AN-219

Intercom Integration using Credential Types in Protege GX

Application Note

ICTeSecurity®

Publication Date: January 2017

Contents

Intercom Integration using Credential Types

Intercom integration allows data to be passed directly from the intercom device to the Protege GX Controller and can be implemented through either the use of the Protege GX intercom service, or by utilizing the **Credential Types** feature.

This application note provides instructions on using **Credential Types** to implement intercom integration with Protege GX.

Credential Types

Credential types are created within the Protege GX interface and are applied to custom **Door Types** as the **Entry Reading Mode** and/or the **Exit Reading Mode**. The intercom device or software that is used to collect the credential data is configured as a **Smart Reader**, with data being sent to the controller by either the onboard RS-485 reader ports or over Ethernet.

Prerequisites

This integration requires:

- An operational Protege GX system using version 4.2.187 or higher.
- A Protege GX controller running firmware version 2.08.0752 or higher.
- The required number of smart reader licenses applied to the relevant Protege GX SSN.

Overview

The steps required to implement the intercom integration using credential types within Protege GX are:

- Configuring the onboard Reader Expander.
- Creating a new **Credential Type** and **Door Type** unique to the needs of the Intercom.
- Creating a virtual door and **Smart Reader**.
- Creating virtual Outputs.
- Creating **Floors** and **Schedules**.
- Creating **Access Levels** and user credentials.
- Assigning **Access Levels** to **Users**.

Setup and Configuration

Programming Walkthrough

We will set up a simple scenario that demonstrates how to implement intercom integration in Protege GX through the use of the **Credential Types** feature. This will give you an idea of what to expect when it comes to setting up your own intercom.

In this scenario we are implementing intercom integration in a building where we have:

- Eight floors in total.
- There are seven secured floors, starting at the first floor, with floor seven at the top of the building. The ground floor is freely accessible and contains an Intercom.
- One elevator car with access to every floor.
- Each floor (excluding the ground floor) contains three apartments, where suite 502 refers to apartment 2 on level 5.

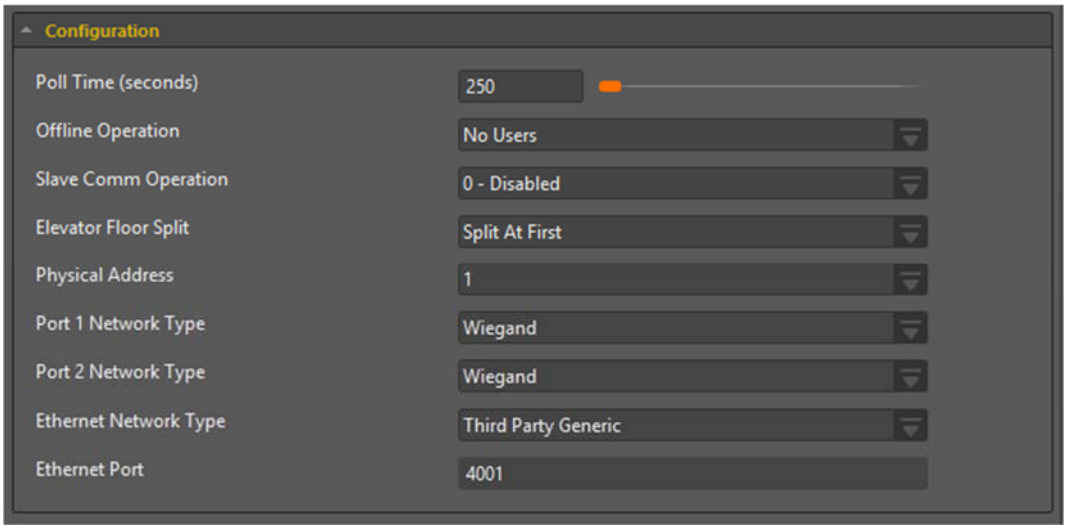
Configuring the Onboard Reader Expander

To enable the third party device or application to communicate with the Protege GX controller, you need to configure the controller's onboard reader expander.

If the third party device uses an RS-232 connection, you must use an RS-232 to RS-485 converter to connect it to the Protege GX controller.

If the device is connected over Ethernet:

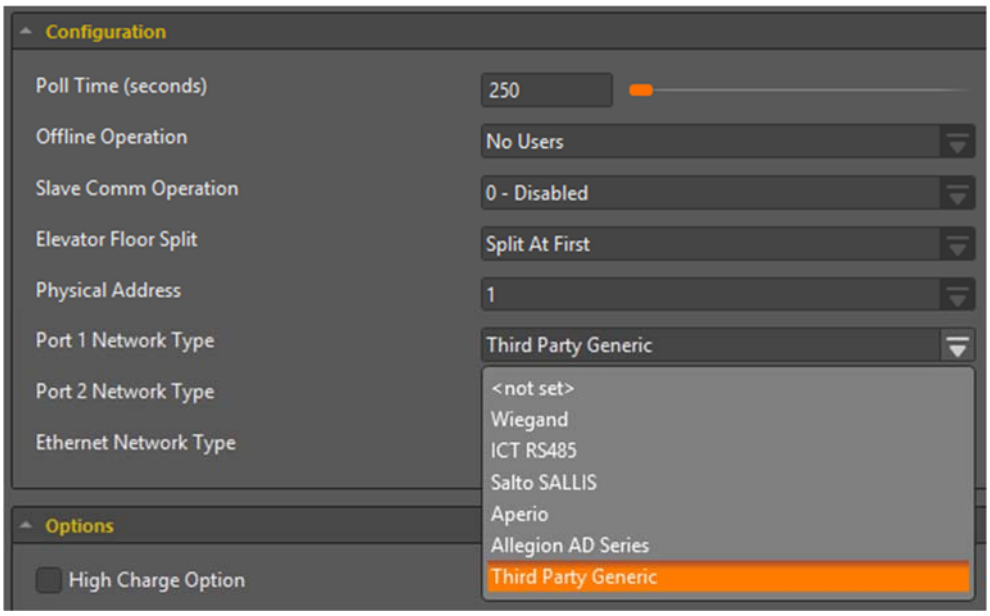
1. Navigate to **Expanders | Reader Expanders.**
2. Select the controller's onboard reader expander.
3. In the **Configuration** section, set the following options:



   - **Ethernet Network Type**: **Third Party Generic.**
   - **Ethernet Port**: Defines the TCP/IP port that the controller listens on. The intercom device must have this port open in order to send data to the controller. Contact your network administrator to find out which port to use
4. Click **Save**.

If the device is connected to one of the onboard reader expander reader ports:

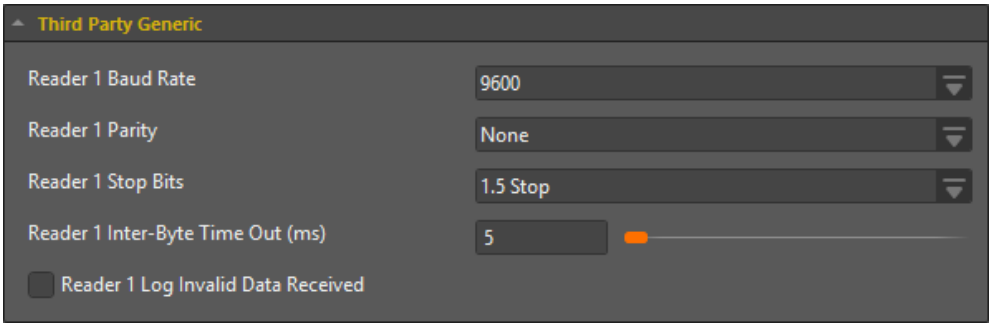
1. Navigate to **Expanders | Reader Expanders.**
2. Select the controller's onboard reader expander.
3. In the **Configuration** section, set the following options:



- **Port Network Type:** Assign the **Third Party Generic** option from the drop down menu to either the **Port 1 Network Type** or **Port 2 Network Type** depending on which port is in use.
- **Ethernet Network Type**: **Disabled.**

4. Select the **Reader 1** or **Reader 2** tab depending on which port is in use.

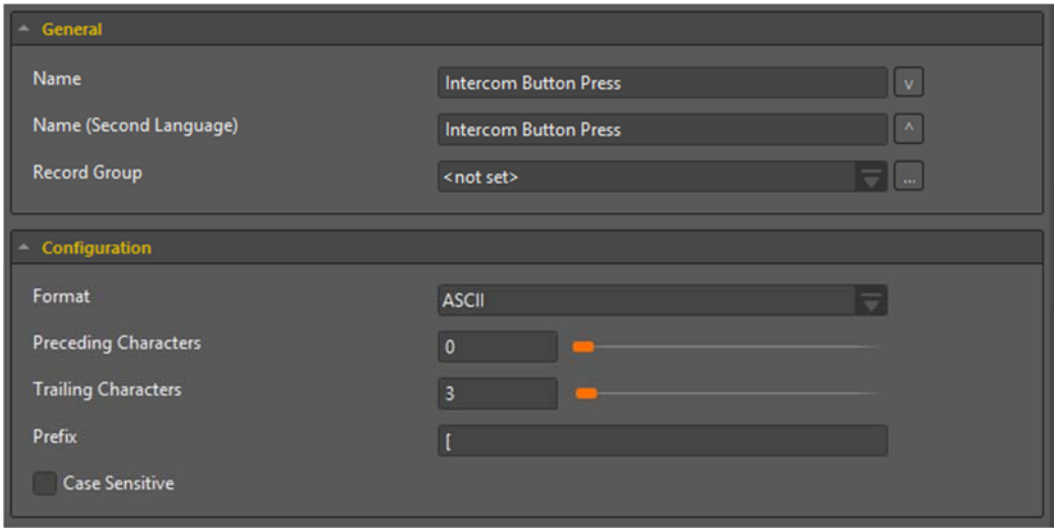
   In this example we have used Reader Port 1 and as a result the **Reader 1** tab is selected.



5. Scroll down to the **Third Party Generic** section and set the following options:
   - **Baud Rate:** The rate at which information is transferred between the third party device and the Protege GX controller.
   - **Parity:** Defines the method of calculating the parity for the block.
   - **Stop Bits:** Defines the number of stop bits used.
   - **Inter-Byte Time Out:** Defines the time in milliseconds allowed between receiving bytes of data.
   - **Log Invalid Data Received:** When enabled, logging begins for instances where invalid data is received.
6. Click **Save.**

Creating the Intercom Credential Type

1. Navigate to **Sites | Credential Types**.
2. Click **Add**.
3. Enter a **Name** for the new credential type.



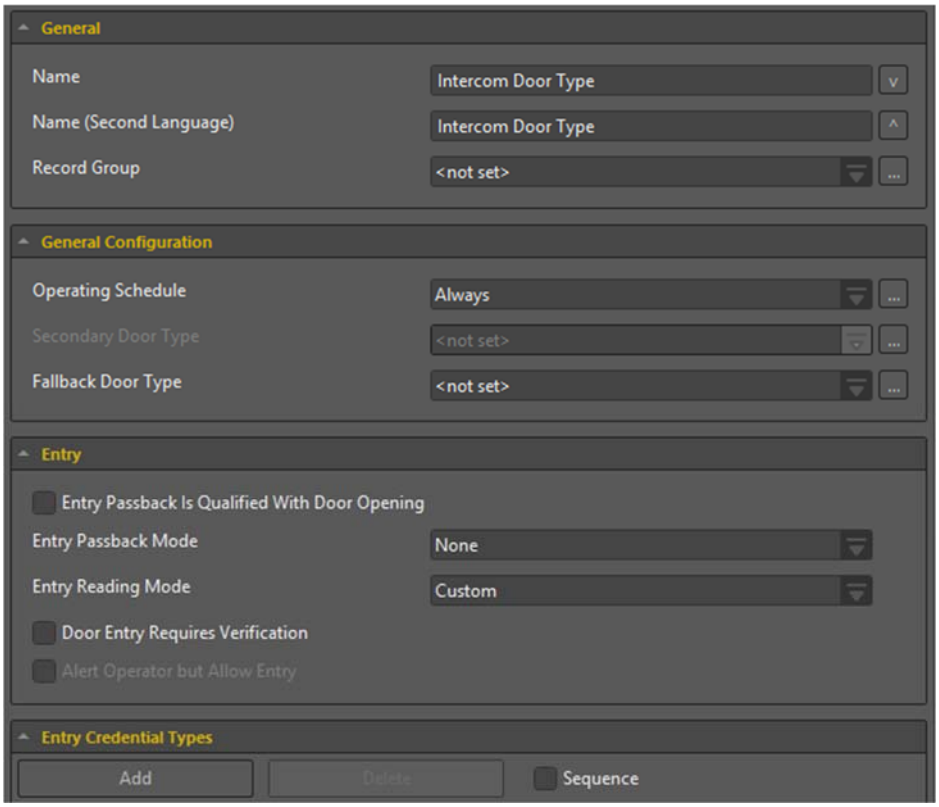
- **Format:** The format of the data that is sent to the Protege GX controller by the third party device.
- **Preceding Characters:** The maximum number of characters to be ignored at the start of the data packet being sent to the controller. This is determined by the third party device/application.
- **Trailing Characters:** The maximum number of characters to be ignored at the end of the data packet being sent to the controller. This is determined by the third party device/application.
- **Prefix:** The characters that are required at the start of the credential data in the packet sent to the controller. This is determined by the third party device/application.

4. Click **Save**.

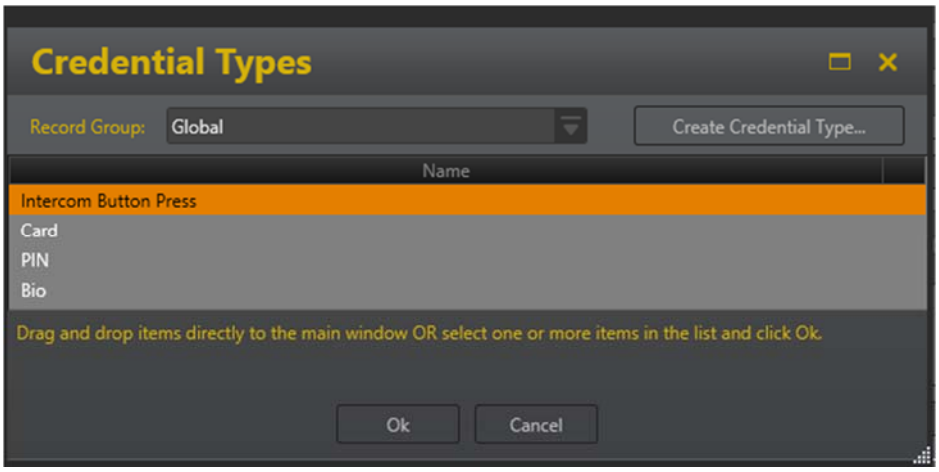
Creating a New Door Type

A custom **Door Type** is required to instruct the door to respond to the defined credential type.

1. Navigate to **Programming | Door Types**.
2. Click **Add**.
3. Enter a **Name** for the new door type and set the **Entry Reading** mode to **Custom**.



- Under the **Entry Credential Types**, click **Add**.
- Select the **Intercom Button Press** credential type created previously (see page 7) and click **Ok**.

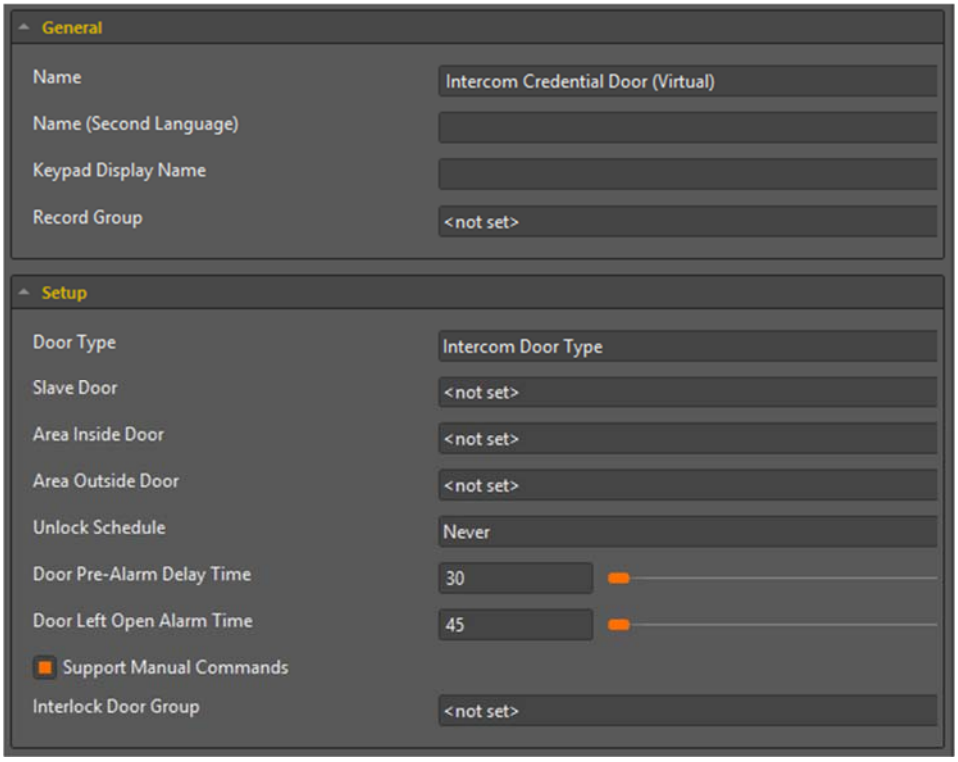


4. Repeat the steps above to assign the **Intercom Button Press** credential type to the **Exit Reading Mode**.
5. Click **Save**.

Creating a Virtual Door

Once the **Door Type** has been configured, it must be assigned to the same door that the smart reader is linked to.

1. Navigate to **Programming | Doors**.
2. Click **Add**.
3. Enter a **Name** for the new door.
4. Set the **Door Type** to the **Intercom Door Type** created previously (see page 8).

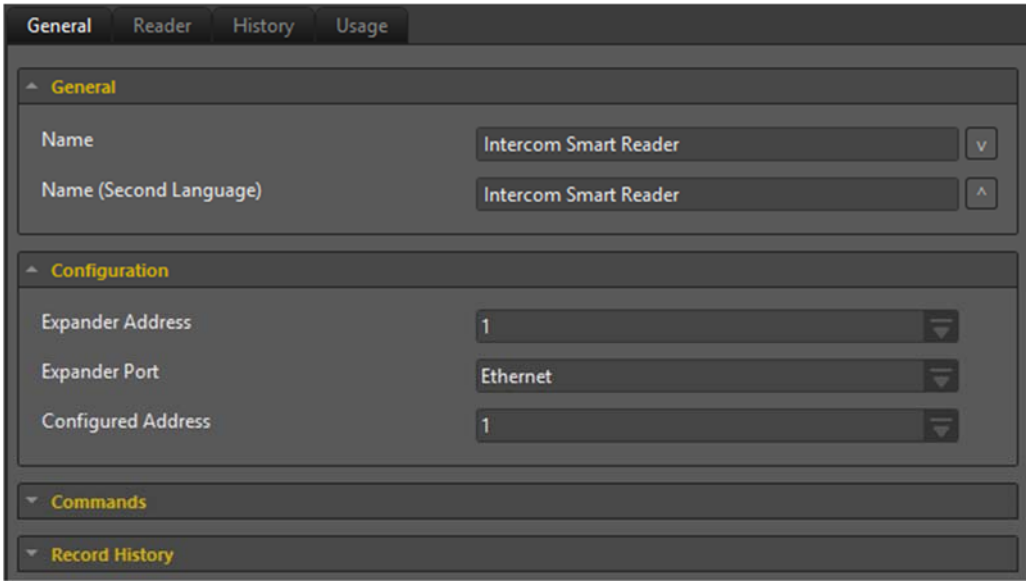


5. Click **Save**.

Creating a Smart Reader

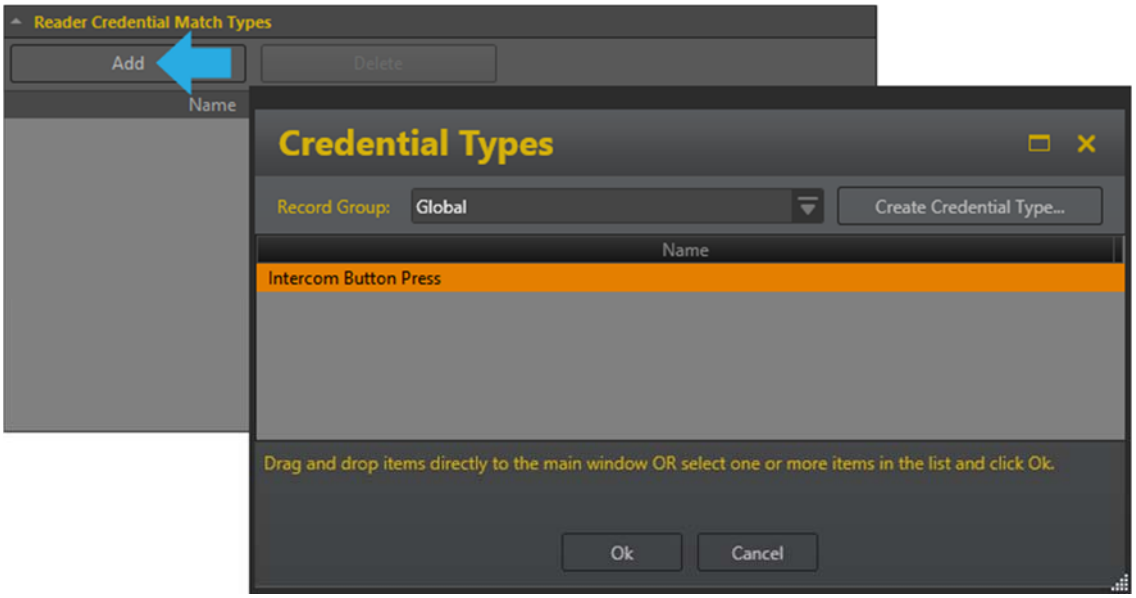
In order to use this feature for access control, you must program a smart reader. The smart reader does not represent a physical device, but it is required to link the credential type functionality to a door which then allows valid credentials to activate their respective access level output.

1. Navigate to **Expanders | Smart Readers**.
2. Click **Add**.
3. Enter a **Name** for the smart reader.

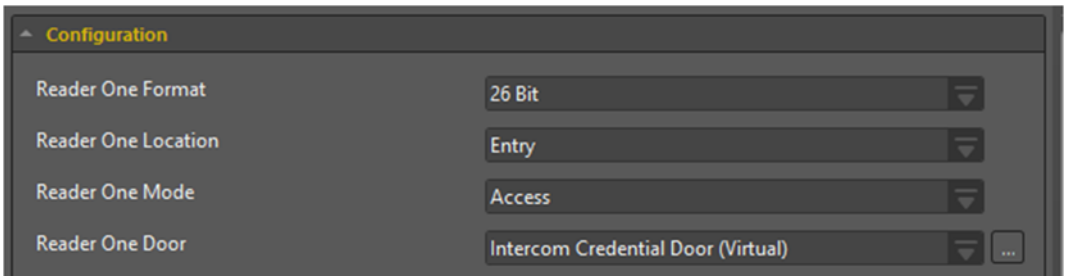


- **Expander Address:** Address of the controller's onboard reader expander.
- **Expander Port:** If the intercom device is connected over Ethernet, assign **Ethernet** to this field, else assign the correct Port (either **Port 1** or **Port 2**) depending on which onboard reader expander reader port the intercom device is connected to.
- **Configured Address:** A placeholder which must be unique.

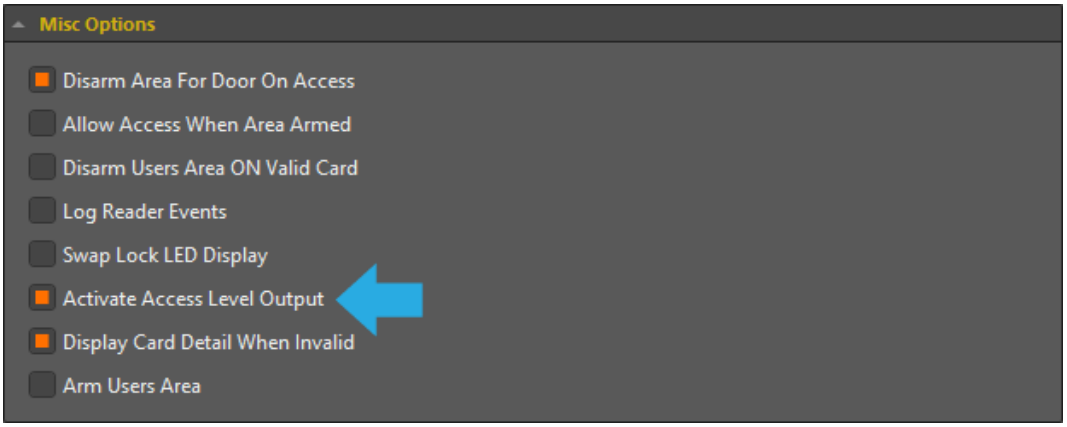
4. Click on the **Reader** tab.
5. Within the **Reader Credential Match Types** section, click **Add**.
6. The **Credential Types** window will appear. Select the **Intercom Button Press** credential type created previously (see page 7), then click **Ok**.



7. In the **Configuration** section, set the **Reader One Door** to the **Intercom Credential Door (Virtual)** created previously (see page 9).



8. In the **Misc Options**, select the **Activate Access Level Output** check box.



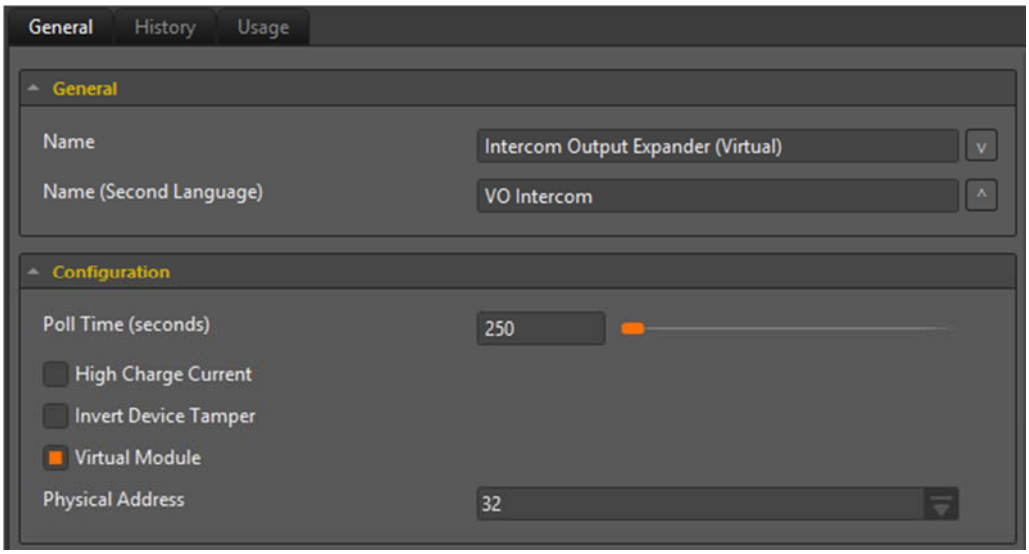
9. Click **Save**.

Creating Virtual Outputs

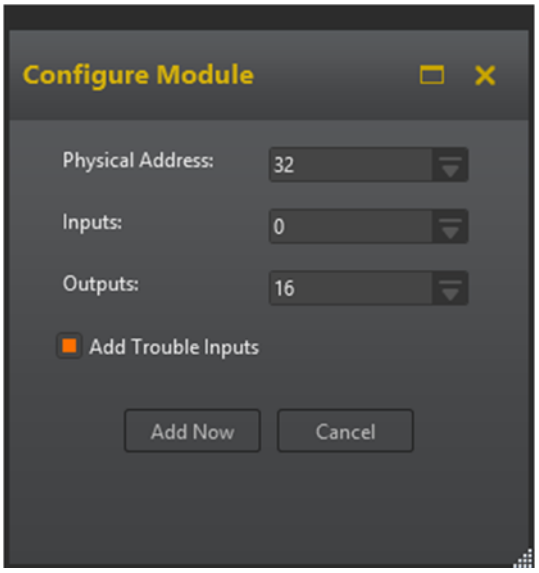
We will now add a virtual module which allows us to create virtual outputs.

Creating a Virtual Module

1. Navigate to **Expanders | Output Expanders**.
2. Click **Add**.
3. Enter a **Name** for the virtual module.



4. Enable the **Virtual Module** check box and click Save. The **Configure Module** window will appear.

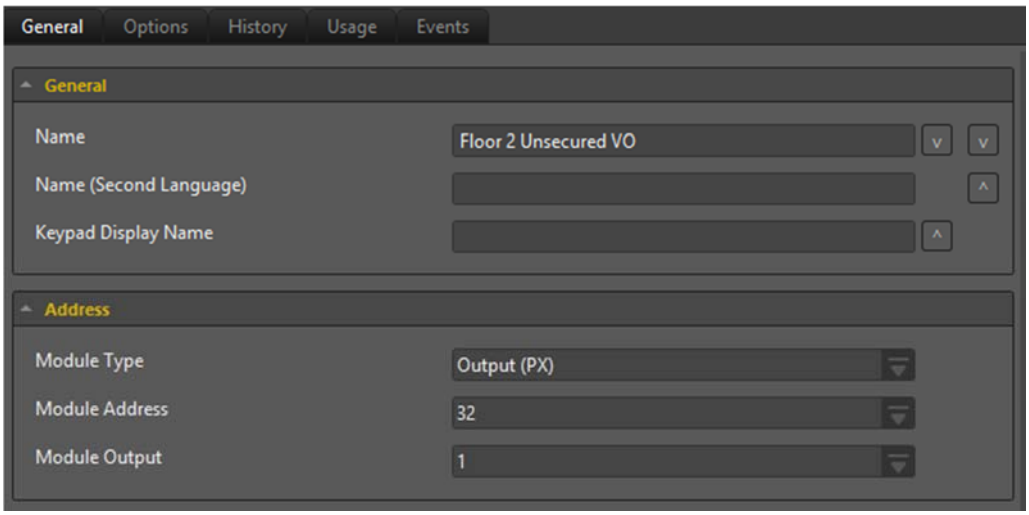


Enter the following details:

- **Physical Address:** Assign a value to this field ensuring that this address has not been assigned to a module already. In this example we have assigned address 32.
- **Inputs:** The number of inputs to be created automatically. As we are only creating this module for the purpose of creating virtual outputs, set this field to zero.
- **Outputs:** Select the number of outputs you wish to create with a maximum of 16. In this example we have created 16 outputs even though we do not require that many.

Configuring the Virtual Outputs

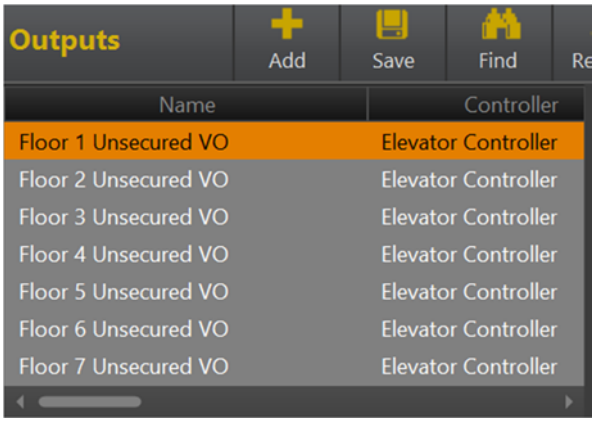
1. Navigate to **Programming | Outputs**.
2. Select one of the newly created outputs and enter a new **Name** for the virtual output. Ensure you name this output in such a way that it can be easily identified as the validation output for the schedule.



- **Module Type:** Set this field to Output (PX) as per the virtual output expander module created previously.
- **Module Address:** Set this address to the address of the virtual output expander module created previously.

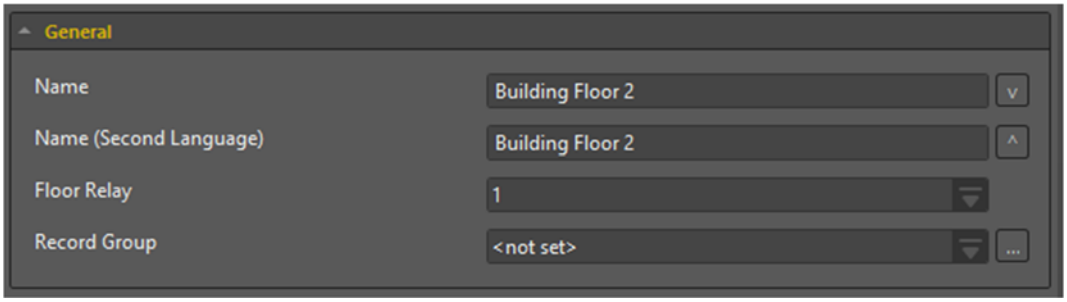
3. Click **Save**.

Repeat this process for each floor that requires a virtual output. In the scenario for this application note (see page 5), the following virtual outputs have been added:



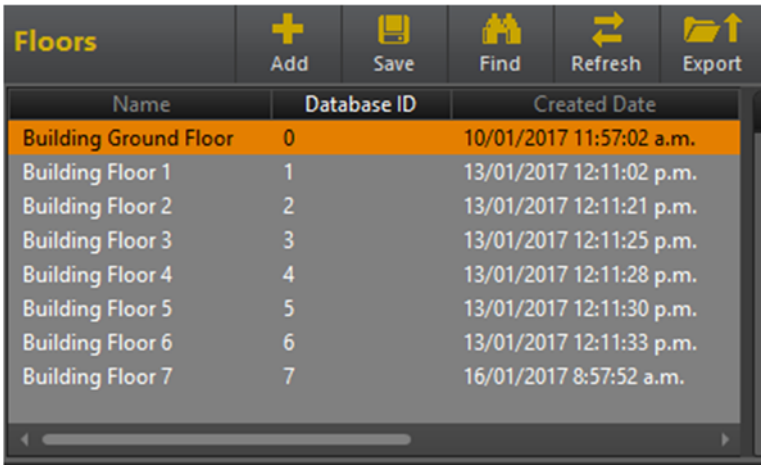
Creating Floors

1. Navigate to **Programming | Floors**.
2. Click **Add**.
3. Enter a **Name** for the floor.



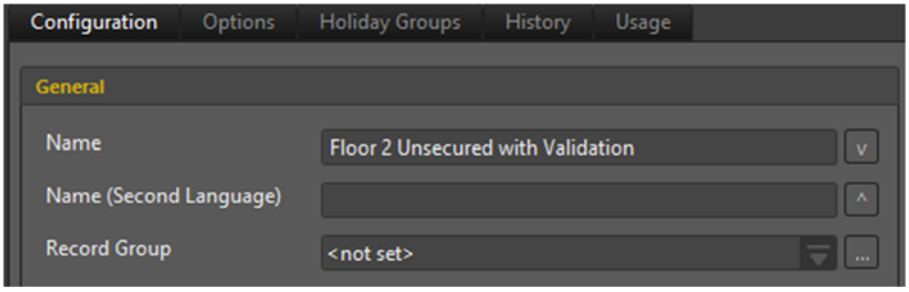
4. Click **Save**.

Repeat this process for each floor within the building. In the scenario for this application note (see page 5), the following floors have been added:

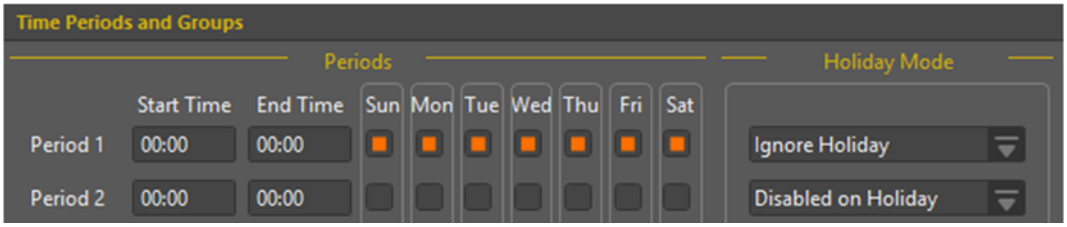


Creating Floor Schedules

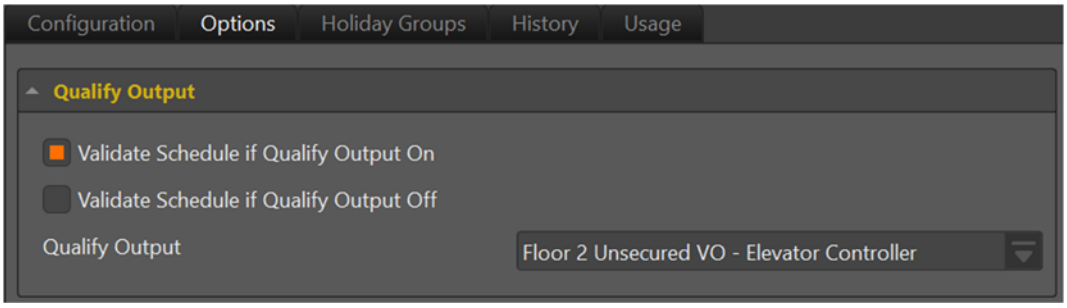
1. Navigate to **Sites | Schedules**.
2. Click **Add**.
3. In the **Name** field, enter **Floor 2 Unsecured with Validation**.



4. Select Sunday through to Saturday in **Period 1** and set the **Holiday Mode** to **Ignore Holiday**.

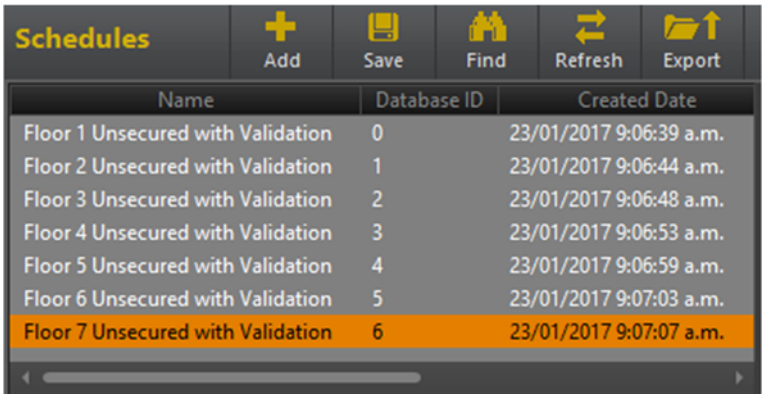


5. Click on the **Options** tab and enable the **Validate Schedule if Qualify Output On** option.
6. Set the **Qualify Output** to **Floor 2 Unsecured VO**.



We have created a schedule that is valid 24/7 regardless of holidays, however it requires that the **Floor 2 Unsecured VO** is ON before the schedule becomes valid.

Repeat this process to create a schedule corresponding to each floor within the building and remember to assign the relevant output in the **Qualify Output** field. In the scenario for this application note (see page 5), the following schedules have been added:



Note that a schedule does not need to be created for the ground floor.

Assigning Floor Schedules

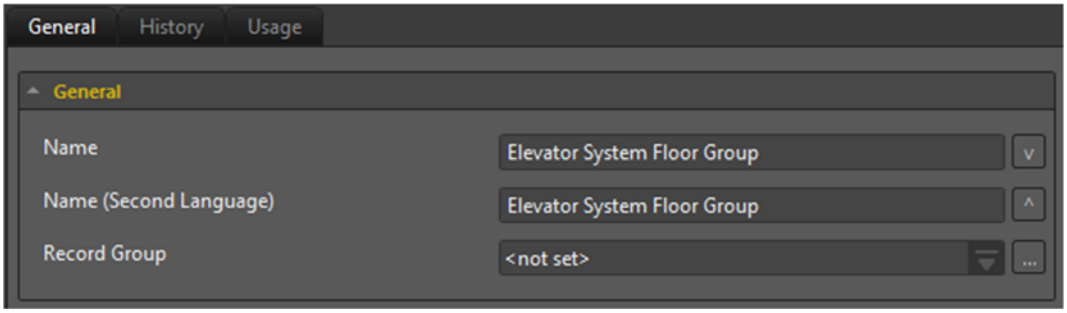
Assigning schedules to floors can be accomplished through the use of either **Floor Groups** or **Elevator Cars** depending on the type of elevator system Protege GX is integrating with.

Creating a Floor Group

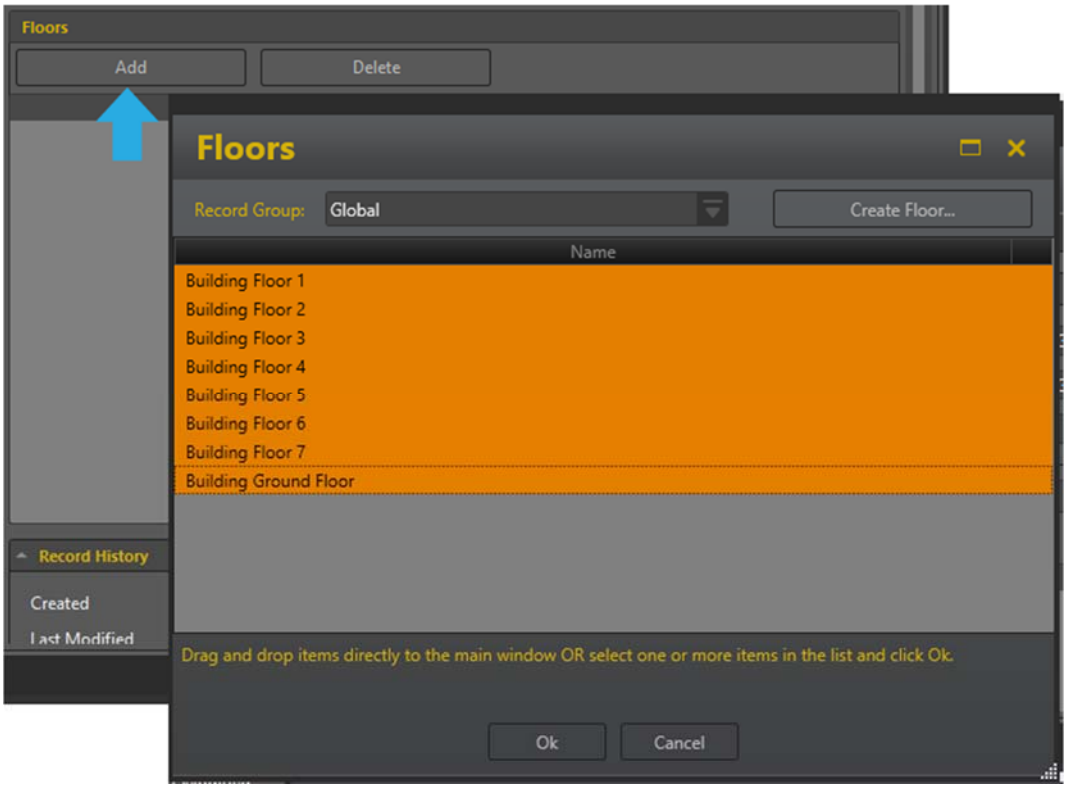
Schedules are used in conjunction with **Floor Groups** to define when certain floors are accessible. When integrating with a third party HLI elevator system, we use a floor group to define the default operation of each floor within the building.

If integrating with a third party HLI elevator system:

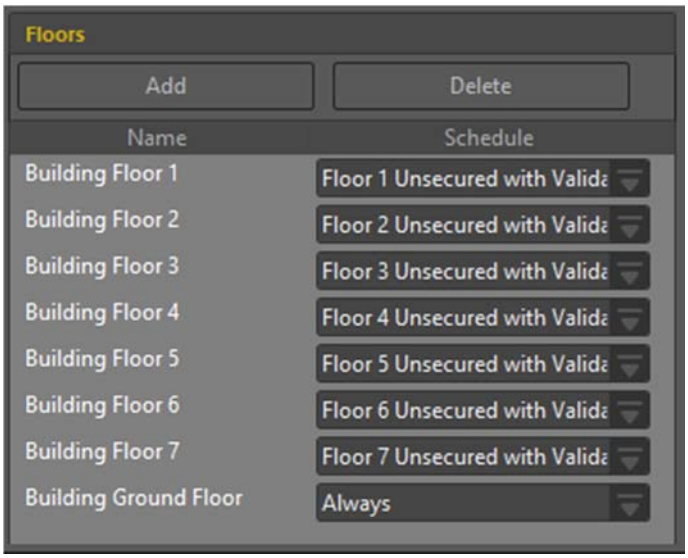
1. Navigate to **Groups | Floors Groups**.
2. Click **Add**.
3. Enter a **Name** for the floor group.



4. In the **Floors** section, click **Add**.
5. Select the all the floors accessible by the elevator system, then click **OK**.



6. Assign the **Schedule** relevant to the floor from those created previously (see page 15). The **Building Ground Floor** will be assigned the **Always** schedule as this floor is always freely accessible.



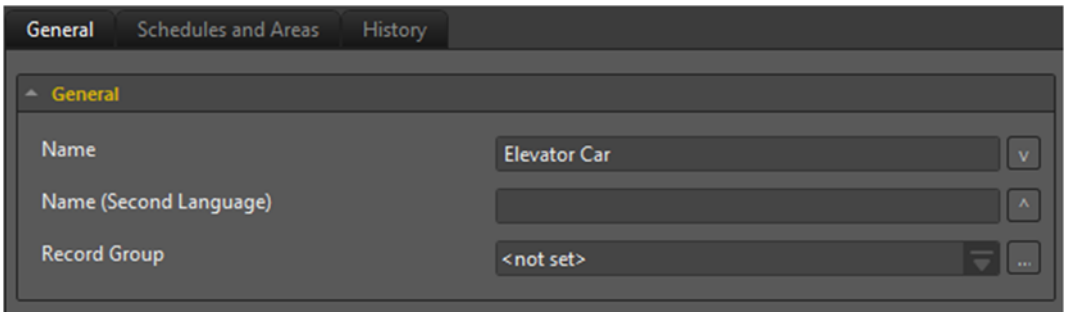
7. Click **Save**.

Creating an Elevator Car

Schedules are used in conjunction with **Elevator Cars** to define when certain floors are accessible. When integrating with a standard elevator system, we use an elevator car to define the default operation of each floor within the building.

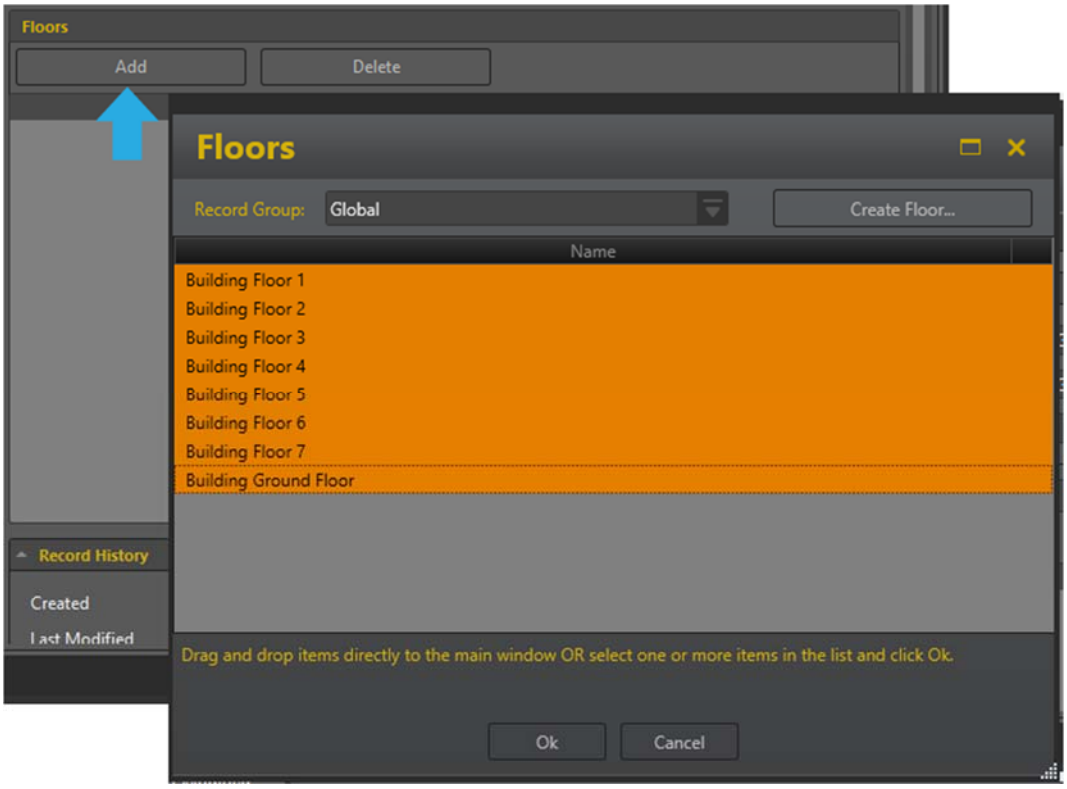
If integrating with a standard elevator system:

1. Navigate to **Programming** | **Elevator Cars**.
2. Click **Add**.
3. Enter a **Name** for the elevator car.

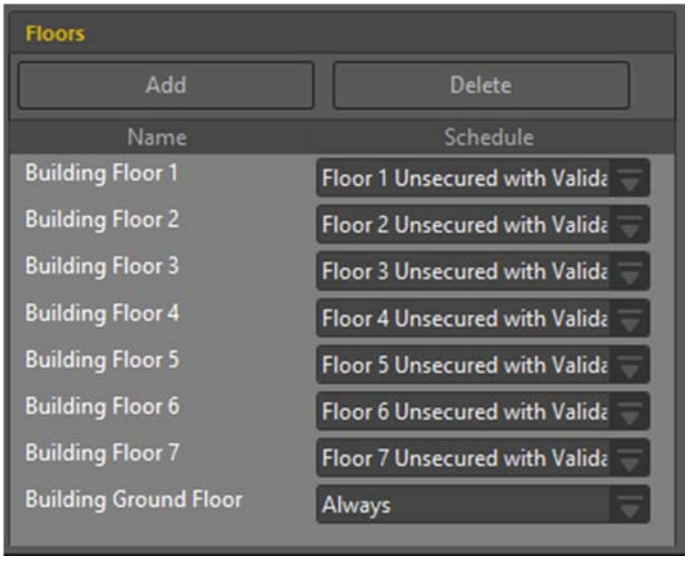


4. In the **Floors** section, click **Add**.

5. Select the all the floors accessible by the elevator system, then click **OK**.



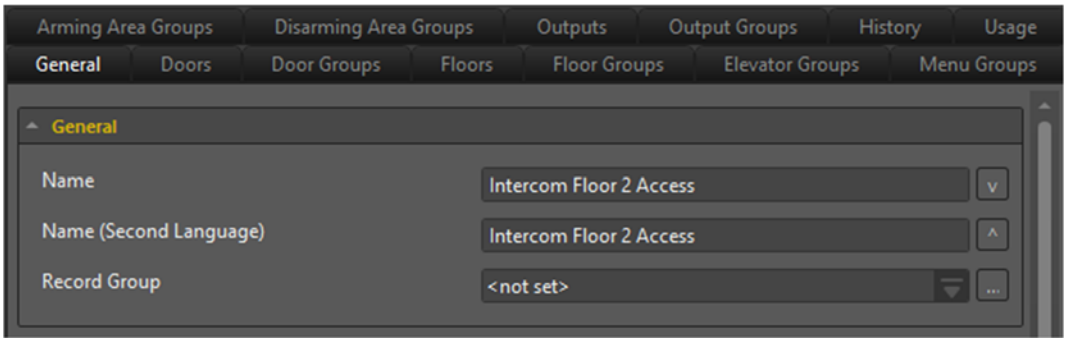
6. Assign the **Schedule** relevant to the floor from those created previously (see page 15). The **Building Ground Floor** will be assigned the **Always** schedule as this floor always freely accessible.



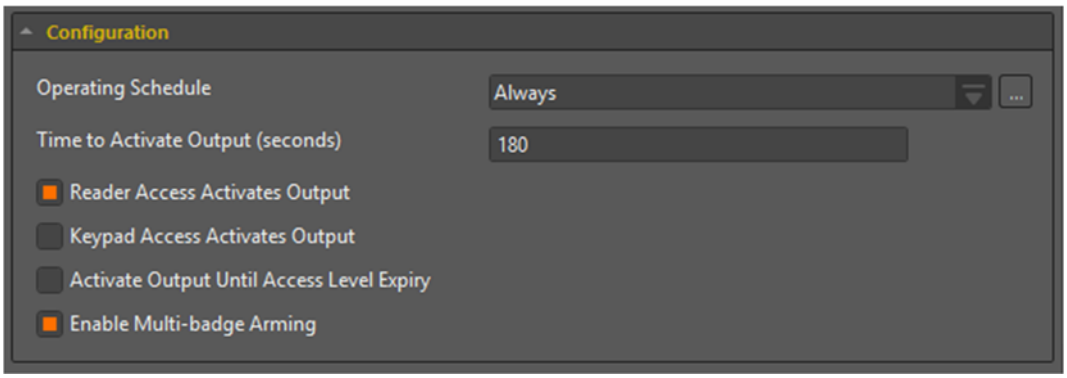
7. Click **Save**.

Creating Access Levels

1. Navigate to **Users | Access Levels**.
2. Click **Add**.
3. Enter a **Name** for the new access level. This field should correspond to a particular floor to be granted access.

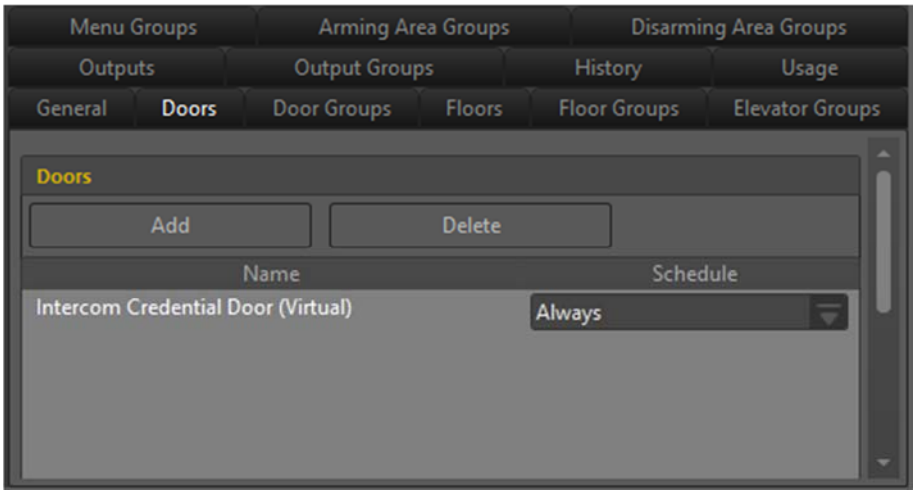


4. In the **Configuration** section of the **General** tab, set the following options:

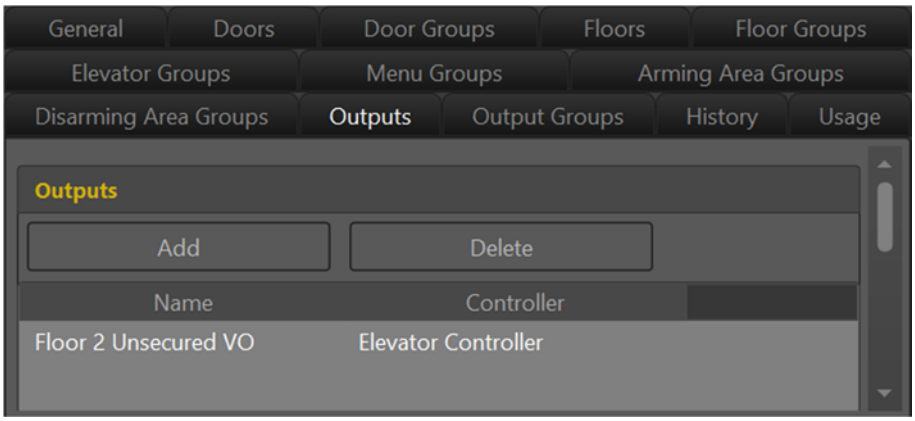


- **Time to Activate Output (seconds)**: Defines how long the floor is to be unsecured for when the intercom button is pressed. This field should be set to a value sufficient for a visitor to make their way to the elevator to select the desired floor after the intercom button has been pressed.
- Select the **Reader Access Activates Output** check box.

5. In the **Doors** tab, ensure that the virtual door is assigned.

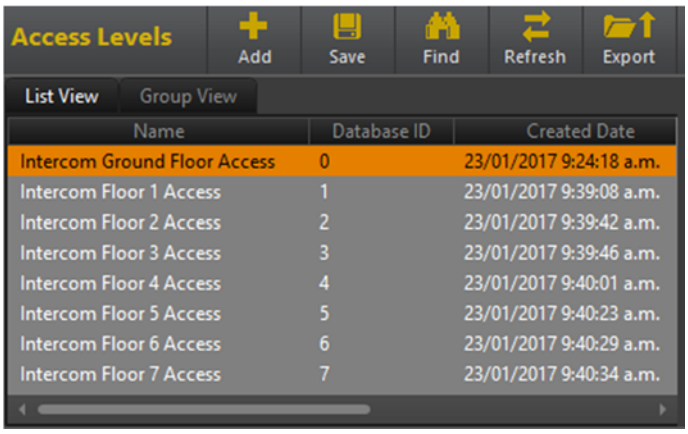


6. In the **Outputs** tab, ensure that the output validating the schedule of the floor to be accessed is added. In this example, we have assigned the **Floor 2 Unsecured VO** output.



7. Click **Save**.

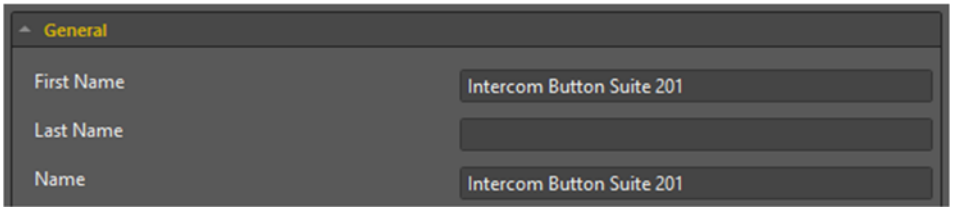
Repeat this process for each access level that corresponds to a floor within the building. In the scenario for this application note (see page 5), the following access levels have been added:



Creating User Credentials

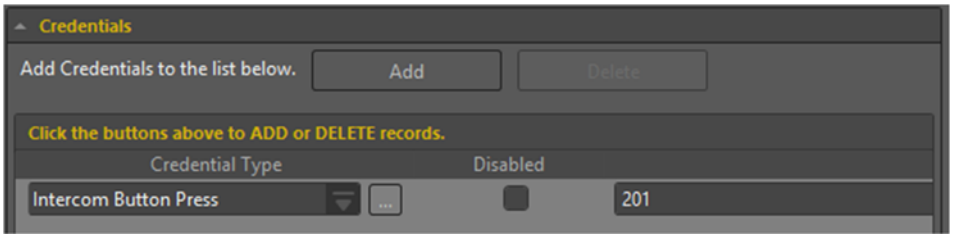
When programming Intercom Integration, **Users** are used to represent a particular access granted button press on the intercom device. In order to use the new credential type, it must be added to their record in Protege GX.

1. Navigate to **Users | Users**.
2. Click **Add**.
3. Enter a **Name** for the new user (access granted button press).



In this example, the new user corresponds to a button press from apartment 1 on floor 2.

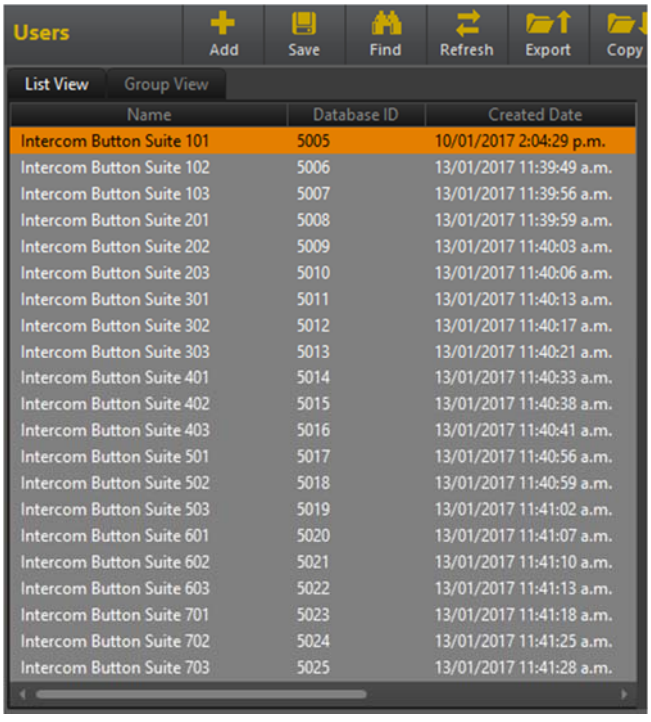
4. In the **Credentials** section, the **Intercom Button Press** credential type created previously (see page 7) will have been automatically added to the user.
5. In the **Credential** field, enter the required credential that will identify the button press from the apartment. This field will be checked against the number passed from the intercom.



In this example, the **Intercom Button Press 201** user has been assigned the credential 201. When this field in Protege GX is matched against button press 201 on the intercom, access will be granted for access to second floor through the elevator system.

6. Click **Save**.

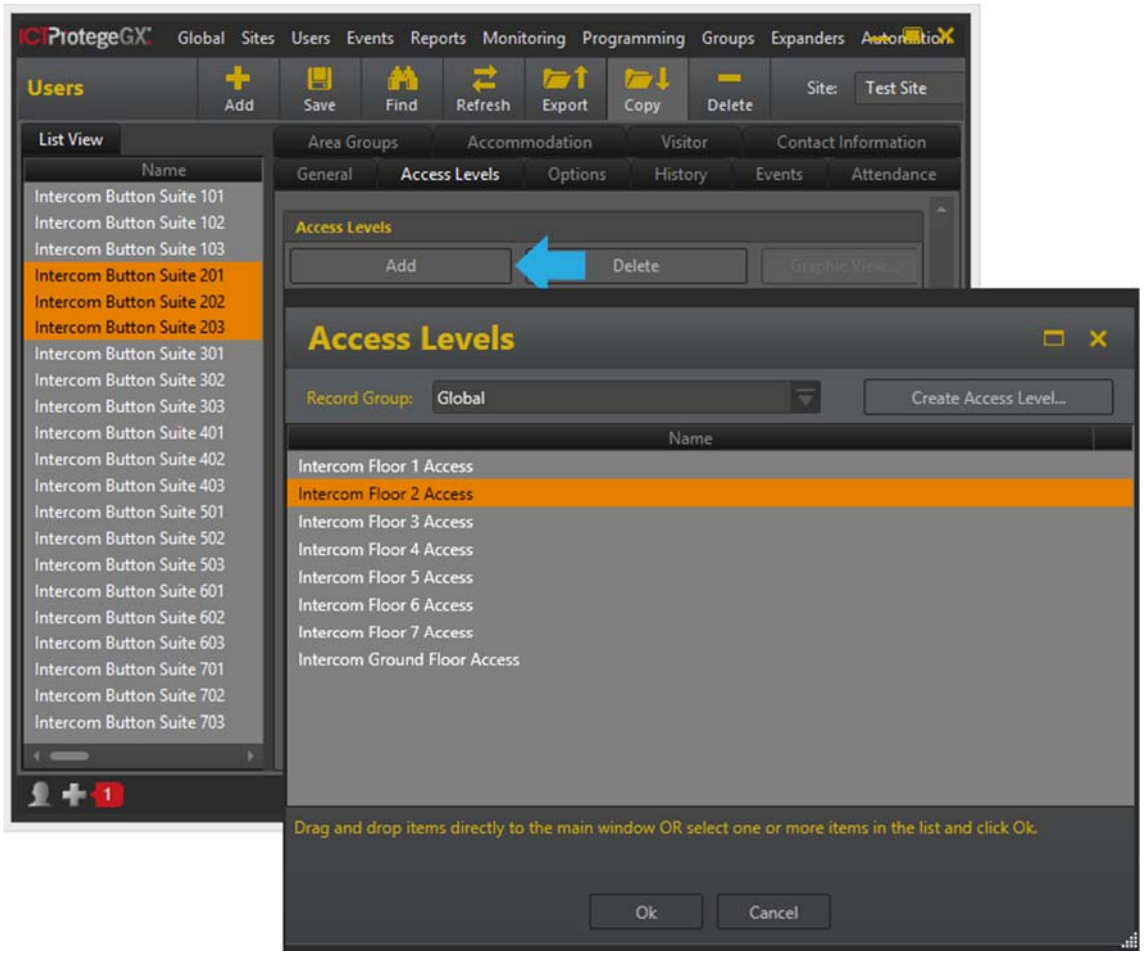
Repeat this process for each unique credential that corresponds to an access granted button press passed from the intercom. In the scenario for this application note (see page 5), the following users have been added:



Assigning Access Levels to Users

An **Access Level** must be added to each user record in order for the intercom to determine access to the corresponding floor upon a button press on the intercom device.

1. Navigate to **Users | Users**.
2. Multi-select the required user records and click on the **Access Levels** tab.
3. Click **Add**.



4. Select the required access level and click **OK**.
5. Click **Save**.

In this example, **Intercom Floor 2 Access** has been assigned to the **Intercom Button Suite 201/202/203** records. This means that an intercom button press from suite 201, 202 or 203 will grant access for floor 2.

Repeat steps 2 to 5 for each set of user records.

Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (http://www.ict.co) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

4 John Glenn Ave
Rosedale
North Shore City 0632
Auckland
New Zealand

Phone: +64-9-476-7124

Toll Free Numbers:

0800 ICT 111 (0800 428 111) - New Zealand

1800 ICT 111 (1800 428 111) - Australia

1855 ICT 9111 (1855 428 9111) - USA/Canada

Email: sales@incontrol.co.nz or support@incontrol.co.nz

Web: www.ict.co

APAC
Integrated Control Technology Limited
4 John Glenn Avenue, Rosedale, Auckland 0632
PO Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: sales@ict.co Toll Free: (0800) 428 111 Phone: 64 (9) 476 7124

AMERICAS
Integrated Control Technology (USA) LLC
5265 S Rio Grande Street, Suite 201, Littleton, CO 80120
Email: ussales@ict.co Toll Free: (855) 428 9111 Phone: 720 442 0767

EMEA
Integrated Control Technology (Europe) Limited
St Mary's Court, The Broadway, Amersham, HP7 0UT, UK
Email: emeasales@ict.co Phone: 44 0 1494 590494

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