



---

## Gallagher Command Centre

### Schindler Call by Profile Feature 8.50

(Supports Command Centre 8.50 or later Command Centre release)

C12814

Release Note

---

---

## **Disclaimer**

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2023. All rights reserved.

## **Copyright Notice**

The software contains proprietary information of Gallagher Group Limited; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Gallagher Group Limited and the client and remains the exclusive property of Gallagher Group Limited. If you find any problems in the documentation, please report them to us in writing. Gallagher Group Limited does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Gallagher Group Limited.

---

## Contents

---

1	Introduction .....	5
2	Installation .....	7
3	Configuration .....	8
4	Live Reporting Interface configuration.....	13
5	Call Manager Interface configuration .....	17
6	Secure/Free floor configuration.....	23
7	Events and Alarms.....	31
8	Upgrading .....	33
9	Uninstallation.....	34
10	Limitations .....	34
11	Consideration.....	34
12	Troubleshooting .....	34
13	Known Issues .....	35



---

# 1 Introduction

---

This release note is for the 'Schindler Call by Profile' feature of Gallagher Command Centre.

**Schindler readers:** If your site is using Schindler readers, then refer to the chapter "*SchindlerID*" in the Gallagher Configuration Client Help.

## 1.1 Purpose

The 'Schindler Call by Profile' feature of Command Centre provides the ability to send a Profile name to the Schindler system after a Cardholder presents their credential at a terminal. Using the Profile name, Schindler will either grant or deny access to the Cardholder.

Command Centre does not send any Cardholder details to the Schindler system. Schindler makes the access decision based on the Profile name only. Although Cardholder details are not sent to Schindler, Command Centre is still able to build an audit trail of Schindler access events.

### Profiles

The Schindler system uses profiles, among other things, to manage access rights. These profiles should be configured with the appropriate access rights in the Schindler system. Once the Schindler integrators have configured the profiles, then they must provide a list of all the profiles to Gallagher integrators who will assign the profiles to the appropriate Cardholders. In Command Centre, the profiles are assigned to Cardholders via a Personal Data Field (PDF).

Each profile name assigned to a Cardholder must match the profile name in the Schindler system. Otherwise, the Cardholder will be denied access.

**Note:** You can only assign one profile per Cardholder.

## 1.2 Compatibility

This feature introduces the following Gallagher software:

- Gallagher Schindler Call Interface Plugin v8.50.029
- Gallagher Schindler Live Reporting Plugin v8.50.014
- Gallagher FTCAPI Middleware Framework vMF8.10.008

This feature supports the following Gallagher software:

- Gallagher Command Centre vEL8.50.1677 (or later Command Centre release)
- Gallagher Controller 6000 vCR8.50.210623c (or later release)

Command Centre and this feature have been tested using the following:

- Command Centre Server: Windows Server 2019
- Command Centre Workstation: Windows 10 (64-bit)
- Database: SQL Server 2019

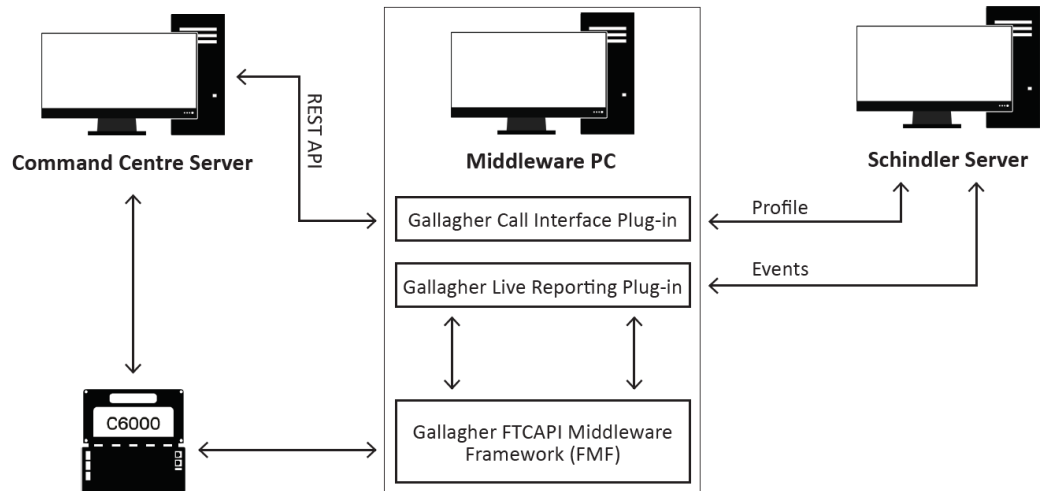
The Call by Profile feature does not support Schindler readers.

This feature has been tested using Schindler v1.3.369.1

This feature is compatible with Schindler Call Interface and Live Reporting Interface protocols as specified in the "Third-PartyCallInterface-060318-2247-2284.pdf" and "Third-PartyLiveReportingInterface-060318-2249-2288.pdf" documents.

This feature has **not** been tested in a Command Centre multi-server environment.

### 1.3 Deployment architecture



---

## 2 Installation

---

**Note:** If a previous version of this feature has been installed and you are upgrading to a newer version, skip section 2 "*Installation*" and refer to section 8 "*Upgrading*" later in this release note.

To install this feature, perform the following procedure:

1. Perform a backup of your Command Centre system.
2. Ensure your Command Centre licence file (Command Centre.lic) contains the following entry:

```
[Features]
SchindlerHLICallbyProfile=1

[Plugin]
Plugin0=SchindlerID-LifeReporting
Plugin1=SchindlerID-CallInterface
```
3. Store the licence file in the following folder:  
C:\ProgramData\Gallagher\Command Centre
4. Exit Command Centre and stop the Command Centre Services.
5. On the Command Centre Server and all Command Centre Workstations, install vEL8.50.1677 (or later Command Centre release) from the Command Centre installation media, if not already installed.
6. Restart the Command Centre Services and Command Centre.

### Installing the FTCAPI Middleware Framework (FMF)

The Middleware PC needs to have the FTCAPI Middleware Framework installed (vMF8.10.008 or later). To install the FMF, refer to the topic "*Installing the FTCAPI Middleware Framework (FMF)*" in the Gallagher Configuration Client Help.

### Installing the Live Reporting and Call Interface Plug-ins

1. Run the installation executables **Gallagher Schindler Live Reporting Plug-in Setup 8.50.xx.msi** and **Gallagher Schindler Call Interface Plug-in Setup 8.50.xx.msi** on the FTCAPI Middleware Framework PC.
2. Once the installation is complete, manually restart the FTCAPI Router Service.
3. To ensure that the Live Reporting and Call Interface plug-ins have been installed correctly, select the Programs and Features utility from the Windows Control Panel. The 'Gallagher Schindler Live Reporting Plug-in' and 'Gallagher Schindler Call Interface Plug-in' programs should be listed as installed.

**Note:** Gallagher Schindler Live Reporting and Gallagher Schindler Call Interface Plug-ins must be installed on the same PC (i.e. Middleware PC).

---

## 3 Configuration

---

To configure this feature, perform the following procedures in Gallagher Configuration Client:

- 3.1 Web Services
- 3.2 REST API Client Item
- 3.3 Create a Schindler Access Zone
- 3.4 Create Schindler Personal Data Fields
- 3.5 Schindler Access Group
- 3.6 Schindler Cardholders
- 3.7 Profile Configuration File

### 3.1 Web Services

Before being able to create a REST API Client, you need to enable REST API. To do this, refer to the topic "*Web Services*" in the Gallagher Configuration Client Help.

### 3.2 REST API Client Item

To configure a REST API Client Item, refer to the topic "*Creating a REST API Client Item*" in the Gallagher Configuration Client Help.

The REST Client Operator requires the following privileges:

Privilege...	is required to...
View Cardholders	view Cardholders
View Events	view Cardholder related events
View Personal Data Definition	view Cardholder Personal Data Fields

Assign the appropriate privileges to the appropriate operators. For instructions on how to assign operator privileges, refer to the topic "*Setting up Operator Groups*" in the Gallagher Configuration Client Help.

### 3.3 Create a Schindler Access Zone

Create an Access Zone. Assign the 'Default Access Zone Secure' schedule to this zone. Then, this Access Zone can be used on all Schindler Terminals.

When a Cardholder is granted access, the Cardholder's Schindler Profile is sent (via a Door) to the Schindler system. The Door is configured later in this release note in section [5.6](#).

### 3.4 Create a Schindler Profile Personal Data Field

Create a Personal Data Field with text-list (recommended) or text data type. Add all the profile names provided by Schindler integrators to this PDF. The name of this PDF must match the PDF name provided in the 'SchindlerPlugin.config' file.

**Note:** The default value for the `profile_pdf_name` parameter is 'Schindler Profile'. This value can be changed in the 'SchindlerPlugin.config' file, but the value must match the name of the PDF used to configure Schindler Profiles (i.e. PDF created in this section).

The screenshot shows the 'Schindler Profile - Properties' dialog box. On the left, there is a sidebar with tabs: 'General', 'Type', 'Group Membership', and 'Notes'. The 'General' tab is active. The 'Data type' is set to 'Text - List'. The 'Required Field' checkbox is unchecked. The 'Default value' is an empty text box. The 'Unique Values' checkbox is unchecked. The 'Default privilege' is set to 'Edit' and the 'Sort Order' is '50'. Below these, there is a 'List Values' section with an empty text box and 'Add' and 'Delete' buttons. A list of values is shown below: 'GGL Level 1', 'GGL Level 2', 'GGL Level 3', 'GGL Level 4', and 'GGL Level 5'. 'GGL Level 5' is selected. A 'Restrict to List' checkbox is checked. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

### 3.5 Schindler Access Group

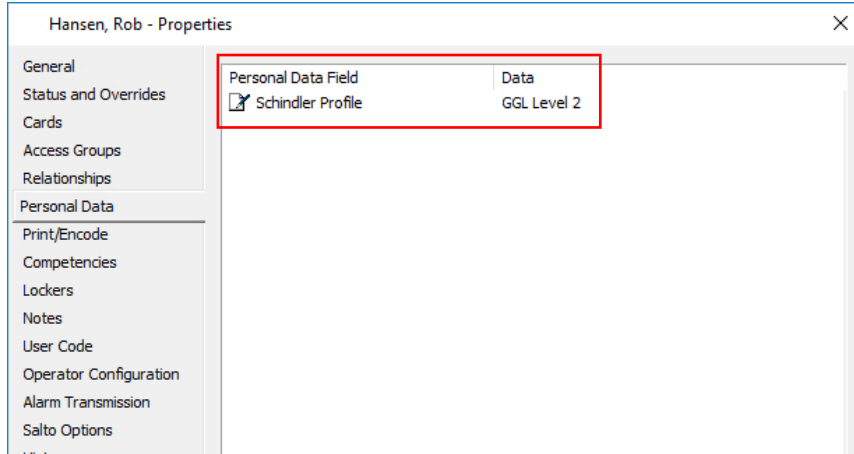
Create an Access Group. Name the Access Group 'Schindler Access Group'. Assign to this Access Group:

- Schindler Cardholders (Cardholders that require access to Schindler readers, terminals and lifts).
- The Schindler Access Zone. Cardholders belonging to this Access Group will inherit access to the Schindler Access Zone.
- The Schindler Cardholder Access Schedule (for the Schindler Access Zone).
- Schindler Personal Data Field. Cardholders belonging to this Access Group will inherit the Schindler PDF (Schindler Profile).

The screenshot shows the 'Schindler Access Group - Properties' dialog box. On the left, there is a sidebar with tabs: 'General', 'Lineage', 'Cardholder Membership', 'Membership Defaults', 'Access', 'Privileges', 'Terminal Access', 'Alarm Zones', 'Personal Data', 'Anti-Passback Response', 'Salto Access', and 'Notes'. The 'Personal Data' tab is active. The main area shows a table with columns 'Name' and 'Description'. A single entry is listed: 'Schindler Profile' with a checked checkbox in the 'Name' column. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

### 3.6 Schindler Cardholders

Create the Cardholders that require access to Schindler readers, terminals and lifts. Configure the Schindler Personal Data Field values for each Cardholder.

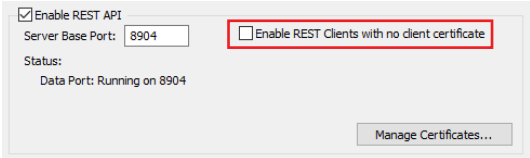


**Note:** The 'Schindler Profile' PDF along with the appropriate profile (i.e. GGL Level 2) must be assigned to all Cardholders that require access to Schindler terminals and lifts. Otherwise, the Cardholder will be **denied** access by the Schindler system.

### 3.7 Profile Configuration File

**Note:** Before configuring the Profile file, ensure that you have installed the FMF and the Call Interface on the Middleware PC. Refer to section 2 "Installation" earlier in this release note.

Parameter	Description
call_by_profile	When it is set to 'true', it enables the Call by Profile functionality. By default, it is set to false (i.e. Command Centre will use the SchindlerID feature).
profile_pdf_name	The name of the Command Centre PDF that is configured with Schindler Profiles. Ensure that this name matches the name of the PDF created in Configuration Client.
default_Schindler_profile	The name of the Schindler profile that has no access rights configured. This profile is used for a Cardholder who does not belong to the 'Schindler Access Group' or has not been assigned a profile.
rest_api_url	The base URL for the REST API on the destination CC server machine. It consists of the Fully-Qualified Domain Name (FQDN) of the machine hosting the Command Centre Server and the REST API Port.  "api_url": "https://[hostname].[domain]:[Rest API Port]/api/"  "api_url": "https://gnz-pc1507.gallagher.local:8904/api/"  OR,  "api_url": "https://[CC server IP address]: [Rest API Port]/api/"  "api_url": "https://10.60.12.10:8904/api/"

Parameter	Description
rest_api_key	<p>The API Key from the 'API Key' tab of the REST Client item in Configuration Client.</p> <p>The Command Centre Server requires the client to include the 'API Key' with every request it sends. This key is generated when you create a REST Client item in the Command Centre Server.</p> <p><b>Note:</b> You must keep the API Key secure.</p>
certificate_thumbprint	<p>A certificate thumbprint uniquely identifies a certificate. For more information, refer to the topic "<i>Creating the Client Certificate</i>" in the Gallagher Configuration Client Help.</p> <p>You only need to enter this when the 'Enable REST Clients with no client certificate' option is unchecked and/or your REST Client item has a 'Client Certificate Thumbprint' assigned.</p>  <p><b>Note:</b> The self-assigned certificate created for the REST Client must be stored in the Local Machine certificate store under the 'Personal' folder.</p>
validate_rest_server_certificates	<p>When it is set to 'false', a self-signed certificate can be used. When set to 'true', a trusted certificate is required to connect to the Command Centre Server.</p>
schindler_zone_status_delay_milliseconds	<p>Sets a delay in milliseconds between each zone change message/command (i.e. change between free and secure states) sent from Command Centre to the Schindler system. This can help prevent Schindler losing messages due to queue overload. The default value is 1000 milliseconds.</p> <p>If enabling this parameter, Gallagher recommends starting with 1000 ms, then changing if required. The optimal value may depend on your Schindler server and other system factors.</p> <p>To enable the parameter, remove the <code>&lt;!--</code> before the <code>&lt;add key=</code> and remove the <code>--&gt;</code> after the <code>value="n"/&gt;</code> in the file.</p> <p>If the parameter is removed, set to 0, or given no value (<code>value=""</code>), there is no delay between messages. Range is from 1-5000. If a value over 5000 is entered, the maximum of 5000 milliseconds is used.</p>

1. On the Middleware PC, navigate to the following directory: `C:\Program Files (x86)\Gallagher\FTCAPI\Middleware Framework\Plugin`
2. Double-click the 'SchindlerPlugin.config' file.
3. Configure as required.
4. Save the file.

**Note:** After modifying the 'SchindlerPlugin.config' file, you must restart the FTCAPI Router Service. Otherwise, the changes made to the config file will not be applied.

---

### Configuration example

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <appSettings>
    <!-- Set this option to "true" to use "Call By Profile". Default is set to "Call By ID"-->
    <add key="call_by_profile" value="true"/>

    <!-- The Command Centre PDF that stores the Schindler profile names -->
    <add key="profile_pdf_name" value="Schindler Profile"/>

    <!-- The name of the Schindler Profile that has no access configured, default is set to "No
    Access" -->
    <add key="default_Schindler_profile" value="No Access"/>

    <!-- The server url for REST API. By default, it is set to "https://localhost:8904/api" -->
    <add key="rest_api_url" value="https://localhost:8904/api"/>

    <!-- The REST Client API Key. This can be found on the "API Key" property page for the REST Client
    in Configuration Client -->
    <add key="rest_api_key" value=" 558C-2837-F0B4-050C-36A7-8A4A-
    4DE2-61E0"/>

    <!-- The REST Client Certificate Thumbprint-->
    <add key="certificate_thumbprint" value="
    F2AED9AC8CE86E832FA6A9C97C3E7008F94CA1B5"/>

    <!-- Set this option to "true" to validate REST server certificate. Default is set to "true" -->
    <!--<add key="validate_rest_server_certificates" value="true"/>-->
  </appSettings>
</configuration>
```

## 4 Live Reporting Interface configuration

To configure the Live Reporting Interface, perform the following procedures in Gallagher Configuration Client:

- 4.1 External System Server
- 4.2 External System (Reporting Interface)
- 4.3 External System Items (Floors)
- 4.4 External System Item (dummy Floor)

### 4.1 External System Server

If you are using Command Centre vEL7.80 or later, you should have an External System Server item to represent your Middleware PC. If one is not configured already, refer to the topic "*Configuring an External System Server*" in the Gallagher Command Centre Help.

### 4.2 External System (Live Reporting Interface)

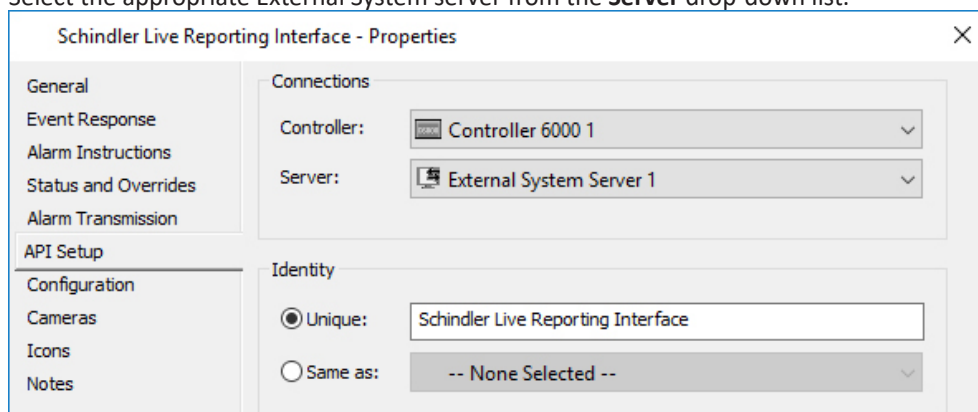
This procedure describes how to create an External System (Live Reporting Interface) that will enable Command Centre to build an audit trail for lift access events. This External System is used to interface with the Logging Task Interface in Schindler.

#### Before you begin

Request Schindler integrators to create a Logging Task Interface in Schindler, and provide the TCP/IP Port Number shown on the Logging Task Interface. This TCP/IP Port is required later in this procedure.

#### Procedure

1. Click **Configure** from the menu bar then **External Systems**.
2. Right-click and select **New... > External System**.
3. Type in the Name, (e.g. Schindler Live Reporting Interface) Description and select the Division.
4. Click the **Event Response** tab and assign a primary Alarm Zone for all events.
5. Click the **API Setup** tab.
6. Select the appropriate **Controller** from the drop-down list.
7. Select the appropriate External System server from the **Server** drop-down list.



8. Click the **Unique** radio button in the 'Identity' section of this screen and type in a unique identity string, (e.g. Schindler Live Reporting Interface). The string entered here only needs to be unique and does not need to match any name or string from the Schindler system. This field is limited to a maximum of 64 characters.
9. Click the **Configuration** tab.

**Note:** This tab only appears if 'Identity' on the **API Setup** tab is set to 'Unique'.

The screenshot shows a dialog box titled "Schindler Live Reporting Interface - Properties". On the left is a sidebar with tabs: General, Event Response, Alarm Instructions, Status and Overrides, Alarm Transmission, API Setup, Configuration (selected), Cameras, Icons, and Notes. The main area shows "System Type:" with a dropdown menu set to "SchindlerID Life Reporting". Below this is a "Configuration" section with two input fields: "IP Address:" containing "0 . 0 . 0 . 0" and "Port:" containing "6060". At the bottom right are three buttons: "OK", "Cancel", and "Apply".

10. Select the 'SchindlerID Life Reporting', (i.e. The middleware plug-in to be used) from the **System Type** drop-down list. The 'Configuration' section of this screen becomes populated accordingly.
11. Enter the Schindler server IP Address in the **IP Address** field.
12. Enter the TCP/IP Port Number of the Schindler Logging Task Interface in the **Port** field, as shown below in the Logging Task Interface. Range 0-65535.

To enable live reporting, in the Schindler system ensure the Logging of Personal Data is set to **Always** and the Live Reporting **Active** check-box is ticked.

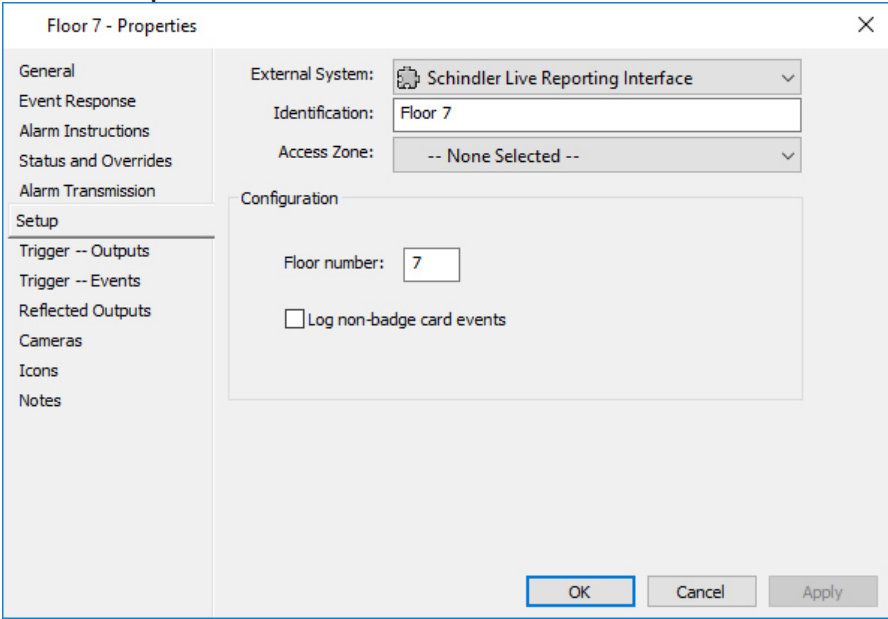
**Note:** Schindler advises that storing personal data may violate local laws. However, if the local laws are fulfilled and you want to log the personal data using the Live Reporting Interface, you need to select the option **Always** for Logging of Personal Data in the Logging Task Interface.

13. Click the **OK** button.

### 4.3 External System Items (Floors)

An External System Item is required for each floor in the building. The External System Items represent Schindler floors in Command Centre. Live reporting events are logged against these floors.

1. Click **Configure** from the menu bar then **External Systems**.
2. Right-click and select **New... > External System Item**.
3. Type in the Name, (e.g. Floor 7) Description and select the Division.
4. Click the **Event Response** tab and assign a primary Alarm Zone for all events.
5. Click the **Setup** tab.



The screenshot shows a dialog box titled "Floor 7 - Properties" with a close button (X) in the top right corner. On the left is a vertical list of tabs: General, Event Response, Alarm Instructions, Status and Overrides, Alarm Transmission, Setup (highlighted), Trigger -- Outputs, Trigger -- Events, Reflected Outputs, Cameras, Icons, and Notes. The main area is divided into sections. The "External System" section has a dropdown menu showing "Schindler Live Reporting Interface". Below it, the "Identification" field contains the text "Floor 7". The "Access Zone" section has a dropdown menu showing "-- None Selected --". The "Configuration" section contains a "Floor number" field with the value "7" and a checkbox labeled "Log non-badge card events" which is currently unchecked. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

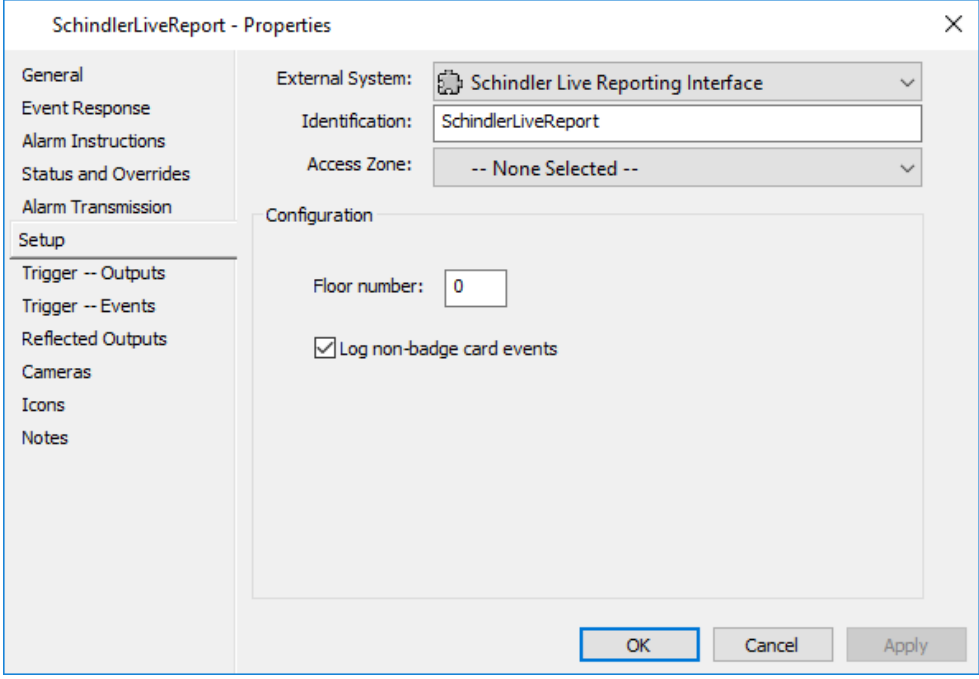
6. Select the **External System** (Schindler Live Reporting Interface) from the drop-down list that this External System Item belongs to.  
**Note:** If you do not select an External System, this item will display at the root level of the External System window tree until it is assigned an External System as a parent.
7. Enter a string value in the **Identification** field, (e.g. Floor 7).  
**Note:** The Identification string entered is checked for uniqueness within the same External System and is limited to 64 characters. The string entered here only needs to be unique and does not need to match any name or string from the Schindler system.
8. Enter a floor number in the **Floor** field, (e.g. 7). This floor number must correspond with a floor in Schindler.
9. If required, check the **Log non-badge card events** checkbox. Selecting this option will enable Command Centre to receive 'non-badge card events' from the Schindler system.  
**Note:** A 'non-badge card event' is a Schindler allocation event that doesn't have an ID or person number, but has a destination floor.
10. Click the **OK** button.
11. Repeat this procedure to configure an External System Item for each floor.  
**Note:** For any further configuration required, refer to the chapter "*External Systems*" in the Gallagher Configuration Client Help.

## 4.4 External System Item (dummy Floor)

A dummy floor is used to log all events that do not map to any configured floors (i.e. access denied events from the Schindler system.)

### Procedure

1. Click **Configure** from the menu bar then **External Systems**.
2. Right-click and select **New... > External System Item**.
3. Type in the Name, (e.g. Schindler Dummy Floor) Description and select the Division.
4. Click the **Event Response** tab and assign a primary Alarm Zone for all events.
5. Click the **Setup** tab.



The screenshot shows the 'SchindlerLiveReport - Properties' dialog box with the 'Setup' tab selected. The 'External System' dropdown is set to 'Schindler Live Reporting Interface'. The 'Identification' field contains 'SchindlerLiveReport'. The 'Access Zone' dropdown is set to '-- None Selected --'. The 'Configuration' section has 'Floor number' set to '0' and the 'Log non-badge card events' checkbox checked. The 'OK' button is highlighted.

6. Select the **External System** (i.e. Schindler Live Reporting Interface) from the drop-down list that this External System Item belongs to.  
**Note:** If you do not select an External System, this item will display at the root level of the External System window tree until it is assigned an External System as a parent.
7. Enter the unique string used by the Live Reporting Interface External System (e.g. Schindler Live Reporting Interface) into the **Identification** field. This will enable the logging of access denied events from the Schindler system.  
**Notes:**
  - The Identification string should be unique and should not be the same as the External System name. It is checked for uniqueness within the same External System and is limited to 64 characters.
  - The default value for **Floor number** is '0'. This value must **not** be changed.
8. If required, check the **Log non-badge card events** checkbox. Selecting this option will enable Command Centre to receive 'non-badge card events' from the Schindler system.  
**Note:** A 'non-badge card event' is a Schindler allocation event that doesn't have an ID or person number, but has a destination floor.
9. Click the **OK** button.

## 5 Call Manager Interface configuration

**Note:** If you are not using Gallagher Readers on elevator terminals and are not controlling a floor's secure/free state from Command Centre, you do not need to create the Call Manager Interface, hence the information in this section is not applicable.

To configure the Call Manager Interface, perform the following procedures in Gallagher Configuration Client:

- 5.1 External System (Call Manager Interface)
- 5.2 External System Items (Terminals)
- 5.3 Alarm Zone
- 5.4 Action Plans
- 5.5 Readers
- 5.6 Dummy Doors

### 5.1 External System (Call Manager Interface)

This procedure describes how to create an External System (Call Manager Interface) that will be used to interface with the Call Manager Interface in Schindler.

#### Before you begin

Request Schindler integrators to create the Call Manager Interface in Schindler, and provide the TCP/IP Port Number of the Schindler Call Manager Interface shown in the **Port** field.

#### Procedure

1. Click **Configure** from the menu bar then **External Systems**.
2. Right-click and select **New... > External System**.
3. Type in the Name, (e.g. Schindler Call Manager Interface) Description and select the Division.
4. Click the **Event Response** tab and assign a primary Alarm Zone for all events.
5. Click the **API Setup** tab.
6. Select the appropriate **Controller** from the drop-down list.
7. Select the appropriate External System server from the **Server** drop-down list.

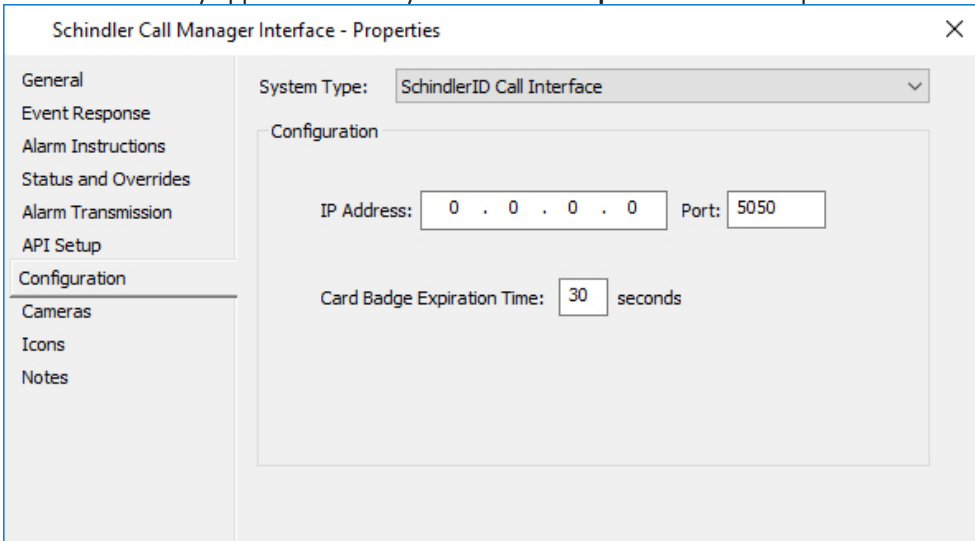
The screenshot shows the 'Schindler Call Manager Interface - Properties' dialog box. The 'API Setup' tab is active. Under the 'Connections' section, the 'Controller' dropdown is set to 'Controller 6000 1' and the 'Server' dropdown is set to 'External System Server 1'. Under the 'Identity' section, the 'Unique' radio button is selected, and the text field next to it contains 'Schindler Call Manager Interface'. The 'Same as' radio button is unselected, and its dropdown menu shows '-- None Selected --'. The 'OK', 'Cancel', and 'Apply' buttons are visible at the bottom of the dialog.

- Click the **Unique** radio button in the 'Identity' section of this screen and type in a unique identity string, (e.g. Schindler Call Manager Interface). The string entered here only needs to be unique and does not need to match any name or string from the Schindler system. This field is limited to a maximum of 64 characters.

**Note:** If you have more than 1000 terminals, click the **Same as** radio button and link the identity of this terminal to be the same as another by selecting a terminal from the drop-down list.

- Click the **Configuration** tab.

**Note:** This tab only appears if 'Identity' on the **API Setup** tab is set to 'Unique'.



The screenshot shows a window titled "Schindler Call Manager Interface - Properties" with a close button (X) in the top right corner. On the left is a vertical navigation menu with the following items: General, Event Response, Alarm Instructions, Status and Overrides, Alarm Transmission, API Setup, Configuration (highlighted), Cameras, Icons, and Notes. The main area of the window is titled "Configuration" and contains the following fields: "System Type:" with a dropdown menu showing "SchindlerID Call Interface"; "IP Address:" with a text box containing "0 . 0 . 0 . 0"; "Port:" with a text box containing "5050"; and "Card Badge Expiration Time:" with a text box containing "30" followed by the word "seconds".

- Select 'SchindlerID Call Interface', (i.e. The middleware plug-in to be used) from the **System Type** drop-down list. The 'Configuration' section of this screen becomes populated accordingly.
- Enter the Schindler server IP Address in the **IP Address** field.
- Enter the TCP/IP Port Number of the Schindler Call Manager Interface in the **Port** field. Range 0-65535.
- If required, enter a **Card Badge Expiration Time**. Range 1-600 seconds.  
If a user badges their card, this information is sent from the Controller to the Middleware Framework. The time between the information being sent is checked by the Middleware Framework. If this time exceeds the Card Badge Expiration Time, the terminal is not enabled and an event is logged, as it assumes a network delay has occurred and the person may no longer be at the terminal.
- Click the **OK** button.

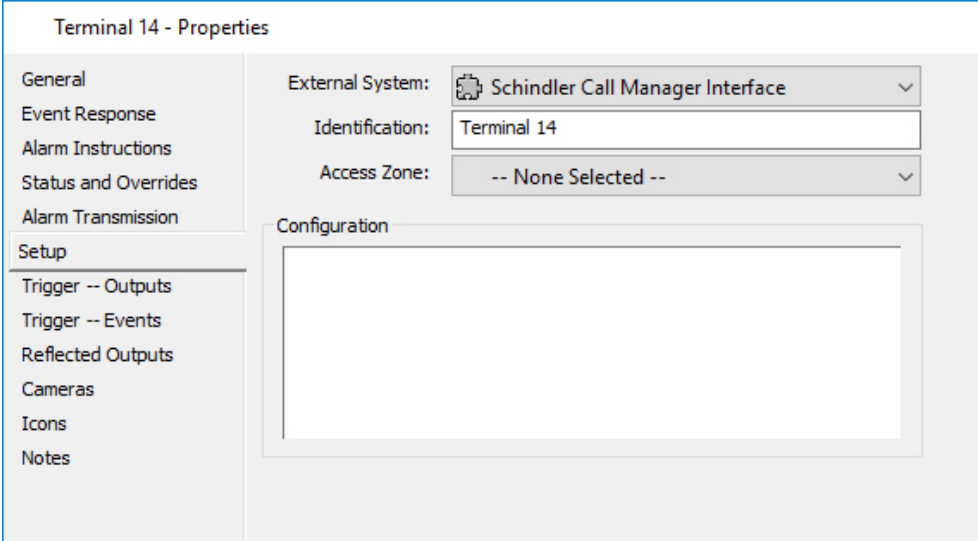
## 5.2 External System Items (Terminals)

An External System Item is required for each terminal in the building. The External System Items represent Schindler terminals in Command Centre. A building may have more than one terminal per floor.

**Note:** Contact Schindler integrator to obtain the Terminal IDs in Schindler.

Perform the following procedure to configure a terminal:

1. Click **Configure** from the menu bar then **External Systems**.
2. Right-click and select **New... > External System Item**.
3. Type in the Name, (e.g. Terminal 14) Description and select the Division.
4. Click the **Event Response** tab and assign a primary Alarm Zone for all events.
5. Click the **Setup** tab.



6. Select the **External System** (Schindler Call Manager Interface) from the drop-down list that this External System Item belongs to.

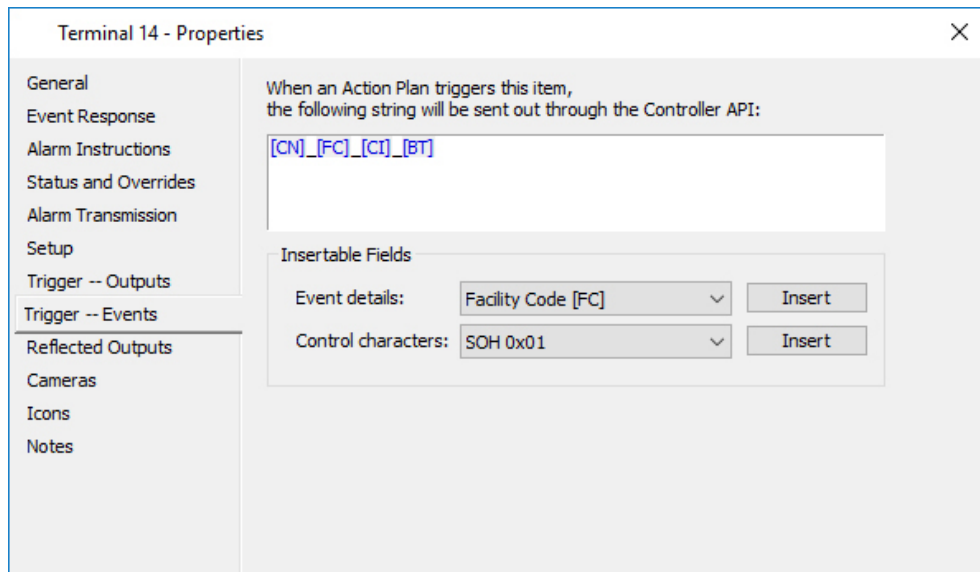
**Note:** If you do not select an External System, this item will display at the root level of the External System window tree until it is assigned an External System as a parent.

7. Enter a string value in the **Identification** field, (e.g. Terminal 14).

**Note:** The Identification string entered is checked for uniqueness within the same External System and is limited to 64 characters.

8. Enter a Terminal ID in the **Terminal** field, (e.g. 14). This Terminal ID must match a Terminal ID in Schindler. Range 0-255. The origin of this range limit is in the Schindler External Call Manager Settings.

9. Click the **Trigger -- Events** tab.



**Notes:**

- For cards only, the following fields are required: [CN]\_[FC].
- For cards and Mobile Credentials, the following fields are required: [CN]\_[FC]\_[CI]\_[BT].
- Manually typing in [CN], [FC], [CI], and [BT] will result in an error message, later on.

10. Select **Card Number [CN]** from the Event Details drop-down list and click **Insert**.
11. Type an underscore then select **Facility Code [FC]** from the Event Details drop-down list and click **Insert**.
12. Do you need to support Mobile Credentials?  
If **yes**, go to step 13 of this procedure.  
If **no**, go to step 15 of this procedure.
13. Type an underscore then select **Cardholder ID [CI]** from the Event Details drop-down list and click **Insert**.
14. Type an underscore then select **Badge Type [BT]** from the Event Details drop-down list and click **Insert**.
15. Click the **OK** button.
16. Repeat this procedure to configure an External System Item for each terminal in the building.

**Note:** For any further configuration required, refer to the "External Systems" chapter in the Gallagher Configuration Client Help.

### 5.3 Alarm Zone

Configure an Alarm Zone for all Schindler items. Refer to the topic "Setting up Alarm Zones" in the Gallagher Configuration Client Help.

## 5.4 Action Plans

This Action Plan is used to associate the dummy Door (configured in 5.6) with the External System Item (terminal). An Action Plan is required for each terminal in the building.

1. Click **Configure** from the menu bar then **Action Plans**.
2. Right-click and select **New... > Action Plan**.
3. Type in the Name, (e.g. Terminal 14 Action Plan) Description and select the Division.
4. Click the **Armed** tab.

The screenshot shows the 'Action Plan 1 - Properties' dialog box with the 'Armed' tab selected. The 'Alarm Priority' is set to 'Message Only' and the 'Alarm Transmitter' is set to '-- None Selected'. The 'Outputs' grid is empty, and the 'Cameras, Macros, and External System Items' grid contains 'Terminal 14'. The 'Deactivate' dropdown is set to 'Deactivate outputs when alarm is acknowledged'. The 'Escalation Rules' section has five checkboxes, all of which are unchecked, with corresponding time/alarms values set to 0.

5. Select **Not an Event** from the Alarm Priority drop-down list.  
**Note:** Ensure the Action Plan has an Alarm Priority that is set to 'Not an Event' otherwise you will get a lot of unnecessary events about access through the Door. For debugging during the installation it may be useful to configure the priority to 'Message Only'.
6. Drag and drop the External System Item (terminal) to be triggered into the **Cameras, Macros and External System Items** grid, (e.g. Terminal 14).
7. Click the **Disarmed** tab and repeat steps 5-6. These settings define the responses when the item triggering the Action Plan is in the disarmed state.
8. Repeat steps 5-6 for the next two tabs also, (i.e. **User 1** and **User 2** tabs).
9. Click the **OK** button.
10. Repeat this procedure to create an Action Plan for each terminal.  
**Note:** For any further configuration required, refer to the topic "*Creating a new Action Plan*" in the Gallagher Configuration Client Help.

## 5.5 Readers

Configure the readers required for this integration. Refer to the topic "*Creating Readers*" in the Gallagher Configuration Client Help.

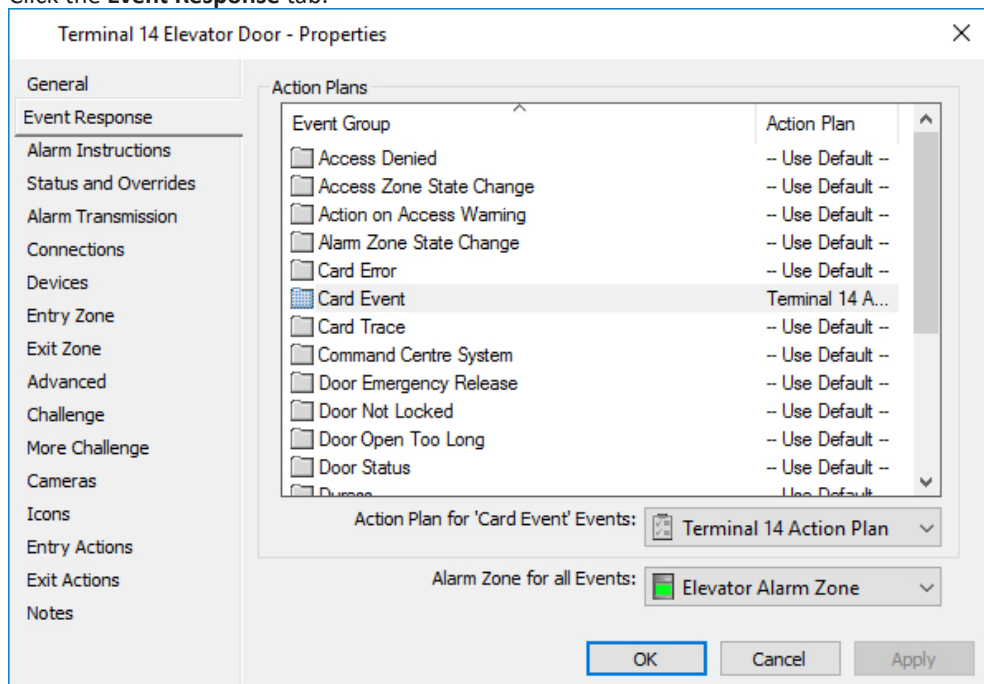
## 5.6 Dummy Doors

A dummy Door is required for each terminal in the building.

**Note:** You do not need to create a dummy Door for simulated terminals, used to control the secure/free state of floors.

Perform the following procedure to configure a dummy Door:

1. Click **Configure** from the menu bar then **Doors**.
2. Right-click and select **New... > Door**.
3. Type in the Name, (e.g. Terminal 14 Elevator Door) Description and select the Division.
4. Click the **Event Response** tab.



5. Select the **Card Event** Event Group and assign the Action Plan created for the terminal corresponding to this dummy Door.
6. Select an **Alarm Zone** from the drop-down list that is common to all terminals in the Schindler system.  
**Note:** Doors must be placed into an Alarm Zone before you will receive Door Events.
7. Click the **Connections** tab and assign the Door to the Controller that will host this Door. This must be the same Controller assigned to the External System Item representing each terminal.
8. Click the **Entry Zone** tab.
9. Select an **Access Zone** from the drop-down list. Ensure the Schindler Access Zone Schedule (previously created) is assigned to the zone, and that Cardholder Access to this zone is 'Secure - No PIN' at all times.
10. From the **Reader(s)** drop-down list, select the appropriate reader that provides entry for this terminal.
11. Click the **OK** button.
12. Repeat this procedure to configure a dummy Door for each terminal.

## 6 Secure/Free floor configuration

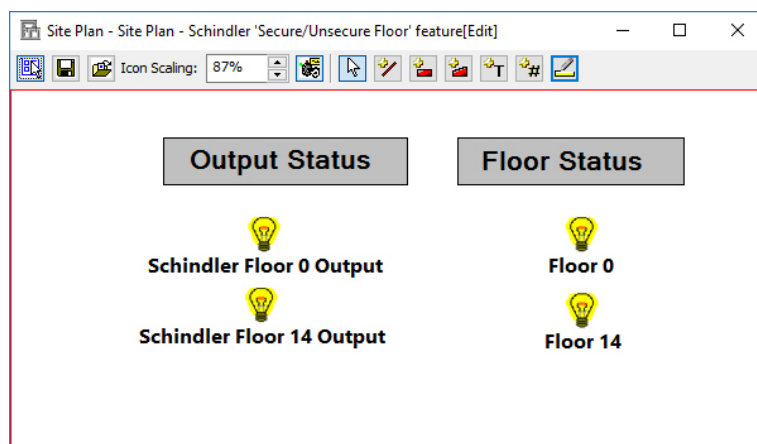
The secure/free floor component of the Call Manager Interface enables an operator to either secure or free a floor.

Floor State	Description
Secure	A valid access card is required to gain access to the floor
Free	An access card is not required

You will need to configure a virtual output for each floor you wish to secure. An operator can change the state of a floor to either secure or free by performing an override on the virtual output for the appropriate floor.

You will also need to configure an External System Item (Floor) for each floor you wish to secure. This item uses Schindler Time Patterns to reflect the true state of the floor. An operator can then observe the state of the floor from within Command Centre.

If the simulated terminal has not received the override command, the output state may differ from the External System Item state. The operator can then repeat the override action. If all is well, the virtual output state should be the same as the External System Item state.



Whenever Command Centre reconnects to Schindler (after being disconnected), all floor states are resent from Command Centre to Schindler. This helps to ensure all floor states in Schindler are correct.

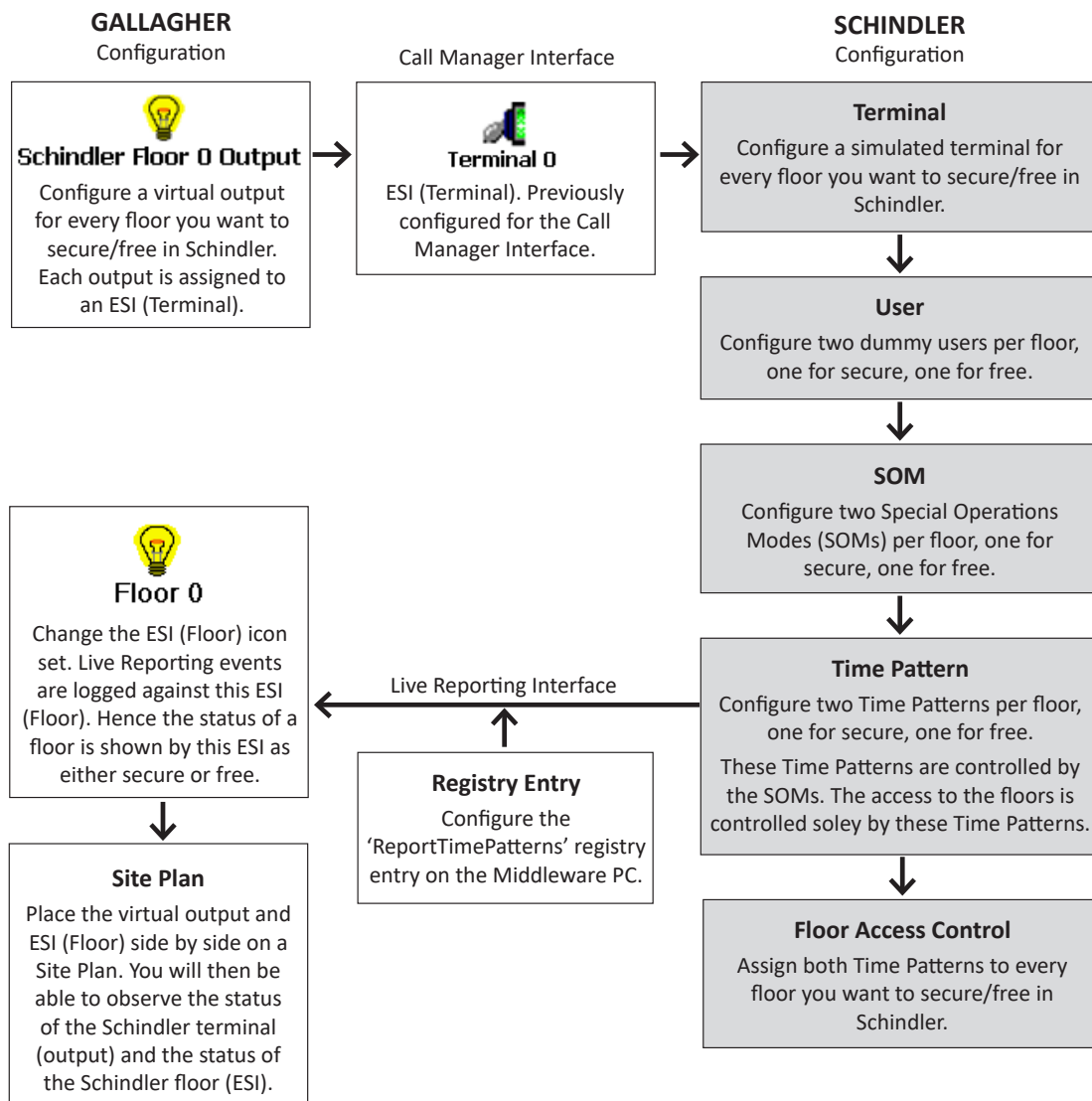
## Configuration process

Command Centre doesn't control the state of the floors directly. Instead Command Centre uses Special Operation Modes (SOMs) that control the Time Patterns assigned to the floors in Schindler. Therefore the proper functionality depends on the correct configuration of these Schindler items.

The following diagram provides an overview of the configuration process you will need to follow to secure/free floors. This process identifies the various items you will need to configure in both Command Centre and Schindler.

### Notes:

- This configuration process has been tested and is a suggestion as to how Schindler can be configured to secure/free floors. Your configuration of Schindler may vary, depending on your requirements.
- An additional configuration option (`schindler_zone_status_delay_milliseconds`) exists in the configuration file 'SchindlerPlugin.config'. This option adds a delay between each zone change message/command sent from Command Centre to Schindler, to help mitigate queue overload. For details, refer to section 3.7 "[Profile Configuration File](#)" earlier in this release note.



---

Perform the following procedures (in the order listed below) to configure each of the items required to secure/free floors:

- 6.1 Configuring Time Patterns (In Schindler)
- 6.2 Configuring Floor Access Requirements (In Schindler)
- 6.3 Configuring Special Operation Modes (SOMs) (In Schindler)
- 6.4 Configuring Dummy Users (In Schindler)
- 6.5 Configuring Simulated Terminals (In Schindler)
- 6.6 Configuring the 'ReportTimePatterns' registry (On Middleware PC)
- 6.7 Configuring a virtual output for each floor (In Command Centre)
- 6.8 Assigning each virtual output to an ESI (Terminal) (In Command Centre)
- 6.9 Changing the ESI (Floor) icon set (In Command Centre)
- 6.10 Configuring a Site Plan for the Secure/Free floor feature (In Command Centre)

### 6.1 Configuring Time Patterns (In Schindler)

Contact Schindler integrator to configure time patterns as required.

**Note:** The Time Pattern names must start with `Secure/Free` followed by the `floor number`. Additional strings are permitted after the floor number

**For example:**

```
[Secure|Free] [Floor Number] [additional strings]
Free 10
Secure 10 Level 1
```

### 6.2 Configuring Floor Access Requirements (In Schindler)

Contact Schindler integrator to configure floor access requirements.

### 6.3 Configuring Special Operation Modes (SOMs) (In Schindler)

Contact Schindler integrator to configure the Special Operation Modes as required.

### 6.4 Configuring Dummy Users (In Schindler)

Contact Schindler integrator to configure dummy users.

**Note:** The dummy user names must start with `Secure/Free` followed by the `floor number`. Additional strings are permitted after the floor number

**For example:**

```
[Secure|Free] [Floor Number] [additional strings]
Free 10
Secure 10 Level 1
```

### 6.5 Configuring Simulated Terminals (In Schindler)

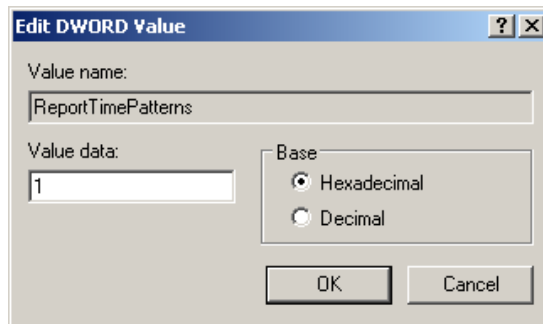
Contact Schindler integrator to complete this procedure.

## 6.6 Configuring the 'ReportTimePatterns' registry

To enable Time Pattern status reporting you will need to create the registry entry 'ReportTimePatterns' on the Middleware PC.

Perform the following procedure to create the 'ReportTimePatterns' registry:

13. From the Start menu, open the Windows Run command window (or press **Win + R**).
14. Type in 'regedit' and click **OK**. The Registry Editor opens.
15. Path your way to `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GALLAGHER\Command Centre`
16. Right-click in an empty space, then select **New > DWORD Value**. Your new DWORD Value is populated at the bottom of the registry values list.
17. Enter the DWORD Value name 'ReportTimePatterns'.
18. Double-click your newly created DWORD Value. The Edit DWORD Value window displays.

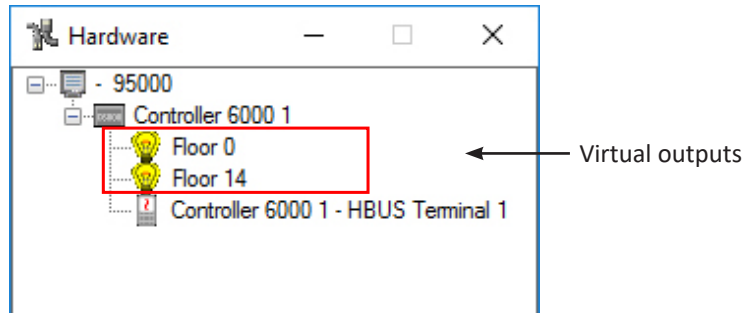


19. Select **Decimal** as the Base then enter a value, (e.g. 1) and click **OK**.

**Note:** If a value is not entered or the 'ReportTimePatterns' entry is not defined, Time Pattern status reporting will not be supported.

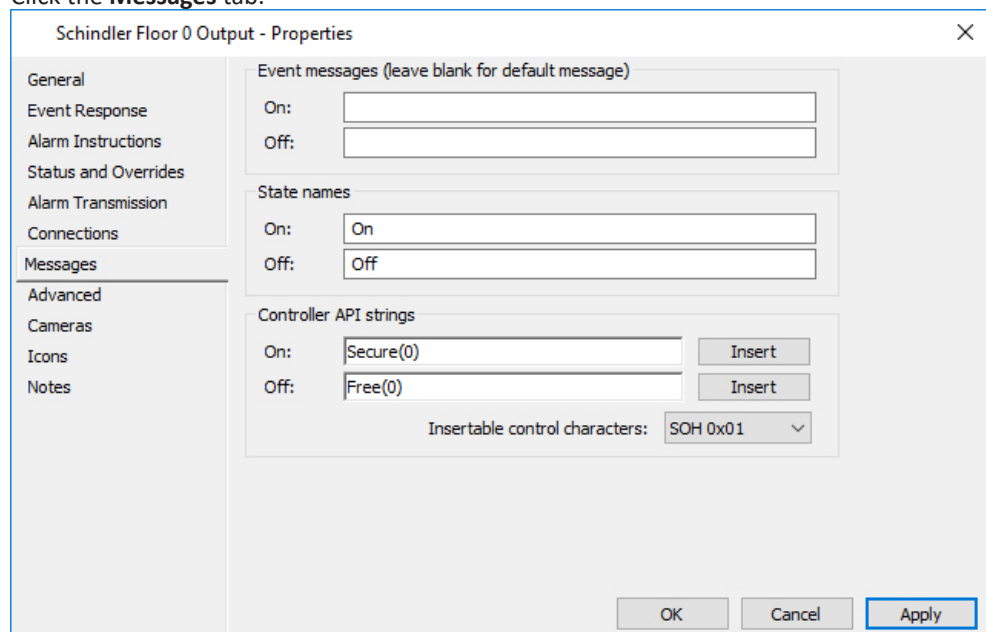
## 6.7 Configuring a virtual output for each floor

To configure Command Centre to Secure/Free floors, you will need to create a virtual output for each floor.



Perform the following procedure to configure a virtual output:

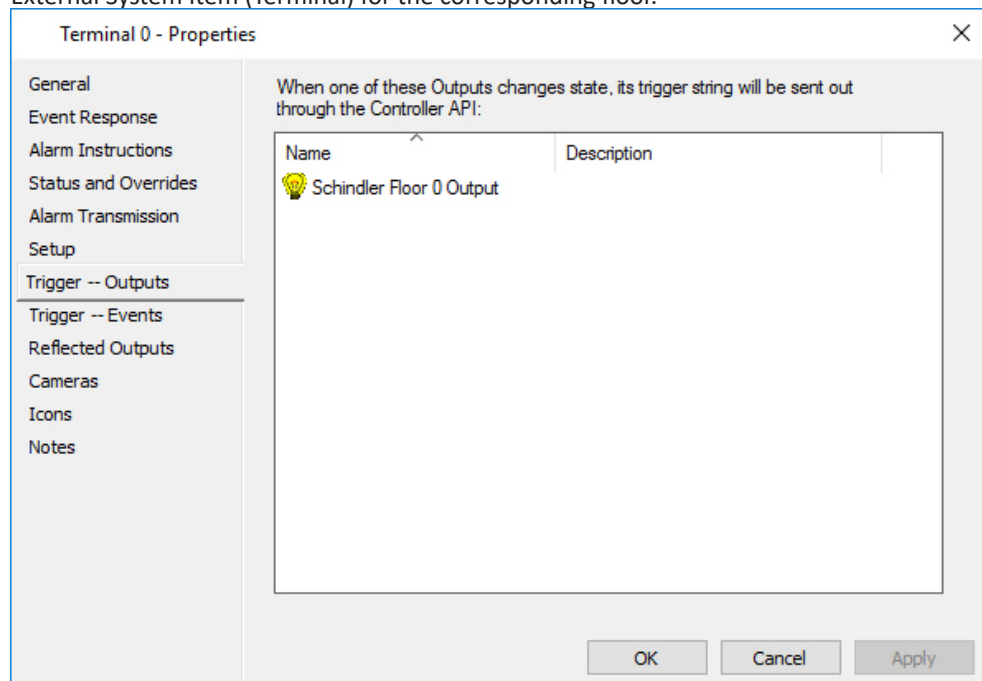
1. In Command Centre, click **Configure** from the menu bar then **Hardware**.
2. Right-click and select **New... > Input/Output**.
3. Type in the Name, (e.g. Schindler Floor 0 Output) Description and select the Division.
4. Click the **Messages** tab.

A screenshot of a dialog box titled 'Schindler Floor 0 Output - Properties'. The dialog has a sidebar on the left with several tabs: 'General', 'Event Response', 'Alarm Instructions', 'Status and Overrides', 'Alarm Transmission', 'Connections', 'Messages' (which is selected), 'Advanced', 'Cameras', 'Icons', and 'Notes'. The main area of the dialog is divided into three sections: 'Event messages (leave blank for default message)' with 'On:' and 'Off:' text boxes; 'State names' with 'On:' (containing 'On') and 'Off:' (containing 'Off') text boxes; and 'Controller API strings' with 'On:' (containing 'Secure(0)') and 'Off:' (containing 'Free(0)') text boxes, each with an 'Insert' button. Below these is a dropdown menu for 'Insertable control characters' set to 'SOH 0x01'. At the bottom right, there are 'OK', 'Cancel', and 'Apply' buttons, with 'Apply' being highlighted with a blue border.

5. To configure the output to on:
  - Enter the **Personal Number** of the dummy user (to **Secure** the corresponding floor) configured in Schindler into the FT Controller API String 'On' field, e.g. Secure(0).
6. To configure the output to off:
  - Enter the **Personal Number** of the dummy user (to **Free** the corresponding floor) configured in Schindler into the FT Controller API String 'Off' field, e.g. Free(0).
7. Click **OK** to exit and save your changes.

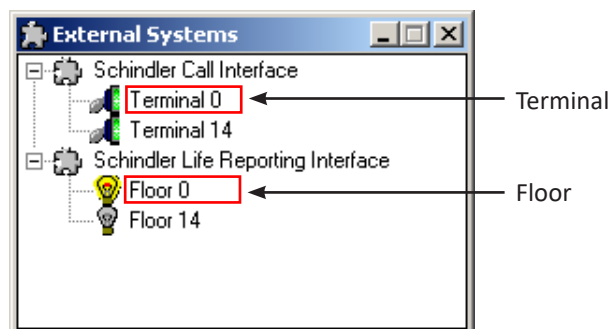
## 6.8 Assigning each virtual output to an ESI (Terminal)

1. You would have already configured the External Systems Items (Terminals).
2. Assign each virtual output (previously created) to the **Trigger -- Outputs** tab of the External System Item (Terminal) for the corresponding floor.



## 6.9 Changing the ESI (Floor) icon set

You would have already configured the External Systems Items (Floors). Live Reporting events are logged against these floors.

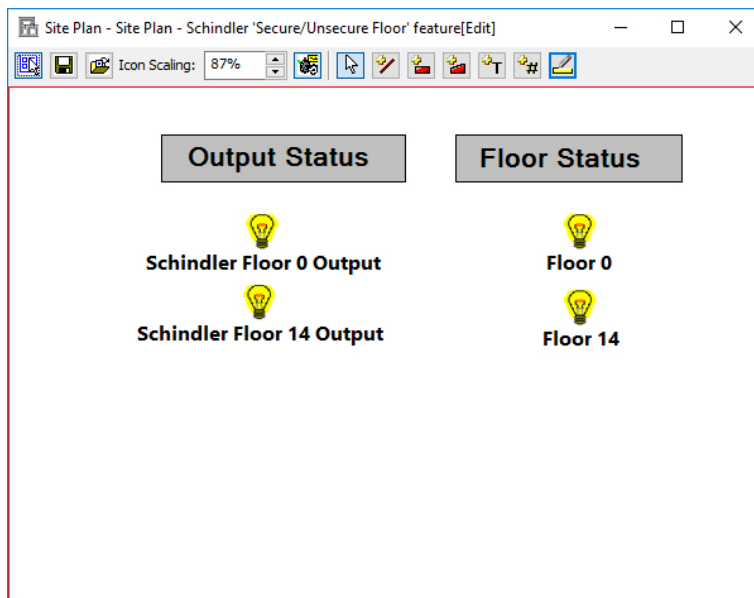


You will need to create a new icon set for the External System Items (Floors). This will enable you to easily observe the status of the building when the External System Item (Floor) is added to the 'Secure/Free Floor' Site Plan.

Refer to the topic "*Creating a new Icon Set*" in the Gallagher Configuration Client Help for further detail.

## 6.10 Configuring a Site Plan for the Secure/Free floor feature

Drag the External System Item (Floor) onto a Site Plan beside the virtual output. When placed on the Site Plan side by side, it is easily seen whether the Free/Secure action succeeded or whether it needs to be repeated.



If all goes fine, the status of the virtual output will match the status of the External System Item (Floor).

If a user overrides a virtual output at the moment when the Schindler simulated terminal is still processing the previous request (and therefore the latter one is thrown away), the status of the External System Item (Floor) reflects the last successful change, therefore differs from the External System Item (Terminal) status, and this way informs the operator that they should repeat the action.

## 6.11 Events and Alarms

The following Events and Alarms are raised only upon a Time Pattern state change.

Secure/Free Floor Operator Events:

Event Text	"[Floor]" is secured
Explanation	Occurs when a floor has been set to the Secure state
Event Group	Operator Event
Event Type	Operator Modified Item
Generated By	Command Centre

Event Text	"[Floor]" is free
Explanation	Occurs when a floor has been set to the Free state
Event Group	Operator Event
Event Type	Operator Modified Item
Generated By	Command Centre

Secure/Free Floor Command Centre System Medium High Priority Alarms:

Event Text	"[Floor]": Both Secure and Free Time Patterns are not active
Explanation	Occurs when both the Secure and Free Time Patterns are not active
Event Group	Command Centre System
Event Type	External Event 3
Generated By	Command Centre

Event Text	"[Floor]": Secure Time Pattern is not defined
Explanation	Occurs when the Secure Time Pattern has not been defined for this floor. If the Secure Time Pattern is deleted, this alarm will be generated. This alarm is only generated once, (i.e. If another override is performed on the output, this alarm will not be generated).
Event Group	Command Centre System
Event Type	External Event 3
Generated By	Command Centre

Event Text	"[Floor]": Free Time Pattern is not defined
Explanation	Occurs when the Free Time Pattern has not been defined for this floor. If the Free Time Pattern is deleted, this alarm will be generated. This alarm is only generated once, (i.e. If another override is performed on the output, this alarm will not be generated).
Event Group	Command Centre System
Event Type	External Event 3
Generated By	Command Centre

Secure/Free Floor Command Centre System High Priority Alarm:

Event Text	Time Patterns to secure/free "[Floor]" have been deleted
Explanation	Occurs when Time Patterns have been set for the floor then deleted. If the middleware services or Schindler system are disconnected from the network and then the Time Patterns are deleted, this alarm will not be generated.
Event Group	Command Centre System
Event Type	External Event 2
Generated By	Command Centre

---

## 7 Events and Alarms

---

The Event Viewer enables you to view events and alarms occurring at your site. To see further details about an alarm or event, double click the event or alarm message.

### Live Reporting (Event Logging) Events and Alarms

The following events or alarms may be displayed in the Event Viewer:

**Access granted:** If a cardholder is granted access to a destination floor, the following event is logged:

Summary: *<Cardholder> was granted access to <destination floor> at <ESI> (floor name).*

**Access denied:** If a cardholder is denied access to a destination floor, the following event is logged:

Summary: *<Cardholder> was denied access to <destination floor> at <ESI>( floor name).*

### Call Interface (Command Centre Lift Readers) Events and Alarms

The following events or alarms may be displayed in the Event Viewer:

**Card badge expired:** If a user badges their card, this information is sent from the Controller to the Middleware Framework. The time between the information being sent is checked by the Middleware Framework. If this time exceeds the Card Badge Expiration Time, the terminal is not enabled and the following event is logged.

Summary: *Card badge expired for <Cardholder> at <ESI> (terminal name).*

Details: *The card was badged <seconds> ago.*

**Card badge delayed:** If a user badges their card, this information is sent from the Controller to the Middleware Framework. The time between the information being sent is checked by the Middleware Framework. If this time does not exceed the Card Badge Expiration Time but is still longer than 10 seconds, the terminal is enabled and the following event is logged:

Summary: *Card badge delayed for <Cardholder> at <ESI> (terminal name).*

Details: *The card was badged <seconds> ago.*

---

**Wrong acknowledgement:**

If a user badges their card, this information is sent from the Middleware Framework to the Schindler system. After the message has been sent to the Schindler system, the Middleware Framework waits for an acknowledgement. If a wrong acknowledgement is received the following event is logged:

Summary: *Wrong acknowledgement received from <ESI> (terminal name).*

**Wrong trigger:**

If a user badges their card and the trigger string for the terminal has been incorrectly configured, the terminal is not enabled and the following event is logged:

Summary: *Wrong Trigger received <ESI> (terminal name).*

Details: *Please configure the Trigger Events to [CN]\_[FC].*

**Trigger queue overflow:**

If a user badges their card and the queue has exceeded the badge overflow limit (100 badges), the following event is logged and the trigger queue will be emptied.

Summary: *Trigger queue overflow.*

The overflow limit of 100 cannot be changed.

---

## 8 Upgrading

---

### 8.1 Upgrading this feature from vEL8.10 (or earlier) to vEL8.50

1. Perform a backup of your Command Centre system.
2. Exit Command Centre and stop the Command Centre Services.
3. Upgrade Command Centre to vEL8.50.1677 (or later Command Centre release). Refer to the document "*3E0068 Release Note Command Centre vEL8.50.1677 (Upgrade Procedures).pdf*" located on the Command Centre installation media, for further detail.
4. Back up the 'SchindlerPlugin.config' file located in the following: C:\Program Files (x86)\Gallagher\FTCAPI\Middleware Framework\Plugin
5. Using the Windows **Programs and Features** utility, remove the following programs from the middleware PC:
  - Gallagher FTCAPI Middleware Framework
  - Gallagher Schindler Live Reporting Plug-in
  - Gallagher Schindler Call Interface Plug-in
6. Unzip the new files you have been provided and run the installation executables **FMFSetup\_8.xx.xx**, **SchindlerCallInterfacePlugin\_v8.50.xx**, and **SchindlerLiveReportingPlugin\_v8.50.xx** on the middleware PC.
7. Navigate to: C:\Program Files (x86)\Gallagher\FTCAPI\Middleware Framework\Plugin
8. Replace the new **SchindlerPlugin.config** with the backup file.
9. Restart the Command Centre Services and Command Centre.
10. Upgrade the Controllers to vCR8.50.210623c (or later vCR8.50 release). Refer to the document "*3E2203 Release Note Controller 6000 vCR8.50.210623c.pdf*" located on the Command Centre installation media.
11. Test to ensure this feature operates as before.

### 8.2 Upgrading this feature on vEL8.50

1. Back up the 'SchindlerPlugin.config' file located in the following: C:\Program Files (x86)\Gallagher\FTCAPI\Middleware Framework\Plugin
2. Using the Windows **Programs and Features** utility, remove the following programs from the middleware PC:
  - Gallagher FTCAPI Middleware Framework
  - Gallagher Schindler Live Reporting Plug-in
  - Gallagher Schindler Call Interface Plug-in
3. Unzip the new files you have been provided and run the installation executables **FMFSetup\_8.xx.xx**, **SchindlerCallInterfacePlugin\_v8.50.xx**, and **SchindlerLiveReportingPlugin\_v8.50.xx** on the middleware PC.
4. Navigate to: C:\Program Files (x86)\Gallagher\FTCAPI\Middleware Framework\Plugin
5. Replace the new **SchindlerPlugin.config** with the backup file.
6. Test to ensure this feature operates as before.

---

## 9 Uninstallation

---

To permanently uninstall this feature, perform the following procedure:

1. Perform a backup of your Command Centre system.
2. Exit Command Centre and stop the Command Centre Services.
3. Using the Windows **Programs and Features** utility, remove the program 'Gallagher Schindler Call Interface Plug-in' and 'Gallagher Schindler Live Reporting Plug-in' from the Middleware PC.
4. Restart the Command Centre Services and Command Centre.

## 10 Limitations

---

- The 'Code only' access mode is not supported in this feature.
- Command Centre logs access events as 'Unknown Cardholder' after a credential is presented at a turnstile terminal. This is because the Live Reporting Interface does not support this functionality.
- When Command Centre logs an access denied event, the name of the Cardholder is not included, instead it is logged as 'Unknown Cardholder'. This is because the Schindler system does not support this functionality.

## 11 Consideration

---

If the Command Centre Server disconnects the FTCAPI Middleware Framework (FMF), Cardholders attempting to access the elevators for the first time will be denied access. Once the Command Centre Server re-connects to the FMF, those Cardholders will be granted access.

## 12 Troubleshooting

---

Errors are either reported in Command Centre, or they will be logged in the following directory: `C:\Program Files (x86)\Gallagher\FTCAPI\Middleware Framework\Log\FMF.log`

---

## 13 Known Issues

---

- **Cardholder access not updated due to cache**

The Call Interface and the Live Reporting plug-ins store Cardholder details in the **SchindlerProfileData** and **SchindlerTempMap** files (cached files). These cached files speed up query times and allow the Schindler system to function while Command Centre is offline (i.e. the Schindler system continues to grant and deny access). When updating the cached data, the plug-ins monitor changes made directly to a Cardholder but not to an Access Group.

### Example

A site uses two Access Groups. One is used to manage the Schindler profile PDF, and the other is used to manage the Access Zones.

An operator opens the properties of the Access Group that has the Schindler Profile PDF and removes a Cardholder from the list to revoke access. Because the plug-ins do not monitor Access Group events, this change is not synced and the cached data are now incorrect.

Therefore, because the Cardholder still has access to the zone, and the cached files are not updated correctly, the Cardholder may gain access to the elevators.

### Workaround

#### Option 1

If you are using two Access Groups to manage the Schindler Profile PDF and the Access Zones as described in the example above. Then, use the Access Group that has Access Zones configured to manage a Cardholder's access.

**IMPORTANT:** It is assumed that if a Cardholder is not part of the Access Zone Access Group, or the Cardholder membership 'until time' has expired, the Cardholder will not be able to gain access to the zone and use the cached data to access.

#### Option 2

Use only one Access Group to manage the Schindler Profile PDF and the Access Zones. Configure this Access Group with the Schindler profile PDF and the required Access Zones.

**IMPORTANT:** If a Cardholder is not part of this Access Group, or the Cardholder membership 'until time' has expired, Command Centre will not allow the Cardholder into the zone.

#### Option 3

After any relevant Access Group changes:

1. Stop the FTCAPI Middleware Framework services.
2. Navigate to: C:\ProgramData\Gallagher\FMF\Schindler
3. Delete the **SchindlerProfileData** and **SchindlerTempMap** files.
4. Restart the FTCAPI Middleware Framework.

- **'Unknown Cardholder' access events**

If a Cardholder badges a Mobile Credential at a Terminal (External System Item) that is missing the Badge Type ([BT]) from its trigger string (on its 'Trigger -- Events' tab), the credential details are cached incorrectly. Access events will show 'Unknown Cardholder'. To fix this:

1. Configure the External System Item's 'Trigger -- Events' tab correctly, as per section 5.2 "[External System Items \(Terminals\)](#)".
2. On the Middleware PC, navigate to C:\ProgramData\Gallagher\FMF\Schindler and delete the files named **SchindlerProfileData** and **SchindlerTempMap**.
3. Restart the FTCAPI Router Service.

---

- **'Unknown' External System Item status due to Time Patterns**

When Time Patterns are configured, the ESI status will be displayed as 'unknown'. After removing the configured Time Patterns, the ESI status will be displayed correctly.

- **Floor state change events not being raised**

If a floor in the Schindler system is configured with only a free time pattern, Command Centre will not raise confirmation events to confirm its floor state changes (i.e. after you send a floor state change from Command Centre to Schindler). For floor state change confirmation events to be raised, there must be at least one free and one secure time pattern configured against the floor in the Schindler system.