

Integration with Gallagher Command Centre



TORUS

<https://torus-technology.com>

Document details

Title	Integration with Gallagher Command Centre
Description	This document explains the steps to create integration between Torus and Gallagher Command Centre 8.6 and above.

Document Revision History

Version	Date	Author	Comments
V.1.0	October 09, 2023	AA	First Draft
V.1.1	November 03, 2023	TL	Minor edits
V.1.2	December 05, 2023	AA	Updated details in prerequisites sections including support for both online and onsite authentication options

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 Pty Ltd (Torus). 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 Pty Ltd.

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 Pty Ltd, and you may not sell it without permission. CIC Technology Pty Ltd 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 Pty Ltd, 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 Pty Ltd. Please be aware that disclosure, copying, distribution or use of this document and the information contained therein is strictly prohibited.

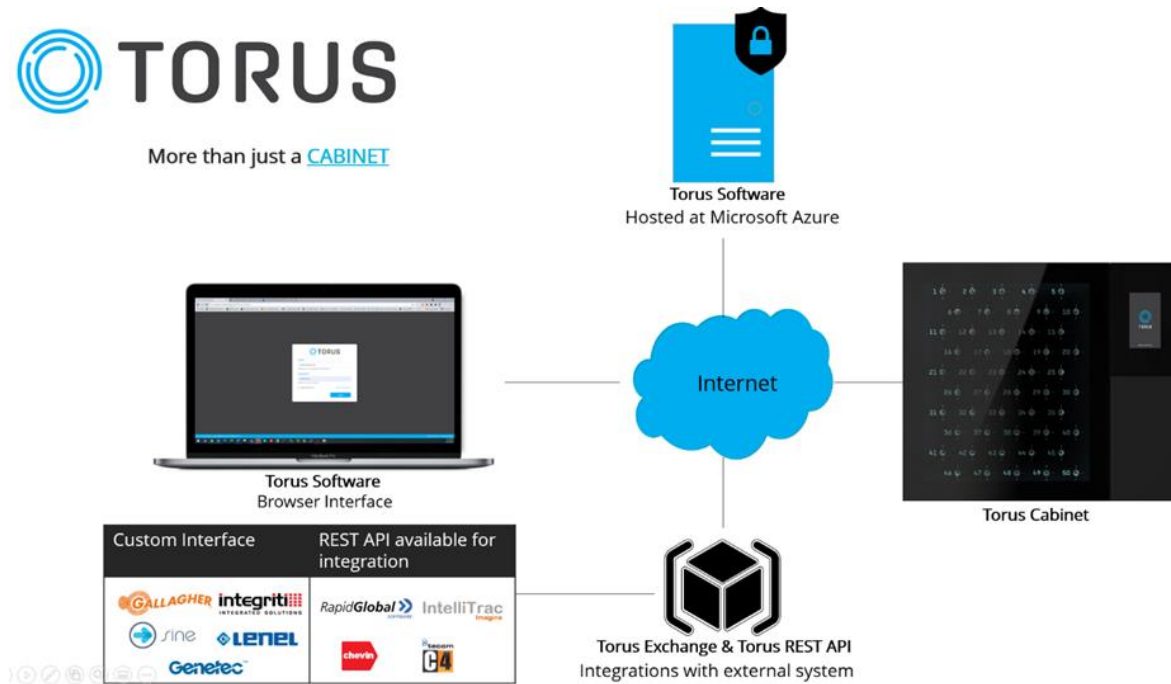
CONTENTS

TORUS INTEGRATIONS	6
GALLAGHER COMMAND CENTRE HLI	7
Torus Exchange prerequisites	7
Command Centre setup prerequisites	10
Integration overview	12
STEPS FOR INTEGRATION	13
1 – CREATE INTEGRATION RECORD	13
2 – CONFIGURE COMMAND CENTRE REST API	14
3 – INSTALL TORUS EXCHANGE	17
4 – COMPLETE USER SYNCHRONISATION SETTINGS	19
4.1 – Select Command Centre Access Groups in Torus	19
4.2 – Mapping of Command Centre User fields with Torus User fields	20
4.3 – Cardholder Synchronisation	22
5 – EVENTS EXPORT SETUP	23
6 – GRANTING CARDHOLDER ACCESS TO KEYS IN TORUS CABINETS	26
6.1 – Granting access to keys to an imported user	26
6.2 – Granting access to keys to users using Command Centre Access Group	27
7 – CARDHOLDER LOGIN AT TORUS CABINET	30
7.1 – Option 1 : When Card reader is connected with Torus Cabinet	30
7.2 – Option 2 : When Card reader is connected with Command Centre	33
7.2.1 – Create Door in Command Centre	34
7.2.2 – Map Door with Torus cabinet	36
8 – ANTI-TAILGATING SETUP	37
8.1 – Create an External System Server in Command Centre	37
8.2 – Create an External System in Command Centre	39
8.3 – Create an External System Item in Command Centre	41
8.4 – Create virtual entry and exit readers in Command Centre	44
8.5 – Create virtual zone in Command Centre	45
8.6 – Create virtual door in Command Centre	47

TORUS INTEGRATIONS

Torus provides an easy and simple way to integrate with 3rd party software. The intention is to remove the complexities involved in building HLI. Torus Exchange is utilised to provide a custom integration with **Gallagher Command Centre** which is an enterprise grade Access Control System.

The Torus HLI enables customers to import cardholder details from **Gallagher Command Centre** into Torus. This HLI exports Torus cabinet events and alarms to OnGuard. This enables customers to utilise **Gallagher Command Centre** as a single source of truth for their cardholder and key management.

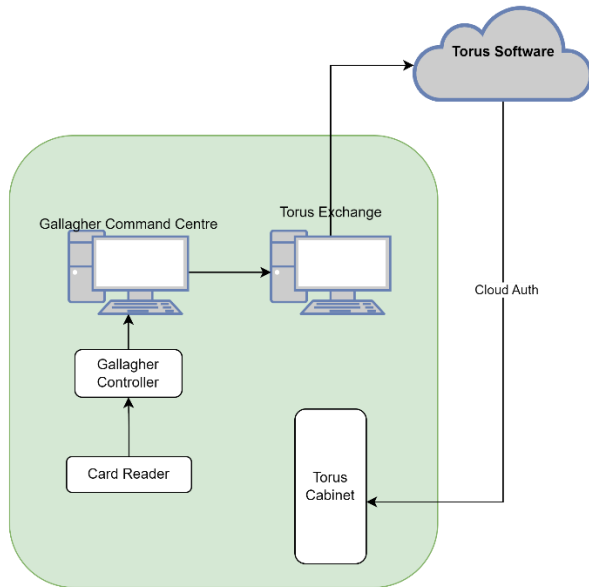


GALLAGHER COMMAND CENTRE HLI

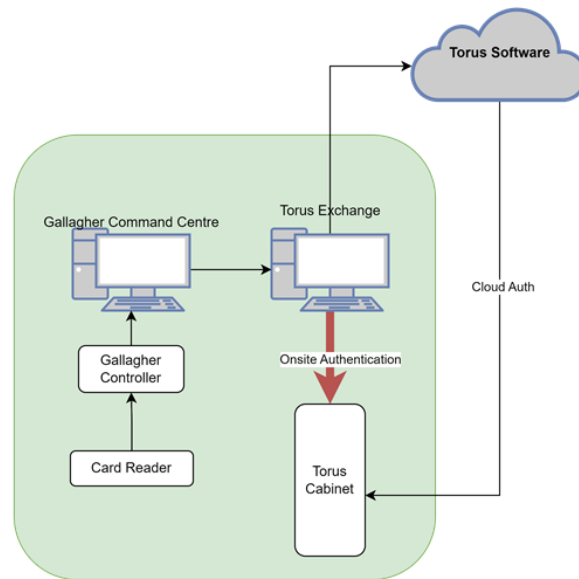
For Command Centre integration Torus utilises a middleware application called Torus Exchange which is a Windows plugin supporting integration with Command Centre Version 8.6 and above.

Torus and Gallagher Command Centre integration supports Online or Onsite authentication of user credentials as outlined with the below two options which are further detailed below.

Online Authentication



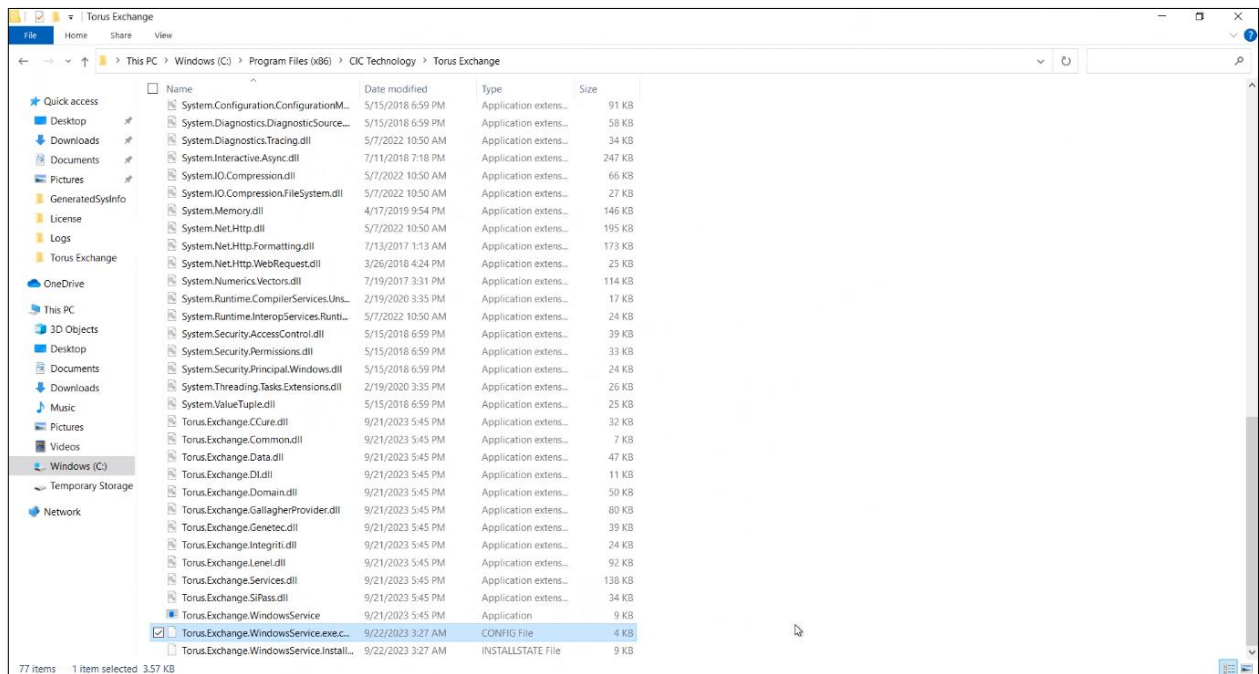
Onsite Authentication



Torus Exchange prerequisites

- Integration record created in Torus software.
- 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.
- Torus Exchange **Version 1.1.10** or above, is required for this setup. Download latest version from integration record in Torus software.
- Torus Exchange must be allowed to access required URL & port in server and network firewall. These are required for Torus Exchange to establish connection with Torus software.
 - URL= <https://hliapi-au.Torus-technology.com>
 - Port: 443 over HTTPS
- **Online Authentication - Card Reader connected using a Wiegand Protocol Converter.**
 - Option 1 is required when data-mask and cardholder's card data is imported to Torus and enforced on cabinet card reader for cardholder authentication.
 - In this type of setup cardholder authentication at Torus cabinet is performed by Torus Cabinet.

- Online Authentication – Card Reader wired to Gallagher Controller. This option is required to support Gallagher Mobile Connect and the Onsite Authentication capability.
 - Option 2 is required when data-mask and cardholder's card data is not imported to Torus cabinet. Cardholder authentication at Torus cabinet is performed by Gallagher Controller.
 - Torus Exchange establishes direct communication with the Cabinet over LAN-based message routing. This avoids the risk of any WAN latency, which may hinder real-time access to keys.
 - Following are the steps which need to be performed:-
 - Torus Cabinet IP's must be accessible from the server where Torus Exchange is installed. (Ping test can be used to verify this connectivity)
 - Server IP where Torus Exchange is installed should be accessible from all cabinet's in the network. (Ping test can be used in any device within site where device must be connected with LAN to verify this connectivity)
 - Allow port **49856 TCP/UDP** in LANs/vLANs/Firewall for communication between Torus cabinets and Torus Exchange. *(Note: If this port is not available for Torus Exchange in the host server, then after installation Torus Exchange windows services will not start. However, this Port is a configuration value and can be updated in the Torus Exchange file in server. To update this port open file Torus Exchange config in Notepad. File location is Program files (x86) > CIC Technology > Torus Exchange.*



- Before editing the port number please stop Torus Exchange services.
- Edit the port value for key = "CabinetLogineventPortNumber", and after editing the port save the file and start Torus Exchange service.

```

<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="AuthKey" value="OEH8-9MSY-3YNZ-R6BE" />
    <!--<add key="ApiUrl" value="http://localhost:7073/api/" />-->
    <!--<add key="ApiUrl" value="https://dev-apim-au.torus-technology.com/generic/api/">-->
    <!-- <add key="ApiUrl" value="https://uat-apim-au.torus-technology.com/generic/api/" /> -->
    <add key="ApiUrl" value="https://apim-au.torus-technology.com/generic/api/" />
    <add key="BatchSize" value="200" />
    <add key="PollingIntervalInSeconds" value="30" />
    <add key="InactiveIntegrationPollingIntervalInSeconds" value="60" />
    <add key="DataSyncIntervalInSeconds" value="10" />
    <add key="LoginEventDelayInMilliseconds" value="200" />
    <add key="ErrorRetryDelayInMilliseconds" value="10000" />
    <add key="ContinueDelayInMilliseconds" value="10000" />
    <add key="CabinetLoginEventPortNumber" value="49856" />
    <add key="SiPassCardholderGetBatchSize" value="200" />
    <add key="OnSiteAuthBindingDelayInMilliseconds" value="5000" />
    <add key="CCureClientVersion" value="3.0" />
    <add key="GallagherEventTypeGroup" value="Torus Event Group" />
    <add key="GallagherEventType" value="Torus Events" />
  </appSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
  </startup>

```

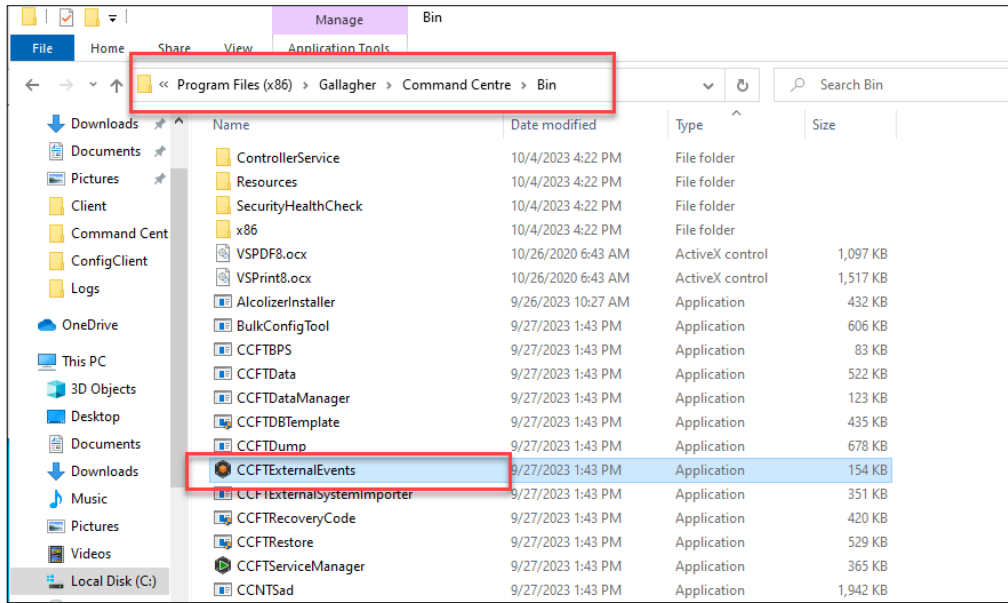
Command Centre setup prerequisites

- REST client setup in Command Centre to generate an API Key. This API key is required by Torus Exchange.
 - Operator who creates REST Client (API Key) in Command Centre must have privileges to utilise the required endpoints for integration.
- Hardware, access zones, alarm zones, and doors correctly setup in Command Centre.
- Install Cardax API in the same PC where the Torus Exchange middleware service is installed. (*only required for Anti-Tailgating feature*)
 - The hardware (controller) should be functioning properly in Command Centre (Go to Configure > Hardware > right click Properties > Status and overrides and verify that status is 'Normal')

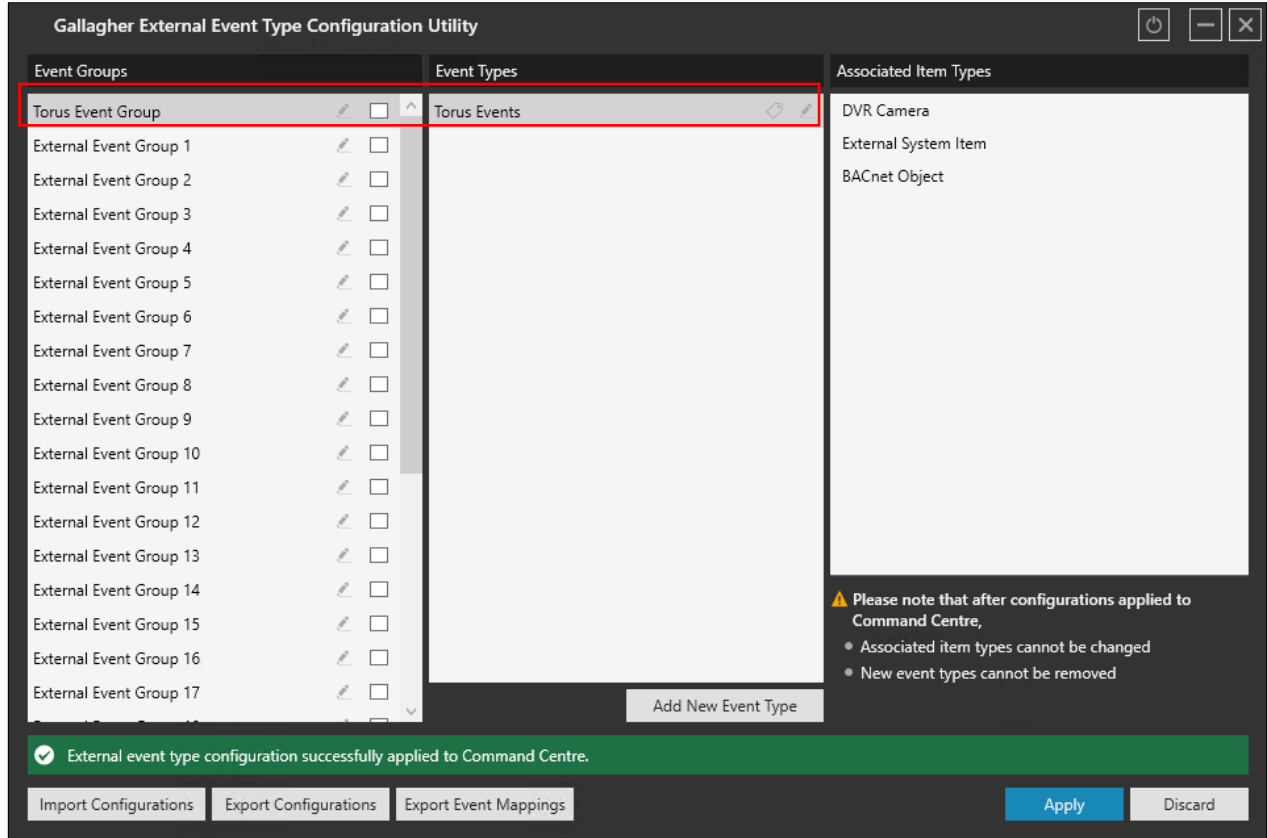
Mandatory licensed features in Command Centre V8.6 and above.

Gallagher License Feature	Gallagher Feature SKU	Gallagher API	Purpose	Gallagher REST API Endpoint used by Torus Exchange
RESTEvents	Alarms and Events REST API (C12772)	Event Alarm	Get card events updates (kind of subscription)	GET /api/events/updates
			Export Torus events and alarms	GET /api/events/groups
RESTCreateEvents	Inbound Events REST API (C12820)		Export Torus events and alarms (<i>Please note this is a separate feature in command centre license.</i>)	POST /api/events
RESTStatus	Status REST API (C12810)	Status and overrides	Get door IDs to export Torus events and to filter card events	GET /api/doors
RESTOverrides	Overrides REST API (C12812)			
RESTCardholders	Cardholder REST API (C12784)	Cardholder	Get Data masks	GET /api/card_types
			Get Access groups	GET /api/access_groups
			Get Cardholders	GET /api/access_groups/{id}/cardholders
			Get Cardholders	GET /api/cardholders/{id}
FTCAPI	FTCAPI	Controller API	Anti Tailgating feature.	implemented through external system item

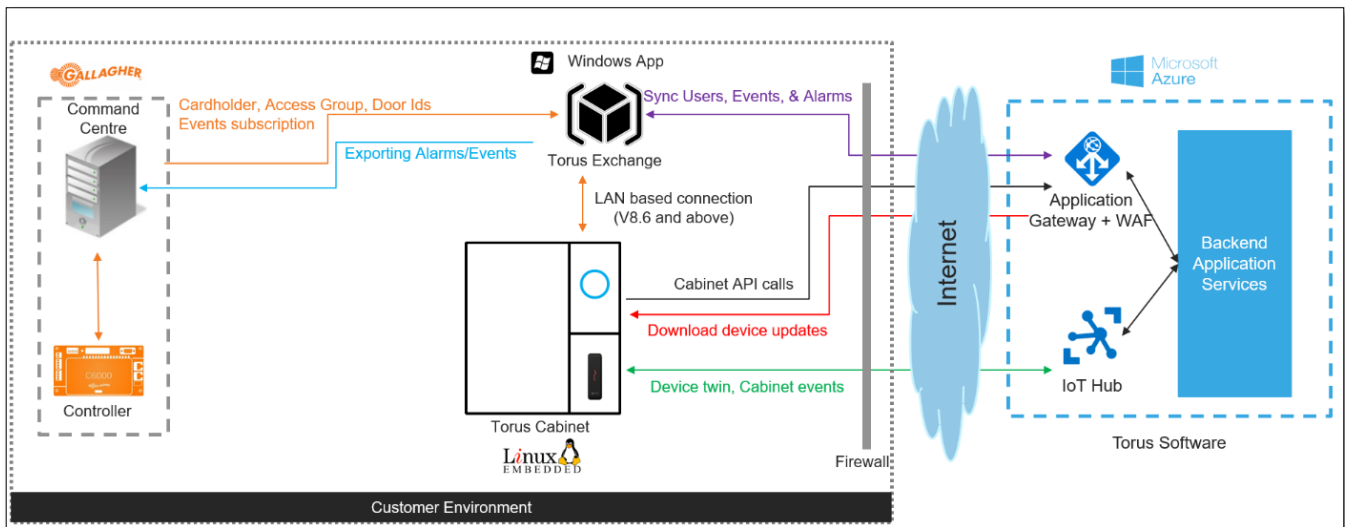
- When integrating Torus with Command Centre V8.6 and higher there is an additional step which need to be performed to create **Event Group** and **Event Type** in Command Centre using **External Event Type Configuration Utility (CCFTEExternalEvents)**. This Command Centre Utility can be found at following location **Program File (x86) > Gallagher > Command Centre > Bin**



- Open this utility, and pick an unused default Event Group and rename it to **Torus Event Group**
- Create a New Event Type i.e., **Torus Events** under **Torus Event Group** or rename an existing Event Type to **Torus Events** under **Torus Event Group**
- After completing this activity apply these changes.
- After applying these changes restart Command Centre Server (ideally) or Command Centre Server Services (At-minimum).
- It is also recommended to restart Torus Exchange services after completing all above steps.



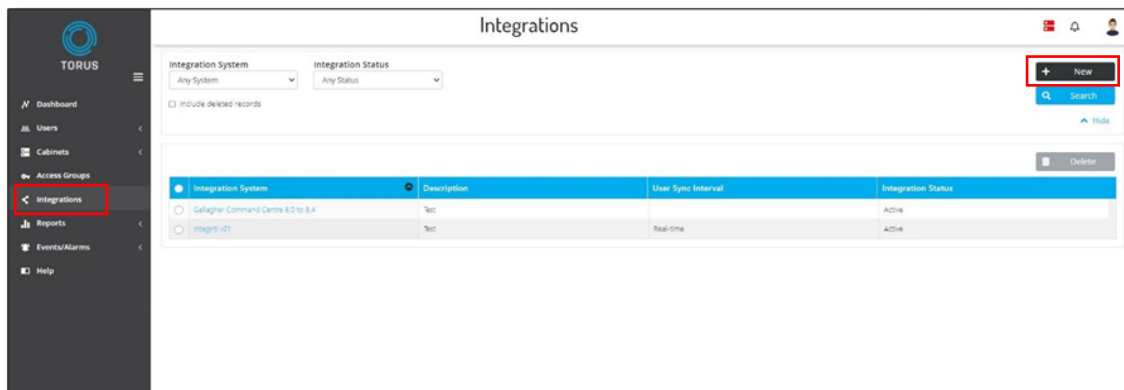
Integration overview



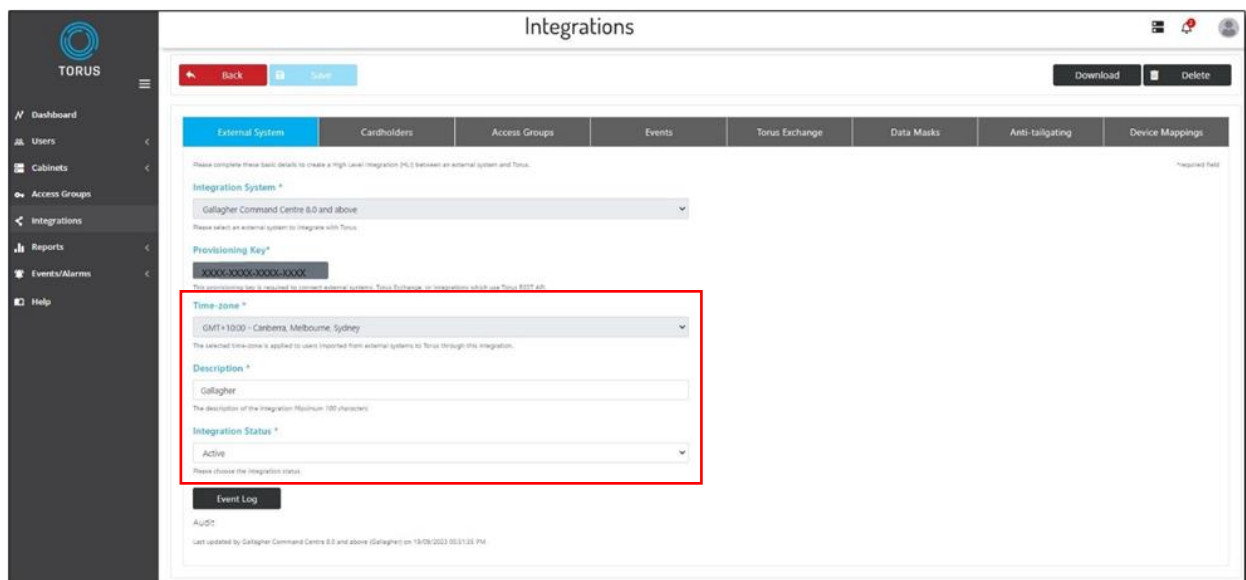
STEPS FOR INTEGRATION

1 – CREATE INTEGRATION RECORD

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

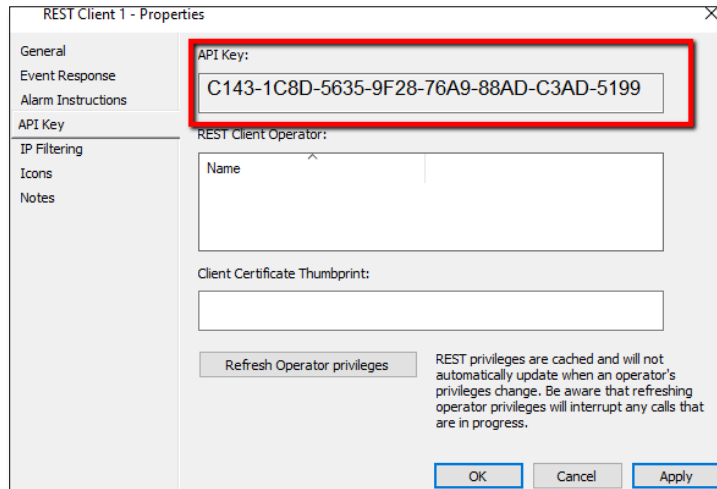


- Complete the details for new External system details.
- Select Command Centre from Integration systems Drop down field and provide a description of this integration.
- Select the time zone which is applied to users imported from external system.



2 – CONFIGURE COMMAND CENTRE REST API

- Open 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.



- Go to Torus Software and open the new integration details page.
- Select Torus Exchange Tab and paste 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):			Offline		
This shows the connection status of Torus Exchange with Torus Web					
Torus Exchange - External System (Connectivity):			Unknown		
This shows the connection status of Torus Exchange with the External System					
External System Configuration*					
Configuration	Description	Value			
API Key	API Key of the Gallagher Instance				

- Go to 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

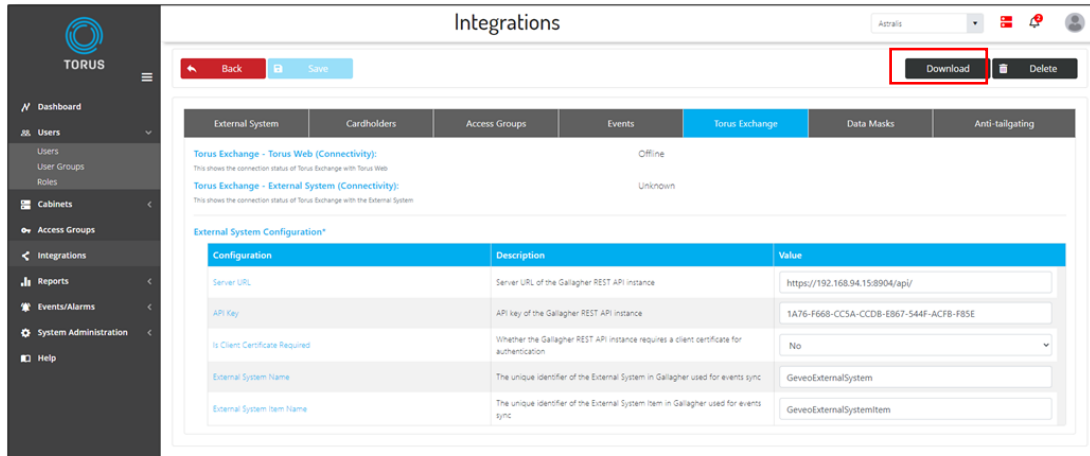
- For the 'Server URL' field in the 'Torus Exchange' tab of Integration record, provide the URL in the following format: *https://<IP address of PC where Commend Centre is installed>:<Server Base Port>/api/*

The screenshot shows the TORUS web interface for managing integrations. The 'Integrations' page is active, displaying a table of external systems. The 'Torus Exchange' tab is selected, showing configuration details for an external system. A red box highlights the 'Server URL' field in the configuration table, which contains the value 'https://192.168.94.15:8904/api/'.

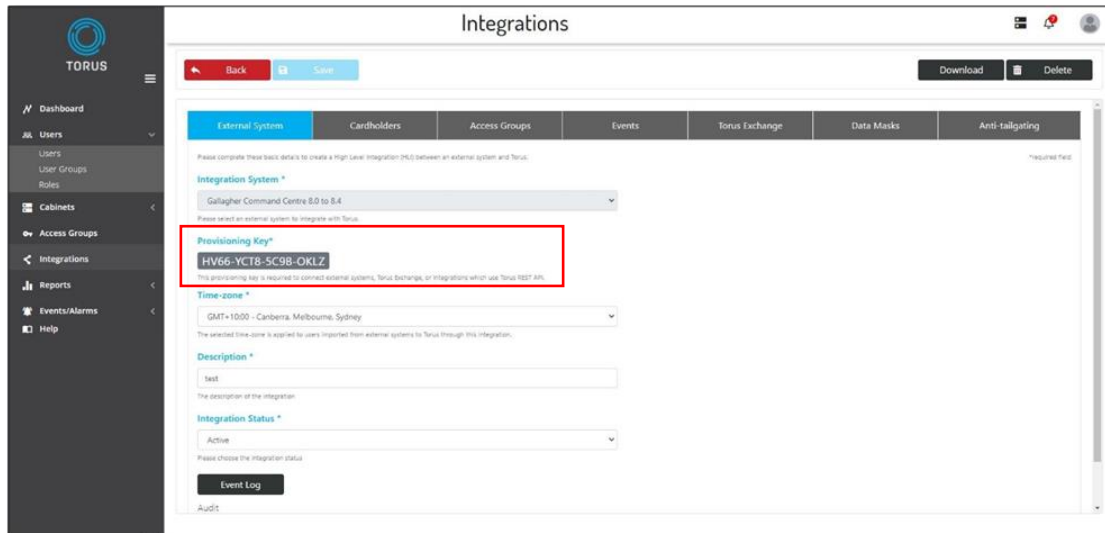
Configuration	Description	Value
Server URL	Server URL of the Gallagher REST API instance	https://192.168.94.15:8904/api/
API Key	API key of the Gallagher REST API instance	1A76-F668-CC5A-CCDB-E867-544F-ACFB-F85E
Is Client Certificate Required	Whether the Gallagher REST API instance requires a client 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 – INSTALL TORUS EXCHANGE

- After completing details for Torus Exchange, download Torus Exchange and install it on the 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.

The screenshot displays the TORUS web interface for managing integrations. The main content area is titled "Integrations" and features a navigation bar with tabs for External System, Cardholders, Access Groups, Events, Torus Exchange, Data Masks, and Anti-tailgating. The "Torus Exchange" tab is active, showing two entries:

- Torus Exchange - Torus Web (Connectivity):** Status: Offline
- Torus Exchange - External System (Connectivity):** Status: Unlinkdown

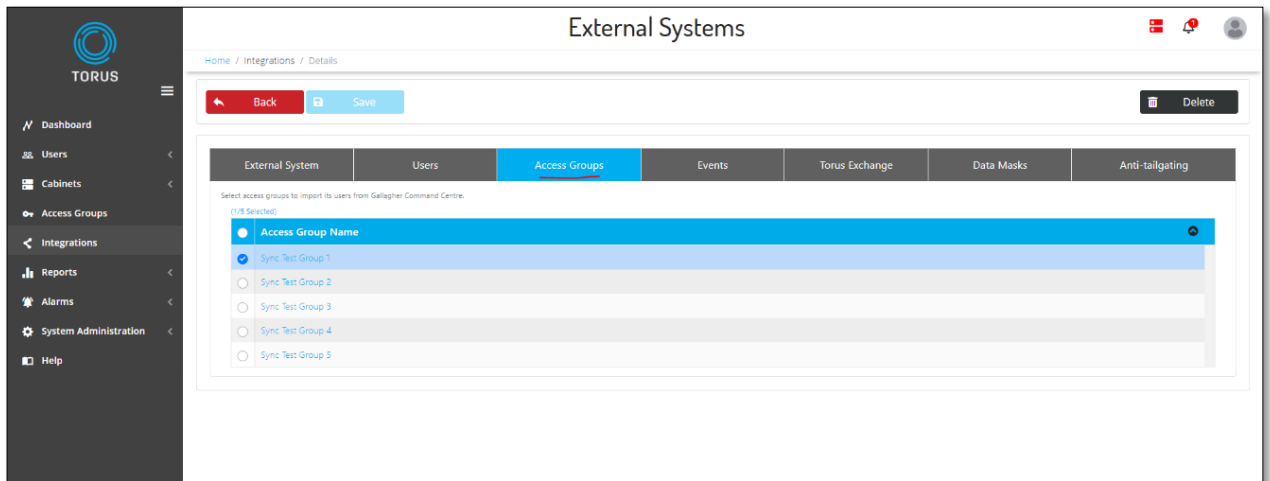
Below these entries is the "External System Configuration" section, which contains a table of configuration parameters:

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-CCSA-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	GevecoExternalSystem
External System Item Name	The unique identifier of the External System item in Gallagher used for events sync	GevecoExternalSystemItem

4 – COMPLETE USER SYNCHRONISATION SETTINGS

4.1 – 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.

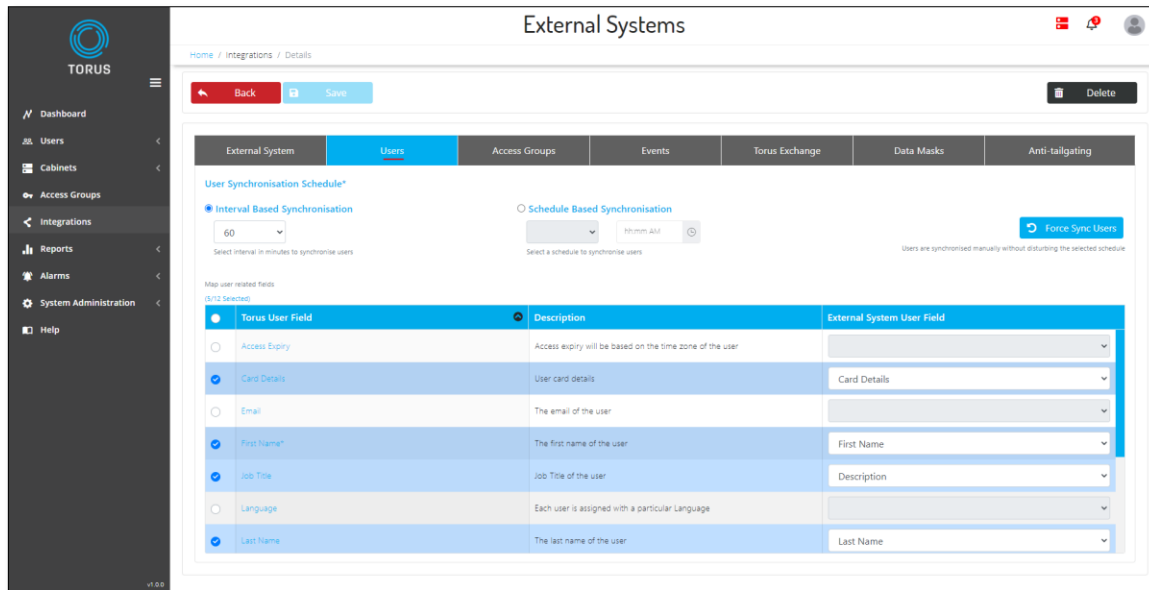


Torus only imports Users which are part of Selected Access Group(s). Important points to remember include:-

1. Torus only imports Users from Command Centre when the relevant Command Centre Access Group is selected in Integration Record.
2. Only selected Access Groups are imported, and they are saved as User Group in Torus.
3. If User deselects an Access Group in Access Groups Tab and saves 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 in the following:-
 - a. If Access Group name is edited in Command Centre, then corresponding User Group name in Torus will also change.
 - b. If Access Group is deleted in Command Centre, then the respective User Group in Torus will also be deleted, along with its Users.

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

User record field mapping is required to import a User record from Command Centre into Torus. By default, mandatory field mapping is created at the time of creation of the integration record. User field mapping can be configured in User 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 Note: Torus does not support special character for cardholder first name field. If a first name has a special character for example: "-" then cardholder will not be imported to Torus.
User Group	Access Group
Card Details	Card Details (Becomes mandatory when a Data Mask is selected in Data Mask tab)

Other optional user fields in Torus can also be mapped with Command Centre cardholder's fields.

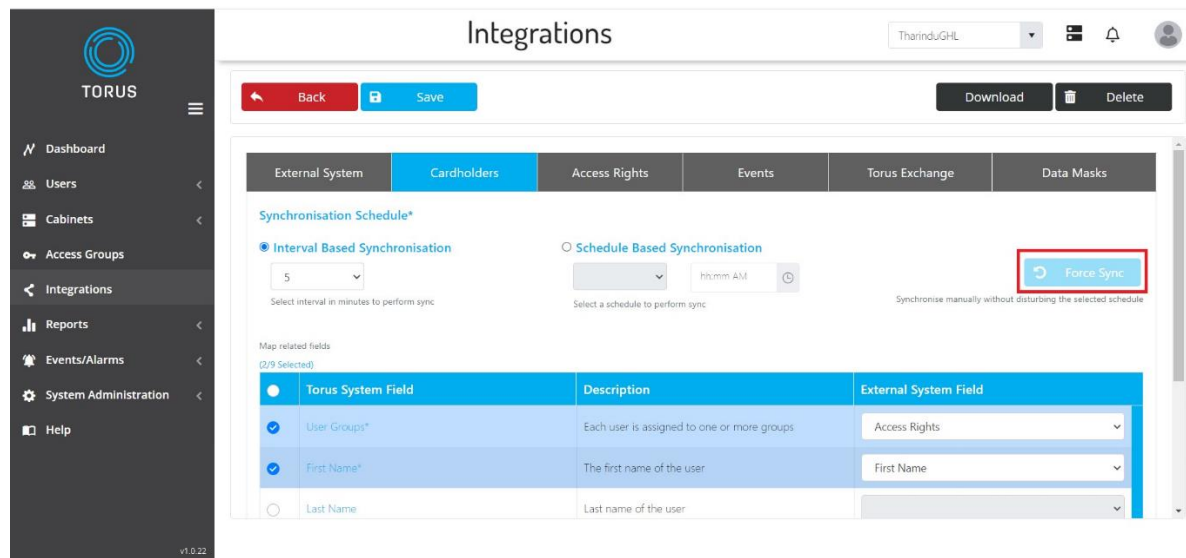
Custom field	User-defined field in	Description
Last Name	LastName	Last Name of cardholder Note: Torus does not support special character in data field. If a last name has a special character for example: "-" then cardholder will not be imported to Torus

Job Title	Job Title	Job Title
Mobile	Mobile / Phone number	<p>Mobile number of cardholder</p> <p>Contact number of visitor.</p> <p>Torus use this information to send relevant SMS alert to imported user.</p> <p>Note 1: Torus requires a complete number including the country code e.g., +614XXXXXXXXXX.</p> <p>Note 2: Torus does not support special character for cardholder phone number field. If a phone number has a special character for example: '-', the cardholder will not be imported to Torus.</p>
Email	E-Mail	Email of cardholder
Company	Company	Company of the visitors.
Access Expiry	Access Expiry	<p>Expiry date/time of the cardholder in Command Centre.</p> <p>Note: This can be mapped with Torus user field and user will also loses access on keys in Torus Cabinet after Expiry Date/time.</p>
Card Details	Cards	<p>Card Details of the cardholder.</p> <p>When this filed is mapped then Torus can import top 5 active cards issued to cardholder in Command Centre. This imports following information of each card.</p> <ul style="list-style-type: none"> • Card ID • Card Issue code/ Issue code • Facility code <p>Note: This requires additional configurations for Torus cabinet. Please see Data Mask Setup</p>

4.3 – Cardholder Synchronisation

Cardholder Synchronisation pre-requisite is to select the required Access Group in the integration record so Torus can import all associated cardholders as USERS from Command Centre. There are three options to synchronise Cardholders with Command Centre.

- Option 1 – Interval based synchronisation.**
 In this option user can configure time interval for cardholder synchronisation. Default interval is 5 minutes.
- Option 2 – Schedule based synchronisation.**
 In this option user can configure a specific day and time for cardholder to synchronise. The synchronisation job will only run at configured time on a specific day.
- Option 3 – Force synchronisation.**
 Force Sync option can also be used to synchronise the users at any time. When this option is used, then Torus software performs forced synchronisation of Access Group and its associated Cardholder. Force Synchronisation is a handy tool to test synchronisation between Torus and Command Centre.



5 – EVENTS EXPORT SETUP

Torus cabinet events can be exported to Command Centre through Torus Exchange. User 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.

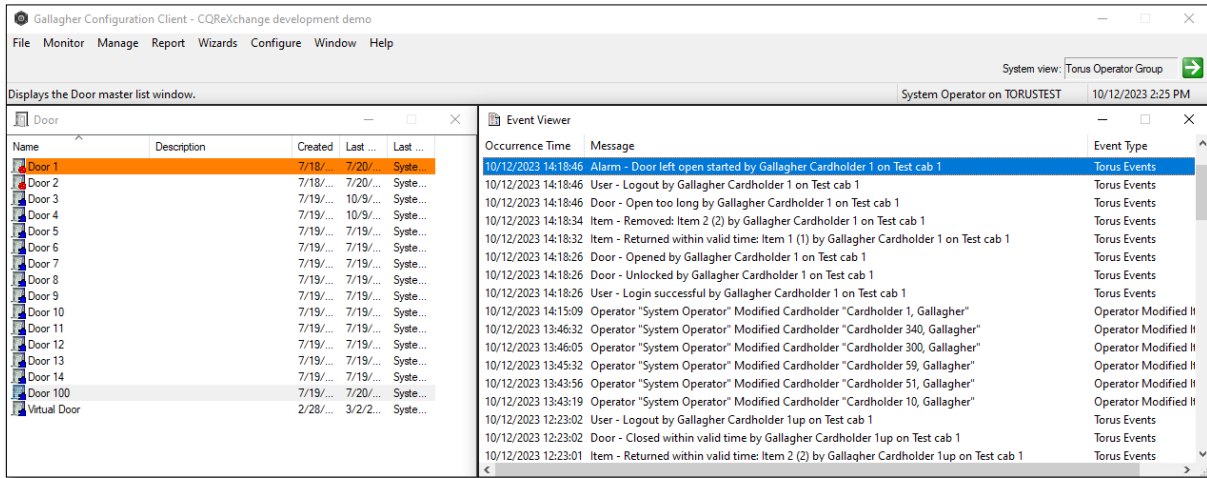
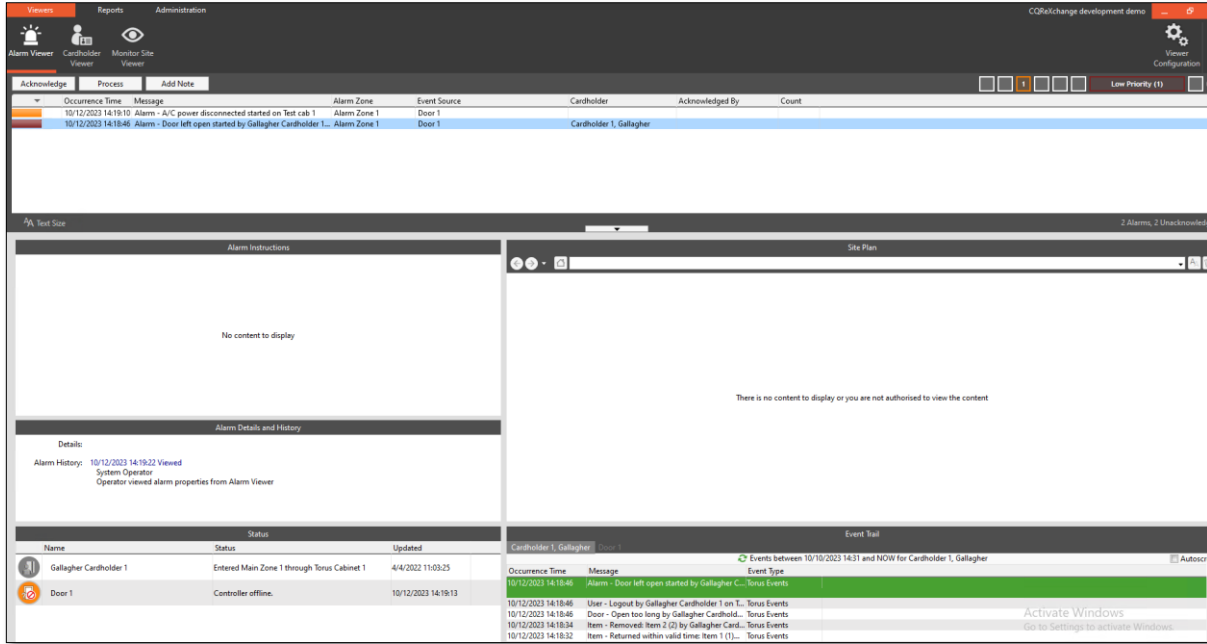
Exported events/Alarms are listed under Doors mapped with respective cabinet.

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.

The screenshot displays the 'External Systems' configuration page in the TORUS interface. The 'Events' tab is selected, showing a list of events to be exported. The events are listed in a table with columns for Event Name, Priority, and Description. A 'Test Events Sync' button is located in the top right corner of the event list area.

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

Exported events and alarms are listed under Doors associated with Cabinets in Command Centre. Door mapping with cabinet explained in section [Map Door with Torus cabinet](#).



Events and alarms which contains a cardholder context are also listed under in cardholder's event trail.

Viewers | Reports | Administration

Alarm Viewer | Cardholder Viewer | Monitor Site Viewer

Search: Gallagher Cardholder 1 | By Name | Simple Search | Actions | Create Cardholder | Delete Cardholder

First Name	Last Name	Description	Division	Card Number	Last Zone Entered	Authn...
Gallagher	Cardholder 401		Root Division		Never accessed	Yes
Gallagher	Cardholder 1034		Root Division		Never accessed	Yes
Gallagher	Cardholder 10	Operator user	Root Division	1313, 1316	13/12/2023	Yes

Found: 157

Event Trail

Events between 10/10/2023 14:31 and NOW for Gallagher Cardholder 1

Occurrence Time	Message	Event Type
10/12/2023 14:18:46	Alarm - Door left open started by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 14:18:46	User - Logout by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 14:18:46	Door - Open too long by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 14:18:34	Item - Removed: Item 2 (2) by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 14:18:32	Item - Returned within valid time: Item 1 (1) by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 14:18:26	Door - Opened by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 14:18:26	Door - Unlocked by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 14:18:26	User - Login successful by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 14:15:09	Operator - System Operator Modified Cardholder "Cardholder 1, Gallagher"	Operator Modified Item
10/12/2023 13:23:02	User - Logout by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 12:23:02	Door - Closed within valid time by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 12:23:01	Item - Returned within valid time: Item 2 (2) by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 12:22:58	Item - Removed: Item 2 (2) by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 12:22:58	Item - Returned: Item 1 (1) by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 12:22:55	Door - Opened by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 12:22:55	Door - Unlocked by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/12/2023 12:22:55	User - Login successful by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/10/2023 14:31:38	Alarm - Door left open started by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/10/2023 14:31:38	User - Logout by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/10/2023 14:31:38	Door - Open too long by Gallagher Cardholder 1 on Test cab 1	Torus Events
10/10/2023 14:31:34	Item - Returned within valid time: Item 1 (3) by Gallagher Cardholder 1 on Test cab 1	Torus Events

Alarm - Properties

First Occurred: 10/12/2023 14:18:46 | Priority: 3

Last Occurred: 10/12/2023 14:18:46 | Occurrences: 1

Escalation: Non-escalated.

Alarm - Door left open started by Gallagher Cardholder 1 on Test cab 1

General | History | Details

Logged Time: 10/12/2023 14:19:11

Source: Door 1

Item: Cardholder 1, Gallagher

Zone: -- None Selected --

Event Group: Torus Event Group

Alarm Notes: View next alarm

[F1] False alarm [F2] Equipment fault

[F3] Security sent to investigate [F4] Staff error

[F5] No apparent reason [F6] Other

Comments:

Site Plan... Acknowledge Process Next Close

Event - Properties

Occurrence Time: 10/12/2023 14:18:34 | Priority: 1

Item - Removed: Item 2 (2) by Gallagher Cardholder 1 on Test cab 1

General | Details

Logged Time: 10/12/2023 14:18:51

Source: Door 1

Item: Cardholder 1, Gallagher

Zone: -- None Selected --

Event Group: Torus Event Group

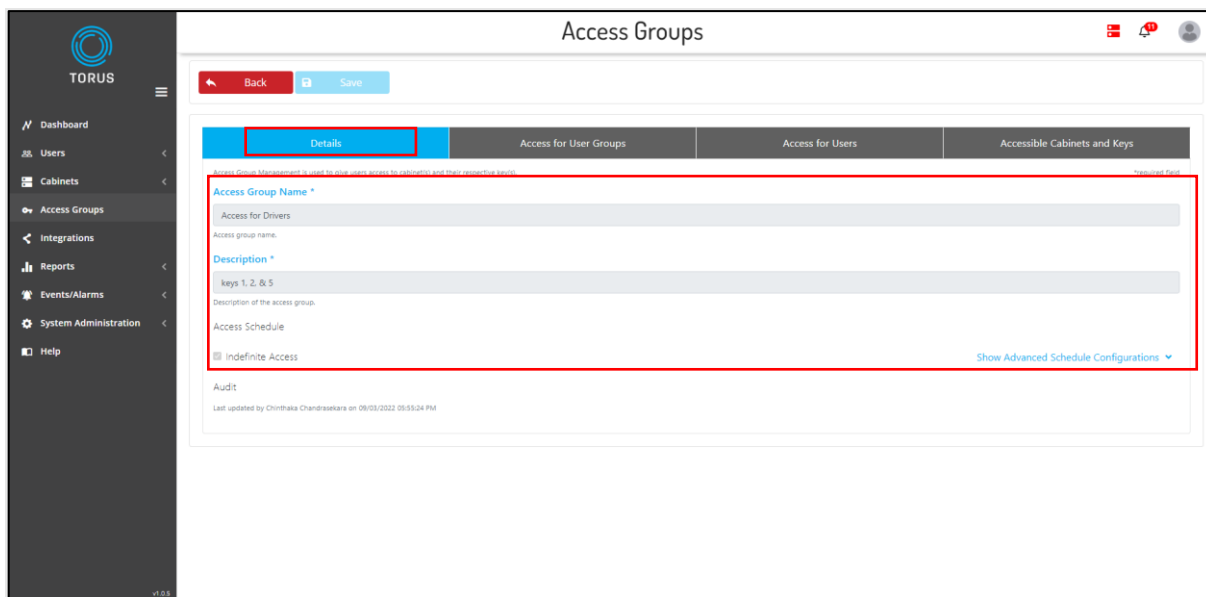
Site Plan... Close

6 – GRANTING CARDHOLDER ACCESS TO KEYS IN TORUS CABINETS

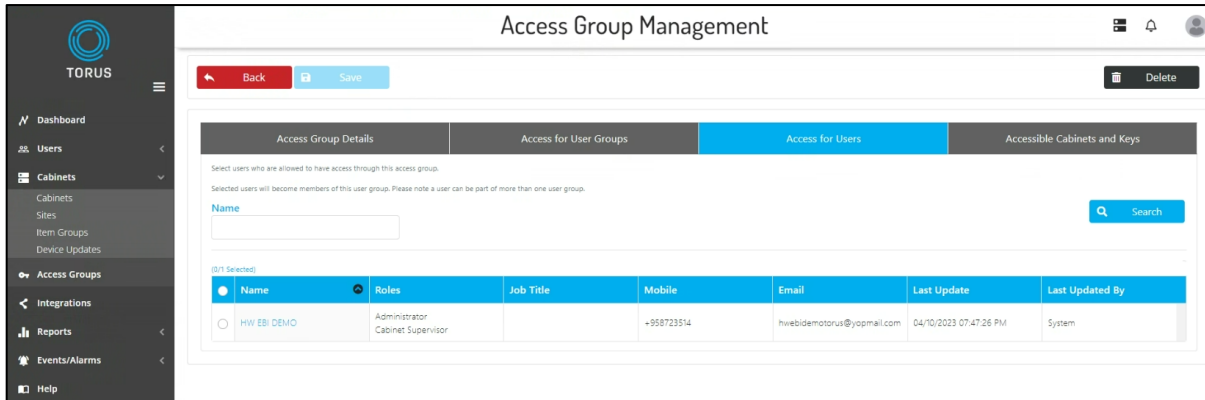
In Torus software, Access Groups are used to grant users access to keys. Following steps need to be completed to grant imported users access to keys.

6.1 – Granting access to keys to an imported user

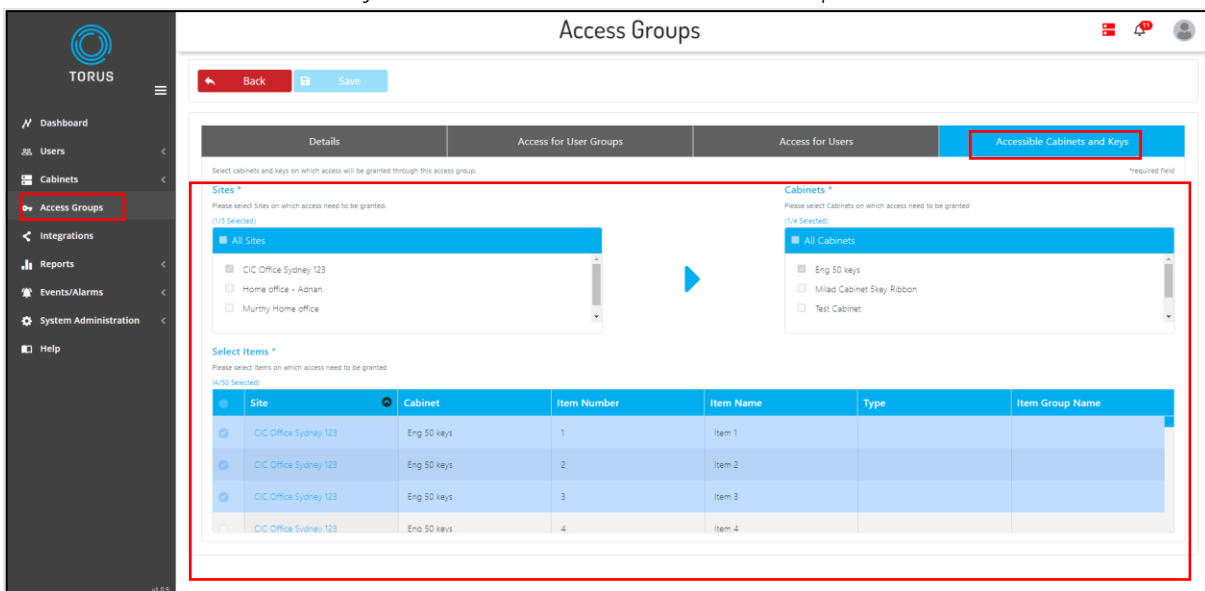
- Cardholders from Command Centre are imported to Torus when their corresponding Access Group is selected in Torus integration record.
- Once card holders are imported to Torus they are listed as Users.
- Next step is to grant access to keys using Access Group in Torus software.
- Create a new Access Group or use an existing Access Group already created. To create a new Access Group:-
 - Select Access Groups from main menu
 - Select '+ New'
 - Input Access Group Name and Description and Save the record.



- Then select Tab – Access for Users. Select the imported user(s) from list.



- o Then select Tab - Accessible Cabinets and Keys
- o Select the keys / cabinets on which access is required

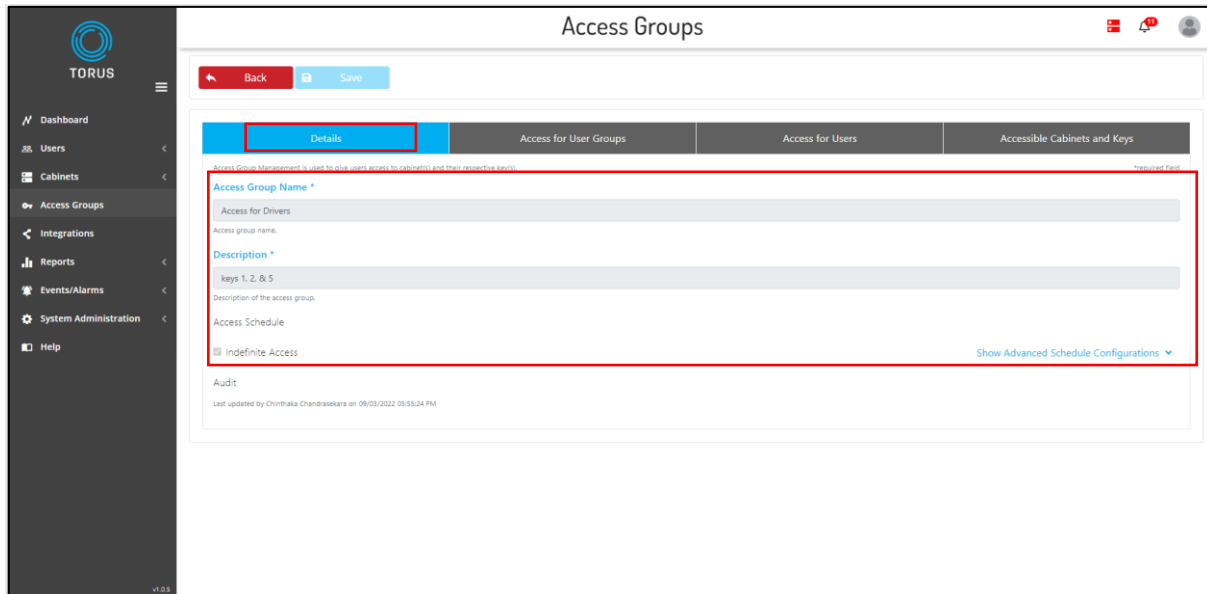


- o Save, and Torus software synchronise access data with Torus cabinet.
(Please note one Access Group record can be used to grant access to multiple users (Cardholders) to one or many keys in Torus cabinets.)

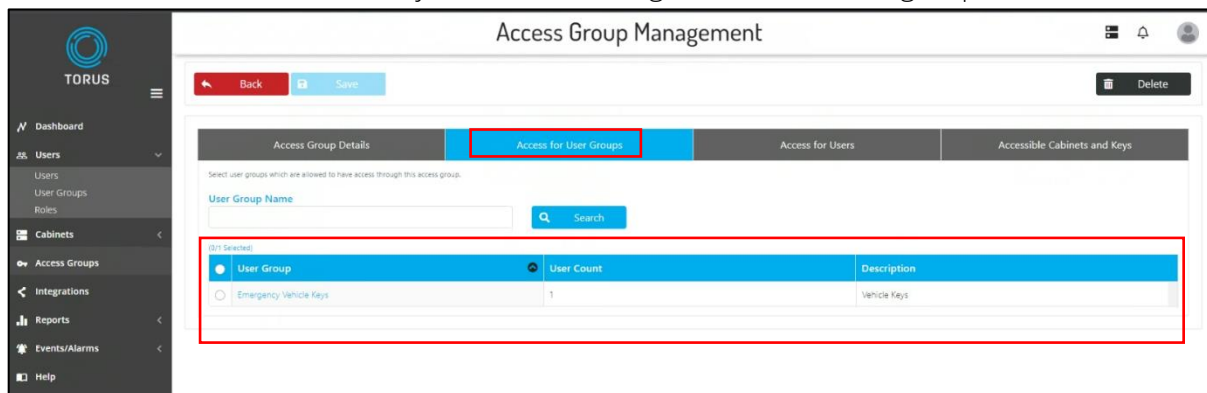
6.2 – Granting access to users using Command Centre Access Group

- Cardholders from Command Centre are imported to Torus when their corresponding Access Group is selected in Torus integration record. Where imported users are connected with their imported Users Groups.
- Once Access Group is imported to Torus they are listed as User Groups.
- Next step is to grant access to keys using Access Group feature in Torus software. (Please note Torus Access Group is feature which is designed to manage user's access to Torus cabinet.)
- Create a new Access Group or use an existing Access Group already created.
To create a new Access Group:-

- Select Access Groups from main menu
- Select '+ New'
- Input Access Group Name and Description and Save the record.



- Then select Tab – Access for User Groups. Select the imported User Group from list.
- When an access is granted to a user group then all of its associated users get the access on the keys which are configured in an access group record in Torus.



- Then select Tab - Accessible Cabinets and Keys
- Select the keys / cabinets on which access is required.
This is important to note that any time if a cardholder is removed or added to an Access group withing Command Centre then this change is reflected in Torus automatically.

The screenshot shows the 'Access Groups' configuration interface. The 'Accessible Cabinets and Keys' tab is selected, and a red box highlights the configuration area. This area includes:

- Sites:** A dropdown menu showing 'All Sites' selected, with options for 'CIC Office Sydney 123', 'Home Office - Adnan', and 'Murthy Home office'.
- Cabinets:** A dropdown menu showing 'All Cabinets' selected, with options for 'Eng 50 keys', 'Milad Cabinet Skay Ribbon', and 'Test Cabinet'.
- Select Items:** A table listing selected items. The table has the following data:

Site	Cabinet	Item Number	Item Name	Type	Item Group Name
CIC Office Sydney 123	Eng 50 keys	1	Item 1		
CIC Office Sydney 123	Eng 50 keys	2	Item 2		
CIC Office Sydney 123	Eng 50 keys	3	Item 3		
CIC Office Sydney 123	Eng 50 keys	4	Item 4		

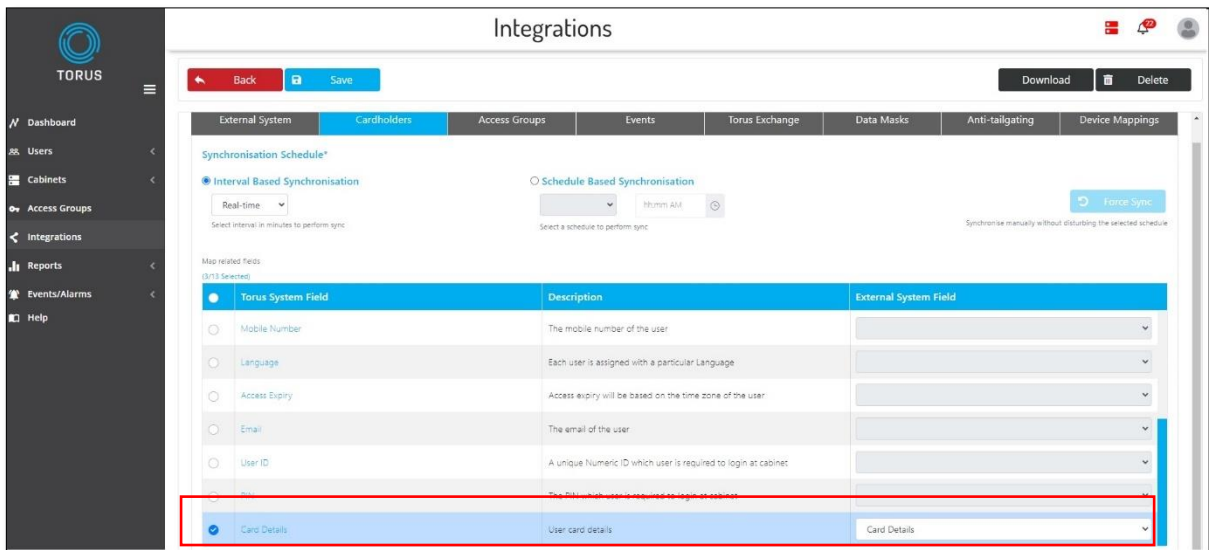
- Save, and Torus software synchronise access data with Torus cabinet.
(Please note one Access Group record can be used to grant access to multiple user groups (Cardholders) to one or many keys in Torus cabinets.)

7 – CARDHOLDER LOGIN AT TORUS CABINET

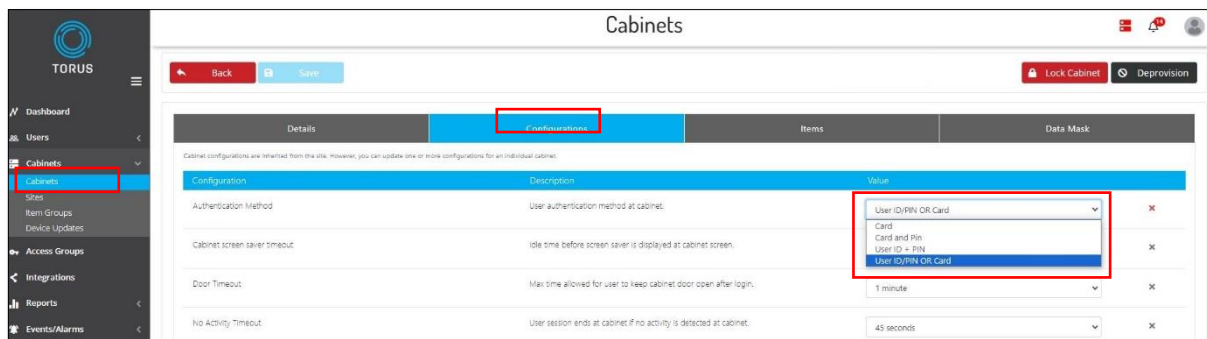
7.1 – Option 1 : When Card reader is connected with Torus Cabinet

In this type of card holder login at cabinet, card data is required from Command Centre. To achieve this authentication method following are three pre-requisites.

1. Card reader installed on Torus cabinet using Weigand port.
2. Command Centre cardholder’s card detail mapping with Torus in User field mapping.

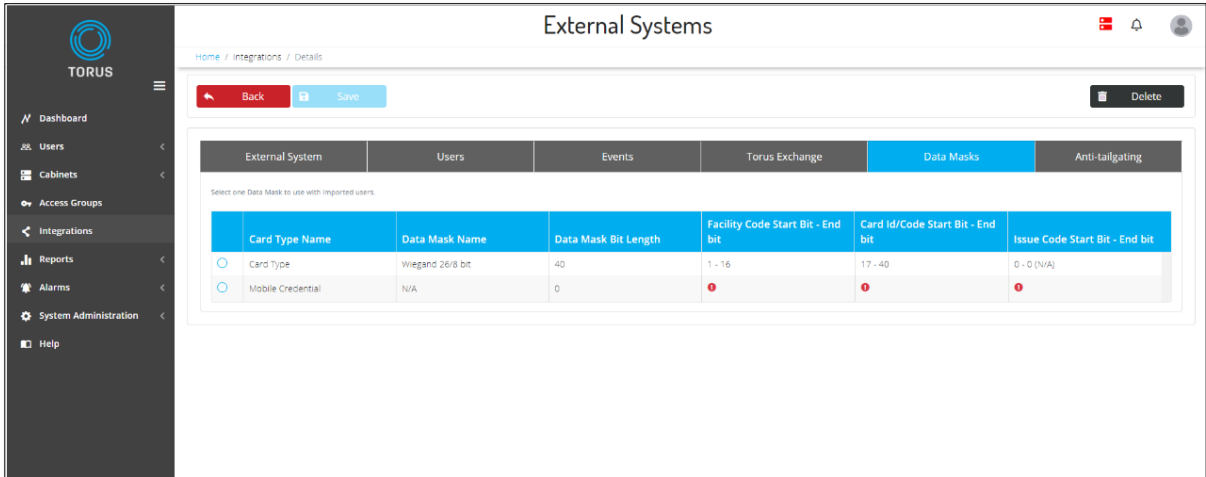


3. Authentication method at cabinet is set to any of the following methods
 - a. Card
 - b. Card and PIN
 - c. User ID/PIN or Card

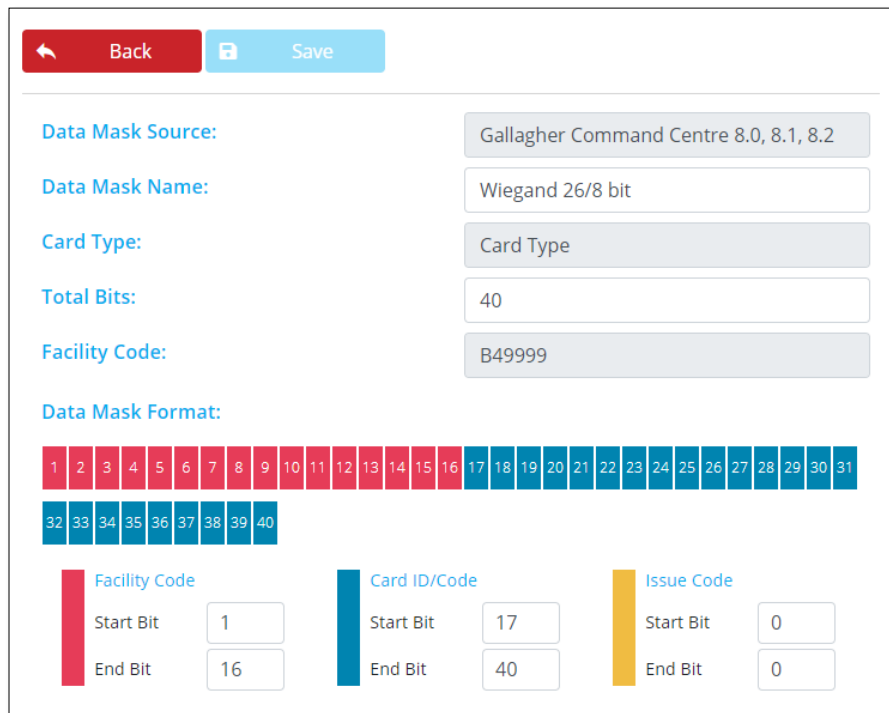


4. Users (Cardholders) access is properly configured through Access Groups in Torus Software. (As explained above in [GRANTING CARDHOLDER ACCESS TO KEYS IN TORUS CABINETS](#))
5. Data Mask setup at cabinet using following steps.

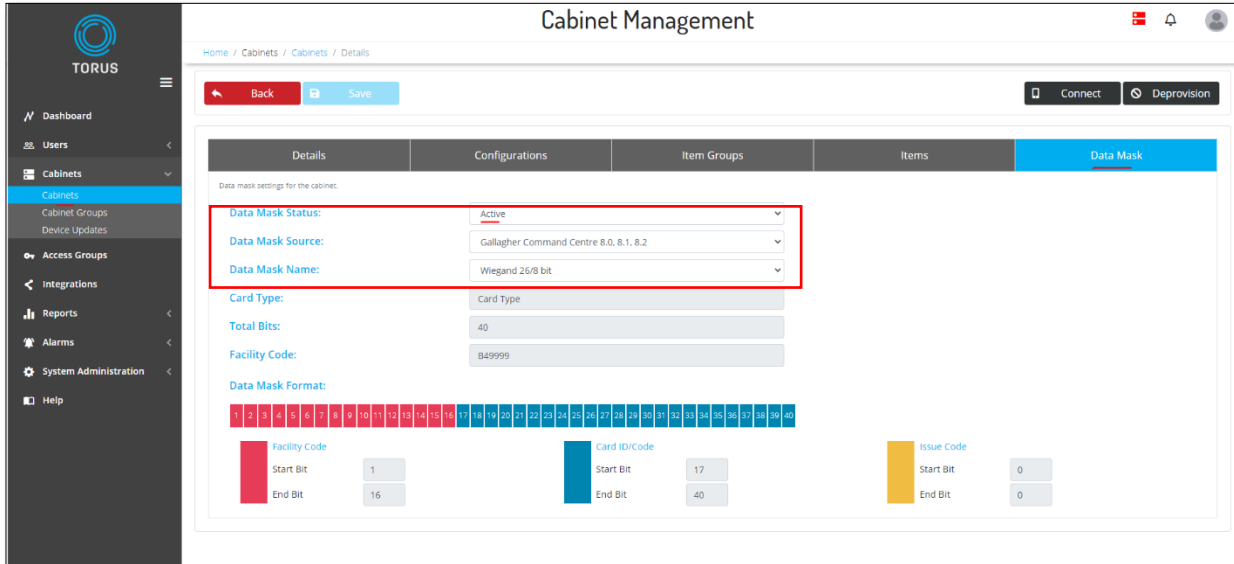
- a. Torus automatically imports Data Mask definitions from Command Centre. Imported data masks are listed under Data Masks tab in Torus for Integrity integration.



- b. User can compare the Data Mask configuration with Command Centre and can edit Data Mask details in Torus. Data Masks are listed as Card Types in Command Centre. *Please note multiple data masks can also be applied on single cabinet at any given time*

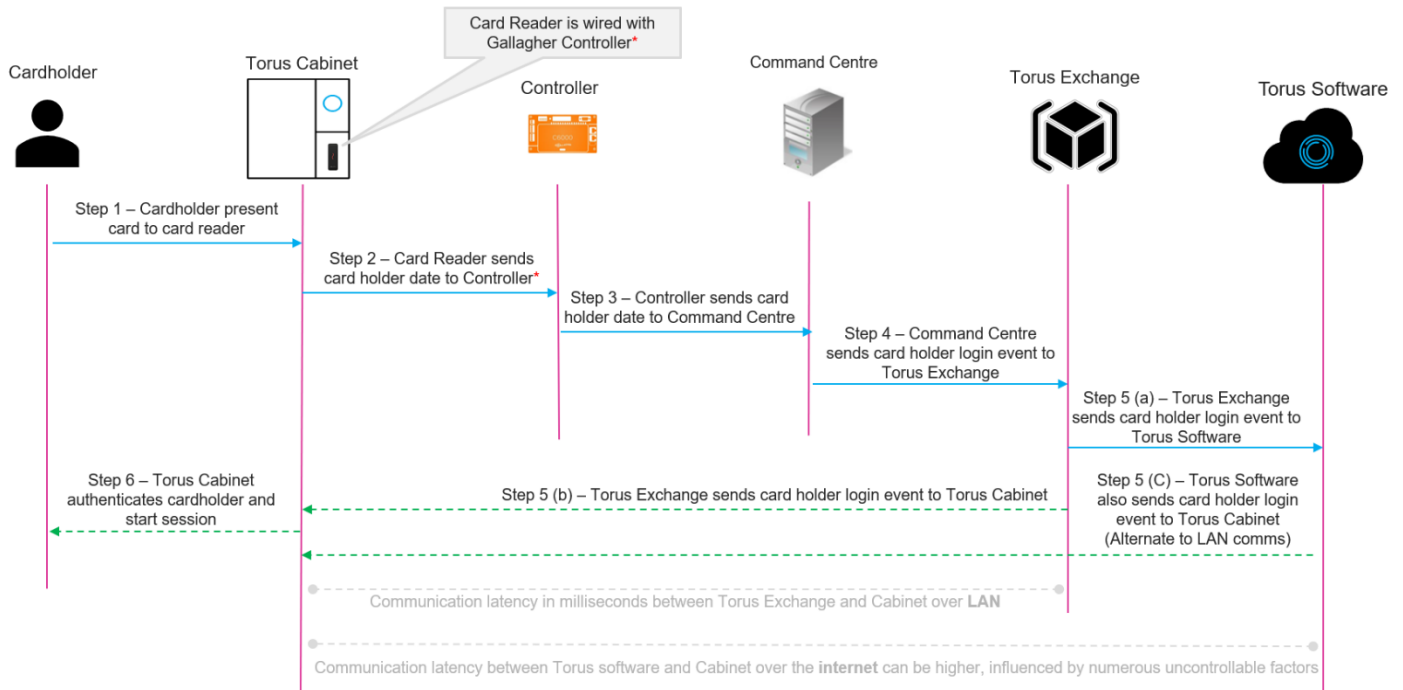


- c. Apply Data Mask to cabinet from cabinet configurations in Torus. Go to cabinet record and select the correct Data Mask source from drop down and select relevant integration record and relevant data mask name.



7.2 – Option 2 : When Card reader is connected with Command Centre

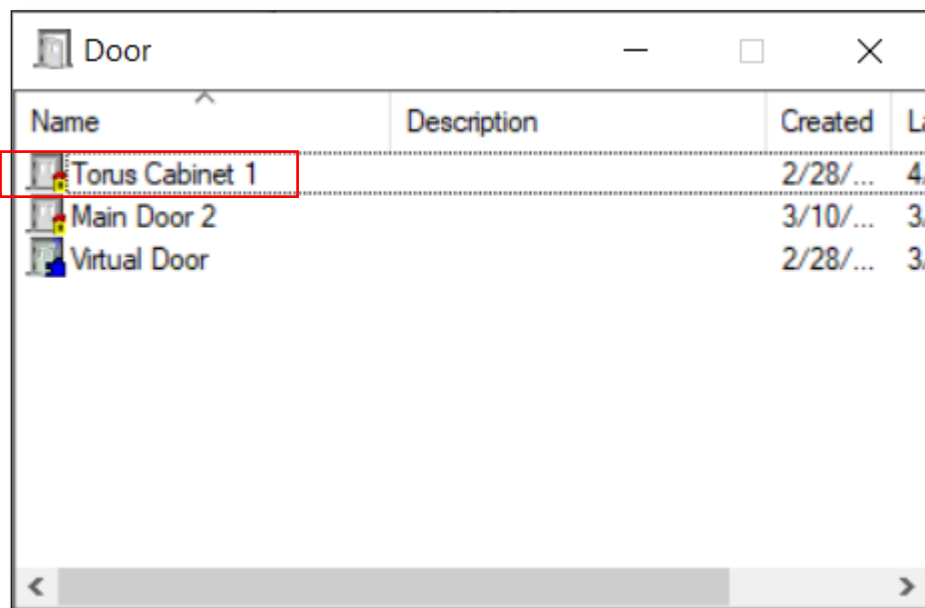
Command Centre’s REST API Alarms & Events is used to enable card holders to login at Torus cabinet when card reader is not wired directly with Torus cabinet. In this type of setup Card reader is physically mounted on Torus cabinet but it is directly wired with Controller.



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 Controller. Furthermore, there is no need to configure any data mark on the cabinet where the card reader is directly connected with Controller for this type of setup. This feature allows card or mobile connect users to use their credentials at card readers mounted at Torus cabinet.

7.2.1 – Create Door in Command Centre

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



- 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

7.2.2 – 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 Command Centre.
- Go to External System Devices tab to input door name which is linked with Card Reader mounted at corresponding cabinet.
- Add imported users to respective Access groups to grant access on desired items in Torus cabinet.

The screenshot shows the 'Integrations' page in the Torus software. The 'Device Mappings' tab is selected and highlighted with a red box. Below the tab, there is a table with the following data:

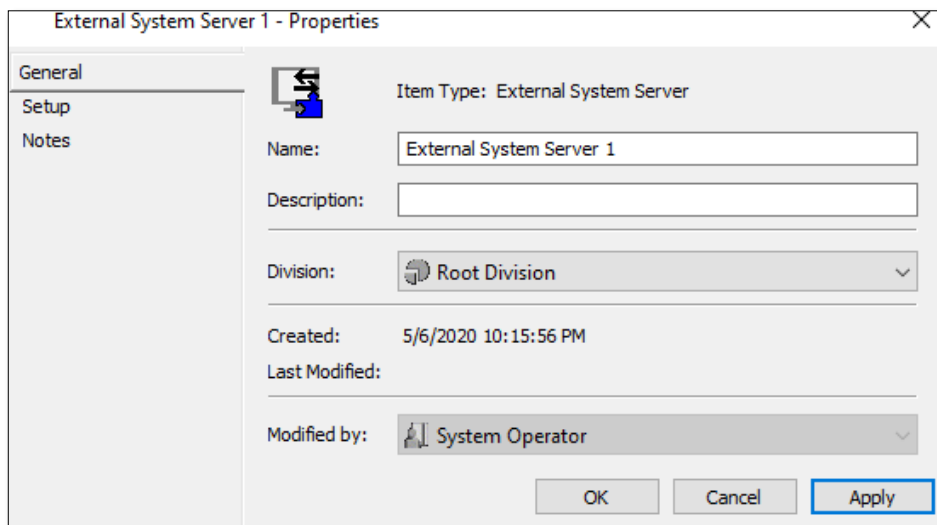
Cabinet Name	Size	Site	External System Device
S Keys Cabinet	5	Test Site	Torus Cabinet 1
Demo cabinet	50	Test Site	Torus Cabinet 2
MM's 5K UAT	5	Test Site	Torus Cabinet 3
Murthy S U3 keys cabinet	5	Murthy Home Office	Torus Cabinet 4
test cabinet 2	5	Test Site	Torus Cabinet 5

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.
- External system server and items configuration need to be completed for this feature.

8.1 – Create an External System Server in Command Centre

- Open 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:

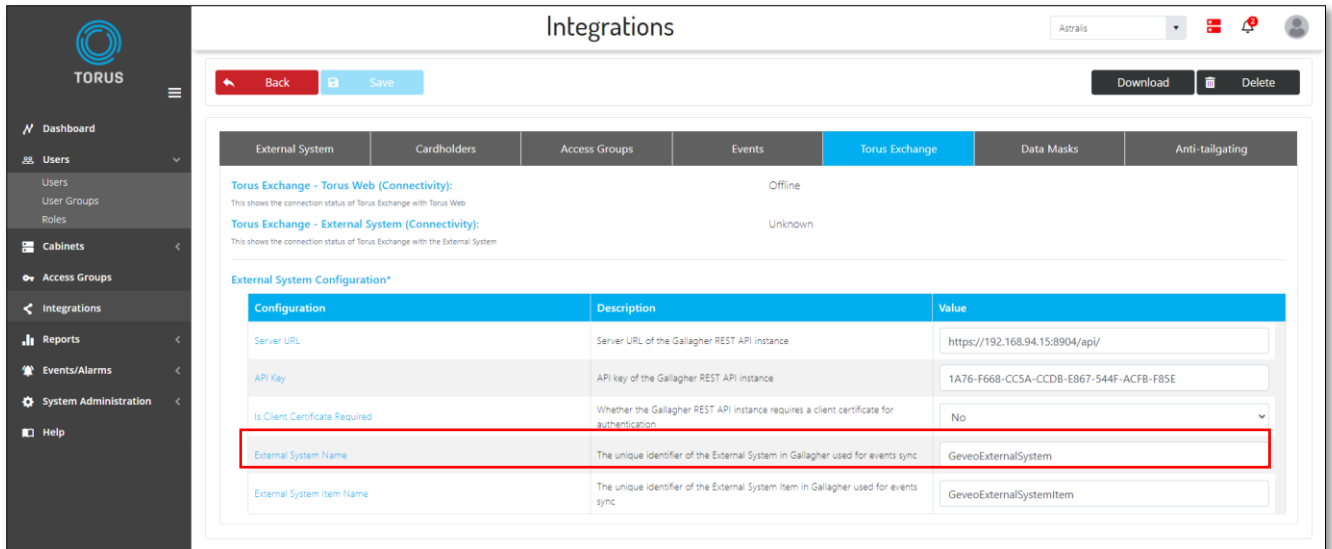
Division: Root Division

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

Last Modified:

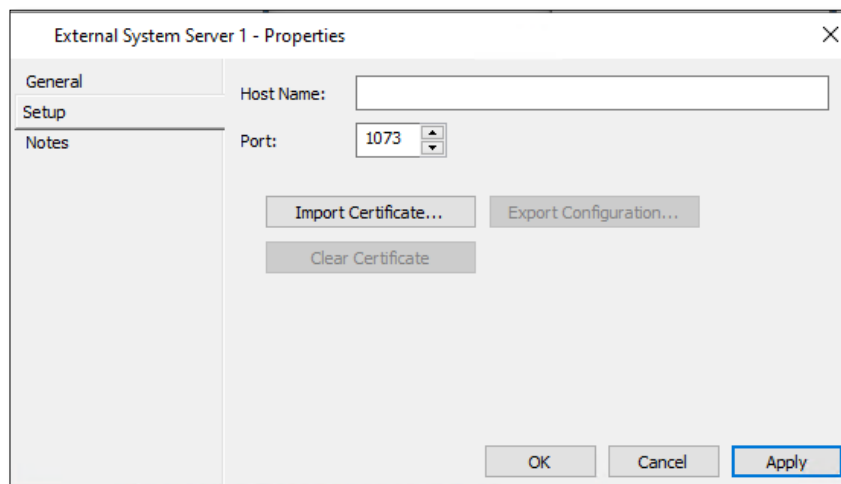
Modified by: System Operator

OK Cancel Apply



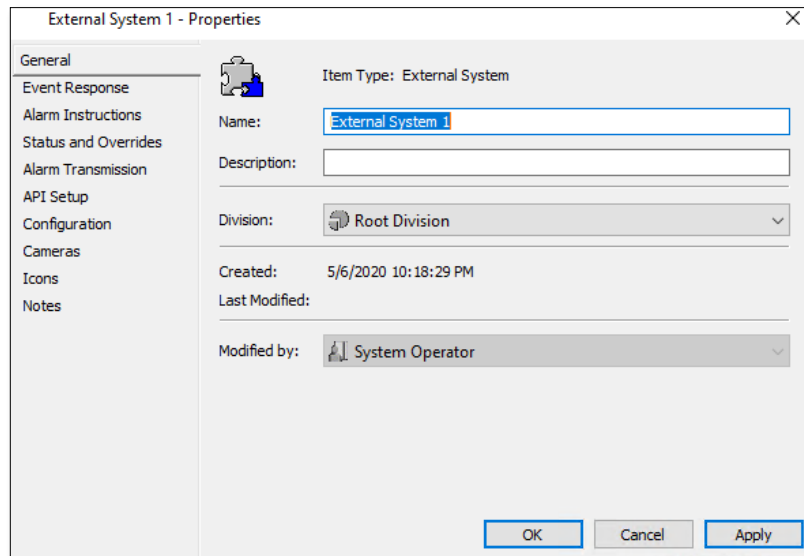
❖ Setup Tab

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

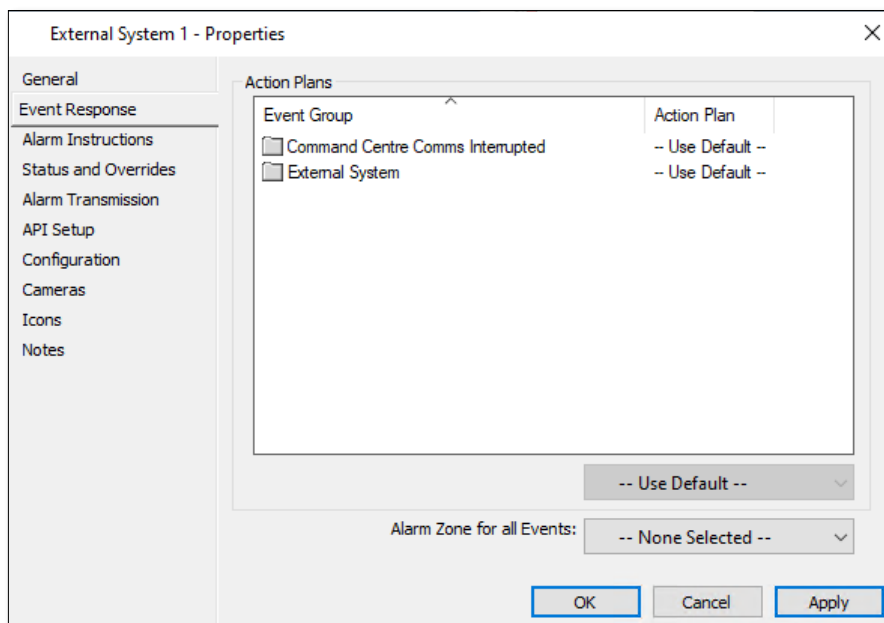


8.2 – Create an External System in Command Centre

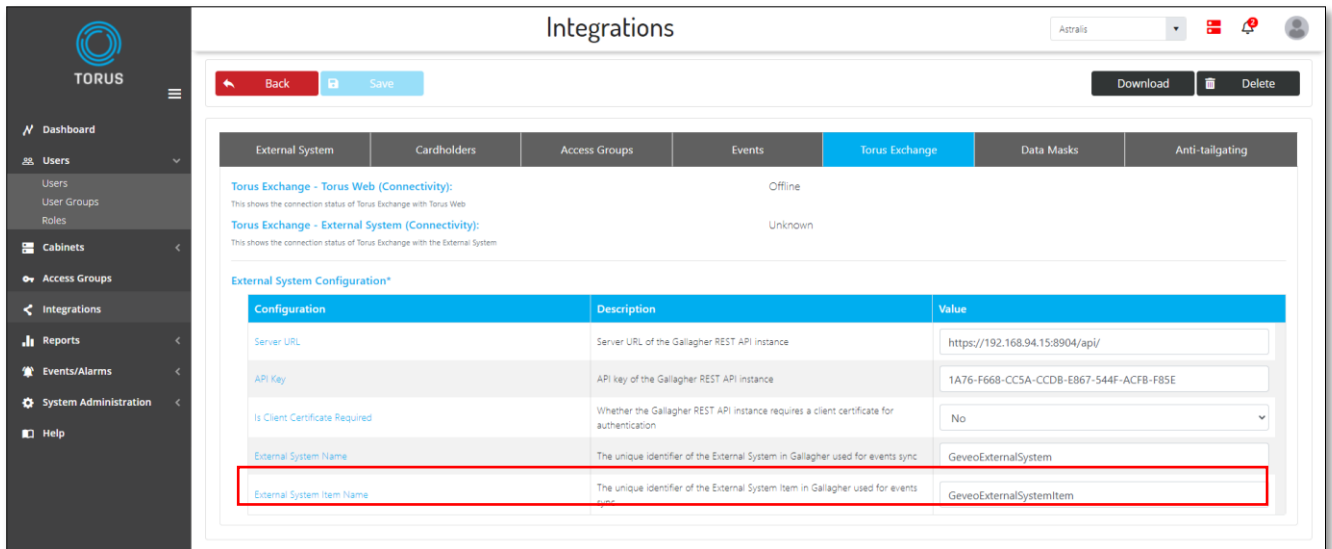
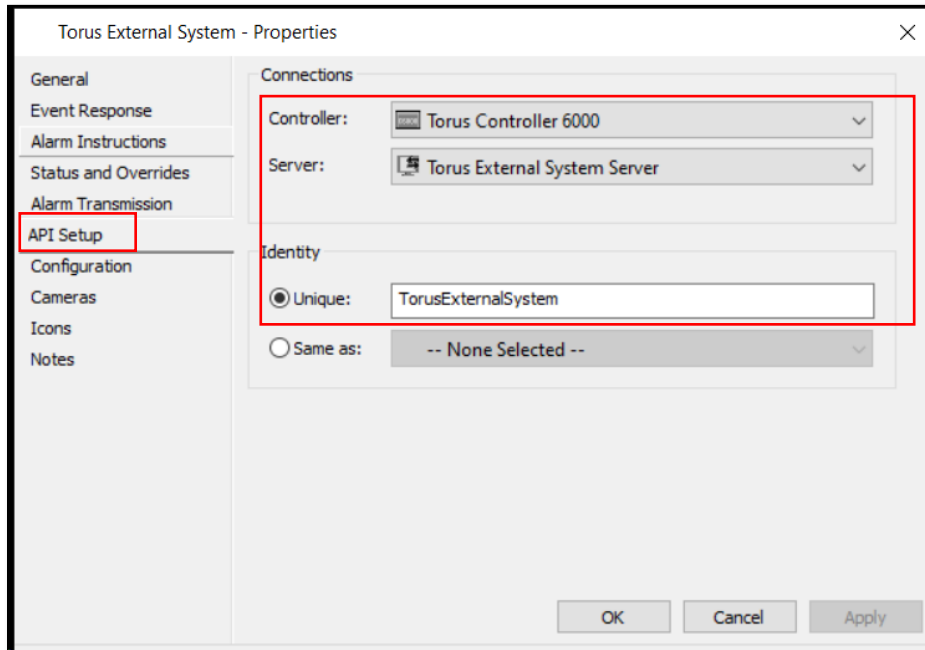
- Right click the created external system server and create a new item type **External System**.
 - ❖ General Tab
 - Give any name to External system, it is ideal to use the same name as Unique name for API setup



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

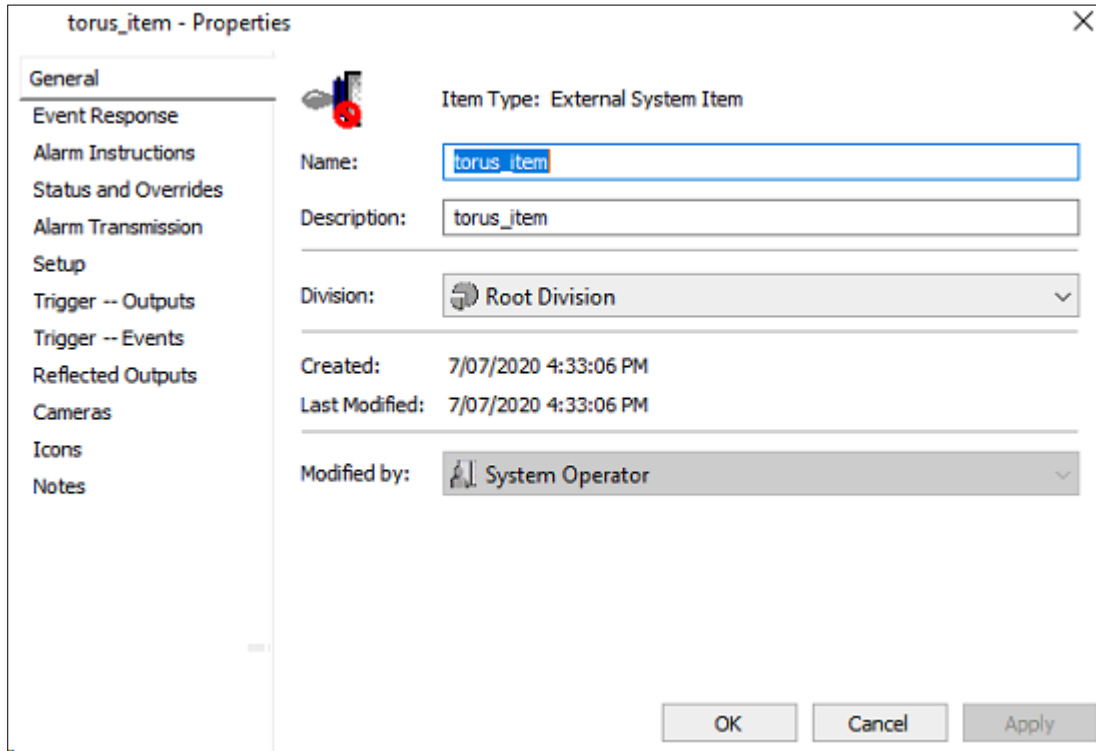


- ❖ API Setup Tab
 - Select the correct Controller and the External System Server.
 - For the Unique field, give the same name used in the Torus Exchange External System Item Name field of the integration record.

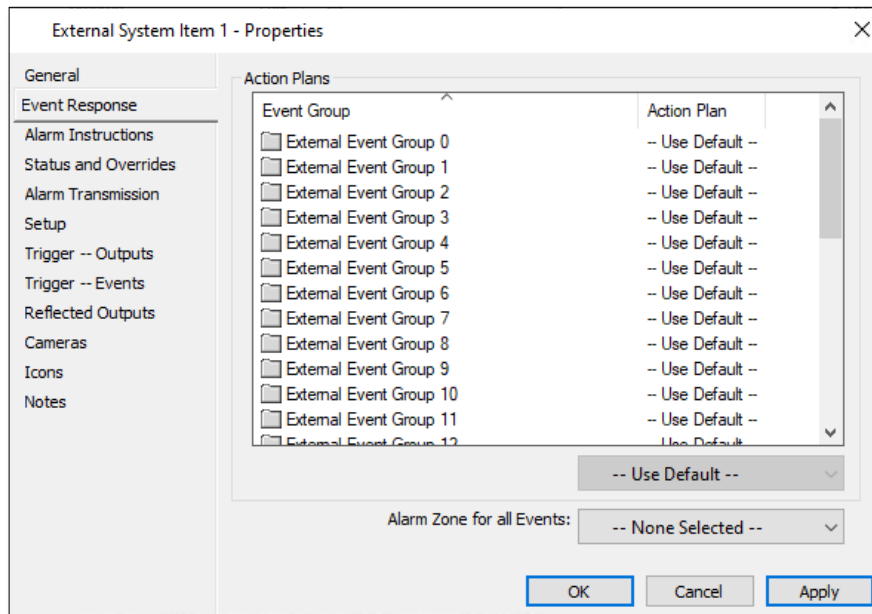
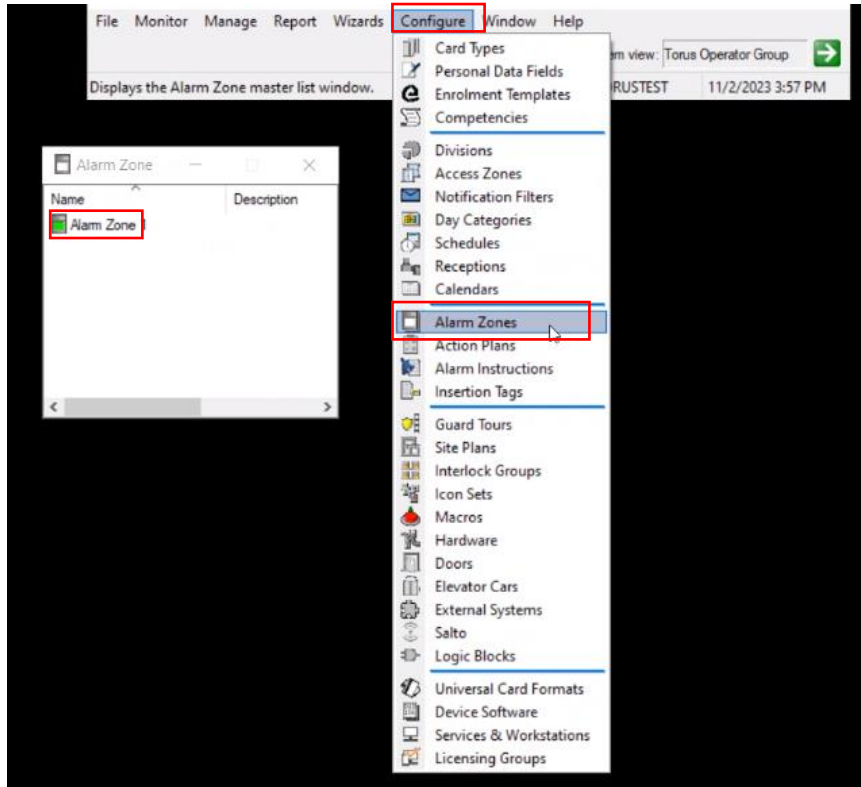


8.3 – Create an External System Item in Command Centre

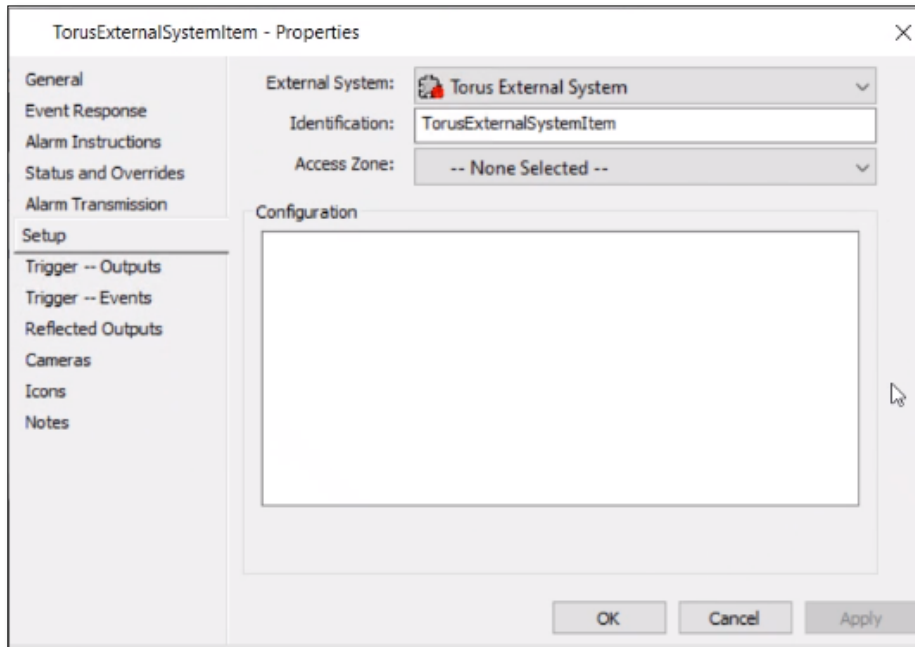
- Right click the external system and create a new item type **External System Item**.



- ❖ Event Response Tab
 - For external system item Select the relevant Alarm Zone.
 - To create alarm zone in command Centre go to Command Centre Configuration client > Configure > Alarm zone

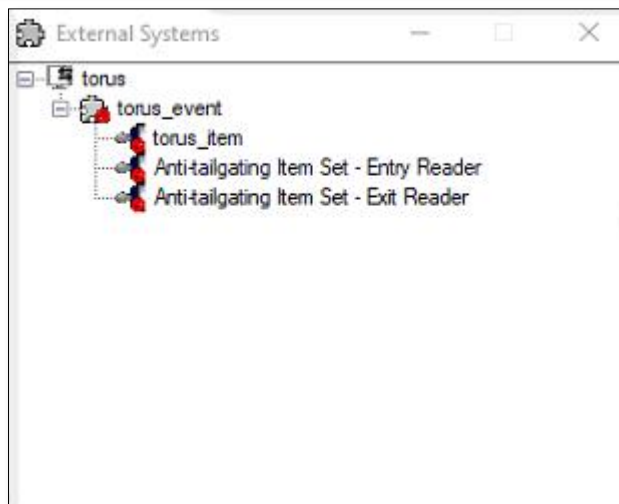
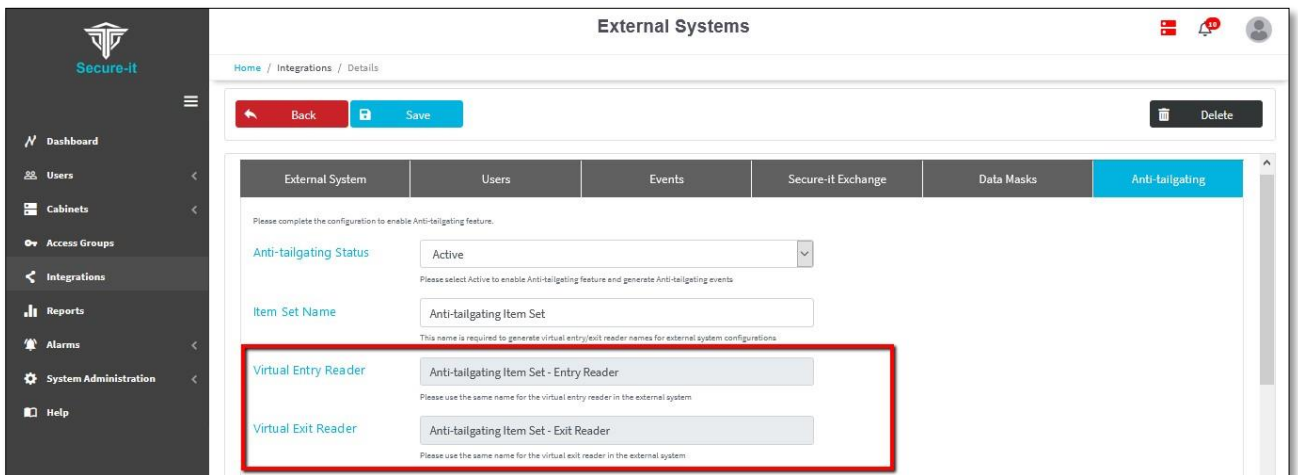


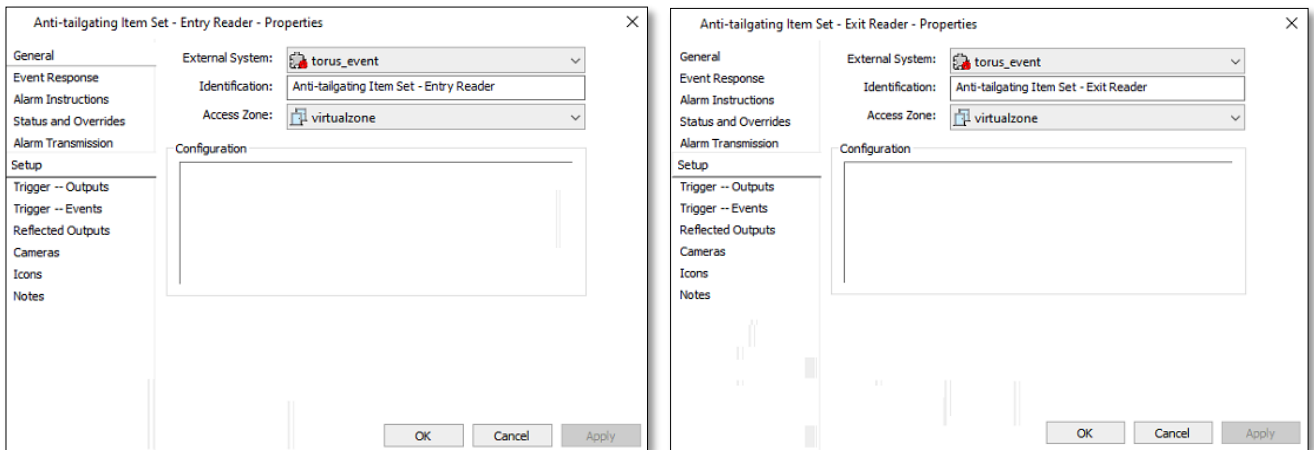
- ❖ Setup Tab
 - Select relevant External System and Access Zone.
 - Identification field - Give the same name as used in the External System Item Name field in the Torus Integration Record.



8.4 – Create virtual entry and exit readers in Command Centre

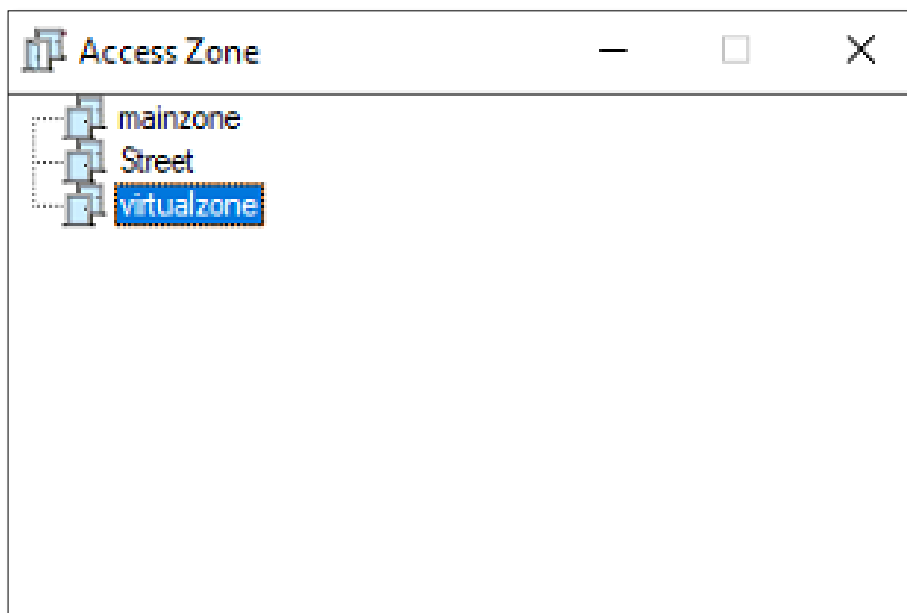
- To setup anti tailgating, create two more external items which are virtual entry and exit readers.
- For each external item **identification** field please use the names as shown in Torus External system entry and exit reader names in the anti- tailgating tab of the integration record.

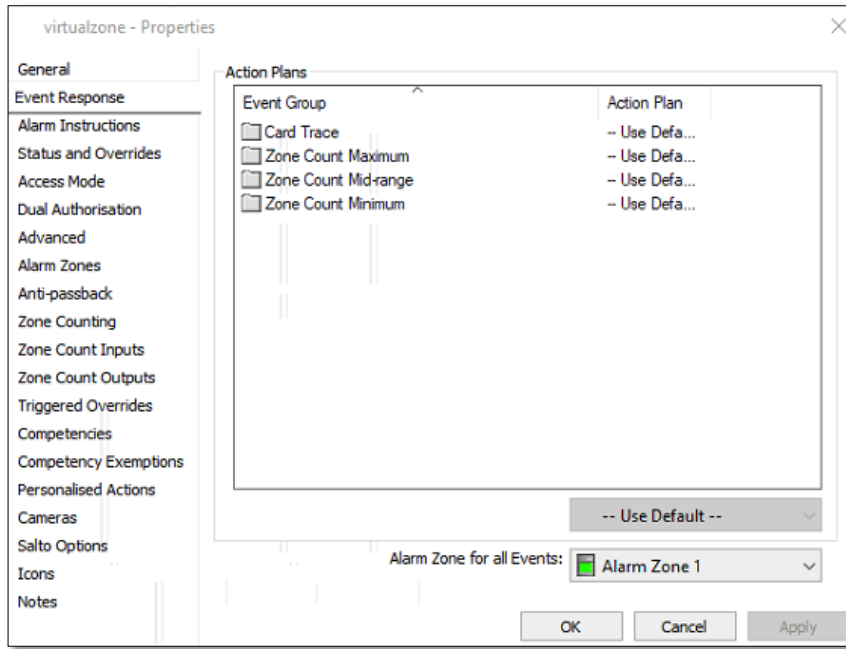




8.5 – Create virtual zone in Command Centre

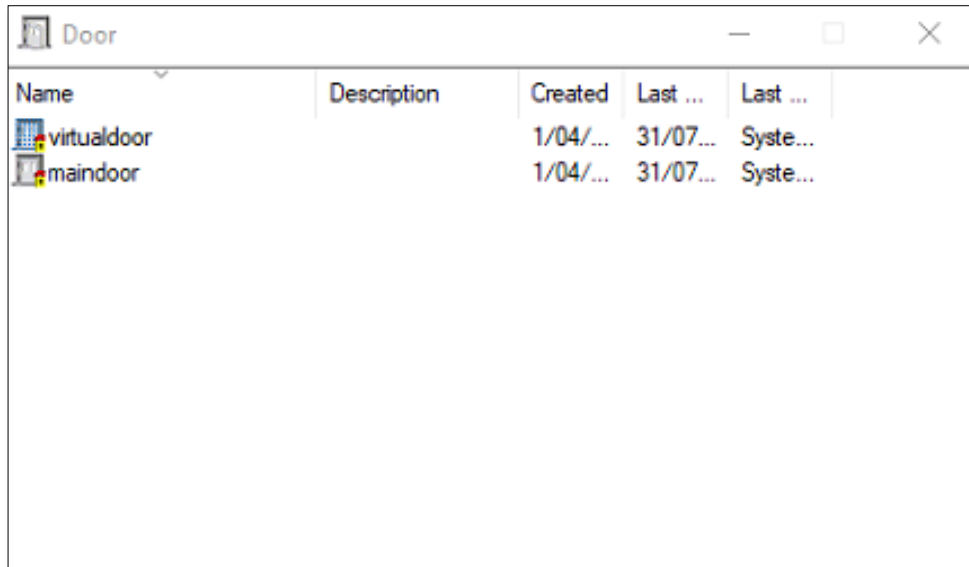
- A virtual zone is also required to virtually place the Torus cabinets inside this Virtual Zone.
- Create a Virtual Zone and select the correct Alarm Zone for tailgating events. Go to Command Centre, configure>Access Zones and create a virtual Zone.



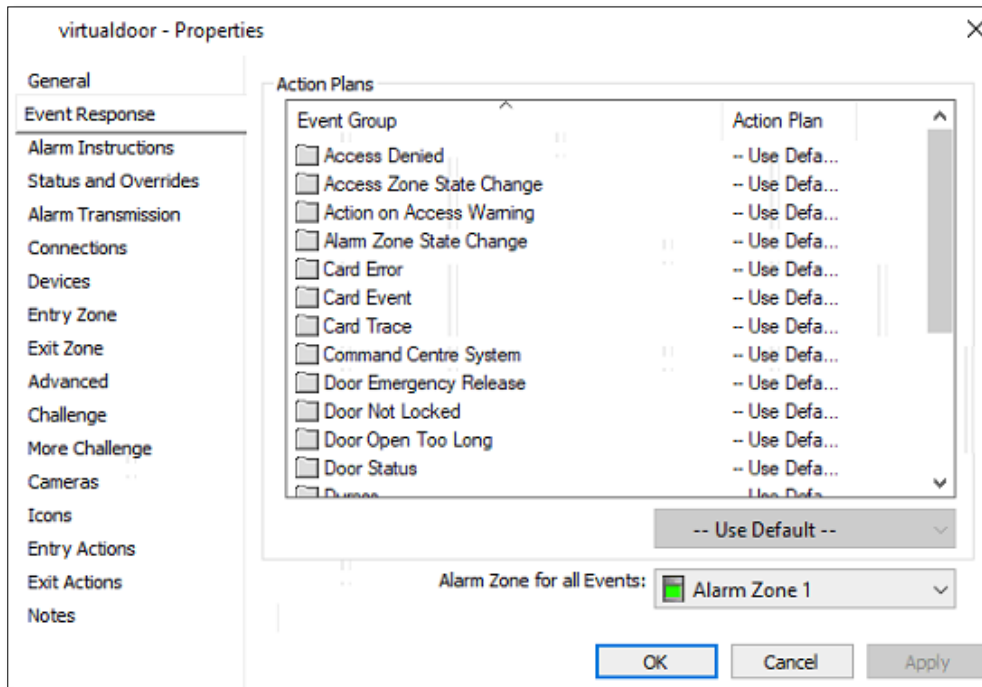


8.6 – Create virtual door in Command Centre

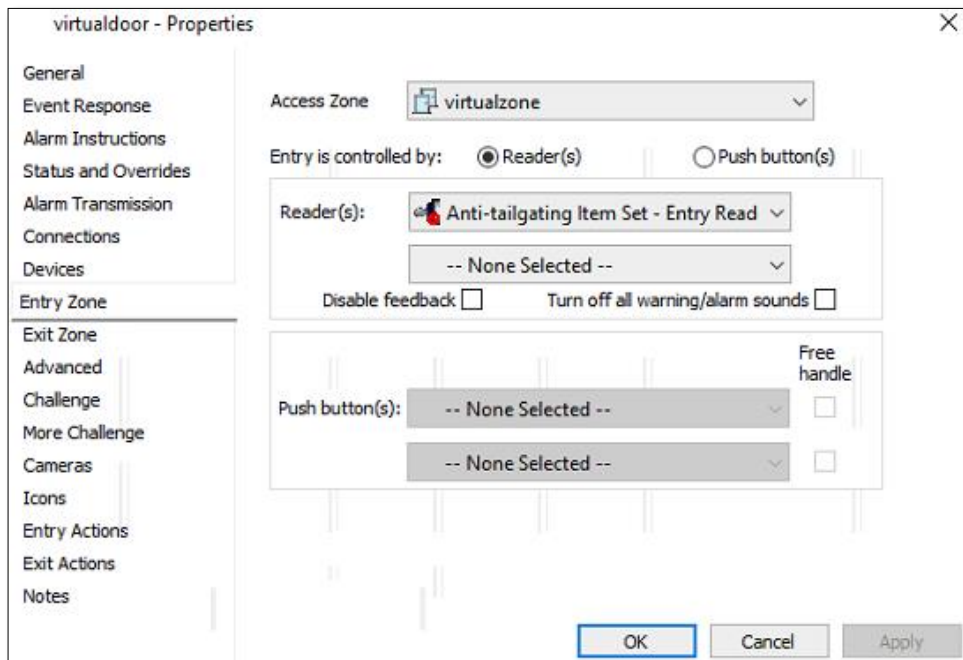
- For Anti-Tailgating, a virtual door is required. Go to Command Centre, Configure >Door and create a virtual door.



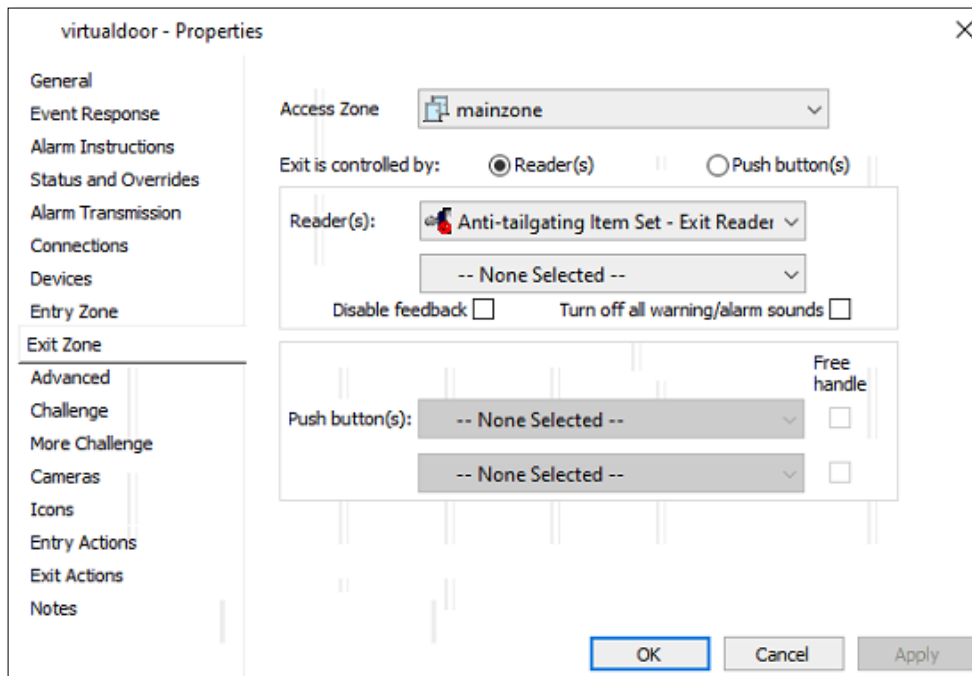
- Use correct Alarm Zone for anti-tailgating event.



- 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



- 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



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.

