AN-286

Programming Compliance Types in Protege GX

Application Note

Last Published: 09-Nov-21 1:47 PM

Contents

Introduction

Protege GX Compliance Types allow you to control access to doors based on compliance requirements, extending the existing functionality of Credential Types. Any custom requirement from industry certifications to site safety training can be used as a credential alongside standard cards and PINs to improve compliance on site.

Possible applications for Compliance Types include:

- Health and Safety Training that users are required to complete periodically.
- Completion of company or job site induction.
- A certain class of driver's license or vehicle certification.
- Industry Training certificates or qualifications.

With a compatible reader display, such as the ICT Touchscreen Card Reader, you can even display messages to the user to inform them of their compliance status and prompt them to take action.

This application note describes the basic steps required to set up Compliance Types in the Protege GX software.

Prerequisites

- An operational Protege GX system running software version 4.3.285 or higher.
- A Protege GX Controller with firmware version 2.08.1000 or higher.
- Reader Expanders using this feature require firmware version 1.12.582 or higher.
- If the warning and expiry message features are to be used, Protege card readers with screens (such as the PRT-TS35) are required to display this text to the user. The controller firmware will automatically detect when a compatible display is present on the onboard Reader Expander.

Programming Steps

The programming for Compliance Types is very similar to that for regular Credential Types, with some additional options. The main programming steps are:

- Creating a Compliance Type
- Creating a Door Type for the Compliance Type
- Assigning the Door Type to doors
- Assigning the Compliance Type to users

Creating a Compliance Type

1. Navigate to **Sites | Credential Types** and add a new Credential Type.
2. Set the **Format** to Compliance.
3. When compatible card readers are installed, they can display a warning message to users for a set period before their compliance expires, and an expiry message after it expires. These messages are displayed when the user badges their card at the reader, and must be acknowledged before access is granted.

   If you wish to set up warning and expiry messages for users with this Compliance Type, set the following:

   - **Warning Period**: The number of days before the compliance expires that the **Warning Text** will be displayed to the user.
   - **Warning Text**: The message that will be displayed on the card reader screen to warn users that their compliance is about to expire. Users must acknowledge the warning before they will be granted access.
   - **Expiry Text**: The message that will be displayed on the card reader screen to inform users that their compliance has expired. If the compliance type is configured for soft failure, the user must acknowledge the expiry notice before they will be granted access.

     Due to the size of the reader screen, compliance messages are restricted to 32 characters.

4. Set what will happen when this Compliance Type expires for a user:

   - **Hard Failure**: When this option is enabled the user will be denied access when their compliance has expired.

     When this option is disabled (soft failure), if a user's compliance has expired the expiry message will be displayed but access is still granted. The user must acknowledge the expiry notice before they will be granted access.
   - **Never Expires**: When this option is enabled the compliance type will be treated as if it never expires for any user, regardless of whether an expiry date has been set. Both the **Start Date** and the **End Date** in the user programming will be ignored.

Creating and Assigning the Door Type

1. Navigate to **Programming | Door Types** and create a new door type.
2. In the **General** tab, set the **Entry Reading Mode** to Custom.
3. This opens the **Entry Credential Types** field. Click **Add** to add the required credentials, e.g. card and compliance type.

   Door types must always include a physical credential (e.g. card, PIN, biometric) alongside the compliance type, otherwise access will be denied to all users. Physical credentials must always be presented first before compliance is checked, regardless of the position of the compliance type in the credential list and whether sequencing is enabled or not.

4. If required, repeat the above for the **Exit Reading Mode**.

5. Scroll back up to the **General Configuration** section. Set the following as required:
   - **Allow soft failure on missing compliances**: When a user who does not have the required compliance type requests access, they will not be denied access. If connected, a touchscreen card reader can display a notification message that must be acknowledged before access is granted.

     This option is enabled by default.
   - **Message**: Enter the message that will be displayed when a user is missing a required compliance type. The maximum message length is 32 characters.
6. Navigate to **Programming | Doors** and select the doors that are required to check compliance for access. In the **General** tab, set the **Door Type** to the one created above.

Assigning the Compliance Type to Users

1. Navigate to **Users | Users** and select the users who have the required compliance qualifications.
2. In the **General** tab, scroll down to **Credentials**. Click **Add** to add a new credential and set the **Credential Type** to the Compliance Type created above.
3. Configure the following options as required:
   - **Disabled**: Disables that credential for the user without deleting it.
   - **Start**: Set a start date for the credential.
   - **End**: Set an expiry date for the credential.

     It is not necessary to enter any data in the **Credential** field for a Compliance Type.

A user can have up to 32 unique Compliance Types assigned to them. However, duplicates of the same Compliance Type cannot be assigned to a single user.

Acknowledgment and Reporting

When the Warning and Expiry Text features are in use with a compatible reader display, the user is required to acknowledge any compliance related messages before access is granted or denied for the door.

This acknowledgement will generate an event in Protege GX:

- **Warning Event**: User <USER_NAME> Acknowledged Compliance Warning <CREDENTIALTYPE_NAME> at Door <DOOR_NAME>.
- **Expiry Event**: User <USER_NAME> Acknowledged Compliance Failure <CREDENTIALTYPE_NAME> at Door <DOOR_NAME>.

  > The Expiry event will be displayed regardless of whether the expired Compliance Type is set to soft or hard failure.

- **Missing Event**: User <USER_NAME> Acknowledged Compliance Missing <CREDENTIALTYPE_NAME> at Door <DOOR_NAME>.

These events can be used to generate reports containing a record of the user's acknowledgement of any compliance issues. You can search for all users who have generated a specific event with a User Report (**Reports | Setup | User**) by setting the **Report Type** to All Users by Events and applying an appropriate Event Filter.

Programming Scenario: Soft Compliance

Many facilities require regular health and safety training to ensure that machinery, chemicals and other dangerous items are handled correctly on site. Missing or expired certification should be brought to the attention of employees, but access to factory or laboratory areas should not be denied.

This programming example demonstrates how to set up a 'soft compliance' scenario for health and safety certification. When a user has missing or expired health and safety certificate or when their certificate is about to expire, they will receive a warning whenever they attempt to enter a working area. They must acknowledge the warning before they are allowed to enter.

An event will be generated in Protege GX when the warning is acknowledged, allowing operators to report on users who need health and safety training.

Follow these steps to program to the software to meet the above requirements:

1. Navigate to **Sites | Credential Types**.
2. Add a credential type called Health & Safety.
3. In the Configuration section, set the credential type **Format** to **Compliance**.
4. Set the **Warning Period** to 30 days.
5. Add a **Warning Text** message: H&S Cert expires soon. See HR.
6. Add an **Expiry Text** message: H&S Cert expired. See HR today.
7. Uncheck the **Never Expires** option.
8. Uncheck the **Hard Fail** option.
9. **Save** the record.
10. Navigate to **Programming | Door Types**. Assign the compliance credential type to the **Entry Credential Types** for the required Door Type.
11. Check the **Allow soft failure on missing compliances** option.
12. Add a **Message**: H&S Cert not completed. See HR.
13. In **Programming | Doors**, assign the new Door Type to the relevant doors. In this example, this should be the entry doors for the factory or laboratory.
14. In **Users | Users**, assign the **Credential Type** to Users and set an **Expiry Date** based on your site's certification data.
15. A User Report can be used to track which users have acknowledged compliance messages:
    - In **Events | Event Filters**, add a new Event Filter called Compliance Acknowledgements. In the **Event Types** tab, add the 'User acknowledged Compliance Failure', 'User acknowledged Compliance Missing' and 'User acknowledged Compliance Warning' events.
    - In **Reports | Setup | User**, add a new User Report called Users who need H&S Training. Set the **Report Type** to All Users by Events and add the **Event Filter** created above.
    - Now the report can be run manually from **Reports | User**, or automatically exported using the **Email** or **File Export** tabs.

Programming Scenario: Hard Compliance

Some high-risk or strictly regulated industries require high standards of compliance to ensure that only certified people can enter working areas. Any user with missing or expired industry certification should not be allowed to enter restricted areas, even if they meet other access requirements.

This programming example demonstrates how to set up a 'hard compliance' scenario for industry certification. The user will receive a warning when their access is about to expire, but if certification is expired or missing access will be denied.

Follow these steps to program to the software to meet the above requirements:

1. Navigate to **Sites | Credential Types**.
2. Add a credential type called Special Certification.
3. In the Configuration section, set the credential type **Format** to **Compliance**.
4. Set the **Warning Period** to 30 days.
5. Add a **Warning Text** message: Cert expires soon. Contact Admin.
6. Add an **Expiry Text** message: Cert has expired.
7. Uncheck the **Never Expires** option.
8. Check the **Hard Fail** option.
9. **Save** the record.
10. Navigate to **Programming | Door Types**. Assign the compliance credential type to the **Entry Credential Types** for the required Door Type.
11. Uncheck the **Allow soft failure on missing compliances** option.
12. Uncheck the **Message** option. Leave the text field blank.
13. In **Programming | Doors**, assign the new Door Type to the relevant doors. In this example, this should be the entry doors for the restricted areas.
14. Assign the **Credential Type** to Users and set an **Expiry Date** based on your site’s certification data.

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

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.