AN-327

Configuring Security Enhancements in Protege WX

Application Note

Last Published: 13-Dec-21 5:15 PM

Contents

Security Enhancements in Protege WX

The security enhancement feature in Protege WX provides greater control over keypad security and the use and maintenance of user PINs.

With this feature you can require users to present dual credentials (both User ID and PIN code) to gain access to a keypad. In addition, security enhancement settings allow you to specify PIN expiry periods, PIN generation and complexity rules, and whether the site will allow duplicate PINs.

This application note provides instructions on programming security enhancement settings in Protege WX, applying these settings to user credentials, and performing the relevant operations at a keypad.

Prerequisites

The following versions are required to use this feature.

Component	Version
PRT-WX-DIN	4.00.611 or higher
PRT-WX-DIN-1D	

Configuring Security Enhancements

Security enhancements fall under two categories - dual credential settings and PIN complexity rules - which can be configured independently of one another.

1. To configure security enhancement settings, navigate to **System | Settings**.
2. Open the **Security enhancement** tab and define the settings as required.
   - Require dual credential for keypad access
   - Allow PIN duplication
   - Default PIN length (select from 4 digits up to 8 digits)
   - Minimum PIN length (select from 1 to 8 digits)
   - Maximum sequential digits (select from 2 to 4)
   - Maximum repetitive digits (select from 2 to 4)
   - PIN expiry time (select from Never, 1 month, 2 months, 3 months, 6 months, 12 months).
3. Then click **Save**.

Dual Credential Settings

Once enabled, the dual credential requirements will apply to all users.

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.

The Allow PIN duplication option is not accessible until the feature is enabled.

Allow PIN Duplication

Enabling this feature allows the creation of identical PINs among user records for the site. Each user will be required to enter a unique User ID to identify themselves as well as a PIN, allowing the system to accurately identify the user logging in to the keypad and maintaining the integrity of site security.

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

PIN Complexity Rules

The following settings allow you to define the rules which dictate PIN security requirements for the site.

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. This option prevents simple PINs with obvious sequential digits, such as 1234 or 4321.

For example, selecting 3 will allow a PIN to include a numerical sequence of 123 or 321, but not 1234.

Maximum Repetitive Digits

The maximum number of repeated digits permitted for PINs, between 2 and 4 digits. This option prevents simple PINs such as 1111 or 2222 where the same digit is used repeatedly.

For example, selecting 3 will allow a PIN containing 222, but not 2222.

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.

Assigning Dual Credentials to a User

If the dual credential feature is enabled, all users will require both a valid PIN and a User ID in order to be authenticated at a keypad.

1. Navigate to **Users | Users**.
2. Add a new user or select a user to assign a PIN and User ID to.
3. In the **PIN Code** section, enter a PIN from 1 to 8 digits (depending on your PIN complexity settings).

   If your dual credential settings do not allow PIN duplication, you will not be able to enter a PIN that is already assigned to another user.

4. Optionally, select the **PIN Expiry Time** for the user's PIN.
   If selected, this overrides the **PIN Expiry Time** setting set in the security enhancement programming.
5. Open the **Credentials** tab. The user will have a default User ID **Credential Type** assigned.
6. In the **Credential** field, enter a unique ID for the user, up to a maximum of 16 digits.

   The ID must be unique. You will not be able to enter an ID that is already assigned to another user.

7. Once a PIN and User ID have been added to the user, an appropriate Access Level will need to be assigned in order for the user to be granted access to keypads. Open the **Access Levels** tab and **Add** the required level(s).
8. Click **Save**.

Once the **Require dual credential for keypad access** option is selected, no user can be added or edited without a valid User ID. Attempting to add or update a user without a User ID will produce an **Error** warning.

Operation

Logging In to a Keypad Using ID+PIN

When the site has been configured to **Require dual credential for keypad access**, a user is required to enter both their ID and PIN when logging in to a keypad. The steps are as follows:

1. The user enters their **User ID** on the keypad and presses **Enter**. The keypad will display **Enter user PIN**.
2. The user enters their **PIN** and presses **Enter**.
3. Depending on the options set in the keypad, the user will be presented with a welcome message, or the status of an area will be displayed.
4. The user can then use the scroll keys to navigate the menu to arm/disarm areas, acknowledge alarms, and otherwise operate the keypad as normal.

Changing a PIN Using a Keypad

A user can change their PIN through the keypad. The steps are as follows:

1. The user logs in to the keypad by entering their ID and PIN.
2. The user presses the **Menu** key.
3. The user presses the **Arrow Up** key to advance to the **Users** option, then presses the **Enter** key to select.
4. The **Edit PIN** option will be displayed and the user presses **Enter** to select.
5. The keypad display will prompt the user to enter a new PIN.
6. The keypad display will then prompt the user to re-enter their new PIN.
7. The keypad will display **Verified. Saving Changes** and will automatically log the user out of the keypad. They may then log in using their ID and new PIN.

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