Gallagher Command Centre

Schindler ID Feature

Release Note

Copyright © Gallagher Group Limited

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 2026. 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 4
- 1.1 Purpose 4
- 1.2 Compatibility 5
- 1.3 Licensing 6
- 1.4 Deployment architecture 6

2 The Schindler Cardholder Management Interface 7
- 2.1 Configuring a Schindler Access Zone Schedule 8
- 2.2 Configuring a Schindler Cardholder Access Schedule 8
- 2.3 Configuring a Schindler Access Zone 8
- 2.4 Configuring Schindler Personal Data Fields 9
- 2.5 Configuring a Schindler Access Group 10
- 2.6 Configuring Schindler Cardholders 11
- 2.7 Configuring a Schindler Card Type 18
- 2.8 Configuring a SchindlerID System 20
- 2.9 Synchronising databases 25

3 The Live Reporting Interface (plugin) 26
- 3.1 Installing the Live Reporting Interface 26
- 3.2 Configuring an External System Server 27
- 3.3 Configuring a Live Reporting External System 27
- 3.4 Configuring External System Items (floors) 29

4 The Call Manager Interface (plugin) 31
- 4.1 Installing the Call Manager Interface 31
- 4.2 Configuring an External System Server 32
- 4.3 Configuring a Call Manager External System 32
- 4.4 Configuring External System Items (terminals) 34
- 4.5 Configuring a Schindler Alarm Zone 36
- 4.6 Configuring Schindler Action Plans 37
- 4.7 Configuring Gallagher Readers 38
- 4.8 Configuring Schindler Dummy Doors 38
- 4.9 Configuring Secure/Free Floors 41
- 4.10 Events/Alarms 50

5 Events and Alarms 52
- 5.1 Cardholder Management (Third Party Interface) Events and Alarms 52
- 5.2 Live Reporting (Event Logging) Events and Alarms 53
- 5.3 Call Interface (Command Centre Lift Readers) Events and Alarms 54

6 Considerations 55

7 Uninstallation 56

Copyright © Gallagher Group Limited

1 Introduction

About this release note

This release note is for the 'Schindler ID' feature of Gallagher Command Centre.

1.1 Purpose

What this feature does

The SchindlerID System integrates Command Centre and the SchindlerID individualization and access control system v1.3.369.1

This integration is comprised of three parts:

Part	Description
The Schindler Cardholder Management Interface	• Synchronises the Schindler user database with the Command Centre Cardholder database. • Allows one access card to be used for building doors and the lift system. • Can convert Badge Numbers from decimal to hexadecimal format. • Allows Cardholder cards to be automatically formatted as hexadecimal Badge Numbers according to their Card Type specification. • Assigns a Cardholder's MIFARE Card Serial Number (MIFARE CSN) to the Badge Number field of the corresponding Schindler user. • Reports on access events at a turnstile/ barrier.
The Live Reporting Interface (plugin)	• Builds an audit trail of Schindler access events in Command Centre. • Enables Command Centre to receive non-badge card events from Schindler.
The Call Interface (plugin)	• Enables a Gallagher reader to be used at a Schindler terminal to identify the Cardholder to the Schindler system. • Enables Command Centre to set the status of a floor to 'Secure' or 'Free' via a schedule or operator override.

Copyright © Gallagher Group Limited

Alternative feature	As an alternative to the Gallagher Schindler ID (Cardholder Management Interface) feature, Gallagher provides a 'Schindler Call by Profile' feature. Call by Profile 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. Unlike the Schindler ID feature, Command Centre does not send any Cardholder details to the Schindler system. Schindler makes the access decision based on the Profile name only. Command Centre is able to build an audit trail of Schindler access events. Note that you should only use *one* of the Gallagher Schindler features (Schindler ID or Call by Profile), not both. For more information about the Schindler Call by Profile feature, refer to the document *"Release Note Schindler Call by Profile (vx.xx).pdf"* stored on the Command Centre installation media under *Utilities**System Interfaces**Schindler*.

1.2 Compatibility

SchindlerID Call Interface protocol	This integration is compatible with the SchindlerID Call Interface protocol as specified in the document J 41900402.
Components	The following components are compatible with the Schindler interface: • Third-Party Database Online Interface J41900401:153324 (11-09-01) • Call Interface to External Security Systems J41900402: 153324 (11-09-01) • Third Party Life Reporting Interface v2.8: (12-03-26) • Schindler ID v1.3.369.1
Card number support	Card numbers greater than 16,777,215 are *not* supported.
Multi-Server support	The following Command Centre multi-server functionality has been tested: • All Gallagher-Schindler communications (including Cardholder Sync and Live Reporting) occur from server 1. • Live Reporting events are replicated to server 2. • Cardholders can be created on either server (assuming Card Types exist on server 1) and are replicated. • Floor overrides can occur from both servers.

Copyright © Gallagher Group Limited

1.3 Licensing

Required licenses

The following licence entries are required:

```
[Limits]
SchindlerID Systems=n
```

Where *n* is the maximum number of SchindlerID Systems that can be created. Once the maximum number has been reached, the option to create additional SchindlerID Systems will be disabled.

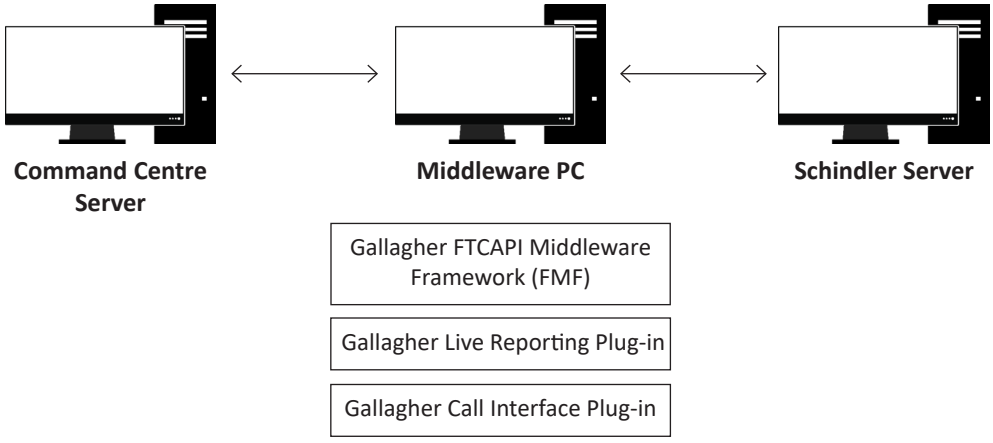
If using SchindlerID plugins, the following licence entries are also required:

```
[Plugin]
PluginX=SchindlerID-LifeReporting
PluginX=SchindlerID-CallInterface
```

1.4 Deployment architecture

Example

The Schindler ID feature can be deployed as shown below:



Copyright © Gallagher Group Limited

2 The Schindler Cardholder Management Interface

Syncing Cardholders to Schindler

The Cardholder Management Interface enables the Command Centre Cardholder database to be synchronised to the Schindler user database.

If a change is made in the Command Centre Cardholder database, the Schindler user database will be updated to match. If a user has been manually added to the Schindler user database and *not* the Command Centre Cardholder database, the user will *not* be removed when an update occurs.

Command Centre should be used to add, change and delete all Cardholders.

Schindler Personal Numbers

When syncing Card Types, a Command Centre Cardholder's Card Number and Facility Code are encoded into the Schindler Personal Number; when syncing Mobile Credentials, a Command Centre Cardholder's Mobile Credential ID (number) followed by '_MOBILE' is encoded into the Schindler Personal Number. This Personal Number is what identifies a user in the Schindler user database. The user is then granted lift access depending on their allowed access profile configured within Schindler.

Therefore, Cardholders *must* be assigned at least one card or Mobile Credential in Command Centre in order to be synchronised to the Schindler user database.

In this section

To configure the Schindler Cardholder Management Interface, perform the following procedures:

2.1 Configuring a Schindler Access Zone Schedule
2.2 Configuring a Schindler Cardholder Access Schedule
2.3 Configuring a Schindler Access Zone
2.4 Configuring Schindler Personal Data Fields
2.5 Configuring a Schindler Access Group
2.6 Configuring Schindler Cardholders
2.7 Configuring a Schindler Card Type
2.8 Configuring a SchindlerID System
2.9 Synchronising databases

Copyright © Gallagher Group Limited

2.1 Configuring a Schindler Access Zone Schedule

Refer to Help topic

Create an Access Zone Schedule. Refer to the topic *"Creating a new Schedule"* in the Gallagher Configuration Client Help.

- Name the Schedule 'Schindler Access Zone Schedule'.
- Set the State/Action to **Secure - No PIN** at all times.

This Schedule will be assigned to the 'Schindler Access Zone'.

2.2 Configuring a Schindler Cardholder Access Schedule

Refer to Help topic

Create a Cardholder Access Schedule. Refer to the topic *"Creating a new Schedule"* in the Gallagher Configuration Client Help.

- Name the Schedule 'Schindler Cardholder Access Schedule'.
- Set the State to **Grant Access** at all times.

This Schedule will be assigned to the 'Schindler Access Group'.

2.3 Configuring a Schindler Access Zone

Refer to Help topic

Create an Access Zone. Refer to the topic *"Adding a new Access Zone"* in the Gallagher Configuration Client Help.

- Name the Access Zone 'Schindler Access Zone'.
- Assign the 'Schindler Access Zone Schedule' to this zone.

Copyright © Gallagher Group Limited

2.4 Configuring Schindler Personal Data Fields

Refer to Help topic

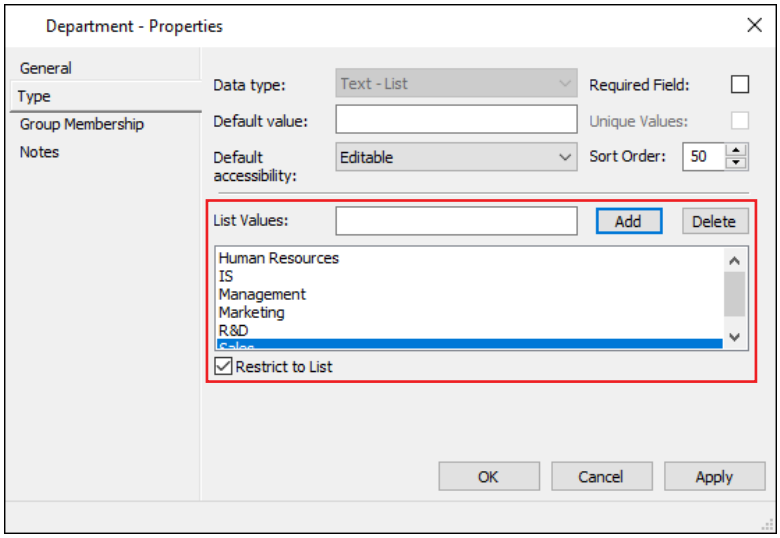
Create a Personal Data Field (PDF) for each Schindler field listed below. Set each PDF's 'Name' to the 'Schindler field' name specified below, and set the PDF's 'Data type' to the 'Data type' specified below.

Schindler field	Data type
User Template	Text - List
Master Group	Text - List
Department	Text - List
Badge Number 1	Text (only required if Direct PDF option is used)
Badge Number 2	Text (only required if Direct PDF option is used)
Badge Number 3	Text (only required if Direct PDF option is used)

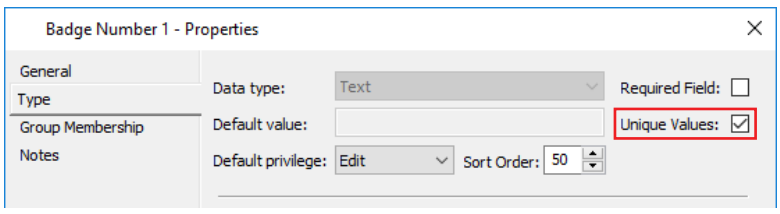
Refer to the topic *"Creating a new Personal Data Field"* in the Gallagher Configuration Client Help.

Notes

- The PDF 'Name' is arbitrary, but the 'Data type' must match the Schindler field for which the PDF is created.
- Configure the 'Text - List' data type PDFs with each of the available options in Schindler. For example:



- Ensure the Badge Number 1, Badge Number 2, and Badge Number 3 PDFs are configured as 'Unique Values', as shown below:



Copyright © Gallagher Group Limited

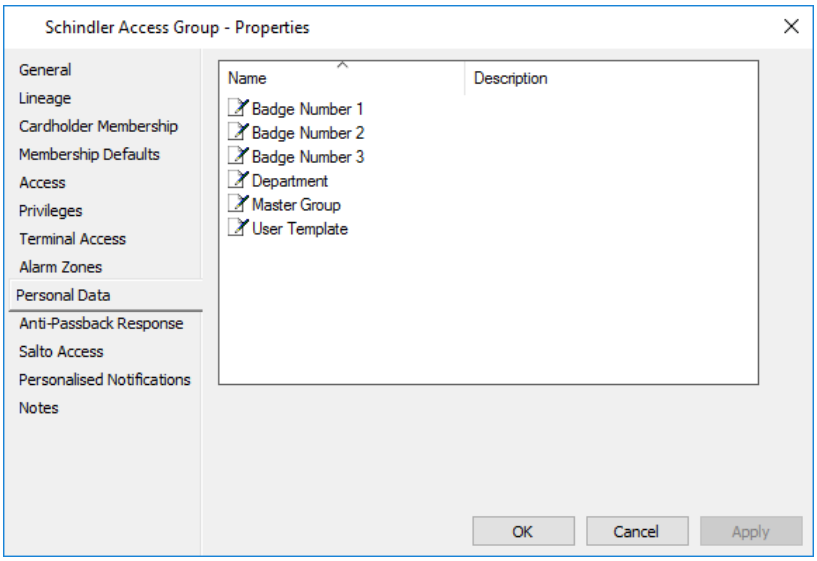
2.5 Configuring a Schindler Access Group

Refer to Help topic

Create a Schindler Access Group. Refer to the topic Setting up Access Groups. Name the Access Group 'Schindler Access Group'.

Assign to this Access Group:

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



Notes

- If a Cardholder is removed from the Schindler Access Group (thus the Cardholder no longer has the Schindler PDFs assigned), then an update will occur and the Cardholder will be removed from the Schindler user database.
- The Cardholder's last name must not be left empty, as this is a mandatory field in Schindler. If the Cardholder's last name is empty, the corresponding Schindler user will be deleted.
- If a Cardholder is removed from an Access Group that does not have the Schindler PDFs assigned, then an update will not occur.
- If a Cardholder has been assigned to a Temporary Access Group that has the Schindler PDFs assigned, then the Cardholder will be removed from the Schindler user database, once the temporary access has expired.

Copyright © Gallagher Group Limited

2.6 Configuring Schindler Cardholders

About this section

Before Cardholders can be mapped from Gallagher Command Centre to Schindler, you must do the following in Command Centre:

- Create the Cardholders that require access to Schindler readers, terminals, and lifts.
- Configure the Schindler Personal Data Field (PDF) *values* for each Cardholder.
- Assign each Cardholder at least one card; Cardholders without a card are not synchronised.

In this section

To map the Schindler Personal Data Field values, perform the following procedures:

2.6.1 Mapping the Schindler User Template
2.6.2 Mapping the Schindler Master Group
2.6.3 Mapping Schindler Badge Numbers

Cardholder requirements

To be imported into Schindler, each Cardholder in Command Centre *must*:

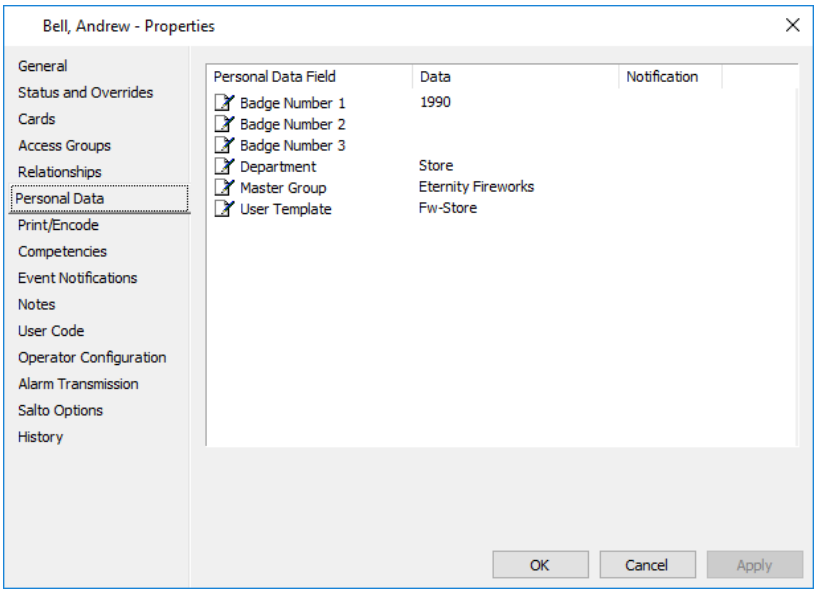
- Have a Last Name, as this is a mandatory field in Schindler. If a Cardholder's last name is empty, the corresponding Schindler user will be deleted.
- Be in an Access Group with the Schindler 'User Template' and 'Master Group' PDFs, and have a value assigned for these PDFs. Otherwise, the Cardholder is not imported into the Schindler user database.
- Have at least one card assigned. Otherwise, the Cardholder is not imported into the Schindler user database.

Notes

- If a Cardholder has the Schindler 'User Template' and 'Master Group' PDFs assigned and has two or more cards assigned, then the Cardholder is imported as two or more users into the Schindler user database (one user record per card).
- If a Cardholder has the Schindler 'User Template', 'Master Group', *and* 'Badge Number' PDFs assigned and two cards assigned, then only one user will be imported into the Schindler user database. This user will have the badge numbers assigned. Secondary users for the Cardholder cannot be imported because the unique badge numbers are already assigned to the first user.
- If a Cardholder does not have the 'Badge Number' PDFs assigned or has them assigned with blank values, when an update occurs, any Badge Numbers already configured for this user in the Schindler user database will be removed. To avoid this, assign the 'Badge Number' PDFs to the Cardholder and simply type "ignore" as the value for the first badge number and leave the other two badge numbers empty.

Copyright © Gallagher Group Limited

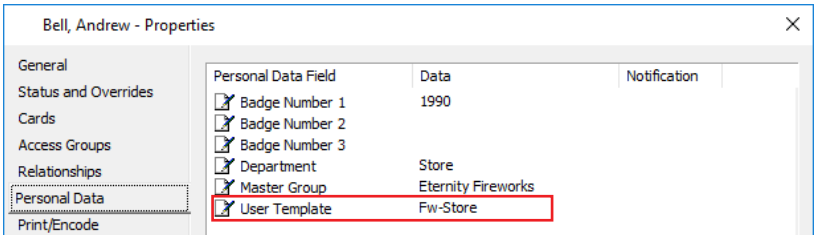
Example of Cardholder's PDFs



2.6.1 Mapping the Schindler User Template

Assign User Template PDF values

Each Cardholder's 'User Template' PDF value must match exactly their User Template in Schindler. User Templates are used, among other things to configure the access rights. A User Template is applied when the user is transferred to Schindler.



The access rights can be configured in two different ways in Schindler. Either you can configure it directly on the User Template tab, or you configure an Access Profile and assign it to the User Template. Access Profiles are configured on another button located near the User Templates button.

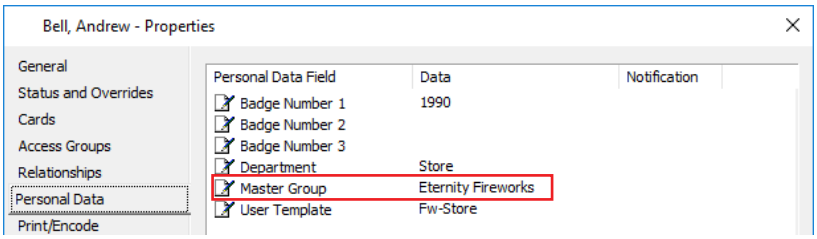
Copyright © Gallagher Group Limited

2.6.2 Mapping the Schindler Master Group

Assign Master Group PDF values

Each Cardholder's 'Master Group' PDF value must match exactly their Master Group in Schindler.

The Master Group in Schindler typically refers to the "master" company whose operator manages the company's employees in Schindler.



Copyright © Gallagher Group Limited

2.6.3 Mapping Schindler Badge Numbers

About Badge Numbers

Schindler allows three Badge Numbers (card credentials) to be populated for each user. This means a Command Centre Cardholder with more than three credentials (e.g. cards) must have the three chosen that will be mapped to the Schindler system.

The Badge Numbers are used by Schindler for matching card data that is read by Schindler-controlled readers. The basic format of a Badge Number is a hexadecimal number string. Its length and interpretation are dependent on Schindler configuration.

Assign Badge Number PDF values

A 'Badge Number' PDF can have a value assigned in one of the following ways:

- A Cardholder's MIFARE Card Serial Number (MIFARE CSN) is *automatically* formatted as a hexadecimal number string upon updating. This option corresponds to the '**MIFARE CSN**' Badge Number Preference, selectable on the SchindlerID External System item.
- A Cardholder's card can be *automatically* formatted as a hexadecimal number string. This option corresponds to the '**Card Type Specified**' Badge Number Preference, selectable on the SchindlerID External System item.

  Card formats 'Wiegand 26/8 bit', 'Wiegand 35/12 bit (HID Corporate 1000)', and 'Wiegand 37/16 bit (HID H10304)' are supported. Multiple Card Types (thus multiple Facility Codes) can be used.
- A Command Centre operator can *manually* enter a *decimal* number as a value of a Text data type Personal Data Field (PDF) for a Cardholder. This value is automatically converted to a hexadecimal string upon updating. This option requires some Windows hexadecimal conversion registry values to be set up on the Command Centre server. This option corresponds to the '**Direct PDF**' Badge Number Preference selectable on the SchindlerID External System item.
- A Command Centre operator can *manually* enter a *hexadecimal* number string as a value of a Text data type Personal Data Field (PDF) for a Cardholder. This option corresponds to the '**Direct PDF**' Badge Number Preference, selectable on the SchindlerID External System item.

Copyright © Gallagher Group Limited

About Badge Number conversion

Badge Number conversion is only required if you will use the 'Direct PDF' option for the Badge Number Preference, *and* operators will enter *decimal* (not hexadecimal) numbers as Cardholder's Badge Number PDF values. If this is not the case, skip this procedure.

When using 'Direct PDF', each Cardholder's Badge Number PDF values are imported into Schindler as the Schindler Badge Number. By configuring the registry values, badge numbers can be converted from decimal format to hexadecimal format when imported into Schindler.

Required registry values

In order to perform the conversion, you must create the following registry values and define the appropriate values for each:

Registry value name	Type	Value	Meaning
BadgeNumberConvert	REG_DWORD	1	The conversion is performed and the BadgeNumberConstant is added to the *front* of the converted Badge Number PDF value.
		2	The conversion is performed and the BadgeNumberConstant is added to the *end* of the converted Badge Number PDF value.
		0/other/ none	The conversion is *not* performed.
BadgeNumberLength	REG_DWORD	Set this to the length of the whole Badge Number once converted. The length cannot be more than the sum of 'HI' and 'LO' number of digits configured in Schindler, as configured in Schindler under **Network**, **Elevators**, **Tools** > **3rd party database interface**.	
BadgeNumberConstant	REG_SZ	Set this to a constant in hexadecimal notation that is added to the front or end of every converted Badge Number.	

Create a registry entry

To create the registry entries, perform the following procedure. The registry entries must be created on *each* Command Centre workstation. If a registry value is changed, ensure all other workstation registry values are updated the same.

Step	Action	Description
1	**Open 'Run'**	From the Start menu, open the Windows **Run** program.
2	**Enter 'regedit'**	Type in 'regedit' and click **OK**. The Registry Editor opens.

Continued on next page

Copyright © Gallagher Group Limited

3	**Navigate to Key**	If using a 64 bit system, path your way to: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ GALLAGHER\Command Centre If using a 32 bit system, path your way to: HKEY_LOCAL_MACHINE\SOFTWARE\GALLAGHER\Command Centre
4	**New DWORD Value**	Right-click, then select **New** > **DWORD Value**. Your new DWORD Value is populated at the bottom of the registry values list.
5	**Name the value**	Enter the DWORD Value name, (e.g. BadgeNumberConvert).
6	**Double-click the value**	Double-click your newly created DWORD Value. The 'Edit DWORD Value' window displays.
7	**Select 'Decimal', enter value**	Select **Decimal** as the Base, then enter your new value, (e.g. 1) and click **OK**.
8	**Repeat**	Repeat this procedure to create the other registry values as specified earlier in this section. **Note:** The BadgeNumberConstant value is created via **New** > **String Value**.

Check conversion requirements

To perform successful Badge Number conversions, check the following is done:

- All three registry entries mentioned are present.
- The 'BadgeNumberConvert' value is 1 or 2.
- The Badge Number PDF value is a decimal number (0 - 4294967294).
- The length of a converted value plus the length of the 'BadgeNumberConstant' is less than or equal to the 'BadgeNumberLength'.

Notes

- When a number is converted into hexadecimal notation, leading zeros are added to the converted value so its length equals the 'BadgeNumberLength'.
- Badge Numbers that are successfully imported into Schindler can be found in Schindler under **Users/Building** > **Users** (select a user) > **Assigned ID media**.
- If the conversion is *not* successful, the card number is imported as is.

Copyright © Gallagher Group Limited

Conversion examples

The following table includes examples of how Badge Numbers are converted:

Registry Entries			Badge Number PDF Value	Badge Number sent to SID	Comment
BadgeNumberConvert	BadgeNumberLength	BadgeNumberConstant			
-blank-	*-blank-*	*-blank-*	4568	4568	No registry entry; no conversion.
1	16	01000000ABC1	1990	01000000ABC107C6	1990(dec)=7C6(hex) 0 - leading '0' added (to get length of 16) Convert=1; Constant was prepended
2	16	01000000ABC1	1990	07C601000000ABC1	1990(dec)=7C6(hex) 0 - leading '0' added (to get length of 16) Convert=2; Constant was appended
1	16	01000000ABC1	0B000000AAFF07C6	0B000000AAFF07C6	No conversion required.
1	16	01000000ABC1	-12	-12	Conversion failed; import as is.
1	16	01000000ABC1	1990 hello	1990 hello	Conversion failed; import as is.
1	14	01000000ABC1	1990	1990	Conversion failed because value would be more than 14 characters; import as is.

Copyright © Gallagher Group Limited

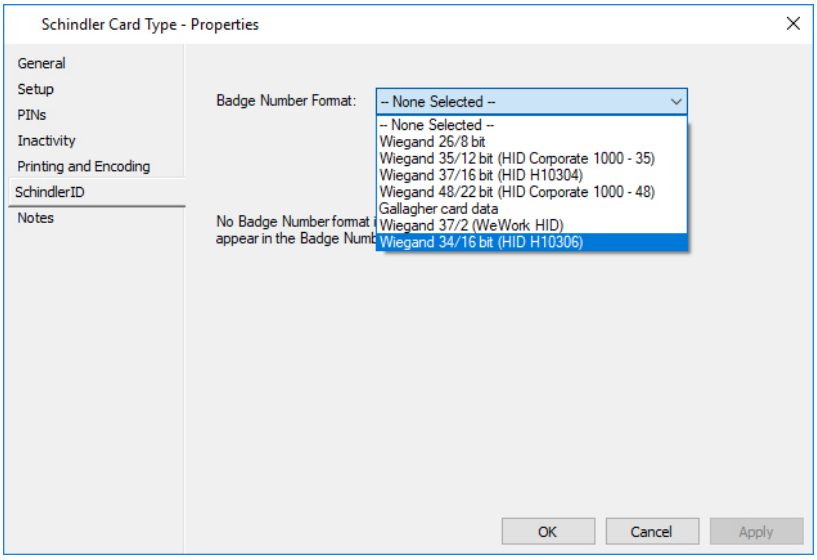
2.7 Configuring a Schindler Card Type

About this section

Note: This topic is only applicable for Card Types, not Mobile Credentials. Mobile Credential types do not have a 'SchindlerID' tab.

If you are using a Cardholder's card to populate a Schindler **Badge Number**, you must:

- select 'Card Type Specified' as the corresponding Badge Number Preference on the SchindlerID System item, and
- specify the expected **Badge Number Format**, (e.g. Wiegand 26/8 bit) for the Card Type of the Cardholder's card.



Refer to the table below about the available Badge Number Formats.

Badge Number Formats

The following table describes each Badge Number Format, which can be selected on a Card Type's 'SchindlerID' tab:

Option	Description
-- None Selected --	This is the default. Combined with the 'Card Type Specified' **Badge Number Preference** option (mentioned later) indicates that there will be no conversion/population for the cards of this Card Type.
Wiegand 26/8 bit	Specifies a Wiegand 26/8 bit card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]

Continued on next page

Copyright © Gallagher Group Limited

Wiegand 35/12 bit (HID Corporate 1000 - 35)	Specifies a Wiegand 35/12 bit (HID Corporate 1000) card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Wiegand 37/16 bit (HID H10304)	Specifies a Wiegand 37/16 bit (HID H10304) card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Wiegand 48/22 bit (HID Corporate 1000 - 48)	Specifies a Wiegand 48/22 bit (HIS Corporate 1000-48) card format, including 22 bits of Facility Code, 23 bits of Card Number and 3 parity bits. Applicable cards are formatted accordingly and populated in the Badge Number field in the update message. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Gallagher card data	Specifies a 64-bit Gallagher encoded data. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - MIFARE DESFire [23] **Note:** The Schindler terminals need to have SAM cards deployed that have been provisioned to read Gallagher-encoded data. For more information, contact your local Gallagher representatives.
Wiegand 37/2 bit (WeWork HID)	Specifies a Wiegand 37/2 bit card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Wiegand 34/16 bit (HID H10306)	Specifies a Wiegand 34/16 bit (HID H10306) card format, including 16 bits of Facility Code, 16 bits of Card Number and 2 parity bits. Applicable cards are formatted accordingly and populated in the Badge Number field in the update message. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]

Copyright © Gallagher Group Limited

2.8 Configuring a SchindlerID System

About this section

This section describes how to create a SchindlerID System item in Gallagher Configuration Client. The SchindlerID System interfaces with the Schindler Third Party Database Interface.

Notes:

- Operators require the 'Edit Site' Operator Privilege to add, modify, and delete SchindlerID System items.
- The total number of SchindlerID Systems you can create is determined by your licence file.

Before you begin

Before performing this procedure, request Schindler integrators to create a Schindler Third Party Database, and provide the following database information:

- The Schindler server name or IP Address of the computer used to create the Schindler Third Party Database.
- The TCP/IP Port Number of the Schindler Third Party Database.

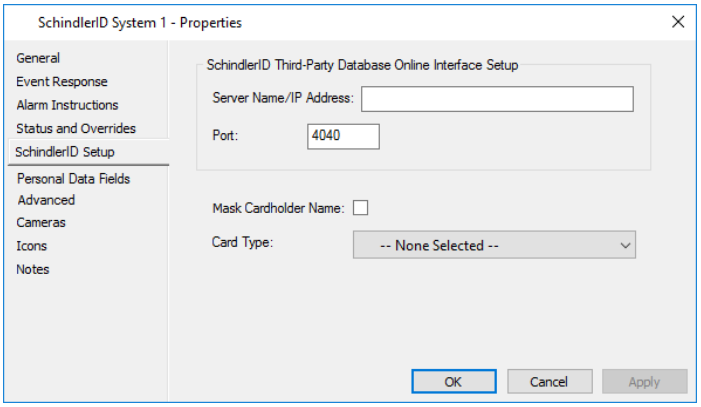
Procedure

To create the SchindlerID System item, perform the following procedure:

Step	Action	Description
1	**Open the External Systems list window**	Click **Configure** from the Configuration Client menu bar, then **External Systems**. The External Systems list window opens.
2	**New SchindlerID System**	Right-click and select **New...** > **SchindlerID System**. The **General** tab displays.
3	**General fields**	Complete the General tab fields as required.
4	**Event Response tab**	Click the **Event Response** tab, and configure as required.
5	**Alarm Instructions tab**	Click the **Alarm Instructions** tab, and configure as required.

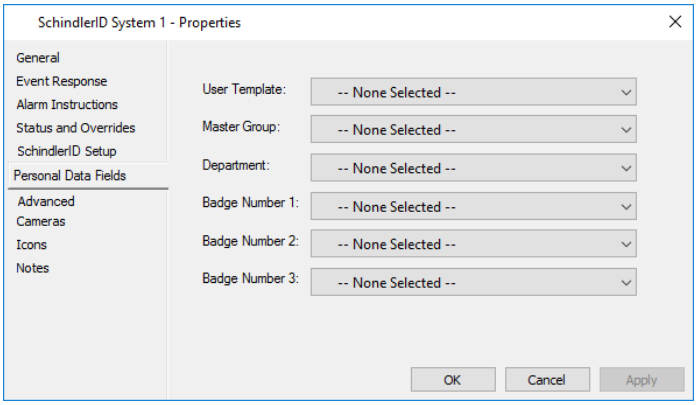
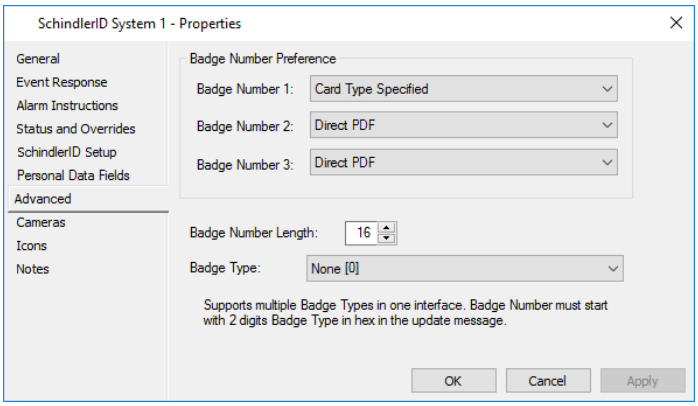
Continued on next page

Copyright © Gallagher Group Limited

6	**Click the SchindlerID Setup tab**	
7	**Server PC Name/IP Address**	Enter the Schindler server PC's IP Address in the **Server PC Name/IP Address** field. This field is limited to 255 alpha-numeric characters.
8	**Port**	Enter the TCP/IP Port Number of the Schindler Third Party Database Interface in the **Port** field. This value is located in the Schindler Third Party Database Interface. Valid range 1 – 65535.
9	**Mask Cardholder Name**	Select the **Mask Cardholder Name** check box to hide Cardholders' names within this Schindler system (to ensure Cardholder privacy). Since Cardholders require a first and last name in the Schindler system, selecting this check box replaces each Cardholders' both first and last names with their card number and facility code, in the format [card number]_[facility code]. This check box does not hide or change any Cardholder names within Command Centre. If you select this check box, all existing Cardholder names in the Schindler system are also masked. Likewise, if you deselect this check box, all existing Cardholder entries in the Schindler system are updated with their real names.
10	**Card Type**	If required, select a Card Type or Mobile Credential from the **Card Type** drop-down list. If selected, only Cardholders configured with this Card Type or Mobile Credential will be imported into the Schindler user database. If left as '-- None Selected --', all Cardholders that have *any* Card Type card or Mobile Credential will be imported into the Schindler user database.

Continued on next page

Copyright © Gallagher Group Limited

11	**Click the Personal Data Fields tab**	
12	**User Template**	Select the PDF that you created for the Schindler **User Template** field.
13	**Master Group**	Select the PDF that you created for the Schindler **Master Group** field.
14	**Department**	Select the PDF that you created for the Schindler **Department** field (optional).
15	**Badge Numbers**	Select the PDF that you created for each of the Schindler **Badge Number** fields (optional). **Note:** If using Schindler readers, the Badge Number PDFs are required.
16	**Click the Advanced tab**	**Note:** If you selected a Mobile Credential type for the Card Type on the **SchindlerID Setup** tab, the **Advanced** tab is not applicable. Only configure the **Advanced** tab if you selected a 'Card Type' type. 

Continued on next page

Copyright © Gallagher Group Limited

<table>
<tr>
<td>17</td>
<td>Badge Number Preference</td>
<td>Select the appropriate Badge Number Preference for each Badge Number.

Badge Number options are:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Direct PDF</td><td>This option uses the value of the Badge Number PDF (selected on the 'Personal Data Fields' tab) as the Badge Number in Schindler.</td></tr>
<tr><td>MIFARE CSN</td><td>This option uses the Cardholder's MIFARE CSN as the Badge Number field in Schindler. This option is allowed for one Badge Number field only. This option supports 4-byte and 7-byte CSN only.

Cardholder cards may need to be (re) captured in Command Centre in order to store each card's CSN in the Command Centre database. A Cardholder's CSN can be captured by presenting the card to a USB MIFARE Encoder in a Cards tile in the Command Centre Client, or in Configuration Client > Monitor > Read MIFARE Card.

Important: If a Badge Type of -- None Selected -- has been configured in the SchindlerID System item, it assumes that the Badge Type MIFARE [1] is configured in Schindler. Otherwise, the Badge Type in the SchindlerID System item must be set to the same Badge Type that is configured in Schindler.

Command Centre constructs the hexadecimal string using the card's MIFARE CSN and prepends the string with the leading zeros to extend the string length to the configured Badge Number Length.

For example: 000000000A436AC1 (16 hexadecimal digits).</td></tr>
<tr><td>Card Type Specified</td><td>If this option is selected, the Badge Number hexadecimal number string is constructed according to the specification of the Badge Number Format configured for the relevant Schindler Card Type. This option is allowed for one Badge Number field only.</td></tr>
</table>
Note: After a 'Badge Number Preference' is changed on a SchindlerID System item, an automatic resync of the item is performed in order to update each Cardholder's relevant Badge Number field.</td>
</tr>
</table>

Continued on next page

Copyright © Gallagher Group Limited

<table>
<tr><td>18</td><td>Badge Number Length</td><td>To specify the Badge Number Length, enter the required length in the Badge Number Length field. Zeros will be prepended to the hexadecimal string to extend the string length to this number of characters. Default = 16.</td></tr>
<tr><td>19</td><td>Badge Type</td><td>If you selected the 'Card Type Specified' option for any of the 'Badge Number Preference' fields, select the required Schindler Badge Type from the Badge Type drop-down list.

Important: The Badge Type configured here must correspond to the Badge Type configured in Schindler.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-- None Selected --</td><td>This is the default and is backward compatible with the existing 'MIFARE CSN' Badge Number Preference option.

This option only supports 4-byte MIFARE CSN when the 'MIFARE CSN' Badge Number Preference has been selected.</td></tr>
<tr><td>None [0]</td><td>For supporting multiple Badge Types. Each Badge Number hexadecimal number string in the update message must explicitly specify a two-digit Badge Type at the start.

If 'MIFARE CSN' is selected as a Badge Number field, this option supports both 4-byte and 7-byte CSN.</td></tr>
<tr><td>MIFARE [1]</td><td>Only for 4-byte CSN.</td></tr>
<tr><td>InterISO14443A [21]</td><td>Only for 7-byte CSN.</td></tr>
<tr><td>Pure Wiegand [37]</td><td>For Wiegand formats with parity bits.</td></tr>
<tr><td>MIFARE DESFire [23]</td><td>Supports MIFARE® DESFire® card data including Gallagher encoded card data.</td></tr>
</table>
</td></tr>
<tr><td>20</td><td>Icons tab</td><td>Click the Icons tab if you want to change the Icon Set for this SchindlerID System.</td></tr>
<tr><td>21</td><td>Notes tab</td><td>Click the Notes tab if you want to add a note(s) about this SchindlerID System.</td></tr>
<tr><td>22</td><td>Click OK</td><td>Click OK to close and save your changes.</td></tr>
</table>

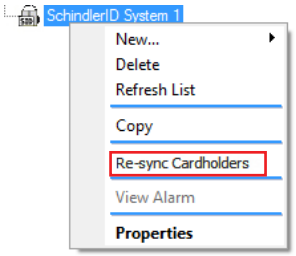
Copyright © Gallagher Group Limited

2.9 Synchronising databases

Re-Sync Cardholders

It may be necessary to perform a manual Cardholder re-sync occasionally.

To perform a manual re-sync, right-click the SchindlerID System in the External Systems list window (Configuration Client > **Configure** > **External Systems**), and select **Re-sync Cardholders**.



A re-sync then occurs and the Schindler user database is updated to match the Command Centre database.

Copyright © Gallagher Group Limited

3 The Live Reporting Interface (plugin)

About this section

The Live Reporting Interface builds an audit trail of Schindler access events in Command Centre, and enables Command Centre to receive non-badge card events from Schindler.

The Live Reporting Interface is an optional licensed plugin of Command Centre. This plugin must be installed on the middleware PC (PC hosting the FTCAPI Middleware Framework).

In this section

To configure the Live Reporting Interface, perform the following procedures:

3.1 Installing the Live Reporting Interface
3.2 Configuring an External System Server
3.3 Configuring a Live Reporting External System
3.4 Configuring External System Items (Floors)

3.1 Installing the Live Reporting Interface

Procedure

To install the Live Reporting Interface plugin, perform the following procedure:

Step	Action	Description
1	**Install FTCAPI Middleware Framework**	Install the FTCAPI Middleware Framework on the middleware PC (if not already installed). Refer to the topic *"Installing the FTCAPI Middleware Framework (FMF)"* in the Gallagher Configuration Client Help.

2	**Licence file**	Ensure your Command Centre licence file (CommandCentre.lic) contains the following entry:
		`[Plugin]`
		`PluginX=SchindlerID-LifeReporting`
		(where `X` is a number)

3	**Run installer file**	Run the installation executable **Gallagher Schindler Live Reporting Plugin-Setup x.xx.xx.msi** on the middleware PC. This file can be found with the Command Centre installation files in the folder: Utilities\System Interfaces\Schindler\SchindlerLiveReportingPlugin **Note:** The FTCAPI Router Service restarts as part of the install.
4	**Verify installation**	To ensure that the Live Reporting plugin has installed correctly, select the Windows **Programs and Features** utility from the Windows Control Panel. The program 'Gallagher Schindler Live Reporting Plug-in' should be listed.

Copyright © Gallagher Group Limited

3.2 Configuring an External System Server

Refer to Help topic Create an External System Server item. Refer to the topic "*Configuring an External System Server*" in the Gallagher Configuration Client Help.

3.3 Configuring a Live Reporting External System

About this section This section describes how to create an External System (Live Reporting Interface) that enables 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.

Note: Operators require the 'Edit Site' Operator Privilege to add, modify, and delete External Systems.

Before you begin Before performing this procedure:

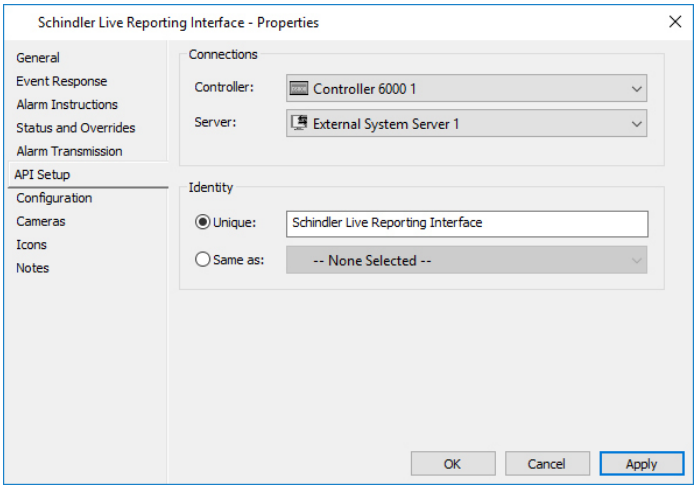
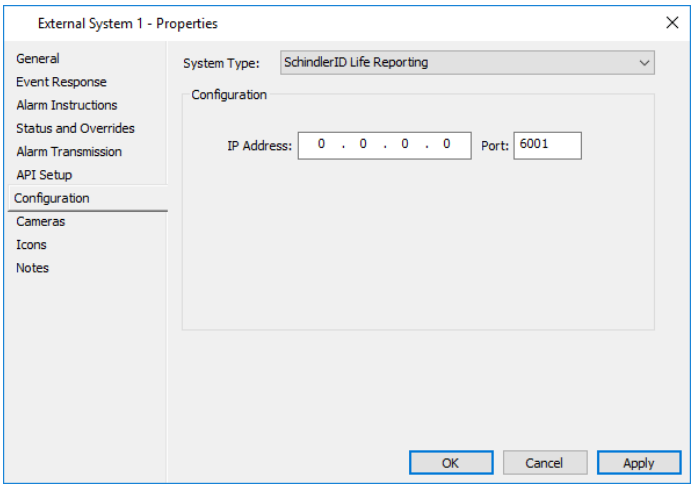
- Request Schindler integrators to create a Logging Task Interface in Schindler.
- Request the TCP/IP Port Number shown on the Logging Task Interface. This TCP/IP Port is required later in this procedure.

Procedure To configure the Live Reporting External System, perform the following procedure in Gallagher Configuration Client:

Step	Action	Description
1	**Open the External Systems list window**	Click **Configure** from the Configuration Client menu bar, then **External Systems**. The External Systems list window opens.
2	**New External System**	Right-click and select **New...** > **External System**. The **General** tab displays.
3	**General fields**	Complete the General tab fields as required.
4	**Event Response tab**	Click the **Event Response** tab, and configure as required.
5	**Alarm Instructions tab**	Click the **Alarm Instructions** tab, and configure as required.

Continued on next page

Copyright © Gallagher Group Limited

6	**Click the API Setup tab**	
7	**Controller**	Select the appropriate **Controller** from the drop-down list. **Note:** Only standard Gallagher Controllers will work, (i.e. Gallagher UltraSec Controllers will not work).
8	**Server**	Select the appropriate External System Server from the **Server** drop-down list.
9	**Unique Identity**	Click the **Unique** radio button in the 'Identity' section of this screen and type in a unique identity string. This field is limited to a maximum of 64 characters.
10	**Click the Configuration tab**	 **Note:** This tab only appears if 'Identity' on the API Setup tab is set to 'Unique'.
11	**System Type**	Select the 'SchindlerID Life Reporting' middleware plug-in from the **System Type** drop-down list. The 'Configuration' section of this tab displays the appropriate settings.
12	**IP Address**	Enter the Schindler server IP address in the **IP Address** field.

Continued on next page

Copyright © Gallagher Group Limited

13	**Port**	Enter the TCP/IP Port Number of the Schindler Logging Task Interface in the **Port** field. Range 0-65535. To enable Live reporting, ensure the 'Logging of Personal Data' is set to **Always** and the 'Live Reporting' **Active** check box is checked. **Note:** Schindler advises that storing the 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.
14	**Icons tab**	Click the **Icons** tab if you want to change the Icon Set for this External System.
15	**Notes tab**	Click the **Notes** tab if you want to add a note(s) about this External System.
16	**Click OK**	Click **OK** to close and save your changes.

3.4 Configuring External System Items (floors)

About this section

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 items (floors).

Note: Operators require the 'Edit Site' Operator Privilege to add, modify, and delete External System Items.

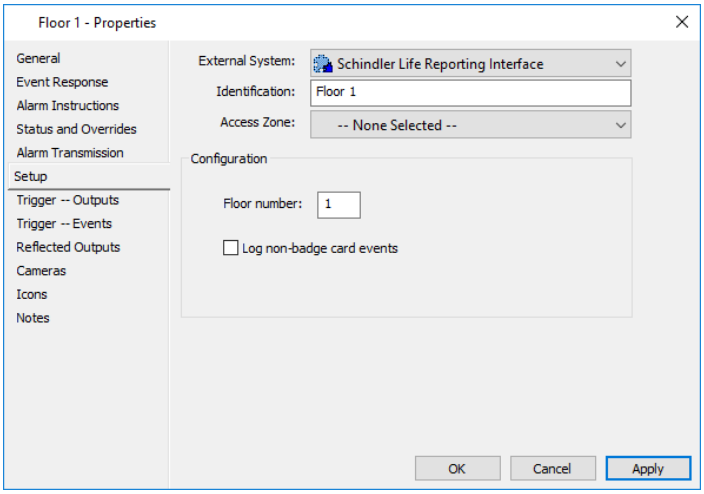
Procedure

To configure an External System Item to represent a floor, perform the following procedure in Gallagher Configuration Client:

Step	Action	Description
1	**Open the External Systems list window**	Click **Configure** from the Configuration Client menu bar, then **External Systems**. The External Systems list window opens.
2	**New External System Item**	Right-click and select **New...** > **External System Item**. The **General** tab displays.
3	**General fields**	Complete the General tab fields as required. Name the item after the floor it represents.
4	**Event Response tab**	Click the **Event Response** tab, and configure as required.
5	**Alarm Instructions tab**	Click the **Alarm Instructions** tab, and configure as required.

Continued on next page

Copyright © Gallagher Group Limited

6	**Click the Setup tab**	
7	**External System**	From the **External System** drop-down list, select the External System you created in section 3.3 *"Configuring a Live Reporting External System"*.
8	**Identification**	Enter a string value in the **Identification** field, for example "Floor "1". **Note:** The Identification string is checked for uniqueness within the same External System. It is limited to 64 characters.
9	**Floor number**	Enter the floor number in the **Floor number** field. This number must correspond to a floor in Schindler.
10	**Log non-badge card events**	If required, select the **Log non-badge card events** check box. Selecting this option enables Command Centre to receive 'non-badge card events' from Schindler. **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.
11	**Icons tab**	Click the **Icons** tab if you want to change the Icon Set for this External System Item.
12	**Notes tab**	Click the **Notes** tab if you want to add a note(s) about this External System Item.
13	**Click OK**	Click **OK** to close and save your changes.
14	**Repeat**	Repeat this procedure to configure an External System Item for each floor.

Copyright © Gallagher Group Limited

4 The Call Manager Interface (plugin)

About this section

The Call Manager Interface enables Gallagher readers to be used at Schindler terminals to identify Cardholders in Schindler. The interface also enables Command Centre to set the status of a floor to 'Secure' or 'Free' via a schedule or operator override.

If you do *not* require this functionality, then you do not need to create the Call Manager Interface and the information in this chapter is not applicable.

The Call Manager Interface is an optional licensed plugin of Command Centre. This plugin must be installed on the middleware PC (the PC hosting the FTCAPI Middleware Framework).

⚠ Securing/ unsecuring floors

When using the Call Manager Interface to secure or unsecure floors from Command Centre, it is strongly recommended that all floor control is managed *only* from Command Centre. This is because the interface does not allow changes made to a floor's status in Schindler to be reflected through to Command Centre.

In this section

To configure the Live Reporting Interface, perform the following procedures:

4.1 Installing the Call Manager Interface
4.2 Configuring an External System Server
4.3 Configuring a Call Manager External System
4.4 Configuring External System Items (Terminals)
4.5 Configuring a Schindler Alarm Zone
4.6 Configuring Schindler Action Plans
4.7 Configuring Gallagher Readers
4.8 Configuring Schindler Dummy Doors

4.1 Installing the Call Manager Interface

Procedure

To install the Call Manager Interface plugin, perform the following procedure:

Step	Action	Description
1	**Install FTCAPI Middleware Framework**	Install the FTCAPI Middleware Framework on the middleware PC (if not already installed). Refer to the topic *"Installing the FTCAPI Middleware Framework (FMF)"* in the Gallagher Configuration Client Help.

2	**Licence file**	Ensure your Command Centre licence file (CommandCentre.lic) contains the following entry:
		`[Plugin]`
		`PluginX=SchindlerID-CallInterface`
		(where `X` is a number)

Continued on next page

Copyright © Gallagher Group Limited

3	**Run installer file**	Run the installation executable **Schindler Call Interface Plug-in Setup x.xx.xx.msi** on the middleware PC. This file can be found with the Command Centre installation files in the folder: Utilities\System Interfaces\Schindler\ SchindlerCallInterfacePlugin **Note:** The FTCAPI Router Service restarts as part of the install.
4	**Verify installation**	To ensure that the Call Interface plugin has installed correctly, select the Windows **Programs and Features** utility from the Windows Control Panel. The program 'Gallagher Schindler Call Interface Plug-in' should be listed.

4.2 Configuring an External System Server

Refer to Help topic

Create an External System Server item. Refer to the topic *"Configuring an External System Server"* in the Gallagher Configuration Client Help.

Note: If you already created an External System Server when configuring the Live Reporting Interface (in section 3.2 *"Configuring an External System Server"*), you do *not* need to create another one.

4.3 Configuring a Call Manager External System

About this section

This topic describes how to create a Schindler Call Manager External System.

Note: Operators require the 'Edit Site' operator privilege to add, modify, and delete External Systems.

Before you begin

Before performing this procedure, 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.

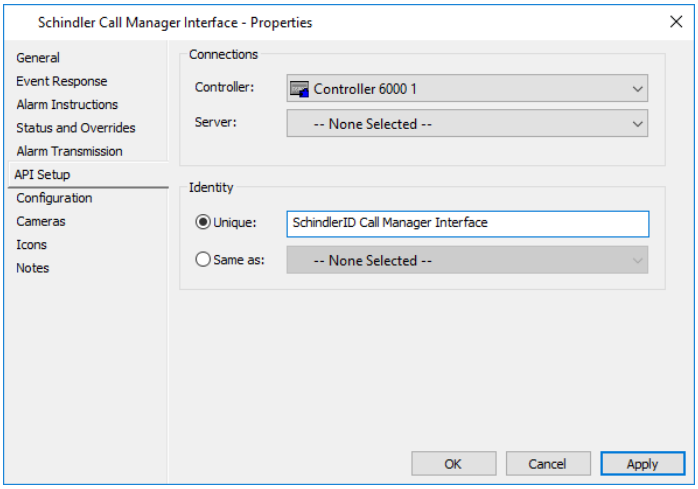
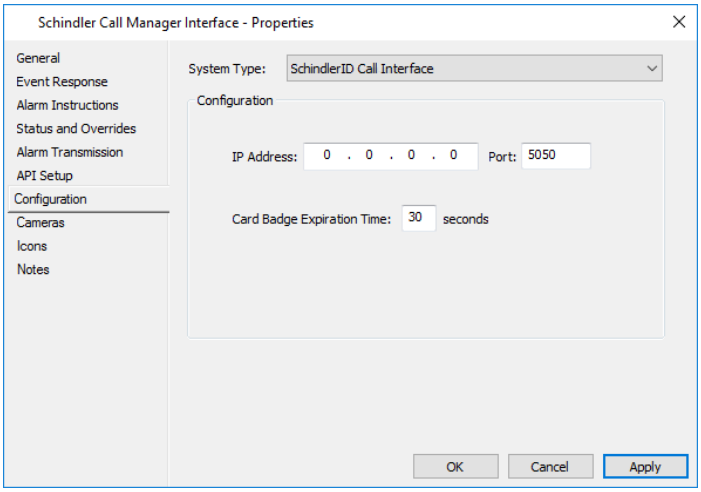
Procedure

To configure the Call Manager External System, perform the following procedure in Gallagher Configuration Client:

Step	Action	Description
1	**Open the External Systems list window**	Click **Configure** from the Configuration Client menu bar, then **External Systems**. The External Systems list window opens.
2	**New External System**	Right-click and select **New...** > **External System**. The **General** tab displays.

Continued on next page

Copyright © Gallagher Group Limited

3	**General fields**	Complete the General tab fields as required.
4	**Event Response tab**	Click the **Event Response** tab, and configure as required.
5	**Alarm Instructions tab**	Click the **Alarm Instructions** tab, and configure as required.
6	**Click the API Setup tab**	
7	**Controller**	Select the appropriate **Controller** from the drop-down list. **Note:** Only standard Gallagher Controllers will work, (i.e. Gallagher UltraSec Controllers will not work).
8	**Server**	Select the appropriate External System Server from the **Server** drop-down list.
9	**Unique Identity**	Click the **Unique** radio button in the 'Identity' section of this screen and type in a unique identity string. This field is limited to a maximum of 64 characters.
10	**Click the Configuration tab**	
11	**System Type**	Select the 'SchindlerID Call Interface' middleware plug-in from the **System Type** drop-down list. The 'Configuration' section of this tab displays the appropriate settings.

Continued on next page

Copyright © Gallagher Group Limited

12	**IP Address**	Enter the Schindler server IP address in the **IP Address** field.
13	**Port**	Enter the TCP/IP Port Number of the Schindler Logging Task Interface in the **Port** field. Range 0-65535.
14	**Card Badge Expiration Time**	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 Middleware Framework checks the time between the information being sent and received. 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.
15	**Icons tab**	Click the **Icons** tab if you want to change the Icon Set for this External System.
16	**Notes tab**	Click the **Notes** tab if you want to add a note(s) about this External System.
17	**Click OK**	Click **OK** to close and save your changes.

4.4 Configuring External System Items (terminals)

About this section

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

⚠ **Terminal IDs**: Contact your Schindler integrator to obtain the Terminal IDs in Schindler

Note: Operators require the 'Edit Site' operator privilege to add, modify, and delete External System Items.

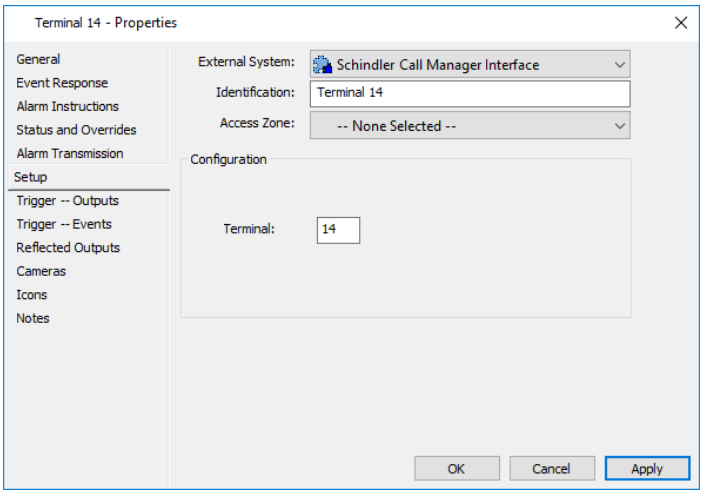
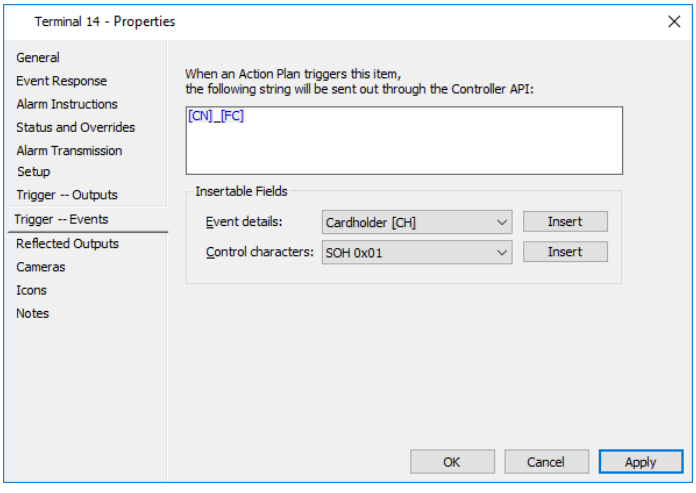
Procedure

To configure an External System Item to represent a Schindler terminal, perform the following procedure in Gallagher Configuration Client:

Step	Action	Description
1	**Open the External Systems list window**	Click **Configure** from the Configuration Client menu bar, then **External Systems**. The External Systems list window opens.
2	**New External System Item**	Right-click and select **New...** > **External System Item**. The **General** tab displays.
3	**General fields**	Complete the General tab fields as required. Name the item after the terminal it represents.
4	**Event Response tab**	Click the **Event Response** tab, and configure as required.

Continued on next page

Copyright © Gallagher Group Limited

5	**Alarm Instructions tab**	Click the **Alarm Instructions** tab, and configure as required.
6	**Click the Setup tab**	
7	**External System**	From the **External System** drop-down list, select the External System you created in section 4.3 "*Configuring a Call Manager External System*".
8	**Identification**	Enter a string value in the **Identification** field, for example "Terminal 14". **Note:** The Identification string entered is checked for uniqueness within the same External System. It is limited to 64 characters.
9	**Terminal**	Enter a Terminal ID in the **Terminal** field. 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).
10	**Click the Trigger -- Events tab**	

Continued on next page

Copyright © Gallagher Group Limited

11	**Card Number [CN]**	Select **Card Number [CN]** from the Event Details drop-down list, and click **Insert**.
12	**Facility Code [FC]**	Type an underscore, then select **Facility Code [FC]** from the Event Details drop-down list, and click **Insert**. **Note:** Manually typing in '[CN]' or '[FC]' will later result in an error message.
13	**Icons tab**	Click the **Icons** tab if you want to change the Icon Set for this External System Item.
14	**Notes tab**	Click the **Notes** tab if you want to add a note(s) about this External System Item.
15	**Click OK**	Click **OK** to close and save your changes.
16	**Repeat**	Repeat this procedure to configure an External System Item for each terminal in the building.

4.5 Configuring a Schindler Alarm Zone

Refer to Help topic

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

- Name the Alarm Zone 'Schindler Alarm Zone'.
- Assign the 'Schindler Alarm Zone' to *all* Configuration Client items that have been configured for the SchindlerID Feature. Refer to the topic *"Adding multiple items to Alarm Zones"* in the Gallagher Configuration Client Help.
- Also assign all items you create in the rest of this release note to this Alarm Zone.

Copyright © Gallagher Group Limited

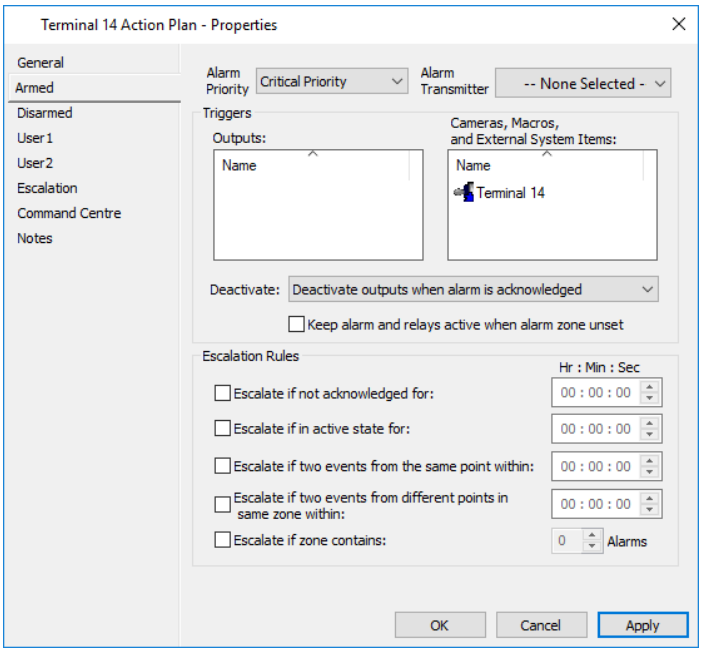
4.6 Configuring Schindler Action Plans

About this section

A Schindler Action Plan is required to associate the dummy door (yet to be created) with the External System Item (terminal). An Action Plan is required for each terminal in the building.

Procedure

To configure a Schindler Action Plan for an External System Item (terminal), perform the following procedure in Gallagher Configuration Client:

Step	Action	Description
1	**Open the External Systems list window**	Click **Configure** from the Configuration Client menu bar, then **Action Plans**. The Action Plan list window opens.
2	**New External System Item**	Right-click and select **New...** > **Action Plan**. The **General** tab displays.
3	**General fields**	Complete the General tab fields as required.
4	**Click the Armed (or Set) tab**	 These settings define the responses when the terminal item is linked with the Armed Alarm Zone.
5	**Alarm Priority**	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 many unnecessary events about access through the door. For debugging during the installation, it may be useful to configure the priority to 'Message Only'.

Continued on next page

Copyright © Gallagher Group Limited

6	**Add terminal to grid**	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	**Disarmed tab**	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	**User tabs**	Also repeat Steps 5-6 for the **User 1** and **User 2** tabs.
9	**Notes tab**	Click the **Notes** tab if you want to add a note(s) about this Action Plan.
10	**Click OK**	Click **OK** to close and save your changes.
11	**Repeat**	Repeat this procedure to configure an Action Plan for each terminal in the building.

4.7 Configuring Gallagher Readers

Refer to Help topic Create the Reader items required for this integration. Refer to the topic *"Creating Readers"* in the Gallagher Configuration Client Help.

4.8 Configuring Schindler Dummy Doors

About this section A dummy Door is required for each terminal in the building. This is a Door item that does not represent a physical door.

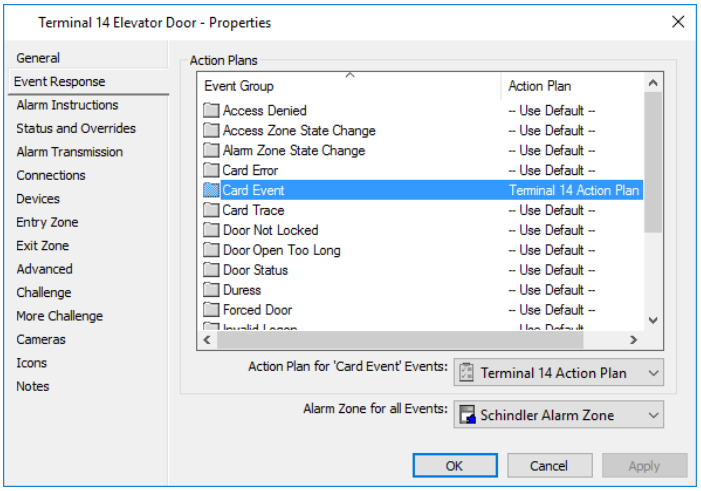
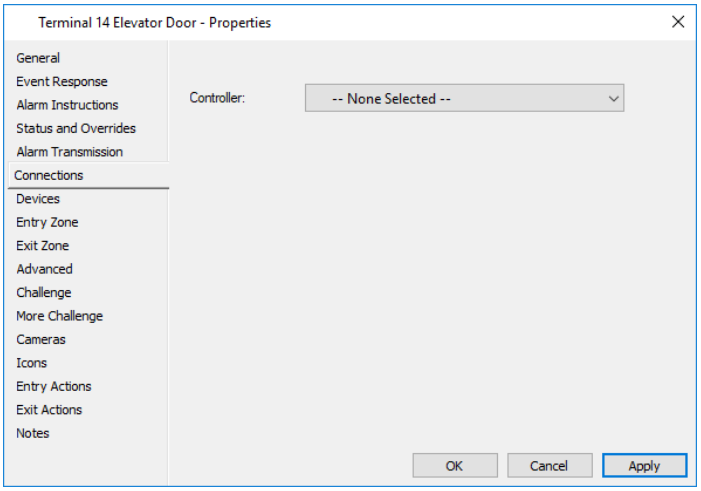
Note: You do not need to create a dummy Door for simulated terminals that are used to control the secure/free state of floors.

Procedure To configure a dummy Door for an External System Item (terminal), perform the following procedure in Gallagher Configuration Client:

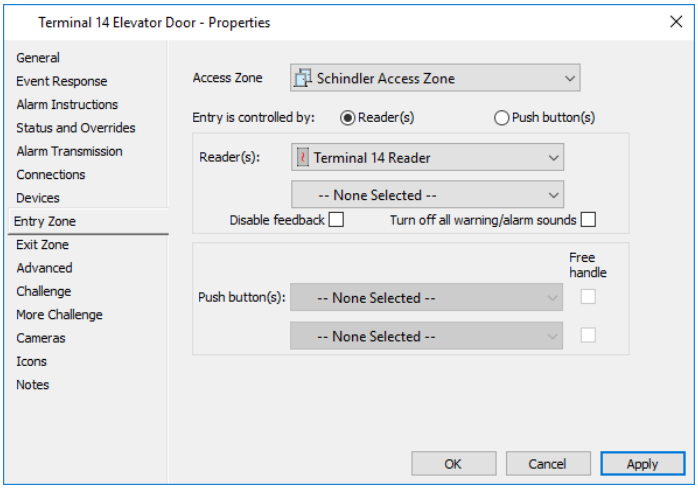
Step	Action	Description
1	**Open the External Systems list window**	Click **Configure** from the Configuration Client menu bar, then **Doors**. The Door list window opens.
2	**New External System Item**	Right-click and select **New...** > **Door**. The **General** tab displays.
3	**General fields**	Complete the General tab fields as required.

Continued on next page

Copyright © Gallagher Group Limited

4	**Click the Event Response tab**	
5	**Action Plan for Card Events**	Select the **Card Event** Event Group and assign the **Action Plan** created for the terminal corresponding to this dummy door.
6	**Alarm Zone for all Events**	Select the Schindler **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 for you to receive Door Events.
7	**Click the Connections tab**	
8	**Controller**	Assign the Door to the **Controller** that will host the dummy door. This should be the same Controller that is assigned to the External System that the External System Items (terminals) belong to.

Copyright © Gallagher Group Limited

9	**Click the Entry Zone tab**	
10	**Access Zone**	Select an **Access Zone** from the drop-down list. Ensure the Schindler Access Zone Schedule (previously created) is assigned to this Access Zone, and that Cardholder Access to this zone is 'Secure - No PIN' at all times.
11	**Reader(s)**	From the **Reader(s)** drop-down list, select the appropriate Reader that provides entry for this terminal.
12	**Icons tab**	Click the **Icons** tab if you want to change the Icon Set for this Door.
13	**Notes tab**	Click the **Notes** tab if you want to add a note(s) about this Door.
14	**Click OK**	Click **OK** to close and save your changes.
15	**Repeat**	Repeat this procedure to configure a dummy Door for each terminal in the building.

Copyright © Gallagher Group Limited

4.9 Configuring Secure/Free Floors

About this section

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

- **Secure:** A valid access card is required to gain access to the floor.
- **Free:** An access card is not required.

Virtual Output for each floor

You must 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.

External System Item for each floor

You must also configure an External System Item (floor) for each floor you wish to secure. If you have configured the Live Reporting Interface plugin, you will already have these items configured. If not, then complete section 3.4 "*Configuring External System Items (floors)*" earlier in this release note.

These items use 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.

Synchronisation from Command Centre to Schindler

If the simulated terminal has not received the override command, the virtual 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.

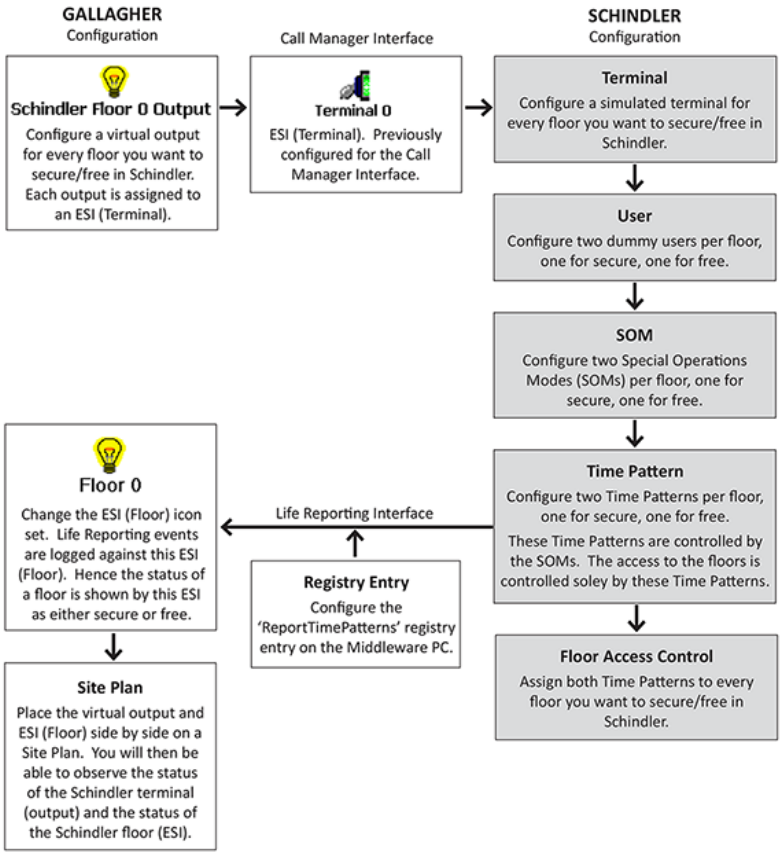
Whenever Command Centre reconnects to Schindler (after being disconnected), all floor states are re-sent from Command Centre to Schindler. This helps to ensure all floor states in Schindler are correct.

Copyright © Gallagher Group Limited

Configuration Process

Command Centre doesn't control the state of the floors directly. Instead, Command Centre uses Schindler 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 must follow to secure/free floors. This process identifies the various items you need to configure in both Command Centre and Schindler.



Configuration Process 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.
- Schindler integrators should configure the Special Operations Modes and provide their names to Gallagher integrators.
- An additional configuration option (schindler_zone_status_delay_ milliseconds) exists in the Schindler plugin 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 about the configuration file, refer to the document *"Release Note Schindler Call by Profile (vx.xx)"* located on the Command Centre installation media.

Copyright © Gallagher Group Limited

In this section

To configure secure/free floors, perform the following procedures in the order listed below:

In the Schindler system:

4.9.1 Configuring Time Patterns
4.9.2 Configuring Floor Access Requirements
4.9.3 Configuring Special Operation Modes (SOMs)
4.9.4 Configuring Dummy Users
4.9.5 Configuring Simulated Terminals

On the middleware PC:

4.9.6 Configuring the 'ReportTimePatterns' Registry

In Gallagher Configuration Client:

4.9.7 Configuring a virtual Output for each Floor
4.9.8 Assigning each virtual Output to an ESI (terminal)
4.9.9 Changing the External System Item (floor) icon set
4.9.10 Configuring a Site Plan for Secure/Free Floors

4.9.1 Configuring Time Patterns

Schindler Integrator

Contact your Schindler integrator to configure two Time Patterns per floor; one for secure and one for free. These Time Patterns are controlled by the Special Operation Modes. The access to the floors is controlled solely by these Time Patterns.

4.9.2 Configuring Floor Access Requirements

Schindler Integrator

Contact your Schindler integrator to configure floor access requirements. Both Time Patterns must be assigned to every floor you want to Secure or Free.

4.9.3 Configuring Special Operation Modes (SOMs)

Schindler Integrator

Contact your Schindler integrator to configure two Special Operation Modes per floor; one for secure and one for free.

4.9.4 Configuring Dummy Users

Schindler Integrator

Note: Before creating dummy users, Schindler integrators need to create an Access Profile (Allow All). This profile will allow access to all zones in the building.

Contact your Schindler integrator to configure two dummy users per floor; one for secure and one for free.

Copyright © Gallagher Group Limited

4.9.5 Configuring Simulated Terminals

Schindler Integrator

For every floor you want to Secure/Free in Schindler, you need to create a simulated terminal. Contact Schindler integrators to create simulated terminals as required.

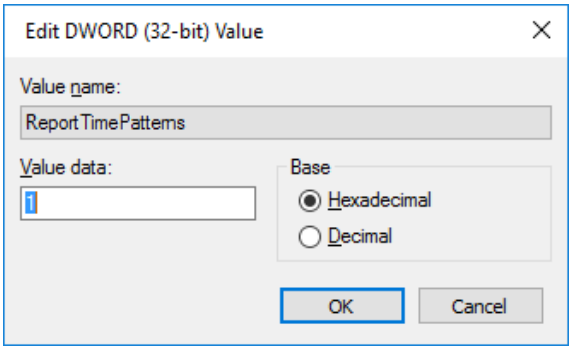
4.9.6 Configuring the 'ReportTimePatterns' Registry

About this section

To enable Time Pattern status reporting, you must create the registry entry 'ReportTimePatterns' on the middleware PC.

Procedure

To create the 'ReportTimePatterns' registry, perform the following procedure on the middleware PC:

Step	Action	Description
1	**Open 'Run'**	From the Start menu, open the Windows **Run** program.
2	**Enter 'regedit'**	Type in 'regedit' and click **OK**. The Registry Editor opens.
3	**Navigate to Key**	If using a 64 bit system, path your way to: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GALLAGHER\Command Centre If using a 32 bit system, path your way to: HKEY_LOCAL_MACHINE\SOFTWARE\GALLAGHER\Command Centre
4	**New DWORD Value**	Right-click, then select **New** > **DWORD Value**. The new DWORD Value is populated at the bottom of the registry values list.
5	**Name the value**	Enter the DWORD Value name 'ReportTimePatterns'.
6	**Double-click the value**	Double-click your newly created DWORD Value. The 'Edit DWORD Value' window displays. 
7	**Select 'Decimal', enter value**	Select **Decimal** as the Base, then enter '1' as the Value data, and click **OK**.

Copyright © Gallagher Group Limited

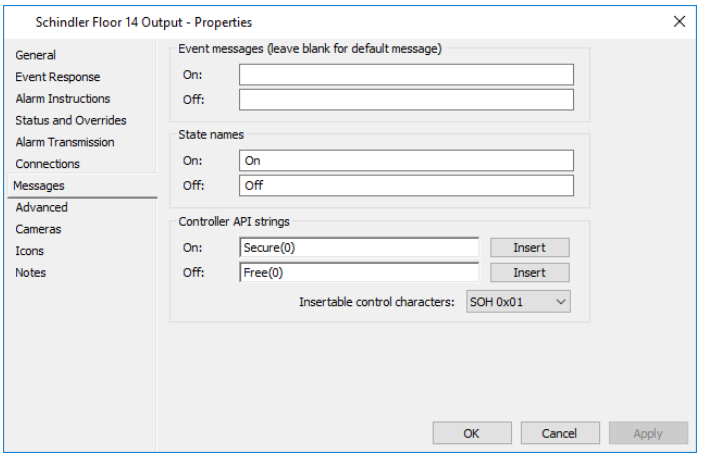
4.9.7 Configuring a virtual Output for each Floor

About this section

You need to create a virtual Output for each floor you wish to secure/free. A "virtual Output" simply refers to a regular Command Centre Output item that does not represent a physical output device.

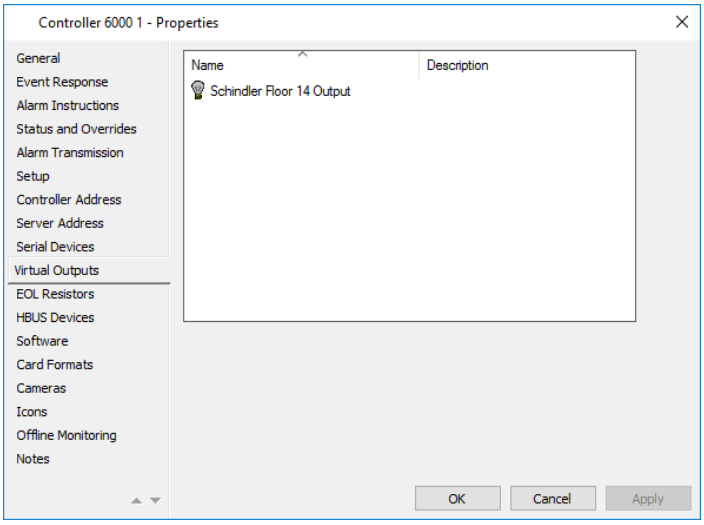
Procedure

To configure a virtual Output for each floor, perform the following procedure in Gallagher Configuration Client:

Step	Action	Description
1	**Open the Hardware list window**	Click **Configure** from the Configuration Client menu bar, then **Hardware**. The Hardware list window opens.
2	**New Output**	Right-click and select **New...** > **Output**. The **General** tab displays.
3	**General fields**	Complete the General tab fields as required.
4	**Event Response tab**	Click the Event Response tab, and configure as required.
5	**Click the Messages tab**	
6	**'On' API string**	To configure the Output to On: Enter the Personal Number of the dummy user (to Secure the corresponding floor) configured in Schindler into the Controller API strings 'On' field. For example, 'Secure(0)'.
7	**'Off' API string**	To configure the Output to Off: Enter the Personal Number of the dummy user (to Free the corresponding floor) configured in Schindler into the Controller API strings 'Off' field. For example, 'Free(0)'.
8	**Click OK**	Click **OK** to close and save your changes.

Continued on next page

Copyright © Gallagher Group Limited

9	**Open Controller properties**	From the Hardware list window, open the Controller that the virtual Output is to be assigned to
10	**Click the Virtual Outputs tab**	
11	**Add virtual Output**	Drag and drop the virtual Output you have just created into the grid on this screen.
12	**Click Apply**	Click **Apply**.
13	**Repeat procedure**	Repeat this procedure to configure a virtual Output for each floor you wish to secure/free.

Copyright © Gallagher Group Limited

4.9.8 Assigning a virtual Output to an ESI (terminal)

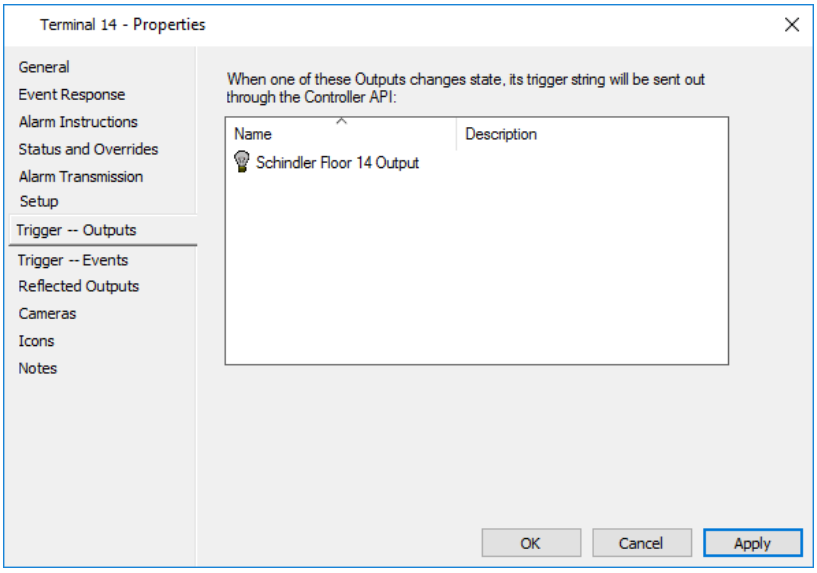
About this section

You will have already configured the External Systems Items to represent each terminal.

Assign each floor's virtual Output (previously configured) to the **Trigger -- Outputs** tab of the External System Item (terminal) that resides on the same floor.

Example

A virtual Output (floor Output) assigned to its appropriate External System Item (terminal):



Copyright © Gallagher Group Limited

4.9.9 Changing the External System Item (floor) icon set

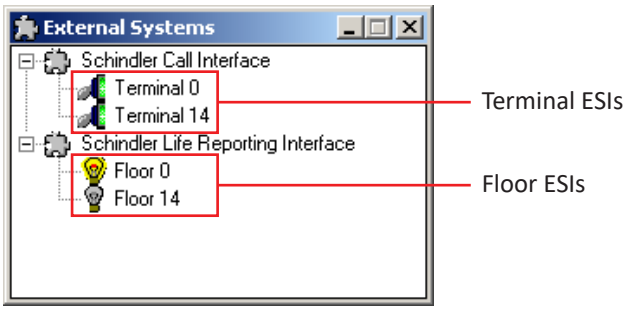
Before you begin

An External System Item (floor) must be configured for each floor you wish to secure. If you have configured the Live Reporting Interface plugin, you will already have these items configured. If not, then complete section 3.4 "*Configuring External System Items (floors)*" earlier in this release note.

Change the icon set

You should use a new icon set for the floor External System Items. 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.

In the example below, the existing Output Icon Set has simply been applied to the floor External System Items:



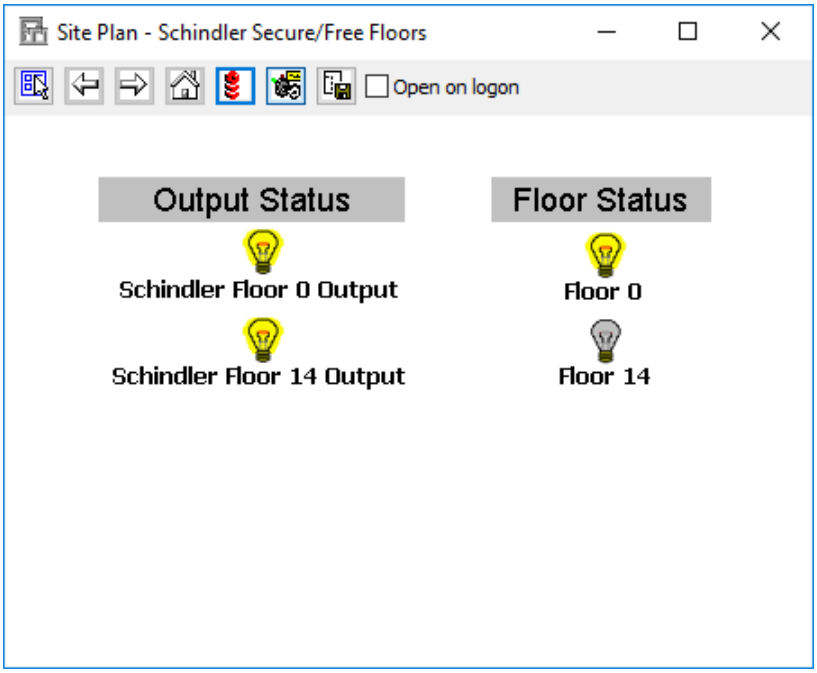
To create a new icon set for the floor External System Items, refer to the topic *"Creating a new Icon Set"* in the Gallagher Configuration Client Help.

Copyright © Gallagher Group Limited

4.9.10 Configuring a Site Plan for Secure/Free Floors

Add the floor External System Items to Site Plans

Drag the External System Item (floor) onto a Site Plan beside its corresponding 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.



Icon set: In the example above, the Output Icon Set has been applied to the External System Items (floors). This enables you to view the status of a floor easily, when the External System Item (floor) is added to the Site Plan. Refer to the topic *"Creating a new Icon Set"* in the Gallagher Configuration Client Help for further details.

Item status consistency/ inconsistency

If all configuration is correct, the status of the virtual Output will match the status of the External System Item (floor).

The status of the External System Item (floor) reflects the last *successful* change. Therefore, if a user overrides a virtual Output while the Schindler simulated terminal is still processing the previous request (and therefore the more recent one is thrown away), the status of the External System Item (floor) differs from the External System Item (terminal) status, and this way informs the operator that they should repeat the action.

Copyright © Gallagher Group Limited

4.10 Events/Alarms

Time Pattern state change events

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

Secure/Free 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 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 is not generated.
Event Group	Command Centre System
Event Type	External Event 2
Generated by	Command Centre

Copyright © Gallagher Group Limited

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

Copyright © Gallagher Group Limited

5 Events and Alarms

Schindler events 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.

5.1 Cardholder Management (Third Party Interface) Events and Alarms

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

Event Type	Card already assigned
Explanation	If a cardholder has the Schindler 'User Template', 'Master Group' and 'Badge Numbers' PDFs assigned, and two cards assigned, then only one user will be imported into the Schindler database. This user will have the badge numbers assigned. The second user is *not* imported because the badge numbers are already assigned to the first user, and this event is logged.
Event Details	Card already assigned to another user.

Event Type	Wrong length of badge number
Explanation	If a Cardholder has an incorrect length of badge number, this event is logged and the Cardholder is *not* updated in the Schindler database. This length of badge number is configurable in the Schindler Third Party Database Interface. This length of badge number is configured using the sum of 'HI' and 'LO' digits.
Event Details	Wrong length of badge number.

Event Type	Wrong format for badge number
Explanation	If a Cardholder's badge number is of the wrong format, this event is logged and the cardholder is *not* updated in the Schindler database.
Event Details	Wrong format for badge number.

Copyright © Gallagher Group Limited

Reporting options Select the appropriate Schindler reporting option in the Schindler Third Party Database.

If you select...	then...
Report an error	If a Command Centre Cardholder has two cards assigned, then only one user will be imported into the Schindler database. This user will have the badge numbers assigned. The second user will not be imported because the badge numbers are already assigned to the first user. The event 'Card already assigned' is logged in Command Centre.
Leave the card assigned to the existing user	If a Command Centre Cardholder has badge numbers assigned that match the badge numbers of an existing Schindler user, then the Command Centre Cardholder's badge numbers will simply not be imported. No event is logged in Command Centre.
Assign the card to the new user	If a Command Centre Cardholder has badge numbers assigned that match the badge numbers of a Schindler user, then the badge numbers are removed from the Schindler user and assigned to the Command Centre Cardholder. No event is logged in Command Centre.

5.2 Live Reporting (Event Logging) Events and Alarms

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

Event Type	Access granted
Explanation	If a cardholder is granted access to a destination floor, this event is logged.
Event Text	<Cardholder> was granted access to <destination floor> at <ESI> (floor name).

Event Type	Access denied
Explanation	If a cardholder is denied access to a destination floor, this event is logged.
Event Text	<Cardholder> was denied access to <destination floor> at <ESI> (floor name).

Copyright © Gallagher Group Limited

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

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

Event Type	Card badge expired
Explanation	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 this event is logged.
Event Text	Card badge expired for <Cardholder> at <ESI> (terminal name).
Event Details	The card was badged <seconds> ago.

Event Type	Card badge delayed
Explanation	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 this event is logged.
Event Text	Card badge delayed for <Cardholder> at <ESI> (terminal name).
Event Details	The card was badged <seconds> ago.

Event Type	Wrong acknowledgement
Explanation	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, this event is logged.
Event Text	Wrong acknowledgement received from <ESI> (terminal name).

Event Type	Wrong trigger
Explanation	If a user badges their card and the trigger string for the terminal has been incorrectly configured, the terminal is not enabled and this event is logged.
Event Text	Wrong Trigger received <ESI> (terminal name).
Event Details	Please configure the Trigger Events to [CN]_[FC].

Event Type	Trigger queue overflow
Explanation	If a user badges their card and the queue has exceeded the badge overflow limit (100 badges), this event is logged and the trigger queue is emptied. **Note:** The overflow limit of 100 cannot be changed.
Event Text	Trigger queue overflow.

Copyright © Gallagher Group Limited

6 Considerations

Controller event rate limit	Where Gallagher readers on a Controller are connected to the elevator terminals, it is recommended that the maximum Controller loading is no more than 2 card events per second (this is the sum of the card events for all connected readers).
Multiple Call Manager connections	• A Schindler Call Manager can handle only one connection. Several Call Managers can be created in a Schindler system. • Command Centre is able to connect to several Schindler systems. In such a case, several External Systems (Call Interfaces) are created in Command Centre. • Command Centre is not supposed to connect to several Call Managers of the *same* Schindler system. • A separate Call Manager in the Schindler system would be needed if there is another system besides Command Centre that is going to call the lifts.
Terminal request processing	When a terminal is processing a request, the terminal will not accept any other requests until such time as the original request is processed.
Time Patterns and SOMs	If a Time Pattern is deleted, you will also need to delete the SOM related to it. When creating the Time Pattern again, you will need to create a new SOM. If you don't do this, you may find that the behaviour of the SOM is inconsistent.
If Time Patterns are deleted	If a Time Pattern is deleted, an alarm is raised advising the operator that one of the Time Patterns is not defined. If the alarm is acknowledged it will not be raised again, (e.g. When an override is performed on the Output, the alarm is not raised again). **Note:** If the middleware services or the Schindler system are disconnected from the network and both Time Patterns are deleted from a floor, then Command Centre will not report the Time Pattern deletion.
If only a 'Free' Time Pattern is configured	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.
Evacuation Report not supported	The Evacuation Report is not supported by this feature.

Copyright © Gallagher Group Limited

7 Uninstallation

About this section

The 'SchindlerID' feature is a part of the Command Centre system, enabled via licensing. This cannot be uninstalled, but the Live Reporting Interface plugin and Call Manager Interface plugin can be uninstalled (if you have installed them).

Procedure

To uninstall the Live Reporting Interface plugin and/or the Call Manager Interface plugin, perform the following procedure:

Step	Action	Description
1	**Backup**	Perform a backup of your Command Centre system.
2	**Remove redundant External System Items**	Remove all the Schindler External System Items that are no longer required. **Note:** Some items configured for the Live Reporting Interface plugin are likely reused by the Call Manager Interface plugin. If you are only uninstalling one plugin, refer to chapters 2 "*The Live Reporting Interface (plugin)*" and 3 "*The Call Manager Interface (plugin)*" to see which items are used by which plugins, and thus must not be deleted.
3	**Stop Command Centre and Services**	Exit Command Centre and stop the Command Centre Services.
4	**Uninstall program(s)**	On the middleware PC(s), select **Programs and Features** from the Windows Control Panel and uninstall: • the 'Gallagher SchindlerID Live Reporting Plug-in' program, and/or • the 'Gallagher SchindlerID Call Interface Plug-in' program.
5	**Start Services and Command Centre**	Restart the Command Centre Services and Command Centre.

Copyright © Gallagher Group Limited