PRT-WX-DIN

Protege WX

End User Guide

ICTProtegeWX®

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 2003-2015. All rights reserved.

Publication Date: December 2015

Contents

Understanding your System 5

Before You Begin 5

Logging In 5

Managing Users 6

Adding a User 6

Setting Start and Expiry Dates (Optional) 7

Creating an Access Level 8

Adding Doors to an Access Level 8

Adding Areas to an Access Level 9

Deleting Users 9

Disabling Users 9

Using Schedules and Holiday Groups 10

Creating a Holiday Group 10

Creating or Editing a Schedule 11

Using a Schedule to Automatically Unlock a Door 13

Using a Schedule to Control User Access 14

Schedules and Multiple Time Spans 14

Different Hours for Weekends 14

Shorter Hours on a Holiday 15

Overnight Schedules 15

Overlapping Periods 16

Rules for Schedules and Holidays 16

Working with Reports 17

Creating an Event Report 17

Common Reporting Scenarios 18

Using a Keypad to Arm/Disarm your System 19

Keypad Status Indicators 19

Keypad Functions 20

Logging into the Keypad 21

Logging Off 21

Arming Your System 22

Stay Arming an Area 22

Force Arming an Area 23

Disarming Your System 23

Entering a Duress Code or Panic Alarm 24
Acknowledging an Alarm 24
Using Card Readers 25
Presenting Cards 25
Entry Mode 26
Arming and Disarming 26

Understanding your System

Protege WX is a flexible web-based system that allows you to program, monitor, and control a site from any smartphone, tablet, or computer with a fixed or mobile network connection. It combines access control, alarm intrusion, and automation and control all into one unified package.

The system can include a number of components:

- The **Protege WX Controller** which is the central processing unit of the system. The controller will be mounted in an out of the way area such as a utility room or cupboard, and in most circumstances there is no reason for anyone but your security professional or property manager to require physical access to this unit.
- Various **detection sensors** (referred to as **inputs**) such as motion detectors or door contacts which are connected to the controller. If your system is armed and a sensor is activated, the input is 'opened' and sends a signal to the controller to trigger an alarm. The controller automatically transmits these details to your monitoring station or guardhouse, and the keypad will beep. Entering your access code and disarming the system will turn off the alarm.
- A **keypad** which is used to arm/disarm the system and display the current system status. The keypad will typically be located in a convenient location inside your premises close to the exit-entry door.
- One or more **card readers** which are used to provide access control on the door(s) in your building.

Before You Begin

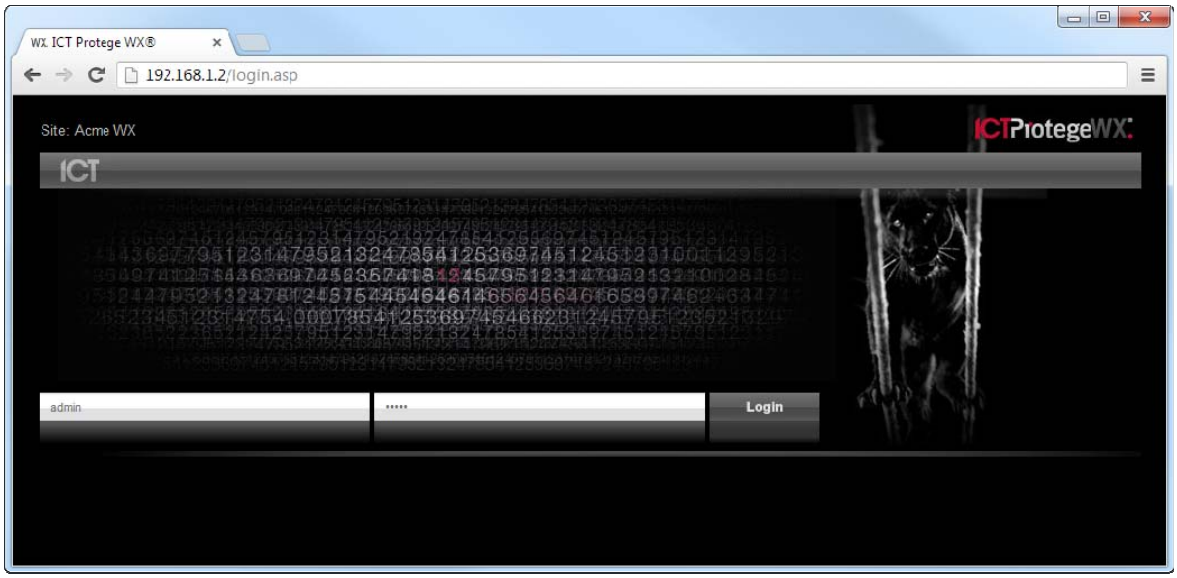
The flexibility of the Protege WX system allows an integrator to program functionality and system behavior to suit the site. This guide is aimed at explaining the most common settings.

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

Logging In

1. Open a web browser and enter the IP address provided by your installer.

   The Login window is displayed.



2. Enter your login and password.
3. Click **Login**.

While all popular modern web browsers are supported, we recommend using Chrome for the best user experience.

Managing Users

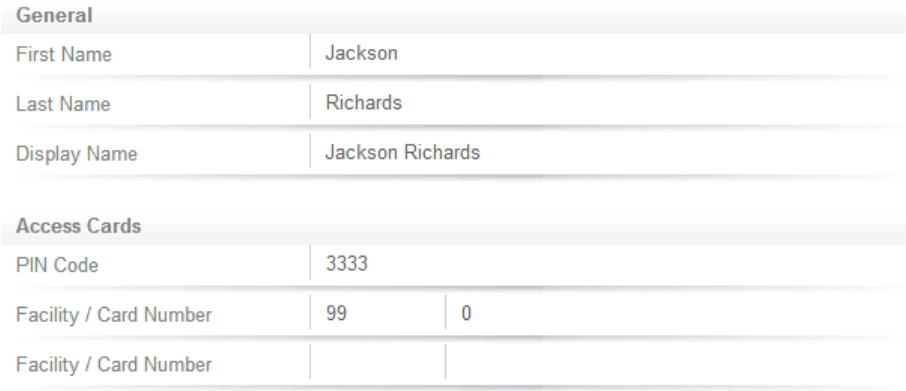
A User is a person that requires access to the facility being controlled by the system. They identify themselves to the system using credentials such as access cards and PIN codes, and use these credentials to unlock doors and disarm the alarm system.

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

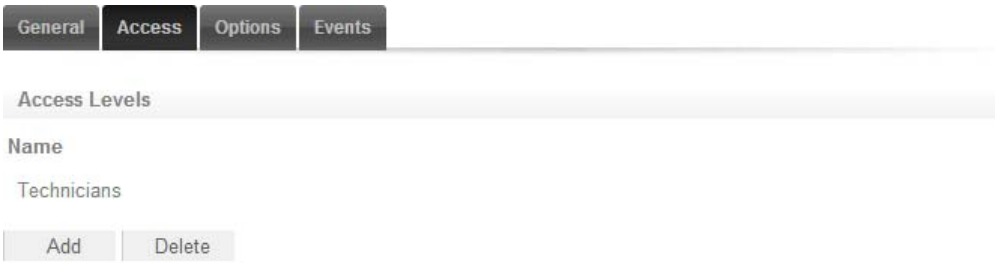
There are several methods for creating users. This guide describes the steps for adding users from the Users menu. For instructions on using alternative methods, talk to your installer.

Adding a User

1. Navigate to **Users | Users**, click **Add**
2. Enter a **First Name** and **Last Name** for the user.



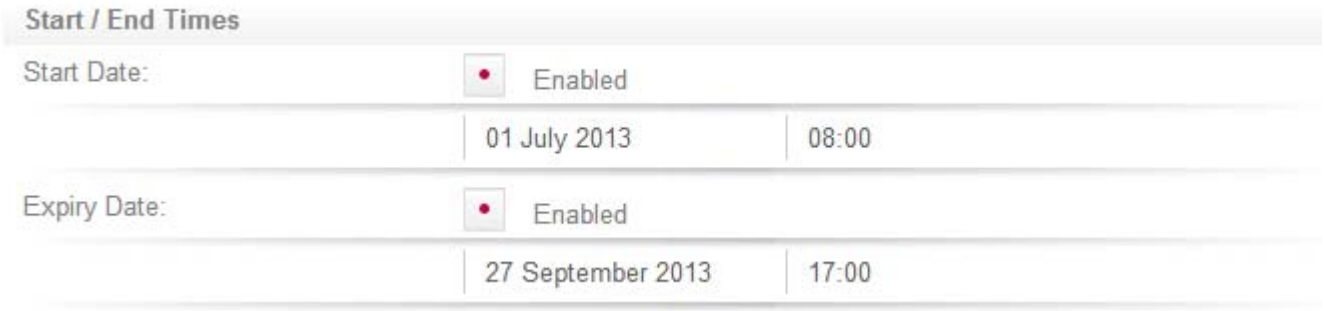
3. Enter a **PIN Code**. This is the number the user must enter when logging in to a keypad or accessing a door that requires PIN credentials.
4. Enter the cards credentials by typing the facility code and card number into one of the available fields.
5. Each user can have up to 8 card numbers. Multiple card numbers allow the use of ICT wireless remotes or cards and fobs for the same user, without the need to program duplicate user records.
6. Select the **Access** tab to add the required access level(s) to the user. When the user performs an action, the system checks the access level(s) to ensure the user has the relevant permissions to perform the requested action.



7. Click **Add** to open the Select Record window
8. Select the relevant Access Level(s) and click **OK**.

Setting Start and Expiry Dates (Optional)

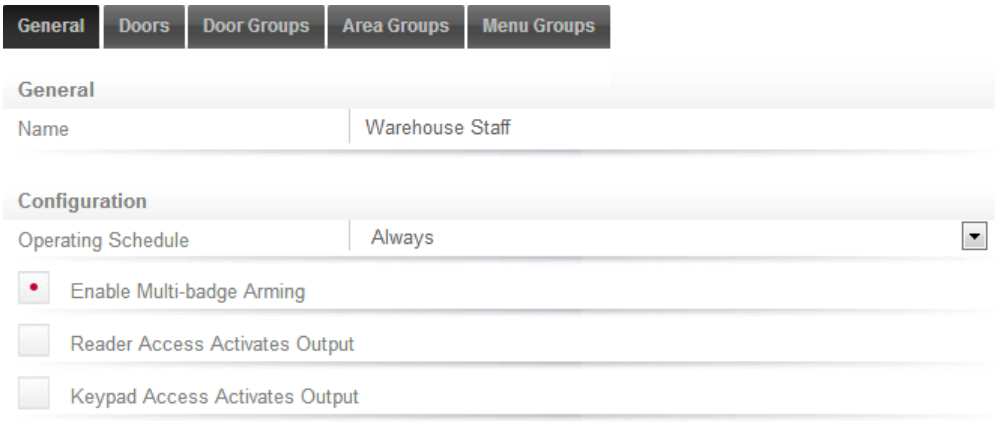
Each user can be set with access for a defined period by checking the Start and/or Expiry options and setting a date and time:



This allows cards to be issued and sent out prior to access being enabled, and allows for user access to be stopped on a future date. For example, an employee that has not yet started, or a contractor that is due to finish on a set date.

Creating an Access Level

1. Navigate to **Users | Access Levels**, click **Add**
2. Enter a name for the Access Level and click **Save**



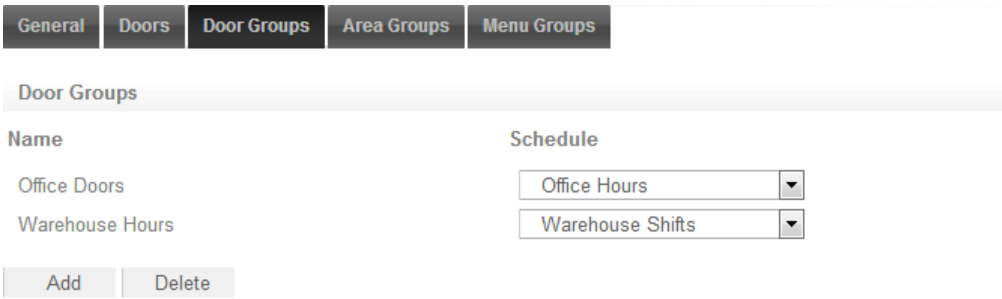
Adding Doors to an Access Level

Doors and Door Groups define which doors a user has access to, and the schedule that is used.

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

To Add Doors to an Access Level:

- Select the Doors or Door Groups tab and click Add
- Choose the relevant Doors or Door Group and click OK
- Set the Schedule to be used. By default, the schedule is set to Always, meaning access to the defined doors is permitted at all times. Assigning another schedule will restrict access to doors within that group for the period set in the schedule. For example, limiting access to an office so it may only be entered during office hours.



- Save your changes.

Protege WX has a default door group called All Doors that allows access to all doors, all of the time. This group should be used with caution. When a new door is created, it is automatically assigned to the All Doors group which means that anyone that has that group in their access level will automatically have access to the new door.

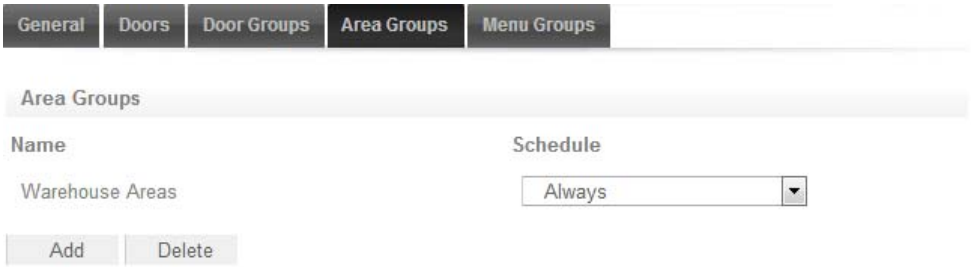
Adding Areas to an Access Level

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

If advanced mode is enabled, the Area Groups within an Access Level are separated into **Arming Area Groups** and **Disarming Area Groups** enabling you to differentiate between the areas a user is allowed to arm or disarm. For example, cleaners may be allowed to arm an area but not disarm it.

To Add an Area Group to an Access Level:

- Select the Area Groups tab and click Add
- Choose the relevant Area Group and click OK
- Set the Schedule to be used. By default, the schedule is set to Always, meaning users can arm/disarm areas within that group at all times. Assigning another schedule will restrict arming and disarming to the period set in the schedule.



- Save your changes.

Protege WX has a default Area Group called **All Areas** that allows access to all areas, all of the time. This group should be used with caution. When a new area is created, it is automatically assigned to the **All Areas** group which means that anyone that has that group in their access level will automatically have access to arm/disarm the new area.

Deleting Users

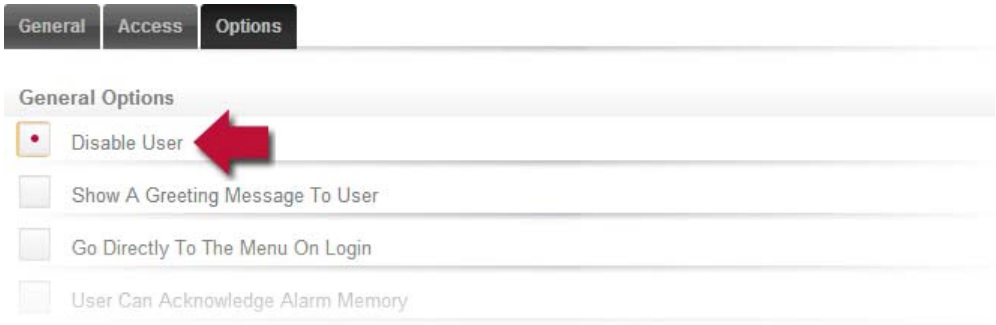
You can easily delete user records that are no longer required.

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

Important: Deleting a user, removes **all** reference to that user from the event log. The recommended method for removing an active user is to first disable them (see page 9) until their events are no longer required.

Disabling Users

The **Disable User** setting (found under the Options tab) removes access immediately while still retaining the user record and it's details.



This is ideal for removing access temporarily such as when staff are away on extended leave.

Using Schedules and Holiday Groups

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

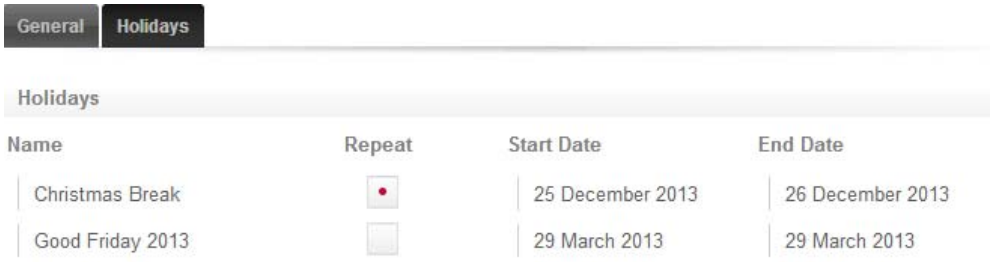
As schedules are commonly used to control access or to secure areas, it's a common requirement to have the schedule behave differently on a holiday. This is achieved by adding **Holiday Groups** which are then used to prevent (or allow) periods within a schedule to function during the holiday duration.

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

Creating a Holiday Group

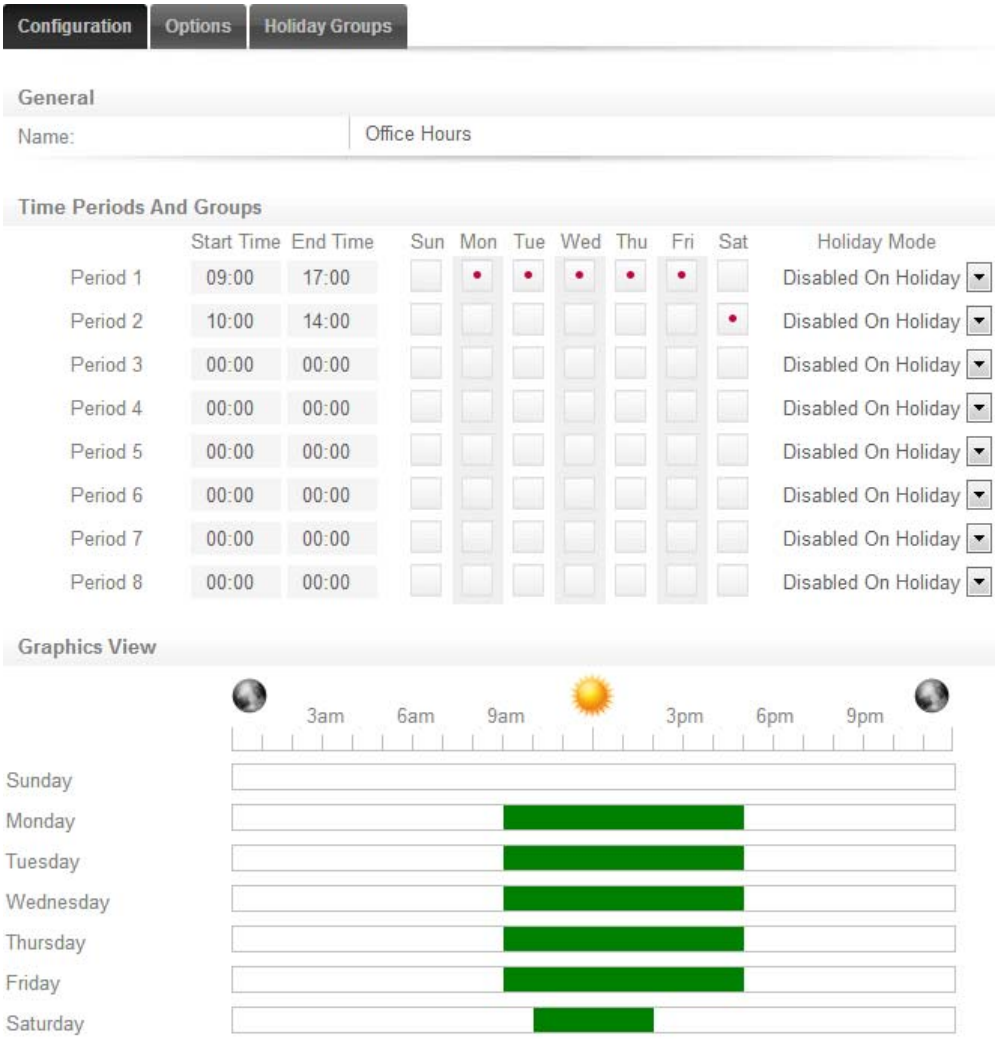
1. Navigate to **Scheduling | Holiday Groups** and click **Add**
2. Enter a name for the holiday group then select the **Holidays** tab to add holidays to the group



- Enable the **Repeat** option for holidays that occur on the same day every year.
- For holiday periods that span multiple days (such as Christmas and Boxing Day), set a different start and end date.
- For holidays that fall on a different day each year (such as Easter), these need to be programmed for each occurrence, but adding multiple entries allows you to program many years in advance.
- Click **Save**. Once you have programmed your holiday group(s), they can be applied to your schedules.

Creating or Editing a Schedule

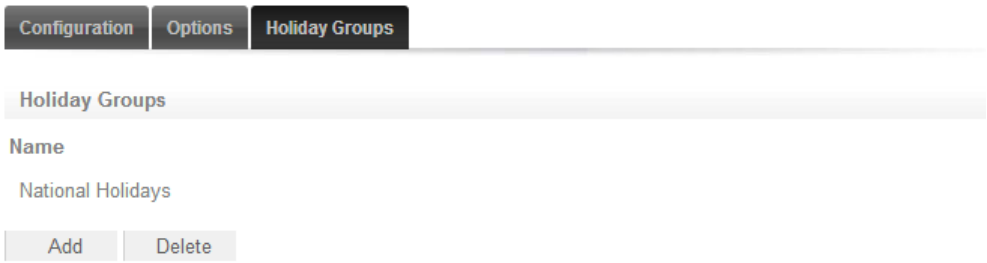
1. Navigate to **Scheduling | Schedules**
2. Select the schedule you wish to edit, or click **Add** to create a new schedule
3. Enter the start and end time for each period and select the days you wish the schedule to operate on by enabling the appropriate boxes.



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

4. For each period, choose the **Holiday Mode** to define how the schedule will operate during a holiday period. Choose from:
   - **Disabled on Holiday**: When selected, the period will **not** make the schedule valid on a holiday. In other words, if a door is programmed to unlock by this schedule, it will not unlock on a holiday when this option is selected. This is the default mode of operation for schedules.
   - **Enabled on Holiday:** When selected, the period will only ever make the schedule valid **on** a holiday.
   - **Ignore Holiday:** When selected, the period will make the schedule valid **regardless** of whether the day is a holiday or not.
5. Select the **Holiday Groups** tab to choose the holidays that apply to the schedule.

6. Click **Add** and select the group or groups of holidays that you wish to apply to this schedule.



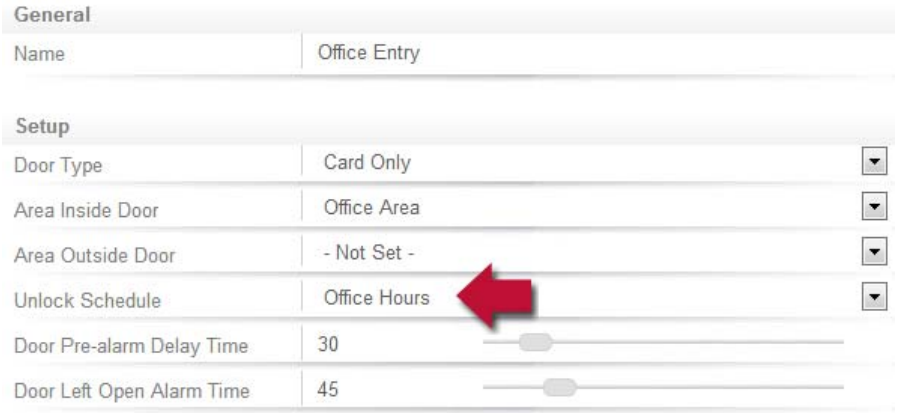
This tells the schedule **which days** are holidays, but it does not tell the schedule **what to do** if it is a holiday. That is defined by the **Holiday Mode**.

7. Click **Save**. Your schedule is now ready to use.

Using a Schedule to Automatically Unlock a Door

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

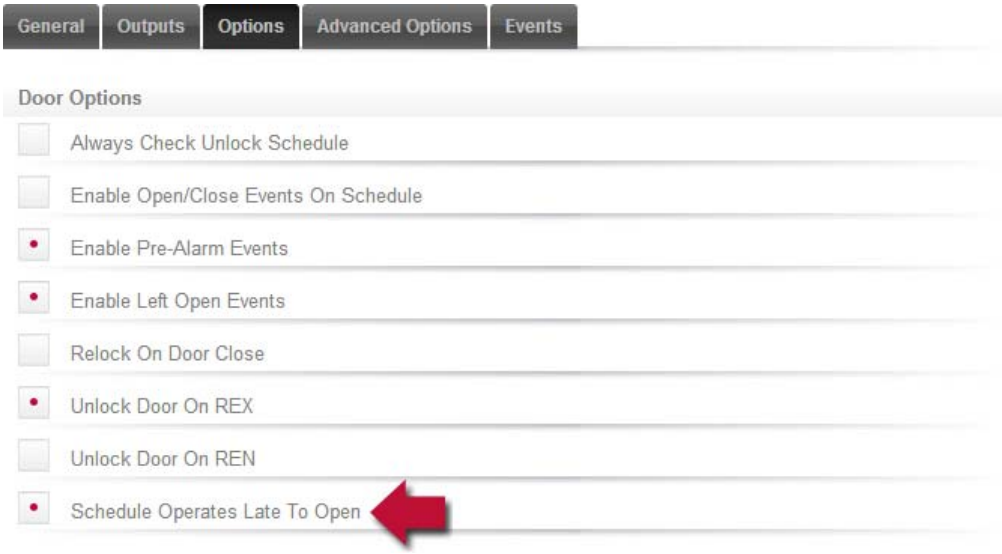
1. Navigate to **Programming | Doors**
2. Choose the door you wish to control, then select the **Unlock Schedule**



3. Save your changes.

   In many cases, you'll also need to prevent the door from unlocking if nobody turns up for work. A simple way to achieve this is using the Schedule Operates Late to Open feature.

4. Select the **Options** tab and enable the **Schedule Operates Late to Open** option and save your changes.



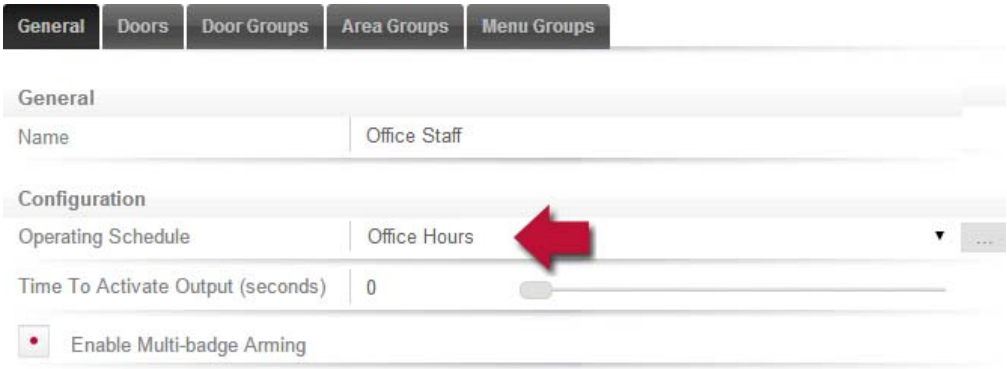
   This prevents the door from unlocking until the first user accesses the door.

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

Using a Schedule to Control User Access

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

1. Navigate to **Users | Access Levels**
2. Select the access level you wish to add the schedule to, then select the **Operating Schedule**



3. Save your changes.

You can also assign a schedule to the doors within an access level (see page 8) to restrict access to the hours defined, and/or to the area groups (see page 9) to restrict arming/disarming to a specific period. This provides more flexibility by allowing you to define access at a more granular level. For example, you may wish to restrict access to one group of doors to scheduled office hours, but permit access to another group outside these hours.

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

Schedules and Multiple Time Spans

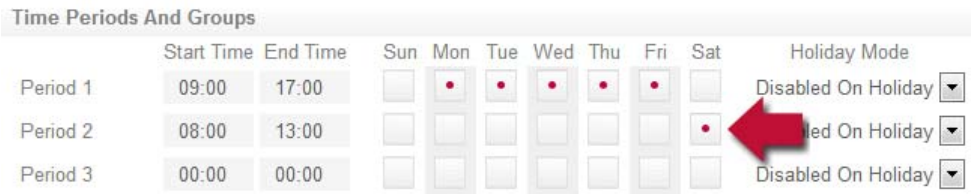
There may be times when schedules need to turn on and off more than once, or at different times on different days. Each schedule has 8 periods to allow for these scenarios.

Let's look at some examples of when you might use this.

Different Hours for Weekends

Premises may need to open for shorter hours on a weekend.

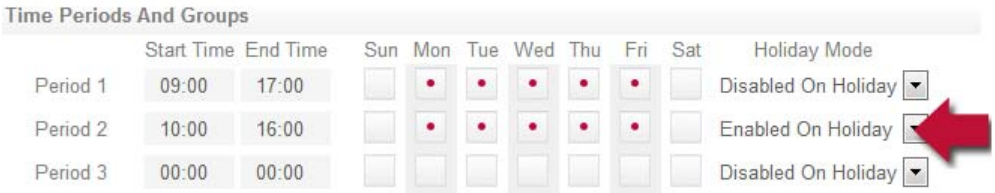
To set this up, you simply add the second period of shorter hours and select the relevant day (in this example Saturday):



Shorter Hours on a Holiday

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

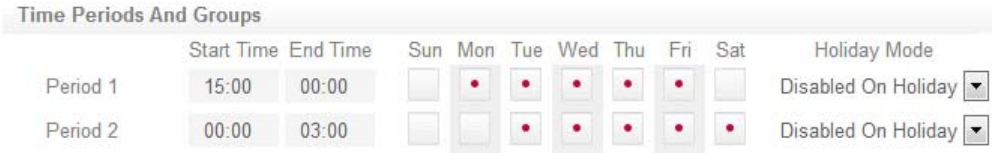
In this example, the schedule will be valid from 9am to 5pm, Monday to Friday on normal days. If the day is a holiday, the schedule will only be valid from 10am to 4pm.



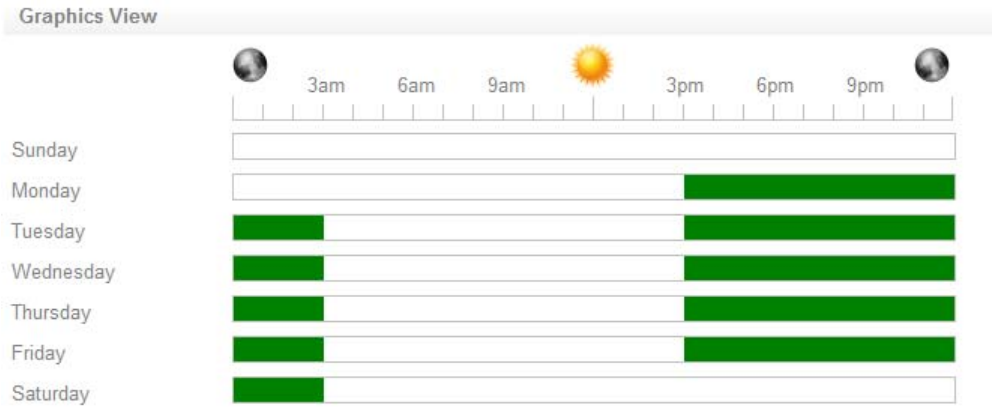
Overnight Schedules

Where a schedule is required to operate overnight, enter a start time, but leave the end time as 00:00. 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. In this example, the schedule will become valid at 3pm on Monday, and stay valid until 3am the following morning. By extending the days the period is valid, we can create an overnight Monday to Friday shift:

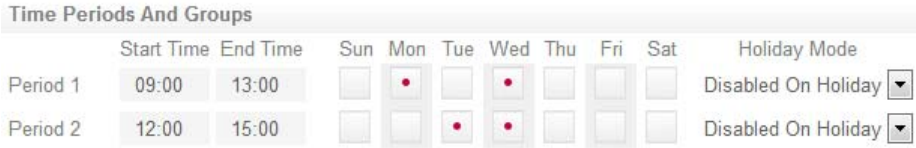


The Graphics View is used to show when the schedule will be valid:

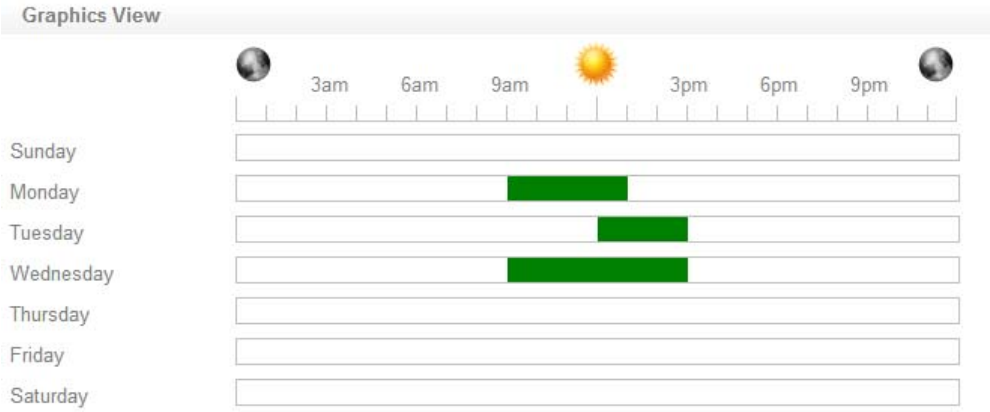


Overlapping Periods

Where overlapping periods are present, the schedule will take the sum of all periods.



In this example, Wednesday has two periods that overlap. The two periods are combined, and as a result, the schedule will be valid from 9am to 3pm on Wednesday.



Rules for Schedules and Holidays

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

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

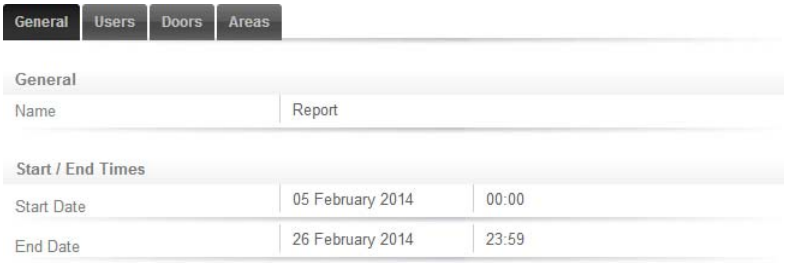
1. The holiday must be programmed in a holiday group
2. That holiday group must be applied to the schedule
3. The holiday mode must be programmed as **Disabled on Holiday**

Working with Reports

Event Reports allow an operator to create, view and export customized reports based on users, doors and areas.

Creating an Event Report

1. Navigate to **Monitoring | Reporting | Event Reports**.



2. Enter a **Name** for the report.

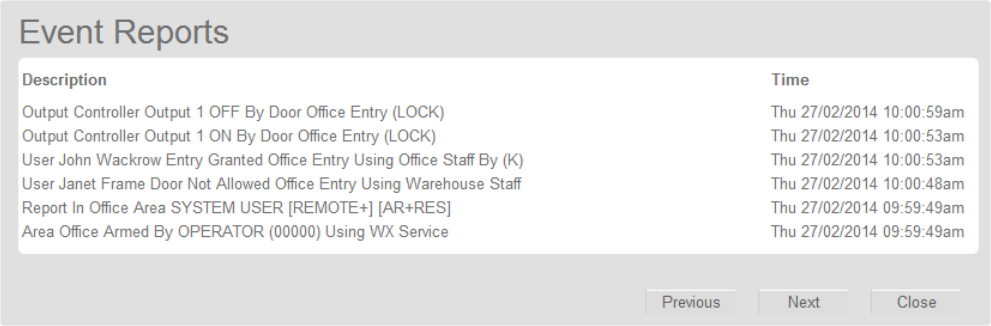
   A name is only required if you wish to save the report. If you wish to view events 'on the fly', the name is optional.

3. Enter a valid **Start Date** and **End Date**.
4. To include **all** events click Save, View or Export.

   -or-

   To filter based on Users, Door and/or Areas, use the additional tabs. A number of common reporting scenarios and the filter criteria required, are outlined in the following section.

5. Click **View** to display the relevant events.



6. Click **Export** to save the events in CSV format enabling you to extract event data which can then be formatted and manipulated as required.

   Depending on your browser settings you may be prompted to save the file, otherwise it is downloaded automatically to your Downloads folder.

Common Reporting Scenarios

The following scenarios cover common reporting requirements and the options that should be selected.

To view what a particular user or group of users has accessed on site:

1. Define the date/time range
2. Select the user(s)
3. Select View or Export

To view which users have been through a specific door or group or doors:

1. Define the date/time range
2. Select the door(s)
3. Select View or Export

To view whether an individual user has been through a particular door:

1. Define the date/time range
2. Select the user
3. Select the door
4. Select View or Export

To view which user has armed an area:

1. Define the date/time range
2. Select the area
3. Select View or Export

To view whether an individual user has disarmed a particular area:

1. Define the date/time range
2. Select the user
3. Select the area
4. Select View or Export

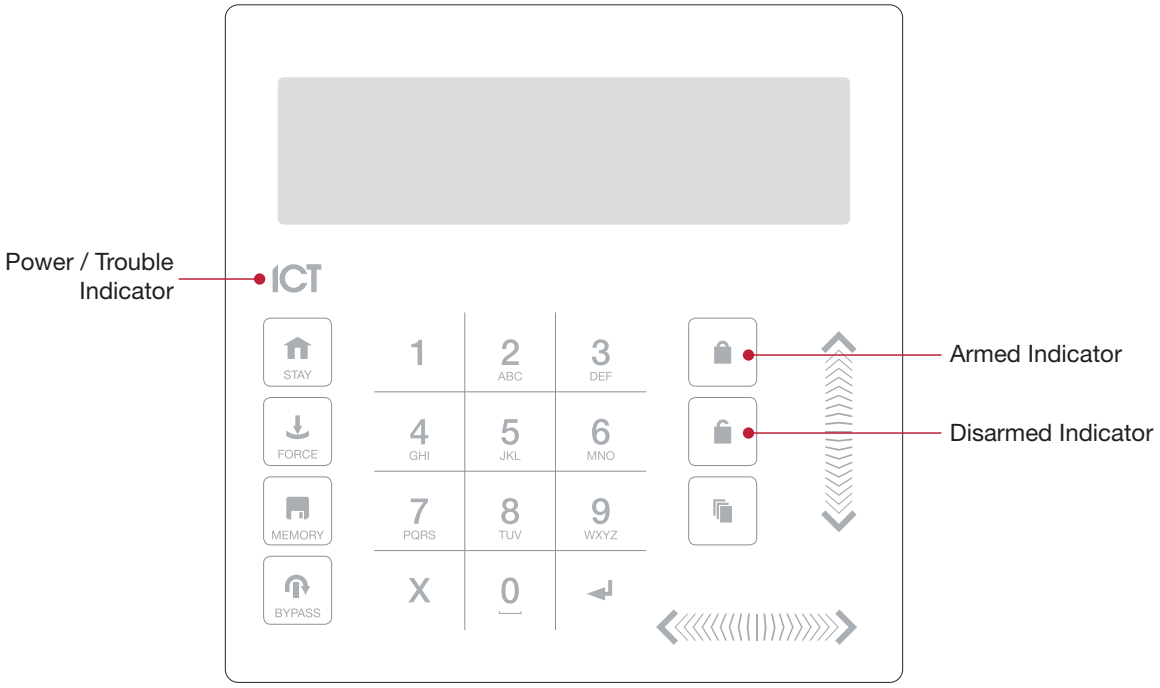
Using a Keypad to Arm/Disarm your System

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

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

Keypad Status Indicators

The Touch Sense keypad features three status indicator lights that show the condition of your Protege system.



Power/Trouble Indicator

- When **ON**, the system is powered and operating normally
- If there is a complete power failure this indicator will be **OFF**
- If the Power/Trouble Indicator is **FLASHING**, it is showing that a trouble condition is present. Contact your installer for assistance.

Armed/Disarmed Indicators

The Armed / Disarmed indicators are programmed by your installer and are typically used to show the state of the primary area associated with the keypad.

- Green is normally used to indicate the area is disarmed.
- Red is normally used to indicate the area is armed.

Operation may vary however, and your installer will be able to advise of expected behavior.

Keypad Functions

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

Logging into the Keypad

- To logon, enter your [USER CODE] and press [ENTER].

```
Enter user
code: ******
```

  To restart the entry process, press [CLEAR].

- Once a valid code is entered you are presented with a welcome screen.

```
Good Evening
J Smith
```

- After a short period you are taken to the area control menu.

```
Warehouse
is DISARMED
```

Depending on your system, entering an invalid user code three times may lock the keypad for a short period preventing further login attempts by any user. This is an optional setting that may be enabled by your installer. The duration between the welcome screen displaying and when you are taken to the area control menu is a setting that is programmed by your installer.

Logging Off

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

The period of inactivity is defined by the Time User is Logged In setting under the keypad programming. If no key presses are detected during this time, you will be logged off automatically and will need to log in again before you can proceed.

Arming Your System

When leaving your building, you'll need to arm (or activate) the areas within your system. You may have a single area or multiple areas that can be armed independently, such as an office area and warehouse area.

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

   If enabled, you may be able to arm a group of areas by pressing the right arrow key. Your installer can provide more information on this feature.
4. Press the [ARM] key to start the arming process.
5. The system checks that all inputs (detection sensors) are closed before going into exit delay. This will provide you with enough time to exit the area before the system arms completely. The keypad will beep during the exit delay period.

   If you attempt to arm the system while an input is open, the keypad will emit a beep and display a warning message onscreen. You will either need to close the input before you can proceed with arming the system, or you can choose to bypass the input. Bypassing an input allows you to program the system to temporarily ignore (or deactivate) that input until the next time the system is armed. For example, you may wish to disarm a sensor in a room where you're making repairs or renovations or keep a window open to allow fresh air in.
6. To bypass an open input, press [BYPASS]. A prompt appears advising that the system has xxx number of bypassed inputs. Press [ARM] to confirm the action or [DISARM] to halt the arming process and return the area to the DISARMED state.
7. Press [CLEAR] to logout.

Even if the system has been programmed to automatically log you out after a short period of inactivity, it is good security practice to get into that habit of logging out when you walk away from the keypad.

Stay Arming an Area

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

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

1. Enter your [USER CODE] and press [ENTER] to login to the system.
2. A greeting is displayed. Press any key to continue or wait a few seconds for the greeting to timeout.
3. Press the [STAY] key to start the stay arming process.
4. The system checks that the normal inputs (exterior sensors) in the area are closed while bypassing the stay inputs (interior sensors)
5. If all the normal inputs are closed, the area goes into exit delay. Once the exit delay time has elapsed, the area is stay armed.

Force Arming an Area

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

Force Arming allows you to arm the system without waiting for all the inputs in the system to close. It is commonly used when a motion detector is protecting an area that is occupied by a keypad. For example, if the motion detector has been programmed as a force input, the system will allow you to arm even if the input is open.

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

Disarming Your System

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

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

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

   If enabled, you may be able to arm a group of areas by pressing the right arrow key. Your installer can provide more information on this feature.
4. Press the [DISARM] key to start the disarm the system.

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

Entering a Duress Code or Panic Alarm

Duress Codes

If you are forced to arm or disarm your system, entering a **duress code** will arm or disarm the system and immediately transmit a silent message to the monitoring station.

Depending on how your system has been configured, you may either have a designated duress user code that applies to the whole site, or your duress code may be your regular user code +1. For example, if your pin was 1234, the duress code would be 1235. Note that the +1 counter applies to the last digit only. This means if the user pin is 1239, the pin to trigger a duress code would be 1230.

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

Panic Alarms

The Protege system can provide three panic alarms that immediately generate an alarm after simultaneously pressing and holding two specific buttons for three seconds. Based on your needs, these panic alarms can generate audible alarms (sirens or bells) or silent alarms and can communicate specific messages to your monitoring station or property manager.

- Press and hold keys **[1]** and **[3]** for the **panic** alarm.
- Press and hold keys **[4]** and **[6]** for a **medical** alarm.
- Press and hold keys **[7]** and **[9]** for a **fire** alarm.

Panic Alarm activations **must be enabled** before they can be used. Your installer can confirm if this feature has been configured.

Acknowledging an Alarm

Alarms are stored in memory until they have been acknowledged.

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

Using Card Readers

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

Presenting Cards

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

While there is little visible difference between the various card types, what happens behind the scenes is quite different.

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

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

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

Entry Mode

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

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

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

Arming and Disarming

Depending on how your system has been programmed, badging your card will usually disarm an armed area when unlocking a door.

In many cases, your system may also be programmed so that presenting your card multiple times will start the arming process. If Double Badge Arming is enabled, two successive reads from the same card will start the arming process. If Triple Badge Arming is enabled, three successive reads from the same card will start the arming process.

Your installer can confirm if either of these options are enabled.

To Arm an Area Using Double or Triple Badge Arming:

1. Present your card at the reader. You will hear a short beep.
2. Present your card a second time.
3. If triple badging has been enabled, present your card a third time.
4. The reader will generate three short beeps to indicate the area is arming.

NEW ZEALAND
Integrated Control Technology Limited
4 John Glenn Avenue, Rosedale, Auckland 0632
PO Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: sales@incontrol.co.nz Toll Free: (0800) 428 111 Phone: 64 (9) 476 7124

USA
Integrated Control Technology (USA) LLC.
5265 S Rio Grande Street, Suite 201, Littleton, CO 80120
Email: ussales@incontrol.co.nz Toll Free: (855) 428 9111 Phone: 720 442 0767

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2015. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of these products, 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 Integrated Control Technology policy of enhanced development, design and specifications are subject to change without notice