AN-174

Protege GX Otis Compass HLI Integration

Application Note

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2026. All rights reserved.

Last Published: 12-Jun-26 8:49 AM

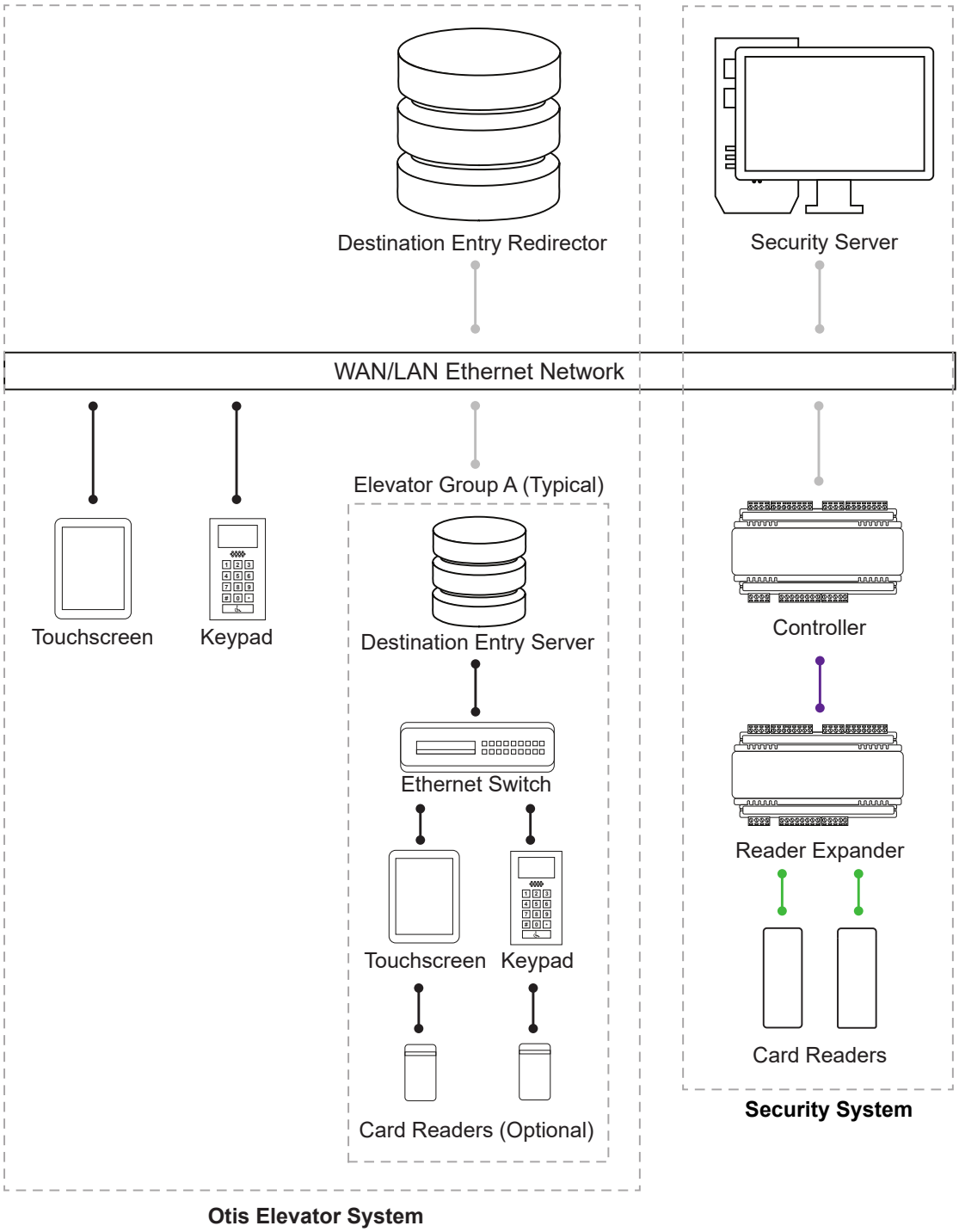
Contents

Introduction 4
Prerequisites 5
Networking Requirements 5
Network Switch Configuration 6
Separating the Otis Compass and Protege GX Networks 6
Unsupported Features 6
Floor Mapping 7
Floor Relay Numbering 7
Skipped Floor Numbers 7
Lowest Basement Floor 8
Floors with Rear Doors 9
Programming Steps 11
Configuring the Controller 11
Configuring up to 128 Floors 11
Adding Floors 12
Adding Floor Groups 12
Configuring the Otis Compass DECs 13
Programming Antipassback 13
Programming the Reader Expander 14
Configuring Access Levels 15
Otis Compass Special User Functions 15
Configuring Reader Formats 16
Appendix: Commands 18

Introduction

High level integration between Protege GX and Otis Compass elevator systems provides the full advantage of a complete destination dispatch solution combined with access control and intruder detection.

Users and access credentials are configured within Protege GX and transferred to the Otis Compass system. When a user presents their access card at an Otis Compass terminal, the Otis Compass system verifies their credentials using the information supplied by Protege GX. Once access has been verified, the Otis Compass system automatically calls an elevator to transport the user to the selected floor.



The Protege GX Otis Compass HLI elevator integration supports up to 128 floors.

This integration is a licensed feature.

Prerequisites

The Protege GX Otis Compass HLI integration requires the following software and hardware. All items must be installed and operational to configure this integration.

Software	Version	Notes
Protege GX	4.0.128 or higher	
Protege GX Controller	2.08.582 or higher	
Otis Compass Elevator System	This integration has been tested and validated against both ICD2 and ICD3 protocols.	These are the **ONLY** tested and supported versions for this integration.

It is the responsibility of the installation professional to verify the version of the proposed third-party system and supported components with the version listed in this document. ICT will not accept responsibility for the failure to verify integrated system versions and requirements.

Protege GX Licensing Requirements

License	Order Code	Notes
Protege GX Otis Elevator High Level Interface (HLI) License	PRT-GX-ELV-HLI-OT	1 license per controller used for this integration
Protege GX Door License	PRT-GX-DOR-1	1 license per destination entry computer (DEC) used in the integration
	PRT-GX-DOR-10	
	PRT-GX-DOR-50	

Networking Requirements

In order to interface with the Otis Compass system, the controller running the integration must have the following network settings.

- **IP address**: 192.168.50.250
- **Subnet mask**: 255.255.255.0
- **Gateway**: 192.168.50.254

These can be set in the **Adaptor - Onboard Ethernet** tab of the controller's web interface. Alternatively you can use the controller's USB ethernet interface (see next page).

Otis Compass elevator systems utilize a number of different ethernet network subnets for their various interface connections. To isolate the network communications between the Protege GX controller and the Protege GX system from the controller's Otis Compass network communications, avoid the following subnets for Protege GX communications. This will prevent unnecessary networking issues.

- 192.168.1.xxx - 192.168.8.xxx inclusive
- 192.168.10.xxx
- 192.168.20.xxx
- 192.168.60.xxx

It is recommended that Protege GX communications begin well above these subnets to avoid future conflicts, e.g. 192.168.100.xxx.

Network Switch Configuration

Protege GX controllers support IGMPv2 only. Some Otis Layer 3 switches use IGMPv3 as the default setting, which prevents the Protege GX controller from connecting to the Otis server.

To prevent this issue, ensure that Otis configures **Port 1 and Port 21** on the Layer 3 switch to use **IGMPv2**.

Separating the Otis Compass and Protege GX Networks

It is possible to physically separate the Otis Compass and Protege GX networks to prevent any communication conflicts. In this configuration, the controller communicates with the Otis Compass system using the standard RJ45 ethernet adaptor, and uses the USB ethernet adaptor to communicate with the Protege GX server and other components.

This requires a Protege GX controller with an **onboard USB port** running firmware version **2.08.1245 or higher**.

1. Connect the controller to the Protege GX server using the built-in RJ45 ethernet connection.
2. In Protege GX, navigate to **Sites | Controllers | Configuration**.
3. Expand the **Elevator HLI** section and set the **Elevator HLI type** to OTIS.
4. Return to the **General** tab and expand the **Commands** section.
5. Enter the following command:
   `OTISUseUSBForMainComms = true`
6. Click **Save** and wait for the programming to be downloaded.
7. Connect a USB ethernet adaptor to the controller's USB port. Switch the ethernet cable to the USB port.
8. Power cycle the controller. You should now be able to communicate with the controller using the USB ethernet connection.
9. Browse to the controller's web interface and log in.
10. Open the **Settings** page. You should see the following IP address settings:
    - **Adaptor - Onboard Ethernet**: 192.168.50.250
    - **Adaptor - USB Ethernet**: The original IP address, e.g. 192.168.1.2
11. Connect the controller's built-in RJ45 ethernet port to the Otis Compass network. Now all Otis Compass communications should be physically separated from Protege GX traffic.

The controller will retain this configuration even if the Otis HLI service is disabled or removed. To swap the Protege GX communication back to the standard ethernet connection you must default the controller.

Unsupported Features

Protege GX does not support the following optional features of the Otis Compass 360 system:

- Encrypted communications between Protege GX and Compass
- Unicast heartbeats

Floor Mapping

Before beginning to program the elevator integration, it is important to correctly map the layout of the elevator system. All elevator-accessible floors need to be identified and mapped in sequential order from bottom to top. You need to identify which (if any) floors have rear doors, and which (if any) floors are considered 'below ground' in the elevator system programming. This is essential for Protege GX to correctly map floors for event reporting and 'home floor' functionality.

Floor Relay Numbering

Each floor accessed by the elevator system needs to be programmed in Protege GX, with a unique **Floor relay** number assigned. The floor relay number tells the controller where the physical floor is located, creating a map in Protege GX of accessible floors.

Floor relay numbers must be **unique**, programmed in **numerical order** (starting at 1), and beginning at the **lowest accessible floor**, including any basement floors.

The lowest accessible floor must be assigned a floor relay of **1**, as shown in the example below.

Physical Floor	Floor Relay Number
Basement 2	1
Basement 1	2
Ground Floor	3
Level 1	4

Skipped Floor Numbers

Numbers are commonly skipped in floor labels due to superstitions surrounding specific numbers, and technicians may also skip these in the elevator controller programming. Where this occurs a placeholder floor record must be created in Protege GX to maintain the required sequential floor relay numbering, as in the example below.

Physical Floor	Elevator System Floor Relay	Floor Relay Number
Ground	0	1
Level 1	1	2
...	...	...
Level 12	12	13
N/A	Not programmed	14 (Placeholder)
Level 14	14	15

In this example a placeholder floor record is added with relay number 14 to maintain the sequential numbering and represent the skipped programming in the elevator system. Had the sequence been maintained in the elevator system (i.e. Level 14 programmed with elevator system floor relay 13) no placeholder floor would be required.

Lowest Basement Floor

The Protege GX floor programming must match the elevator system setup, or the integration will not function correctly. To do this you need to identify which floor is programmed as the first aboveground floor in the elevator system configuration, then count the number of elevator-accessible floors below this one. This number becomes the controller's **Lowest basement floor** setting in the controller configuration.

Depending on the building layout and elevator system configuration, the first aboveground floor could be the ground floor, the first floor, a lobby, or even a carpark. The labels and numbering of the floors is not important, only the configuration of the relay numbering in the elevator system.

The floor programmed with relay '0' in the elevator system is the first aboveground floor. Any floor programmed with a negative relay number is treated as a basement floor.

Examples are provided to illustrate the Protege GX programming required for different elevator system scenarios.

Lowest Basement Floor Examples

1. In the first scenario the building has no basement floors, with standard relay programming beginning from '0'. As there are no belowground floors the **Lowest basement floor** setting is 0.

Physical Floor	Elevator System Floor Relay	Floor Relay Number
Ground Floor	0	1
Level 1	1	2
Level 2	2	3
Level 3	3	4

2. In the next scenario the building has two basement floors, with relay programming sequentially numbered. With two belowground floors the **Lowest basement floor** setting is 2.

Physical Floor	Elevator System Floor Relay	Floor Relay Number
Basement 2	-2	1
Basement 1	-1	2
Ground Floor	0	3
Level 1	1	4

3. In the following scenario the building has two basement floors, however the ground floor is programmed as relay '1' instead of '0'. A placeholder floor record is required in Protege GX to maintain the relay sequence, and the **Lowest basement floor** setting is 2.

Physical Floor	Elevator System Floor Relay	Floor Relay Number
Lower Carpark	-2	1
Upper Carpark	-1	2
	Not programmed	3 (Placeholder)
Ground Floor	1	4

Floors with Rear Doors

For some floors it may be possible to exit the elevator at the rear as well as the front. Each 'rear floor' must also be programmed in Protege GX.

The rules for programming rear floors are as follows:

- The **Floor relay** number of the rear floor must be equal to that of the corresponding front floor.
- Each rear floor must be programmed with the command `Rear`.
- The controller must be programmed with the command `HLI_128_FLOORS = true`.

The `Rear` and `HLI_128_FLOORS = true` commands are supported in controller firmware version 2.08.1158 or higher. For earlier firmware versions, rear doors must be programmed with relay numbers from 65-128.

The table below demonstrates front and rear floor relays in a building with 50 aboveground floors and two basement floors.

Physical Floor	Front Floor Relay	Rear Floor Relay
Basement 2	1	1
Basement 1	2	2
Ground Floor (no rear access)	3	-
Level 1 (no rear access)	4	-
Level 2	5	5
...	...	...
Level 48	51	51
Level 49	52	52

It is not necessary to program rear floor records for any floors that do not have rear access, but you may want to do this to keep the programming tidy.

Rear Floor Relays 65-128

For sites with up to 64 floors the rear floor relays can be programmed from 65-128 without using the `Rear` command. To calculate the rear floor relay, add 64 to the front floor relay.

This is a legacy programming option which provides backward compatibility for existing installations and controller firmware versions prior to 2.08.1158, but is not recommended for new installations. It supports a maximum of 64 floors and is not available if the controller has been configured to support 128 floors.

The table below demonstrates front and rear floor relays in a building with 50 aboveground floors and two basement floors where the **Rear** command is not used and rear floor relays start at 65.

Physical Floor	Front Floor Relay	Rear Floor Relay
Basement 2	1	65
Basement 1	2	66
Ground Floor (no rear access)	3	-
Level 1 (no rear access)	4	-
Level 2	5	69
...	...	...
Level 48	51	115
Level 49	52	116

Programming Steps

The following instructions outline the steps required to configure the integration within Protege GX. These include:

- Enabling controller HLI and configuring connection with the Otis system
- Adding the floors
- Creating floor groups
- Configuring door records as Otis Compass destination entry computers (DECs)
- Programming the reader expander for access control
- Assigning floor groups and default floors to access levels
- Enabling Otis Compass special user functions

Configuring the Controller

1. Navigate to **Sites | Controllers** and select the controller to be used for the integration.
2. Open the **Configuration** tab and scroll down to the **Elevator HLI** section.
3. Set the **Elevator HLI type** to OTIS, then configure the required options:
   - **Network adaptor**: Only Cable is supported for this integration.
   - **Lowest basement floor**: The lowest physical underground floor accessible by an elevator. For example, if there are five underground floors the value should be 5. If there are no underground floors, set to 0.

     What is considered an underground floor is determined by the elevator system configuration.
4. Click **Save**.

Configuring up to 128 Floors

By default the controller supports up to 64 floors for this integration. However, with some additional configuration the integration can support up to a maximum of 128 floors.

This feature requires controller firmware version 2.08.1158 or higher.

1. Navigate to **Sites | Controllers** and select the controller to be used for the integration.
2. Expand the **Commands** field and enter the following commands:
   - `HLI_MAX_FLOORS = X`

     Where **X** is the total number of floors in the building. This can be a value from 1-128.
   - `HLI_128_FLOORS = true`

     This command is required to enable the controller to support using the `Rear` command for rear floors.
3. Click **Save**.

Adding Floors

Each floor accessed by the elevator system needs to be configured in Protege GX with a floor relay number assigned. This tells the controller where the physical floor is located, creating a map of accessible floors.

1. Navigate to **Programming | Floors**.
2. Add a floor record for each elevator-accessible physical floor, assigning the **Floor relay** for each floor as explained in the Floor Mapping section (see page 7).
3. If the floor is a 'rear floor' add the `Rear` command in the **Commands** field.

   The `Rear` command is supported in controller firmware version 2.08.1158 and above. The controller must also be programmed with the `HLI_128_FLOORS = true` command.

4. Click **Save**.

Adding Floor Groups

There are two categories of floor groups that are used in this integration.

Floor Groups assigned to DECs

These floor groups contain the floors that each Otis Compass DEC is able to access. For example, some DECs may be able to access all floors, while others might only have a subset of floors accessible. Once a floor is added to a floor group, a schedule can be applied to the floor to define when it is freely accessible without credentials.

1. To create a floor group for the floors that are accessible to a DEC, navigate to the **Groups | Floor groups** menu, click **Add** and **Name** the floor group, (e.g. All Otis Floors).
2. In the **Floors** window, click **Add** to select the floors to be included in the floor group. Drag and drop items into the main window or select one or more floors and click **Ok**.
3. In the **Schedule** column, apply a schedule to each floor:
   - If the Always option is selected, the floor will be freely accessible without credentials at all times.
   - If a specific schedule is selected, the floor will be freely accessible when the schedule is valid, and will require valid credentials to access when the schedule is invalid.
4. Click **Save**.

Floor Groups assigned to Access Levels

These floor groups define the floors that any given user is permitted to access using their credentials. Note that it is not strictly necessary to create floor groups for this purpose, as floors may be assigned directly to the access level.

1. Navigate to the **Groups | Floor groups** menu and create a new floor group.
2. In the **Floors** window, click **Add** to select the floors to be included in the floor group. Drag and drop items into the main window or select one or more floors and click **Ok**.
3. In the **Schedule** column, you may apply a schedule to each floor:
   - If the Always option is selected, the user will be able to access this floor at all times when the floor group is valid within the access level.
   - If a specific schedule is selected, the user will be able to access this floor only when this schedule is valid, provided that the floor group is valid within the access level.
4. Click **Save**.

Configuring the Otis Compass DECs

The destination entry computer (DEC) is the Otis computer controlling the display that directs a user to the appropriate elevator car. DECs are represented by door records within the Protege GX system. Each DEC on each floor requires a record to be created in Protege GX.

1. Navigate to the **Programming | Doors** menu and **Add** the door records that will represent DECs.
2. For each door record, enter a **Name** that describes the type of device and its location, e.g. 'OTIS DEC LB5'.
3. Under the **Elevator HLI** section, enable the **Door used for elevator HLI** option and select the **Controller**. When enabled, only options relevant to the specific elevator configuration are displayed.
4. In the **Operator panel type** field, select DOP (Destination Operating Panel).

   For Otis Compass integrations DOP must be selected, as only landing-based DECs are supported. The COP option is not supported.

5. Select the relevant controller, then set the following:
   - **DOP ID**: This information is provided by the Otis Compass elevator system and specifies the unique ID of the Otis Compass DEC. This needs to match the fourth octet of the DEC's IP address.
   - **Floor group**: This floor group defines all of the floors that the DEC is able to access. When the schedules assigned to the floors in this group are valid the floors will be unlocked for free access.
   - **Group number**: This information is provided by the Otis Compass elevator system and must match the third octet of the DEC's IP address.
   - **DEC operation mode**: This defines the DEC operation mode (this must match the mode supplied by the Otis Compass elevator system). The following modes are supported:
     - **(1) Default floor**: The user presents their credentials to the card reader or enters a PIN at a DEC device. If the user's credentials are valid the security system sends the user's default floor to the DEC. If floor access is denied the DEC provides textual and/or audible feedback to the user informing them that the call request has been denied.

       The default floor is set as the **Elevator destination floor** in **Users | Access levels | General**.

     - **(3) User entry of destination floor**: Without the need for credentials, the user selects their destination floor. If the destination floor is free access the DEC forwards the call request to the DES. If the floor selected is not free access the user is prompted to present their credentials.
     - **(4) Default floor or user entry of destination floor**: The user presents their credentials and, if valid, their default floor is sent to the DEC. Within a defined timeframe the user is able to override the default floor selection and choose another destination floor.

       The default floor is set as the **Elevator destination floor** in **Users | Access levels | General**.

6. Click **Save**.
7. Repeat the above steps for each DEC.
8. It is convenient to use door groups when you assign DECs to access levels. Navigate to **Groups | Door groups** and add one or more door groups containing DECs.

Programming Antipassback

Optionally, you can use antipassback with operating panels in HLI elevator integrations. For example, you could enable hard antipassback on a turnstile to prevent users from entering the turnstile then passing their card back to someone on the other side.

The operation is the same as standard door antipassback: the system tracks which area each user is in based on their access activity, and reports an antipassback violation if the user is not recorded in the correct area required to enter or exit the door.

Requirements for Elevator HLI Antipassback

- This feature is available in controller firmware version **2.08.1297 or higher**.
- Antipassback should only be used on turnstiles, security gates or similar operating panels with **entry and exit readers** to record movement into and out of the area. When the user enters the turnstile, the system will update their user area and call an elevator based on their home floor or selection. When the user exits the turnstile, it will update their user area without calling an elevator.
- User area tracking is based on the **inside and outside area** programmed in the door record, **not** the floor that the user has selected. For example, the outside area might be the ground floor reception. When a user accesses the turnstile, it grants entry to the elevator lobby and calls an elevator.

  Antipassback should not be enabled for operating panels which are only used to select a floor (such as car operating panels), as the user could be going to any floor instead of entering a specific physical area such as a lobby.
- User credentials must be processed by the Protege GX controller, not the elevator system.
- Optionally, you can use the **Entry/Exit passback is qualified with door opening** setting. This prevents the user's antipassback status from being updated unless they actually pass through the gate after badging. To use this feature, you must have a **Door position input** connected to the gate to detect when someone passes through.
- The **Reader 1/2 elevator** in the reader expander programming must be <not set>.

Programming Antipassback for a Turnstile

1. Navigate to **Programming | Door types** and add a new door type.
2. Set the **Entry passback mode** to control entry through the turnstile and **Exit passback mode** to control exit. The options are:
   - **Hard passback**: Access will be denied if a user attempts to enter/exit the turnstile from the wrong area.
   - **Soft passback**: Access will be granted even if a user attempts to enter/exit the turnstile from the wrong area, but a 'Soft Passback Violation' event will be logged.
3. Optionally, enable **Entry/Exit passback is qualified with door opening**. When this is enabled, antipassback status is only updated when the user passes through the gate.
4. Program any other settings required for this door type such as the **Entry/Exit reading mode**, then click **Save**.
5. Navigate to **Programming | Doors** and select a door record which represents a turnstile, security gate or other operating panel.
6. Set the **Door type** to the one programmed above.
7. Set the **Area inside door** and **Area outside door** for the turnstile.
8. If you used **Entry/Exit passback is qualified with door opening** in the door type: In the **Inputs** tab, select the **Door position input**.
9. Click **Save**.

Programming the Reader Expander

This integration also provides the opportunity to use ICT readers for elevator access control. If you want to implement this option, the Protege GX door records that represent each DEC need to be assigned to the reader expander port that the associated card reader is physically connected to. This creates the link in Protege GX between the reader and the 'door' (DEC) that the reader will control access to.

1. Navigate to **Expanders | Reader expanders**.
2. Select the reader expander that one of the readers wired to a DEC is connected to.
3. Select the **Reader 1/2** tab for the reader port that the reader is connected to.
4. Set the **Reader 1/2 door** to the door record which represents the relevant DEC.
5. Set the **Reader 1/2 mode** to Elevator so the reader is treated as part of the Otis Compass elevator system.

6. Click **Save**. Wait for the programming to be downloaded to the controller, then right click on the reader expander record and click **Update module**.
7. Repeat the above steps to assign the remaining DEC door records to their associated readers.

Note: As setting **Reader 1/2 mode** to Elevator disables the **Reader 1/2 door** option, assign the door before setting the reader mode.

Configuring Access Levels

Access levels determine which floors and DECs users are allowed to access.

1. Navigate to **Users | Access levels** and create or edit access levels.
2. In the **Doors** or **Door groups** tabs, assign the DECs that the user will have access to.
3. You can assign either individual floors in the **Floors** tab, or floor groups in the **Floor groups** tab. In both cases, you can select a **Schedule** which defines when the user has access to those floors.

Important: If schedules are defined in both the access level programming and the floor group programming, these schedules must both be valid for the user to have access to a floor.

When the access levels are complete, you can assign them to users to grant access to the elevator system.

Assigning Home Floors to Access Levels

You can also set the home floor for an access level, which is used when the **DEC operation mode** is set to either (1) Default floor or (4) Default floor or user entry of destination floor.

For example, if a company has offices on a particular floor of the building, you can set it as the default floor for all staff members in that company. When a user badges at the DEC, an elevator will automatically be dispatched to transport them to the floor they work on.

You can set the **Elevator destination floor** in **Users | Access levels | General**, under the **Elevator HLI** section.

Otis Compass Special User Functions

The following Otis Compass special user functions are available in **Users | Users | Options | OTIS elevator HLI options**:

- **User is a VIP**: VIP users have non-stop priority service to their destination floor in dedicated elevator cars. This must be configured in the Otis system.
- **Enable Vertigo**: When vertigo is enabled the Otis system will select specific elevator cars for this user based on a particular characteristic (as configured in Otis). For example, passengers with vertigo will not be assigned to glass elevator cars.
- **Enable split group operation**: Enables contract special 1, as configured in the Otis system.
- **Enable Vertigo 2**: Following from **Enable Vertigo** above, this option further defines which type of elevator the user will be assigned, as configured in the Otis system. For example, elevators may be slowed for this passenger.
- **Enable cart service**: This feature minimizes cases of an elevator car arriving without the physical capacity required for a passenger and cart (e.g. in hotel/hospital service elevators).
- **Enable CIM override**: When CIM operation is enabled in the Otis system, the system prevents specified groups of users from sharing elevator cars or traveling to the same floors. Enable this option for users who need to access all elevator cars and floors, such as building managers.

Configuring Reader Formats

By default, this integration uses the HID 34 Bit format for reading credentials. If your site uses different credentials you can set one or more alternative reader formats. This may also be needed when Otis card readers are used on site, as the Otis system commonly sends credentials to Protege GX in ASCII format.

From controller firmware version 2.08.1363 you can program up to four reader formats. Prior to this version only one reader format is supported.

Enter the following command in the controller programming:

```
OTISReaderFormat = #,#,#,#
```

Where each **#** is a number corresponding to a reader format.

The following table shows the available reader formats and their corresponding values:

Value	Reader Format
0	26 Bit
1	ICT 37 Bit
2	Keyscan 36
3	NCS 25/29 Bit
4	Northern 34 Bit
5	Kantech 32 Bit
6	STID ISO T2
7	Sentrax 9000 T2
8	Propel Track 2
9	40 Bit
10	Mirage 33 Bit
11	Motorola 27 Bit
12	ABA T2
13	Multi 26/32 Bit
14	First 4 T2
15	Kantech 39 Bit
16	Setec 37 Bit
17	Motorola ABA T2
18	Hotel T2
19	32 Bit
20	32 Bit (Rev)
21	WSE 34 Bit
22	HID 32 Bit
23	First 6 Track 2
24	30 Bit

Value	Reader Format
25	37 Bit
26	36 Bit
27	Rusco 40 Bits
28	ABA BIN T2
29	ABA Card T2
30	NCS 29 Bit
31	HID 34 Bit
32	HID 26/34 Bit
33	Auto - Wiegand
34	Auto - Magnetic
35	36 Bit (IEI)
36	34 Bit (Pass)
37	34 Bit (Pass NP)
38	Any Bit (RAW)
39	26 Bit (NP)
40	34 Bit (NP)
41	First 5 Track 2
42	Apollo 44 Bit
43	CANSEC 37 Bit
44	Tecom 27 Bit
45	Custom Format This can be programmed in **Sites | Controllers | Custom reader format**.
46	HID Corp 1000
100	ASCII This is used for situations where the Otis system sends credentials to the Protege GX controller in ASCII format. Protege GX will interpret this as normal card data - there is no need to program a separate credential type.

Appendix: Commands

This appendix provides a list of configuration commands that are relevant to this integration. Commands allow you to configure optional settings that are not available in the user interface.

You can enter commands in **Sites | Controllers | Configuration | Commands**.

Command	Description
`OTISDebug = true`	Enables debugging for the Otis Integration.
`OTISNotResync = true`	Disables the periodic resync of the DEC operation mode packet every 15 mins.
`OTISPriority = true`	With this command enabled, the integration will prioritize processing card reads over schedule changes. This can resolve issues with card reads not being processed quickly enough.
`OTISDECTxRetryCount = x`	Defines the number of retries when sending packets to the DECs. Default value is 3.
`OTISDECReplyTimer = x`	Defines the number of seconds to wait for a reply from a DEC. Default value is 2.
`OTISNoOTISCommsWD = true`	When enabled, the controller will restart automatically if no communication can be established with Otis after 5 mins or there are more than 10 unacknowledged packets.
`OTISNoCTRLCommsWD = true`	Used when the controller is using cross controller operations. When enabled, The controller will restart automatically if no cross controllers are online after 5 minutes.
`OTISNoDECOnlineTimeout = x`	Defines a timeout (seconds) to wait for a "DEC Online" message after establishing heartbeat connections on startup. After the timeout, the controller re-initializes the connection to Otis. Default value is 60.
`OTISUseUSBForMainComms = true`	When enabled, the controller will use the USB ethernet adapter for Protege GX comms and the standard ethernet adapter for Otis communication so the networks can be isolated. See Separating the Otis Compass and Protege GX Networks for more information.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2026. All rights reserved.

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.