AN-275

Configuring Site Security Enhancements in Protege GX

Application Note

Last Published: 13-Dec-21 5:09 PM

Contents

Site Security Enhancements in Protege GX

The site security enhancement feature in Protege GX 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. User IDs can be automatically generated for each user, or entered manually to allow use of existing identifiers such as employee or student ID numbers. 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 site security enhancement settings in Protege GX, 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
Protege GX software	4.2.251 or higher The **Autopopulate User ID credential value** feature is available from version 4.3.308.2
PRT-CTRL-DIN	2.08.692 or higher
PRT-CTRL-DIN-1D	

Configuring Site Security Enhancements

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

1. To configure site security enhancements, navigate to **Global | Sites** and select the site to update.
2. Open the **Site defaults** tab and in the **Site security enhancement** section define the settings as required.
   - Require dual credential for keypad access
   - Autopopulate User ID credential value
   - 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).
   - New PIN to be generated by system
3. Then click **Save**.

Dual Credential Settings

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

Important: When the dual credential feature is enabled, operators are no longer able to view user PIN codes in the user interface. This includes operators with the **Show PIN numbers for users** option enabled.

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 remaining dual credential settings are not accessible until this feature is enabled.

Autopopulate User ID Credential Value

This option is available from software version 4.3.308.2.

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.

On very large sites, it may take a long time for the system to generate a unique User ID for every user when this option is enabled for the first time. Do not close the Protege GX client during this process.

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.

New PIN to be Generated by System

With this option enabled, when a user's PIN expires the system will automatically generate a unique random PIN that follows the PIN complexity guidelines. Any permanent PIN (other than a temporary single-use PIN created by the operator) must be generated by the system. If an expired PIN is used to log in at a keypad the system will automatically present the user with a new PIN. A user can also request a new PIN when logging in at a keypad.

Requires **PIN expiry time** to be set.

Assigning Dual Credentials to Users

If the dual credential feature is enabled, all users will require both a valid PIN and a User ID in order to log in to a keypad. Various methods for adding and editing user records are outlined below.

Adding/Editing Users in the Users Menu

When the dual credential feature is enabled, the system will not allow operators to add or edit user records in the **Users | Users** menu without adding a valid, unique User ID.

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** section, enter a PIN or create a random PIN by clicking on the **4**, **5** or **6** digit PIN generator button.

   Note down the user's PIN, as it will not be visible to operators after the record has been saved. If the **PIN expiry time** has been set in the site programming above, this is a single use PIN which the user must change the first time they log in to the keypad.
4. Optionally, select the **PIN expiry time** for the user's PIN. If selected, this overrides the **PIN expiry time** setting set in the site programming above.
5. Scroll down to the **Credentials** section to configure the User ID credential type:
   - In the **Credential** field, enter a unique User ID value. This may have 1-10 digits.
   - To automatically generate a unique 8-digit PIN, enter **SYSTEM** in the **Credential** field. A random, unique 8-digit PIN will be generated for this user when the record is saved.
   - If **Autopopulate User ID credential value** is enabled, the **SYSTEM** feature will be used by default. Alternatively, you can manually set a custom value.
6. 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 access level(s).
7. 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.

Adding/Editing Users from Events

When an unknown card or other credential type is detected, operators can right click on the 'Read Raw Data' event to add the credential to a new or existing user record. With the dual credential feature enabled, the software also requires you to assign a User ID to the user record.

To add a new card/credential and User ID:

1. Badge an unknown card or other credential.
2. On a status page or floor plan, you should see a 'Read Raw Data' or 'Read Raw Credential Data' event.
3. Right click on the event and click either **Add new user** or **Add card number to existing user**.
4. If you are creating a new user, or adding the credential to an existing user without a User ID assigned, you will be required to assign a User ID before saving the user record:
   - If **Autopopulate User ID credential value** is enabled, a unique 8-digit User ID is automatically assigned.
   - If **Autopopulate User ID credential value** is disabled, the **Credential population options** window will pop up. You can either select **Autopopulate User ID credential value** to automatically generate a unique 8-

digit number, or enter a custom number in the field below and click **Ok**.

5. The user record is saved or updated.

Importing and Batch Adding Users

When the dual credential feature is enabled, it is not possible to import or batch add users without valid User IDs.

- If **Autopopulate User ID credential value** is enabled, a unique 8-digit User ID will be automatically assigned to each user when the import or batch add process is completed.
- If **Autopopulate User ID credential value** is disabled, an error will inform you that it is not permitted to add new users without a User ID. No user records will be added.

Before Protege GX version 4.3.308.2, it is possible to import and batch add users without User IDs. If this occurs, the operator must go to the **Users | Users** menu and manually assign IDs to the new users (see previous page).

Adding/Editing Users with the SOAP Service

When **Require dual credential for keypad access** is enabled, the following rules apply for adding/editing users via the Protege GX SOAP service:

- When adding a user via SOAP, you can add or update the User ID with the `<UserCredentialGroupData>` tag.
- If **Autopopulate User ID credential value** is disabled, it is not possible to add or update a user record without a User ID. If a new or existing user record does not have a User ID, the SOAP call will return error code 9 (`CREDENTIAL_SAVE_FAILED`). The `<UserID>` credential type must be defined in the SOAP call to assign a unique value to the user.

  If an existing user record already has a User ID assigned, it is not necessary to reassign the ID in future SOAP calls.

- If **Autopopulate User ID credential value** is enabled, you can add or edit a user record without a User ID credential type. The system will automatically generate a unique 8-digit User ID and assign it to the user.

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.