Schneider Electric

Security Expert Schindler HLI Integration

Application Note

AN-196

January 2018

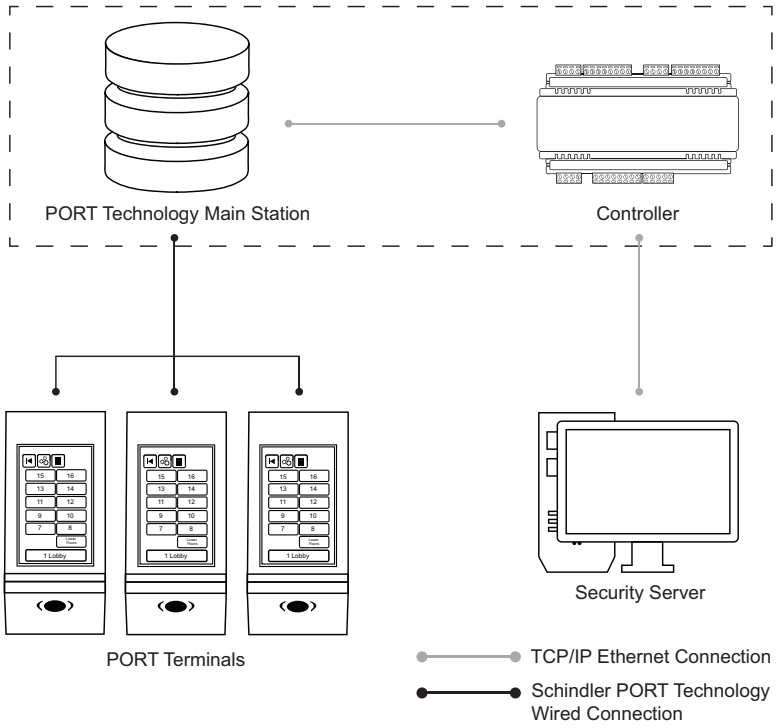
Legal Information

Table of Contents

Schindler HLI Elevator Integration

High level integration between Security Expert and the Schindler PORT Technology Elevator Security Management System enables you to take full advantage of a complete destination dispatch solution while providing access control and intruder detection.

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



Note: This integration is a licensed feature

Prerequisites

This integration requires:

- An operational Security Expert system with software version 4.1.180 or higher
- An operational Schindler PORT Elevator system
  (This integration has been tested and validated against version 1.2.359.1)
- A Security Expert Controller using SP-C firmware version 2.08 Build 703 or higher
- A Security Expert Schindler Elevator High Level Interface License applied to the server

You will also need a list of user profile templates from the Schindler system.

Integration Overview

The following instructions outline the steps required to configure the integration within Security Expert. These include:

- Configuring the controller to enable the HLI settings and programming the various properties to connect to the Schindler server
- Adding the required Floors and Floor Groups
- Configuring outputs to trigger SOMs (Special Operating Modes) from within Security Expert

Floor Groups and Access Levels

Floor access is controlled by the user profile templates in the Schindler system. To link these templates to users in Security Expert, you need to create a floor group for each template, then use an access level to assign the floor group to the users. This means that each user can only be associated with one access level (as they can only be associated with one user profile template).

In most cases, your access levels will correspond to the Schindler user profile templates, however you may have more than one access level that use the same floor group but that has different permissions to other items. For example, if you have a Schindler template named CEDA, you would have a floor group named CEDA, but you could have several access levels that each use this floor group, but that have different access to the doors and area groups within the Security Expert system.

Programming Steps

Configuring the Controller

1. Select the controller connected to the Schindler server then click the Configuration tab
2. Set the **Elevator HLI Type** to **Schindler** and enter the required HLI options:
   - **PORT System Primary IP:** The primary IP address of the Schindler server
   - **PORT System Secondary IP:** The secondary IP address of the Schindler server
   - **Online Database Port:** The TCP port of the Schindler Online Database Interface
   - **Call Interface Port:** The TCP port of the Schindler Call Interface
   - **Life Reporting Interface Port:** The TCP port of the Schindler Life Reporting Interface
   - **Lowest Basement Floor:** The lowest physical underground floor the elevators can access
   - **Default Floor Group:** The floor group containing all accessible floors and the schedules used to control when each floor can be freely accessed

Note that this group **must be created** (see page 7) and defined here for the integration to work correctly.

   - **Enable Call Interface:** Enables the Schindler Call Interface
   - **Enable Life Reporting Interface:** Enables the Schindler Life Reporting Interface
   - **Enable Elevator HLI Debug:** Enables debug messages to be logged for troubleshooting
3. Click **Add** to define the site code format(s) that are used and enter the:
   - **Site Code** - also referred to as a facility number - of the access cards being used

- **Format** used by the Schindler system
- **Subformat** (If required), set to 0 by default

Whenever user card details are sent to Schindler, the system identifies all cards with the defined site code(s). It then takes the site code and card number and converts this to a single string based on the Schindler format defined.

You can define up to 32 site code formats.

Program the Floors and Floor Groups

All floors that can be accessed from an elevator must be programmed within Security Expert and a unique relay assigned to each floor.

To control access to the floors, you must also create a floor group for each user profile template in the Schindler system. The name of the floor group **must** match the name of the user profile template.

You also need to create a group that contains **all** of the floors in the system and define the schedules that are applied to each floor. This group is required as part of the process for configuring scheduled floor operation.

Adding Floors

1. Add a floor for each floor in the system, assigning relays as follows:

   Floor relays must be **unique**, programmed in **numerical order** (starting at 1), and start at the **lowest accessible floor**, including any basement floors. This means the floors created within Security Expert should look something like this:

Actual Floor	Assigned Floor Relay
Basement 2	1
Basement 1	2
Ground Floor	3
Level 1	4
Level 2	5
…	…
Basement 2 (Rear)	65
Basement 1 (Rear)	66
…	…

2. Set the required **Elevator HLI Options**:

   - **Schindler Schedule Valid Time Pattern**: Defines the message that is sent to the Schindler Call Interface when the schedule assigned to the floor becomes valid
   - **Schindler Schedule Invalid Time Pattern**: Defines the message that is sent to the Schindler Call Interface when the schedule assigned to the floor becomes invalid
   - **Schindler Primary Terminal ID**: Defines the ID of the Schindler terminal that the schedule valid/invalid message is sent to when the controller is communicating via the primary IP address
   - **Schindler Secondary Terminal ID**: Defines the ID of the Schindler terminal that the schedule valid/invalid message is sent to when the controller is communicating via the secondary IP address

Adding Floor Groups

1. Create a new floor group for each user profile template, ensuring the name of the group matches the name of the template, and add at least one floor to the group

   The floors that can be accessed are determined by the user profile template. You can assign any floor to the group but must add at least one floor to ensure the Security Expert system recognizes the group.

2. Create an additional floor group containing **all** floors used by the Schindler system
3. Set the **Schedule** for each floor to define when that floor can be freely accessed:
   - If the floor should be freely accessible, set the schedule to **Always.**
   - If the floor should only be accessed during specified hours, create and assign a schedule to define these hours.
4. Set this as the **Default Floor Group** for the controller being used.

Configuring Schindler SOMs

SOMs (Special Operating Modes) are used within the Schindler system to perform specific functions such as enabling VIP service when a certain passenger badges their card, or stopping all cars at the nearest floor and opening the doors when a fire alarm is triggered.

Configuring a SOM as an output enables you to trigger it from Security Expert. When the output is activated, the Controller sends a message to the Schindler system which then takes the relevant action – such as dispatching an express elevator, locking down all elevators, releasing trapped passengers, etc.

When adding an output to Security Expert, you need to define the address of the module the output is attached to. As these are virtual outputs used to trigger functions, there is no physical hardware required so you can associate them with Security Expert using a virtual module.

Create a Virtual Module

1. Add an output expander ensuring the **Virtual Module** option is enabled
2. Set the **Physical Address** to a value between 1 and 32 (making sure it doesn't conflict with the address of an existing output expander) then click **Save**
3. Select the number of outputs to be added (up to a maximum of 16) then click **Add Now**

This automatically creates and addresses the first 16 virtual outputs ready to configure. If you need additional outputs, they can be added manually.

You can assign up to 255 outputs to one virtual output expander. If there are more than 255 SOMs required, simply add another virtual module.

Configure the Virtual Outputs (SOMs)

1. Configure an output for each SOM ensuring the **Keypad Display Name** matches the name of the SOM in the Schindler system
2. Enable the **Output Used For Elevator HLI** option then set the required options:
   - **SOM Activation Mode**: Sends a message to the Schindler system when the output changes state. Choose from *On*, *Off* and *On Change*. If using a single output to activate and deactivate a SOM, select the On Change SOM activation mode.
   - **Append Output State to SOM Message:** When selected, the state of the output is added to the end of the SOM message. Enable this option if the SOM activation mode is set to *On Change*.

- **SOM Primary Terminal ID:** Defines the ID of the terminal that the schedule on/off message is sent to when the controller is communicating via the primary IP address.
- **SOM Secondary Terminal ID:** Defines the ID of the terminal that the schedule on/off message is sent to when the controller is communicating via the secondary IP address.

Configuring Users and Access Levels

Access levels are required to link the user profile template/floor group to a user. Because each user can only be associated with one user profile template, you can only associate them with one access level.

Your access levels may simply correspond to the user profile template/floor group or you may create multiple access levels that use the same floor group but that have different permissions to other items (such as doors and area groups) within the Security Expert system.

Restarting the HLI

When the HLI service is first started, **all** user details are sent to the Schindler system. After this, changes are only pushed out when a user's name, card details, start and end dates, or access level are modified within Security Expert.

In the event that the Schindler server fails, the HLI service must be restarted. This resynchronizes the systems by importing all user details into the Schindler Online Database again.

1. Select the controller and click the **Configuration** tab
2. Click on the **Restart HLI** button:

Schneider Electric

www.schneider-electric.com

January 2018