



PRT-WX-DIN

Protege WX

End User Guide



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

Copyright © Integrated Control Technology Limited 2003-2022. All rights reserved.

Last Published: 06-Sep-22 01:47 PM

Contents

Understanding your Protege WX System	5
Before You Begin	5
Signing In	5
Browsing to Less Secure Controllers	5
Managing Users	7
Adding a User	7
Setting Start and Expiry Dates (Optional)	7
Creating an Access Level	7
Adding Doors to an Access Level	7
Adding Areas to an Access Level	8
Deleting Users	8
Disabling Users	8
Configuring Schedules and Holidays	9
Creating Holiday Groups	9
Creating and Editing Schedules	9
Using a Schedule to Automatically Unlock a Door	10
Using a Schedule to Control User Access	10
Schedules and Multiple Time Spans	10
Different Hours for Weekends	11
Different Hours on a Holiday	11
Multiple Periods in a Single Day	11
Overlapping Periods	11
Overnight Schedules	11
Rules for Schedules and Holidays	11
Working with Reports	12
Creating an Event Report	12
Common Reporting Scenarios	12
Using a Keypad to Arm/Disarm your System	13
Status Indicators	13
Audible Feedback	14
Keypad Functions	15
Logging in to the Keypad	15
Logging Off	16
Arming Your System	16
Stay Arming an Area	16

Force Arming an Area	17
Disarming Your System	17
Entering a Duress Code	17
Acknowledging an Alarm	18
Using Card Readers	19
Presenting Cards	19
Card Types	19
Entry Mode	19
Arming and Disarming from a Card Reader	20

Understanding your Protege WX 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. A siren or other alarm device is activated, and the controller automatically transmits these details to your monitoring station or guardhouse. Entering your access code and disarming the system will turn off the alarm.
- One or more **keypads** which are used to arm/disarm the system and display the current system status. Each 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 for the door(s) in your building.

Before You Begin

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

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

Signing In

To access the system after the initial setup you need to sign in with a valid operator username and password.

1. Open a web browser and enter the controller's IP address, with the prefix `https://` (e.g. `https://192.168.1.2`).
If you cannot access the controller with this URL, remove the `https://` prefix (e.g. `192.168.1.2`).
2. If you are presented with a security warning when accessing the HTTPS web page, use the advanced options to proceed to the controller web page.
3. The **Sign In** window is displayed.
4. Enter your operator **Username** and **Password**.
5. Click **Sign In**.

Repeatedly entering incorrect passwords at the sign in window forces a login stand down. Three consecutive incorrect attempts will result in the sign in process being locked for 5 seconds. If another three attempts fail, the sign in process is locked for 60 seconds between all subsequent attempts until a valid login is made. It is not possible to configure the length of time for the login stand down.

If you still cannot browse to the controller, additional web browser configuration may be required. For more information, see [Browsing to Less Secure Controllers](#) (below).

Browsing to Less Secure Controllers

Some controllers use older hardware types or operating systems which do not support more recent security protocols and cipher suites. Most web browsers will not allow users to access the web interface of these controllers, even if users trust the site and accept the risk.

If you see one of the following errors when browsing to the controller, it means that the controller has an HTTPS security certificate installed, but only supports the older TLS 1.0 protocol.

The error messages you receive may differ depending on your server security settings.

- Chrome:
 - "This site can't provide a secure connection. 192.168.1.2 uses an unsupported protocol." (ERR_SSL_VERSION_OR_CIPHER_MISMATCH)
 - "This site can't be reached. 192.168.1.2 unexpectedly closed the connection." (ERR_CONNECTION_CLOSED)
- Edge:
 - "The connection for this site is not secure. 192.168.1.2 uses an unsupported protocol." (ERR_SSL_VERSION_OR_CIPHER_MISMATCH)
 - "Hmmm... can't reach this page. It looks like 192.168.1.2 closed the connection." (ERR_CONNECTION_CLOSED)
- Firefox:
 - "Secure Connection Failed. Peer using unsupported version of security protocol." (SSL_ERROR_UNSUPPORTED_VERSION)
 - "Secure Connection Failed" (PR_END_OF_FILE_ERROR)

In this situation the recommended solution is to allow access to the controller's web interface by creating a Firefox profile with downgraded security.

To avoid security vulnerabilities it is recommended to use this profile only for accessing controllers.

1. Download and install Firefox from the [Mozilla website](#) if you do not have it already.
2. Open Firefox, type **about:profiles** into the URL bar and press **Enter**.
3. Click **Create a New Profile** to open the wizard.
4. Click **Next**.
5. Enter a descriptive profile name (e.g. Controller).
6. Click **Finish**.
7. Click **Launch profile in new browser**.

You can return to the **about:profiles** page at any time to switch between profiles or set a default profile.

8. In the new browser, type **about:config** into the URL bar and press **Enter**.
9. Click **Accept the Risk and Continue**.
10. In the search bar, enter **security.tls.version.enable-deprecated**.
11. By default this is set to false. Click the toggle button on the right to set it to true.
12. Attempt to browse to your controller on <https://192.168.1.2> (use your controller's configured address if it has been changed from the default). Firefox will report that there is a potential security risk, because the controller has a self-signed certificate.
13. Click **Advanced...**
14. Click **Accept the Risk and Continue**.
15. The browser will present the controller's login screen. In future, you should be able to browse to less secure controllers using this Firefox user profile.

Managing Users

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

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

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

Adding a User

1. Navigate to **Users | Users**, then 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 user's credential(s) by typing the relevant facility and card numbers into the available fields. Each user can have up to 8 card numbers assigned. Multiple card numbers allow the same user to have multiple credentials (such as cards, fobs, mobile credentials and wireless remotes), without the need to program duplicate user records.
5. Select the **Access Levels** tab to add the required access level(s) to the user. When the user performs an action, the system checks the access level(s) to ensure the user has the relevant permissions to perform the requested action.

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

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

Setting Start and Expiry Dates (Optional)

Each user can be assigned access for a defined period by checking the **Start** and/or **Expiry** options and setting a date and time.

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

Creating an Access Level

1. Navigate to **Users | Access Levels**, then click **Add**.
2. Enter a **Name** for the access level 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 determines when. Most likely your installer has already programmed the doors required for your site.

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

To Add Doors to an Access Level:

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

Adding Areas to an Access Level

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

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:

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

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

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 below) 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 its details. This is ideal for removing access temporarily, such as when staff are away on extended leave, or removing access while still retaining the user information.

Configuring Schedules and Holidays

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

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

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

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

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

Creating Holiday Groups

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

There is no need to program weekends as holiday groups.

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

Creating and Editing Schedules

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

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

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

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

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

Using a Schedule to Automatically Unlock a Door

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

1. Navigate to **Programming | Doors**.
2. Choose the door you wish to control and set the **Unlock Schedule**.
3. Save your changes.

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

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

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

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

Using a Schedule to Control User Access

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

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

You can also assign a schedule to the doors within an access level (see page 7) to restrict access to the hours defined, and/or to the area groups to restrict arming/disarming to a specific period. This provides more flexibility by allowing you to define access at a more granular level. For example, you may wish to restrict access to one group of doors to scheduled office hours, but permit access to another group outside these hours.

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

Schedules and Multiple Time Spans

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

Below are some examples of when you might use this.

Different Hours for Weekends

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

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

Different Hours on a Holiday

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

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

Multiple Periods in a Single Day

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

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

Overlapping Periods

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

Overnight Schedules

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

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

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

Rules for Schedules and Holidays

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

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

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

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** and enter a **Name** for the report.

A name is only required if you wish to save the report. If you simply wish to view events as they happen, entering a name is optional.

2. Enter a valid **Start Date** and **End Date**.

3. To include all events, simply 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 below.

The limit on the number of records you can select is 1500. If you select more than this number of records and attempt to save the report you will see an error. Due to a known limitation it is not possible to remove excess records and save the report again; you will need to recreate the report from scratch.

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

5. 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, will be automatically downloaded automatically to your Downloads folder.

Common Reporting Scenarios

The following scenarios cover common reporting requirements and the options to select:

- To view the activity of a particular **user or users**, define a date/time range and select the relevant users.
- To view activity at a particular **door or doors**, define a date/time range and select the relevant doors.
- To determine whether a **specific user has gained access to a particular door**, define a date/time range and select the relevant user and door.
- To determine **which user has armed or disarmed an area**, define a date/time range and select the relevant area.
- To determine whether a **specific user has armed or disarmed a particular area**, define a date/time range and select the relevant user and area.

Using a Keypad to Arm/Disarm your System

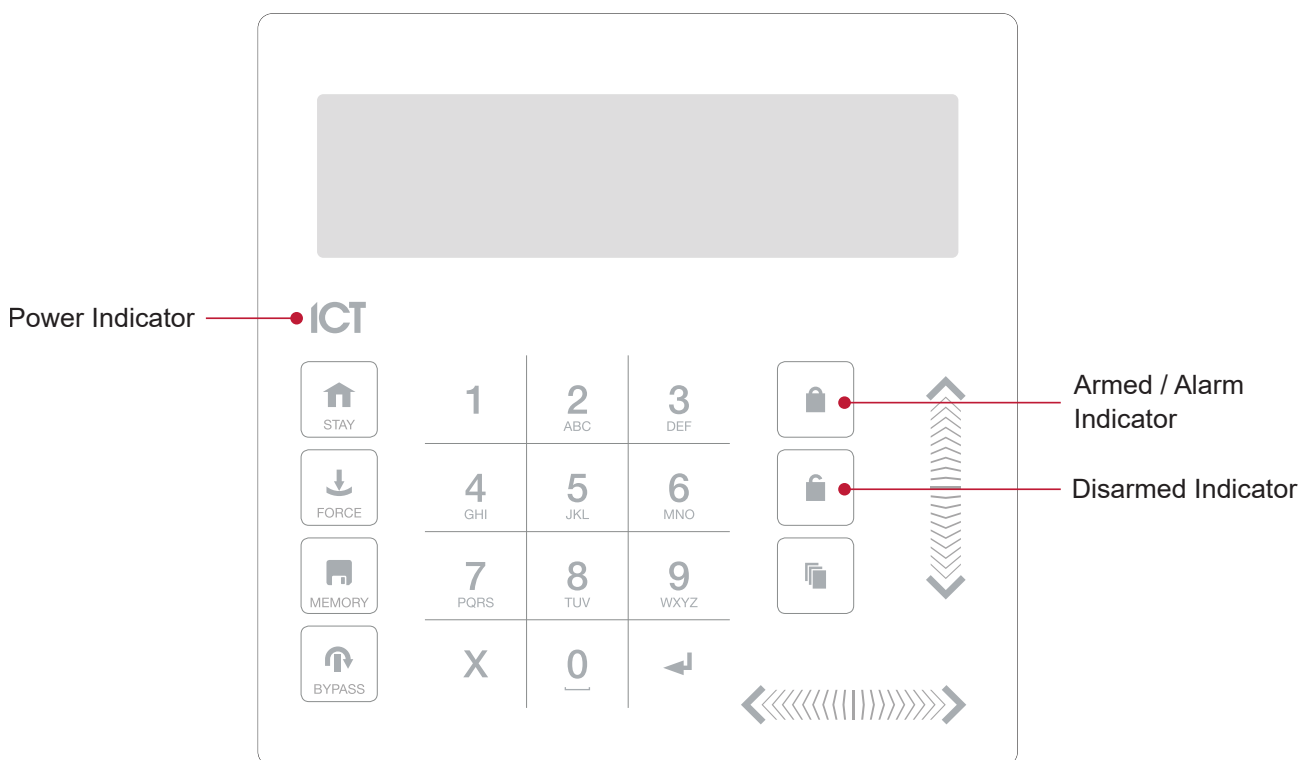
Keypads are typically located near an entrance or door to allow areas within the system to be armed and disarmed.

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

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

Status Indicators

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



Power Indicator

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

Armed / Alarm Indicator

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

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

Disarmed Indicator

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

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

Confidentiality Mode

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

Audible Feedback

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

Confirmation Tone










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

Rejection Tone

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

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

Keypad Functions

Key	Function
0-9	The primary function of the numeric keys is to enter user codes. When controlling devices the [1] key turns the device on, the [2] turns the device off, and in the on state the [3] key latches the device.
	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, which can be programmed to unlock a door.
	The [STAY] key is used to initiate 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 an area is breached during an arming process to bypass the displayed input.
	The [CLEAR] key will log off the user currently logged in to 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.
ARROW KEYS	The arrow keys are used to scroll the menu, move the focus of a program window to the next screen, and move the cursor when programming or editing values.

Logging in to the Keypad

Single Credential Login

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

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

Dual Credential Login

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

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

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

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

Logging Off

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

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

Arming Your System

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

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

Stay Arming an Area

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

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

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

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

Force Arming an Area

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

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

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

Disarming Your System

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

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

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

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

Entering a Duress Code

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

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

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

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

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

Acknowledging an Alarm

Alarms are stored in memory until they have been acknowledged.

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

Using Card Readers

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

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.

Card Types

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

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

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

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

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

Entry Mode

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

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

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

Arming and Disarming from a Card Reader

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

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

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

Your installer can confirm whether these options are enabled.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2022. 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.