module goes offline. With this option enabled the output turns on. With this option disabled the output turns off.

## Manual Output Commands

Right clicking an output record in **Programming | Outputs** or an output icon on a floor plan or status page opens a menu with manual commands for that area.

### Control

- **Activate**
- **Deactivate**
- **Activate timed** (activate the output for the time entered in the field below)

# Trouble inputs

Trouble inputs are used to monitor the status and condition of the system. Like physical inputs, trouble inputs have a binary on-off state; however, they represent system troubles such as power failures, communications faults, tampers and other issues.

Trouble inputs can be programmed into areas with specific input types so that they are monitored by the system and reported to the monitoring station. Unlike regular inputs, trouble inputs generate 24hr / tamper alarms when they are opened, instead of regular alarms. Typically they are programmed into a dedicated 'system area' that always has its 24hr portion enabled, using the preconfigured Trouble Silent and Trouble Bell input types (see page 221).

Each module type has its own specific trouble inputs, which are added automatically when that module record is added to the system. The **Module input** of each trouble input corresponds to a particular system trouble for that module, such as power supply failure or module tamper. Doors also have dedicated trouble inputs for door left open, door duress and door forced conditions.

See the Trouble Inputs section of the relevant installation manual for a full list for each module.

## Trouble inputs | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.

### Address

- **Module type**: The type of device that the trouble input is associated with (e.g. controller, reader expander, door).
- **Module address**: The **Physical address** of the module or name of the door that the trouble input is associated with.
- **Module input**: The index of the trouble input on the associated module. This determines what system trouble the trouble input monitors and the event code that is sent to the monitoring station when this trouble input generates an alarm. For example, trouble input 3 on an analog expander opens when there is a 'Battery Low / Missing' condition, and sends an event code of 302.

  See the Trouble Inputs section of the relevant installation manual for a full list for each module.

### Configuration

- **Trouble group**: The trouble groups and associated **Trouble group options** below determine how trouble conditions will be displayed on the keypad. Setting these fields will allow this trouble input to be displayed on the keypad in the Installer View menu, which is useful for technicians checking the system for issues. In addition, a custom message based on the selected trouble group option will be displayed in the Trouble View menu, and if enabled on the keypad, also in the Offline Trouble View menu.

  There is typically no need to edit the trouble groups as they are automatically set for each trouble input.

  The available trouble groups are as follows:

- **0 - None**: This trouble input does not fall under any of the categories below and will not be displayed on the keypad. This option is used for trouble inputs that technicians on site do not need to be aware of (e.g. 'Installer Logged In').
- **1 - General**: This trouble group consists of troubles that are relevant to the general operation of the system. This includes conditions such as AC failure, reporting issues and input faults.
- **2 - System**: This trouble group is used for module related troubles (e.g. module tamper).
- **3 - Access**: This trouble group is used for troubles that are related to access control and door operation (e.g. forced door, too many access attempts).

Users can access the Trouble View menu by logging in to a keypad and pressing **[MENU] [5] [2]**, and the Installer View menu by pressing **[MENU] [4] [1] [2]**. Here they can view the current system troubles.

If enabled on the keypad (**Expanders | Keypads | Options 2**), the Offline Trouble View menu can be accessed by pressing **[MENU] [2]**, without logging in to the keypad.

These fields do not affect the event codes used for reporting.

- **Trouble group options**: The trouble group option determines what message will be displayed on keypads when this trouble input is open. Each option that can be selected has one or more variants, depending on the **Trouble group** selected above. If the trouble group is set to 1 the first entry in each option will be used, and so on.

  There is typically no need to edit the trouble group options as they are automatically set for each trouble input.

- **Reporting ID**: The trouble input's reporting ID is the **Zone ID** index which will represent that trouble input to the monitoring station. You can manually assign an ID to each input, allowing a high amount of flexibility in input reporting. For example, if two inputs have the same Reporting ID they will both report as the same input.

  Every trouble input must have a reporting ID assigned, so each newly created trouble input will be automatically assigned the lowest available ID. If a trouble input has been assigned a number higher than the maximum that can be reported to a particular service the highest possible number will be reported.

  You can view and export Reporting IDs using the **Report map generator** (**Reports | Central station report**). Inputs and trouble inputs share the same range of Zone IDs but trouble inputs typically use higher indexes.

### Graphics

- **Floor plan**: Associating a floor plan with a trouble input allows you to right click on any trouble input event in an event window to open the floor plan.

### Commands

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

### Record history

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

## Trouble inputs | Areas and input types

Like inputs, trouble inputs can be assigned to up to four areas, with a separate input type programmed in each. The input type defines how the trouble input will function in that area.

Trouble inputs are used in system areas to generate 24hr alarms (using the preconfigured Trouble Silent and Trouble Bell input types).

### Assigned areas

- **Area 1-4**: Each trouble input can be programmed into up to four different areas. Typically trouble inputs are assigned to a 'system area' which is used to monitor system troubles.
- **Input type 1-4**: The input type defines how the trouble input will operate in that particular area. For example, the Trouble Silent input type will allow the trouble input to generate 24hr / tamper alarms without activating the area's bell output, while the Trouble Bell input type will cause the bell output to be activated.

## Trouble inputs | Options

### General options

- **Log to event buffer**: When this option is enabled (by default) the trouble input will generate an event whenever it is opened or closed. Disable this option to prevent trouble input events from being generated, reducing their impact on event storage. Reports will still be sent to the monitoring station.
- **Bypassing not allowed**: It is possible to bypass trouble inputs from the keypad, but the bypass can only be removed by power cycling the controller. Therefore, it is recommended that you disable bypassing for trouble inputs.
- **Latch bypassing not allowed**: It is possible to bypass trouble inputs from the keypad, but the bypass can only be removed by power cycling the controller. Therefore, it is recommended that you disable bypassing for trouble inputs.

### Advanced options

- **No bypass if any area armed**: It is possible to bypass trouble inputs from the keypad, but the bypass can only be removed by power cycling the controller. Therefore, it is recommended that you disable bypassing for trouble inputs.

# Elevator cars

Elevator car records are used for low level elevator control, which enables the system to control and monitor user access to floors in a multi-story building. When a user badges their card at the associated reader the elevator car briefly unlocks the floors that they have access to. Elevator cars can also be wired for destination reporting, allowing Protege GX to monitor exactly which floor the user has selected.

Elevator cars can be added to status pages and floor plans, where they will display the status of available floors and allow basic manual control.

For information and programming instructions for low level elevator control and destination reporting, see Application Note 248: Low Level Elevator Control in Protege GX and Protege WX. Elevator car records are also used in some Elevator HLI Integrations. See the relevant application note.

## Elevator cars | General

### General

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

### Configuration

- **Reader expander**: Elevator cars must be associated with the reader expander that is used to control user access in that car.

  The **Reader 1/2 mode** and **Reader 1/2 elevator** must also be set correctly for that reader expander (**Expanders | Reader expanders | Reader 1/2**).

- **Reader port**: The reader expander port that controls access in this elevator car.
- **Unlock access time**: The length of time (in seconds) that the floor outputs will be activated when a user is granted access. When destination reporting is not enabled the user will have this length of time to select a floor. When destination reporting is enabled the selected floor will be activated for this length of time.
- **Unlock intercom time**: The length of time (in seconds) that a floor will be unlocked when it is triggered by an intercom service. Once access has been granted at the intercom the user will have this length of time to enter the elevator car and select a floor.

  For more information on programming the intercom and elevator integration, see the Protege Vandal Resistant Touchscreen Entry Station Installation Manual.

- **Floor select time**: When destination reporting is enabled the user has this time (in seconds) to press a floor button after they are granted access. This option is not required when destination reporting is not enabled.
- **Destination reporting enable**: Destination reporting allows the system to track which floor a user has selected. When a user is granted access, instead of immediately unlocking all floors the system will wait for an input activation. The user can select a single floor that they have access to, and only that floor will be unlocked. In addition, an event will be logged recording the specific floor the user has selected.

  This is useful for higher security situations where it may be important to know specifically which floors users are traveling to. It also prevents users pressing multiple floor buttons after gaining access.

  Destination reporting has specific wiring requirements which are different from those for basic elevator control.

- **Authentication mode**: The type of credential required to gain access to this elevator car (card, card and PIN, card or PIN, PIN only). If this is left as <not set> the elevator car will use the card operation.

  Elevator cars can use custom credential types when the **Authentication mode** is set to <not set>. The **Reader 1/2 format** in **Expanders | Reader expanders | Reader 1/2** must be set to Custom credential. In this authentication mode, the reader port will match card data against this first programmed credential type with a compatible bit length.

### Commands

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

### Record history

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

## Elevator cars | Schedules and areas

This tab allows you to add the floors that are accessible from this elevator car, and configure how that floor will operate. Floors can be programmed in **Programming | Floors**.

### Floors

Click **Add** to add a new floor to the elevator car, and set the following:

- **Schedule**: This field sets an unlock schedule for the floor. When this schedule is valid the floor can be accessed freely from this elevator car without credentials. When the schedule is invalid credentials are required to access the floor.

  By default, the unlock schedule only controls the floor when the schedule changes state (becomes valid or invalid). The floor can still be controlled by other methods between these times. To ensure the floor remains in the scheduled state enable **Schedule verify**.
- **Area**: This field sets the inside area for this floor (i.e. the area that users enter when they disembark from the elevator car). The inside area must be set to allow integration of area control with elevator access using the **Follow area status** and **Enable area control** options.
- **Late to open**: With this option enabled, when the **Schedule** becomes valid the floor will not unlock until a user has successfully gained access. This prevents floors from unlocking on schedule on days when no one arrives.

  This feature requires destination reporting.
- **Schedule verify**: With this option enabled the floor state will be checked every minute and updated to match the schedule. If the schedule is valid the floor will be unlocked. If the schedule is invalid the floor will be locked.
- **Follow area status**: When this option is enabled the floor will follow the status of the assigned **Area**. If the area is armed the floor will lock. If the area is disarmed the floor will unlock.
- **Input**: The input set here corresponds to the floor select button in the elevator car. This is a required setting for destination reporting. This field is not required if destination reporting is not in use.
- **Output**: The relay output set here corresponds to the floor select button in the elevator car. One output is required per controlled floor in every elevator car, but not for uncontrolled floors (always unlocked). This is required configuration for both basic control and destination reporting.
- **Enable area control**: When this option is enabled the **Area** for this floor will be automatically disarmed whenever a user with sufficient permissions is granted access. In addition, if the area is armed and the user does not have sufficient permissions to disarm it the user will be denied access.

  This feature requires destination reporting.

# Manual Elevator Car (Floor) Commands

When an elevator car has been added to a status page or floor plan the floors that can be accessed from that elevator car are displayed. Right clicking on a floor icon opens a menu with manual commands for that floor.

## Control

- **Activate** (latch unlock the floor until it is locked again)
- **Deactivate** (lock the floor)
- **Activate timed** (unlock the floor for the time set in the field below)

Manual commands only affect access to the floor via that specific elevator car. For example, if you unlock the floor with a command it may be freely accessible from one elevator car, but not from others.

# Floors

Floor records represent a physical floor on site. In low level elevator integration they are applied to the elevator cars that can access them (see page 249). Floors are also used in elevator HLI integrations.

For more information, see Application Note 248: Low Level Elevator Control in Protege GX and Protege WX or the relevant elevator HLI application note.

## Floors | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Floor relay**: The floor relay represents the level of the floor as programmed in the system. Floor relays must be unique, programmed in numerical order (starting at 1), and start at the lowest accessible floor, including any basement floors. Rear elevator doors should be programmed with floor relays starting from 65.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

### Elevator HLI options

For more information, see Application Note 196: Protege GX Schindler HLI Integration.

- **Schindler schedule valid time pattern**: Defines the message that is sent to the Schindler Call Interface when the schedule assigned to the floor becomes valid.
- **Schindler schedule invalid time pattern**: Defines the message that is sent to the Schindler Call Interface when the schedule assigned to the floor becomes invalid.
- **Schindler primary terminal ID**: Defines the ID of the Schindler terminal that the schedule valid/invalid message is sent to when the controller is communicating via the primary IP address.
- **Schindler secondary terminal ID**: Defines the ID of the Schindler terminal that the schedule valid/invalid message is sent to when the controller is communicating via the secondary IP address.

### Commands

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

### Record history

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

# Daylight savings

Daylight savings records are associated with a controller and instruct it to modify its **Field time** when local daylight savings starts or ends. This is necessary to ensure that the controller time is updated correctly for its time zone.

When you program and save a daylight savings record, if it is currently daylight savings time the controller's time will adjust automatically. You should check that the controller's time is set correctly.

- If the controller time is set manually you can check the current time by right clicking on the record in **Sites | Controllers**. To update the time click **Set controller date time**.
- When using a time server the time provided is always in UTC (Coordinated Universal Time), which has no time zone and is not subject to any daylight saving time rules. This means that you must correctly configure the time server, the time zone that the controller is operating in, and the daylight savings settings for the time to be synchronized correctly. Failure to configure any of these will result in the time being inaccurate. Check the time server settings in the **Sites | Controllers | Time update** tab.

Once this is done the controller's time will automatically adjust for daylight savings time.

For a demonstration, see Configuring Daylight Savings in Protege GX on the ICT YouTube channel.

## Daylight savings | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Start day**: The day when daylight savings begins, i.e. the clock rolls forward one hour. This is based on a day of the week (e.g. the first Sunday).
- **Start month**: The month when daylight savings begins.
- **End day**: The day when daylight savings ends, i.e. the clock rolls back one hour. This is based on a day of the week (e.g. the first Sunday).
- **End month**: The month when daylight savings ends.

### Record history

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

## Daylight savings | Options

### Options

- **Apply to all controllers**: By default, each daylight savings record only applies to a single controller (selected in the toolbar). With this option enabled the record will apply to all controllers in this site.

# Phone numbers

Phone number records can be assigned to reporting services that communicate using a telephone connection. Programming these as separate records makes it easy to update if the phone number changes, and allows you to set up a secondary phone number that can be used for after hours calls.

Phone numbers are only used by controller models with inbuilt modem dialers.

## Phone numbers | General

### General

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

### Configuration

- **Operating schedule**: This schedule determines when this phone number can be called. When the schedule is valid the phone number set in this record will be called. When the schedule is invalid the secondary phone number will be called. This allows you to set an alternative phone number to call after hours.
- **Secondary phone number**: This phone number record will be used when the **Operating schedule** is invalid. The operating schedule of the secondary phone number must be valid.
- **Phone number**: The telephone number that will be used by this record.

### Record history

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

# Services

Services mediate interactions between Protege GX and external systems such as reporting stations, automation controllers and intercoms. They allow Protege GX controllers to communicate directly with other systems via ethernet, USB ethernet or the onboard modem dialer.

Once you have programmed a service you can start or stop the service by right clicking on the record. If you edit and save the service record the service will automatically stop and start again to implement the changes.

Services may require the use of onboard hardware devices or expansion devices. Not all controller models support all connection channels, so consult the documentation for your controller model before programming services.

## Setting up Reporting Services

Some service types are reporting services which send reports to offsite monitoring stations either over a phone line or via the IP network. The three types of reporting service are:

- Contact ID (see page 256)
- SIA (see page 261)
- Report IP (see page 267)

When a reporting service is added to an area it can send reports relating to area arming/disarming and events for inputs and trouble inputs programmed in that area. The following steps briefly describe how to create a reporting service and begin reporting on an area.

For a demonstration, see Configuring Offsite Monitoring in Protege GX on the ICT YouTube channel.

1. In **Programming | Services** select the **Controller** which will use this reporting service.
2. Add a new reporting service with a **Service type** of ContactID, SIA or Report IP.
3. Configure the communication settings required to send reports to the monitoring station, such as the **Client code** and any phone numbers or IP channels.
4. Select which event types this service will report (open, close, alarm, tamper, restore and/or bypass) in the **Options** tab.
5. For Report IP services add and configure a **Backup service** if required. This allows the controller to report over an alternate IP connection or phone line if the connection fails.
6. **Save** the service.
7. Navigate to **Programming | Areas** and select the area(s) which will be monitored by this service.
8. In the **Configuration** tab, scroll down to the **Reporting services** section and click **Add**.
9. Select the new reporting service and click **OK**. **Save** the area(s).
10. You may be required to provide a central station report to your monitoring station so they can identify the areas, inputs and users in the reports. For more information, see Central Station Report (page 172).
11. Return to **Programming | Services**. Right click on the new service and click **Start**.

Now the reporting service can report the selected event types for those specific areas to the monitoring station.

## Services | Service Type

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.

- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

## Type

- **Service type**: The service type determines which kind of operation or communication this service will perform. Different programming tabs will be available depending on which service type is selected. The following options are available:
  - **ContactID** (phone line reporting service)
  - **Serial printer** (event sending service)
  - **SIA** (phone line reporting service)
  - **Automation and control** (integration service)
  - **Modbus** (integration service)
  - **C-Bus** (integration service)
  - **Report IP** (IP reporting service)
  - **Intercom** (integration service)
  - **Link me** (cross controller communication service)
  - **VizIP** (integration service)
- **Service mode**: Determines how the service will start. The 0 - Manual mode setting ensures that the service will only start by manual command from an operator (right clicking on the record). The 1 - Start with controller OS setting configures the service to start automatically when the controller boots up.

## Commands

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

## Record history

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

# Contact ID

This reporting service sends alarms, tests and other events to a monitoring station over a phone line using the controller's onboard modem dialer. Reports are sent in the standard Ademco Contact ID format.

Phone line reporting is only available for controller models with onboard modem dialers.

For more on the Contact ID format see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.

## Contact ID | General

Phone numbers can be programmed in **Programming | Phone numbers**.

- **Client code**: This code represents the controller or site in reports to the central monitoring station. This is typically a hexadecimal number with 4 digits but the format may depend on the receiver compatibility. This will be issued by the monitoring station.

  Client codes can also be set for individual areas in **Programming | Areas | Configuration**.

- **PABX number**: If the controller is connected to an internal phone network it will first dial this number to gain an external phone line. If the PABX number is disabled by an **Operating schedule** (**Programming | Phone numbers | General**) the external number will be dialed immediately.
- **Phone number 1**: The primary phone number for the monitoring station. The controller will dial this number first to report events.
- **Phone number 2**: This phone number is used when the controller cannot make a connection with either **Phone number 1** or the **Phone backup**.
- **Phone backup**: This phone number is used when the controller cannot make a connection with **Phone number 1**. The sequence of dialing attempts depends on whether **Use alternate dialing method** is enabled in the **Options** tab.

## Contact ID | Options

- **Use alternate dialing method**: This option determines the order in which the service will try the various phone numbers programmed in the **General** tab if **Phone number 1** fails.

  The options are:

  - **Sequential** (this option disabled): When **Phone number 1** fails the service continues to try this phone number until it reaches the maximum **Dial attempts** (**General** tab). If all attempts fail the service repeats this process with the **Phone backup**, then with **Phone number 2**.
  - **Alternate** (this option enabled): When **Phone number 1** fails the services tries the **Phone backup** once, then tries **Phone number 1** again, then repeats in an alternating fashion. When both numbers have reached the maximum **Dial attempts** the service tries **Phone number 2** until it also reaches the maximum number of attempts.

  When all numbers have reached the maximum dial attempts the Reporting Failure trouble input is opened.
- **Pause after PABX**: When this option is enabled the dialer will insert a pause of 2.5 seconds after dialing the PABX number.
- **Report open**: When this option is enabled the service will report disarming (opening) for all areas using this service.
- **Report close**: When this option is enabled the service will report arming (closing) for all areas using this service.
- **Report alarms**: When this option is enabled the service will report input alarms.
- **Report tampers**: When this option is enabled the service will report input tampers and trouble input alarms.
- **Report restore**: When this option is enabled the service will report input restores.
- **Report bypass**: When this option is enabled the service will report input bypasses.

- **Service operates as backup**: When operating as a backup the service will not begin reporting unless it is initiated by another service that has failed to report. This service will report any messages from the primary service which failed to send, and then return operation to the primary. The backup service starts and stops at the same time as the primary service.

  Only Report IP services have the option to set a **Backup service** (**General** tab).

- **Log modem events to event buffer**: When this option is enabled, detailed events describing the call progression will be saved to the event log for every report. This can be used for troubleshooting issues but should be turned off during normal operation as large numbers of events will be generated.

# Contact ID | Settings

## Settings

- **Cid mapping**: This option is not required for most Contact ID reporting formats. Reporting codes are set in the programming for individual users, inputs, trouble inputs and areas, and can be reset to a specific mapping scheme if necessary when an operator generates the central report map (**Reports | Central station report**). However, when the SIMS II mapping is in use this option must be set to SIMS II.

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

- **Dial attempts**: Determines how many times the controller will attempt to dial each number before moving on to the next backup number. This limit applies even when the report was successful.

  This setting may be overridden by the **Modem country**. For UL/ULC installations (with **Advance UL operation** enabled in **Sites | Controllers | Options**) the controller will not allow values above 8.

- **Port attempts**: Determines how many times the service will attempt to gain access to the onboard modem before reporting a communications failure. This may occur when another service is using the same port for communications.
- **Report count**: Determines how many reports the service can send in each call to the monitoring station. When set to 0, all pending reports can be sent in one call. This is acceptable for most scenarios, but confirm with your central monitoring station.

  When using multiple reporting paths that can report the same event to multiple locations, a limit of 8-16 is recommended. If the limit is reached, the controller will dial out again to send any remaining messages.
- **Handshake time**: The length of time (in seconds) that the controller will wait to receive a handshake message response from the remote receiving unit. This can be adjusted if a longer than normal call completion time is required.
- **Dial time**: The length of time (in seconds) that the controller will wait following a failed reporting attempt before redialing or dialing a backup number. The minimum value is 10 seconds.
- **Off hook output / output group**: This output or output group is activated when the service begins using the modem and is deactivated when the communication is completed. It can be used with remote exchange systems that require ground start communication connections.
- **Report OK output / output group**: This output or output group is activated when the service successfully completes a report. It is not deactivated automatically, and should be programmed with an **Activation time** (**Programming | Outputs**) to ensure that it is turned off between reports.

## Background monitoring

- **Enable background monitoring**: When background monitoring is enabled the service will regularly send polling messages to confirm that the phone lines are operational. This ensures that issues in any of the phone lines (whether primary or backup) are detected.
  - **Background poll time when OK**: Determines how often (in seconds) the controller will check the status of the service when there are no known issues.
  - **Background poll time when known failure**: Determines how often (in seconds) the controller will check the status of the service when there is a known issue.

- **Test report CID code / group / zone**: The Contact ID event code, group number and zone number that the controller will send for the test report.
- **Phone 1 failed CID code / group / zone**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with **Phone number 1**.
- **Phone 2 failed CID code / group / zone**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with **Phone number 2**.
- **Backup phone failed CID code / group / zone**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with the **Backup phone**.

## Version 3 settings

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

# Serial printer

This service enables the controller to send events as ACSII text over an ethernet connection. This can be used for integrated monitoring applications, allowing events to be viewed from another application without use of the Protege GX client software. The service can be programmed to include specific event groups and details.

The serial printer service uses the **Keypad display name** for devices instead of the software name. Records that do not have a keypad display name may not be displayed correctly.

## Serial printer | General

### Configuration

- **Port number**: The port number must be set to TCP/IP for DIN rail controllers.
  The External Comm Port 1-4 options are only used for legacy PCB controllers using the PRT-COMM serial communications interface.
- **Port speed**: The baud rate for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.
- **Parity**: The parity for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.
- **STX**: This byte is appended to the beginning of each message that is transmitted if **Include start of frame (STX) char** is enabled (**Options** tab). The decimal index represents a single ASCII character.
- **ETX**: This byte is appended to the end of each message that is transmitted if **Include end of frame (ETX) char** is enabled (**Options** tab). The decimal index represents a single ASCII character.
- **ACK**: This byte should be sent to the controller to confirm that each sent message has been received correctly. The controller will expect this acknowledgment if **Event requires acknowledge** is enabled (**Options** tab). The decimal index represents a single ASCII character.
- **IP port number**: The TCP/IP port that the service will use to communicate. This is not required if a PRT-COMM module is in use.

### Version 3 settings

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

## Serial printer | Options

### Options

- The following options allow you to select which events will be transmitted by the serial printer service:
  - **System events**
  - **Service events**
  - **Modem events**
  - **User events**
  - **Input events**
  - **Trouble input events**
  - **Output events**
  - **Schedule events**
  - **Area events**
  - **Module events**
  - **Door events**
  - **Elevator events**
  - **Reader events**
  - **Report events**

- **Special events**
- **All controller events**

The events that are included in each category can be viewed in the event filter programming. Navigate to **Events | Event filters | Event types** and click **Add** to view the event types.

- **Display in text format**: When this option is enabled, events will be displayed in text format. When it is disabled only ASCII control characters will be received.
- **Display time**: When this option is enabled the time (hours, minutes and seconds) will be prefixed to each transmitted event.
- **Display day of week**: When this option is enabled the day of the week (in three-letter format) will be prefixed to each transmitted event.
- **Display month**: When this option is enabled the date (in the format dd/mm/yyyy) will be prefixed to each transmitted event.
- **Display milliseconds**: When this option is enabled the milliseconds will be prefixed to each transmitted event. **Display time** must also be enabled.
- **Display raw mode**: This is a legacy option that has no effect.
- **Display raw mode ASCII (off=binary)**: This is a legacy option that has no effect.
- **Not used**: This is a legacy option that has no effect.
- **Event requires acknowledge**: When this option is enabled the controller will expect an acknowledgment packet from the receiving device after each message is successfully received. The controller will resend the message regularly until an acknowledgement is received.

  The expected **ACK** is set in the **General** tab.
- **Include sequence number**: This is a legacy option that has no effect.
- **Print trouble inputs**: This is a legacy option that has no effect.
- **Include byte count**: This is a legacy option that has no effect.
- **Include start of frame (STX) char**: When this option is enabled, a start of frame character (STX) will be prefixed to the event text. The **STX** is set in the **General** tab.
- **Include end of frame (ETX) char**: When this option is enabled, an end of frame character (ETX) will be suffixed to the event text. The **ETX** is set in the **General** tab.

# SIA

This reporting service sends alarms, tests and other events to a monitoring station over a phone line using the controller's onboard modem dialer. Reports are sent in the standard SIA Level 2 format.

Phone line reporting is only available for controller models with onboard modem dialers.

For more on the SIA Level 2 format see Application Note 317: SIA L2 Reporting in Protege GX and Protege WX.

## SIA | General

- **Client code**: This code represents the controller or site in reports to the central monitoring station. This is typically a hexadecimal number with 4 or 6 digits, depending on receiver compatibility. This will be issued by the monitoring station.

  See the additional client code settings in the **Options** tab.

- **PABX number**: If the controller is connected to an internal phone network it will first dial this number to gain an external phone line. If the PABX number is disabled by an **Operating schedule** (**Programming | Phone numbers | General**) the external number will be dialed immediately.
- **Phone number 1**: The primary phone number for the monitoring station. The controller will dial this number first to report events.
- **Phone number 2**: This phone number is used when the controller cannot make a connection with either **Phone number 1** or the **Phone backup**.
- **Phone backup**: This phone number is used when the controller cannot make a connection with **Phone number 1**. The sequence of dialing attempts depends on whether **Use alternate dialing method** is enabled in the **Options** tab.
- **Number of dialing attempts**: Determines how many times the controller will attempt to dial each number before moving on to the next backup number. This limit applies even when the report was successful.

  This setting may be overridden by the **Modem country**. For UL/ULC installations (with **Advance UL operation** enabled in **Sites | Controllers | Options**) the controller will not allow values above 8.

- **Number of port open attempts**: Determines how many times the service will attempt to gain access to the onboard modem before reporting a communications failure. This may occur when another service is using the same port for communications.
- **Remote handshake/connection time**: The length of time (in seconds) that the controller will wait to receive a handshake message response from the remote receiving unit. This can be adjusted if a longer than normal call completion time is required.

  For example, this time may need to be increased when handshakes for lower speed formats must occur before the SIA handshake.
- **Time between redials on message failure**: The length of time (in seconds) that the controller will wait following a failed reporting attempt before redialing or dialing a backup number. The minimum value is 10 seconds.
- **Output / Output group turns on/off when dialer goes on/off hook**: This output or output group is activated when the service begins using the modem and is deactivated when the communication is completed. It can be used with remote exchange systems that require ground start communication connections.
- **Output / Output group turns on when good message is sent**: This output or output group is activated when the service successfully completes a report. It is not deactivated automatically, and should be programmed with an **Activation time** (**Programming | Outputs**) to ensure that it is turned off between reports.

### Version 3 settings

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

## SIA | Options

- **Alternate dialing**: This option determines the order in which the service will try the various phone numbers programmed in the **General** tab if **Phone number 1** fails.

  The options are:

  - **Sequential** (this option disabled): When **Phone number 1** fails the service continues to try this phone number until it reaches the maximum **Dial attempts** (**General** tab). If all attempts fail the service repeats this process with the **Phone backup**, then with **Phone number 2**.
  - **Alternate** (this option enabled): When **Phone number 1** fails the services tries the **Phone backup** once, then tries **Phone number 1** again, then repeats in an alternating fashion. When both numbers have reached the maximum **Dial attempts** the service tries **Phone number 2** until it also reaches the maximum number of attempts.

  When all numbers have reached the maximum dial attempts the Reporting Failure trouble input is opened.
- **Dial DTMF tone**: When this option is enabled the modem will use DTMF (tone) dialing when dialing out to **Phone number 1** (**General** tab). When the option is disabled it will use pulse dialing.
- **Dial DTMF tone 2**: When this option is enabled the modem will use DTMF (tone) dialing when dialing out to **Phone number 2** (**General** tab). When the option is disabled it will use pulse dialing.
- **Report open**: When this option is enabled the service will report disarming (opening) for all areas using this service.
- **Report close**: When this option is enabled the service will report arming (closing) for all areas using this service.
- **Report alarms**: When this option is enabled the service will report input alarms.
- **Report tampers**: When this option is enabled the service will report input tampers and trouble input alarms.
- **Report restore**: When this option is enabled the service will report input restores.
- **Report bypass**: When this option is enabled the service will report input bypasses.
- **Log modem events to event buffer**: When this option is enabled, detailed events describing the call progression will be saved to the event log for every report. This can be used for troubleshooting issues but should be turned off during normal operation as large numbers of events will be generated.
- **Send 4 digits client code**: When this option is enabled the SIA service will send a 4 digit client code instead of the standard 6 digits. This can be used with receivers that do not comply to the full SIA specification or software that cannot accept large point numbers.

  Verify the receiver configuration with the monitoring company prior to setting this option.
- **Area client code will be 6 digits**: SIA Level 2 can accept client codes of either 4 or 6 digits. When this option is enabled, if the **Client code** set for an area (**Programming | Areas | Configuration**) is 4 digits long, it will be extended to 6 digits by adding 00. This option can be overridden by the **Send 4 digits client code** option.

  Verify the receiver configuration with the monitoring company prior to setting this option.
- **Report 5 digit input numbers**: When this option is enabled the SIA service will send input identifiers as 5 digits instead of the standard 4. This allows larger input numbers to be specified.

  The SIA Level 2 format supports 5 digit input codes, but this may not be supported by all receivers.

  Verify the receiver configuration with the monitoring company prior to setting this option.
- **Report user numbers in hexadecimal**: When this option is enabled the SIA service will send the user identifier as a 4 digit hexadecimal number. This option can override the **Report user number in 5 digits** option.

  Verify the receiver configuration with the monitoring company prior to setting this option.
- **Report user number in 5 digits**: When this option is enabled the SIA service will send user identifiers as 5 digits instead of the standard 4. This allows larger user numbers to be specified.

  The SIA Level 2 format supports 5 digit user codes, but this may not be supported by all receivers.

  Verify the receiver configuration with the monitoring company prior to setting this option.

# Automation and control

This integration service provides a generic interface for communication with third-party automation systems (e.g. Control 4, Crestron, AMX, C-Gate, Command Fusion) and other programs. This allows the Protege system to be monitored and controlled externally through custom made applications.

External applications can log in to the Protege controller using a valid user PIN code. Messages are sent and received via the ICT Automation and Control Protocol. For more information, contact ICT.

## Automation and control | General

### Configuration

- **Port number**: The port number must be set to TCP/IP for DIN rail controllers.

  The External Comm Port 1-4 options are only used for legacy PCB controllers using the PRT-COMM serial communications interface.
- **Port speed**: The baud rate for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.
- **Parity**: The parity for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.
- **IP port**: The TCP/IP port that the service will use to communicate. This is not required if a PRT-COMM module is in use.
- **Encryption level**: Sets the encryption type used to encrypt messages from the service. The encryption settings here must match those in the receiving device so that the messages can be decrypted.
- **Encryption key**: If the **Encryption level** is set, this field defines the associated encryption key. The key is any sequence of letters and numbers shared with the receiving device. For 128 bit encryption the key must be 16 characters long; for 192 bit it must be 24 characters; and for 256 bit it must be 32 characters.
- **Checksum type**: Sets the type of checksum that will be appended to the end of each control packet. 8 bit Sum is a simple addition of all previous bytes in the packet. 16 bit CRC is a standard CRC (Cyclic Redundancy Check) based on the CRC-16-CCITT polynomial.

### Options

- **Numbers are big endian**: The default method of sending multi byte numbers is Little Endian (least significant byte first). With this option selected, multi byte numbers will be sent as Big Endian (most significant byte first).
- **Allow status requests when not logged in**: When this option is enabled the external program connected to the service can request and receive status updates (e.g. area status) without logging in. The program cannot send control commands (e.g. disarming the area) without logging in with a valid user PIN.
- **Use logon lock out timer if incorrect PIN is supplied**: When this option is enabled, if an incorrect PIN is supplied three times in a row the service will block further attempts for 60 seconds.
- **ACK commands**: With this option enabled the service will send an acknowledgment (ACK) packet to the external program after it successfully receives a control command.
- **Expect ACK for status monitoring**: With this option enabled the service will expect an acknowledgment (ACK) packet to be returned after it sends a status update. If no ACK is returned within 3 seconds the status update will be resent.
- **Resend status monitoring if not ack after 5 attempts**: If **Expect ACK for status monitoring** is enabled above, this option controls the cut off criteria for unacknowledged status updates.

  When this option is enabled the service will resend each status message until it receives an ACK from the external program. When this option is disabled the service will stop sending a status update if it has not been acknowledged after 5 attempts.
- **Expect ack for events**: With this option enabled the service will expect an acknowledgment (ACK) packet to be returned after it sends an event. If no ack is returned within 3 seconds the event will be resent.
- **Resend events if not ack after 5 attempts**: If **Expect ack for events** is enabled above, this option controls the cut off criteria for unacknowledged events.

When this option is enabled the service will continue sending each event until it receives an ACK from the external program. When this option is disabled the service will stop sending an event if it has not been acknowledged after 5 attempts.

# Modbus

This integration service configures the Protege GX controller to act as a Modbus server, allowing it to receive monitoring and control messages from client systems via the Modbus protocol. This includes standard industrial automation systems such as Citect, Wonderware, The FIX and DAQ Factory.

For more information and programming instructions, see Application Note 023: Protege GX Modbus Server Integration. There is a separate integration which enables the controller to act as a Modbus client - see Application Note 353: Protege GX Modbus Client Integration.

## Modbus | General

### Configuration

- **Port number**: The port number must be set to TCP/IP for DIN rail controllers.
  The External Comm Port 1-4 options are only used for legacy PCB controllers using the PRT-COMM serial communications interface.
- **Port speed**: The baud rate for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.

  The default speed for Modbus applications is 9600.
- **Parity**: The parity for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.

  The default parity for Modbus applications is Even.
- **Client address**: The device address for the module in the Modbus communication network. This should be a unique hexadecimal number which is not 0x00 or 0xFF. The client address is typically provided by the automation company or SCADA system that the controller will be connected to.
- **Poll time**: This field defines the maximum length of time (in seconds) expected between polls from the Modbus client. For example, if the poll time is set to 60 the controller will expect a poll every 60 seconds. If there is no poll an error will be logged in the event log and the **Output / Output group turns on when polling fails** will be activated.
- **Output / Output group turns on when polling fails**: This output or output group is activated when the **Poll time** set above expires with no polling messages received. It is deactivated when the Modbus service completes a valid communication. Use this option to notify users that there is an issue in the Modbus system.

### Options

- **Log communication events**: When this option is enabled, events will be logged for all Modbus communications. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log communication errors**: When this option is enabled, events will be logged for all Modbus communication errors.
- **Integers as big endian**: The default method of sending multi byte numbers is Little Endian (least significant byte first). With this option selected, multi byte numbers will be sent as Big Endian (most significant byte first).
- **Use remote register variables**: This is a legacy option that has no effect.
- **Enable coil input translation**: This is a legacy option that has no effect.

# C-Bus

This integration service communicates with a C-Bus Network Interface (CNI) for automation control.

For more information and programming instructions, see Application Note 289: C-Bus Integration with Protege GX and Protege WX.

## C-Bus | General

### Configuration

- **Port number**: The port number must be set to TCP/IP for DIN rail controllers.
  The External Comm Port 1-4 options are only used for legacy PCB controllers using the PRT-COMM serial communications interface.
- **Port speed**: The baud rate for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.
- **Parity**: The parity for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.
- **CNI IP address**: The IP address of the C-Bus network interface that the controller is communicating with.
- **CNI port**: The IP port used to communicate with the C-Bus network interface. This should be the same port used for communications between the CNI and the C-Bus Toolkit software.
- **Communication failure output / output group**: This output or output group is activated when there is a communication failure with the CNI.

### Options

- **Enable text output**: Enable this option to convert communications from the controller to a human readable format. This allows for debugging if a monitoring device is used in place of the CNI; however, the integration will not function with this option enabled.
- **Add CR to text output**: When **Enable text output** is in use, enabling this option adds a carriage return character onto the end of each message.
- **Add LF to text output**: When **Enable text output** is in use, enabling this option adds a line feed character onto the end of each message.
- **Log C-Bus PCI failure message**: With this option enabled, error events will be logged when the CNI fails to initialize. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log C-Bus ack message**: With this option is enabled, events will be logged for each acknowledgement (ACK) packet received from the CNI. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log C-Bus data activity**: With this option enabled, events will be logged for all packets sent to and received from the CNI. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.

# Report IP

This reporting service sends alarms, tests and other events to a monitoring station over an IP connection. The Report IP service supports a number of formats over UDP and TCP connections, either encrypted or unencrypted, allowing it to send more informative reports more cheaply and securely than traditional phone line reporting.

As well as the onboard ethernet connection, some Protege GX controller models include a USB-ethernet interface which enables you to connect a Protege DIN Rail Cellular Modem to send reporting messages over a 4G cellular network. For more information and configuration instructions, see the Protege DIN Rail Cellular Modem Configuration Guide.

In addition, the Report IP service can be configured to send push notifications to the Protege Mobile App. For more information, see Application Note 201: Protege GX Push Notification Setup.

## Report IP | General

### Configuration

- **Client code**: This code represents the controller or site in reports to the central monitoring station. An account code for Report IP can be up to 8 digits. Any leading zeros will be truncated so that the minimum number of digits possible is sent (e.g. 004311 is shortened to 4311). If the client code is longer than the reporting format allows it will be truncated.
- **Reporting protocol**: The Report IP Service supports a number of reporting formats. This includes versions of traditional formats that can be sent over an IP connection, providing maximum flexibility.
  - **Armor IP**: ArmorIP is a proprietary IP reporting protocol by ICT. Reports are sent to an installed ArmorIP server which provides a standard Ademco 685 output and allows routing and redirection of messages to other receivers. This format provides full textual transmission that includes the names of the records (user, area, input) that generated the report and additional information such as field time and controller name. It also includes standard ContactID codes for automation.

    ArmorIP reporting is available in both UDP and TCP modes, and either encrypted or unencrypted.

    For more information, see the ArmorIP Version 3 Internet Monitoring Application User Manual.
  - **SIA over IP (DC09)**: Communicates in the SIA Level 2 format using the SIA DC09 specification for digital communication.
  - **CID over IP**: Communicates in the Contact ID format using the SIA DC09 specification for digital communication.
  - **CSV IP**: CSV IP is an IP reporting protocol used by Alarm New Zealand. This is a generic ASCII protocol which takes the form: username, password, client code, message. This service sends report messages in Contact ID format.
  - **Patriot LS30**: Patriot LS30 is a proprietary IP reporting protocol by Patriot Systems. This service sends report messages in a variant of the Contact ID format.
- **CSV IP username / password**: The username and password required for the CSV IP protocol.
- **Encryption level**: Sets the encryption type used to encrypt messages from the service. The encryption settings here must match those in the receiving device so that the messages can be decrypted.
- **Encryption key**: If the **Encryption level** is set, this field defines the associated encryption key. The key is any sequence of letters and numbers shared with the receiving device. For 128 bit encryption the key must be 16 characters long; for 192 bit it must be 24 characters; and for 256 bit it must be 32 characters.
- **Poll time**: The time (in seconds) between polling messages sent from the controller to the receiving server. The polling message format depends on the **Reporting protocol** set above.

  Ensure that the same poll time is set at both the controller and the receiver.
- **Backup service**: The backup service will be used when the Report IP service suffers a communication loss. It is useful to select a service that connects over the phone line to ensure that reports can be sent over an alternative connection when there is a cable failure or internet outage.

The service selected here must have **Service operates as backup** enabled in the **Options** tab.

- **CID map settings**: This option is not required for most Contact ID reporting formats. Reporting codes are set in the programming for individual users, inputs, trouble inputs and areas, and can be reset to a specific mapping scheme if necessary when an operator generates the central report map (**Reports | Central station report**). However, when the SIMS II mapping is in use this option must be set to SIMS II.

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

- **Time before backup**: If a **Backup service** is configured above, this field defines the length of time (in seconds) that the IP connection must be lost before the service will activate the backup.

### Primary / Secondary channel settings

The secondary channel provides a backup path for communication with the monitoring station should the primary channel fail. If the primary channel cannot be used the service will try the secondary channel before starting the backup service.

The two channels should at minimum have different IP addresses and/or port numbers. For higher reliability use two different mediums for internet access, such as both wired and wireless connections.

- **IP address / Host name**: The address of the receiver that messages are sent to.
- **IP port number**: The port used for communication with the receiver. This will depend on the configuration of the receiver software or hardware.
- **Adaptor**: The network adapter on the controller that the Report IP service uses for communication. This should be set to Cable to use the onboard ethernet interface, or USB ethernet to use a cellular modem.

3G reporting is only available with the 3G enabled controller (PRT-CTRL-DIN-3G).

- **Port open attempts**: The number of times the service should attempt to open the communications port before logging a communication failure and switching to the other channel or a backup service. To bypass this setting use the **Switch secondary IP immediately** option (**Options** tab).
- **Ack wait time**: The length of time (in seconds) that the service will wait for an acknowledgement (ACK) packet from the receiver before resending the report.
- **Report fail output / output group**: This output or output group is activated when the service experiences a communication failure. It is deactivated when communication is restored.
- **Enable offline polling**: Offline polling occurs when the service is not normally in use, i.e. operating as a backup. If the backup service loses connection the Reporting Failure trouble input will open and a report will be sent to the monitoring station. This ensures that any issues are detected before the backup service is required.
  - **Channel failed CID code / group / zone**: The Contact ID event code, group number and zone number sent when the offline polling fails.
  - **Offline poll count**: The number of offline polls that must fail before the connection failure is reported.
  - **Offline test report time**: The time between offline polls, in seconds.

### Version 3 settings

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

## Report IP | Options

- **Switch secondary IP immediately**: With this option enabled, when the primary channel fails to connect the service will immediately attempt the secondary channel instead of making multiple attempts to connect over the primary (i.e. the **Port open attempts** setting is ignored).
- **Report open**: When this option is enabled the service will report disarming (opening) for all areas using this service.
- **Report close**: When this option is enabled the service will report arming (closing) for all areas using this service.
- **Report alarms**: When this option is enabled the service will report input alarms.

- **Report tampers**: When this option is enabled the service will report input tampers and trouble input alarms.
- **Report restore**: When this option is enabled the service will report input restores.
- **Report bypass**: When this option is enabled the service will report input bypasses.
- **Log acknowledge response**: When this option is enabled, an event will be logged whenever an acknowledgment (ACK) packet is received from the monitoring receiver. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log polling message**: When this option is enabled, an event will be logged whenever a polling message is sent to the monitoring receiver. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log message retries**: When this option is enabled, an event will be logged whenever the service resends a failed message.
- **Log reporting failure**: When this option is enabled, an event will be logged whenever communications have failed completely and the service is waiting to make another attempt.
- **Service operates as backup**: When operating as a backup the service will not begin reporting unless it is initiated by another service that has failed to report. This service will report any messages from the primary service which failed to send, and then return operation to the primary. The backup service starts and stops at the same time as the primary service.

  Only Report IP services have the option to set a **Backup service** (**General** tab).

# Intercom

This integration service communicates with specific first- and third-party intercoms, allowing users to unlock elevators floors and doors from the intercom.

To integrate with a Protege entry station see the Protege Vandal Resistant Touchscreen Entry Station Installation Manual.

Application Note 143 is available on request for integration with legacy third-party intercoms.

## Intercom | General

### Configuration

- **Port number**: The port number must be set to TCP/IP or UDP/IP for DIN rail controllers.
  The External comm Port 1-4 options are only used for legacy PCB controllers using the PRT-COMM serial communications interface.
- **Port speed**: The baud rate for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.
- **Parity**: The parity for the serial communications, which can be adjusted to match the host configuration. This has no effect when the **Port number** is set to TCP/IP.
- **TCP/IP port**: The TCP/IP port that the service will use to communicate. This is not required if a PRT-COMM module is in use.
- **Intercom type**: The type or brand of intercom this service will communicate with. Intercoms with serial interfaces must be integrated using a suitable serial-ethernet converter, such as a Moxa DE-211 or Moxa DE-311, to allow the Protege GX controller to communicate with the intercom over TCP/IP.

  Legacy PCB controllers can communicate over the serial interface using a PRT-COMM module.

  - **Siedle**
  - **Sentex Infinity multi point**
  - **Sentex Infinity single**
  - **Enterphone** (the Enterphone unit does not support multi units and therefore does not need to have the intercom address set)
  - **SES Intercom** (TEC2 and TEC4 intercoms)
  - **Mesh** (used for integrating MESH intercoms from Viscount and Protege entry stations)
- **Log elevator debug events**: When this option is enabled, events will be generated for each packet received from the intercom. This can be used for diagnosing issues but should be disabled during normal operation to save event storage.
- **Enable intercom 1 address**: By default, the **Elevator Group** set below is used to determine which elevator cars a user can access from the intercom. With this option enabled the elevator group defined in the user's access level will be used instead.
- **Communication timeout**: The maximum idle time between bytes before the communication is considered to time out. This ensures that the controller waits a suitable time for a fragmented data packet from the intercom to be completed. This option has no effect when the **Port number** is set to TCP/IP above.
- **Intercom 1-4 address**: The intercom service can connect to up to four intercoms, each controlling a single door (**Door 1-4** below). If door control is required set the address of the intercom which will control each corresponding door.
- **Identify user type**: When a user requests access to unlock a door or floor from the intercom they must enter an identification number. This allows the controller to validate the request for access against the user's access level and log an accurate event. The type of ID number used can be one of the following:
  - **User index number**: The user's Database ID in the Protege GX system.
  - **User PIN**: The PIN of the user, set in **Users | Users | General**.

  - **User card number**: The card number of the user, set in **Users | Users | General**. The facility number should be set to 0 or the facility number specified in the intercom documentation.
  - **User index offset number**: The user's Database ID added to the **User index offset value** defined below. For example, if the offset is equal to 1 the user must enter their Database ID + 1 at the intercom.
- **Elevator group**: The elevator cars that can be accessed from this intercom. When a user accesses a floor group from the intercom the floors are unlocked in all elevators in the group.
- **Floor group**: The floors that can be accessed from this intercom. When a user enters their ID number at the intercom all floors that are both in this group and in the user's access level will be unlocked.

  For example, if the floor group set here contains all floors in the building but the user only has access to their home floor they can enter their ID at the intercom to unlock their home floor only.
- **Valid intercom request output / output group**: This output or output group is activated when a request from the intercom is received and decoded successfully. It is not deactivated automatically and should be programmed with an **Activation time** (**Programming | Outputs | General**) to ensure that it is turned off between requests.
- **Access granted output / output group**: This output or output group is activated when access is successfully granted to a user via the intercom. It is not deactivated automatically and should be programmed with an **Activation time** (**Programming | Outputs | General**) to ensure that it is turned off between access requests.
- **User index offset value**: When the **Identify User Type** field above is set to User Index Offset Number this field sets the offset number. This is subtracted from the number entered by the user to obtain the database ID.

## Doors

- **Door 1 - 4**: The intercom service can connect to up to four intercoms, each of which controls a door. When a user enters their ID at one of the intercoms the corresponding door is unlocked (provided the user has the correct permissions in their access level).

# Link me

This control service allows you to map outputs between two Protege GX controllers so that outputs on the secondary controller follow the state of those on the primary controller. A Link Me Service must be programmed in both the leading controller and the following controller so that signals can be both sent and received.

This is a legacy feature. A more simple and flexible option for linking two controllers is provided by cross controller operations (see page 24).

## Link me | General

### Configuration

- **Function**: The Link Me Service can either send or receive data. If it is sending data this controller will be the primary that controls the output status. If it is receiving data this controller will be the secondary that follows the primary output status.
- **IP address / Host name**: The address of the other controller that this service is communicating with.
- **IP port number**: The TCP/IP port that the service will use to communicate. The same port must be set in the corresponding Link Me Service programmed in the other controller.
- **Poll time**: The length of time (in seconds) between poll messages sent between the two controllers. Setting a shorter time ensures that the output statuses will remain synchronized.
- **Linked output start**: The first output mapped between the two controllers.
- **Linked output count**: The total number of outputs that will be mapped between the two controllers, including the **Linked output start**. The count begins at the start and counts by database ID until it includes the number of outputs set here.

  Whenever any output in this range changes status the change will be sent to the other controller and the corresponding output will be updated. The count value must be the same in both of the controllers linked by this service so that each output has an equivalent on the other controller.
- **Poll OK output / output group**: This output or output group is activated when communication is successfully established between the two controllers. It is deactivated when communication is lost.
- **Poll failed output / output group**: This output or output group is activated when communication between the two controllers fails. It is deactivated when communication is reestablished.

## Link me | Options

- **Log event acknowledge**: When this option is enabled, events will be generated whenever an acknowledge (ACK) communication packet is received. This is useful for initial configuration but should be disabled during normal operation to save event storage.
- **Log poll accept**: When this option is enabled, events will be generated whenever polling has been accepted by the other controller. This is useful for initial configuration but should be disabled during normal operation to save event storage.
- **Log communication retry**: When this option is enabled, events will be generated whenever the service retries to establish communication after a network failure or loss of service.
- **Log communication failure**: When this option is enabled, events will be generated whenever communication has failed completely and the service is waiting to make another attempt.

# VizIP

This integration service communicates with DVRs over an IP connection using the VizIP protocol. This allows you to map Protege GX outputs to alarm outputs on the DVR, removing the need for physical wiring connections between the DVR and the Protege GX system controller.

## VizIP | VizIP

- **VizIP IP address / Host name**: The address of the DVR which the VizIP Service will connect to.
- **VizIP IP port**: The TCP/IP port which the service will use to communicate with the DVR.
- **VizIP poll time**: The interval (in seconds) between poll messages sent from the controller to the DVR. Setting a shorter time ensures that the output statuses will remain synchronized.
- **Start of out outputs**: The first output mapped between the controller's network and the DVR's alarm outputs.
- **Number of out outputs**: The total number of outputs that will be mapped between the controller's network and the DVR's alarm outputs. The mapping begins at the **Start of out outputs** and increments the output address until it includes the number of outputs set here. Whenever any output in this range changes status, the change will be sent to the DVR and the corresponding alarm output will be updated.

  This number should correspond to the number of alarm outputs on the DVR that will be controlled.

- **Comms fail output / output group**: This output or output group is activated when communication between the controller and DVR fails. It is deactivated when communication is reestablished.
- **Log acknowledge**: When this option is enabled, an event will be generated whenever an acknowledge (ACK) communication packet is received. This is useful for initial configuration but should be disabled during normal operation to save event storage.
- **Log poll OK**: When this option is enabled, an event will be generated whenever a poll message is sent to the DVR. This is useful for initial configuration but should be disabled during normal operation to save event storage.

# Apartments

Apartments in Protege GX enable you to manage access control and intruder detection for individual apartment suites within buildings and condominium complexes. This software feature is used alongside the EliteSuite range of keypads, which is designed for apartment complex management.

You can add a maximum of 248 master EliteSuite keypads per controller. Each master keypad may have a slave network consisting of up to 3 slave keypads and up to 4 Nano Prox or Vario Prox readers (with the use of PRX-SAM units).

The apartments programming menu provides a centralized place to program the settings for each EliteSuite keypad and the devices connected to it. Adding or editing an apartment record automatically creates and updates the associated keypads, inputs, trouble inputs, outputs, areas and users. This is more convenient than programming in the EliteSuite keypad itself.

Records associated with apartments can be viewed in the relevant programming menus, but can only be edited in the apartments programming. To update the programming in the EliteSuite keypad navigate to **Sites | Controllers** and perform a **Force download** command on the controller. Then navigate to **Expanders | Keypads** and perform a **Module update** on the keypad record.

Apartments are a licensed feature. For more information, see Application Note 184: Configuring Apartments in Protege GX. See also the relevant installation and user manuals for the EliteSuite keypad range.

This is a legacy feature. Hardware described above may not be available for purchase.

## Apartments | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Description**: A description of the apartment for the convenience of a building manager or other operator.
- **Address**: The address of the apartment.
- **Phone**: The phone number of a contact for the apartment.
- **Email**: The email address of a contact for the apartment.
- **Challenge question**: A challenge question can be used by the building manager in situations where they need to identify the apartment's master user.
- **Challenge answer**: The answer to the **Challenge question**. The master user is expected to know this answer.
- **Account code**: This code represents the apartment in reports to the central monitoring station. This is typically a hexadecimal number but the format may depend on the receiver compatibility and reporting service in use.

### Record history

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

## Apartments | Options

### Time Options

- **Entry time**: The duration of the area's entry delay, in seconds. If an entry delay input is triggered while the area is armed the area will go into entry delay. If the area is not disarmed before this period elapses the alarm will be activated.

If this time is set to 0 the area will immediately go into alarm, regardless of the input that is activated.

- **Exit time**: The duration of the area's exit delay, in seconds. Whenever the area is armed the exit delay will begin, giving users time to exit the area before it is armed. When the exit delay time elapses the area will be armed. If this time is set to 0 the area will arm immediately.
- **Siren time**: The duration (in minutes) that the bell output will stay on when the area alarm is activated. The minimum alarm time is 1 minute.
- **1k + 1k EOL inputs**: When this option is enabled the inputs connected to this keypad are set to 1K Alarm, 1K Tamper EOL resistor configuration. When this option is disabled the EOL configuration is set to No Resistors.
- **Duplex input mode**: When this option is enabled the keypad can support up to 4 inputs wired in duplex configuration. Additional inputs should be addressed as inputs 3-4 on the keypad.
- **Beep on trouble**: When this option is enabled, if there is a trouble condition in the area the keypad beeper will beep every 2 minutes until the trouble is viewed. Troubles can be viewed by pressing **[MENU] [4]**.
- **Power up disarmed**: With this option enabled, when the EliteSuite keypad powers up the area is disarmed, regardless of the area status when power was lost.

  With this option disabled the behavior depends on the area status when power was lost. If the area was in exit delay or armed the area will begin the exit delay and arm again. If the area was in entry delay or in alarm the area will go into alarm. If the area was disarmed it will remain disarmed.
- **Smoke reset output**: When this option is enabled the EliteSuite keypad's spare output (address 1) can be used to reset the smoke alarm. When the **[CLEAR]** and **[ENTER]** keys are held down together for 2 seconds the output is activated to disable the smoke alarm.

  Enabling this option automatically sets the **Smoke reset output** under the **Keypads | Configuration** tab.
- **Output follows alarm status**: With this option enabled the EliteSuite keypad's spare output (address 1) will be activated when the area goes into alarm and deactivated when the alarm is silenced.
- **Output follows area status**: With this option enabled the EliteSuite keypad's spare output (address 1) will be activated when the area is armed and deactivated when the area is disarmed.
- **Output output inverted**: When this option is enabled the **Output follows alarm status** and **Output follows area status** options will operate in an inverted manner. For example, using **Output follows area status** the output will be deactivated when the area is armed and activated when the area is disarmed.
- **Display not ready message**: With this option enabled the EliteSuite keypad will display messages when there are open inputs. The 'Zone Open' messages are displayed on the home screen and when the user attempts to arm the area.
- **24hr time format**: When this option is enabled the keypad displays the time in 24hr format. When this option is disabled the keypad displays the time in 12hr format.
- **Fast arm allowed**: When this option is enabled a user can arm the area by holding down the **[ARM]** key for 2 seconds. This allows the area to be armed without entering a user PIN.
- **Fast stay arm allowed**: When this option is enabled a user can stay arm the area by holding down the **[STAY]** key for 2 seconds. This allows the area to be stay armed without entering a user PIN.

  When an apartment area is stay armed inputs with the **Input is a stay input** option enabled will not be monitored. This is the opposite behavior to the **Stay input** option in **Programming | Input types | Options (1)**.
- **Fast instant arm allowed**: When this option is enabled the area can be instant armed. This means that the area is stay armed but all inputs that would normally initiate the entry delay instead trigger the alarm immediately (i.e. all inputs are treated as 'instant' inputs).

  A user can instant arm the area by beginning the stay arming process then holding down the **[STAY]** key for 2 seconds while the area is in exit delay. The exit delay will be canceled and the area will instant arm immediately.

  When an apartment area is stay armed inputs with the **Input is a stay input** option enabled will not be monitored. This is the opposite behavior to the **Stay input** option in **Programming | Input types | Options (1)**.
- **Fast force arm allowed**: When this option is enabled a user can force arm the area by holding down the **[FORCE]** key for 2 seconds. This allows the area to be force armed without entering a user PIN.

Only inputs with the **Force arming on input allowed** option enabled in the **Inputs** tab can be force armed.

- **Report arm/disarm**: When this option is enabled the EliteSuite keypad will notify the controller when it is armed or disarmed. Arming and disarming events will be saved to the event log and reported to the monitoring station. This option allows you to view the area status on a status page or floor plan and send manual arm/disarm commands.
- **Report alarm activation**: When this option is enabled the EliteSuite keypad will notify the controller when the alarm is activated, silenced or timed out. Alarm events will be saved to the event log and reported to the monitoring station. This option also allows you to view the area alarm status on a status page or floor plan.
- **Report input bypass**: When this option is enabled the EliteSuite keypad will notify the controller when the area is armed with a bypassed input. Bypass events will be saved to the event log and reported to the monitoring station.

Apartment input status cannot be viewed on a status page or floor plan.

- **Report input tamper**: When this option is enabled the EliteSuite keypad will notify the controller when a connected input has a tamper or short condition. Tamper events will be saved to the event log and reported to the monitoring station.

Apartment input status cannot be viewed on a status page or floor plan.

- **Report master menu access**: When this option is enabled the EliteSuite keypad will notify the controller when any user logs in to the keypad. This event will be saved to the event log.
- **Report installer menu access**: When this option is enabled the EliteSuite keypad will notify the controller when the installer (user 3) logs in to the local installer menu. This event will be saved to the event log.
- **Report advanced information**: When this option is enabled the EliteSuite keypad will notify the controller about extended information, such as device tamper and fire input trouble conditions. These events will be saved to the event log and reported to the monitoring station.
- **1+3 Keys generate panic alarm**: With this option enabled the EliteSuite keypad will generate a panic alarm when the **[1]** and **[3]** keys are held together for 2 seconds. This activates the area alarm and sends an event to the event log and the monitoring station.
- **4+6 Keys generate medical alarm**: With this option enabled the EliteSuite keypad will generate a medical panic alarm when the **[4]** and **[6]** keys are held together for 2 seconds. This activates the area alarm and sends an event to the event log and the monitoring station.
- **7+9 Keys generate fire alarm**: When this option is enabled the EliteSuite keypad will generate a fire alarm when the **[7]** and **[9]** keys are held together for 2 seconds. This activates the alarm and the keypad beeper. The keypad sends an event to the event log and the monitoring station.
- **User eight is duress user**: When this option is enabled the eighth user associated with the apartment (see the **Users** tab) is a duress user. When this user's PIN is entered at a keypad or reader PIN pad they can disarm areas and access menus as normal without activating the alarm, but a duress event will be sent to the event log and the monitoring station.

# Apartments | Keypads

Keypads added here can be viewed, but not edited, under **Expanders | Keypads**.

## General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad address**: The index (network address) of the keypad on the controller network. This must be set to a unique value before the apartment record can be saved.

Valid addresses are 1-248. You can add a maximum of 248 EliteSuite keypads to a single controller with this feature.

### Commands

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

### Configuration

- **Area this LCD belongs to**: This field indicates the area associated with the EliteSuite keypad (read only). The area can be configured in the **Areas** tab.
- **Smoke reset output**: If **Smoke reset output** is enabled (**Options** tab), this field indicates that output 1 on the EliteSuite keypad will be activated when a user resets the smoke alarm from the keypad.

## Apartments | Inputs

The sixteen inputs which can be associated with an EliteSuite keypad are automatically created here. Only inputs 1-4 are configurable within Protege GX: The remaining inputs belong to any connected slave keypads. If all four inputs are physically in use, ensure that the **Duplex input mode** option is enabled in the **Options** tab.

For information on configuring slave keypads, consult the relevant EliteSuite keypad installation manual.

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.

### Address

- **Module type**: Indicates that the input is connected to a keypad (read only).
- **Module address input**: Indicates the **Keypad address** of the keypad this input is connected to (read only).
- **Module input**: Indicates the index of the input on the keypad (read only).

### Configuration

- **Control output / output group**: This option is not supported for apartments.
- **Control automation**: This option is not supported for apartments.
- **Support manual commands**: This option is not supported for apartments.
- **Reporting ID**: The input's reporting ID is the zone number which will represent that input to the monitoring station. This field is read only for apartment inputs.
- **Alarm input speed**: This option is not supported for apartments.
- **Restore input speed**: This option is not supported for apartments.
- **Enable input lockout**: This option is not supported for apartments.
- **Input lockout count**: This option is not supported for apartments.

### Commands

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

### Graphics

- **Camera**: Associating a camera with an input allows you to right click on any input event in an event window to open an archived camera feed from the time of the event.
- **Floor plan**: Associating a floor plan with an input allows you to right click on any input event in an event window to open the floor plan.

### Areas and input types

### First assigned area

- **Area**: The area that monitors this input, i.e. the area associated with the apartment (read only).
- **Input type**: The input type defines how the input will function in that particular area. The input types available for apartment inputs are Delay, Delay follow, Instant, 24 hour alarm, Fire and Fire delay.

### General options

- **Input bypassing enabled**: When this option is enabled the input can be bypassed from the EliteSuite keypad to arm the apartment area. This means the area can be armed even when that input is open or tampered, but the input will not be monitored and will not cause the area to go into alarm.
- **Input is a stay input**: With this option enabled this input will not be monitored when the area is stay armed. With this option disabled this input will be monitored when the area is stay armed.

  To guard the perimeter of the apartment while there are people inside you could enable this option for any internal inputs such as PIRs, and disable it for external inputs such as door and window contacts.

  This option has the opposite behavior to the **Stay input** option in **Programming | Input types | Options (1)**.
- **Force arming on input allowed**: When this option is enabled the area can be force armed when this input is open without bypassing it. The input is monitored and can still generate alarms if closed and opened again.

## Apartments | Areas

Each apartment has one associated area, which can be armed and disarmed from the EliteSuite keypad or from Protege GX.

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

### Graphics

- **Camera**: Associating a camera with an area allows you to right click on any area event in an event window to open an archived camera feed from the time of the event.
- **Floor plan**: Associating a floor plan with an area allows you to right click on any area event in an event window to open the floor plan.

### Configuration

### Setup

- **Child area**: This option is not supported for apartments.
- **Maximum bypass input count**: This option is not supported for apartments.
- **Max user count**: This option is not supported for apartments.
- **Client code**: This code represents the area in reports to the central monitoring station. This is typically a hexadecimal number but the format may depend on the receiver compatibility. If the client code for the area is left at the default value (FFFF) the area will use the **Client code** set in the reporting service (**Programming | Services | General**).

  Typically apartments should have unique reporting codes as tenants may contract security services individually.
- **Interlock area group**: This option is not supported for apartments.
- **Smart input count**: This option is not supported for apartments.
- **Reporting ID**: The area's reporting ID is the group number which will represent that specific area to the monitoring station. In this case there is only one area per apartment so the reporting ID is set to 1 (read only).
- **Lock door group on arming**: This option is not supported for apartments.

### Reporting services

This field allows you to assign the reporting services that will send reports for this area and any inputs or trouble inputs programmed in it.

Services can be programmed in **Programming | Services**.

## Apartments | Users

Each apartment can manage 8 users. These are automatically populated when the apartment is created. By default, user 1 is considered the 'master user' and user 3 the 'installer user'.

Apartment users can arm and disarm the apartment area and access connected card readers, and may also have access to other parts of the Protege GX system (e.g. doors that serve the entire complex).

Apartment users are not visible in the standard **Users | Users** page of Protege GX. However, they are included in the users page of the web client. These records should **not** be edited in the web client, as the options for apartment users are not the same as those for regular users.

### General

- **First name**: The first name of the user.
- **Last name**: The last name of the user.
- **Name**: The display name of the user as it appears on keypads and within the software. This name will not appear on the EliteSuite keypad.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.
- **Default language**: Defines the language that will be used when the user logs in to a keypad. This may be any supported language and is not limited by the Protege GX installation.

Only English is supported on EliteSuite keypads. This option will apply to other keypads in the Protege GX system.

## Card Numbers

- **PIN**: A user's PIN is used to log in to keypads and access doors (via card readers with PIN pads). This PIN can be used both within the EliteSuite network and in the rest of the Protege GX system.

  The maximum number of digits for this PIN is 4. Click the **[4]** button to automatically generate a new PIN of this length. Site security enhancements (e.g. PIN complexity rules in **Global | Sites | Site defaults**) do not apply to apartment users.

- **Facility/Card number**: Each apartment user can be assigned a credential, made up of a facility number (or site number) and an individual card number. This can be used both within the EliteSuite network and in the rest of the Protege GX system.

  Only one credential can be assigned to each apartment user.

  **Note**: The Protege GX database cannot store user facility or card numbers of 2147483648 or above. Events referencing these cards will display no data. This is a known limitation.

## Configuration

- **Reporting ID**: The code which will be used to identify this user in reports to monitoring stations. Contact ID, SIA and Report IP use this code. This field is read only for apartment users.

## General options

- **Code can arm system only**: When this option is enabled this user can arm the apartment area but cannot disarm it. This might be used for contractors or cleaners so they cannot enter without a resident present but can secure the apartment when they leave.
- **User can modify other users**: When this option is enabled this user can access the **User setup** menu on the EliteSuite keypad (by pressing **[MENU] [5]**). This allows them to edit user PINs, card numbers and other options.

  When an operator performs a module update on the EliteSuite keypad any records modified locally will be overwritten. This allows records to be reset if the tenants in the apartment change.

  This option is enabled by default for the 'master user' (user 1).

- **Disarm on single badge enabled**: With this option enabled the user can disarm the apartment area by badging their card once at the entry reader.

  This option only applies to readers connected to the EliteSuite keypad's slave network.

- **Arm on 3 badge enabled**: With this option enabled the user can arm the apartment area by badging their card three times in succession at a reader.

  This option only applies to readers connected to the EliteSuite keypad's slave network.

- **3 badge latch door toggle**: With this option enabled the user can toggle a door between locked and latch unlocked by badging their card three times in succession at the reader.

  This option only applies to readers connected to the EliteSuite keypad's slave network.

- **3 badge latch door 2 hours**: With this option enabled the user can latch unlock a door for two hours by badging their card three times in succession at the reader. While the door is latch unlocked they can badge their card three times to lock the door.

  This option only applies to readers connected to the EliteSuite keypad's slave network.

- **3 badge latch door 4 hours**: With this option enabled the user can latch unlock a door for four hours by badging their card three times in succession at the reader. While the door is latch unlocked they can badge their card three times to lock the door.

  This option only applies to readers connected to the EliteSuite keypad's slave network.

- **3 badge latch door 8 hours**: With this option enabled the user can latch unlock a door for eight hours by badging their card three times in succession at the reader. While the door is latch unlocked they can badge their card three times to lock the door.

  This option only applies to readers connected to the EliteSuite keypad's slave network.

### Access levels

All users associated with an apartment can arm and disarm the apartment's area and access any connected doors at all times; however, you can also assign access levels here to grant the user access to other parts of the Protege GX system. For example, as well as their own apartments users might require access to shared spaces such as entrances, carparks and gyms.

Click **Add** to add a new access level.

- **Name**: The name of the access level assigned to the user.
- **Access level expires**: When this option is enabled the access level will expire based on the defined start and end dates. The user will only be able to use this access level between the expiry start and end dates.

  Multiple copies of the same access level can be assigned to a single user with different expiry times, allowing for periodic access. For example, a technician may only be able to access the building for a few days per month.
- **Expiry start**: This access level will not be valid for the user before this date and time.
- **Expiry end**: This access level will not be valid for the user after this date and time.
- **Schedule**: This schedule determines when the permissions provided by the access level are valid for this user. This is combined with any schedules set in the access level itself, as well as in door or floor groups.

  The user only has access if all relevant schedules are valid.

## Manual Apartment Commands

Right clicking an apartment record in **Programming | Apartments** opens a menu allowing you to send a message to the keypad. This enables building managers to send messages to the tenants of each apartment.

Users can read messages by pressing the **[MENU]** key, logging in with their PIN, and pressing **[2]**. They can delete each message by pressing the **[FORCE]** key.

# Batch add apartments

The batch add apartments feature allows you to create a number of apartments that will be assigned to a controller.

## Adding Apartments as a Batch

1. Navigate to **Programming | Batch add apartments**.
2. Set the number of apartments (between 5 and 248).
3. Enter a **Name** prefix that will be used by all of the new apartments. Sequential numbers will be added after the prefix (e.g. Apartment 1, Apartment 2, etc).
4. Enter the **Keypad address start**, which defines the **Keypad address** of the first apartment. The subsequent addresses will be assigned sequentially.

   When apartments are batch added the first **Keypad address** is one higher than the **Keypad address start** selected. This is a known issue.

5. Select the **Controller** the apartments will be assigned to.
6. Click **OK**.
7. Edit individual apartment details as required.

# Groups Menu

Grouping devices such as doors, areas and outputs provide a convenient way of assigning multiple items to access levels and controlling multiple devices with a single function. For example, you might create an output group containing multiple beepers and LEDs which can be used for warning users when an area is about to arm.

In addition, menu groups allow you to determine which menus each user can access at each keypad.

## Door groups

When assigned to an access level, door groups are used to define which doors a user can access and/or control. They can also be used with the **Interlock door group** (**Programming | Doors | General**) and **Lock door group on arming** ( **Programming | Areas | Configuration**) features, and in door control programmable functions.

### Door groups | General

#### General

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

#### Door group expiry date/time

Door group expiry allows you to enable/disable the door group across all user access levels at a particular date and time. For example, you could use this to pre-program a section of the building that is under construction and make it accessible to all staff on the day it is opened.

- **Start**: With this option enabled the door group will not be accessible before the specified date and time.
- **End**: With this option enabled the door group will not be accessible after the specified date and time.

#### Doors

Click **Add** to assign doors to the group. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

- **Schedule**: The schedule determines when the door is a valid member of this door group. When the schedule is valid the door is included in the group. When the schedule is invalid the door is not included in the group.

#### Record history

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

# Area groups

Area groups can be assigned to access levels to define the areas that a user is allowed to arm and disarm. They can be assigned as either arming area groups (only arming allowed) or disarming area groups (both arming and disarming allowed). Area groups are also assigned to keypads (**Expanders | Keypads | Configuration**), used with the **Interlock area group** feature (**Programming | Areas | Configuration**) and used in area control programmable functions.

## Area groups | General

### General

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

### Areas

Click **Add** to assign areas to the group. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

### Record history

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

# Keypad groups

Keypad groups can be assigned to menu groups to determine which keypads users have access to. They can also be used with the **Defer warning keypad group** feature in **Programming | Areas | Configuration**.

## Keypad groups | General

### General

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

### Keypads

Click **Add** to assign keypads to the group. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

### Record history

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

# Menu groups

When assigned to an access level, menu groups define which keypad menus and other features a user has access to. Menu groups can also be assigned to specific keypads (**Expanders | Keypads | Configuration**) to further limit the menus that can be accessed. If access to a menu is denied by either the access level or the keypad programming the user will not be able to access that menu from that keypad.

## Menu groups | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Operating schedule**: The operating schedule determines when this particular menu group is active in an access level. When the schedule is valid the settings in this menu group will be used. When the schedule is invalid the settings from the **Secondary menu group** below will be used.
- **Secondary menu group**: When the **Operating schedule** above is invalid the secondary menu group will be used by access levels.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

### Settings

- **Area (1)**: When this option is enabled, users can access the area menu by pressing **[MENU] [1]** on the keypad. This menu allows users to arm and disarm areas.
- **User (2)**: When this option is enabled, users can access the user menu by pressing **[MENU] [2]** on the keypad. This menu allows users to change their own PIN.
- **Events (3)**: When this option is enabled, users can access the events menu by pressing **[MENU] [3]** on the keypad. This menu allows users to view events saved on the controller.
- **Installer (4)**: When this option is enabled, users can access the installer menu by pressing **[MENU] [4]** on the keypad. This menu allows users to view and control the status of devices in the system and change the IP address of the controller.
- **View (5)**: When this option is enabled, users can access the view menu by pressing **[MENU] [5]** on the keypad. This menu allows users to view and control the alarm memory, system troubles and some device statuses.
- **Time (6)**: This is a legacy option that has no effect.
- **Bypass (7)**: When this option is enabled, users can access the bypass menu by pressing **[MENU] [7]** on the keypad. This menu allows users to bypass inputs.
- **System (8)**: This is a legacy option that has no effect.
- **Advanced installer (4, 8)**: This is a legacy option that has no effect.
- **Extended time menus (6, 2-4)**: This is a legacy option that has no effect.
- **Bypass trouble input (7, 2)**: This is a legacy setting that should not be used.

  It is possible to bypass trouble inputs from the keypad, but the bypass can only be removed by power cycling the controller. Therefore, it is recommended that you disable bypassing for trouble inputs.

- **Area group control allowed**: When this option is enabled, users can press the **[RIGHT]** arrow key from the area menu to arm/disarm the keypad's area group.

  The keypad must have an **Area group for this keypad** set (**Expanders | Keypads | Configuration**) and **Allow area group selection access** enabled (**Expanders | Keypads | Options 1**).

- **Tamper area control allowed**: When this option is enabled, users can press the **[LEFT]** arrow key from the area menu to arm/disarm the 24hr portion of each area.

  The keypad must also have **Allow 24hr area access** enabled (**Expanders | Keypads | Options 1**).

- **Stay arming**: When this option is enabled, users can stay arm areas by pressing the **[STAY]** key. The area(s) must have stay arming enabled in **Programming | Areas | Options 2**.
- **Force arming**: When this option is enabled, users can force arm areas by pressing the **[FORCE]** key. The area (s) must have force arming enabled in **Programming | Areas | Options 2**.
- **Instant arming**: When this option is enabled, users can instant arm areas by holding the **[STAY]** key (instant stay arm) or **[FORCE]** key (instant force arm) for two seconds. The area(s) must have instant arming enabled in **Programming | Areas | Options 2**.

### Keypad groups

You can assign keypad groups to a menu group to restrict the menu permissions to those keypads only. This allows you to grant users specific permissions at different keypads by assigning multiple menu groups to a single access level.

If there are no keypad groups assigned here the menu group applies to all keypads on this site.

It is important that there is only one menu group applied to each keypad that a user can access. If multiple menu groups are available for a keypad the controller will not know which permissions should be presented to the user. This can result in undefined system operation.

### Record history

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

## Menu groups | Options

- **User advanced menu**: This is a legacy option that has no effect.
- **Installer menu group**: This option can be enabled for menu groups used by site installers and technicians. When a user with this menu group logs into the keypad the Installer Logged In trouble input is opened.

  In addition, users with this menu group assigned can stay logged in to the keypad indefinitely, regardless of the **Time user is logged in** setting in **Expanders | Keypads | Configuration**. This is convenient for installers who will be commissioning and maintaining the site.
- **Show user greeting**: Enable this option for the keypad to display a personal greeting to the user when they log in. For example, when the user John Smith logs in to the keypad at 9am it will display the message, 'Good Morning John Smith'. This option may be disabled to decrease the time it takes to log in to a keypad.

  This option is equivalent to the **Show a greeting message to user** option in **Users | Users | Options**. The greeting will be displayed if either option is enabled for the user.

- **User can acknowledge alarm memory**: When this option is enabled, users with this menu group assigned are able to acknowledge alarms in the alarm memory. Users can access the alarm memory by pressing **[MENU] [5] [1]**. The user must also have access to the **View** menu (**General** tab).

  When this option is disabled, users can view alarms but cannot acknowledge them.

  This option is equivalent to the **User can acknowledge alarm memory** option in **Users | Users | Options**. Alarms can be acknowledged if either option is enabled for the user.

- **Show user alarm memory on logon**: When this option is enabled the keypad will automatically display the alarm memory for the keypad's primary area to the user when they log in to the keypad. The user must also have access to the **View** menu (**General** tab).

  This option is equivalent to the **Show alarm memory on login** option in **Users | Users | Options**. The alarm memory will be shown if either option is enabled for the user. The keypad's primary area can be set as the **Area this LCD belongs to** (**Expanders | Keypads | Configuration**).

# Output groups

Output groups are used to allow a number of outputs to be controlled by a single function. Most features that control outputs - such as door and area output functions, input and input type control, access level outputs and programmable functions - can instead control output groups.

There are a variety of applications where it is beneficial to use a group of outputs instead of only one. For example, output groups can improve accessibility by including both visual and audible cues in notifications and alarms; instead of using a single keypad beeper for entry and exit delays, you could create an output group containing a number of beepers and LEDs to ensure the signal can be heard and seen throughout the room. There are also applications in automation; allowing a single input or output activation to trigger a range of other effects (one-to-many programming).

## Output groups | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.
- **Output time**: The duration (in seconds) that the output group will be activated for. When this time elapses, all of the outputs in the group will be deactivated. If this is set to 0 the outputs will remain on continuously until they are deactivated.

  The output time set here overrides the **Activation time** set in the individual outputs.

### Outputs

Click **Add** to assign outputs to the group. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

### Record history

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

# Elevator groups

When assigned to an access level, elevator groups are used to define which elevator cars a user has access to.

Assigning an elevator group to an access level does not grant the user access to the floors assigned to those elevators. Floor groups must be assigned to the access level separately.

Usage may vary depending on the integration being configured. For more information, see the specific application note for your elevator integration.

## Elevator groups | General

### General

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

### Elevators

Click **Add** to assign elevator cars to the group. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

### Record history

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

# Floor groups

When assigned to an access level, floor groups define which floors a user has access to.

Assigning a floor group to an access level does not grant the user access to the elevator cars which service those floors. Elevator groups must be assigned to the access level separately.

Usage may vary depending on the integration being configured. For more information, see the specific elevator application note for your integration.

## Floor groups | General

### General

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

### Floors

Click **Add** to assign floors to the group. You can drag and drop individual records into the field, or select multiple records with Shift + Click. Then click **OK**.

### Record history

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

# Expanders Menu

Expanders represent the physical modules connected to the Protege module network. This includes Protege keypads and expander modules as well as smart readers (external third-party readers connected to the system).

## Module Updates

Generally when you update the configuration of an expander module in the software the new programming will not be implemented in the module immediately. You must perform a module update to update the configuration in the expander module itself. This applies to most changes made in the **Expanders** programming menus (excluding smart readers).

If a module update is required the controller will generate a health status message stating the module that requires updating. To update an expander module:

1. Edit the configuration as required and click **Save**.
2. Wait for the programming to be downloaded to the controller. To download immediately, navigate to **Sites | Controllers**, right click on the controller and click **Force download**.
3. On the **Expanders** programming page, right click on the expander record and click **Update module**.
4. The module will restart, temporarily dropping offline. When it connects again it will use the new configuration. The software displays the progress of the module update.

It is recommended that you use this method to update modules one at a time instead of the **Update modules** command on the controller, which restarts every module connected to the controller (regardless of whether the programming has changed).

## Virtual Modules

Virtual modules are modules that are programmed and addressed in the system, but do not correspond to physical modules. They act as logical placeholders, allowing you to program virtual inputs and outputs for use with programmable functions, output follows input programming and other advanced features. This enables you to automate your system without using additional hardware.

Virtual modules have the following features:

- Inputs and outputs can be assigned to the virtual module as normal. They act as memory placeholders in the controller with a binary state. Virtual analog expanders can also be used to download data values to the controller.
- Trouble input processing is disabled and the module does not affect the controller's health status.
- The module does not require module updates.
- The module does not appear in the controller's module addressing window.
- Physical and virtual modules cannot be programmed with the same **Physical address**. If a virtual module already exists, a physical module connected to the system will fail to come online and flash an error code.

  To ensure that physical and virtual modules do not overlap, it is recommended that virtual modules are addressed with higher numbers than physical expanders.

To program a virtual module, add a new expander module with the required inputs and outputs, set the **Physical address** to a high value (e.g. 32) and enable the **Virtual module** option.

# Keypads

Keypads are the main on-site interface for the Protege GX system. They can be used to arm and disarm the system, view the alarm memory, unlock doors, review device status, system troubles and events, and configure the controller's IP address.

For more information on programming and operating keypads, see:

- The relevant keypad installation manual
- Application Note 222: Protege Keypad Menu Reference
- Application Note 338: Programming Protege Keypads

## Keypads | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Physical address**: The network address of the module on the controller network. Connected expander modules can be addressed with the controller's **Module addressing** function (right click on the controller record).

  Alternatively, keypads can be addressed using the inbuilt configuration menu (see the relevant installation manual).

  The maximum physical address available for keypad modules is 200.

### Display

- **Default display line one / two**: The default text which is shown on the keypad when no user is logged in. This custom text will be displayed when the **Display custom message** option is enabled (**Options 1** tab). Each line on the keypad can display up to 16 characters, which may be letters, numbers or punctuation.

  These fields also support format codes which can be used to display the time and date on the keypad in various formats. See the table below for the available format codes:

  If any of the other **Display options** available in the **Options 1** tab are enabled they will override this text.

| Format Code | Displayed Text |
|---|---|
| &T | Time in 12 hour format with AM/PM in upper case (e.g. 9:15AM). |
| &t | Time in 12 hour format with am/pm in lower case (e.g. 9:15am). |
| &M | Time in 24 hour (military) format with a leading space for single digit hours (e.g. 9:15, 21:15). |
| &m | Time in 24 hour (military) format with a leading zero for single digit hours (e.g. 09:15, 21:15). |
| &G | Time in 12 hour format with no am/pm symbol (e.g. 9:15). |
| &A | AM/PM symbol in upper case (e.g. AM). |
| &a | AM/PM symbol in lower case (e.g. am). |
| &D | Day of the month with a leading space for single digit days (e.g. 3, 27). |
| &R | Day of the week in abbreviated three character format (e.g. Mon, Fri). |

| Format Code | Displayed Text |
|---|---|
| &V | Name of the month in abbreviated three character format (e.g. Mar, Nov). |
| &v | Number of the month with a leading space for single digit months (e.g. 3, 11). |
| &s | Number of the month with a leading zero for single digit months (e.g. 03, 11). |
| &Y | Year in two digit format, i.e. final two digits of the year (e.g. 21). |
| &C | Century, i.e. first two digits of the year (e.g. 20). |

Often the displayed text of a format code uses more characters than the code itself. Ensure there is enough whitespace around each format code for it to display in full without being overlapped by other text.

### Commands

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

### Record history

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

## Keypads | Configuration

### Configuration

- **Area this LCD belongs to**: The primary area for this keypad; generally the area that the keypad is physically located in. The keypad will display the primary area by default in the area and alarm memory menus.

  Ensure that the primary area is included in the **Area group for this keypad** (below).
- **Dual code timeout**: This is a legacy option that has no effect.
- **Max invalid PIN entry attempts**: When **Lock keypad on excess attempts** is enabled (**Options 1** tab) this field defines the maximum number of invalid PIN attempts that the keypad will accept. For example, if this is set to 3, after three incorrect PIN entries the keypad will prevent any further attempts.
- **Lockout keypad time**: When **Lock keypad on excess attempts** is enabled (**Options 1** tab) this field defines the time (in seconds) that the keypad will lock out after several invalid PIN attempts. During this period the keypad will display a 'Keypad is locked out' message and ignore all user input.
- **Door connected to keypad**: Setting a door in this field allows users to unlock it from the keypad using the **[FUNCTION]** key (holding the **[MENU]** key for 2 seconds on the PRT-KLCS). You must also enable either **Function key unlocks door when logged in (REX)** or **Function key unlocks door when logged out (REX)** in the **Options 1** tab.
- **Menu group for this keypad**: Defines the menus that are accessible from this keypad. For a user to access a menu, the menu must be permitted by both the keypad and the user's access level.

  If this field is <not set> all menus will be accessible from this keypad.
- **Area group for this keypad**: Defines the areas that can be viewed and controlled from this keypad. For a user to view and control an area, the area must be permitted by both the keypad and the user's access level.

  In addition, the area group set here can be armed/disarmed together from this keypad by pressing the **[RIGHT]** key in the area menu. **Allow area group selection access** must be enabled in the **Options 1** tab, and **Area group control allowed** must be enabled in the user's menu group.

  If this field is <not set> all areas associated with the controller will be accessible from this keypad, and area group arming/disarming will not be available.
- **Smoke reset output / output group**: This output or output group is activated when a user holds the **[CLEAR]** and **[ENTER]** keys on the keypad for 2 seconds. This can be used to activate a relay that resets the smoke alarm.

**Note**: The output or output group is not deactivated automatically.

- **Time user is logged in**: The time (in seconds) that a user can be logged in to the keypad without pressing any keys. For example, if this is set to 20 seconds, after 20 seconds of no input the keypad will automatically log the user out.

  This should not be set to Never Logout except for demonstration and testing purposes. Users with the **Installer menu group** option enabled (**Groups | Menu groups | Options**) can stay logged in to the keypad indefinitely.

# Keypads | Options 1

## Display options

- **Display custom message (lines 1 and 2)**: With this option enabled, when there is no user logged in the keypad will display the text set in **Default display line one / two** (**General** tab).

  This option can be overridden by the alternative options below.

- **Display primary area status**: With this option enabled, when there is no user logged in the keypad will display the primary area status. The primary area is set as the **Area this LCD belongs to** (**Configuration** tab).
- **Display scrollable area group**: With this option enabled, when there is no user logged in the keypad will display the areas included in the **Area group for this keypad** (**Configuration** tab). Users can scroll the areas with the **[UP]** and **[DOWN]** keys.
- **Display trouble message**: With this option enabled, whenever there is a system trouble the keypad will beep and display the message 'Trouble fault check system'.
- **Display bypass message**: When this option is enabled, whenever an area has been armed with one or more inputs bypassed the keypad will beep and display the message 'System has bypassed input(s)'.

  This is only displayed when the area is armed.

- **Display alarm message**: When this option is enabled, whenever there is an alarm in the keypad's alarm memory the keypad will beep and display the message 'System has Alarm in memory'.
- **Display primary area messages only**: When this option is enabled the keypad will only display messages related to the primary area when there is no user logged in. This applies to the **Display bypass message** and **Display alarm message** options.

  When this option is disabled, messages will be displayed for any area included in the **Area group for this keypad** (**Configuration** tab).

  The primary area is set as the **Area this LCD belongs to** (**Configuration** tab).

- **Display defer area warning messages**: With this option enabled, when an area begins a defer arming cycle the keypad will beep and display the message '*WARNING* System is about to ARM!'. The keypad must be part of the **Defer warning keypad group** set in **Programming | Areas | Configuration**.

  To enable defer arming for an area, see **Defer automatic arming** (**Programming | Areas | Options 2**).

- **Show time and attendance detail**: With this option enabled, whenever a user gains access at the associated door the keypad will display their name, the current time and the date. This is useful for notifying employees of the time they have arrived at work.

  The door used is set as the **Door connected to the keypad** (**Configuration** tab).

- **Length of time to display attendance detail**: When **Show time and attendance detail** is enabled, this is the length of time (in seconds) that the time and attendance message will be displayed on the keypad.
- **Attendance detail format**: When **Show time and attendance detail** is enabled, this field defines the format that will be used for the date. Choose from month-first or day-first formats.

### Access options

- **Function key unlocks door when logged in (REX)**: When this option is enabled, users can unlock a door by logging in to the keypad and pressing the **[FUNCTION]** key (holding the **[MENU]** key for 2 seconds on the PRT-KLCS). You can set the **Door connected to keypad** in the **Configuration** tab.
- **Keypad can access only primary area**: When this option is enabled, users can only view and control the keypad's primary area (**Area this LCD belongs to** in the **Configuration** tab), regardless of the area group assigned to the keypad.
- **Allow 24hr area access**: When this option is enabled, users can view and control the 24hr portions of any areas available on the keypad. This is accessed by pressing the **[LEFT]** key while viewing an area.

  The user must also have **Tamper area control allowed** enabled in their menu group (**Groups | Menu groups | General**).
- **Allow area group selection access**: When this option is enabled, users can view and control the area group assigned to this keypad (**Area group for this keypad** in the **Configuration** tab). This is accessed by pressing the **[RIGHT]** key while viewing an area.

  The user must also have **Area group control allowed** enabled in their menu group (**Groups | Menu groups | General**).
- **Function key unlocks door when logged out (REX)**: When this option is enabled, users can unlock a door by pressing the **[FUNCTION]** key (holding the **[MENU]** key for 2 seconds on the PRT-KLCS) without logging in to the keypad. You can set the **Door connected to keypad** in the **Configuration** tab.
- **Auto logout after user arming**: When this option is enabled the keypad will automatically log the user out when an area is successfully armed or disarmed. This can prevent third parties from accessing the keypad if the user forgets to log out.
- **Activate access level output**: When this option is enabled the output(s) associated with the user's access level will be activated when the user successfully logs in to this keypad. These outputs are set in the **Users | Access levels | Outputs / Output groups** tabs. The **Keypad access activates output** option must also be enabled (**Users | Access levels | General**).

  By default, the user requires valid access to the keypad menus from their access level. To remove this restriction enable **Always activate access level output** (**Options 2** tab).
- **Lock keypad on excess attempts**: When this option is enabled, if someone attempts to log in with an invalid user PIN several times the keypad will lock out any further attempts for a set period. When the keypad is locked out the Too Many Attempts trouble input will be opened.

  The **Max invalid PIN entry attempts** and **Lockout keypad time** are set in the **Configuration** tab.

## Keypads | Options 2

### Offline options

- **Offline access to automation menu**: When this option is enabled, users can access the automation menu by pressing **[MENU] [1]** without logging in to the keypad. Automations can be linked to outputs or output groups, providing a convenient method for users to control devices such as lighting, sprinklers and HVAC.
- **Allow access to the trouble view menu**: When this option is enabled, users can access the trouble view menu by pressing **[MENU] [2]** without logging in to the keypad. This is convenient for technicians diagnosing troubles in the system.
- **Allow access to the event review menu**: When this option is enabled, users can access the events menu by pressing **[MENU] [3]** without logging in to the keypad. This is convenient for guards reviewing recent events.
- **Allow access to the information menu**: When this option is enabled, users can access the information menu by pressing **[MENU] [4]** without logging in to the keypad. This includes information such as the controller firmware version, controller serial number, time and date.

- **Keypad login requires card**: When this option is enabled, users must badge a card and enter a PIN to access the keypad (two factor authentication).

  The keypad must be associated with a reader port or smart reader. After a user badges at the reader they can enter their PIN at the keypad and press **[ENTER]** to log in. PINs cannot be entered directly at the keypad without badging a card first.

  To enable this feature it is necessary to configure the following options in the reader expander programming:

  - **Reader 1/2 door**: Must be set to a door which requires card and PIN access for either entry or exit (corresponding to the side of the door where the keypad is located)
  - **Reader 1/2 keypad type**: LCD Keypad
  - **Keypad to use for PINs reader 1**: This keypad

In addition to the offline options outlined above it is also possible to view any open inputs in the primary area in the offline menu, by adding the command `OfflineInputView = true`. To view all inputs in the primary area, also include the command `ClosedInputsInOfflineView = true`.

### General options

- **Disable the LCD keypad beeper**: When this option is enabled the keypad will not beep when keys are pressed. Other beeper operations will still function.

  Enabling this setting overrides the **Clear key can disable keypress beeper** option below.

- **Duplex inputs (4 keypad inputs)**: When this option is enabled the keypad can support up to 4 inputs wired in duplex configuration. Additional inputs should be addressed as inputs 3-4 on the keypad.

  For wiring instructions, see the relevant keypad installation manual.

- **Beep on communication failure**: This is a legacy option that has no effect.
- **Clear key can disable keypress beeper**: When this option is enabled, users can press and hold the **[CLEAR]** key to disable the keypad beeper. This will disable all beeper functions (e.g. key press response, alarms and entry/exit delays, manual control, etc.). Pressing and holding the **[CLEAR]** key again will enable the beeper.

  This setting has no effect while the **Disable the LCD keypad beeper** option above is enabled.

- **Virtual module**: Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.

### Output options

- **Activate access level output only on valid access**: This option is not used. This is the default behavior for access level outputs.
- **Always activate access level output**: When this option is enabled the user's access level output or output group will always be activated whenever they enter their PIN code at the keypad, regardless of whether they have access to use that keypad. This can allow users to control a specific output or output group from the keypad without giving them keypad access.

  **Activate access level output** (**Options 1** tab) must be enabled. Access level outputs are assigned in **Users | Access levels | Outputs / Output groups**.

## Manual Keypad Commands

Right clicking a keypad record in **Expanders | Keypads** opens a menu with manual commands for that keypad.

### Control

- **Reset users**: This is a legacy option that has no effect.
- **Update module**: Updates the programming in the keypad. For more information, see Module Updates (page 291).

# Analog expanders

Analog expander records are used to monitor and control analog channels. They can be configured as either analog inputs (receiving data) or analog outputs (sending data), in conjunction with data values and variables.

Protege analog input and analog output expanders can be used to connect a variety of analog detectors (such as temperature and humidity sensors) and industrial automation devices (such as HVAC modules) to the system. Analog channels can be monitored directly within Protege GX and can control or be controlled by programmable functions. This allows you to unify your site security and automation functions.

For information on connecting analog expanders, see the relevant installation manual.

Protege power supplies register as analog expanders in the system. This allows you to monitor four input channels: core voltage, V1 voltage, V2 voltage and current. For more information, see Monitoring Power Supply Voltage and Current (next page).

## Analog expanders | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Expander personality**: The expander personality should be set to the product code of the connected Protege module.

### Configuration

- **Invert device tamper**: When this option is enabled the module's tamper input will be inverted. This should be enabled when the tamper switch has a normally open configuration.
- **Virtual module**: Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.
- **Physical address**: The network address of the module on the controller network. Connected expander modules can be addressed with the controller's **Module addressing** function (right click on the controller record).

  The maximum physical address available for analog expander modules is 32.

### Commands

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

### Record history

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

## Analog expanders | Channel 1-4

### Options

- **Enable channel**: When this option is enabled the analog expander will begin processing the analog channel. The channel can act as either an analog output (sending data) or an analog input (receiving data) depending

on the hardware. When this option is disabled the channel will perform no function.

- **Channel uses 0-20mA input (disabled uses 0-10v)**: Each channel can be configured for either current or voltage operation. By default, the input or output will operate in 0-10V mode. When this option is enabled it will operate in 0-20mA mode. The option selected will depend on the connected devices.

  In current mode the acceptable signal range is 0-20mA, which allows the connection of standard 4-20mA devices.

- **Preset DAC output power up**: When this channel is used for an analog output (DAC), enable this option to set the output to a fixed value when the module is powered up. The preset value is determined by the option below. When this option is disabled, when the output is powered up it will be set to the last known value.
- **Preset to 100 percent (disabled preset to 0)**: When **Preset DAC output power up** is enabled, this option determines the state of the analog output when the module is powered up. When this option is enabled the output will be set to 100% (the maximum value). When this option is disabled, the output will be set to 0% (the minimum value).
- **Send ADC value in diff mode**: When this channel is used for an analog input (ADC), this option determines how the input values are sent to the controller.

  By default (when this option is disabled), the analog value is sent to the controller at set intervals. The frequency of the updates is set as the **Channel 1-4 update time** below.

  When this option is enabled the analog value is sent to the controller only when it has changed by a certain amount (the diff). The amount the value must change before an update is sent is set as the **Channel diff comparison value** below.
- **Log channel data**: When this option is enabled, all data updates from the channel are logged as events. This is useful for initial configuration and troubleshooting, but to save event storage should not be left enabled during normal operation.

### Channel settings

- **Channel update Time**: When **Send ADC value in diff mode** is disabled the channel will send updates to the controller at regular intervals. This field sets the time between updates (in seconds), and the data is averaged over the period of time being sampled.

  It is recommended that the update time is scaled to match the expected rate of change and required level of supervision. A long update time is generally sufficient and reduces the risk of 'spikes' in the data.
- **Channel diff comparison value**: When **Send ADC value in diff mode** is enabled the channel will send updates to the controller when the value has changed by a defined amount. This field sets the diff value that is used to compare the current value with the most recent update.

  For example, when monitoring the core voltage of a power supply this value may be set to 10. If the last updated value is 1367 (13.67V) the channel will not set an update to the controller until the voltage reaches either 1357 (13.57V) or 1377 (13.77V).
- **Channel data value**: Each channel can be assigned to a data value, which allows the system to set and store analog data from the channel. When connected to an analog input the data value stores and displays the data from the channel. When connected to an analog output the data value sets the output value and sends it to the hardware.

  Data values are programmed in **Automation | Data values**.

## Monitoring Power Supply Voltage and Current

Protege power supplies can be addressed as analog expanders in the system. This allows you to configure and monitor 4 analog input channels representing the voltage and current in the power supply.

The channels represent the following information:

| Channel Number | Function |
|---|---|
| 1 | V2 Voltage |

| Channel Number | Function |
|---|---|
| 2 | V1 Voltage |
| 3 | Core Voltage |
| 4 | Current |

Using data values and variables it is possible to monitor these values so that operators can remain aware of the power draw of the system.

1. Connect the power supply to the module network as instructed in the relevant installation manual.
2. Address the power supply as an analog expander (see page 92).
3. Create an analog expander record in **Expanders | Analog expanders** with a **Physical address** corresponding to that of the power supply.
4. Set the **Expander personality** to the type of power supply connected.
5. 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**.
6. A data value must be used to store the data. Click the ellipsis **[...]** beside **Channel 1 data value** to open a breakout window with data value programming. Create a new data value with the name V2 Voltage. Click **Save**.
7. Close the breakout window and set the **Channel 1 data value** to the V2 Voltage data value.
8. Repeat the above for Channel 2 (V1 Voltage), Channel 3 (Core Voltage) and Channel 4 (Current).
9. Click **Save**. Wait for the programming to be downloaded to the controller, then right click on the analog expander record and click **Update module**.
10. Variables must be used to display the channel data. Navigate to **Automation | Variables**. Create four new variables with the names V2 Voltage Variable, V1 Voltage Variable, etc.
11. For each variable, set the **Scale** to 0.01 and the **Data value** to the corresponding data value programmed above. Click **Save**.
12. The variables can now be displayed on a floor plan. Navigate to **Monitoring | Setup | Floor plan editor** and select an existing floor plan or create a new one.
13. Expand the **Devices** section and click **Add**.
14. Set the **Device type** to Variable and drag the four variables onto the floor plan. You can also add text to label each variable display. Click **Save**.
15. Now you can open the floor plan from **Monitoring | Floor plan view** and monitor the variable values.

# Input expanders

Input expanders extend the number of inputs available within the system, allowing you to monitor more devices such as door contacts, elevator inputs, PIRs and panic buttons. Virtual input expanders can also be used to generate alarms via input follows output programmable functions.

For wiring instructions, see the relevant installation manual.

## Input expanders | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **High charge current**: When this option is enabled a legacy PCB module will allow the connected battery to charge at 700mA. The default charging rate is 350mA. This option is not used for DIN rail modules.
- **Virtual module**: Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.
- **Invert device tamper**: When this option is enabled the module's tamper input will be inverted. This should be enabled when the tamper switch has a normally open configuration.
- **Physical address**: The network address of the module on the controller network. Connected expander modules can be addressed with the controller's **Module addressing** function (right click on the controller record).

  The maximum physical address available for input expander modules is 248.

### Commands

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

### External integration

This section allows you to configure either the Redwall or Inovonics integration for this input expander. The options available will depend on the **Integration type** in **Sites | Controllers | Configuration**.

For more information, see Application Note 181: Protege GX Redwall Integration or Application Note 183: Protege GX Inovonics Integration.

- **Redwall**
  - **Module IP address**: The IP address of the Redwall Redscan module which this input expander record represents.
- **Inovonics**
  - **Module serial number**: The serial number of the Inovonics wireless device which this input expander represents.

## Record history

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

# Output expanders

Output expanders extend the number of outputs available within the system, allowing you to control more devices such as lock relays, door pumps, LEDs, beepers and sirens. Virtual output expanders can also facilitate a variety of advanced programming features, such as logic control programmable functions.

For wiring instructions, see the relevant installation manual.

## Output expanders | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **High charge current**: When this option is enabled a legacy PCB module will allow the connected battery to charge at 700mA. The default charging rate is 350mA. This option is not used for DIN rail modules.
- **Invert device tamper**: When this option is enabled the module's tamper input will be inverted. This should be enabled when the tamper switch has a normally open configuration.
- **Virtual module**: Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.
- **Physical address**: The network address of the module on the controller network. Connected expander modules can be addressed with the controller's **Module addressing** function (right click on the controller record).

  The maximum physical address available for output expander modules is 32.

### Commands

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

### Record history

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

# Reader expanders

Reader expanders extend the number of reading devices available within the system. Each reader expander has two reader ports, each of which can be used to control a door or elevator car.

A reader expander record can also be associated with the controller's onboard reader expander. The address of this reader expander is set in the **Register as reader expander** field (**Sites | Controllers | Configuration**).

For wiring instructions, see the relevant installation manual.

## Reader Expanders | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Offline operation**: This field defines how the reader expander will operate when it loses connection with the controller. The options are:
  - **No users**: The reader expander will not grant access to any users.
  - **Any card**: The reader expander will grant access to any card that can be read. This will allow anyone with a card in the correct format to gain access to the door, even if the card is not programmed in the system.
  - **First 10 users plus cache**: When this option is enabled the reader expander will store a certain number of cards and grant access to those cards when it is offline. All other cards will be denied access.
    - The reader expander will grant access to the first 10 users downloaded to the controller. These are the first 10 users by database ID with access to anything on the controller, regardless of whether they have access to the doors on this expander. Only the first programmed card will be recognized.
    - In addition, the reader expander will store the most recent 150 cards which have gained access at this expander. These users will have access to both doors, regardless of their normal level of access.

  When the reader expander is offline, each time access is granted the reader will beep four times. PIN use is not supported by offline reader expanders, and all doors will allow card only access.
- **Slave comm operation**: Some legacy PCB reader expanders have an additional RS-485 port which allows the connection of a slave network. This option sets the function of the slave network. This option is not used for DIN rail modules.
- **Elevator floor split**: When **Slave comm operation** is set to 1 - Elevator Floor Control, this option defines where the floor relays are split. This option is not used for DIN rail modules.
- **Physical address**: The network address of the module on the controller network. Connected expander modules can be addressed with the controller's **Module addressing** function (right click on the controller record).

  The maximum physical address available for reader expander modules is 64.
- **Port 1/2 network type**: These fields determine how each reader port will operate (i.e. what kind of data it will send and receive). The options are:
  - **Wiegand**: Used for any standard Wiegand reader.
  - **ICT RS-485**: Used for card readers wired in RS-485 configuration (recommended).

- **OSDP**: Used when connecting OSDP readers. When you select this option the software will automatically create two smart readers in **Expanders | Smart readers** to represent the entry and exit OSDP card readers on this port. For more information, see Application Note 254: Configuring OSDP Readers in Protege.
- **Salto SALLIS**: Used to connect a SALLIS RS-485 router, which can control up to 16 wireless locks (configured as smart readers). For more information, see Application Note 148: Protege GX Salto SALLIS Integration.
- **Aperio**: Used to connect up to 15 Aperio communication hubs via RS-485, which can control up to 60 wireless locks (configured as smart readers). For more information, see Application Note 147: Protege GX Aperio RS-485 Hub Integration.
- **Allegion AD Series**: Used to connect Allegion PIMs (supporting up to 16 wireless locks) or wired locks. For more information, see Application Note 182: Allegion Integration with Protege GX.
- **Third party generic**: This option allows you to configure the reader expander to recognize third-party readers or other generic sources of serial data on this reader port (See the **Third party generic** options in the **Reader 1/2** tab). For more information, see Application Note 276: Configuring Credential Types in Protege GX.
- **ICT wireless lock update reader**: Used to connect an update reader for use with Protege wireless locks in offline mode. The **Reader 1/2 format** must be set to Custom credential. For more information, see the Protege Offline Wireless Lock Configuration Guide.

- **Ethernet network type**: When this reader expander record is used for the controller's onboard reader expander you can set the function of the ethernet port here. This is used when a third-party system is sending reader data to the controller

  The options are:
  - **Disabled**: The ethernet port is not used for reader data. This does not affect the controller's connection to the IP network.
  - **SALLIS**: Used to connect a SALLIS POE router, which can control up to 64 wireless locks (configured as smart readers). Smart readers are required to configure door control. For more information, see Application Note 148: Protege GX Salto SALLIS Integration.
  - **Third party generic**: Allows you to connect custom data sources to the controller for use as readers, via the IP network. Any data input that can be configured as a credential type can be used, along with a smart reader to configure door control. For more information, see Application Note 276: Configuring Credential Types in Protege GX.
  - **VingCard Visionline**: Used to connect to a VingCard Visionline server, which communicates with wireless locks (configured as smart readers). For more information, see Application Note 215: Protege GX VingCard Visionline Integration.
- **Ethernet port**: When the **Ethernet network type** above is set to Third party generic this field defines the TCP/IP port which the controller will communicate over. This port is used by smart readers to receive data from third-party 'readers'.

  If the controller needs to listen on multiple ports for different data sources, enter the command `SmartReaderPortOffset = true` in the **Commands** field below. The port used by each smart reader corresponds to the **Ethernet port** plus the **Configured address** (**Expanders | Smart readers | General**).
- **SALLIS router port**: When the **Ethernet network type** above is set to SALLIS this field defines the port used to communicate with the SALLIS router.
- **SALLIS Router IP**: When the **Ethernet network type** above is set to SALLIS this field defines the IP address used to communicate with the SALLIS router.

## Options

- **High charge option**: When this option is enabled a legacy PCB module will allow the connected battery to charge at 700mA. The default charging rate is 350mA. This option is not used for DIN rail modules.

- **Multiple reader input port 1/2**: When the **Port 1/2 network type** is set to Wiegand, select these options to enable multiple reader processing for each reader port. This allows you to connect two readers to the specified reader port to act as entry and exit readers. When these options are disabled the reader port will only process a single connected reader.

  This setting is not required for RS-485 connections. For wiring instructions, see the relevant installation manual.

- **Virtual module**: Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.
- **Invert device tamper**: When this option is enabled the module's tamper input will be inverted. This should be enabled when the tamper switch has a normally open configuration.

### Ethernet card data options

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

  For more information, see the relevant application note for your integration.

  This field sets the encryption key for SALLIS readers connected to this reader expander.

### Commands

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

### Record history

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

## Reader expanders | Reader 1/2

These tabs allow you to configure the operation of each reader port separately. Different options will be available depending on the **Port 1/2 network type** set in the **General** tab.

### Configuration

- **Reader 1/2 format**: This field defines the type of data the reader port will receive from the connected readers. Protege reader expanders support a wide variety of publicly available protocols, as well as some special protocols. Any 26 or 37 bit reader that conforms to the standard format specification will function with the reader expander.

  Ports on reader expanders also support custom credentials provided by third-party devices:
  - The Custom format option uses the format programmed in **Sites | Controllers | Custom reader format**.
  - The Custom credential option uses a credential type programmed in **Sites | Credential types**. The credential type used is determined by the door type.
- **Reader 1/2 location**: The location informs the reader expander whether the connected reader is installed at the entry or exit side of the door. This is only relevant when the **Port 1/2 network type** is set to Wiegand, as the wiring configuration is used to determine location for RS-485 connections.

  When multiple readers are connected to a port in Wiegand configuration the reader that is wired to the secondary port is always counted as the exit reader.

- **Reader 1/2 mode**: Each reader port can be configured for one of the following operation modes:
  - **Access**: Controls access through a door. Set the **Reader 1/2 door** as required. This mode should also be used for controlling an elevator call button.

- **Elevator**: Controls floor access in an elevator car. Set the **Reader 1/2 elevator** as required.
- **Area control**: Controls area arming and disarming only. Set the **Reader 1/2 area control area** as required. In this mode the card reader will accept either card or PIN credentials. Users with appropriate permissions can arm the area using the method defined in **Reader 1/2 arming mode**, and disarm the area by entering their credentials once (when the **Disarm area for door on access** option is enabled).

  Reader ports used for door access can also be used for area control by setting the **Area inside door** and **Area outside door** (**Programming | Doors | General**).

- **Reader 1/2 door**: When the **Reader 1/2 mode** is set to Access, this field sets the door that is controlled by this reader port. The same door may be controlled by more than one reader port (entry and exit).
- **Reader 1/2 keypad type**: The reader port supports a number of different PIN pad formats connected in Wiegand configuration. When configured for RS-485 operation only the ARK-501 and LCD keypad options are available.
  - **LCD keypad**: This option allows you to associate an LCD keypad module with this reader port (the **Keypad to use for PINs reader 1/2** below). When a user badges at the reader the keypad will prompt them to enter their PIN and press the **[FUNCTION]** key to unlock the door.

    To unlock the door the user **must not press [ENTER]** after entering their PIN. The **[FUNCTION]** key must immediately follow the PIN code. If the user presses **[ENTER]** the keypad will log them in (see below).

    In addition, this option allows you to use two factor authentication for keypad access. This is required when **Keypad login requires card** (**Expanders | Keypads | Options 2**) is enabled. When the user badges their card they can enter their PIN and press **[ENTER]** to log in to the keypad.
  - **ARK-501**: The standard Motorola® format used by ICT card readers. Each keypress is encoded as 8 bits of data, with the first 4 bits inverted from the remaining 4. The user must press the **[ENTER]** or **#** key to complete the PIN.
  - **26 bit (site 0)**: 26 bit Wiegand format used by a PIN pad connected in parallel with the reader. The PIN pad data has a site code of 0.

    PIN codes cannot begin with 0. The maximum PIN for this format is 65535.

  - **4 bit**: 4 bits of data for each keypress.
  - **4 bit parity**: 4 bits of data plus a parity bit for each keypress.
  - **4 bit buf**: 4 bits of data per keypress. The data is buffered and sent only when the user presses the **[ENTER]** or **#** key to complete the PIN.
  - **4 bit buf & par**: 4 bits of data plus a parity bit for each keypress. The data is buffered and sent only when the user presses the **[ENTER]** or **#** key to complete the PIN.
  - **36 bit (IEI S0)**: 36 bit Wiegand format typical of an IEI keypad, which can be set to decode PIN codes from 0-999999

    PIN codes cannot begin with 0. The maximum PIN for this format is 999999.

- **Keypad to use for PINs reader 1/2**: If the **Reader 1/2 keypad type** above it set to LCD keypad, this keypad can be used for PIN entry at the door.
- **Reader 1/2 arming mode**: This setting enables users to arm areas or control outputs by presenting their credentials to the card reader in a specific pattern. The options are:
  - **Arm area on 2 reads**: Users can enter their credentials twice to arm the associated area.
  - **Read and input 4/8 of expander**: Users can hold input 4 (for reader port 1) or input 8 (for reader port 2) and enter their credentials to arm the associated area.

    If input 4/8 is monitored by the area that is being armed, arming may fail because the input is open. To prevent this ensure that **Exit alley input do not test it** is enabled in the input type (**Programming | Input types | Options (1)**).

  - **Arm area on 3 reads**: Users can enter their credentials three times to arm the associated area.
  - **Toggle function output on 3 reads**: Users can enter their credentials three times to toggle the function output or output group on or off.

- **Activate function output on 3 reads**: Users can enter their credentials three times to activate the function output or output group. The output(s) will not be deactivated by this function.

  This option is not supported when the card reader is controlling an elevator car.

When the **Reader 1/2 mode** is set to Access the entry reader controls the **Area inside door** and the exit reader controls the **Area outside door** (set in **Programming | Doors | General**). When set to Area control, both readers control the **Reader 1/2 area control area** below. For output control options, both readers control the **Reader 1/2 function output / output group**.

If the chosen setting requires multiple reads, the user must present the same credential within 5 seconds of the previous read. All required credentials must be entered each time (e.g. Card and PIN).

The reader will beep twice to signal that the function has succeeded.

The user must have **Enable multi-badge arming** checked in **Users | Access levels | General** (regardless of whether the function is area or output control). If inputs in the area may be open, **Always force arm using card reader** may be enabled in **Programming | Areas | Options (2)**.

- **Reader 1/2 area control area**: When the **Reader 1/2 mode** is set to Area control, this field sets the area that is controlled by this reader port.
- **Reader 1/2 elevator**: When the **Reader 1/2 mode** is set to Elevator, this field sets the elevator car that is controlled by this reader port.
- **Reader 1/2 secondary format**: The secondary reading format is used when the reader expander cannot decode a card read using the primary format. This option is useful for sites with multiple card types in use.

  For more information on available formats, see **Reader 1/2 format** above.

- **Reader 1/2 function output / output group**: This output or output group can be activated when the user enters their credentials multiple times, based on the **Reader 1/2 arming mode** above.
- **Reader 1/2 dual authentication pending output**: This output is activated when the first user enters their credentials at a door which requires dual authentication. It is deactivated when the **Reader 1/2 dual authentication wait time** below expires or the second user enters their credentials.

  For doors connected to the controller's ethernet port, use the command `DualAuthOutputEth = #`, where **#** is the Database ID of the output.

- **Reader 1/2 dual authentication wait time**: When a door is configured to require dual authentication the reader expander will wait for this time (in seconds) after the first user enters their credentials. The second user can enter their credentials during this period to unlock the door. If this period expires the door will not unlock and the process must be restarted.

  For doors connected to the controller's ethernet port, use the command `DualAuthTimeEth = #`, where **#** is the wait time in seconds.

  Dual authentication settings are configured in **Programming | Door types | Options**.

## Reader options

- **Allow reading opened/unlocked**: When this option is enabled (by default) the reader expander will process card reads even when the door is already open or unlocked. This is useful for correct operation of antipassback, time and attendance, muster reports and area control, as it allows users to register at the door even when it is already open or unlocked.

  When this option is disabled, any card reads received when the door is unlocked or open will not be processed and no events will be generated.
- **Send format errors**: When this option is enabled the reader expander will send detailed information to the controller if it reads a card with a format error. Format errors include bit count, byte count, parity, checksum and LRC calculation failures. This information will appear in the event log.

  The **Log reader events** option must also be enabled.

- **Intelligent reader tamper mode**: ICT card readers offer intelligent reader tamper operation. When this feature is enabled in both the reader and the reader expander, the card reader will check in with the reader expander every 30 seconds. When the connection is lost the Reader 1/2 Tamper / Missing trouble input is opened to generate a tamper alarm.

  This option is always enabled in RS-485 mode.

## Card data options

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

  For more information, see the relevant application note for your integration.

  This field sets the encryption key for locks connected to this reader port.

## Third party generic

The options below are used to define the structure of generic serial data being sent to the reader port. This can be used for third-party readers and other devices.

This section is only displayed when the **Port 1/2 network type** is set to Third party generic. For programming examples, see Application Note 219: Intercom Integration using Credential Types in Protege GX and Application Note 276: Configuring Credential Types in Protege GX.

- **Reader 1/2 baud rate**: The rate at which generic serial data is transferred between the third-party device and the reader expander.
- **Reader 1/2 parity**: The method of calculating the parity for the block of generic serial data. This can be even, odd or none.
- **Reader 1/2 stop bits**: The stop bits for generic serial data. This is either 1, 1.5 or 2.
- **Reader 1/2 inter-byte time out**: This field defines the time (in milliseconds) allowed between receiving bytes of generic serial data.
- **Reader 1/2 log invalid data received**: Enable this option to allow the reader expander to log detailed information about any invalid data packets received from a generic third-party reader.

## Misc options

- **Disarm area for door on access**: When this option is enabled the associated area will be automatically disarmed when a user enters valid credentials, provided the user has access to disarm the area. When the reader is used for door control the area behind the door will be disarmed. When the reader is used for area control the control area set above will be disarmed.
- **Allow access when area armed**: When this option is disabled (by default), users can be denied access to a door when the area behind it is armed. They will only be allowed access if they have the ability to disarm the area.

  This option can be enabled to allow users through any door they have access to regardless of the area status. Be aware that this can easily cause false alarms as users will be able to enter areas that they cannot disarm.
- **Disarm users area on valid card**: This option allows users to disarm a personal area or area group when they gain access at the reader. For example, this could be used to allow a single reader to service a row of personal offices which users can arm and disarm individually.

  The **User area** is set in **Users | Users | General**, or an area group can be set in the **Area groups** tab. The user must have this area available in **Users | Access levels | Disarming area groups**.

  This feature is not supported when the card reader is controlling an elevator car.
- **Log reader events**: Enable this option to allow the reader to send format error information to the controller (with the **Send format errors** option enabled above). Other reader events are always sent to the controller.

- **Swap lock LED display**: This option is not used.
- **Activate access level output**: When this option is enabled the output or output group assigned to the user's access level will be activated when the user gains access to the door.

  The outputs are assigned in the **Outputs** or **Output groups** tab of **Users | Access levels**. The **Reader access activates output** option must be enabled in **Users | Access levels | General**, and further configuration is available there.
- **Display card detail when invalid**: When this option is enabled (by default) the reader expander will send the details of any unrecognized card (facility and card number) to the controller. The event log will display a 'Read Raw Data' event, allowing an operator to right click on the event and assign the card to a user.

  When this option is disabled the card data will not be saved and a 'Card Not Found' event will be displayed in the event log.
- **Arm users area**: This option allows users to arm a personal area or area group at the card reader on this reader port. For example, this could be used to allow a single reader to service a row of personal offices which users can arm and disarm individually.

  The action the user must take to arm the area depends on the **Reader 1/2 arming mode** setting above.

  The **User area** is set in **Users | Users | General**, or an area group can be set in the **Area groups** tab. The user must have **Enable multi-badge arming** checked in **Users | Access levels | General**, and the area must be included in the area groups for that access level.

  This feature is not supported when the card reader is controlling an elevator car.
- **Enable enhanced smart reader outputs**: This feature is used when the readers are wired in RS-485 configuration. The reader expander's BZ, L1 and L2 outputs are not used to control the beepers and LEDs on RS-485 readers, but by default they are reserved and cannot be used. You can enable enhanced smart reader outputs to 'free up' these physical outputs for other functions and gain independent control over the outputs on the RS-485 reader itself.

  This feature changes how reader expander outputs function at various addresses. Read Application Note 295: Enhanced Smart Reader Outputs in Protege GX before activating this option.

  This feature is not related to the smart readers that can be programmed in **Expanders | Smart readers**.

# Reader expanders | Reader 1/2 options

## Options

- **Invert floor relays**: When this option is enabled the PCB reader expander will invert all the relay outputs on the connected PCB output expanders that are used for elevator control. This option is not used for DIN rail modules.

  Elevator floor relay outputs can be inverted individually in **Programming | Outputs | Options**.
- **Control relays on comm failure**: When this option is enabled, a PCB output expander used for elevator control will control the state of the relay outputs when the expander goes offline. If not, the relay outputs will remain in the same state when the expander goes offline. This option is not used for DIN rail modules.
- **Relays activated in comm failure**: When **Control relays on comm failure** is enabled, by default the relay outputs will be turned off when the PCB output expander goes offline. Enable this option to turn the outputs on when the expander goes offline. This option is not used for DIN rail modules.
- **Disable red LED processing**: When this option is enabled the reader expander will not control the L2 output and it can be used for another function. This is useful when the reader is wired in single LED configuration and does not use the L2 output.

  This option is only relevant for readers in Wiegand configuration. For a similar function for RS-485 readers, see **Enable enhanced smart reader outputs** (**Reader 1/2** tab).

- **Disable green LED processing**: When this option is enabled the card reader's green LED will not be activated when the door is unlocked. When used with Wiegand readers, the reader expander will not control the L1 output and it can be used for another function.

  This feature is not available for smart readers.

- **Disable buzzer processing**: When this option is enabled the reader expander will not control the reader beeper. The reader will beep once when a card is read, but will not beep additional times to indicate access granted or denied. The BZ output can be used for another function.
- **Use programmed card expiry**: This is a legacy option that has no effect.

### Offline options

The options below determine the operation of the reader expander when it is offline with the controller. They have no effect on online behavior. Note that no events will be recorded while the expander is offline.

- **Door sense enabled**: When this option is enabled the reader expander will process door sense functions from input 1 (port 1) or 5 (port 2) while it is offline.
- **Bond sense input enabled**: When this option is enabled the reader expander will process bond sense functions from input 3 (port 1) or 7 (port 2) when it is offline.
- **REX enabled**: When this option is enabled the reader expander will process REX functions from input 2 (port 1) or 6 (port 2) when it is offline. This can be used to unlock the door without credentials when the expander is offline.
- **REN enabled**: When this option is enabled the reader expander will process REN functions from input 4 (port 1) or 8 (port 2) when it is offline. This can be used to unlock the door without credentials when the expander is offline.
- **Enable beam function on input 3/7**: When this option is enabled the reader expander will process beam sense functions from input 3 (port 1) or 7 (port 2) when it is offline. The **Door sense enabled** option must also be in use.
- **Invert door state control R1/R2**: With this option enabled the door sense input (input 1 or 5) will be inverted when the reader expander is offline.
- **Invert sense state control**: With this option enabled the bond sense input (input 3 or 7) will be inverted when the reader expander is offline.
- **Invert REX input**: With this option enabled the REX input (input 2 or 6) will be inverted when the reader expander is offline.
- **Invert REN input**: With this option enabled the REN input (input 4 or 8) will be inverted when the reader expander is offline.
- **Always allow REX**: When this option is enabled an offline reader expander will always process REX and unlock the door, even when the door is already open.

  For online operation, see the equivalent option in **Programming | Doors | Inputs**.

- **Recycle door open time on REX**: This is a legacy option that has no effect.

  For online operation, see the equivalent option in **Programming | Doors | Inputs**.

- **Forced door sends door open**: This is a legacy option that has no effect.

  For online operation, see the equivalent option in **Programming | Doors | Inputs**.

- **Recycle REX time**: This is a legacy option that has no effect.

  For online operation, see the equivalent option in **Programming | Doors | Inputs**.

## Reader expanders | Reader 1/2 PIMs

Panel Interface Modules (PIMs) and ENGAGE Gateways (GWEs) are used as the communication interface between wireless locks and Protege controllers for Allegion wireless locking integration. These tabs allow you to add and configure the PIMs and GWEs connected to the reader expander ports for the integration.

These tabs are only visible when the corresponding **Reader 1/2 Network Type** is set to Allegion. For more information and programming instructions, see Application Note 182: Allegion Integration with Protege GX.

### PIMs configuration

- **No.**: Name of the connected PIM.
- **PIM address**: The address of the PIM/GWE connected to the reader port.
- **APM start address**: This defines the value set for the Low APM Range of the PIM/GWE connected to the reader port, which determines the address of the first wireless lock assigned to the device.
- **Number of APM's**: Defines the number of wireless locks connected to the PIM/GWE.

  A maximum of 16 locks can be connected to a PIM. A maximum of 10 locks can be connected to a GWE.

## Manual Reader Expander Commands

Right clicking a reader expander record in **Expanders | Reader expanders** opens a menu with manual commands for that expander.

### Control

- **Update module**: Updates the programming in the reader expander. For more information, see Module Updates (page 291).
- **Activate OSDP install mode**: Select this command to put the reader expander into OSDP installation mode, allowing it to pair with any connected OSDP card readers which are also in installation mode. The reader expander and card reader will establish a shared encryption key to enable secure channel communication.

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

# Smart readers

Smart readers represent non-standard readers connected to the Protege GX system, allowing them to perform normal door control functions.

Alongside credential types, smart readers can be used to interpret a wide variety of custom data types being transmitted over the controller's onboard ethernet port. For example, in a license plate recognition integration each smart reader might represent a camera sending license plate data to the controller over the IP connection. For example, see Application Note 276: Configuring Credential Types in Protege GX.

In addition, smart readers can be associated with a reader expander's reader port, representing third-party modules connected to that port in RS-485 configuration. For example, when the reader expander's **Port 1/2 network type** is set to OSDP, two smart readers are automatically created to represent the entry and exit readers on that reader port. For more information and programming instructions, see Application Note 254: Configuring OSDP Readers in Protege.

Finally, smart readers are used in various third-party integrations for wireless locking devices, such as Allegion, Aperio, Salto SALLIS and VingCard Visionline. Each smart reader represents a single wireless lock. For more information and programming instructions, see the relevant application note.

Each smart reader is a licensed item (except for OSDP readers). The licenses required will vary depending on the type of third-party connection required. Contact ICT Customer Support for more information.

## Smart readers | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Expander address**: The address of the reader expander the smart reader is connected to.
- **Expander port**: The reader expander port that the smart reader is connected to. This may be a reader port, or the ethernet port on the controller's onboard reader expander.

  The **Port 1/2 network type** or **Ethernet network type** determines the function of the smart reader. For example, when connected to a reader port set to OSDP the smart reader will represent an OSDP reader connected via RS-485. When connected to an ethernet port set to Third party generic the smart reader will represent an IP reader such as a camera or barcode scanner.

  Smart readers cannot be connected to reader ports set to Wiegand operation.

- **Configured address**: The module address of the smart reader in the controller network. This may be required to correspond to a specific address provided by the third-party integration.

  For smart readers connected over the ethernet network, the command `SmartReaderPortOffset = true` may be entered in the reader expander programming. In this case the IP port used by the smart reader is determined by the **Ethernet port** (**Expanders | Reader expanders | General**) plus the **Configured address** here.

  The maximum configured address available for smart readers is 248.

- **Linked RSD address**: Used for Allegion wireless lock integrations to define the **PIM address** of the PIM record that the lock is linked to.

For more information and programming instructions, see Application Note 182: Allegion Integration with Protege GX.

### VingCard Visionline integration

- **VingCard Visionline door ID**: When this smart reader is used for VingCard Visionline integration, this field allows you to enter the ID of the lock which this smart reader will represent.

### Commands

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

### Record history

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

## Smart readers | Reader

Different options are available on this page depending on the type of smart reader being configured. Not all options are relevant for all integrations.

### Configuration

- **Reader one format**: The type of credential data received, determined by the third-party device or application. Commonly for smart readers the format is set to Custom credential, which represents a specific credential type:
  - For RS-485 connected smart readers the custom credential is determined by the credential type(s) set in the door type.
  - For ethernet connected smart readers the custom credential is set in the **Reader credential match types** field below.
- **Reader one location**: The location informs the smart reader whether the connected reader is installed at the entry or exit side of the door.
- **Reader one mode**: Each smart reader can be used for door access, elevator control or area control.
- **Reader one door**: When the **Reader one mode** is set to Access, this field sets the door that is controlled by this smart reader. The same door may be controlled by more than one smart reader or reader port (entry and exit).

  Any credential types required by the door type must be entered in the **Reader credential match types** field below.

- **Reader one keypad type**: If a PIN credential is required by the associated door type, this option allows you to set the type of PIN input that is used. ARK-501 and other PIN pad inputs must be connected to a reader port with the same **Reader 1/2 door** as the smart reader.

  When this option is set to LCD keypad the **Keypad to use for PINs reader 1** will request a PIN after the first credential is entered. The user can enter the PIN and then press either the **[FUNCTION]** key to unlock the door, or **[ENTER]** to log in to the keypad. For more information, see **Keypad login requires card** (**Expanders | Keypads | Options 2**).

  To unlock the door the user **must not press [ENTER]** after entering their PIN. The **[FUNCTION]** key must immediately follow the PIN code. If the user presses **[ENTER]** the keypad will log them in.

- **Keypad to use for PINs reader 1**: If the **Reader one keypad type** above is set to LCD keypad, this keypad will request a user PIN when the user enters their credentials.
- **Reader one arming mode**: The function set in this field allows users to arm and disarm areas or control a specific output or output group by entering their credentials. Users must enter the full credential sequence multiple times to activate the function.

- When the **Reader one mode** is set to Access the entry reader controls the **Area inside door** and the exit reader controls the **Area outside door** (set in **Programming | Doors | General**).
- When it is set to Area control the smart reader controls the **Reader one area control area** below.
- For output control the smart reader controls the **Reader one function output / output group**.

The user must have **Enable multi-badge arming** checked in **Users | Access levels | General** (regardless of whether the function is area or output control). If inputs in the area may be open, **Always force arm using card reader** may be enabled in **Programming | Areas | Options (2)**.

- **Reader one area control area**: When the **Reader one mode** is set to Area control, this field sets the area that is controlled by this smart reader.
- **Reader one elevator**: When the **Reader one mode** is set to Elevator, this field sets the elevator car that is controlled by this reader port.
- **Reader one secondary format**: The secondary reading format is used when the smart reader cannot decode a card read using the primary format. This option is useful for sites with multiple card types in use.
- **Reader one function output / output group**: This output or output group can be activated when the user enters their credentials at a card reader three times. The **Reader one arming mode** above must be set to either Toggle function output on 3 reads or Activate function output on 3 reads.

## Reader options

- **Allow reading opened/unlocked**: This option is not used. Doors connected to smart readers always allow reading when open or unlocked.
- **Door sense enabled**: This option is not used. The door sense is configured in **Programming | Doors | Inputs**.
- **Bond sense input enabled**: This option is not used. The bond sense is configured in **Programming | Doors | Inputs**.
- **REX enabled**: This option is not used. The REX input is configured in **Programming | Doors | Inputs**.
- **REN enabled**: This option is not used. The REN input is configured in **Programming | Doors | Inputs**.
- **Send format errors**: When this option is enabled the smart reader will send detailed information to the controller if it reads a card with a format error. Format errors include bit count, byte count, parity, checksum and LRC calculation failures. This information will appear in the event log.

The **Log reader events** option must also be enabled.

- **Intelligent reader tamper mode**: This option is not used.

## Card data options

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

For more information, see the relevant application note for your integration.

This field sets the encryption key for this wireless lock only.

- **Read non ICT programmed sector data**: Enabling this option allows the wireless lock to read card sector data not programmed by ICT; however, the lock will no longer read sector data programmed by ICT. This is used in the Salto SALLIS and Aperio integrations.

Do not enable this option if you require the lock to read both ICT programmed sector data and additional sector data.

## Misc options

- **Disarm area for door on access**: When this option is enabled the associated area will be automatically disarmed when a user enters valid credentials, provided the user has access to disarm the area. When the reader is used for door control the area behind the door will be disarmed. When the reader is used for area control the control area set above will be disarmed.
- **Allow access when area armed**: When this option is disabled (by default), users can be denied access to a door when the area behind it is armed. They will only be allowed access if they have the ability to disarm the area.

  This option can be enabled to allow users through any door they have access to regardless of the area status. Be aware that this can easily cause false alarms as users will be able to enter areas that they cannot disarm.
- **Disarm users area on valid card**: This option allows users to disarm a personal area or area group when they gain access at the reader. For example, this could be used to allow a single reader to service a row of personal offices which users can arm and disarm individually.

  The **User area** is set in **Users | Users | General**, or an area group can be set in the **Area groups** tab. The user must have this area available in **Users | Access levels | Disarming area groups**.

  This feature is not supported when the card reader is controlling an elevator car.
- **Log reader events**: Enable this option to allow the reader to send format error information to the controller (with the **Send format errors** option enabled above). Other reader events are always sent to the controller.
- **Swap lock LED display**: This option is not used.
- **Activate access level output**: When this option is enabled the output or output group assigned to the user's access level will be activated when the user gains access to the door.

  The outputs are assigned in the **Outputs** or **Output groups** tab of **Users | Access levels**. The **Reader access activates output** option must be enabled in **Users | Access levels | General**, and further configuration is available there.
- **Display card detail when invalid**: When this option is enabled, the raw data of any unrecognized credential will be saved to the event log. An operator can right click on the 'Read raw credential data' event to assign the credential to a user. The credential will automatically be assigned to the correct credential type based on the **Reader credential match types** programmed below.
- **Enable beam function on input 3**: This option is not used. You can set a beam input for the door in **Programming | Doors | Inputs**.
- **Always allow REX**: This option is not used. See the equivalent option in **Programming | Doors | Inputs**.
- **Recycle REX time**: This option is not used. See the equivalent option in **Programming | Doors | Inputs**.

## Reader credential match types

When configuring smart readers connected to the controller's ethernet port it is necessary to specify one or more credential types that the smart reader will use. This allows the controller to interpret the data received over the IP network.

If the **Reader one mode** is set to Access then the credential types set here should match those required by the door type. If it is set to Elevator or Area control, any of the credential types set here can be used to access the elevator or control the area.

Credential types can be programmed in **Sites | Credential types**.

# Visitor Menu

The Protege GX visitor management system (VMS) allows you to track and control visitor access on a site. It runs as a special version of the Protege GX client which manages visitor sign in and sign out.

In this menu you can configure the operation and appearance of the visitor management client, the requirements for the sign in process, which workstations will run the VMS, and the access cards that will be signed out to visitors.

The visitor management system is a licensed feature. For more information and full programming instructions, see Application Note 287: Protege GX Visitor Management System.

## Templates

The settings, content and visual design of the visitor management client are configured through a VMS template. Multiple VMS templates can be created and applied to different workstations, allowing you to adapt to the needs of different visitor sign in points on the same site.

For example, front reception and the warehouse entrance might require different details from visitors, or different offices on the same site might have different branding requirements.

### Templates | General

#### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

#### Record history

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

#### Configuration

- **Card template**: The design template used to print labels or cards for visitors. This is required for the visitor management system to function, and may include elements such as visitor details, credentials, a user photo, and bar code for quick sign out. Card templates can be programmed in **Users | Card template editor**.
- **Checkout mode**: Set what happens to the user record created for a visitor when they sign out of the VMS.
  - Disable user will remove the credential from the visitor's user record.
  - Delete user will delete the user record.

  Disabled visitors are not reactivated if they sign in to the VMS again: a duplicate record will be created. However, the visitor can be 'reactivated' by manually assigning them a credential in Protege GX.
- **Requires validation**: This option is not used.
- **Photo required**: With this option enabled the VMS will connect to a webcam or integrated camera to take a photo of the visitor during the sign-in process. This photo will be stored in the **Photo** tab of the user record, and may be printed on a visitor label with an appropriate card template.
- **Stretch photo to fill**: When this option is enabled, visitor photos will be stretched to fit the full space allotted in the card template. This will not preserve the aspect ratio, which may result in distorted images.
- **Download user to controllers**: This option must be enabled for correct operation of the VMS.

- **Show print dialogue**: If this setting is enabled the VMS will show a print dialogue, allowing the user to select a printer for the visitor label. If it is disabled, the computer's default printer will be used. This option is useful for testing as it allows you to cancel the printing of any labels.
- **Show maximize button**: When this option is enabled the VMS interface will include maximize, minimize and close buttons. The ICT logo will be displayed in the top left.
- **Maximize window**: Enabling this option ensures that the VMS window will be automatically maximized, regardless of the settings of the workstation.
- **Email exceptions**: This option is not used.

### Sign out

One or both of these options can be used.

- **Scan bar code**: The visitor will be required to scan a bar code on their printed label to sign out. Bar codes can be added to labels in the card template.
- **Select name from drop down**: The visitor will be prompted to select their name from a drop down menu to sign out.

## Templates | Pages

- **VMS pages**: Add additional custom pages to the VMS sign in process. These can include additional information or custom fields for input. VMS pages can be created in **Visitor | Pages**.

## Templates | Email

- **Operators**: All operators added to this section will receive emails whenever a visitor signs in using this VMS template.

  Automated email features in Protege GX require an SMTP mail server to be configured in **Global | Global settings | Email settings**. Each operator must have an email address entered under **Global | Operators**.

## Templates | Display

After you make changes to the VMS interface you must close and restart any open clients to implement the changes.

- **Images**: Select images for the background, logo, sign in/out buttons and advert images. Click the ellipsis **[...]** button to navigate instantly to **Visitor | Images** to add any required VMS images.
  - **Background image**: Displayed as the background for all screens in the VMS. This will override the **Background color** setting.
  - **Logo**: Displayed above the sign in/out buttons, horizontally centered.
  - **Sign in/out image**: Displayed above the text in the sign in/out buttons respectively.
  - **Advert image 1-4**: Displayed at the bottom of the VMS home screen. This option can be used to add up to four advertisement banners to the VMS interface. If multiple advert images are configured, the home page will cycle through the different images over time.
- **Colors**: Enter the desired color as a hex code, or click the ellipsis **[...]** button to open a color picker.

# Pages

The VMS page menu allows you to add additional pages to the sign in section of the VMS client. These pages can be used to request additional information from visitors and display important notices, such as health and safety warnings.

VMS pages can be added to a VMS template in the **Visitor | Templates | Pages** tab.

## Pages | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Note text

- **Note**: The text entered here will be displayed on this page of the VMS. This is useful for displaying important notices to visitors, such as health and safety policies, contact details and other site information.
- **Show acknowledgement button on the page**: When this option is enabled, visitors will be required to acknowledge that they have read the **Note** before they can proceed to sign in. This helps ensure compliance when people arrive on site.

### Record history

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

## Pages | Custom fields

### Fields

Adding custom fields to a VMS page allows you to request additional information from visitors as they arrive. This information will be saved to the user record that is created when the visitor completes the sign in process. Press **Add** to add custom fields.

The information entered in custom fields will not be saved to the visitor record unless the same field is included in a custom field tab. Ensure that each field has the **Custom field tab** set in **Users | Custom fields | General**.

# Workstations

VMS workstations are computers which can open the Protege GX visitor management client. When an operator logs in to the client on these workstations they are given the option to run the client as the VMS.

## Workstations | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

### Configuration

- **Computer name**: The name of the workstation that will run the VMS. This must be a computer with the Protege GX client installed. Typically this would be an entry station or reception PC.
- **Visitor management template**: This field sets the VMS template that will be used by this workstation. Each workstation can have a different VMS template.
- **User record group**: Any visitor records created by the VMS from this workstation will be automatically assigned to this record group. This is useful for finding, filtering and reporting on visitors on a site.

# Cards

Visitors signing in to the VMS will be assigned a card (or similar credential) from the pool of VMS cards created here. These should be spare credentials that are not assigned to any user. When the visitor signs out the VMS card will be unassigned and ready for use by another visitor.

VMS card records must be created even if physical credentials are not required, as the VMS will not allow any visitor to sign in without a VMS card available.

## Cards | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

### Facility/Card number

- **Facility number**: The facility or site number of this visitor card.
- **Card number**: The card number of this visitor card. It is useful to create a sequence of unique cards that will be assigned to visitors.

  VMS cards are assigned to visitors in the order that they are created, not in order by card number.
- **Card in use**: This is a read only field. The box is checked when this VMS card has been assigned to a visitor, and unchecked when the card is available for use.

# Images

VMS images allow you to personalize the look of the VMS to meet company branding requirements. You can add background images, central logos, sign in/out button icons and advertisement banners.

Images can be added to a VMS template in the **Visitor | Templates | Display** tab.

## Images | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Record history

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

### Image

- **Image**: To add an image, click the ellipsis **[...]** button in the lower right.
  - If the image is already stored on the network, select the ellipsis **[...]** beside **Path** to browse to the image. The image must be accessible from the server machine.
  - If the image does not yet exist set the **Image source** field to capture a new image. You can capture an image from a connected webcam, or from a Topaz signature pad.
  - When complete, click **Next**.

  You can then crop the image if required:
  - Adjust the dotted rectangle's size and position to include the section of the image you wish to keep. Check the **Aspect** option to fix the aspect ratio of the rectangle.
  - To crop the image, check the **Crop** checkbox.
  - Click **Ok**.

  The completed image will be displayed in the image box.

  Ensure that the image is stored on the server or another location that is accessible to all workstations that are running the VMS.

# Automation Menu

Advanced functions relating to control and building automation are found under the automation menu.

## Automation

Automations (also known as automation points) are digital 'switches' in the system which can be used to control outputs. Users can activate and deactivate automations from a keypad, making them a convenient way to control devices that need to be operated regularly. For example, an automation might be used to control outdoor lighting, irrigation or HVAC (heating, ventilation and air conditioning) systems.

Users can activate automations from a keypad by logging in and pressing **[MENU] [5] [5]**. Select an automation and press **[1]** to activate it for a set time, **[2]** to deactivate it and **[3]** to activate it indefinitely. It is also possible to view and control automations from the keypad's offline menu (see **Expanders | Keypads | Options 2**).

Automations are also used in the C-Bus integration to connect inputs and outputs to C-Bus groups. This allows inputs and outputs to control C-Bus groups and C-Bus groups to control outputs, fully integrating building security and automation systems.

For more information and full programming instructions, see Application Note 289: C-Bus Integration with Protege GX and Protege WX.

## Automation | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Keypad display name**: The name that will be downloaded to the controller. This will be displayed on the keypad and in reports by IP monitoring services. The keypad can only display the first 16 characters of the name, so it should concisely describe the physical location and function of the device.

### Configuration

- **Automation output time**: When the automation is activated, by pressing **[1]** on a keypad or by the C-Bus integration, it will remain on for this duration (in seconds). Any outputs activated by the automation will also turn off after this time.

  When this field is set to 0, the automation will remain on indefinitely and the output or output group will use the activation time set in its own programming.

  In the C-Bus integration, this option is only relevant in the case where a C-Bus group controls a Protege output.

- **Automation output / output group**: In normal operation, this output or output group is activated when the automation is activated from the keypad. It is deactivated when the automation is deactivated.

  In the C-Bus integration, this output or output group can either control the C-Bus group or be controlled by the C-Bus group. The usage depends on the **C-Bus automation output** setting in the **Options** tab.
- **C-Bus application code**: The address of the C-Bus application that the automation will communicate with. Application codes can be found in the C-Bus software or system documentation.
- **C-Bus group code**: The address of the C-Bus group that the automation will communicate with. Group codes can be found in the C-Bus software or system documentation.

- **C-Bus service**: The service used for communication between Protege GX and the C-Bus network interface. The service is configured in **Programming | Services** with the **Service type** set to C-Bus.

### Record history

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

## Automation | Options

### Options

- **Display inverted status**: This is a legacy option that has no effect.
- **Enable C-Bus automation functions**: When this option is enabled the automation controls or is controlled by the assigned C-Bus group.

  This option is required for the automation to begin communicating with C-Bus.
- **C-Bus automation output**: When this option is enabled this automation will control the assigned C-Bus group. When this option is disabled the automation will be controlled by the assigned C-Bus group.
- **Use output status in C-Bus function**: When this option is enabled the automation will change or transmit the status of its automation output or output group rather than the status of the automation itself.
- **C-Bus operates on rising edge**: C-Bus processing activates on the rising edge of a change in the output/input state, i.e. changing from off to on. If the option is disabled the C-Bus processing ignores these changes.
- **C-Bus operates on falling edge**: C-Bus processing activates on the falling edge of a change in the output/input state, i.e. changing from on to off. If the option is disabled the C-Bus processing ignores these changes.

# Programmable functions

Programmable functions are special automated processes that can be programmed in the system. Generally these processes have a trigger - such as an output turning on or a data value reaching a defined number - which causes the controller to activate the process.

These functions present an extensive variety of applications for control and automation. For example, you might use them to arm an area based on the state of an output, operate a complex series of devices each time a specific door is unlocked, adjust the temperature based on the number of people in an area, or unlock the doors in the event of a fire alarm.

For examples of advanced programming using programmable functions, see the following application notes:

- Application Note 208: Emergency Egress and Lockdown Programming
- Application Note 278: Access Level Area Counting in Protege GX
- Application Note 282: Programming Door Mechanisms in Protege GX
- Application Note 307: Programming a Man Down Switch in Protege GX
- Application Note 334: Programming Guard Tours in Protege GX

## Starting and Stopping Programmable Functions

Right clicking a programmable function record in **Automation | Programmable functions** opens a menu with manual commands for that programmable function.

### Control

- **Start**: Starts the programmable function on the controller. The process will run when the triggering conditions are met.
- **Stop**: Stops the programmable function on the controller. The controller will generate a health status message indicating that the function has been stopped.

Before you make changes to a programmable function you should first **stop** the function. When the changes have been downloaded to the controller you should **start** the function again. If this procedure is not followed the controller may not correctly implement the changes.

## Programmable functions | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Support manual commands**: When this option is enabled an operator with the appropriate permissions can right click on the programmable function to start or stop the process.

### Type

- **Type**: The type of programmable function determines what kind of operation it will perform. Each type of function has different programming tabs and options available.
  - **None**: The function will perform no action.
  - **Logic control**: Controls an output or output group based on the state of one or two triggering outputs. Several logical operations are available.
  - **Area control**: Arms or disarms an area or area group based on the state of an output.

- **Roof top heat pack**: Manages an HVAC system with up to 4 stages of heating and cooling and two stages of dehumidification.
- **Floor temping**: Manages an air tempering system with single-stage heating and cooling.
- **Value compare**: Compares two data values and activates outputs based on their relative quantities. For example, this can be used to control lighting circuits based on daylight sensor inputs.
- **Ripple output**: Activates a series of outputs in a ripple pattern based on a single triggering output. This can be used to stage large current devices and multiple lighting circuits.
- **Door control**: Locks or unlocks a door or door group based on the state of an output. Can also be used to initiate emergency egress or door lockdown.
- **Virtual door**: Enables defined inputs and outputs to act as a door without programming a door record. Useful for doors that do not have readers and are not monitored by a reader expander but require some door processing.
- **Input follows output**: Controls an input based on the state of an output. Can be used to activate alarms based on an output state.
- **Elevator control**: Locks or unlocks an elevator car or elevator group based on the state of an output.
- **Register counter**: Increments or decrements a data value based on the state of an input.
- **Average**: Calculates the average of up to 8 input data values and writes it to an output data value. For example, this can be used to take an average of multiple temperature sensors.
- **Variable output compare**: Compares a single input data value with a series of 'fixed point' data values. When the input value reaches each fixed point an output data value is updated with a known quantity.

- **Mode**: When this option is set to Normal the programmable function will run every time its triggering conditions are met. If the controller is restarted, the function will start again. When set to Run once only the programmable function will run once when its triggering conditions are met, then stop.
- **State**: This is a legacy option that has no effect.

## Record history

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

# Logic control

A logic control function evaluates the status of one or two outputs and applies a logical operation to control the state of another output or output group (called the control output). A range of logical programming is available including follow/inverted follow (with continuous and pulsed options), OR, AND, NOR, NAND and XOR.

## Configuration

- **Logic function mode**: This field determines the type of logical operation that will be used to control the state of the control output or output group.

  The control mode may be continuous (options 0-1, 6-10) or pulsed (options 2-5). Continuous control modes check the output state every 30 seconds. If the state is not correct the function reasserts control and turns the output on/off. Pulsed or edge triggered modes only change the output state when the triggering conditions are met, and do not affect it at other times.

  The available control options are:

  - **0 - Follow and test first output**: The control output continuously follows the state of the first output. When the first output is ON, the control output is ON. When the first output is OFF, the control output is OFF.
  - **1 - Inverted follow and test first output**: The control output continuously follows the state of the first output in an inverted manner. When the first output is ON, the control output is OFF. When the first output is OFF, the control output is ON.
  - **2 - Follow pulse on first output**: The control output follows the rising edge of the first output. When the first output turns ON, the control output turns ON.
  - **3 - Inverted follow pulse on first output**: The control output follows the rising edge of the first output in an inverted manner. When the first output turns ON, the control output turns OFF.
  - **4 - Follow pulse off first output**: The control output is activated on the falling edge of the first output. When the first output turns OFF, the control output turns ON.
  - **5 - Inverted follow pulse off first output**: The control output is deactivated on the falling edge of the first output. When the first output turns OFF, the control output turns OFF.
  - **6 - Follow logic OR**: The function performs a logical OR operation to determine the state of the control output. If either the first or second output is ON, the control output is ON. If both the first and second output are OFF, the control output is OFF.

    | First Output | Second Output | Control Output |
    |---|---|---|
    | ✓ | ✓ | ✓ |
    | ✓ | ✗ | ✓ |
    | ✗ | ✓ | ✓ |
    | ✗ | ✗ | ✗ |

  - **7 - Follow logic AND**: The function performs a logical AND operation to determine the state of the control output. If both the first and second output are ON, the control output is ON. If either the first or second output is OFF, the control output is OFF.

    | First Output | Second Output | Control Output |
    |---|---|---|
    | ✓ | ✓ | ✓ |
    | ✓ | ✗ | ✗ |
    | ✗ | ✓ | ✗ |

| First Output | Second Output | Control Output |
|---|---|---|
| ✗ | ✗ | ✗ |

- **8 - Follow logic NOR**: The function performs a logical NOR operation to determine the state of the control output. If either the first or second output is ON, the control output is OFF. If both the first and second output are OFF, the control output is ON.

| First Output | Second Output | Control Output |
|---|---|---|
| ✓ | ✓ | ✗ |
| ✓ | ✗ | ✗ |
| ✗ | ✓ | ✗ |
| ✗ | ✗ | ✓ |

- **9 - Follow logic NAND**: The function performs a logical NAND operation to determine the state of the control output. If both the first and second outputs are ON, the control output is OFF. If either the first or second output is OFF, the control output is ON.

| First Output | Second Output | Control Output |
|---|---|---|
| ✓ | ✓ | ✗ |
| ✓ | ✗ | ✓ |
| ✗ | ✓ | ✓ |
| ✗ | ✗ | ✓ |

- **10 - Follow logic XOR**: The function performs a logical XOR operation to determine the state of the control output. If both the first and second outputs are in the same state (both ON or both OFF), the control output is OFF. If the first and second outputs are in different states (one ON, one OFF), the control output is ON.

| First Output | Second Output | Control Output |
|---|---|---|
| ✓ | ✓ | ✗ |
| ✓ | ✗ | ✓ |
| ✗ | ✓ | ✓ |
| ✗ | ✗ | ✗ |

- **First output to check**: The first output that is used to set the control output state. This field must be set for all logic function modes.
- **Second output to check**: The second output that is used to set the control output state. This field is not required for logic function modes 0-5.
- **Output / Output group to control**: This output or output group is the control output for the logic control function. It is activated and deactivated based on the states of the first and second outputs and the **Logic function mode** selected above.

  If you set both an output and an output group, both will be controlled by the function.

# Area control

Area control programmable functions can arm and disarm an area or area group (called the control area) based on the state of an output. You can configure either continuous control (the function always checks the output state and maintains the area status) or pulse control (the function only controls the area status when the output changes state).

This can be used for applications such as arming an area after a period of inactivity or using a key switch to disarm an area.

## Configuration

- **Area function**: This field determines how the control area or area group will be controlled based on the state of the output.

  The control mode may be continuous (options 0-1) or pulsed (options 2-5). Continuous control modes check the area state every 30 seconds. If the state is not correct the function reasserts control and arms/disarms the area. Pulsed or edge triggered modes only change the area state when the triggering conditions are met, and do not affect it at other times.
  - **0 - Area follows output state**: The control area continuously follows the state of the output. When the output is ON, the control area is ARMED. When the output is OFF, the control area is DISARMED.
  - **1 - Area follows inverted output state**: The control area continuously follows the state of the output in an inverted manner. When the output is ON, the control area is DISARMED. When the output is OFF, the control area is ARMED.
  - **2 - Area arms on output turning on**: The control area is armed on the rising edge of the output state. When the output turns ON, the control area is ARMED.
  - **3 - Area disarms on output turning on**: The control area is disarmed on the rising edge of the output state. When the output turns ON, the control area is DISARMED.
  - **4 - Area arms on output turning off**: The control area is armed on the falling edge of the output state. When the output turns OFF, the control area is ARMED.
  - **5 - Area disarms on output turning off**: The control area is disarmed on the falling edge of the output state. When the output turns OFF, the control area is DISARMED.
- **Output to check**: The output that is used to set the control area state.
- **Area / Area group to control**: This area or area group is the control area for the programmable function. It is armed or disarmed based on the state of the **Output to check** and the **Area function** selected above.

  You can set either an area or an area group. If both are set only the area will be controlled by the function.

# Roof top heat pack

This programmable function type manages a roof top heat pack (RTHP) air conditioning system with up to four stages of heating and cooling and up to two stages of dehumidification. The function monitors the temperature and humidity (via analog input channels) and activates the heating, cooling and dehumidifying outputs of the air conditioning unit to achieve the set point temperature and humidity.

Each programmable function of this type can manage the entire air conditioning system for a building. You can program multiple versions of this function that run under certain conditions. For example, you might have alternative functions for day and night based on the building's expected occupancy schedule. Effective programming can significantly increase the building's energy efficiency.

Programming this feature requires understanding of multi-stage HVAC systems.

## Configuration

- **Cooling stage**: The number of cooling stages managed by the RTHP.
- **Heating stage**: The number of heating stages managed by the RTHP.
- **Dehumid stage**: The number of dehumidification stages managed by the RTHP. Only 1 or 2 stage dehumidification can be programmed.
- **Always drive fan (circulate)**: When this option is enabled the **Main fan output / output group** will always be activated to circulate air.
- **Fire fast stage off**: When this option is enabled, during a fire condition the RTHP will quickly shut down to prevent smoke from circulating. This occurs when the **Fire control output input** is activated.
- **Fault fast stage off**: When this option is enabled, during a fault condition the RTHP will quickly shut down. This occurs when the **Fault output input** is enabled.
- **Cooling inter stage delay**: When the RTHP is stepping up the cooling from stage 1 to 4, this is the delay (in seconds) between the activation of each stage.
- **Heating inter stage delay**: When the RTHP is stepping up the heating from stage 1 to 4, this is the delay (in seconds) between the activation of each stage.
- **Dehumidification inter stage delay**: When the RTHP is stepping up the dehumidification from stage 1 to 2, this is the delay (in seconds) between the activation of each stage.
- **Economiser damper stage delay**: The delay (in seconds) before the economizer (damper) is activated.
- **Fresh air cooling time**: The length of time that the system will attempt to use fresh air for cooling. If the cooling set point is not reached within this time, regular cooling will be activated.
- **Cooling inter stage off delay**: When the RTHP is stepping down the cooling from stage 4 to 1, this is the delay (in seconds) between the deactivation of each stage.
- **Heating inter stage off delay**: When the RTHP is stepping down the heating from stage 4 to 1, this is the delay (in seconds) between the deactivation of each stage.
- **Dehumidification inter stage off delay**: When the RTHP is stepping down the dehumidification from stage 2 to 1, this is the delay (in seconds) between the deactivation of each stage.

## Data variables

- **Heat set point data value**: This data value determines the temperature that the RTHP will heat the space to. It is compared to the **Space temperature data variable register** to see whether heating is required.
- **Cool set point data value**: This data value determines the temperature that the RTHP will cool the space to. It is compared to the **Space temperature data variable register** to see whether cooling is required.
- **Humidity set point data value**: This data value determines the humidity level which will trigger the RTHP to begin decreasing the humidity. The current humidity value is determined by the **Space humidity data variable register**.
- **Heat hysteresis data value**: This data value is added to the **Heat set point data value** to define an acceptable range of heating. This allows the heating to drive slightly beyond the set point (hysteresis), preventing it from oscillating between the dead band and heating modes.

- **Cool hysteresis data value**: This data value is added to the **Cool set point data value** to define an acceptable range of cooling. This allows the cooling to drive slightly beyond the set point (hysteresis), preventing it from oscillating between the dead band and cooling modes.
- **Humidity hysteresis data value**: This data value is subtracted from or added to the **Humidity set point data value**, depending on whether the humidity has already exceeded the set point. This allows the dehumidification process to operate only when the humidity is a defined level above the set point, and to drive dehumidification below the set point, avoiding oscillation.
- **Warm up set point data value**: If the warm up set point is not equal to 0 the system will check the internal temperature against the warm up set point when the RTHP starts up. If the internal temperature is below the warm up set point the system will close the fresh air damper and drive the heating to achieve the heating set point in the shortest possible time. Once the heating set point is reached the unit will operate in a normal mode.
- **Fresh set point data value**: If the fresh air cooling set point is not 0 the system will check the fresh air temperature when a cooling demand exists and modulate the dampers to allow free cooling. The system will remain in the free cooling mode for the time set by the **Fresh air cooling time**.
- **Stage 1-4 demand data value**: The demand data values are used to calculate which stage of heating or cooling is required. The current **Output error data value** is compared to each value to determine the level of heating or cooling required. For example, if the plant error exceeds the stage 3 demand value the RTHP will activate the third stage of cooling or heating.
- **Current mode data value**: This data value is set by the function to allow you to monitor the current status of the RTHP system. You can associate the data value with a variable, view the variable on a floor plan or status page, and compare the value with the status table (see next page) to determine the current status of the RTHP system.
- **Plant error data value**: The plant error is the difference between the current temperature (**Space temperature data variable register**) and the heating or cooling set point value. The function writes to this data value as the temperature changes, and uses it to calculate the **Output error**. This data value can be associated with a variable and displayed on a floor plan for use in tuning the heating, cooling and demand set points.
- **Output error data value**: The output error is the result of a custom PID loop calculation. It is derived from the plant error and calculated integral terms. This is compared to the demand set points to determine what stage of heating or cooling is required.
- **Damper fresh set data value**: This field sets the default value of the **Economiser damper data variable register** below. This defines the normal position of the economizer damper when the RTHP is in neither warm up or free cooling mode. The damper position determines the volume of fresh air that is drawn into the building.
- **Space humidity data variable register**: This data value records the current humidity inside the space controlled by the RTHP. The value is updated by a humidity sensor connected to an analog input channel.
- **Space temperature data variable register**: This data value records the current temperature inside the space controlled by the air conditioner. The value is updated by a thermometer connected to an analog input channel.
- **Fresh air temperature data variable register**: This data value records the current temperature of the fresh air outside the space controlled by the air conditioner. The value is updated by a thermometer connected to an analog input channel, typically located in the fresh air intake. If the outside temperature is cool enough the economizer damper may be opened to allow fresh air to cool the building.
- **Economiser damper data variable register**: This data value controls the fresh air damper position. This data value is connected to an analog output channel which controls the physical damper. The default value is the **Damper fresh set data value** above.

  When cooling is required and the fresh air outside is cool the damper opens to allow fresh air to enter the system. When the system requires heating or the air outside is warm the damper closes to limit the flow of fresh air.

## Roof top heat pack | Outputs

### Main fan

- **Main fan output / output group**: This output is used to control the fans in the air conditioning system. It is activated 30 seconds before the RTHP begins any heating, cooling or dehumidification process.

### Enabled

- **Enabled output input**: This output is monitored by the function. When this output is on, this function will run and control the RTHP system. When this output is off, the function will not run.

  For example, this output could be tied to a schedule so that the RTHP only runs when the building is occupied. A separate function can be run at times when the building is not occupied.

  If there is no output set this function will run continuously.

### Fault

- **Fault output input**: This output is monitored by the function and should be used to indicate when there is a fault in the RTHP system. If **Fault fast stage off** is enabled, when this output is activated the RTHP will shut down in the shortest possible time to prevent damage to the system.

### Fire control

- **Fire control output input**: This output is monitored by the function and should be used to indicate when there is a fire in the building. If **Fire fast stage off** is enabled, when this output is activated the RTHP will shut down and halt air conditioning until the fire alarm has been cleared.

### Cool stage

- **Cool stage one-four output / output group**: These outputs and output groups are used to control each cooling stage of the RTHP system. For example, when the second cooling stage is required the **Cool stage two output / output group** is activated.

### Heat stage

- **Heat stage one-four output / output group**: These outputs and output groups are used to control each heating stage of the RTHP system. For example, when the second heating stage is required the **Heat stage two output / output group** is activated.

### Dehumidification stage

- **Dehumidification stage one-two output / output group**: These outputs and output groups are used to control each dehumidification stage of the RTHP system. For example, when the second dehumidification stage is required the **Dehumidification stage two output / output group** is activated. These are typically connected to hot gas reheat valves located in the RTHP unit.

## Roof Top Heat Pack Status

The value of the **Current mode data value** (**Roof top heat pack** tab) indicates the current status of the RTHP system. To monitor the system status associate a variable with this data value and view it on a floor plan or status page.

| Value | Status | Description |
|---|---|---|
| 0 | RTHP Idle Condition | The programmable function is stopped and no processing is taking place. |

| Value | Status | Description |
|---|---|---|
| 1 | RTHP Waiting for Start Signal | The **Enabled output input** is not activated. The function is idle. |
| 2 | RTHP Warm up Check | If the RTHP is programmed to enter a warm up state at the start of operation, it first checks the temperature to verify if the current internal temperature is lower than the warm up set point. If it is, the RTHP will enter the warm up mode. |
| 3 | RTHP Warm up Space | When in warm up mode the RTHP is driven to full capacity to get the space above the heating set point in the fastest possible time. Once the temperature reaches this level the system will operate normally. |
| 4 | RTHP Dead Band Process | No heating, cooling or dehumidification is required. The RTHP will wait for a condition that is outside the set points. |
| 5 | On Call for Space Heating | The space temperature is below the heating set point and the function to start the heating process is active. This will activate the stages required to bring the temperature up to the heating set point. |
| 6 | On Call for Space Cooling | The space temperature is above the cooling set point and the function to start the cooling process is active. This will activate the stages required to bring the temperature down to the cooling set point. |
| 7 | On Call for Fresh Air Space Cooling | The space temperature is above the cooling set point and the outside air is below the free air cooling set point. The RTHP will oscillate the fresh air economizer to cool the space using the fresh air intake. This will remain active until the temperature is below the cooling set point. If free cooling fails to achieve the set point within the **Fresh air cooling time** mode 6 will be entered. |
| 8 | Heating Stage off | Heating stages are being turned off progressively due to the set point being reached. |
| 9 | Cooling Stage off | Cooling stages are being turned off progressively due to the set point being reached. |
| 10 | Dehumidification Cooling plus Reheat | Dehumidification is required and the current set point is above the cooling set point. The dehumidification stage will be activated to reduce the humidity. |
| 11 | Dehumidification Transition | The dehumidification process is in transition between the dehumidification requirements and cooling. |
| 12 | Dehumidification Heating | Dehumidification is required and the current set point is below the heating set point. The dehumidification stage will be activated to reduce the humidity, along with a heating stage. |
| 13 | Dehumidification Heating Stage off | Dehumidification and heating stages are deactivated because the humidity has come under control or the cooling set point (other side of the dead band setting) has been reached. |
| 14 | Dehumidification Cooling Stage off | Dehumidification and cooling stages are deactivated because the humidity has been reduced or the heating set point (other side of the dead band setting) has been reached. |
| 15 | Dehumidification Stage off | Dehumidification stages are deactivated because the humidity has reached the set point and dehumidification is no longer required. |
| 16 | RTHP Shutting Down | The RTHP is completing an orderly shutdown of the currently activated stages and the fan controls. |
| 17 | Fault Condition | A fault condition has activated and caused the RTHP to shut down. |
| 18 | Fire Condition | A fire alarm condition has been activated and caused the RTHP to shut down. |

# Floor temping

This type of programmable function is used to manage a floor temping (or air tempering) system with single stage heating and cooling. The function uses duct and floor temperature inputs, and can manage forward and reverse fan modes.

## Outputs

- **Duct fan output / output group**: This output or output group is used to enable the duct fan. It is activated 30 seconds prior to any heating or cooling.

  The direction of the fan (forward or reverse) is determined by the fan forward and fan reverse outputs below. If a 'fan on' signal is not required the forward and reverse outputs should be used to drive the appropriate contactors.
- **Output to enable this function**: This output is monitored by the function. When this output is on, this function will run and control the tempering system. When this output is off, the function will not run.

  For example, this output could be tied to a schedule so that the tempering system only runs when the building is occupied. A separate function can be run at times when the building is not occupied.

  If there is no output set this function will run continuously.
- **Output to enable fault shutdown**: This output is monitored by the function and should be used to indicate when there is a fault in the tempering system. When this output is activated the tempering system will shut down in the shortest possible time to prevent damage to the system.
- **Output to enable fire shutdown**: This output is monitored by the function and should be used to indicate when there is a fire in the building. When this output is activated the tempering system will shut down and halt air conditioning until the fire alarm has been cleared.
- **Cooling output / output group**: This output or output group is activated when there is a requirement for active cooling. If the tempering system does not have a cooling compressor, do not set this field.
- **Heating output / output group**: This output or output group is activated when there is a requirement for active heating. It is activated in the forward direction only.
- **Fan forward output / output group**: This output or output group is used to drive the fan in the forward direction. When the temperature at the floor is below the set point the forward fan is used to circulate air from the intake through the heating element and towards the floor.
- **Fan reverse output / output group**: This output or output group is used to drive the fan in the reverse direction. When the temperature at the floor is above the set point the reverse fan is used to circulate warm air from the floor out through the intake.
- **Output to control manual heating**: This output is monitored by the function. When it is activated, the fan will operate in forward (heating) mode regardless of the floor temperature.

  If both the manual heating and manual cooling outputs are activated the fan will operate in forward mode.
- **Output to control manual cooling**: This output is monitored by the function. When it is activated, the fan will operate in reverse (cooling) mode regardless of the floor temperature.

  If both the manual heating and manual cooling outputs are activated the fan will operate in forward mode.

## Data variables

- **Floor temperature input data variable output**: This data value records the current temperature at the floor level. The value is updated by a thermometer connected to an analog input channel.
- **Duct temperature input data variable output**: This data value records the current temperature at the duct level. The value is updated by a thermometer connected to an analog input channel. This is typically located in the duct downstream of the duct fan (in forward mode).
- **Floor set point data value**: This data value determines the desired temperature at the floor level. This value is compared to the floor temperature to determine whether heating or cooling is needed, and the direction of the fan.

- **Floor hysteresis data value**: This data value is added to or subtracted from the **Floor set point data value** to define an acceptable range of heating or cooling. This allows the tempering to drive slightly beyond the set point (hysteresis), preventing it from oscillating between different modes.
- **Duct set point data value**: This data value sets the maximum temperature for the duct sensor. It is compared to the duct temperature to control the heating of the duct air.
- **Duct hysteresis data value**: This data value is added to the **Duct set point data value** to define an acceptable range of heating. This allows the tempering to drive slightly beyond the set point (hysteresis), preventing it from oscillating between different modes.
- **Current mode data value**: This data value is set by the function to allow you to monitor the current status of the tempering system. You can associate the data value with a variable, view the variable on a floor plan or status page, and compare the value with the status table (see below) to determine the current status of the tempering system.

## Floor Temping Status

The value of the **Current mode data value** indicates the current status of the tempering system. To monitor the system status associate a variable with this data value and view it on a floor plan or status page.

| Value | Status | Description |
|---|---|---|
| 0 | Floor Temping Idle Condition | The programmable function is stopped and no processing is taking place. |
| 1 | Floor Temping Waiting for Start Signal | The **Output to enable this function** is not activated. The function is idle. |
| 2 | Floor Temping Waiting Check | The floor tempering is checking whether it is required to operate in a manual or automatic mode. |
| 3 | Floor Temping Dead Band Process | No heating or cooling is required. The tempering system will wait for a condition that is outside the set points. |
| 4 | Floor Heating | The floor temperature is below the set point and the heating process is active. This will activate the forward fan and heater that is required to bring the temperature up to the floor set point. |
| 5 | Floor Cooling | The floor temperature is above the set point and the cooling process is active. This will activate the reverse fan and (if applicable) the cooling compressor to bring the temperature below the set point. |
| 6 | Manual Heating Forward | The manual heating output is activated and the tempering system is in heating mode, regardless of the floor temperature. |
| 7 | Manual Cooling Reverse | The manual cooling output is activated and the tempering system is in cooling mode, regardless of the floor temperature. |
| 8 | Floor Temping Shutting Down | The tempering system is completing an orderly shutdown of the currently activated outputs and the fan controls. |
| 9 | Fault Condition | A fault condition has activated and caused the tempering system to shut down. |
| 10 | Fire Condition | A fire alarm condition has been activated and caused the tempering system to shut down. |
| 11 | Mode Delay | The mode has changed from manual to auto mode or vice versa and the function has entered a delay period. |

# Value compare

This type of programmable function allows you to compare two data values (an input value and a set point value) and activate outputs when one is higher or lower than the other. This could be used to activate lighting circuits based on daylight sensors or activate specific outputs depending on the number of users in an area.

## Configuration

- **Output to enable this function**: When this output is on the function will compare the values and activate the resulting outputs. When this output is off the value compare function will not run. If no output is set here the function will always run.
- **Activate output / output group when above set point**: The high output or output group is activated when the input data value is higher than the set point data value (once the hysteresis settings have been accounted for). It is deactivated when the input data value is equal to or below the set point.
- **Activate output / output group when below set point**: The low output or output group is activated when the input data value is lower than the set point data value (once the hysteresis settings have been accounted for). It is deactivated when the input data value is equal to or above the set point.
- **Analog input data variable register**: This data value is the variable input value that is being compared. It may be drawn from an analog input channel measuring a quantity such as temperature, current or light.
- **Hysterisis timer**: This option is not used.
- **Set point data value**: This data value is the set point that the variable input value is being compared to.
- **Hysteresis data value**: This fixed data value is added to and subtracted from the set point to define a range of values. The high and low outputs are only activated when the input value is outside this range. For example, when monitoring current this can be used to define a band of acceptable currents, so that the outputs will only be activated when the current spikes outside this band.
- **Hysteresis time data value**: This data value defines a delay time (in 500 millisecond intervals) before the function will react to any state changes. If a change in the input value triggers an output change it will not occur until this period has elapsed. Multiple output changes will be spaced out by the same interval. If the input value returns to acceptable limits within this time the outputs will not change.

  For example, the hysteresis time data value may be set to 10, i.e. 5 seconds (using the **Preset value** option). If the input value changes from a low value to a high value, after 5 seconds the low output will be deactivated. After an additional 5 seconds the high output will be activated. However, if the input value returns to a low quantity within 5 seconds neither output will change.

# Ripple output

This programmable function ripples a series of outputs on or off when a triggering output changes state. It is ideal for staging large current devices or multiple lighting circuits.

## Configuration

- **Output to enable this function**: When this output is activated the function activates the controlled outputs in sequence (step up). When this output is deactivated the function deactivates the controlled outputs in sequence (step down).
- **Stage 1-8 output / output group**: These fields define up to 8 outputs or output groups that are controlled by this function. When the **Output to enable this function** is activated the function turns these outputs on in sequence from 1 to 8, separated by the **Inter stage on ripple time**. When the **Output to enable this function** is deactivated the function turns these output off in reverse sequence from 8 to 1, separated by the **Inter stage off ripple time**.
- **Inter stage on ripple time**: When the controlled outputs are being stepped up, this is the delay between each output activation (in seconds).
- **Inter stage off ripple time**: When the controlled outputs are being stepped down, this is the delay between each output deactivation (in seconds).

# Door control

The door control programmable function allows you to lock and unlock a door or door group based on the status of an output. It is also used for implementing fire drop (emergency egress) and lockdown states on a door or door group.

## Configuration

- **Door function mode**: This field determines how the door or door group will respond to the output status, i.e. whether the output turns the chosen door control mode on or off. This relationship between the output status and the door control function is referred to as the trigger.

  For example, with the setting 4 - Follow pulse off output the trigger is activated when the output turns OFF. When the trigger is activated, the door might unlock, latch unlock, fire unlock or lock down depending on the door control mode. When the trigger is deactivated the door might lock or clear lockdown.

  The door function may be continuous (options 0-1) or pulsed (options 2-5). Continuous control modes check the door state every 30 seconds. If the state is not correct the function reasserts control and updates the door state. Pulsed or edge triggered modes only change the door state when the triggering conditions are met, and do not affect it at other times.

  The options are:

  - **0 - Follow and test output**: The door continuously follows the state of the output. When the output is ON, the trigger is ON. When the output is OFF, the trigger is OFF.
  - **1 - Inverted follow and test output**: The door continuously follows the state of the output in an inverted manner. When the output is ON, the trigger is OFF. When the output is OFF, the trigger is ON.
  - **2 - Follow pulse on output**: The door follows the rising edge of the output status. When the output turns ON, the trigger turns ON.
  - **3 - Inverted follow pulse on output**: The door follows the rising edge of the output status in an inverted manner. When the output turns ON, the trigger turns OFF.
  - **4 - Follow pulse off output**: The door follows the falling edge of the output status. When the output turns OFF, the trigger turns ON.
  - **5 - Inverted follow pulse off output**: The door follows the falling edge of the output status in an inverted manner. When the output turns OFF, the trigger turns OFF.
- **Door control mode**: This field defines what action the door or door group takes when the trigger is activated or deactivated.
  - **0 - Emulate unlock menu**: When the trigger is activated the door will be unlocked for the duration of the **Lock activation time** (**Programming | Doors | Outputs**). This has the same effect as unlocking the door via REX or credential. When the trigger is deactivated the door is locked.

    The door only unlocks temporarily even when the **Door function mode** is set to a continuous mode.
  - **1 - Latch door unlock**: When the trigger is activated the door will be latch unlocked. When the trigger is deactivated the door will be locked.
  - **2 - Fire control door unlock**: When the trigger is activated the door will be latch unlocked indefinitely. This command overrides other features that might be holding the door locked, such as area status. When the trigger is deactivated the door will return to its previous state.
  - **3 - Door lockdown (deny entry + exit)**: When the trigger is activated the door will be locked down and deny access to all users in both directions. When the trigger is deactivated the lockdown will be cleared and the door will return to its previous state.
  - **4 - Door lockdown (allow entry)**: When the trigger is activated the door will be locked down. Access will be allowed in the entry direction only (including REN). When the trigger is deactivated the lockdown will be cleared and the door will return to its previous state.
  - **5 - Door lockdown (allow exit)**: When the trigger is activated the door will be locked down. Access will be allowed in the exit direction only (including REX). When the trigger is deactivated the lockdown will be cleared and the door will return to its previous state.

- **6 - Door lockdown (allow entry + exit)**: When the trigger is activated the door will be locked down. Access will be allowed in both directions (including REX and REN). When the trigger is deactivated the lockdown will be cleared and the door will return to its previous state.

- **Output to check**: This output is used to control the door or door group. The relationship between the output and the door status is determined by the **Door function mode** above.
- **Door / Door group to control**: This door or door group is controlled by the programmable function. If both a door and door group are selected only the door will be controlled.

# Virtual door

This function enables you to set up defined inputs and outputs to operate like a door. This is useful when some aspects of door processing are required but no readers or reader expander ports are available. For example, roller doors with no readers may require locks, a REX button and left open monitoring. It is also possible to link a virtual door to a regular one, allowing two doors to be controlled from the same reader.

**Note**: Another way of achieving the same effect is creating a door record that is not associated with any reader expander. By that method most of the features of regular doors are available, while the programmable function method is more limited. However, the alternative method requires a door license for each new door record.

## Configuration

- **Request to exit input**: When this input is opened a REX (request to exit) is sent to the virtual door. This causes the programmable function to activate the lock output and grant access.

  The programmable function inverts the REX input by default. Therefore, the **Contact type** in **Programming | Inputs | Options** should be set to the opposite of the physical wiring. If the REX input is wired normally open the **Contact type** should be set to Normally closed. If the REX input is wired normally closed, it should be set to Normally open.

- **Door state input**: This input represents the door contact or door position input for the virtual door. When the input is opened, the door is considered open. When the input is closed, the door is considered closed.
- **Door left open input to control**: This input is opened when the door has been left open for too long (as defined by the **Max open time** below). It can be programmed with an area and input type to allow it to report door left open events from the virtual door (in place of the trouble input available on a regular door).

  A virtual input should be used for this purpose rather than a physical one.

- **Forced door input to control**: This input is opened when the door is forced open. It can be programmed with an area and input type to allow it to report door forced events from the virtual door (in place of the trouble input available on a regular door).

  A virtual input should be used for this purpose rather than a physical one.

- **Unlock time**: The duration (in seconds) that the lock will be activated when the virtual door is unlocked.
- **Max open time**: The duration (in seconds) that the virtual door can be open before it enters a left open state.
- **Lock output / output group**: This output or output group controls the physical lock for the door.
- **Alarm output / output group**: This output or output group is activated when the virtual door enters a left open or forced condition. This should be a beeper or other audible/visible output that can warn users to close the door. It is deactivated when the door is closed.

  The required **Activate alarm output** options must be enabled below.

- **Activate alarm output on door left open**: When this option is enabled the **Alarm output / output group** will be activated when the door is left open too long.
- **Pulse alarm output on door left open**: By default, the alarm output is activated continuously while the door is left open. When this option is enabled it will pulse on and off in 5 seconds intervals.

  **Activate alarm output on door left open** must also be enabled.

- **Activate alarm output on door forced**: When this option is enabled the **Alarm output / output group** will be activated when the door is forced open.
- **Pulse alarm output on door forced**: By default, the alarm output is activated continuously while the door is forced open. When this option is enabled it will pulse on and off in 5 seconds intervals.

  **Activate alarm output on door forced** must also be enabled.

- **Log door left open input event**: With this option enabled the system logs 'Input Opened' and 'Input Closed' events for the **Door left open input to control** when the virtual door is left open too long. Disable this setting to suppress the input events.
- **Log door forced input event**: With this option enabled the system logs 'Input Opened' and 'Input Closed' events for the **Forced door input to control** when the virtual door is forced open. Disable this setting to suppress the input events.
- **Link to door**: This option allows you to associate the virtual door with a regular door. Whenever the regular door is unlocked by access, a keypad or an operator, the virtual door is also unlocked. Whenever the virtual door is unlocked by REX the regular door is also unlocked. This allows two doors to be controlled from a single reader.

# Input follows output

This function allows an input to be triggered by an output. This is useful for generating alarms based on the state of an output rather than a physical input.

## Configuration

- **Input follows output**: This control input is opened when the **Output to follow** is activated, and closed when the output is deactivated. By programming the input into an area with an input type it can be used for alarm reporting.

  A virtual input should be used rather than a physical one.

- **Output to follow**: This output is monitored by the function and controls the state of the control input. This can be set to any physical or virtual output that should trigger an alarm state.
- **Log input events**: When this option is enabled an event will be generated whenever the input changes state due to this programmable function. When this option is disabled no events will be generated.

# Elevator control

This type of programmable function is used to lock and unlock floors in a specific elevator group based on the state of an output. It is also used to implement the fire drop (emergency egress) state on floors.

## Configuration

- **Elevator function mode**: This field determines how the floor group will respond to the output status, i.e. whether the output turns the chosen elevator control mode on or off. This relationship between the output status and the elevator control function is referred to as the trigger.

  For example, with the setting 4 - Follow pulse off output the trigger is activated when the output turns OFF. When the trigger is activated the floors might unlock, latch unlock or fire unlock depending on the **Elevator control mode**. When the trigger is deactivated the floors will lock.

  The control mode may be continuous (options 0-1) or pulsed (options 2-5). Continuous control modes check the floor state every 30 seconds. If the state is not correct the function reasserts control and updates the floor state. Pulsed or edge triggered modes only change the floor state when the triggering conditions are met, and do not affect it at other times.

  The options are:

  - **0 - Follow and test output**: The floors continuously follow the state of the output. When the output is ON, the trigger is ON. When the output is OFF, the trigger is OFF.
  - **1 - Inverted follow and test output**: The floors continuously follow the state of the output in an inverted manner. When the output is ON, the trigger is OFF. When the output is OFF, the trigger is ON.
  - **2 - Follow pulse on output**: The floors follow the rising edge of the output status. When the output turns ON, the trigger turns ON.
  - **3 - Inverted follow pulse on output**: The floors follow the rising edge of the output status in an inverted manner. When the output turns ON, the trigger turns OFF.
  - **4 - Follow pulse off output**: The floors follow the falling edge of the output status. When the output turns OFF, the trigger turns ON.
  - **5 - Inverted follow pulse off output**: The floors follow the falling edge of the output status. When the output turns OFF, the trigger turns OFF.
- **Elevator control mode**: This field defines what action the floor group takes when the trigger is activated or deactivated.
  - **0 - Emulate unlock menu**: When the trigger is activated the floor group will be unlocked for the duration of the **Token time** (below). When the trigger is deactivated the floor group is locked.

    The floor group only unlocks temporarily even when the **Elevator function mode** is set to a continuous following mode.
  - **1 - Latch elevator unlock**: When the trigger is activated the floor group will be latch unlocked. When the trigger is deactivated the floor group will be locked.
  - **2 - Fire control elevator unlock**: When the trigger is activated the floor group will be latch unlocked indefinitely. This command overrides other features that might be holding the floors locked, such as area status. When the trigger is deactivated the floor group will return to its previous state.
- **Output to check**: This output is used to control the floor group. The relationship between the output and the floor status is determined by the **Door function mode** above.
- **Elevator group**: The floor group controlled by this function will be locked/unlocked from the elevator cars in this elevator group. For example, a programmable function might be used to latch unlock the floors in the public elevators but not the maintenance elevators.
- **Floor group**: The floors that will be controlled by this function.
- **Token time**: If the **Elevator control mode** is set to 0 - Emulate unlock menu the floors will be unlocked for this length of time (in seconds) when the trigger is activated.

# Register counter

The register counter function is used to increment or decrement a data value based on the state of an input. For example, you might set up a data value recording how many times a door contact is opened to estimate the total number of people passing through over certain period.

## Configuration

- **Input to count**: This input is monitored by the programmable function. When the input changes state the counter is incremented or decremented.

  To count activations of an output or other features, this function could be paired with an input follows output programmable function to trigger the required input activations.

- **Counter register**: This data value is incremented or decremented by the function based on the options set below.

  The counter data value can store a maximum value of 65535. Each time the count exceeds this value the **Overflow register** is incremented by 1. Therefore, the total count can be calculated as: Total = Counter + (Overflow x 65535).

- **Overflow register**: This data value is incremented by 1 each time the counter data value overflows. Each 1 in the overflow data value represents a count of 65535.
- **Increment on input open**: When this option is enabled the counter will increment whenever the input opens.
- **Increment on input close**: When this option is enabled the counter will increment whenever the input closes.
- **Log counter events:** When enabled the function will log an event for every increment.
- **Decrement on input open**: When this option is enabled the counter will decrement whenever the input opens.

  The data value cannot store negative values. If the count drops below zero the count will 'wrap around' to 65535.

- **Decrement on input close**: When this option is enabled the counter will decrement whenever the input closes.

  The data value cannot store negative values. If the count drops below zero the count will 'wrap around' to 65535.

- **No overflow on register**: When this option is enabled the counter data value will not overflow into the overflow data value. This means that the count has a maximum total of 65535.
- **Reset output**: When this output is activated the counter and overflow data values are set to zero. When this occurs an event is logged with the total count.

  For example, to log a weekly total for a data value you could create a virtual output with an **Activation schedule** that causes it to activate once a week.

# Average

This programmable function takes the average of up to eight input data values and writes this number to an output data value. For example, this function could be used to monitor a room with multiple temperature sensors, where the average is used to determine the desired heating or cooling.

## Configuration

- **Update time**: The length of time (in seconds) between updates to the output data value.
- **Output**: The data value that the average will be written to.

  The output of this function is always a whole number, and will be rounded up or down as necessary.

- **Average 1-8**: The input data values that are used to calculate the average.

# Variable output compare

This type of function allows you to compare an input data value to a series of set points and set a specific output data value depending on the result. The input value is compared with each compare value (up to 16) and the corresponding output value is copied to the output data value.

## Configuration

- **Update time**: The time (in seconds) between updates to the output data value.
- **Input**: The input data value is monitored by the function and compared to the compare values below.
- **Output**: The output data value is set by the function based on the **Output value 1-16** below.

## Compare

- **Compare value 1-16**: This is a series of set point data values which the input value is compared to. The compare value which the input value is closest to determines which output value (below) is set for the output.

  For example, set **Compare value 1** to 5 and **Compare value 2** to 10. When the input value is below, equal to or just above 5, **Output value 1** is used. When the input value is above 5 (7 or higher), equal to 10 or above 10, **Output value 2** is used.

  The input value can exceed the lower compare value by some amount before the output value changes. This depends on the total interval between the two consecutive compare values. It is recommended that you test the operation before use.

- **Output value 1-16**: This is a series of set point data values which determine the value of the output. For each compare value there must be an output value. When the input value matches a particular compare value the corresponding output value is copied to the output data value.

# Data values

Data values (sometimes known as registers) are used by the system to store numerical values for monitoring analog inputs, controlling analog outputs or for use in programmable functions. For example, each channel on an analog expander can be represented by a data value which stores a quantity such as current or voltage. Data values can also be linked to variables, which allow the value to be scaled by a linear equation, monitored and controlled.

Several types of programmable function specifically monitor or manipulate data values, such as value compare, register counter, average and variable output compare. This allows you to use data values for a wide variety of advanced functions.

For monitoring analog channels using data values, see the analog expanders section (see page 298). For an advanced programming application, see Application Note 278: Access Level Area Counting in Protege GX.

If a data value is not generated by a physical module such as an analog expander it may be necessary to set it as the **Channel data value** for a virtual analog expander (**Expanders | Analog expanders | Channel 1-4**) to ensure that it is downloaded to the controller.

## Data values | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Preset power up**: When this option is enabled the data value is set to the **Preset value** each time the controller is powered up. When this option is disabled the data value will revert to the last known value when the controller powers up.
- **Preset value**: When this option is enabled the data value is set to the **Preset value** every time programming is downloaded to the controller. This effectively creates a constant value that can provide a fixed or set point for comparison.

  This option should not be used for data values that monitor analog input channels.

- **Preset value**: If either or both of **Preset power up** and **Preset value** are enabled the data value will be set to this number.

### Record history

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

# Variables

Variables allow you to display the information stored by data values in a human readable form. The data value can be scaled by a linear equation to make the value easier to read.

Variables can be displayed on floor plans or status pages (via a status list). When displayed on a floor plan you can right click on the variable, enter a value and click **Set variable** to manually change the variable value.

For an example of variable configuration, see the analog expander section (see page 298).

## Variables | General

### General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.

### Configuration

- **Scale**: The data value is multiplied by the scale to calculate the variable. This can be used to convert a value to a more readable unit, such as from millivolts to volts.
- **Offset**: The offset is added to the data value to calculate the variable. This can be a positive or negative value.

  The **Scale** is applied before the offset, so the offset is not multiplied.
- **Minimum / Maximum value**: When the variable is displayed on a floor plan it can be displayed on a linear gauge. These options determine the minimum and maximum values that can be displayed on that gauge. Set these to reasonable values to ensure that the gauge is easy to read at a glance.

  These options do not affect the value of the variable itself.
- **Data value**: The data value which provides the base value for the variable.
- **Support manual commands**: When this option is enabled, operators can right click on this variable on a floor plan and manually set the value. This should not be used for variables that are intended to act as constants or monitor physical inputs.

### Record history

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

## Variables | Log

- **Log data**: This option allows you to log the variable value to the event log at regular intervals.

  Alternatively, you can enable logging of the raw data in **Expanders | Analog expanders | Channel 1-4**.

# About Menu

The About menu is used to register and update your software license and view version information.

## Help

The **About | Help** menu allows you to conveniently access the operator reference manual in electronic format directly from the Protege GX client.

Internet access is not required.

## License

This page allows you to view your current Protege GX license details and update your license.

### License | Information

The license information window displays:

- The software serial number (SSN) currently in use
- The time remaining on your software maintenance agreement
- The main application (software) version you are using
- The license version you have
- The licensed features which are enabled on your SSN
- The number of limited licensed items that are used in the system compared to the license cap (e.g. 10 doors in use out of 50 available)
- The expiry dates of the licensed features that are currently enabled (to view, click the toggle arrow beside the relevant licensed item)

### License | Site details

The site details tab displays the site and installer details which are registered to this license in the Protege GX licensing system.

### Registering and Updating Your Software License

Before you can use Protege GX you must register your software license with ICT. You must also repeat this process to update your license file whenever you add new items or features to the license.

#### Requirements for License Registration/Update

To register or update your Protege GX license you will need the following:

- A device with internet access. There are two licensing methods available, depending on the network's internet connectivity:
  - If the Protege GX server or any Protege GX client has internet access you can use **Automatic** licensing.
  - If no Protege GX machine has internet access you must use **Manual** licensing. You will need to use the Protege GX server and another device which can access the internet.
- The operator who activates or updates the license must have access to **all sites** in the system.
- The Windows account used must have local administrative privileges.

### Activating Your License Automatically

1. Log in to Protege GX on any machine with internet access.
2. From the main menu, navigate to **About | License**.
3. Select the **License update** tab.
4. Click **Download license**.
5. Enter the required information and select **OK**.
   The Protege application passes your details to the ICT web registration service, then activates your software automatically.
6. Close and restart the Protege GX software to implement the new license.

### Activating Your License Manually

1. Log in to Protege GX **on the server machine**.
2. From the main menu, navigate to **About | License**.
3. Select the **License update** tab.
4. Click **Generate** to create a license request file. When prompted, save the **ICT_LicenceRequest.req** file to a folder on the network or a portable drive.
5. Note down the link displayed beside "Download your license via the website".
6. Transfer the license request file to a device with internet access.
7. Open a web browser and browse to the link you noted above.
8. Enter the required information and upload the license request file, then click **Submit**.
   Your details are then passed to the ICT web registration service. Once registration is complete you will be prompted to download your license (.lic) file.
9. Transfer the license file to the Protege GX server.
10. In the **License update** tab, click **Browse...** and select the license file.
11. Close and restart the Protege GX software to implement the new license.

## Viewing Version Information

When you log a support ticket you will usually be asked to provide details of the software version you are using. To view the version information, navigate to **About | Version**.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2025. 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.