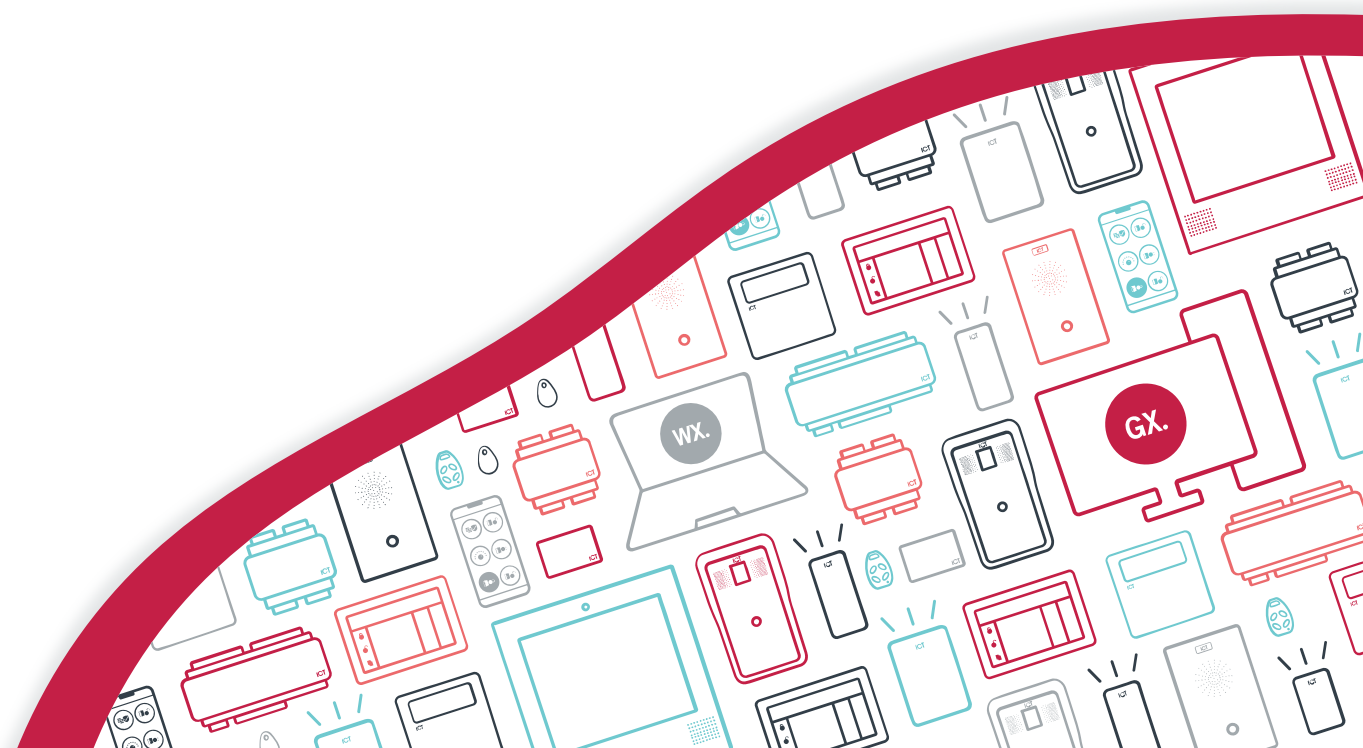
AN-338

Programming Protege Keypads

Application Note



Last Published: 21-Jan-22 4:06 PM

Contents

Introduction

Keypads are the main on-site interface for the Protege system, allowing complete user control of your security and access control system. Protege keypads can be programmed to allow authorized users to perform a wide range of functions beyond simply arming and disarming. They can perform advanced area control, unlock doors, trigger outputs, monitor inputs, and review device status, system troubles and events.

With multiple keypad access controls, the Protege system allows you to easily and precisely define which users are able to access which keypads, and exactly what they can and can't do once they're logged in.

This application note describes keypad features and programming requirements in Protege GX and Protege WX, along with operating procedures for:

- PRT-KLCS Touch Sense LCD Keypad
- PRT-KLCD Alphanumeric LCD Keypad

Some features have minimum software or firmware version prerequisites. It is recommended to always use the latest versions to ensure compatibility with new functionality.

User Keypad Access

To access a Protege keypad, a user will require:

- A PIN to log in
- If dual credential security is implemented, the user will also need a unique User ID
- The user's access level must include a menu group which allows access to the appropriate keypad menu(s)
- Keypad groups may also be used to determine which specific keypads the user is authorized to access

PIN and Dual Credential Settings

A number of configuration options are available to customize keypad login requirements and provide greater control over keypad security. You can require users to present dual credentials (both User ID and PIN code) to gain access to a keypad, and specify PIN expiry periods and rules for PIN complexity and duplicate PINs.

To configure PIN security and keypad access requirements:

- In Protege GX navigate to **Global | Sites | Site defaults**.
  For more information, see Application Note 275: Configuring Site Security Enhancements in Protege GX.
- In Protege WX navigate to **System | Settings | Security enhancements**.
  For more information, see Application Note 327: Configuring Security Enhancements in Protege WX.

Security Enhancement Settings

The security enhancement settings provide the ability to customize the PIN and dual credential configuration which dictates PIN security and keypad access requirements.

- **Require dual credential for keypad access**: With this option enabled, users will be required to 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.

  Both the User ID and the user's PIN will be required for the user to gain access to a keypad.

- **Autopopulate User ID credential value**: This option is only available in Protege GX. 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**: When enabled, this option allows more than one user to have the same PIN.

  This option is only available when the **Require dual credential for keypad access** mode has been enabled.

- **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 save a change to this setting you will be prompted to apply the change to all users. Select **Yes** to override the settings programmed in individual user records with the new default value. This may take some time for sites with a large number of users. If you select **No**, the default setting will only be applied to users added after the change.

- **New PIN to be generated by system**: This option is only available in Protege GX. 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.

Two Factor Keypad Access

For an additional security option, keypads can be used in conjunction with ICT card readers to require two factor authentication (card + PIN) for keypad access.

1. To enable this feature, check the **Keypad login requires card** option (**Expanders | Keypads | Options 2**).

   When this option is enabled, users must badge a card at the assigned reader then enter a PIN to access the keypad (two factor authentication). PINs cannot be entered at the keypad without first badging a card.

2. To operate this feature it is also necessary to configure the following options in the programming of the reader expander (**Expanders | Reader expanders**) that the card reader used for badging is connected to.
   - **Reader 1/2 door**: This door must be configured with a door type which requires Card and PIN access. Otherwise, badging a card will not trigger the associated keypad for entry of a PIN.
   - **Reader 1/2 keypad type**: Set to LCD Keypad.
   - **Keypad to use for PINs reader 1/2**: Select the keypad.

When a user presents a valid card at this door's reader, the keypad selected above will beep rapidly and display User access code:.The user can now enter their PIN at the keypad and press **[ENTER]** to log in.

PIN entry is allowed for the **Time user is logged in** setting duration (**Expanders | Keypads | Configuration**). If this expires before the user enters their PIN they will need to badge their card at the reader again.

- If a PIN is entered which is not associated with the same user record as the card that was presented at the reader, the keypad will display Incorrect code please try again.
- If a user attempts to log in without first badging a card, the keypad will display Present card to login!.

Menu Groups

Menu groups define which keypad menus and other features a user has access to. Before a user can access a keypad, an access level assigned to them must include a menu group which has some level of menu access enabled. Without a menu group giving them access to keypad menus, the user cannot log in to a keypad.

Menu groups can also be assigned to specific keypads to further limit the menus that can be accessed by any user at that keypad (see page 25). If access to a menu is denied via either the access level or the keypad programming the user will not be able to access that menu from that keypad.

To assign a menu group to an access level, navigate to **Users | Access levels | Menu groups** and add the desired menu group for that access level.

When assigning multiple menu groups to access levels, care should be taken to ensure there is only one menu group applied to each keypad that a user can access. If multiple menu groups are available to a user at a single keypad it can result in undefined system operation.

To add or customize menu groups:

- In Protege GX navigate to **Groups | Menu groups**.
  For more information on menu group options, see the Protege GX Operator Reference Manual.
- In Protege WX navigate to **Programming | Menu groups**.
  For more information on menu group options, see the Protege WX Programming Reference Manual.

General

- **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.

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.
- **Bypass trouble input (7, 2)**: When this option is enabled, users can access the trouble input bypass menu by pressing **[MENU] [7] [2]** on the keypad. This menu allows users to bypass trouble inputs.

  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.

Options

- **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**).

Keypad Groups

Keypad groups can be assigned to menu groups (see page 7) to control which keypads the menu group configuration is applied to. This allows you to restrict user access to designated keypads or grant users specific permissions at different keypads.

To add or customize keypad groups:

- In Protege GX navigate to **Groups | Keypad groups**.
- In Protege WX navigate to **Programming | Keypad 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**.

Be mindful of which keypads are added to each keypad group and which menu groups and access levels they will be assigned to. It is important that there is only one menu group applied to each keypad that a user can access.

Arming / Disarming Options

Area Groups

Area groups can be assigned to access levels (**Users | Access levels**) to define the areas that a user is allowed to arm and disarm. They can be included as either arming area groups (only arming allowed) or disarming area groups (both arming and disarming allowed).

Area groups may also be assigned to individual keypads as the **Area group for this keypad** (see page 25), to define which areas can be viewed and controlled from each keypad, including area group arming/disarming.

For a user to view and control an area, the area must be permitted by both the keypad and the user's access level.

To add or customize area groups:

- In Protege GX navigate to **Groups | Area groups**.
- In Protege WX navigate to **Programming | Area 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**.

Area Group Arming / Disarming

With area group arming/disarming it is possible to arm or disarm all of the areas on the keypad at the same time.

All of the areas included in the area group assigned as the **Area group for this keypad** (see page 25) can be armed/disarmed together from the keypad by pressing the **[RIGHT]** key in the area menu and completing the desired arming/disarming command.

To configure area group arming/disarming:

1. Set the **Area group for this keypad** in the **Configuration** section of the keypad programming.
2. To enable area group arming/disarming from the keypad, enable the **Allow area group selection access** option in the **Options 1** tab of the keypad programming.
3. To authorize a user to arm/disarm the area group, enable the **Area group control allowed** option in the **Settings** section of the menu group which provides the user with access to this keypad.
4. At the keypad, log in and access the area menu. Press the **[RIGHT]** key to view the area group controls, then press **[ARM]**, **[DISARM]**, **[STAY]** or **[FORCE]** to control every area in the group.

   If the command succeeds, you will see a success message and return to the area menu.

Stay Arming

Stay arming allows you to remain in the area while it's partially armed. A stay armed area will only monitor selected inputs, usually perimeter inputs, while ignoring activations from other inputs. When an area is stay armed only inputs with the stay input option enabled (see below) are monitored. For example, in a residential installation this would allow the occupants to arm external doors and windows without arming internal inputs such as PIRs.

1. To configure an area to allow stay arming, navigate to **Programming | Areas | Options 2** and check the **Enable stay arming** option in the **Advanced options** section of the area programming.
2. To enable stay arming from the keypad, you need to check the **Stay arming** option in the **Settings** section of the menu group which provides the user with access to this keypad.
3. To configure the monitored inputs for stay arming, you will need an input type which has the **Stay input** option enabled (**Programming | Input types | Options 1**).

4. For each input that you do want to be monitored when the area is stay armed (such as perimeter door and window sensors) the area and the above 'stay input' input type will both need to be assigned in the input programming (**Programming | Inputs | Areas and input types**).
5. At the keypad, log in and access the area menu. Select the area you want to stay arm, then press **[STAY]** to arm the 'stay inputs' in the area without arming the other inputs.

   If the command succeeds, you will see a message that the area 'is STAY' and return to the area menu.

Additional Stay Arming Options

- **Disable exit output on stay arming**: When this option (**Programming | Areas | Options 2**) is enabled the area's exit delay output/output group 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.

- **User rearm in stay mode**: With this option (**Programming | Areas | Options 2**) enabled, when designated users disarm the area it will automatically rearm in stay mode after a defined period of time.
  - Users must have the **Rearm area in stay mode** option enabled (**Users | Users | Options**).
  - The area will remain disarmed for the duration specified in the area's **Rearm area time** setting.

  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.

- **Rearm area in stay mode**: Enabling this option (**Users | Users | Options**) allows a user to automatically rearm in stay mode. When the user disarms an area with the **User rearm in stay mode** option enabled (see above), the area will remain disarmed for the area's **Rearm area time** duration, 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.

Instant Stay Arming

Instant stay arming reduces the exit delay to 1 second, and inputs which normally initiate the entry delay will instead set off the alarm immediately (i.e. all inputs are treated as 'instant'). This feature is commonly used at night while residents are in bed, so that any intruder entering the building will set off the alarm immediately.

The following steps to enable instant arming are required in addition to the stay arming requirements above.

1. To configure an area to allow instant arming, navigate to **Programming | Areas | Options 2** and check the **Enable instant arming** option in the **Advanced options** section of the area programming.
2. To enable instant arming from the keypad, you need to check the **Instant arming** option in the **Settings** section of the menu group which provides the user with access to this keypad.
3. At the keypad, log in and access the area menu. Select the area you want to instant stay arm, then hold down the **[STAY]** key for 2 seconds, or press the **[STAY]** key a second time while the area is in exit delay.

Force Arming

Force arming allows you to arm the system without waiting for designated inputs in the system to close or bypassing them. When an area is force armed it is armed without testing the inputs, and the area will be armed even if there are inputs open, provided these inputs have the force input option enabled. Force arming is commonly used when a motion detector is protecting an area that is occupied by a keypad. If the motion detector has been programmed as a force input, the system will allow you to arm the area even while the input is open.

Forced inputs are still supervised and can still generate alarms if closed and opened again.

1. To configure an area to allow force arming, navigate to **Programming | Areas | Options 2** and check the **Enable force arming** option in the **Advanced options** section of the area programming.

2. To enable force arming from the keypad, you need to check the **Force arming** option in the **Settings** section of the menu group which provides the user with access to this keypad.
3. To configure inputs so they can be forced, you will need an input type which has the **Force input** option enabled (**Programming | Input types | Options 1**).
4. For each input that you want to be ignored when the area is force armed (such as the motion sensor above the keypad) the area and the above 'force input' input type will both need to be assigned in the input programming (**Programming | Inputs | Areas and input types**).
5. At the keypad, log in and access the area menu. Select the area you want to force arm, then press **[FORCE]** to ignore any open 'force inputs' in the area and arm the area.

   If the command succeeds, you will see a message that the area 'is FORCE ARMED' and return to the area menu.

Additional Force Arming Options

- **Input types**: As an alternative to creating an input type which has the **Force input** option enabled, there are a number of preconfigured input types available in **Programming | Input types** that provide additional force arming functionality.
  - Instant Force: When the input is opened in an armed area the area goes into alarm immediately, the same as Instant, but the input can be force armed.
  - Delay Force: When the input is opened in an armed area the area begins the entry delay, the same as Delay, but the input can be force armed.
  - Delay Follow Force: 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. This is the same as Delay Follow, but the input can be force armed.
- **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 (**Programming | Input types | Options 2**) enabled, areas can be force armed even if inputs with this input type are tampered.

  The **Force input** option must also be enabled.

Instant Force Arming

Instant force arming reduces the exit delay to 1 second, and inputs which normally initiate the entry delay will instead set off the alarm immediately (i.e. all inputs are treated as 'instant').

The following steps to enable instant arming are required in addition to the force arming requirements above.

1. To configure an area to allow instant arming, navigate to **Programming | Areas | Options 2** and check the **Enable instant arming** option in the **Advanced options** section of the area programming.
2. To enable instant arming from the keypad, you need to check the **Instant arming** option in the **Settings** section of the menu group which provides the user with access to this keypad.
3. At the keypad, log in and access the area menu. Select the area you want to instant force arm, then hold down the **[FORCE]** key for 2 seconds, or press the **[FORCE]** key a second time while the area is in exit delay.

Defer Arming

Defer arming allows users to delay the normal automatic arming of an area for a specified time period. Whenever the area begins arming automatically by a schedule, 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.

A fixed defer time may be defined that will always be applied when arming is deferred, or the keypad can be configured to prompt users to enter a desired defer time on each occasion. Outputs may also be defined to give users a visual and/or audible indication that the area is about to arm.

Scheduled Automatic Arming

Defer arming is only applicable when the area has scheduled automatic arming configured in **Programming | Areas | Configuration**:

- **Arm/Disarm schedule**: This schedule is used to define when the area will arm and disarm automatically.
- **Arm area when schedule ends**: When this option is enabled the area will automatically arm when the arm/disarm schedule above becomes invalid.

  This feature force arms the area, so the **Enable force arming** option must be enabled (**Options 2** tab).

Programming Defer Arming

1. To configure an area to allow defer arming, navigate to **Programming | Areas | Options 2** and check the **Defer automatic arming** option in the **Arming options** section of the area programming.
2. The **Always verify area schedule** option must be disabled as it will override any defer arming.
3. In the **Configuration** tab, set the **Defer warning time** (in minutes) to define how long users will be warned before the area begins arming. The defer warning time begins when the arming schedule becomes invalid.
4. Select the **Defer warning keypad group**. Keypads in this group will beep once and display a warning message when the defer warning time begins.

   The **Display defer area warning messages** option (**Expanders | Keypads | Options 1**) must also be enabled for each keypad that you want the warning displayed on.
5. Set the **Rearm area time** to define the defer duration (in minutes) before rearming. After this elapses the area will automatically begin to arm again.
6. Alternatively, to enable a defer time to be entered at the keypad, in the **Commands** section add the command:
   `AskForDeferTime = true`

   With this command added to the area programming, when the user defers arming at the keypad they will be prompted to select the number of hours (1-9) to defer arming for.

   The minimum time that arming can be deferred from the keypad is 1 hour and the maximum is 9 hours. Arming can only be deferred in whole hours.

Operation

When the area is about to arm automatically, all keypads in the Defer warning keypad group will beep once and display the message '*WARNING* System is about to ARM!'. If left uninterrupted, the arming process will complete as normal after the configured defer warning time.

1. To defer arming, log in to the keypad during the defer warning time and press the **[DISARM]** key.
   - If your system has been configured to allow user entry of defer time, the keypad will prompt you to enter the defer arm time (in hours). Press any numeric key from **[1]** to **[9]** to select the number of hours to defer arming. Then press **[ENTER]**.

- If not configured to ask for defer time, the keypad will display that the area is disarmed, and arming will be deferred for the duration of the Rearm area time (**Programming | Areas | Configuration**).

2. The area will automatically re-enter the arming process after the defer time has elapsed.

Each time the arming process begins again the defer arming warning and process will repeat and you will have the opportunity to defer arming.

Additional Defer Arming Options

- **Area defer arming started output / output group**: This option (**Programming | Areas | Outputs**) provides an additional method for visual and/or audible notification that the area is about to arm. The output or output group selected here is activated whenever the area begins the defer warning. It is deactivated when the defer warning time expires and the area arms, or when the arming is canceled at a keypad.
  - **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.

Defer Arming + Automatic Rearming

An area can be configured to automatically rearm after being disarmed. If defer arming is to be used in conjunction with automatic rearming, the following programming is required in addition to the defer arming steps above.

1. In the **Options 1** tab of the area programming, check the **Re-arm enabled** option. When this option is enabled, whenever the area is disarmed it will be automatically rearmed after the **Rearm area time** has elapsed.
2. In the **Commands** section, add the command: `ReArmAsDeferArea = true`

   This command is required for defer arming to work alongside automatic rearming, for the system to be able to defer arming for the defined Rearm area time.

Additional Automatic Rearming Options

If you only want the area to automatically rearm when disarmed outside of its arm/disarm schedule, and not while the schedule is valid:

1. To prevent the automatic arming function from rearming the area while the schedule is valid, you will need to check the **Disable re-arm on schedule** option in the **Arming options** section in the **Options 2** tab.
2. In the **Commands** section, add the command: `ReArmLevelTrigger = true`

   This command is required to prevent the automatic arming function from rearming the area while the schedule is valid, in situations where the area is manually disarmed and not disarmed by schedule.

24HR Arming

Areas 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).

If the **Report 24hr area disarming** option is enabled (**Programming | Areas | Options 1**), whenever the 24HR portion of the 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.

Arming / Disarming

The 24HR portion of an area can be armed and disarmed at a keypad, or via manual commands in the Protege system user interface.

24HR Arming / Disarming via Keypad

To arm and disarm the 24HR portion of an area at a keypad, this option needs to be enabled for both the user (via menu group access) and the keypad.

1. To allow 24HR arming/disarming at a keypad, enable the **Allow 24hr area access** option in the **Options 1** tab of the keypad programming.
2. To authorize a user to arm/disarm the 24HR portion of an area, enable the **Tamper area control allowed** option in the **Settings** section of the menu group which provides the user with access to the relevant keypads.
3. At the keypad, log in and access the area menu. Press the **[LEFT]** key to view the current 24HR area status, then press either **[ARM]** or **[DISARM]** as required.

   If the command succeeds, the keypad will display 24HR Enabled or 24HR Disabled.

24HR Arming / Disarming via Manual Commands

To arm or disarm the 24HR portion of an area via manual commands:

- In Protege GX, navigate to **Programming | Areas** and right click on the area record.

  You can also right click on the area icon on a floor plan or status page.

  The operator's role must allow them full access to **manual commands** to perform this action.
- In Protege WX, navigate to **Monitoring | Areas** and click the **Controls** button for the area record.

  The operator's role must have the **Monitoring | Areas** option enabled to access this feature.

Disarm

- **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 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.
- **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.

24HR Arming Configuration

For information on configuring trouble inputs and other options for 24HR monitoring, see the Protege GX Operator Reference Manual or the Protege WX Programming Reference Manual.

Vault Control

Vault control introduces additional levels of keypad access control for high security installations, with a configurable disarm delay and optional dual code authentication.

- Vault control inserts a disarm delay period after the user initiates the disarm procedure at the keypad. This ensures that very high security areas such as bank vaults cannot be disarmed quickly in the event of a hold up.
- Dual code vault control requires that a second user disarms the area within a specified time limit after the above vault disarm delay period has elapsed.

Programming Vault Control

1. To enable vault control for an area, navigate to **Programming | Areas | Options 2** and enable the **Vault control area** option. When this option is enabled the area will not disarm until the delay period elapses.
2. In the **Configuration** tab, set the **Vault disarm delay** period. This field defines the delay time (in minutes) before the area will disarm, after the user initiates the disarm procedure at the keypad.

   If this time is set to 0 the area will be disarmed immediately.

3. To enable dual code vault control for the area, enable the **Dual code vault control** option (**Options 2** tab). When this option is enabled a second user must log in to the keypad and press the disarm button within the defined time restriction, after the above vault disarm delay period has elapsed.

   The **Vault control area** option must be enabled for dual code vault control to operate.

4. If dual code vault control is enabled, set the **Vault dual code delay** limit (**Configuration** tab). 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 exceeds this limit, the disarming process will end and a user would need to log in and restart the disarming process.

   The keypad does not display when the vault disarm delay has expired.

Operation

1. At the keypad, log in and access the area menu, then press **[DISARM]**.
   The keypad will display in DISARM delay.
   - Until the **Vault disarm delay** period has expired, the keypad will display in DISARM delay any time a user logs in, but the keypad will not display or notify when the disarm delay period ends.

   When no user is logged in, the keypad displays the standard idle text.

2. If dual code vault control is **not** enabled, the area will disarm at the end of the **Vault disarm delay** period.
3. If dual code vault control **is** enabled, a second user must log in after the disarm delay period to disarm the area.
   - After the disarm delay period has expired, whenever a user logs in the keypad will display in CODE delay.
   - If a second user logs in during this time and presses **[DISARM]** the area will disarm.
   - If the first user logs in and attempts to disarm the area, the keypad will display The code is not allowed!.
   - If the **Vault dual code delay** period expires before a second user disarms the area, the disarming process will end, the area remains armed and a user would need to log in and restart the disarming process.

Hold Up Area Walk Test

In high risk environments it is paramount that safety features are tested regularly to ensure they remain functional. The Protege GX hold up area walk test feature is designed to ensure that critical inputs such as panic or duress buttons are manually tested on a regular basis.

Once the walk test has been configured, the area will enter walk test mode each time a user disarms the area from a keypad. While in walk test mode, every specified input must be tested (opened) before the area is disarmed.

During the test, an output or output group can be activated to notify users that they need to test nearby inputs. The progress of the test is displayed on the keypad and in the Protege GX event log as each input is tested, and preconfigured Contact ID codes are sent to the monitoring station at each stage of the test.

For programming instructions, see Application Note 197: Configuring a Hold Up Walk Test in Protege GX.

Output Control

Protege keypads provide a range of options for controlling outputs.

User Login Output Control

Outputs can be automatically activated or toggled when authorized users log in to keypads. This is a great way to control lighting and other utilities that may be needed on entry to a space.

Outputs are assigned to access levels to allow management of which users are authorized to control which outputs and when.

1. To assign outputs to access levels, navigate to **Users | Access levels** and select the access level(s) to update.
2. In the **General** tab, enable the **Keypad access activates output** option. When this option is enabled, all the selected outputs will be activated when a user logs in to a keypad using this access level.
3. Select one of the following deactivation options:
   - Set the **Time to activate output** to define a fixed time (in seconds) that the output will remain activated. When this time expires the output will turn off.
   - Check the **Activate output until access level expiry** option to deactivate the output when the access level expires in the user record of the user whose login activated the output.
   - Check the **Toggle access level output** option to toggle the state of the output each time it is triggered by the access level. The first time a user logs in the output will turn on. The next time the output will turn off.
4. In either the **Outputs** or **Output groups** tab, click **Add** and select the output(s) to control, then click **OK**.
5. Click **Save**.
6. Navigate to **Expanders | Keypads | Options 1** and enable the **Activate access level output** option for each keypad that will activate outputs when a valid user logs in.

For programming examples, see Application Note 204: Access Level Outputs in Protege GX.

Arming / Disarming Output Control

The following programming options (**Programming | Areas | Outputs**) allow outputs to be activated in relation to area arming and disarming activities.

- **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.
- **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.

- **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.
- **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 processed 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.
- **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.
- **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.

Automation

Automations 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.

1. For a user to be authorized to access the automation menu at a keypad, the access level that they use to log in to the keypad must have a menu group assigned which has the **View (5)** menu enabled.
2. Users activate automations from a keypad by logging in and pressing **[MENU] [5] [5]**.
   - Scroll up/down the available automation list and select an automation.
   - Press **[1]** to activate the automation for the duration defined in the automation's **Automation output time**.
   - Press **[2]** to deactivate the automation.
   - Press **[3]** to activate the automation indefinitely.

If preferred, automations can be accessed without logging in to the keypad. This needs to be configured on each keypad by enabling the **Offline access to automation menu** option (**Expanders | Keypads | Options 2**). When enabled, users can access the keypad's offline menu by pressing **[MENU] [1]**.

Information on automation options and full programming instructions can be found in the Protege GX Operator Reference Manual and the Protege WX Programming Reference Manual.

Programmable Functions

For advanced output control from keypads, automations can be used to trigger complex control programming functions. Programmable functions are special processes that generally have a trigger - such as an output turning on - which causes the controller to activate the process. This output could easily be set up as an automation so that the programmable function can be manually activated from the keypad.

For an example of advanced programming using programmable functions, see Application Note 208: Emergency Egress and Lockdown Programming.

Door Access Options

Keypads can be used for door access, either using the function key as a simple REX/REN type of access (with or without login) or using the keypad in conjunction with a reader for two factor authentication (card + PIN).

Function Key Door Access

The keypad function key can be used to unlock a specific door from the keypad, either requiring valid user login or as a simple REX/REN door access operation without any login required.

When this feature is enabled, users can unlock the door by pressing the **[FUNCTION]** key (holding the **[MENU]** key for 2 seconds on the PRT-KLCS).

1. Navigate to **Expanders | Keypads | Configuration** and select the **Door connected to keypad**. Setting a door in this field allows users to unlock it from the keypad using the function key.
2. In the **Options 1** tab:
   - To require users to log in to the keypad before pressing the **[FUNCTION]** key to unlock the door, enable the **Function key unlocks door when logged in (REX)** option.
   - To allow users to unlock the door by pressing the **[FUNCTION]** key without logging in to the keypad, enable the **Function key unlocks door when logged out (REX)** option.

For an additional security option, keypads can be used in conjunction with card readers to require two factor authentication (card + PIN) for keypad access before a door can be unlocked using the function key (see page 7).

Keypad as PIN Pad

For an additional security option, the keypad can be used in place of a PIN pad to require two factor authentication (card + PIN) for door access.

With this option enabled, users must badge a card at the assigned reader then enter a PIN at the keypad (two factor authentication) to be granted access to the door.

1. Navigate to (**Programming | Doors**) and select the door.
2. The door must be configured with a **Door type** which requires Card and PIN access, otherwise badging a card will not trigger the associated keypad to require PIN entry.
3. Click **Save**.
4. Navigate to (**Expanders | Reader expanders**) and select the expander for that door's reader.
5. Set the **Reader 1/2 keypad type** to LCD Keypad.
6. Set the **Keypad to use for PINs reader 1/2** to the keypad that will be used for PIN entry.
7. Click **Save**.

Operation

1. When a user presents a valid card at this door's reader, the keypad selected above will beep rapidly and display User access code:.
2. The user can now enter their PIN at the keypad and press **[ENTER]** to be authenticated.
3. If the user is granted access the door will unlock.

PIN entry is allowed for the **Time user is logged in** setting duration (**Expanders | Keypads | Configuration**). If this expires before the user enters their PIN they will need to badge their card at the reader again.

Prompt User for Access Reason

The Protege system can be configured to record an access reason when users access certain doors. 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.

This feature needs to be enabled for the required doors, and linked to the appropriate keypad via the reader expander.

1. Navigate to **Programming | Doors** and select a door to enable this feature for.

   This feature is not supported by doors configured for card and PIN operation.

   - In the **Advanced options** tab, enable the **Prompt user for access reason code** option.
2. Navigate to **Expanders | Reader expanders** and select the reader expander and **Reader 1/2** tab that the door's card reader is connected to.
   - Set the **Reader 1/2 keypad type** to LCD keypad.
   - Set the **Keypad to use for PINs reader 1/2** to a keypad adjacent to the door.

Operation

1. When a user badges their card at the reader, the keypad will prompt them to enter an Area from 001-009.
2. Press any numeric key from **[1]** to **[9]** to enter the required access code, then press **[Enter]**.
3. Door 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.

Keypad Configuration

LED 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**.

Disarmed Indicator

This indicator is programmable and can perform one or more functions in the Protege system. The following are common functions:

- To illuminate this LED when an area is disarmed, program it as the **Disarmed output** for the area.
- To illuminate the LED when an area is ready to arm (i.e. all inputs are closed), program it as the **Ready output** for the area.

Armed / Alarm Indicator

This indicator is programmable and can perform one or more functions in the Protege system. The following are common functions:

- To illuminate this LED when an area is armed, program it as the **Armed output** for the area.
- To flash this LED when an area is in alarm (until the alarm times out or the area is disarmed), add it to the **Bell output group** for the area. Use the **Bell pulse on/off time** settings to pulse the LED on and off.
- To flash this LED when an area has had an alarm (until the area is disarmed), program it as the **Alarm memory output** for the area. Use the **Alarm memory pulse on/off time** settings to pulse the LED on and off.

Confidentiality Mode

Keypads include a confidentiality mode where activation of the onboard output will cause all lights (power, disarm, arm and LCD backlight) to turn off when the keypad is not in use.

When the onboard output is not activated these lights serve their normal functions.

PRT-KLCS

This feature must be enabled by entering the following command in the keypad programming:

```
ConfidentialMode = true
```

Confidentiality mode is available for PRT-KLCS keypads with firmware version 1.09.013 or later.

PRT-KLCD

This feature is enabled by default. It may be disabled by entering the following command in the keypad programming:

```
ConfidentialMode = false
```

Confidentiality mode is available for PRT-KLCD keypads with firmware version 1.46 or later.

Disable Keypad Beeper

In some environments it may be desirable to disable the keypad beeper, to minimize noise from key presses.

Expanders | Keypads | Options 2:

- **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.

- **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.

Keypad Display Settings

The default text which is shown on a keypad when no user is logged in can be configured in the **Display** settings of each keypad's programming (**Expanders | Keypads | General**).

- **Default display line one / two**: Each line on the keypad can display up to 16 characters, which may be letters, numbers or punctuation.

  This custom text will be displayed when the **Display custom message** option is enabled (**Options 1** tab). If any of the other available **Display options** are enabled they will override the custom message.

  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:

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).
&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.

Time and Attendance

Keypads can be configured to display time and attendance details, providing visual feedback and confirmation to a user when signing in or out using an ICT reader. When a user badges at the reader their name and the recorded time and date are displayed on the keypad associated with that door.

Protege GX

To enable time and attendance details to be displayed on a keypad connected to a Protege GX system:

1. Navigate to **Expanders | Keypads** and select the keypad that will be used to display these details.
2. In the **Configuration** tab, ensure that the **Door connected to keypad** is the entry/exit door where users present their credentials when entering or exiting the building or workspace.
3. In the **Options 1** tab, enable the **Show time and attendance detail** option.

   Important: None of the other **Display options** should be selected. All other options take priority and override the time and attendance setting, so if any are selected time and attendance will not be displayed.
4. Specify the **Length of time to display attendance detail** on the keypad (in seconds).
5. Set the **Attendance date format** to be displayed (MM/DD/YY or DD/MM/YY).
6. Click **Save**.

For more information on time and attendance, including configuring shift times to report attendance, breaks and hours worked, and attendance report setup, see Application Note 308: Time and Attendance in Protege GX.

Protege WX

To enable time and attendance details to be displayed on a keypad connected to a Protege WX system:

1. Navigate to **Expanders | Keypads** and select the keypad that will be used to display these details.
2. In the **Commands** field, enter the following commands:

   ```
   ShowT&ADetail = true
   T&ADisplayTime = 10
   Date Format = D/M/Y
   ```

Line	Command	Description
Line 1	ShowT&ADetail	Enables and disables the feature.
Line 2	T&ADisplayTime	Defines (in seconds) how long the details are displayed on the keypad. Valid values are from 1 to 50.
Line 3	Date Format	Defines how the date is displayed. Valid values are D/M/Y or M/D/Y.
3. In the **Configuration** tab, ensure that the **Door connected to keypad** is the entry/exit door where users present their credentials when entering or exiting the building or workspace.
4. In the **Options 1** tab, enable the **Display custom message (lines 1 and 2)** option.

   Important: None of the other **Display options** should be selected. All other options take priority and override the time and attendance setting, so if any are selected time and attendance will not be displayed.
5. Click **Save**.

For more information, see Application Note 177: Time and Attendance on a Protege WX Keypad.

Keypad Programming Settings

The following section describes the configuration settings and options available in the keypad programming.

Many of these settings are dependent on additional requirements and work in conjunction with programming in other areas of the Protege system.

For Protege GX, any settings changed here will require a module update to apply the settings to the keypad. After saving, right click on the keypad record and select **Update module**.

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.

Input 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**.

User Keypad Options

The following settings (found in **Users | Users | Options**) allow keypad access and functionality options to be customized for individual users.

General Options

- **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 can edit user settings from keypad**: This function is only applicable to keypads connected to Protege WX systems. When enabled the user can add new users, modify user settings and delete users, from a keypad. This should generally be enabled for system administration users only.

  When this option is enabled the user is not able to edit their own PIN code on the keypad, except when prompted due to an expired PIN.

  The user's access level menu group must have the **User (2)** menu enabled to access the keypad **User Menu**.
- **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.

User Management

Keypads connected to Protege WX systems can allow authorized users to perform user management functions from the keypad. The keypad user management feature provides a quick and convenient way to manage users on the fly, including adding new users to provide instant access, modifying incorrect user settings, and deleting user records to immediately withdraw access.

1. For a user to be authorized to access user management at a keypad, they must have the **User can edit user settings from keypad** option enabled (**Users | Users | Options**).

   This should generally be enabled for system administration users only.

2. For a user to access the user menu to perform user management, the access level that they use to log in to the keypad must have a menu group assigned which has the **User (2)** menu enabled.

This feature is only available for keypads connected to Protege WX systems.

For more information on user management operation, including adding, modifying and deleting users at the keypad, refer to the appropriate keypad user manual.

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