

Integration with Gallagher Command Centre



TORUS

CIC TECHNOLOGY,

15/39 Herbert Street, St Leonards, NSW – 2065.

www.cictechnology.com

Document details

| | |
|-------------|--|
| Title | Integration with Gallagher Command Centre |
| Description | This document explains the steps to create integration between Torus and Gallagher Command Centre 8.0 and above. |

Document Revision History

| Version | Date | Author | Comments |
|---------|------------------|--------|---|
| V.1.0 | August 20, 2020 | AA | First Draft |
| V.1.1 | October 16, 2020 | AA | Information added, 1 - Details for Gallagher Command Centre API port. 2 - New Feature to import Access Groups from Command Centre. 3 - Updated configuration of User Synchronisation. 4 - Updated configuration for Alarm and Events. |
| V.1.2 | August 13, 2021 | AA | Information added, 1 - Integration overview 2 - URL and ports details of Torus Exchange |
| V.1.3 | April 15, 2022 | AA | Information for new feature added. <ul style="list-style-type: none"> Integration of REST API Alarms & Events Subscription of card holders related events using REST API Alarms and Events |
| | | | |

Abbreviation list

| Abbreviation | Description |
|----------------|--|
| TORUS | Term used to describe overall EKC which includes the hardware, software, and integration plugin. |
| Torus Software | Torus is a cloud application hosted on Microsoft Azure. This software is accessible through any connected browser. |
| Torus Cabinet | Hardware product which is provided to secure the items/keys. |
| Torus Exchange | A windows plugin used for Torus integration with 3 rd party systems. |
| Torus REST API | A generic developer interface which enables HLIs with 3 rd Party software. |
| HLI | High Level Integration, a term used to describe the connectivity between Torus and other 3 rd party Access control systems or software. |
| Azure | Microsoft Azure cloud platform (azure.microsoft.com) |
| EKC | Electronic Key Cabinet. |
| IOT | Internet of things. |
| HTTPS | Hypertext transfer protocol secure. |

Disclaimer

This document gives certain information about products and/or services provided by CIC Technology. Every commercially reasonable effort has been taken to ensure the quality and accuracy of the information in the document however the content is for informational purposes only. The described product or process in this document are subject to change without prior notice, due to continuous development program at CIC Technology.

Neither CIC Technology 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.

Copyright

Torus software, software code, firmware code, database, hardware, and mechanical design are subject to copyright owned by CIC Technology, and you may not sell it without permission. CIC Technology is the owner of all trademarks reproduced in this information. All other products, brands, trademarks which are mentioned in the content of this document are not the property of CIC Technology, are acknowledged and owned by their respective owners.

Confidentiality Notice

This document is confidential and contains proprietary information and intellectual property of CIC Technology. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of CIC Technology. Please be aware that disclosure, copying, distribution or use of this document and the information contained therein is strictly prohibited.

CONTENTS

| | |
|--|-----------|
| TORUS INTEGRATIONS | 6 |
| GALLAGHER COMMAND CENTRE HLI | 7 |
| Integration prerequisites | 7 |
| Integration overview | 8 |
| STEPS FOR INTEGRATION | 9 |
| 1 – CREATE INTEGRATION RECORD | 9 |
| 2 – CONFIGURE GALLGHER COMMAND CENTRE REST API | 10 |
| 3 – CREATE EXTERNAL SYSTEMS IN GALLAGHER COMMAND CENTRE | 13 |
| 3.1 – Create an External System Server in Command Centre | 13 |
| 3.2 – Create an External System in Command Centre | 15 |
| 3.3 – Create an External System Item in Command Centre | 17 |
| 4 – INSTALL TORUS EXCHANGE | 19 |
| 5 – COMPLETE USER SYNCHRONISATION SETTINGS | 21 |
| 5.1 – Select Command Centre Access Groups in Torus | 21 |
| 5.2 – Mapping of Command Centre User fields with Torus User fields | 22 |
| 6 – SELECT EVENTS FOR EXPORT | 24 |
| 7 – DATA MASK SETUP | 25 |
| 8 – ANTI-TAILGATING SETUP | 27 |
| 9 – CARD HOLDER LOGIN AT TORUS CABINET VIA REST API ALARMS & EVENTS | 33 |
| 9.1 – Create Door in Command Centre | 33 |
| 9.2 – Map Door with Torus cabinet | 34 |

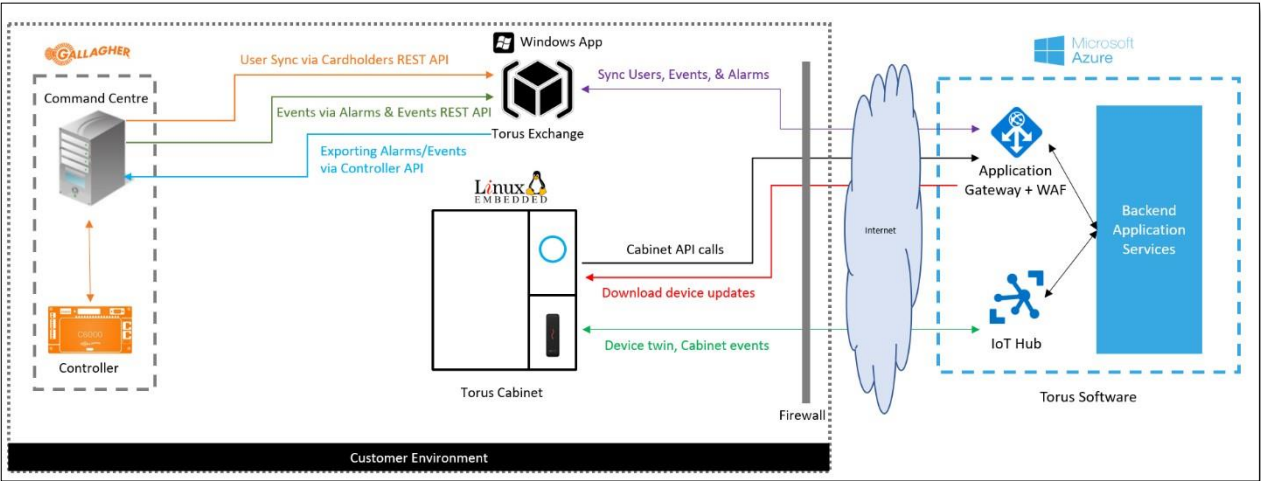
GALLAGHER COMMAND CENTRE HLI

For Gallagher command centre integration CIC Technology has developed a custom middleware application which is called Torus Exchange. This application is a Windows plugin which provides integration (HLI) with Gallagher Command Centre Version 8.0 and above. This plugin is installed on Gallagher Command Centre server, and it utilises Command Centre's Controller API and REST API Cardholder. Customers need to include REST APIs in command centre license as per listed in Integration Prerequisites.

Integration prerequisites

- Gallagher Command Centre licences should include following features
 - REST API - Cardholder (Gallagher SKU/part number: C12784)
 - Controller API (to export events and alarms from Torus to Command centre through Gallagher Controller)
 - **Optional** - REST API - Alarms & Events (Gallagher SKU/Part number: C12772) To subscribe events from Gallagher controller when card reader mounted on Torus cabinet is connected with Gallagher Controller. For more details, [please see page 32](#).
- Correct configurations for the 'Gallagher API Key of the Gallagher instance' and 'URL of the Gallagher REST API' are saved in the Torus integration record.
- Hardware, access zones, alarm zones and doors are correctly setup in Gallagher Command Centre.
- Install Cardax API in the same PC where the Torus Exchange middleware service is installed.
- The hardware (controller) should be functioning properly in Gallagher Command Centre (Go to Configure > Hardware > right click Properties > Status and overrides and verify that status is 'Normal')
- Torus Exchange must be allowed to access required URL & port through client's network firewall.
 - URL= <https://hliapi-au.torus-technology.com>
 - Port: 443 over HTTPS

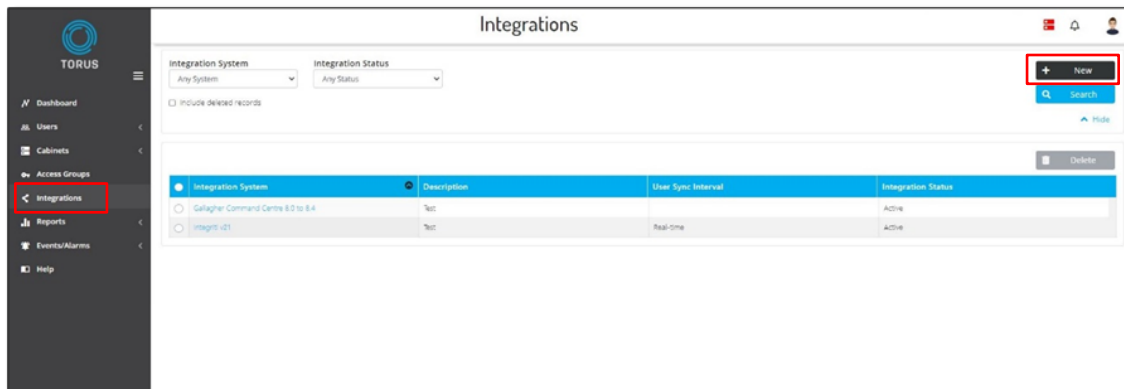
Integration overview



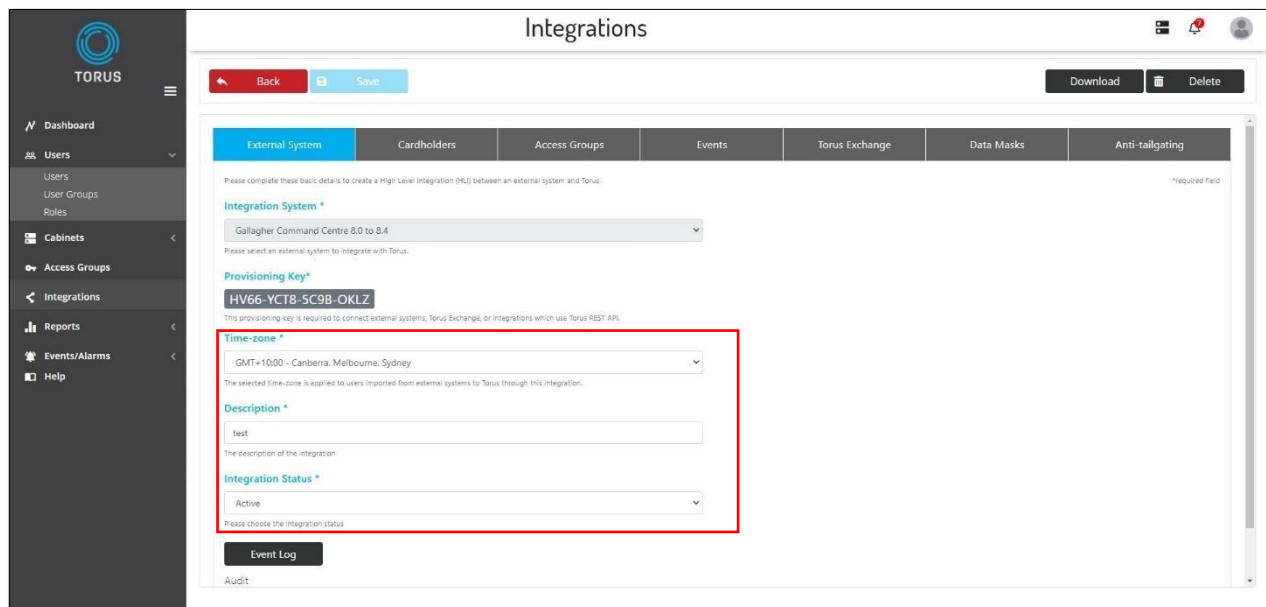
STEPS FOR INTEGRATION

1 – CREATE INTEGRATION RECORD

- Login to Torus Software
- Go to Integrations and select New



- Complete the details for new External system details.
- Select Gallagher Command Centre from Integration systems Drop down field and provide a description of this integration.
- Select the time zone which is applied to users imported from external system.



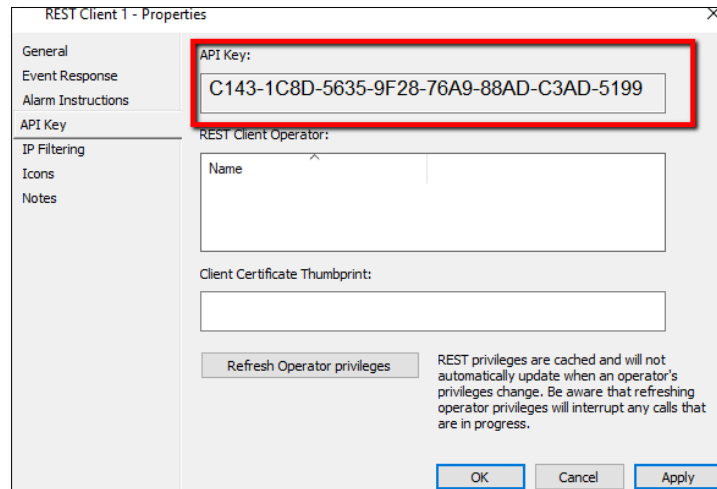
The screenshot shows the 'New' form for creating an integration record. The form is titled 'Integrations' and has tabs for 'External System', 'Cardholders', 'Access Groups', 'Events', 'Torus Exchange', 'Data Masks', and 'Anti-tailgating'. The 'External System' tab is selected. The form contains the following fields:

- Integration System ***: A dropdown menu with 'Gallagher Command Centre 8.0 to 8.4' selected.
- Provisioning Key ***: A text field with the value 'HV66-YCT8-5C9B-OKLZ'.
- Time-zone ***: A dropdown menu with 'GMT+10:00 - Canberra, Melbourne, Sydney' selected. This field is highlighted with a red box.
- Description ***: A text field with the value 'test'.
- Integration Status ***: A dropdown menu with 'Active' selected.

At the bottom of the form, there is an 'Event Log' button and an 'Audit' section.

2 – CONFIGURE GALLGHER COMMAND CENTRE REST API

- Open Gallagher Command centre.
- Go to Configure > Services and Workstations.
- Create a new REST client, give any preferred name, and copy the API key of this client.



REST Client 1 - Properties

General
Event Response
Alarm Instructions
API Key
IP Filtering
Icons
Notes

API Key:
C143-1C8D-5635-9F28-76A9-88AD-C3AD-5199

REST Client Operator:
Name

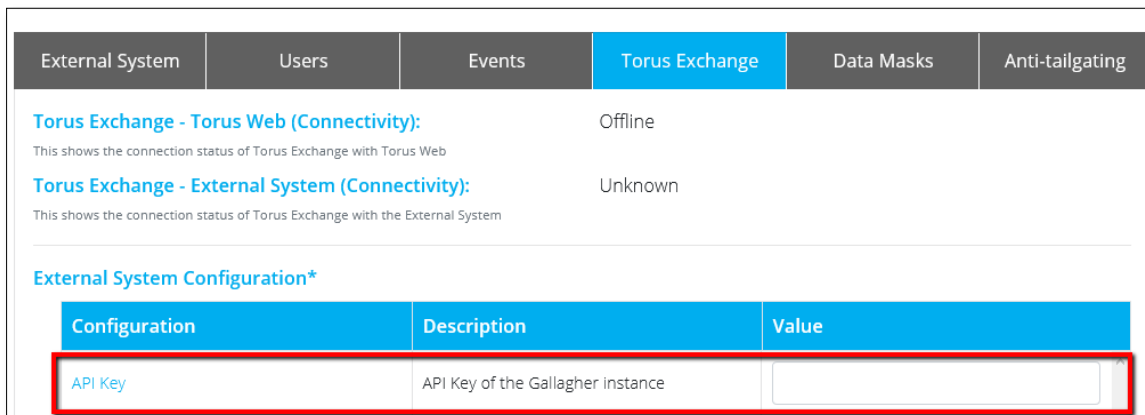
Client Certificate Thumbprint:

Refresh Operator privileges

REST privileges are cached and will not automatically update when an operator's privileges change. Be aware that refreshing operator privileges will interrupt any calls that are in progress.

OK Cancel Apply

- Go to Torus Software and open the new integration details page.
- Select Torus Exchange Tab and paste Gallagher Command Centre REST Client 'API Key' in API Key field.



| External System | Users | Events | Torus Exchange | Data Masks | Anti-tailgating |
|--|-----------------------------------|--------|----------------|------------|-----------------|
| Torus Exchange - Torus Web (Connectivity): This shows the connection status of Torus Exchange with Torus Web | | | Offline | | |
| Torus Exchange - External System (Connectivity): This shows the connection status of Torus Exchange with the External System | | | Unknown | | |
| External System Configuration* | | | | | |
| Configuration | Description | Value | | | |
| API Key | API Key of the Gallagher Instance | | | | |

- Go to Gallagher Command Centre File > Server Properties > Web Services tab.

- Select 'Enable REST API' and 'Do not require pinned client certificates' and save and copy the port number.
- Server base port should be a free port to avoid any conflicts with application. For example, if port 8905 is not available then please use port 8904.

CQReXchange technician demo - Properties

General
Licensing
Event Priorities
Alarm Flooding
Alarm Zone States
Event Defaults
Alarm Instruction Defaults
Alarm Transmission
Alarm Notes
Operator Defaults
User Codes
Competency Messages
State Names
Measurement Units
Advanced
Web Services
Card Security
Software
Notifications
Outgoing Email

☐ Enable Mobile Client Web Services

Server Base Port: 8901 Device Identification: TLS Client Certificate


Status:
Data Port: Stopped

☒ Enable REST API

Server Base Port: 8905 ☒ Do not require pinned client certificates

Status:
Data Port: Running on 8905
Device Identification: API Key only

- For the 'Server URL' field in the 'Torus Exchange' tab of Integration record, provide the URL in the following format. <https://<IP address of PC where Gallagher Command Centre is installed>:<Server Base Port>/api/>



Dashboard
Users
Cabinets
Access Groups
Integrations
Reports
Events/Alarms
System Administration
Help

Integrations

Back
Save
Download
Delete

| External System | Cardholders | Access Groups | Events | Torus Exchange | Data Masks | Anti-tailgating |
|---|--|---|--------|----------------|------------|-----------------|
| Torus Exchange - Torus Web (Connectivity): This shows the connection status of Torus Exchange with Torus Web. | | | | Offline | | |
| Torus Exchange - External System (Connectivity): This shows the connection status of Torus Exchange with the External System. | | | | Unknown | | |
| External System Configuration* | | | | | | |
| Configuration | Description | Value | | | | |
| Server URL | Server URL of the Gallagher REST API instance | https://192.168.94.15:8904/api/ | | | | |
| API Key | API key of the Gallagher REST API instance | 1A76-F668-CC5A-CCDB-E867-544F-ACFB-F85E | | | | |
| Is Client Certificate Required | Whether the Gallagher REST API instance requires a client certificate for authentication | No | | | | |
| External System Name | The unique identifier of the External System in Gallagher used for events sync | GeveoExternalSystem | | | | |
| External System Item Name | The unique identifier of the External System item in Gallagher used for events sync | GeveoExternalSystemItem | | | | |

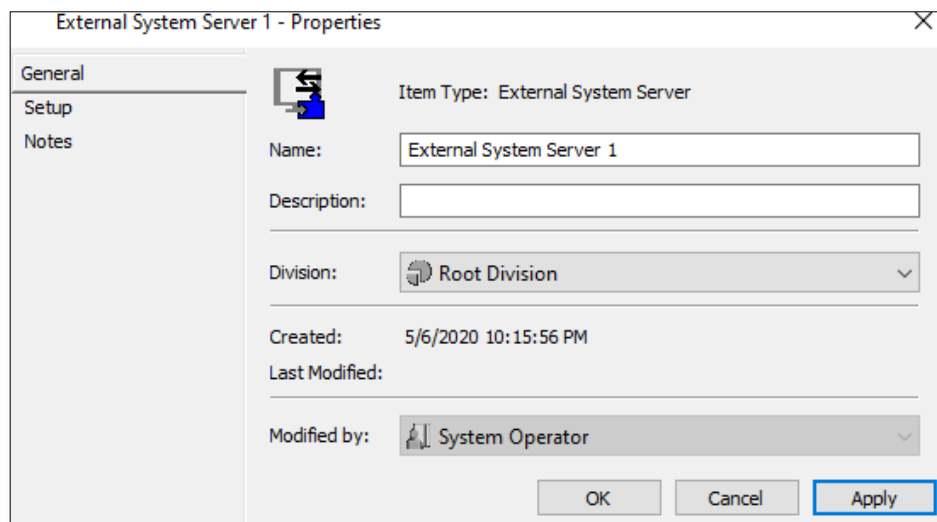
3 – CREATE EXTERNAL SYSTEMS IN GALLAGHER COMMAND CENTRE

3.1 – Create an External System Server in Command Centre

- Open Gallagher Command Centre and go to Configure > External Systems.
- Create a new item type External System Server and complete details as follows.

❖ General Tab

- Give any preferred name and keep other details unchanged.
- Use the same name in Torus Exchange record.



External System Server 1 - Properties

General

Setup

Notes

Item Type: External System Server

Name: External System Server 1

Description:

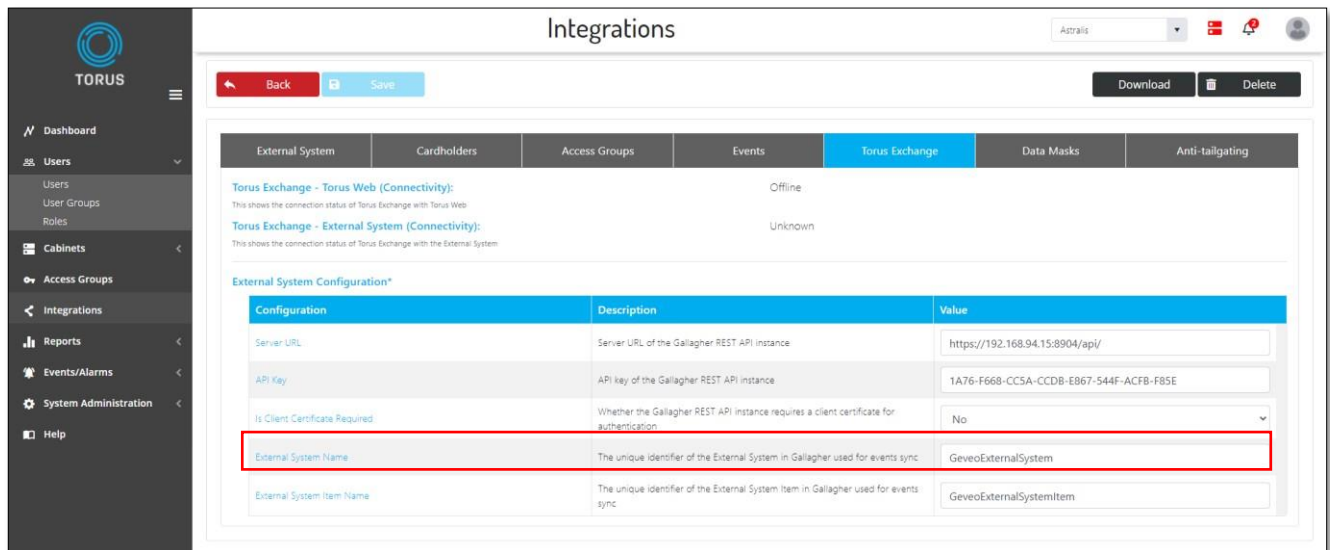
Division: Root Division

Created: 5/6/2020 10:15:56 PM

Last Modified:

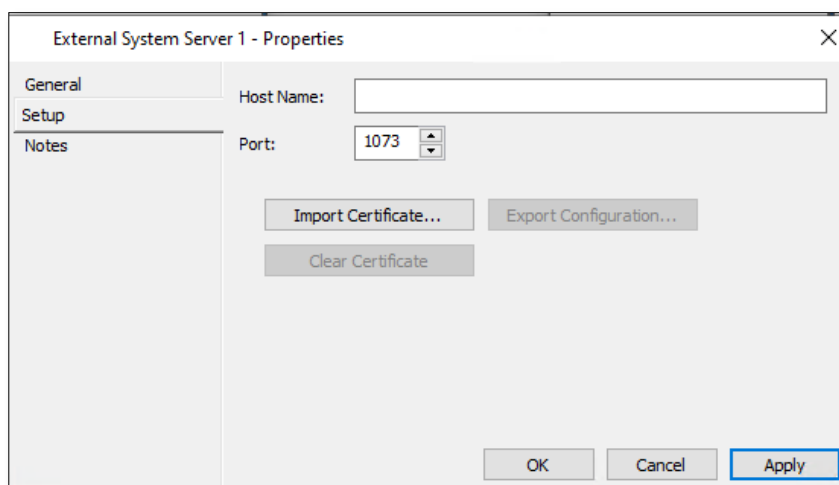
Modified by: System Operator

OK Cancel Apply



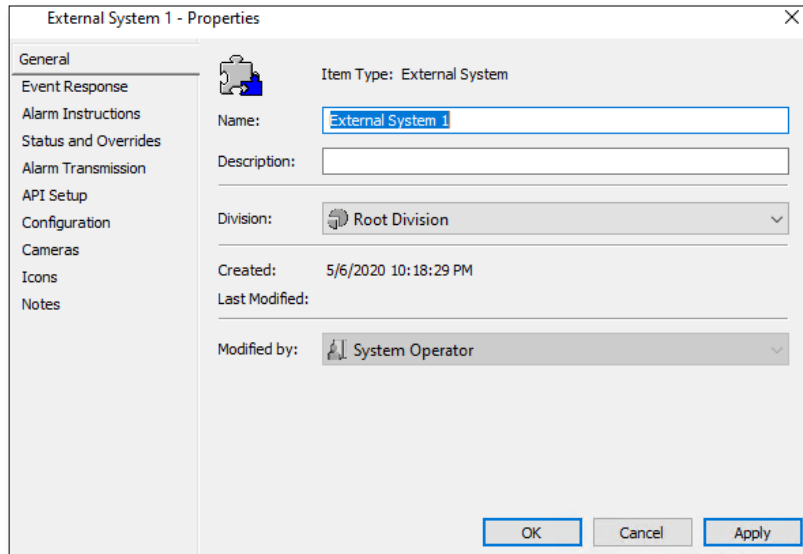
❖ Setup Tab

- Host name - IP address of the PC where the Torus Exchange middleware will be installed.
- Port - Keep unchanged
- Install Gallagher FTCAPI where the Torus Exchange middleware service is installed.
- Import FTCAPI.PEM file from Gallagher program files folder and click apply.
- Export FTCAPI.ini file and place it Gallagher command centre program (Cardax api installation folder). Windows user must have admin permissions to override the existing FTCAPI.ini file.



3.2 – Create an External System in Command Centre

- Right click the created external system server and create a new item type External System.
 - ❖ General Tab
 - Give any name to External system, it is ideal to use the same name as Unique name for API setup



External System 1 - Properties

General

Item Type: External System

Name: External System 1

Description:

Division: Root Division

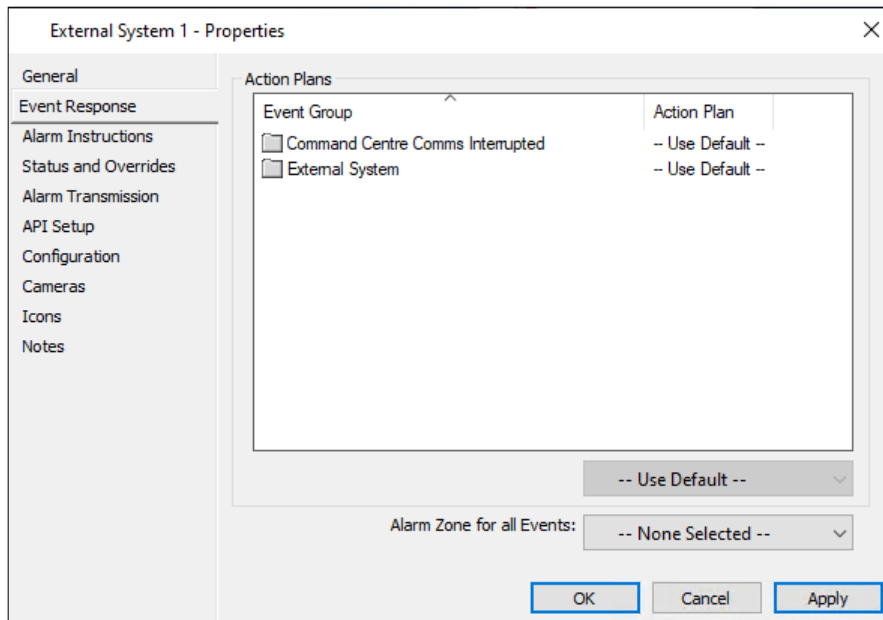
Created: 5/6/2020 10:18:29 PM

Last Modified:

Modified by: System Operator

OK Cancel Apply

- ❖ Event Response Tab
 - Select the relevant Alarm Zone.



External System 1 - Properties

General

Event Response

Action Plans

| Event Group | Action Plan |
|---|-------------------|
| <input type="checkbox"/> Command Centre Comms Interrupted | -- Use Default -- |
| <input type="checkbox"/> External System | -- Use Default -- |

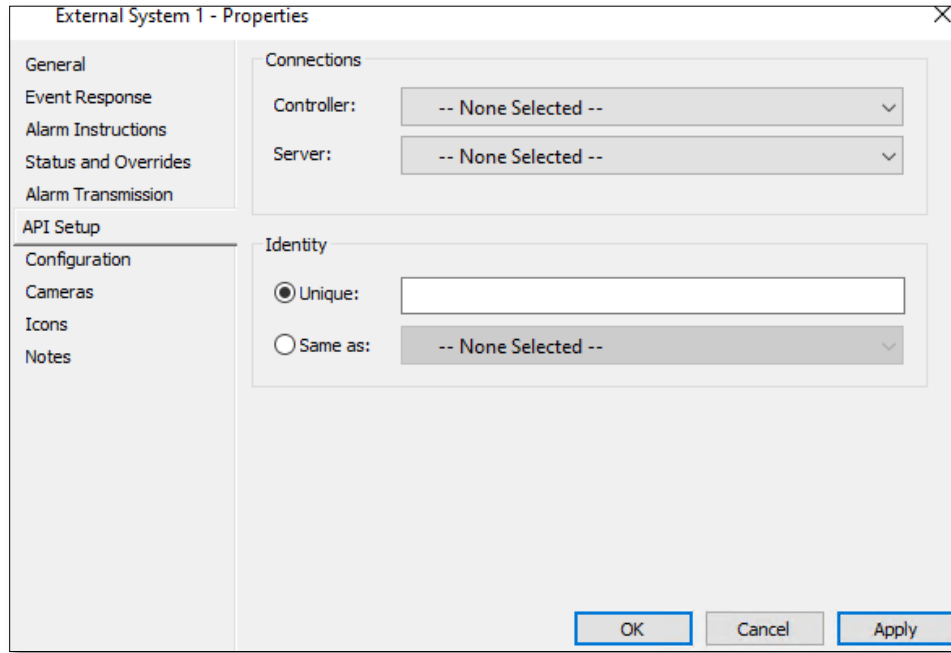
-- Use Default --

Alarm Zone for all Events: -- None Selected --

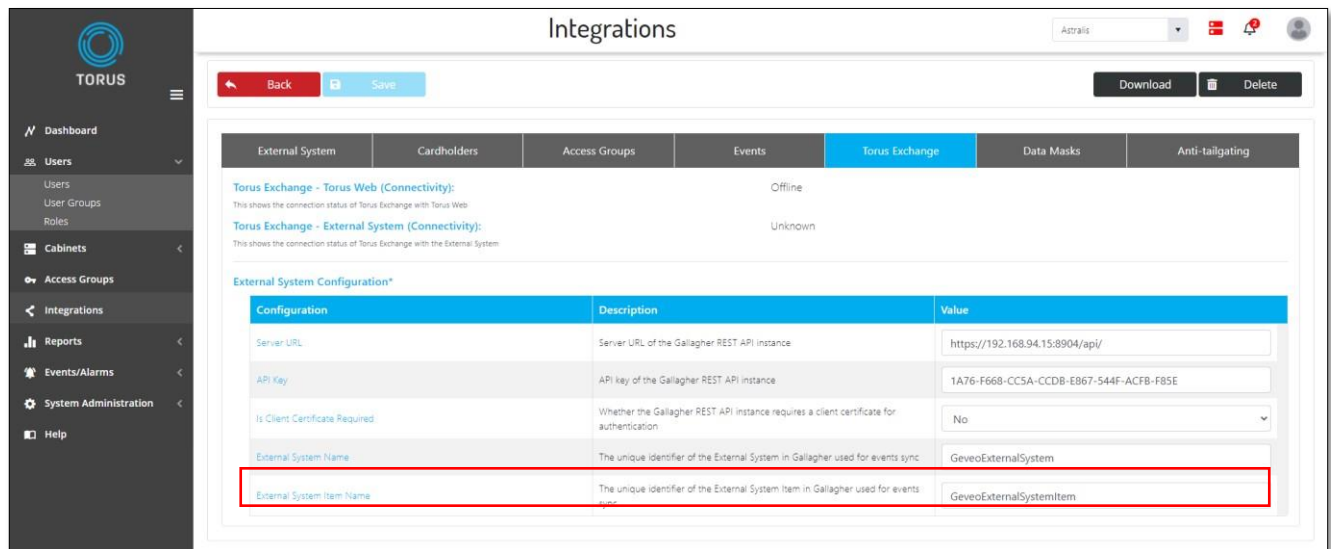
OK Cancel Apply

❖ API Setup Tab

- Select the correct Controller and the External System Server.
- For the Unique field, give the same name used in the Torus Exchange External System Item Name field of the integration record.



The screenshot shows the 'External System 1 - Properties' dialog box with the 'API Setup' tab selected. The 'Connections' section has 'Controller' and 'Server' dropdown menus, both currently set to '-- None Selected --'. The 'Identity' section has two radio buttons: 'Unique' (selected) and 'Same as'. The 'Unique' radio button is followed by a text input field. The 'Same as' radio button is followed by a dropdown menu set to '-- None Selected --'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.



The screenshot shows the 'Integrations' page in the Torus web interface. The left sidebar contains navigation links: Dashboard, Users, Cabinets, Access Groups, Integrations (selected), Reports, Events/Alarms, System Administration, and Help. The main content area shows the 'Integrations' page with a table of integration records. The 'Torus Exchange' tab is selected. The table has columns: External System, Cardholders, Access Groups, Events, Torus Exchange, Data Masks, and Anti-tailgating. The 'Torus Exchange' column shows 'Offline' for 'Torus Exchange - Torus Web (Connectivity)' and 'Unknown' for 'Torus Exchange - External System (Connectivity)'. Below the table is the 'External System Configuration*' section, which contains a table with columns: Configuration, Description, and Value. The 'External System Item Name' field is highlighted with a red box, showing the value 'GeveoExternalSystemItem'.

| Configuration | Description | Value |
|--------------------------------|--|---|
| Server URL | Server URL of the Gallagher REST API instance | https://192.168.94.15:8904/api/ |
| API Key | API key of the Gallagher REST API instance | 1A76-F668-CC5A-CCDB-E867-544F-ACFB-F85E |
| Is Client Certificate Required | Whether the Gallagher REST API instance requires a client certificate for authentication | No |
| External System Name | The unique identifier of the External System in Gallagher used for events sync | GeveoExternalSystem |
| External System Item Name | The unique identifier of the External System item in Gallagher used for events sync | GeveoExternalSystemItem |

3.3 – Create an External System Item in Command Centre

- Right click the external system and create a new item type External System Item.

torus_item - Properties

General

Item Type: External System Item

Name: torus_item

Description: torus_item

Division: Root Division

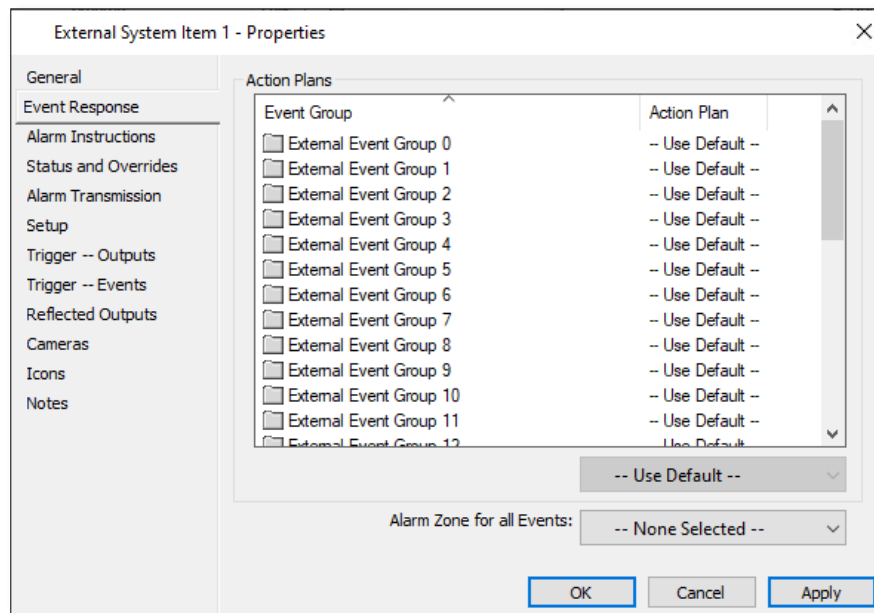
Created: 7/07/2020 4:33:06 PM

Last Modified: 7/07/2020 4:33:06 PM

Modified by: System Operator

OK Cancel Apply

- ❖ Event Response Tab
 - For external system item Select the relevant Alarm Zone.



External System Item 1 - Properties

General

Event Response

Alarm Instructions

Status and Overrides

Alarm Transmission

Setup

Trigger -- Outputs

Trigger -- Events

Reflected Outputs

Cameras

Icons

Notes

Action Plans

| Event Group | Action Plan |
|-------------------------|-------------------|
| External Event Group 0 | -- Use Default -- |
| External Event Group 1 | -- Use Default -- |
| External Event Group 2 | -- Use Default -- |
| External Event Group 3 | -- Use Default -- |
| External Event Group 4 | -- Use Default -- |
| External Event Group 5 | -- Use Default -- |
| External Event Group 6 | -- Use Default -- |
| External Event Group 7 | -- Use Default -- |
| External Event Group 8 | -- Use Default -- |
| External Event Group 9 | -- Use Default -- |
| External Event Group 10 | -- Use Default -- |
| External Event Group 11 | -- Use Default -- |
| External Event Group 12 | -- Use Default -- |

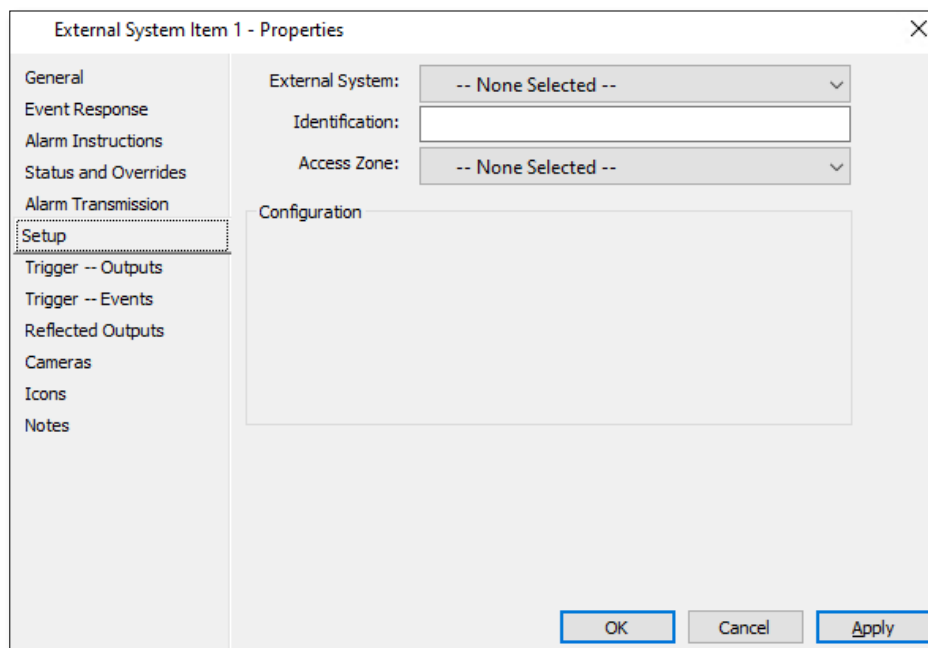
-- Use Default --

Alarm Zone for all Events: -- None Selected --

OK Cancel Apply

❖ Setup Tab

- Select relevant External System and Access Zone.
- Identification field - Give the same name as used in the External System Item Name field in the integration record.



External System Item 1 - Properties

General

Event Response

Alarm Instructions

Status and Overrides

Alarm Transmission

Setup

Trigger -- Outputs

Trigger -- Events

Reflected Outputs

Cameras

Icons

Notes

External System: -- None Selected --

Identification:

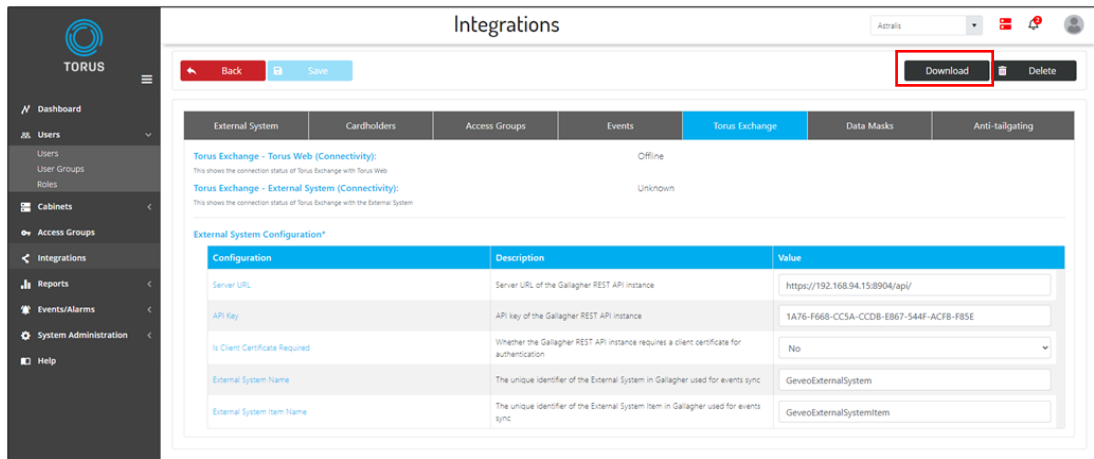
Access Zone: -- None Selected --

Configuration

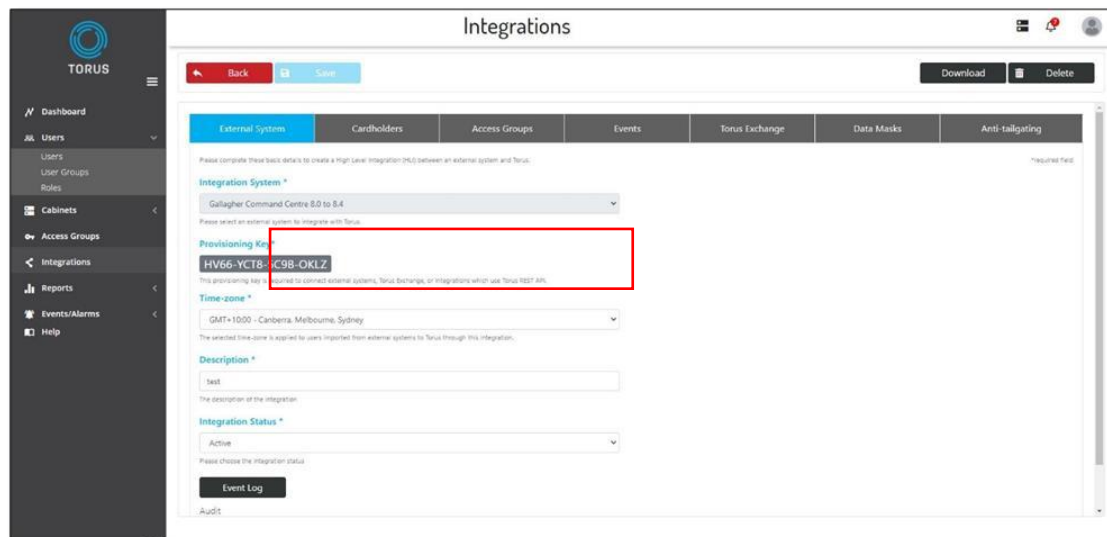
OK Cancel Apply

4 – INSTALL TORUS EXCHANGE


- After completing details for Torus Exchange, download Torus Exchange and install it on the Gallagher Command Centre Server.



- When Torus Exchange setup is executed the installation wizard will require a provisioning key which need to be copied from integration details page.



- Once Torus Exchange is installed, please verify the Torus Exchange services are running.
- After successful integration Torus shows the systems status as online in Torus Exchange tab.



Dashboard

Users

Users

User Groups

Roles

Cabinets

Access Groups

Integrations

Reports

Events/Alarms

System Administration

Help

Integrations

Back

Save

Download

Delete

| External System | Cardholders | Access Groups | Events | Torus Exchange | Data Masks | Anti-tailgating |
|---|-------------|---------------|--------|----------------|------------|-----------------|
| <div> <div>Torus Exchange - Torus Web (Connectivity):</div> <div>You attach the connection status of Torus Exchange with Torus Web.</div> <div>Offline</div> </div> | | | | | | |
| <div> <div>Torus Exchange - External System (Connectivity):</div> <div>You attach the connection status of Torus Exchange with the External System.</div> <div>Unknown</div> </div> | | | | | | |

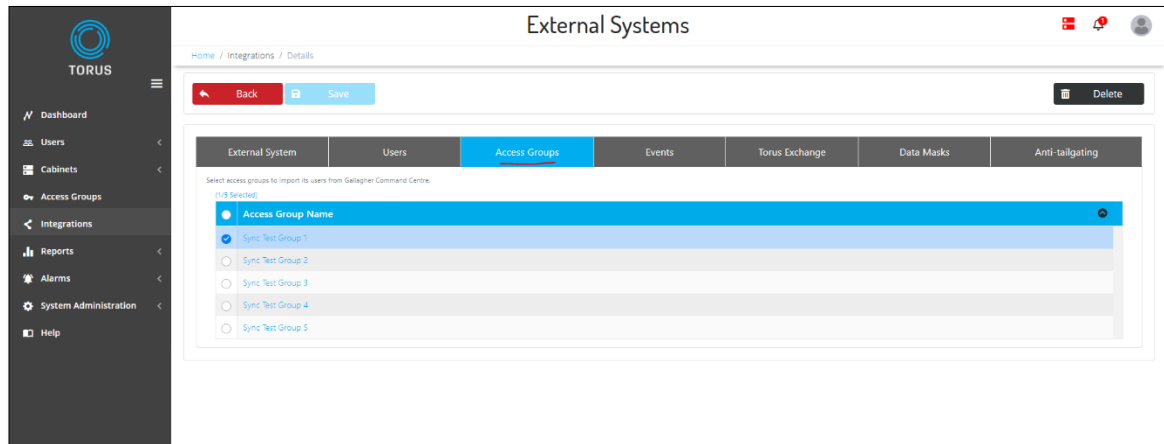
External System Configuration*

| Configuration | Description | Value |
|--------------------------------|--|--|
| Server URL | Server URL of the Gallagher REST API instance | <input type="text" value="https://192.168.94.15:8904/api/"/> |
| API Key | API key of the Gallagher REST API instance | <input type="text" value="1A76-F668-CC3A-CCDB-E867-5448-ACFB-F85E"/> |
| Is Client Certificate Required | Whether the Gallagher REST API instance requires a client certificate for authentication | <input type="text" value="No"/> |
| External System Name | The unique identifier of the External System in Gallagher used for events sync | <input type="text" value="GevecoExternalSystem"/> |
| External System Item Name | The unique identifier of the External System item in Gallagher used for events sync | <input type="text" value="GevecoExternalSystemItem"/> |

5 – COMPLETE USER SYNCHRONISATION SETTINGS

5.1 – Select Command Centre Access Groups in Torus

To import users in Torus from Command Centre, first select Command Centre's Access Group(s) in the Access Group tab.

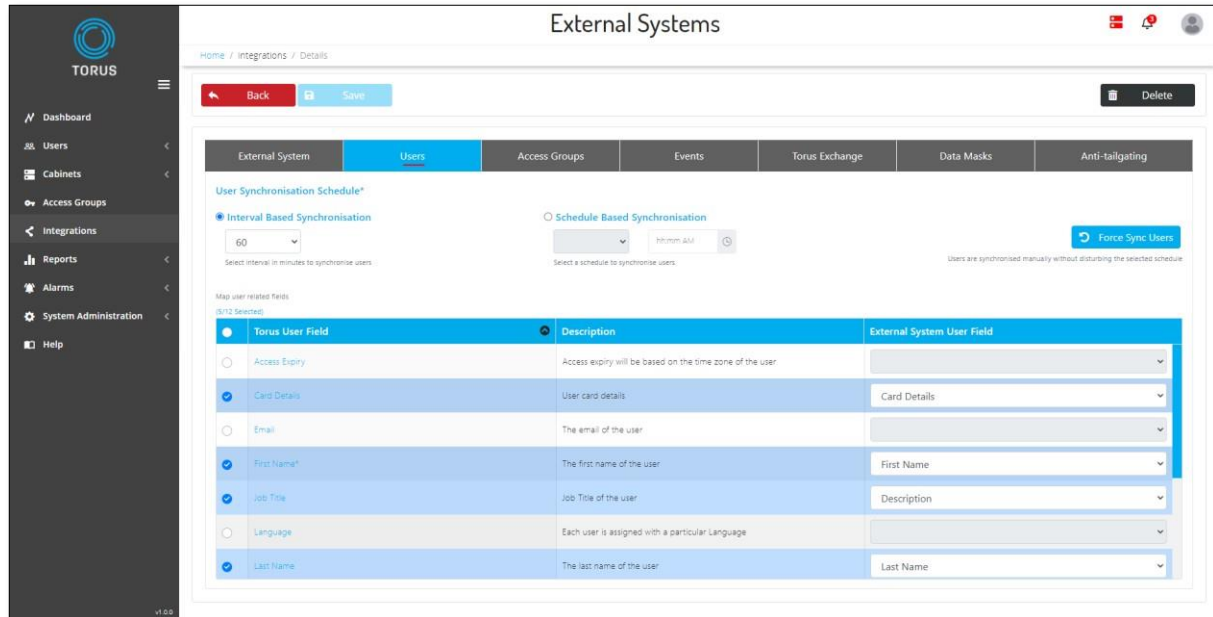


Torus only imports users which are part of Selected Access Group(s). Few important points to remember.

1. Torus only import users from Command Centre when its relative Command Centre's Access Group is selected in integration record.
2. Only selected Access Groups of Command Centre are imported to Torus and they are saved as USER GROUP in Torus.
3. If user deselects an Access Group in Access Group Tab and save the integration record, then its associated USER GROUP and USERS will be removed from Torus.
4. Access Groups are synchronised in real time with Command Centre which can result into following actions.
 - a. If Access Group name is edited in Command Centre, then corresponding USER GROUP name in Torus will also change accordingly.
 - b. If Access Group is deleted in Command Centre, then the respective USER GROUP in Torus will also be deleted, along with its corresponding imported users in Torus.

5.2 – Mapping of Command Centre User fields with Torus User fields

User's record field mapping is required to successfully import a user's record from Command Centre to Torus. By default, mandatory field mapping is created at the time of creation of integration record. User's field mapping can be configured in USERS tab.



Following are mandatory Torus User Fields which must have a corresponding Command Centre User Field.

| Torus User Field | Command Centre User Field |
|------------------|--|
| First Name | First Name |
| User Group | Access Group |
| Card Details | Card Details (Becomes mandatory when a Data Mask is selected in Data Mask tab) |

In this tab User Synchronisation Schedule can also be configured which will synchronise users records with Command Centre on selected schedule. This schedule is only executed once at least one Access Group is selected in the Access Group tab. User must select a User Synchronisation Schedule to keep the user's record updated as per Command Centre user's record.

| User Synchronisation Schedule | Description |
|--------------------------------|--|
| Interval Based Synchronisation | An iterative time interval-based user synchronisation. There is an option of Real Time sync among |

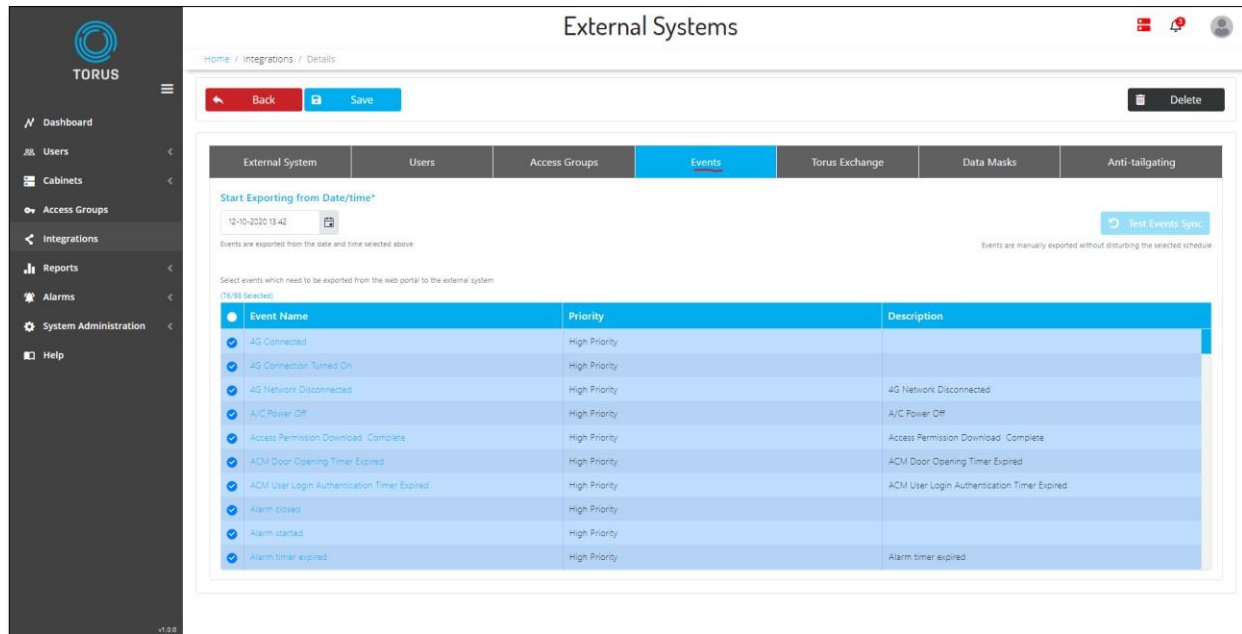
| | |
|--------------------------------|---|
| | the options if real time synchronisation is required. |
| Schedule Based Synchronisation | A weekly schedule in which user must select Date/Time to synchronise users. |

Force Sync Users is an option which can be used to synchronise the users as without disturbing the selected User Synchronisation Schedule. When this option is selected then system will perform a force user synchronisation, which is often a handy way to test the user synchronisation between Torus and Command Centre.

6 – SELECT EVENTS FOR EXPORT

Torus cabinet events can be exported to Command Centre through Torus Exchange. Users can select the required events which need to be exported from Torus to Command Centre. This events configuration can be completed in Events tab. User must select a Start date/time and all events after selected date/time are exported to Command Centre.

Test Events Synchronisation button can be used to send test events to Command Centre and button gets enabled once Torus Exchange setup is completely configured and Integration Status is Active.



Home / Integrations / Details

Back Save Delete

External System Users Access Groups **Events** Torus Exchange Data Masks Anti-tailgating

Start Exporting from Date/time*

12-10-2020 13:42

Events are exported from the date and time selected above

Test Events Sync

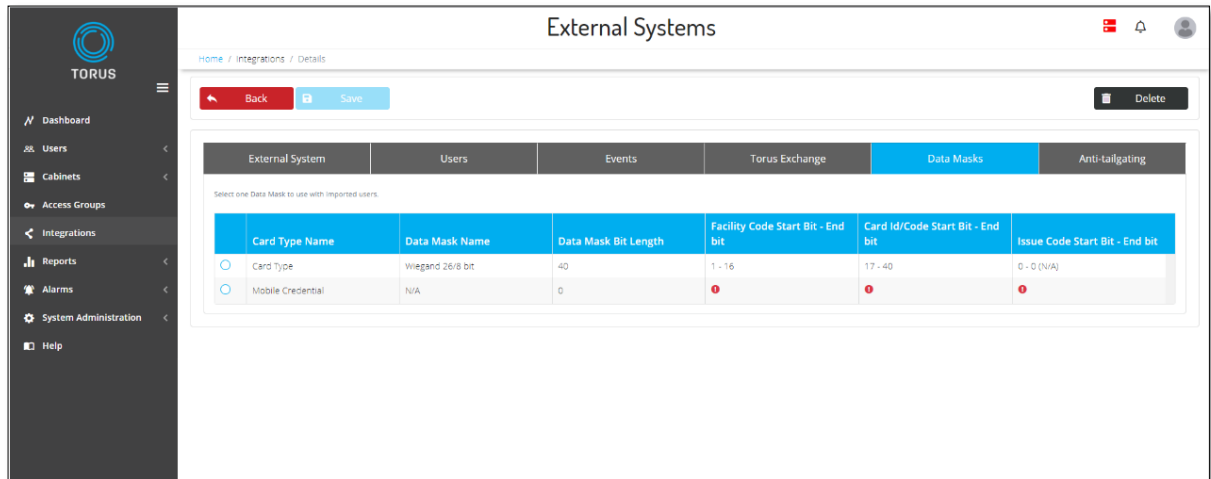
Events are manually exported without disturbing the selected schedule

Select events which need to be exported from the web portal to the external system
(16/16 Selected)

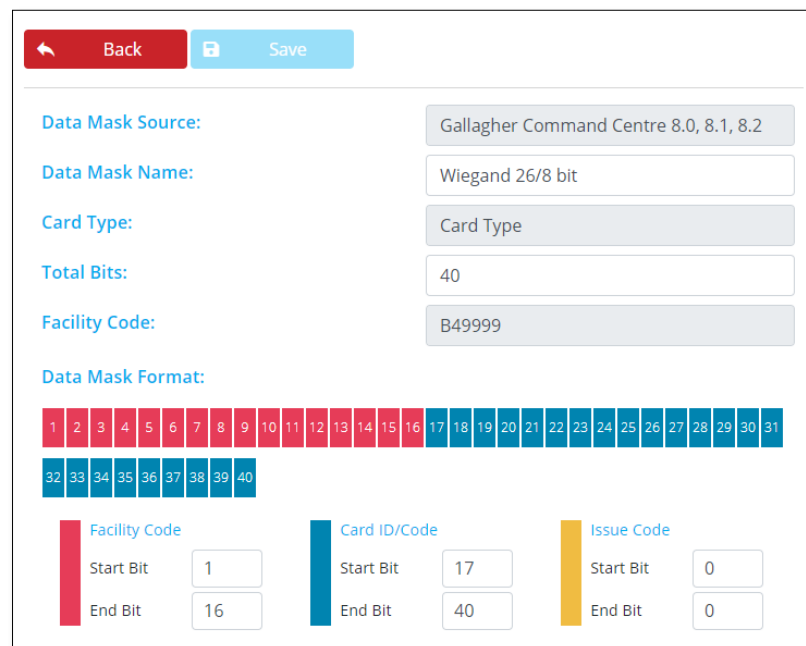
| Event Name | Priority | Description |
|---|---------------|---|
| 4G Connected | High Priority | |
| 4G Connection Turned On | High Priority | |
| 4G Network Disconnected | High Priority | 4G Network Disconnected |
| A/C Power Off | High Priority | A/C Power Off |
| Access Permission Download Complete | High Priority | Access Permission Download Complete |
| ACM Door Opening Timer Expired | High Priority | ACM Door Opening Timer Expired |
| ACM User Login Authentication Timer Expired | High Priority | ACM User Login Authentication Timer Expired |
| Alarm closed | High Priority | |
| Alarm started | High Priority | |
| Alarm timer expired | High Priority | Alarm timer expired |

7 – DATA MASK SETUP

Once the integration is successfully configured Torus automatically imports Data Mask definitions from Gallagher Command Centre. Imported data masks are listed under Data Masks tab in Torus for Integrیتی integration.



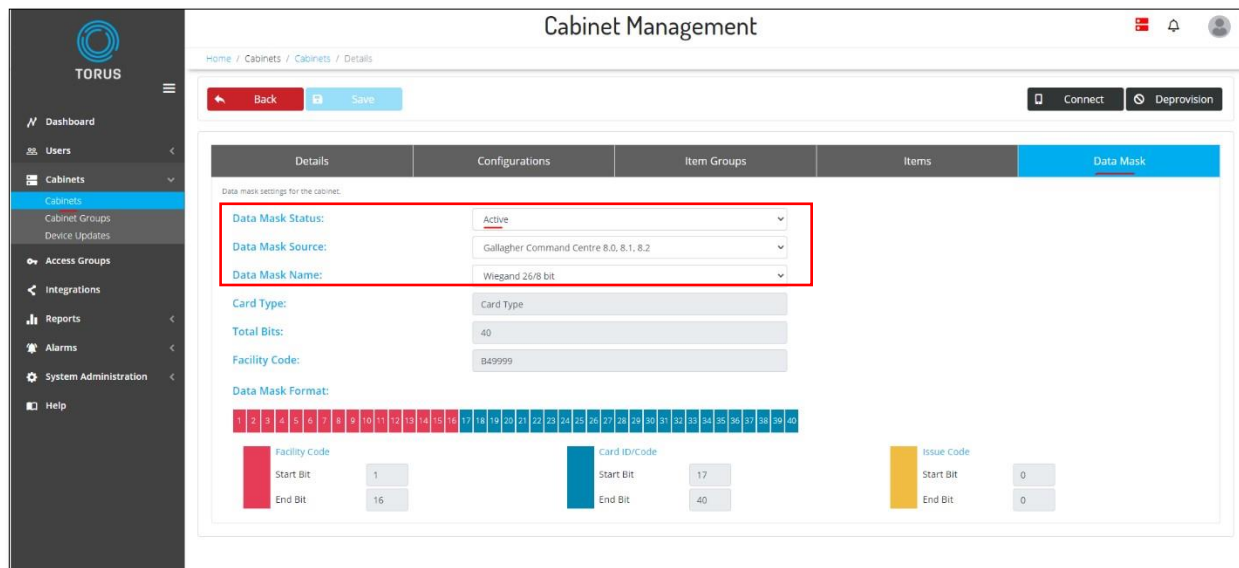
User can compare the Data Mask configuration with Gallagher Command Centre and can edit Data Mask details in Torus.



The screenshot shows the Data Mask configuration form in Torus. The form includes the following fields and sections:

- Data Mask Source:** Gallagher Command Centre 8.0, 8.1, 8.2
- Data Mask Name:** Wiegand 26/8 bit
- Card Type:** Card Type
- Total Bits:** 40
- Facility Code:** B49999
- Data Mask Format:** A visual representation of the 40-bit format, showing bits 1-16 in red (Facility Code), bits 17-40 in blue (Card ID/Code), and bits 0-0 in yellow (Issue Code).
- Facility Code:** Start Bit: 1, End Bit: 16
- Card ID/Code:** Start Bit: 17, End Bit: 40
- Issue Code:** Start Bit: 0, End Bit: 0

A Data Mask can be applied to cabinet from cabinet configurations in Torus. Go to cabinet record in Torus and select the correct Data Mask source from drop down and select relevant integration record and relevant data mask name.

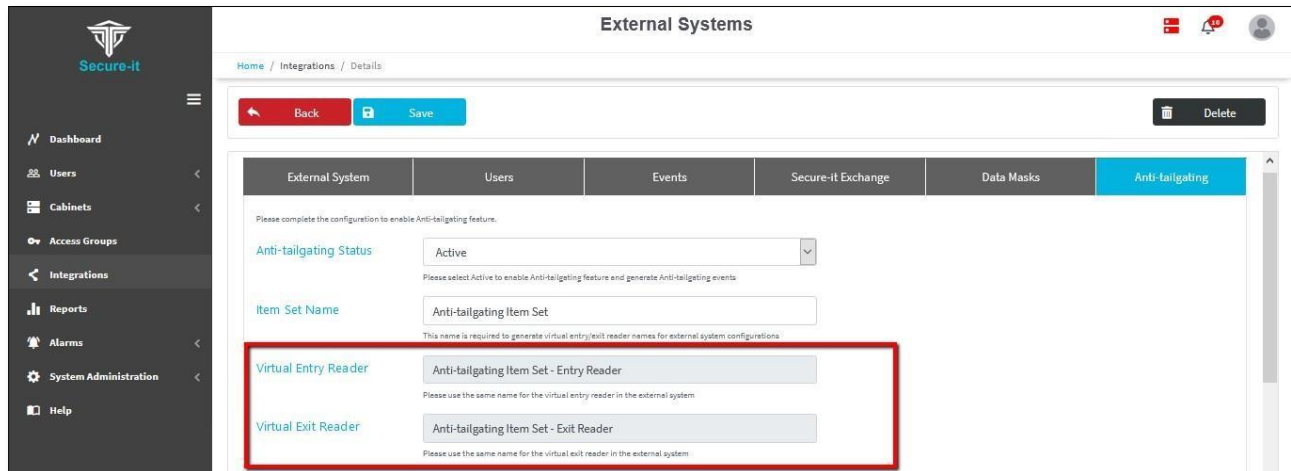


The screenshot shows the 'Cabinet Management' interface in the Torus application. The left sidebar contains navigation links: Dashboard, Users, Cabinets, Cabinet Groups, Device Updates, Access Groups, Integrations, Reports, Alarms, System Administration, and Help. The main content area is titled 'Cabinet Management' and has a breadcrumb trail: Home / Cabinets / Cabinets / Details. Below the breadcrumb are 'Back' and 'Save' buttons. On the right, there are 'Connect' and 'Deprovision' buttons. The interface is divided into tabs: Details, Configurations, Item Groups, Items, and Data Mask (which is currently selected). The 'Data Mask' tab displays the following settings:

- Data Mask Status:** Active (dropdown menu)
- Data Mask Source:** Gallagher Command Centre 8.0, 8.1, 8.2 (dropdown menu)
- Data Mask Name:** Wiegand 26/8 bit (dropdown menu)
- Card Type:** Card Type (text input)
- Total Bits:** 40 (text input)
- Facility Code:** B49999 (text input)
- Data Mask Format:** A visual representation of the 40-bit format, showing bit positions 1 through 40. Bits 1-16 are red, 17-32 are blue, and 33-40 are yellow.
- Facility Code:**
 - Start Bit: 1
 - End Bit: 16
- Card ID/Code:**
 - Start Bit: 17
 - End Bit: 40
- Issue Code:**
 - Start Bit: 0
 - End Bit: 0

8 – ANTI-TAILGATING SETUP

- Anti-tailgating is an optional feature which stops a user to leave the building until the keys are returned to Torus key cabinet.
- For this feature it is mandatory that the building has setup exit card reader at the main exit of the building.
- User needs to define item set name and select the items on which anti-tailgating feature is required. These configurations can be completed from Anti-Tailgating Tab.
- To setup anti tailgating, create two more external items which are virtual entry and exit readers.
- A virtual zone is also required to virtually place the Torus cabinets inside this Virtual Zone.
- For each external item identification field please use the names as shown in Torus External system entry and exit reader names in the anti- tailgating tab of the integration record.

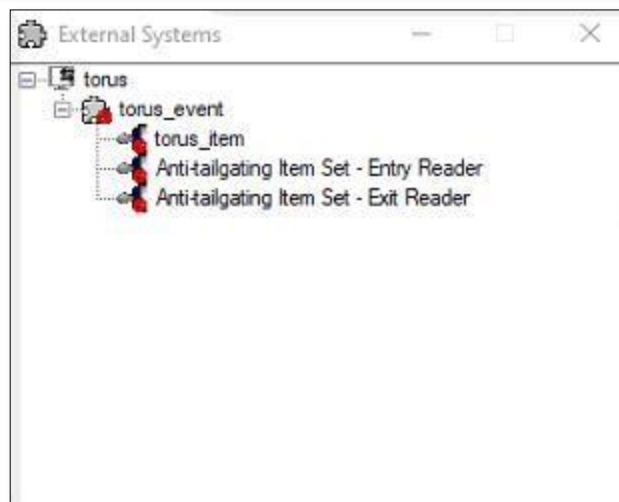


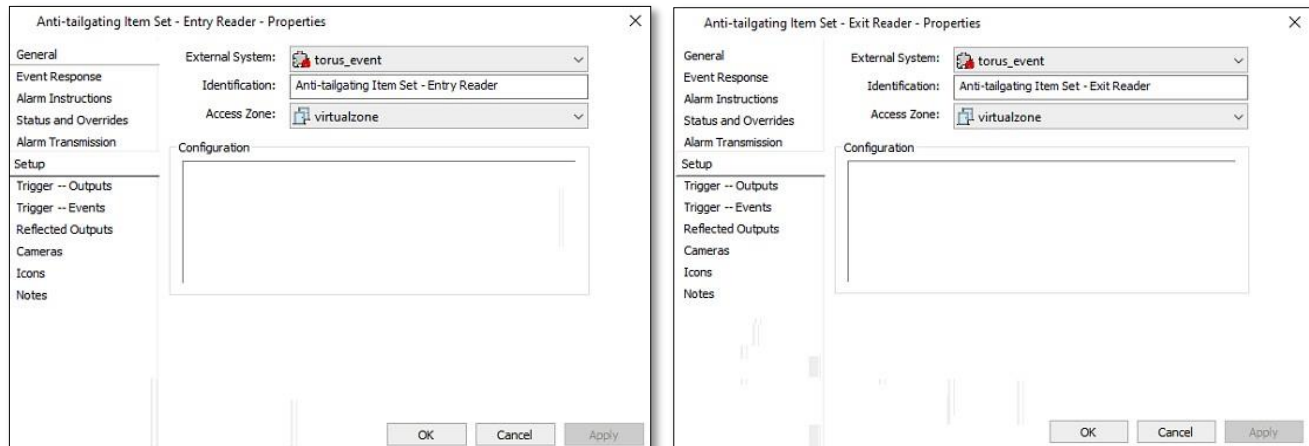
External Systems

Home / Integrations / Details

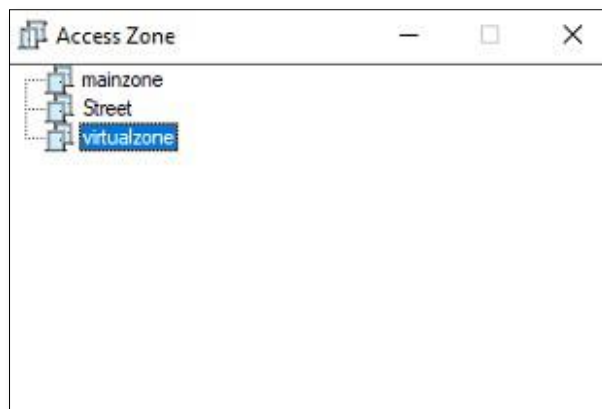
Back Save Delete

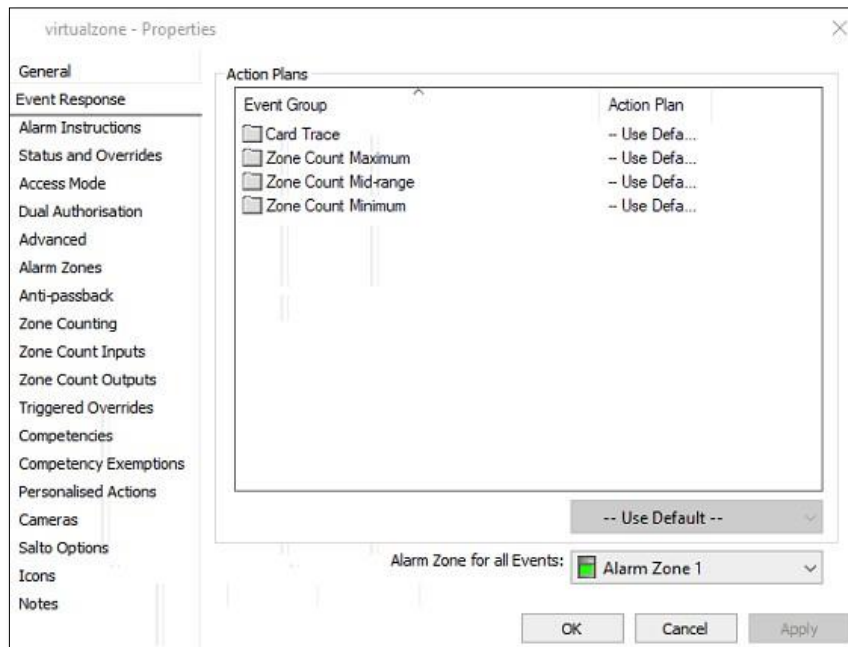
| External System | Users | Events | Secure-It Exchange | Data Masks | Anti-tailgating |
|--|---|--------|--------------------|------------|-----------------|
| Please complete the configuration to enable Anti-tailgating feature: | | | | | |
| Anti-tailgating Status | Active | | | | |
| Please select Active to enable Anti-tailgating feature and generate Anti-tailgating events | | | | | |
| Item Set Name | Anti-tailgating Item Set | | | | |
| This name is required to generate virtual entry/exit reader names for external system configurations | | | | | |
| Virtual Entry Reader | Anti-tailgating Item Set - Entry Reader | | | | |
| Please use the same name for the virtual entry reader in the external system | | | | | |
| Virtual Exit Reader | Anti-tailgating Item Set - Exit Reader | | | | |
| Please use the same name for the virtual exit reader in the external system | | | | | |



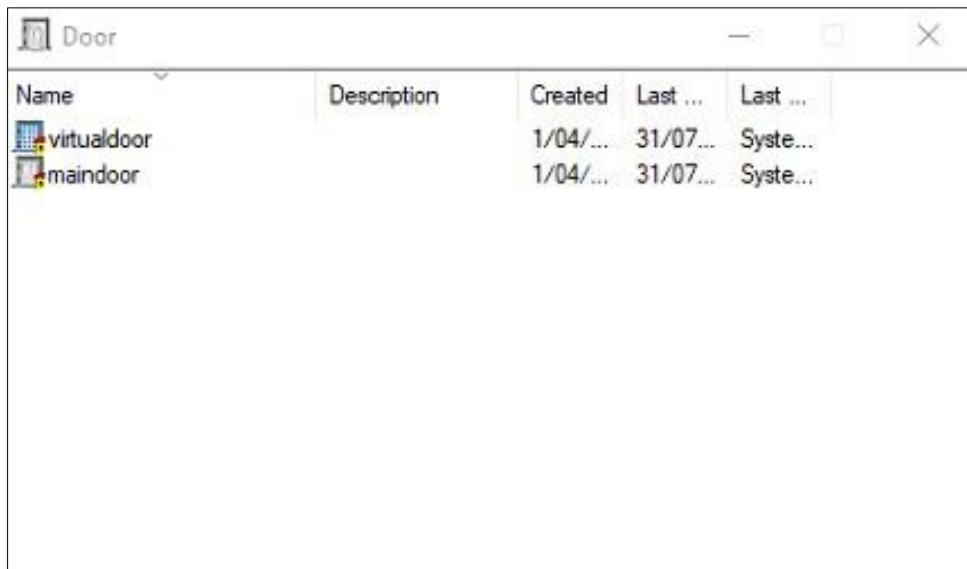


- Create a Virtual Zone and select the correct Alarm Zone for all events. Go to Gallagher Command Centre, configure>Access Zones and create a virtual Zone.

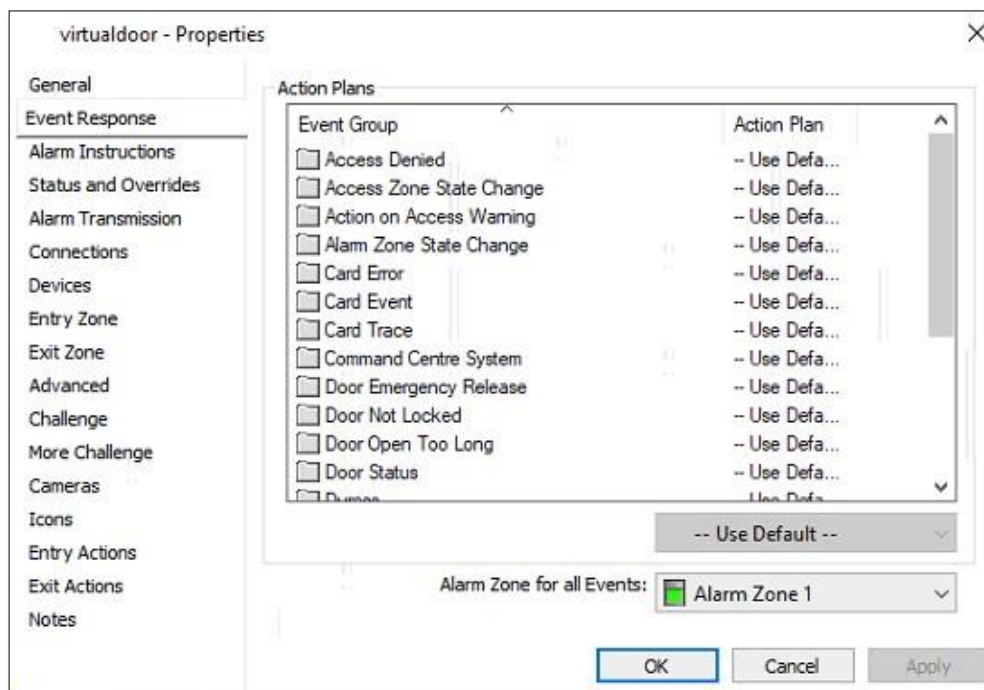




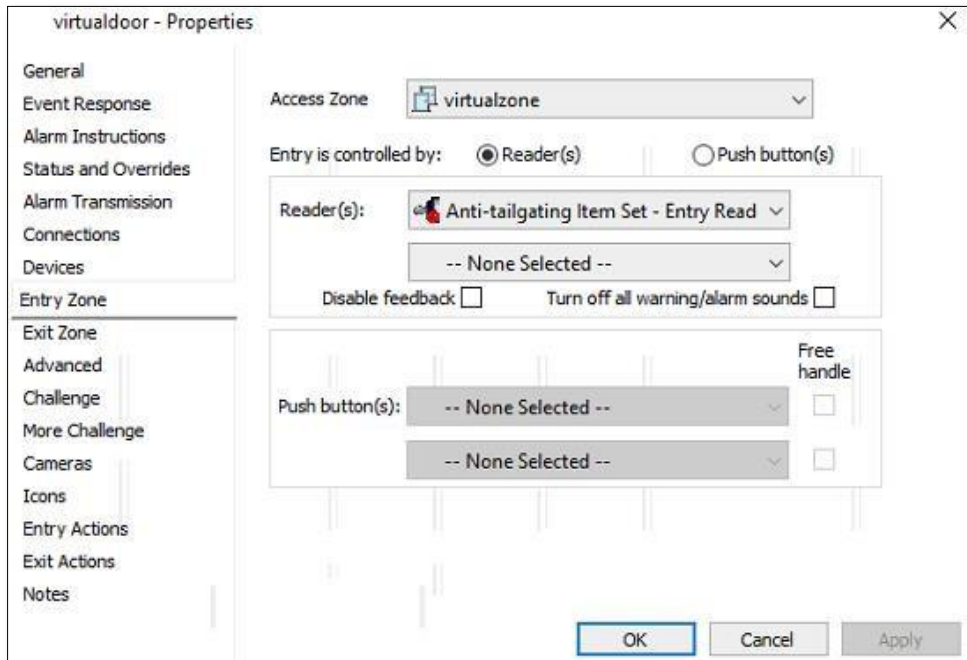
- For Anti-Tailgating, a virtual door is required. Go to Gallagher Command Centre, Configure >Door and create a virtual door.



- Use correct Alarm Zone for all events.



- Use Virtual Zone to link it with Virtual Door's Entry Zone >Access Zone
- In the Virtual door Entry Zone Reader use Anti-Tailgating virtual entry reader



virtualdoor - Properties

General

Event Response

Alarm Instructions

Status and Overrides

Alarm Transmission

Connections

Devices

Entry Zone

Exit Zone

Advanced

Challenge

More Challenge

Cameras

Icons

Entry Actions

Exit Actions

Notes

Access Zone: virtualzone

Entry is controlled by: ☒ Reader(s) ☐ Push button(s)

Reader(s): Anti-tailgating Item Set - Entry Read

-- None Selected --

Disable feedback ☐ Turn off all warning/alarm sounds ☐

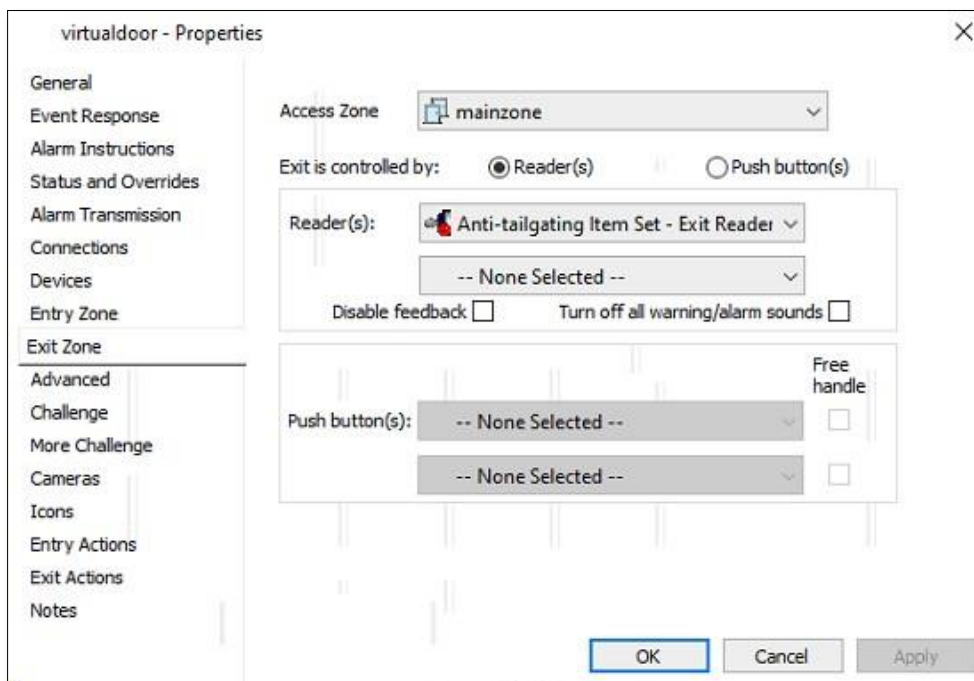
Push button(s): -- None Selected --

-- None Selected --

Free handle ☐

OK Cancel Apply

- Use Main Zone to link it with Virtual Door's Exit Zone >Access Zone
- In the Virtual door Exit Zone Reader use Anti-Tailgating virtual exit reader



virtualdoor - Properties

General

Event Response

Alarm Instructions

Status and Overrides

Alarm Transmission

Connections

Devices

Entry Zone

Exit Zone

Advanced

Challenge

More Challenge

Cameras

Icons

Entry Actions

Exit Actions

Notes

Access Zone: mainzone

Exit is controlled by: ☒ Reader(s) ☐ Push button(s)

Reader(s): Anti-tailgating Item Set - Exit Reader

-- None Selected --

Disable feedback ☐ Turn off all warning/alarm sounds ☐

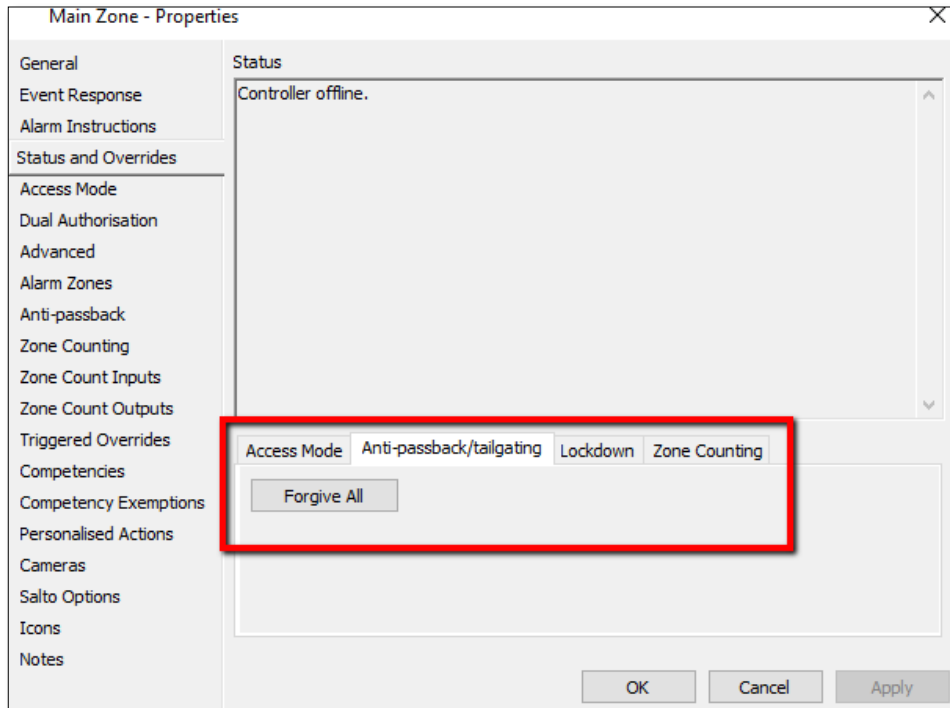
Push button(s): -- None Selected --

-- None Selected --

Free handle ☐

OK Cancel Apply

Note - If alarms still sound when you try to access with an authorized user after correctly setting up, Go to Configure > Access Zones and select the relevant access zone, go to Status and Overrides tab > Anti-



passback/tailgating tab > and click 'Forgive All' button.

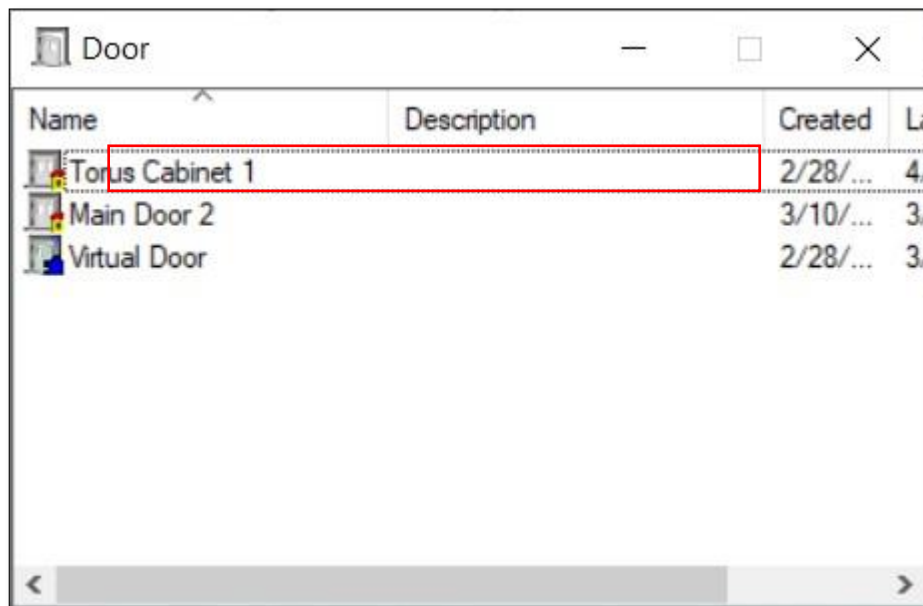
9 – CARD HOLDER LOGIN AT TORUS CABINET VIA REST API ALARMS & EVENTS

Gallagher Command Centre's REST API Alarms & Events is used to enable card holders to login at Torus cabinet when Gallagher card reader is not wired directly with Torus cabinet. In this type of setup Gallagher Card reader is physically mounted on Torus cabinet but it is directly wired with Gallagher Controller.

In this type of setup Card holders data is imported to Torus software and card holder need to be added in Access Group of Torus software to grant access on any item(s) in Torus cabinet. However, this type of card holder record does not need the card details imported to Torus software since the authentication at cabinet card reader is performed by Gallagher Controller. Furthermore, there is no need to configure any data mark on the cabinet where the card reader is connected with Gallagher Controller for this type of setup. This feature allows card or Gallagher mobile connect users to use their credentials at card readers mounted at Torus cabinet.

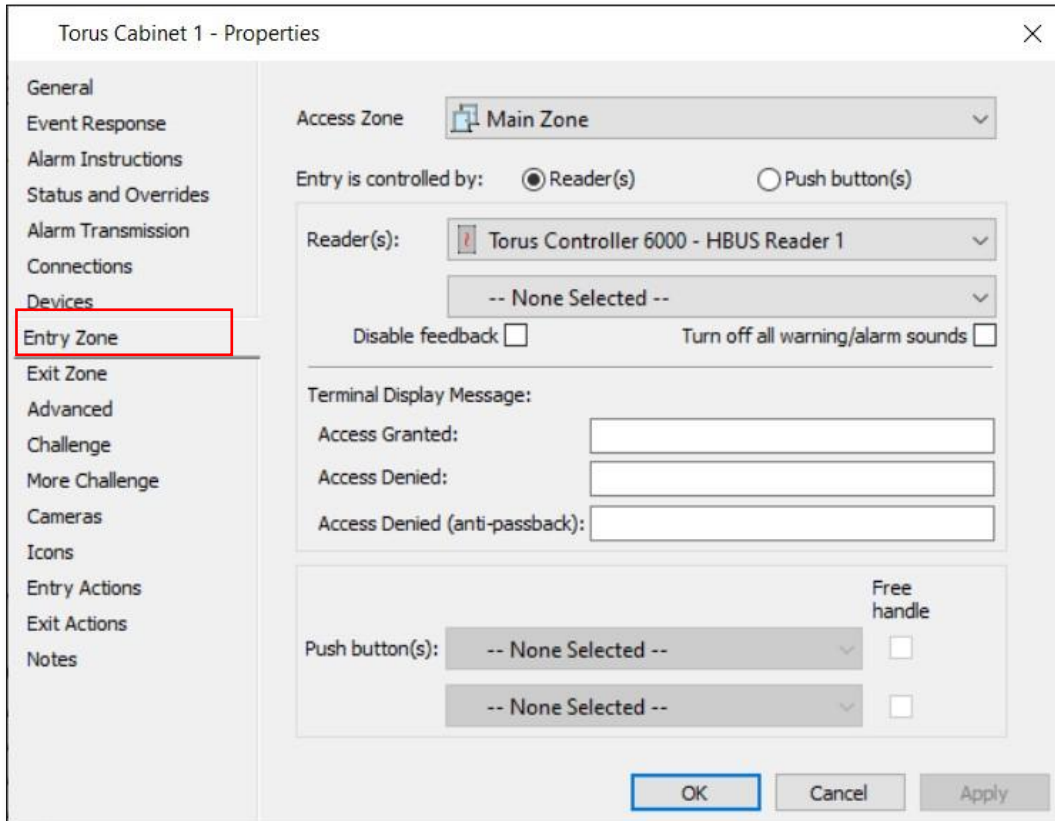
9.1 – Create Door in Command Centre

- Install the Gallagher card reader at Torus cabinet but do not wire it with Torus cabinet CU.
- Connect this Gallagher card reader with Gallagher Controller.
- Create a door record in Command centre.



| Name | Description | Created | Last |
|-----------------|-------------|----------|-------|
| Torus Cabinet 1 | | 2/28/... | 4:... |
| Main Door 2 | | 3/10/... | 3:... |
| Virtual Door | | 2/28/... | 3:... |

- Go to door properties and configure the Entry Zone for the card reader. Use any existing zone or create a new Access Zone for this door.



Torus Cabinet 1 - Properties

General
Event Response
Alarm Instructions
Status and Overrides
Alarm Transmission
Connections
Devices
Entry Zone
Exit Zone
Advanced
Challenge
More Challenge
Cameras
Icons
Entry Actions
Exit Actions
Notes

Access Zone: Main Zone

Entry is controlled by: ☒ Reader(s) ☐ Push button(s)

Reader(s): Torus Controller 6000 - HBUS Reader 1
-- None Selected --

Disable feedback ☐ Turn off all warning/alarm sounds ☐

Terminal Display Message:

Access Granted:
Access Denied:
Access Denied (anti-passback):

Push button(s): -- None Selected -- ☐ Free handle
-- None Selected -- ☐

OK Cancel Apply

9.2 – Map Door with Torus cabinet

- In last step Command Centre door record has to be mapped with Torus cabinet.
- Open Torus software and go to integration record of Gallagher Command Centre.
- Go to External System Devices tab to input door name which is linked with Gallagher Card Reader mounted at corresponding cabinet.
- Add imported users to respective Access groups to grant access on desired items in Torus cabinet.

Dashboard

Users

Cabinets

Access Groups

Integrations

Reports

Events/Alarms

Help

Integrations

BackSaveDownloadDelete

External SystemCardholdersAccess GroupsEventsTorus ExchangeData MasksAnti-tailgatingDevice Mappings

Please complete the device mappings with cabinets. This allows a physical mapping between a device and cabinet, in case external devices are not wired with the cabinet.

Map a cabinet with the correct card/fingerprint reader, or any other external device mounted on the cabinet.

| Cabinet Name | Size | Site | External System Device |
|--------------------------|------|--------------------|------------------------|
| 5 Keys Cabinet | 5 | Test Site | Torus Cabinet 1 |
| Demo cabinet | 50 | Test Site | Torus Cabinet 2 |
| NIM's SK UAT | 5 | Test Site | Torus Cabinet 3 |
| Murthy 5 U3 keys cabinet | 5 | Murthy Home Office | Torus Cabinet 4 |
| test cabinet 2 | 5 | Test Site | Torus Cabinet 5 |

End of Document



15/39 Herbert Street, St Leonards, NSW – 2065.

www.cictechnology.com