Command Centre v8

Feature summary

security.gallagher.com

GALLAGHER

Contents

1 Introduction

Welcome to the latest version of Gallagher Command Centre.

Years of planning and months of continuous development from the Gallagher R&D team brings you Command Centre v8. Grab a coffee, sit back, and take a moment to review the latest features and enhancements introduced in this stunning release.

Note: This document does not describe the entirety of Command Centre — only what's new in v8.

ⓘ Important information

+♡ Business value — why we do what we do

2 Compatibility

This section contains important notices that must be read when considering Command Centre v8.

2.1 Upgrading Command Centre

Command Centre license file

Sites upgrading to Command Centre v8 from a previous version (v7.90 or earlier) will require an updated Command Centre license file (CommandCentre.lic). To obtain an updated license file, a Command Centre software upgrade or software maintenance must be purchased.

Note: Changes made to Command Centre v8 may impact on the configuration of sites upgrading from earlier versions. Refer to the document *"3E0068 Release Note Command Centre vEL8.00.xxx (Upgrade Procedures).pdf"* for details.

Supported upgrade paths

Command Centre v7.60 – Command Centre v8
Command Centre v7.70 – Command Centre v8
Command Centre v7.80 – Command Centre v8
Command Centre v7.90 – Command Centre v8

Controller firmware compatibility

This version of Command Centre is compatible with versions vBT7.80//bxxx and vGR8.00//bxxx Controller firmware. It is also compatible with previous versions of Controller firmware for upgrade purposes only. No configuration changes should be made on pre-version 8.00 Controllers once Command Centre has been upgraded.

Important: vBT7.80//bxxx is the last version for legacy Controllers, (i.e. 5000GL, 5000, 3000-8R, and 3000-4R). While there are no vBT8.00 versions for these Controllers, those on a vBT7.80//bxxx version will still be compatible with vEL8.00 of Command Centre, and Gallagher will continue to support for existing feature related bugs until their end of life in April 2020.

IMPORTANT: Upgrading a Controller 6000 to v8

When upgrading a Controller 6000 from a version prior to v7.30, the upgrade time will be longer than usual. This is to resolve an issue where the Controller may fail after upgrading that was resolved in v7.30.

- The Controller is expected to be **offline for approximately 9 minutes and 30 seconds**. The normal offline time is approximately 2 minutes and 15 seconds.
- While the Controller is offline the Controller's Run LED will enter a slow flash pattern, this is expected and should not be interrupted.
- A version of this fix is available in v7.20 (vGR720685.fts) and v7.10 (vGR710401.fts) from our FTP server. Sites that are on v7.20 or v7.10 can apply this fix to their Controllers to protect them against this issue.
- Controllers with serial number 1508000000 or higher already have this fix applied and therefore will upgrade in the normal expected time.

This longer upgrade will only need to be done once for each Controller. If the Controller has already been upgraded to v7.30 then this will not be an issue and subsequent upgrades including the upgrade from v7.30 to v8 will return to normal timings. For further information, please contact Gallagher Security Technical Support.

2.2 Supported operating systems

Command Centre Server	Minimum Service Pack / Build
Windows 10 Pro / Enterprise	1607
Windows 8.1 Pro / Enterprise	n/a
Microsoft Windows Server 2016	n/a
Microsoft Windows Server 2012 / R2	n/a
Microsoft Windows Server 2008 R2 (64-bit only)	SP1
Microsoft Windows 7 Professional / Ultimate	SP1

Command Centre Workstation	Minimum Service Pack / Build
Windows 10 Pro / Enterprise	1607
Windows 8.1 Pro / Enterprise	n/a
Microsoft Windows 7 Professional / Ultimate	SP1

Note: Command Centre is supported on a virtual server. However, due to virtual server environment configuration variability, if initial fault resolution is inconclusive Gallagher reserves the right to request customer replication of any errors in a non-virtual environment. Command Centre installation is not supported on a Windows domain controller.

2.3 Supported databases

Command Centre Database	Minimum Service Pack
Microsoft SQL Server 2017 / 2017 Express	n/a
Microsoft SQL Server 2016 / 2016 Express	SP1
Microsoft SQL Server 2014 / 2014 Express	SP2
Microsoft SQL Server 2012 / 2012 Express	SP3
Microsoft SQL Server 2008 R2 / 2008 R2 Express	SP3

Note: SQL Server 2017 Express is the default freely available database for Command Centre.
Both 32-bit and 64-bit versions of the above databases are supported.

2.4 Supported monitor resolution

Command Centre v8 is supported on monitors with a minimum vertical resolution of 720px. Command Centre will continue to display correctly on lower resolutions, however some of the larger light boxes, such as the 'Assign Access' light box will be truncated.

2.5 Command Centre licensing changes

Key device policy

From Command Centre v7.00 a new key device policy was introduced. This policy is described below, and relates to the process for changes to key devices in the Command Centre license file.

- **Command Centre licensing**
  Key devices are licensed in Command Centre. A key device can be any Controller permanently installed and communicating with the Command Centre server. Each site can have one or two key devices. The key devices are identified in the license file at the time of its purchase from Gallagher.
- **Key device failure**
  Should a key device fail or be removed from the site for any reason an alarm will be raised in Command Centre. Prior to Command Centre v7.00, only the last key device removed from the system generated an alarm. From Command Centre v7.00 or later, any key device removed will generate an alarm. When the last key device is removed, if the license file is not updated or the key device returned, after an elapsed period of time the system will become read-only.

License updates

When Gallagher is requested by a Certified Channel Partner to update the key devices in a site license file, due to failure or removal of the key device from that site, Gallagher requires that the key device is sent back to the nearest Gallagher regional sales office within 30 days. Should the Channel Partner not be able to return the key device then Gallagher reserves the right to invoice the Channel Partner for the full cost of the site’s Gallagher Command Centre software based on the price list in effect at the date of invoice.

2.6 Command Centre Mobile app compatibility

Device	Operating System
iPhone 4S or later	iOS 9.0 or later
iPad 2, iPad Mini or later	iOS 9.0 or later
Android	5.0 or later

2.7 Command Centre Mobile Connect app compatibility

Device	Operating System
iPhone 5S or later	iOS 10 or later
Android	5.0 or later

3 Features

3.1 Site Plan Viewer

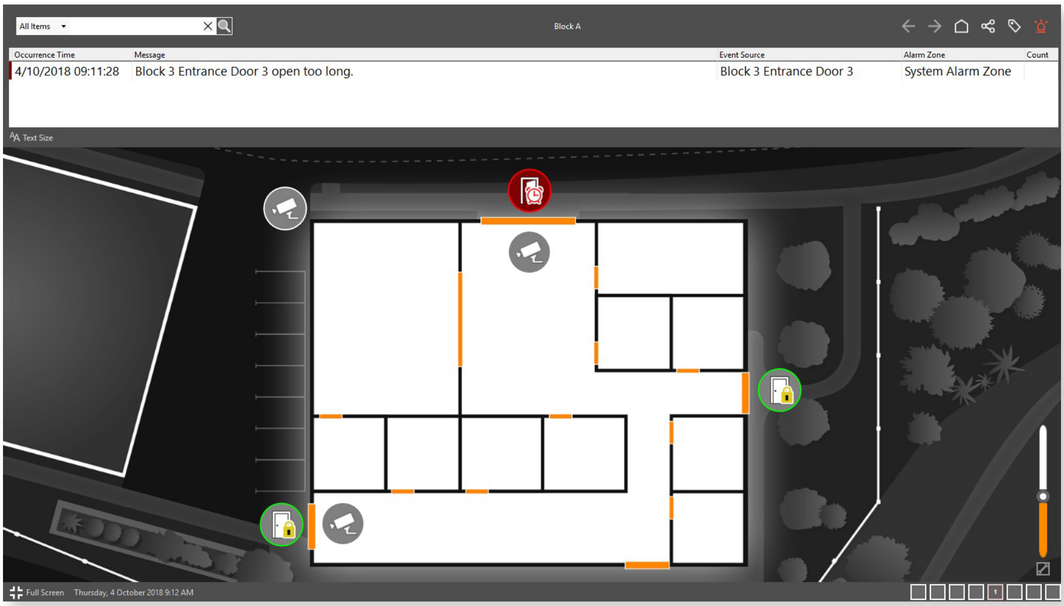
The Site Plan Viewer provides full screen, centralized site management visibility and situational awareness for all site buildings and perimeter, whether local or remote. An operator simply clicks on the item to reveal the information required and is able to perform the action required — the operator need not leave the screen.

Information is displayed in real-time, allowing quick and accurate response to security threats, and ensuring operational continuity and site safety. The improved user experience minimizes operator error, reducing risk on site. The intuitive interface reduces operator training/induction time.

The flexibility in configuration allows for minimizing clutter, working alongside the privilege model means operators won't be distracted with options that are not configured or they do not have the authority to use.

Operators have the ability to search for known items on a site plan, or navigate only to items in alarm.

Newly created site plans provide pan and zoom navigation, improving the operational experience around larger sites, allowing operators to focus on specific areas.



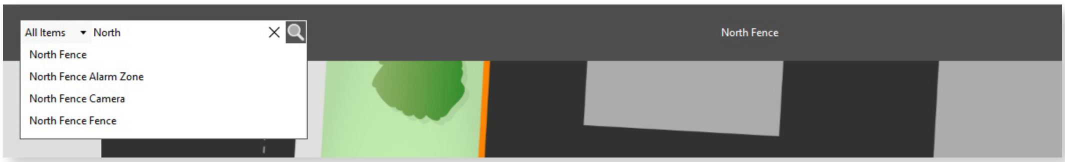
Occurrence Time	Message	Event Source	Alarm Zone	Count
4/10/2018 09:11:28	Block 3 Entrance Door 3 open too long.	Block 3 Entrance Door 3	System Alarm Zone	

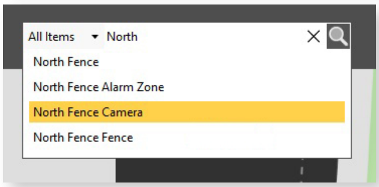
For a number of sites, the Site Plan Viewer will provide a single screen navigation for monitoring and alarm management.

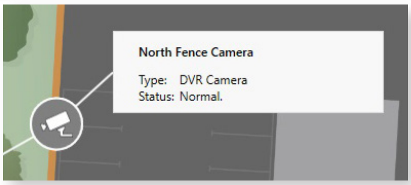
Site Plan tiles in Command Centre will continue to operate as they do presently, although for newly created site plans the ability to pan and zoom is added. The Site Plan Viewer operates slightly differently from a Site Plan tile in that, the Site Plan Viewer is primarily a visual navigation.

Find tool

The Find tool provides operators with a quick and easy way to find items on a site plan.






North Fence Camera

Type: DVR Camera
Status: Normal.

An operator can search on:

- configured item name,
- item description, or
- the label given to the item on the site plan.

Selecting the item takes the operator directly to the item on any site plan and presents the relevant item menu.

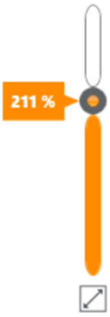
Imagine the control room taking a call from some one in charge of a building being able to find the Door or Access Zone and being able to perform an override immediately. With the item menu configured to display cameras, a quick check can be made to ensure any untoward risk is minimized.

Navigation buttons allow an operator to navigate backwards and forwards through viewed site plans, as well as returning to the home site plan as configured in the Viewer.

Panning and zooming

Panning and zooming provides improved navigation around larger site plans. It is supported in the Site Plan Designer, the Site Plan Viewer and Site Plan tiles.

Within the Site Plan Designer this function is available at all times for creating and editing site plans. Within the Site Plan Viewer and Site Plan tiles, the function allows operators that deal with very busy site plans to focus on a specific area within the site plan.



An operator can disable panning and zooming within the Site Plan's properties.

Note: Site Plans created in the Configuration Client will by default not have panning and zooming enabled.

Sharing site plans

Where information needs to be shared with guards and/or technicians or captured in incident and hand over reports, the information is easily copied, printed and/or shared via email.

Items on a site plan

Alarm presentation options ensure operators don't miss important events. All site items added to a site plan are stateful, (i.e. that is they can display an operational state and an alarm state).

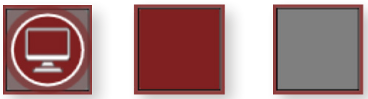
Operational states

For items represented by icons, the operational states are reflected in different icons within the icon set. If the item is represented by a shape or line, the different operational states are displayed in the colors set up against the icon sets.

Alarm states

For icons with items in alarm, the icon will change to the color of the alarm priority and will pulse when in alarm. For shapes and lines with items associated, there is a choice in the configuration for how alarm behavior is presented. This includes:

1. Displaying an alarm indicator (the default icon for the item associated)
2. The full shape flashing
3. Only the shape border pulsing



Selecting an item on the site plan

Selecting an item (icon or shape) on a site plan will present an item menu set up to provide the required information and actions available to the operator. This is determined by whether the item is in alarm or in normal operation.

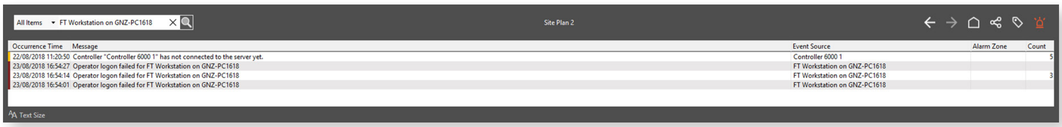
As with the rest of Command Centre, if the operator does not have privileges to see the information, the controls within the item menu will not be displayed.

If the information is not available, or for the item selected there is no configuration for a control this will not be displayed.

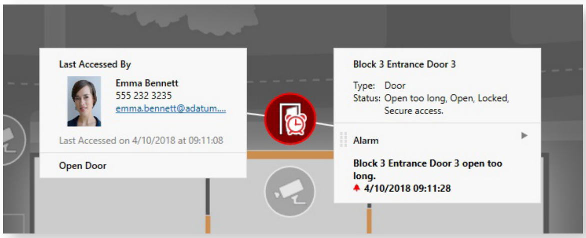
Managing alarms

Items in alarm

A toggle style alarm list provides operators with a list of the highest priority alarms. Selecting the alarm directs the operator immediately to the event source item and presents the relevant alarm information and available actions to be taken.



Occurrence Time	Message	Event Source	Alarm Zone	Count
22/08/2018 11:20:50	Controller "Controller 6000 1" has not connected to the server yet.	Controller 6000 1		5
23/08/2018 16:54:27	Operator logon failed for FT Workstation on GNZ-PC1618	FT Workstation on GNZ-PC1618		
23/08/2018 16:54:14	Operator logon failed for FT Workstation on GNZ-PC1618	FT Workstation on GNZ-PC1618		3
23/08/2018 16:54:01	Operator logon failed for FT Workstation on GNZ-PC1618	FT Workstation on GNZ-PC1618		



Last Accessed By

Emma Bennett
555 232 3235
emma.bennett@adatum....

Last Accessed on 4/10/2018 at 09:11:08

Block 3 Entrance Door 3

Type: Door
Status: Open too long, Open, Locked, Secure access.

Alarm

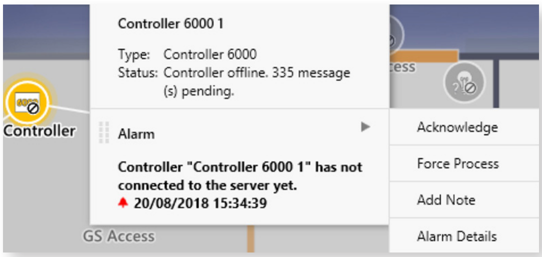
Block 3 Entrance Door 3 open too long.
▲ 4/10/2018 09:11:28

Acknowledging and processing alarms

Selecting an item in alarm will present the item menu configured for this purpose.

The Alarm Summary control is presented and if there is enough information for the operator to acknowledge or process the alarm this option can be taken.

If there are alarm instructions configured these can be displayed as a part of the item menu. This will present alarm instructions as configured in the Configuration Client or launch a browser to the configured URL for web-based instructions/videos. If further alarm details are required, this can be opened and dragged to another monitor if needed.

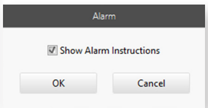


Controller 6000 1

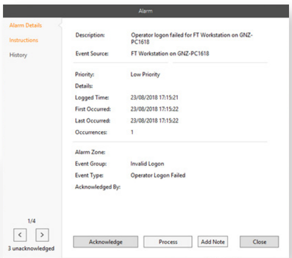
Type: Controller 6000
Status: Controller offline. 335 message (s) pending.

Alarm

Controller "Controller 6000 1" has not connected to the server yet.
▲ 20/08/2018 15:34:39



☑ Show Alarm Instructions



Description: Operator logon failed for FT Workstation on GNZ-PC1618
Event Source: FT Workstation on GNZ-PC1618

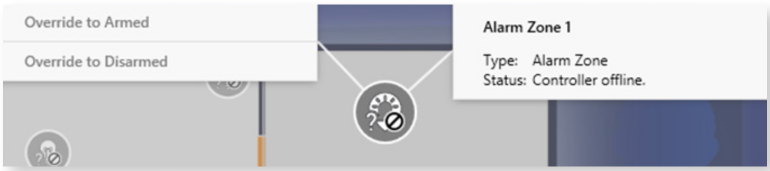
Priority: Low Priority
Details:
Logged Time: 23/08/2018 17:15:21
First Occurred: 23/08/2018 17:15:22
Last Occurred: 23/08/2018 17:15:22
Occurrences: 1

Alarm Zone:
Event Group: Invalid Logon
Event Type: Operator Logon Failed
Acknowledged By:

3 unacknowledged

Arming/disarming alarm zones

The system allows the ability to change alarm zones from one state to another outside the scheduled times by providing overrides for configurable time periods. The change of state is reflected in either the icon or the shape if configured to display the state.



Alarm Zone 1

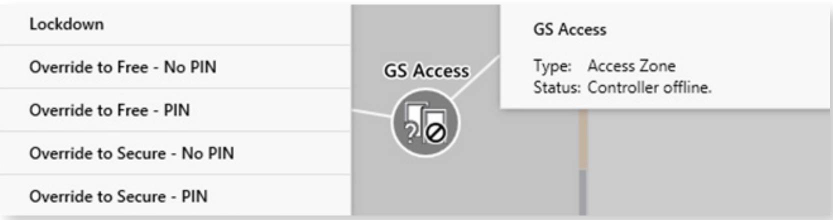
Type: Alarm Zone
Status: Controller offline.

Managing access

Changing access times

The system allows the ability to change Access Zones from one state to another outside the scheduled times by providing overrides for configurable time periods.

For example, 'Free Access' to 'Secure' with a card required. The change of state is reflected in either the icon or the shape if configured to display this.



GS Access

Type: Access Zone
Status: Controller offline.

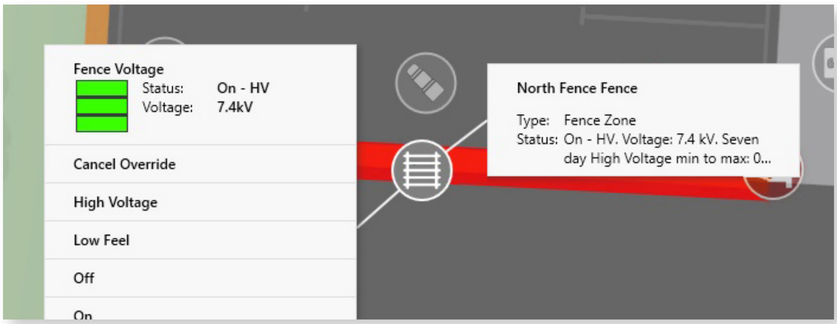
Opening doors

As a button added to the site plan or as a control available as a part of the doors items menu. Paired with a camera control the operator is able to see who is at the door and select the option to open the door remotely.

Arming/disarming perimeter fences

Perimeter fencing can be controlled by schedules or manually managed via overrides. Turning the fence on/off or switching between High Voltage and Low Feel is achieved by performing the overrides that can be presented to an operator in an item menu.

These overrides can also be set up individually as a button. The advantage here is that status and voltage is reflected immediately on the site plan.



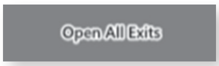
Fence Voltage
Status: On - HV
Voltage: 7.4kV

North Fence Fence

Type: Fence Zone
Status: On - HV. Voltage: 7.4 kV. Seven day High Voltage min to max: 0...

Buttons

Buttons added to the site plan allow for quick repeatable actions such as setting the site to lockdown (or cancelling lockdown), evacuation, running pre-programmed controls (macros), or simply opening a door.



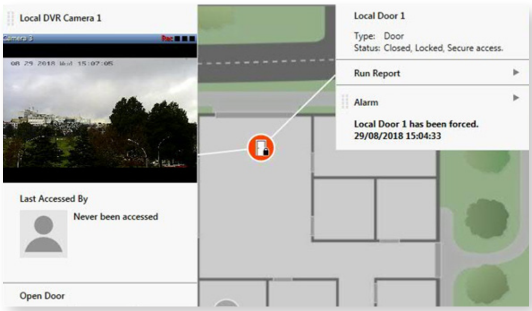
Site monitoring

Camera control

Item menus on the site plan can be configured to display one or multiple cameras providing the ability to view footage associated with an item or alarm triggered activity.

If the operator wishes to maintain visibility, the control can be dragged to another monitor to continue streaming whilst performing other activities on the site plan, or elsewhere in the system.

Cameras can either be set up against a specific item or added to the site plan. Camera systems are integrated as a part of Gallagher's CCVMS Framework.



Local DVR Camera 1

08-29-2018 Wed 15:07:05

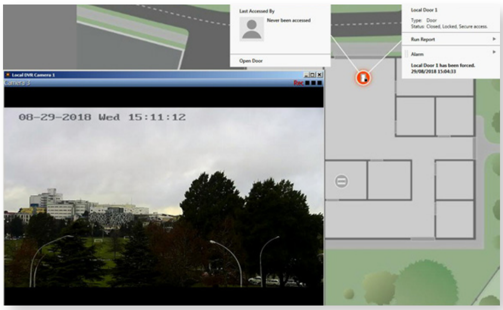
Last Accessed By

Never been accessed

Local Door 1

Type: Door
Status: Closed, Locked, Secure access.

Local Door 1 has been forced.
29/08/2018 15:04:33



Local DVR Camera 1

08-29-2018 Wed 15:11:12

Last Accessed By

Never been accessed

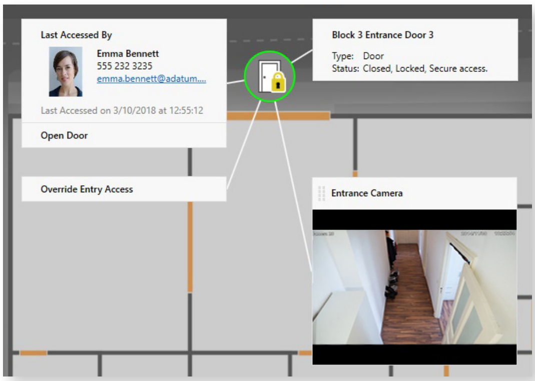
Local Door 1

Type: Door
Status: Closed, Locked, Secure access.

Local Door 1 has been forced.
29/08/2018 15:04:33

Last person through a door

A common request is to understand who the last person through a door was, particularly when there are DOTL alarms. This item menu control can be set up to display the name, contact details, and a photo of the Cardholder last gaining access through a door.



Last Accessed By

Emma Bennett
555 232 3235
emma.bennett@adatum....

Last Accessed on 3/10/2018 at 12:55:12

Block 3 Entrance Door 3

Type: Door
Status: Closed, Locked, Secure access.

Contextual reporting

Understanding activity on the selected item is the driver behind providing an ability to contextually report by selecting the **Run Report** option.

An operator can run a pre-configured report or reports from the selected item, to view the Cardholders that passed through a door, for example or any event activity or statistics on the item.

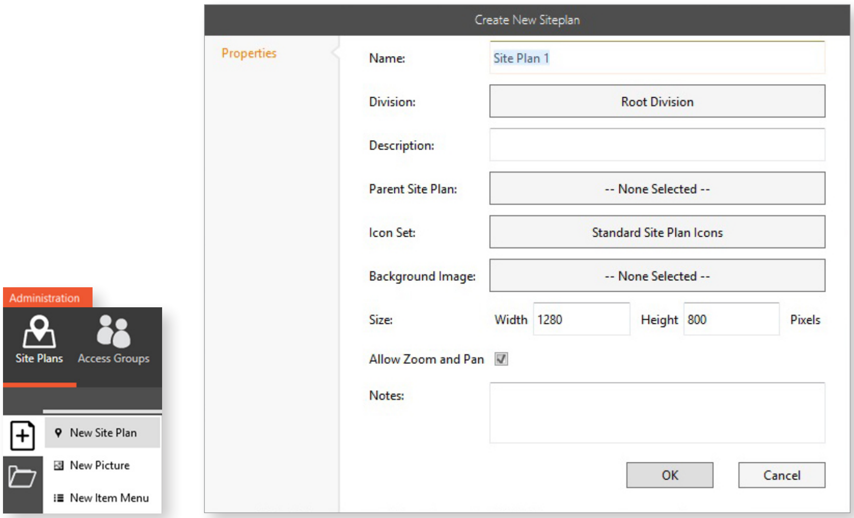
3.2 Site Plan Designer

The Site Plan Designer allows quick and easy creation of a visual representation of the customer's site for security operations (particularly control rooms) managing their security needs.

Time spent configuring and setting up systems can be a sizable expense for channel partners where quite often the physical hardware installation is the primary focus.

Command Centre site plans are quicker to configure, easier to create and maintain, and more intuitive leading to less training time and reduced costs.

The Site Plan Designer is a new tool in the Administration Suite of Command Centre. The designer has been purposefully designed for creating a visual navigation interface for operators in a way that operators looking after site administration can create and maintain site plans with relative ease.



Name: Site Plan 1
Division: Root Division
Description:
Parent Site Plan: -- None Selected --
Icon Set: Standard Site Plan Icons
Background Image: -- None Selected --
Size: Width 1280 Height 800 Pixels
Allow Zoom and Pan ☑
Notes:

Site plan properties

The first step in setting up site plans is deciding what the site plan will be used for, how they are to be structured, and deciding what background is required for location context.

Background images provides a search for any pre-loaded images. Site plans support the following background image file formats: DXF, PDF, PNG, JPEG, or BMP.

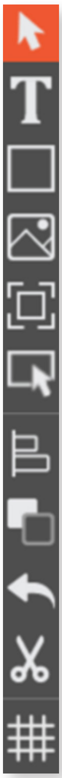
Depending on the purpose of the site plan, the option to allow/not allow zooming and panning is provided as apart of the configuration.

Basic tools

Anyone with a basic drawing package knowledge will have no problem creating spectacular looking site plans. Whilst not specifically a drawing package, most of the tools you would expect are provided, (i.e. snap to grid, cut copy and paste, Z-ordering, and undo/redo).

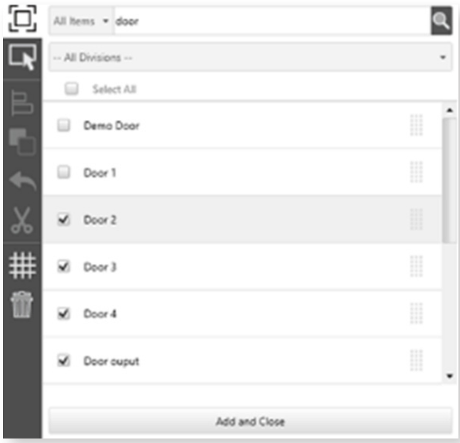
Whether using the existing icons or creating shapes and lines to represent items and areas, the ability to resize, rotate, position and/or align with other items, allows a site plan to be created quickly with little effort or experience required.

The ability to add pictures and text allows for additional contextual information to be added.



Adding items as icons to the site plan

For the most part adding all the items that need to be monitored to a site plan will be represented as an icon.



All Items ▾ door

-- All Divisions -- ▾

□ Select All

□ Demo Door

□ Door 1

☑ Door 2

☑ Door 3

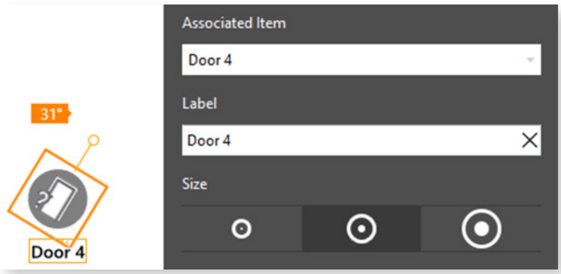
☑ Door 4

☑ Door ouput

Add and Close

The search tool allows multiple items to be added at the same time. Whether searching for a specific item or a group, the selection can be dragged into position on the site plan and organized as required.

Once positioned, the icon can be rotated, sized, and labelled if needed.



Associated Item

Door 4

Label

Door 4

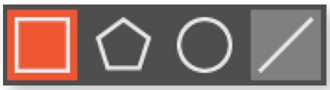
Size

Adding areas or shapes

As an alternative to icons, shapes can be added to the site plan to represent any item. More commonly these are used to represent zones or areas, with lines being used to represent perimeter fences.

Shapes can also be added without any stateful behavior as a part of the drawing background, without associating any monitored system item.

The line and area tool may be used to trace certain areas of the background if the background image is being removed.

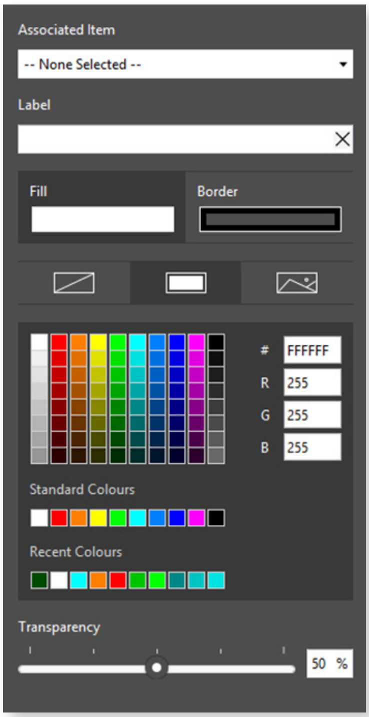


- On completion of drawing a shape, the shape properties are presented where an operator can associate an item, which applies preset colors and provides alarm options

  or

- not associate an item and determine:
  - border color and width
  - fill color or fill picture content.

Labels will default for shapes with associated items but can be changed to something more meaningful (and searchable) to the operator. All labels can also be repositioned.



Associated Item: -- None Selected --

Label:

FFFFFF

R 255

G 255

B 255

Transparency 50 %

Adding buttons

As an alternative to icons, shapes can be added to the site plan to represent any item. More commonly these are used to represent zones or areas, with lines being used to represent perimeter fences.

Adding text and pictures

Pictures can be used in site plans for a number of reasons, identifying other areas of interest to an operator, (e.g. emergency equipment, (i.e. fire hydrants, first aid) important makers for ease of access, muster points, dangerous or high-risk areas, but also for branding, diagram keys, and compass). Rectangles and images can be rotated and resized as required.

Likewise text can be added for annotations and instructions, area names, or labelling. The Text tool supports sizing emphasis alignment and the workstation's available fonts.

Picture management

Site Plan Designer picture management will support the following types of image file formats: DXF, PDF, PNG, JPEG, and BMP.

Picture management supports the loading of picture files for easy retrieval and for updates as the single source of change. This means if you have used this picture in multiple places throughout site plans, swapping the image will make the change everywhere this image appears, (e.g. backgrounds, static icons, branding, diagram keys, and compass).

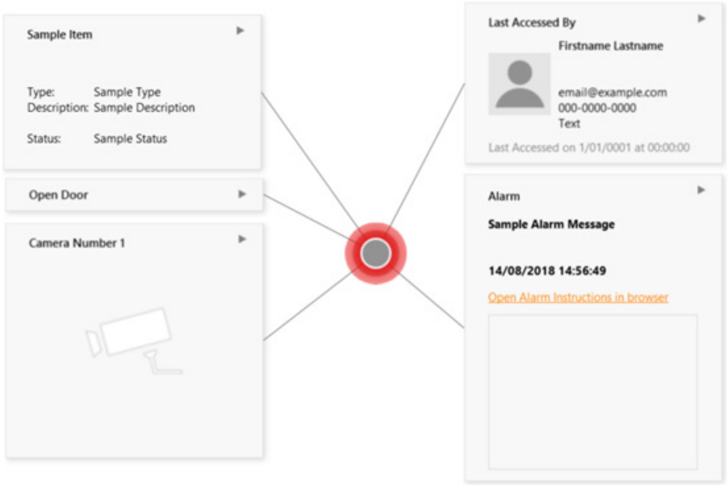
Pictures can be used in site plans for a number of reasons, primarily as background images associated during the initial configuration or for identifying other areas of interest to an operator, (e.g. emergency equipment, (i.e. fire hydrants, first aid) important makers for ease of access, muster points, and dangerous or high-risk areas).

Item menu management

Site Plan Designer item menu management provides the ability to customize what an operator will see when selecting an item on a site plan.

Item menus are pre-configured, that is, there will be default configuration that will not require additional work to set up unless there is a desire to change the layout of the information and available actions.

Note: This method of controlling which overrides are viewable to an operator should *not* be used as a substitute for Command Centre's privilege model.



Sample Item

Type: Sample Type
Description: Sample Description
Status: Sample Status

Open Door

Camera Number 1

Last Accessed By

Firstname Lastname

email@example.com
000-0000-0000
Text

Last Accessed on 1/01/0001 at 00:00:00

Alarm

Sample Alarm Message

14/08/2018 14:56:49

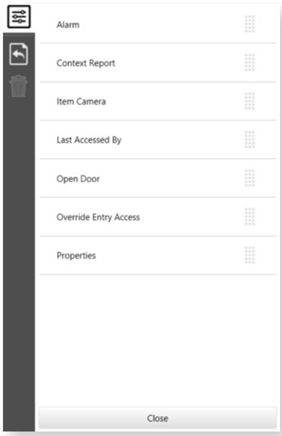
Open Alarm Instructions in browser

Item menus can be configured to appear differently when the item selected is in alarm. The controls provided within the item menus are dependent on the type of item selected.

These may include:

- View who the last person was through the door.
- To see the footage associated with cameras
- Allow operator to perform an override or action
- Run a Macro (pre-programmed control)
- Run a contextual report
- The Alarm Control, allows the operator to view details about an alarm and perform the required action.

The controls can be added by dragging them from the control list and placing them in the preferred position. Some control may have additional parameters to be set. The controls can also be deleted as required.



Upgrading from legacy site plans

The existing Configuration Client legacy site plans will appear slightly different in the Command Centre Client. The legacy icons will automatically switch to the new Command Centre icons and any icon scaling will be applied.

The legacy site plans will work with the newly implemented item menus in the new Site Plan Viewer however all legacy site plans will not have panning and zooming.

Legacy site plans are not editable in the Site Plan Designer, however recreating a Configuration Client site plan in the Command Centre Site Plan Designer is made easier with the existing site plan backgrounds pre-loaded in picture management.

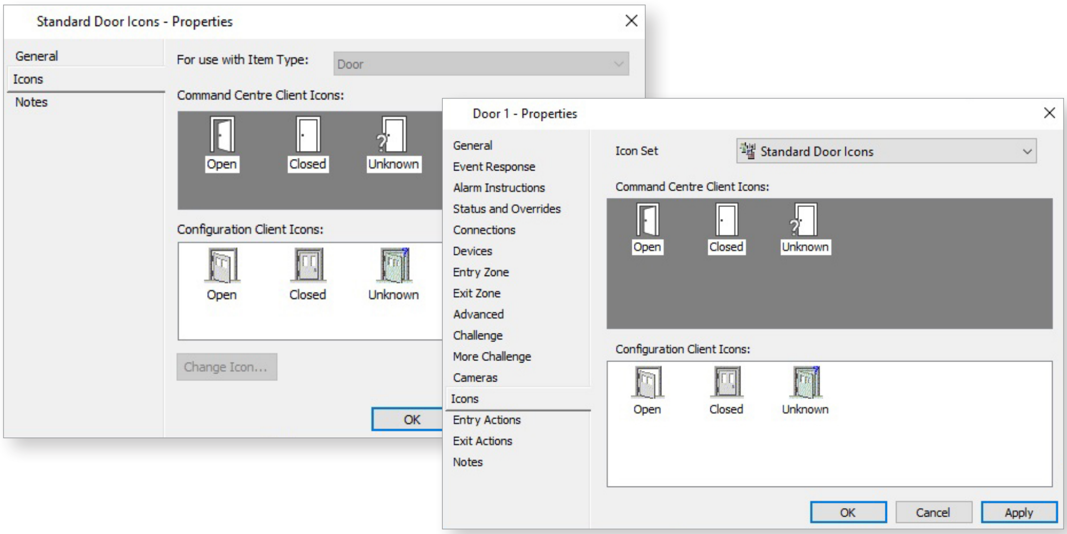
Icons

Fresh new icons and extended support for customizable icons.

For the most part the icons displayed are stateful. They display whether or not an item is functioning normally from an operational perspective, and in what mode or state the item is in.

Icon configuration has been extended to allow different icons to be used in the Configuration Client (for legacy site plan users) and in the Command Centre Client.

The icons themselves are small image files in ICO file format. Version 8 includes the support for PNG icon file format. This allows customers to easily customise or create alternative icons for items, without the need for specialized drawing packages.



Standard Door Icons - Properties

For use with Item Type: Door

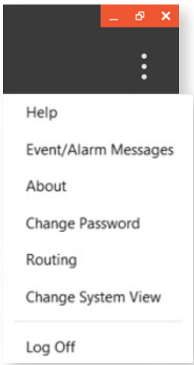
Door 1 - Properties

Icon Set: Standard Door Icons

Overflow menu

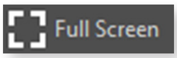
The overflow menu contains functions common across all viewers and tabs in Command Centre.

Note: Depending on license and or privilege, the items in this menu may vary.



Full screen mode

At the bottom of all viewer screens there is now a **Full Screen** option to allow better use of the screen real estate. This is a toggle type button that will hide tabs and other viewer buttons.



3.3 Broadcast Notifications to Mobile Connect

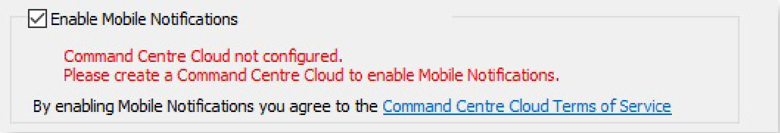
Communicate important information efficiently with Cardholders especially in emergency situations ensuring staff, students, and contractors are well informed of security and safety situations.

Broadcast Notifications is a feature in Command Centre developed to communicate simply and quickly with multiple Cardholders. Complementing existing email and SMS communication methods, Mobile Connect users can now receive Broadcast Notifications sent as push notifications to their device.

In emergency or lockdown situations where Cardholders could be in danger, pre-configured Broadcast Notifications and recipient lists allow security personnel to quickly send critical instructions to multiple Cardholders in one simple step. Broadcast Notifications can also be automatically triggered by alarms and events. In less time-sensitive applications, ad-hoc Broadcast Notifications are a valuable tool to communicate hazards, manage compliance, and prompt Competency renewals for specific Cardholder groups.

Configuration

Broadcast Push Notifications to Mobile Connect leverages the cloud used for Alarm Push Notifications to Command Centre Mobile Clients. To enable mobile notifications check the **Enable Mobile Notifications** check box on the **Mobile/SMS** Server Properties page.



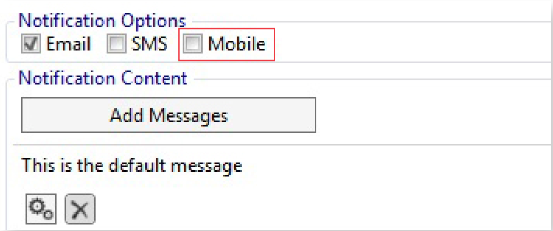
☑ Enable Mobile Notifications

Command Centre Cloud not configured.
Please create a Command Centre Cloud to enable Mobile Notifications.

By enabling Mobile Notifications you agree to the Command Centre Cloud Terms of Service

Operation

The Broadcast Notifications Administration Viewer includes an option to send Broadcast Notifications to email, SMS, and now Mobile.



Notification Options

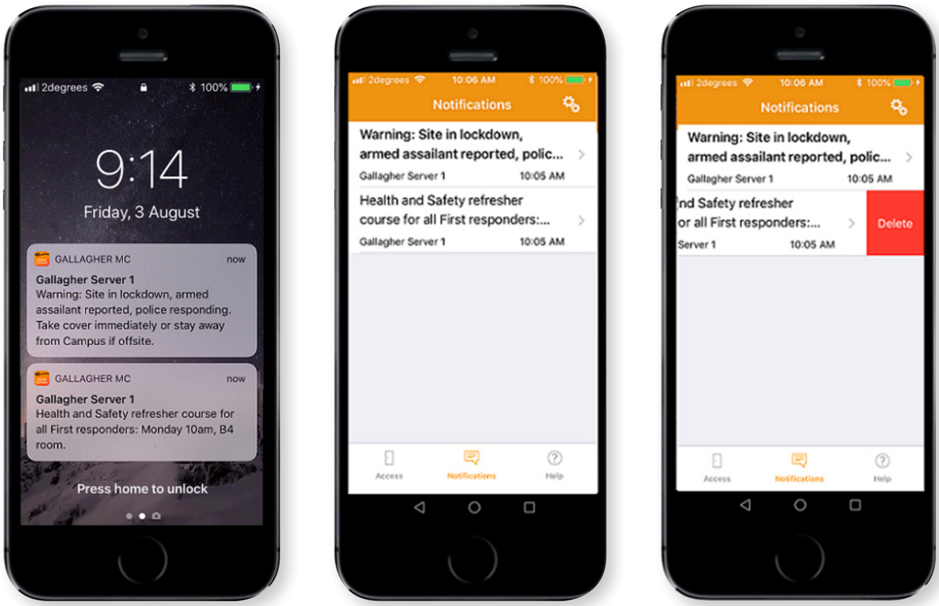
☑ Email ☐ SMS ☐ Mobile

Notification Content

This is the default message

Broadcast Notifications received at the device appear as app notifications, allowing for a fast reliable communication method to staff, contractors, students, and visitors.

If a device has notifications turned off for the Mobile Connect app the above front-screen notifications will not appear. The Mobile Connect app stores the notification inside the app, so a record remains if the initial notification is not seen, ignored, or deleted too soon. The storage of push notifications in the Mobile Connect app will occur regardless of local notification settings.



Gallagher Server 1
Warning: Site in lockdown, armed assailant reported, police responding. Take cover immediately or stay away from Campus if offsite.

Gallagher Server 1
Health and Safety refresher course for all First responders: Monday 10am, B4 room.

Warning: Site in lockdown, armed assailant reported, polic...
Gallagher Server 1 10:05 AM

Health and Safety refresher course for all First responders:...
Gallagher Server 1 10:05 AM

Warning: Site in lockdown, armed assailant reported, polic...
Gallagher Server 1 10:05 AM

nd Safety refresher or all First responders:...
Server 1 10:05 AM

Licensing

Broadcast Push Notifications require a Cardholder to have an active mobile credential. This feature is enabled when a site is licensed for Mobile Credentials.

3.4 Status REST API

The Status REST API provides a set of HTTP functions to query the status of items within Command Centre, allowing developers to integrate multiple systems with Command Centre. It adds to Command Centre's integration flexibility and inter-operability with other systems.

Background

The Status REST API uses HTTP to obtain the current status of items within Command Centre. It is easy to use, easy to test, and provides superior integration performance. A REST API is independent of the language used by each system, hence it promotes longevity and evolution of both systems. It allows a site to use independent developers to quickly integrate their systems. All data is securely transferred using a secure token and a pinned certificate with optional IP filtering.

Solutions that can be achieved via integration using this API are:

- Overlaying door status onto a camera view on a video system
- Displaying live fence voltages on a security dashboard
- Providing floor zone counts to a BMS application to efficiently monitor power

Functionality

Status for the following items is available:

- Door
- Access Zone (including zone count)
- Alarm Zones
- Fence Zones (including fence voltage)
- Outputs

Licensing

The Status REST API is a licensed feature of Command Centre.

Availability

Available with Command Centre v8. The Event and Alarm REST API was released with v7.80.
The Cardholder REST API was released with v7.90.

3.5 Overrides REST API

The Overrides REST API provides a set of HTTP functions to override items within Command Centre, allowing developers to integrate multiple systems with Command Centre. It adds to Command Centre's integration flexibility and inter-operability with other systems.

Background

The Overrides REST API uses HTTP to override specified items within Command Centre. It is easy to use, easy to test, and provides superior integration performance. A REST API is independent of the language used by each system hence it promotes longevity and evolution of both systems. It allows a site to use independent developers to quickly integrate their systems. All data is securely transferred using a secure token and a pinned certificate with optional IP filtering.

Solutions that can be achieved via integration using this API are:

- Provide ability to open a door from a video management platform
- Perform a lockdown from a third party emergency system
- Trigger an open door override from an intercom or phone system
- Escalate a high voltage override of an alarm zone based on triggers from a separate system
- Trigger a macro to perform any number of overrides within Command Centre

Functionality

Overrides for the following items are available:

- Door
- Access Zone
- Alarm Zones
- Fence Zones
- Macros
- Outputs

Licensing

The Overrides REST API is a licensed feature of Command Centre.

Availability

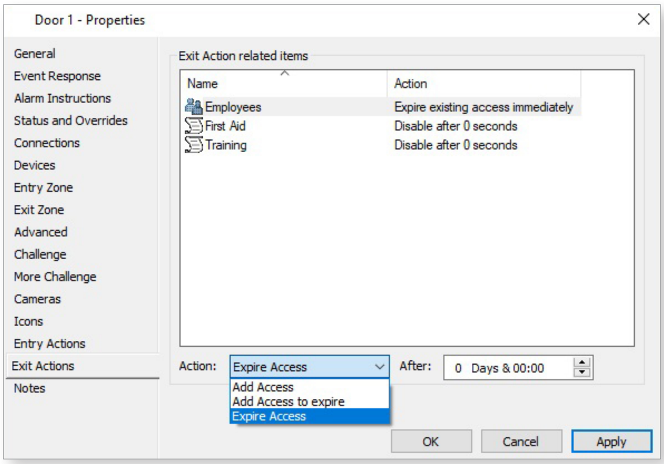
Available with Command Centre v8. The Event and Alarm REST API was released with v7.80.
The Cardholder REST API was released with v7.90.

4 Enhancements

4.1 Action on Access

Expire existing Access Group memberships to restrict entry or re-entry to dangerous, hazardous, or toxic areas. Likewise, existing Competencies can be enabled or disabled for short term periods to further control access to areas based on previous location.

The Action on Access feature introduced in v7.90 allowed Access Group membership to be added for a specified period of time, however existing memberships could not be expired immediately nor after a specified period of time. This can now be achieved using the **Expire Access** option where the Cardholder’s instance(s) of an existing Access Group can be expired immediately (by leaving the time picker at **000 Days & 00:00**) or after a configured period of time has elapsed.



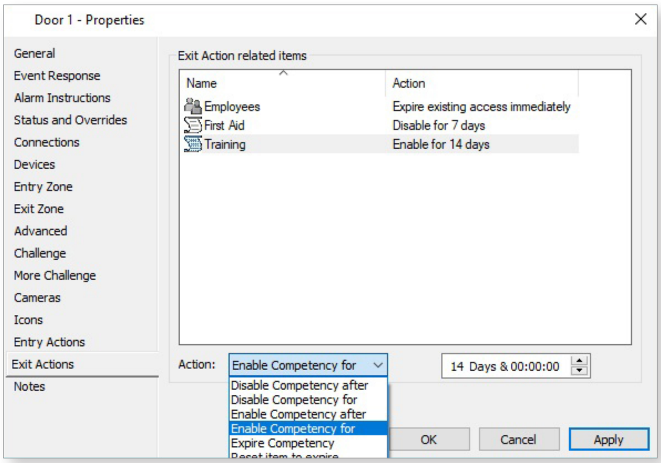
Door 1 - Properties

Exit Action related items

Name	Action
Employees	Expire existing access immediately
First Aid	Disable after 0 seconds
Training	Disable after 0 seconds

Action: Expire Access
After: 0 Days & 00:00

In v7.90 this feature also allowed the enabling or disabling of Competencies immediately (by leaving the time picker at **000 Days & 00:00:00**) or after a configured period of time has elapsed. From Command Centre v8 Competencies can now be enabled or disabled for a configurable period of time. After the time elapses the Competency will revert to the opposite state, (e.g. if the action is to enable the Competency for 14 days, the Competency will disable at the end of that period).



Door 1 - Properties

Exit Action related items

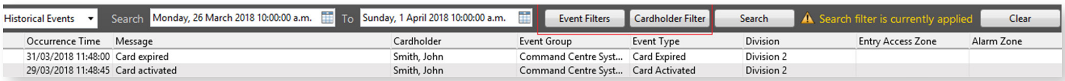
Name	Action
Employees	Expire existing access immediately
First Aid	Disable for 7 days
Training	Enable for 14 days

Action: Enable Competency for
14 Days & 00:00:00

4.2 Event Viewer filtering by Cardholder

Filter live or historical events by Cardholder allowing an operator to monitor or audit the behavior of personnel — audit Cardholders to reduce risk on site.

A Cardholder filter has been added to both the Live and Historical views in the Event Viewer.

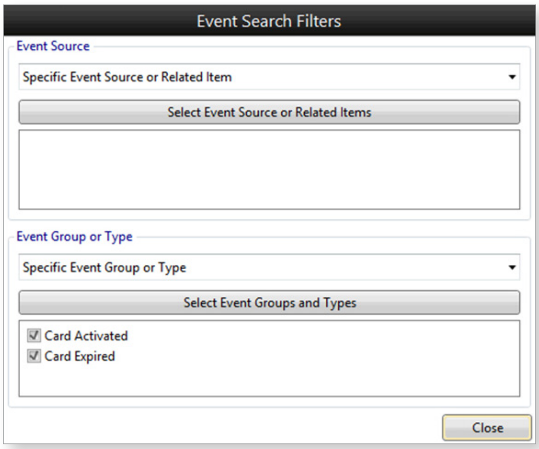


Search: Monday, 26 March 2018 10:00:00 a.m. To Sunday, 1 April 2018 10:00:00 a.m.

⚠ Search filter is currently applied

Occurrence Time	Message	Cardholder	Event Group	Event Type	Division	Entry Access Zone	Alarm Zone
31/03/2018 11:48:00	Card expired	Smith, John	Command Centre Syst...	Card Expired	Division 2		
29/03/2018 11:48:45	Card activated	Smith, John	Command Centre Syst...	Card Activated	Division 2		

An operator can now query or monitor events for specific Cardholders as well as specific event sources, groups, or types.

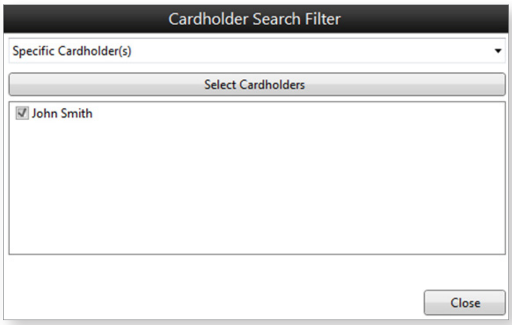

Select Event Source or Related Items
Select Event Groups and Types
Close

Event Search Filters

Event Source: Specific Event Source or Related Item

Event Group or Type: Specific Event Group or Type

☑ Card Activated
☑ Card Expired



Cardholder Search Filter

Specific Cardholder(s)

☑ John Smith

4.3 Alarms management

Alarms management enhancements to provide greater control and flexibility to operators.

Preventing access when a specified Alarm Zone is not armed

This enhancement allows a site to prevent access to an Access Group if a specified Alarm Zone isn't armed or a specified Output isn't on.

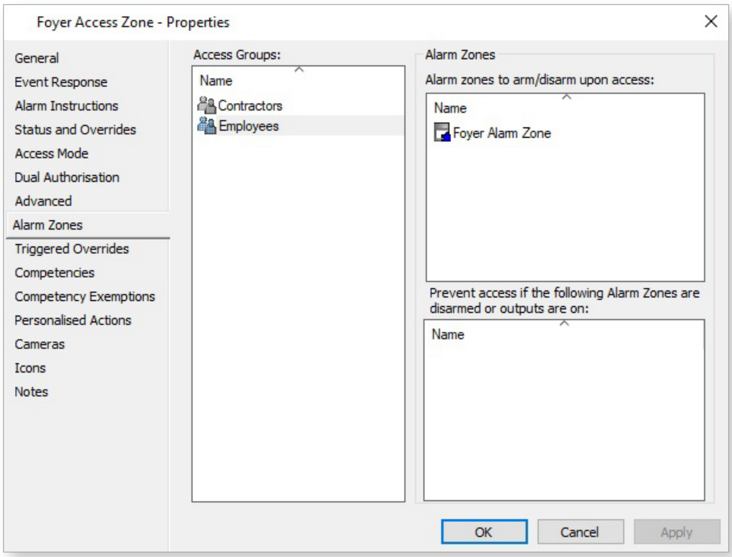
This will allow sites to configure things such as:

- Prevent Cardholders from entering a building if a sensitive area is disarmed
- Prevent access for health and safety reasons such as when fire suppression gas has been deployed in a server room

Arming multiple Alarm Zones when double badging

This enhancement extends existing functionality that allows a Cardholder to arm an Alarm Zone by double badging their card at a reader. From Command Centre v8 it will be possible to select multiple Alarm Zones to be armed in this way. In addition to this, the same set of Alarm Zones will be disarmed when the Cardholder badges their card to gain access.

The above two enhancements can be configured via the new **Alarm Zones** tab on the **Access Zone** properties page.



Foyer Access Zone - Properties

Access Groups:

Name
Contractors
Employees

Alarm Zones

Alarm zones to arm/disarm upon access:

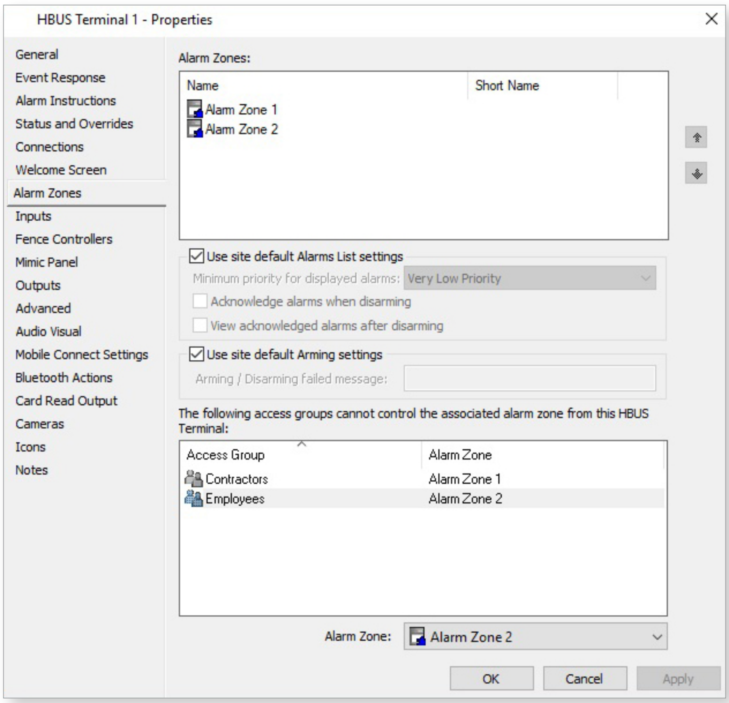
Name
Foyer Alarm Zone

Prevent access if the following Alarm Zones are disarmed or outputs are on:

Name

Restricting control of an Alarm Zone from a specified T20 Terminal

This enhancement will give sites greater control over which Cardholders can control specific Alarm Zones and from which terminal. For instance, some sites have policies that prevent non-senior staff from disarming an internal Alarm Zone from an external terminal but still want them to disarm the internal Alarm Zone from an internal terminal. This is achieved by having a new field on the T20 Terminal that will allow Access Groups and Alarm Zones to be associated with T20 Terminal.



Alarm Zones:

Name	Short Name
Alarm Zone 1	
Alarm Zone 2	

☑ Use site default Alarms List settings

Minimum priority for displayed alarms: Very Low Priority

□ Acknowledge alarms when disarming

□ View acknowledged alarms after disarming

☑ Use site default Arming settings

Arming / Disarming failed message:

The following access groups cannot control the associated alarm zone from this HBUS Terminal:

Access Group	Alarm Zone
Contractors	Alarm Zone 1
Employees	Alarm Zone 2

Alarm Zone: Alarm Zone 2

Prevent disarming when access is gained via a User Code

Some sites have the need to allow a user to gain access via a user code but do not want to give the user permission to disarm. For instance, giving a courier permission to drop a package into a secure area without disarming the Alarm Zone. This enhancement is configured on the HBUS Terminal, HBUS Contact Card Reader, or HBUS Alarms Terminal **Advanced** property page.

Note: If the Cardholder still has the 'Change to Disarm' privilege, the zone will disarm.

4.4 Removal of the Time Report midnight boundary

Time Reports can now span multiple days and record time based purely on entry and exit events. Sites can now measure staff and contractor time for a week or more where access events cross one or more midnights. This enhancement removes complexity and admin burden.

Background

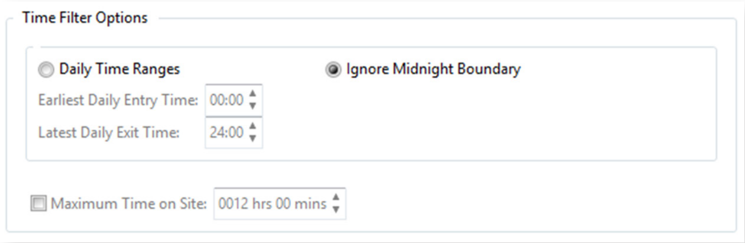
The Time Report has always allowed time to span midnight, however this could only be achieved by setting a *non-default* Daily Time Range. By default the Time Report starts each day at midnight and ends each day at the following midnight.

Configuration

It is now possible to set the 'Report Date and Time' filter to 'Ignore Midnight Boundary'. This option will allow the default case above to span across one or multiple days, ignoring the aforementioned midnight boundary.

This option is available in both the Time Report and the Time Report – Overview. The option is compatible with all other filter options including Filter Days, Maximum Time on Site, Display only First Entry and Last Exit, and all other filters.

By default Daily Time Ranges will be selected. This will remain the default for all upgraded sites.



Time Filter Options

○ Daily Time Ranges

● Ignore Midnight Boundary

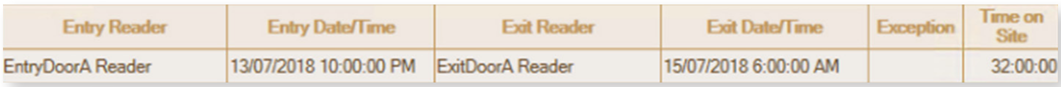
Earliest Daily Entry Time: 00:00

Latest Daily Exit Time: 24:00

□ Maximum Time on Site: 0012 hrs 00 mins

Example

An entry event at 10pm Friday followed by an exit event at 6am Sunday will now report one row with Total Hours 32:00.



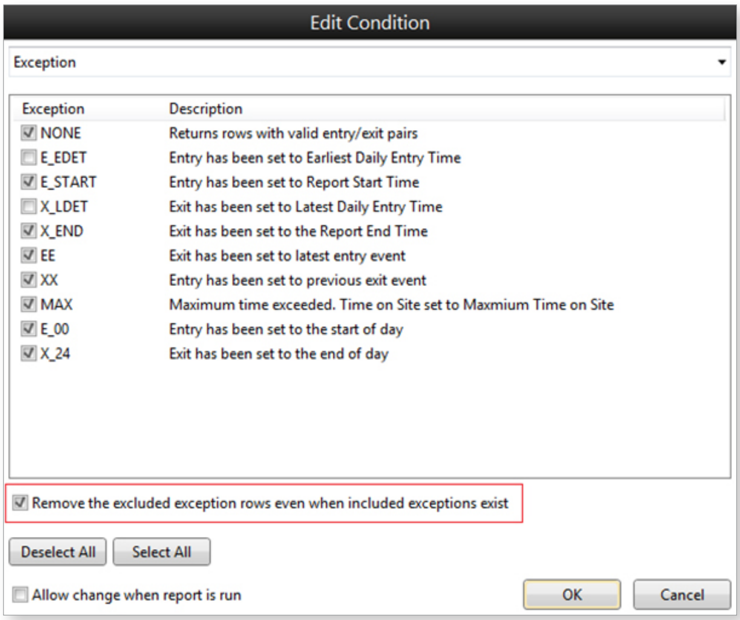
Entry Reader	Entry Date/Time	Exit Reader	Exit Date/Time	Exception	Time on Site
EntryDoorA Reader	13/07/2018 10:00:00 PM	ExitDoorA Reader	15/07/2018 6:00:00 AM		32:00:00

4.5 Time Report Exception filter

Now when excluding an exception value in the Time Report, the row can be excluded regardless of the row containing other exceptions, (e.g. if a site wants to exclude LDET but include MAX, and if a row includes both LDET and MAX, the site can select the new check box option and the row will be excluded).

A new option has been added to the Exception filter to **Remove the excluded exception rows even when included exceptions exist**. This allows the report to exclude a row explicitly when the exception is excluded (deselected in the filter) regardless of other exceptions that may exist for that row. The report will only include the exception rows if ALL of the exceptions are included (selected in the filter). Without the option selected the default behavior will include an exception row when ANY of the exceptions are included.

This allows a site to explicitly remove exception rows when other exceptions coexist for those rows.



Edit Condition

Exception

Exception	Description
☑ NONE	Returns rows with valid entry/exit pairs
□ E_EDET	Entry has been set to Earliest Daily Entry Time
☑ E_START	Entry has been set to Report Start Time
□ X_LDET	Exit has been set to Latest Daily Entry Time
☑ X_END	Exit has been set to the Report End Time
☑ EE	Exit has been set to latest entry event
☑ XX	Entry has been set to previous exit event
☑ MAX	Maximum time exceeded. Time on Site set to Maxmium Time on Site
☑ E_00	Entry has been set to the start of day
☑ X_24	Exit has been set to the end of day

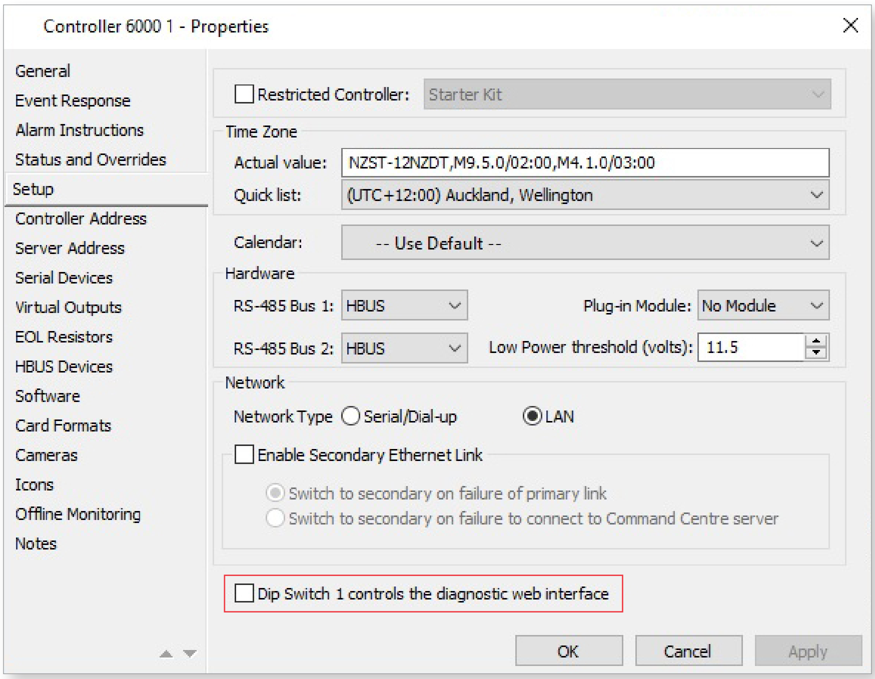
☑ Remove the excluded exception rows even when included exceptions exist

□ Allow change when report is run

4.6 Disable DIP Switch 1 at the server

This enhancement provides greater security for the site. It provides the ability to enable the DIP Switch 1 control of the diagnostic web interface from the Configuration Client. Disabled by default, this added security control requires explicit enabling before the DIP Switch 1 setting becomes active.

DIP Switch 1 can now be disabled in the Configuration Client. A new check box **Dip Switch 1 controls the diagnostic web interface** is configurable per controller in the controller's **Setup** property page.



□ Restricted Controller: Starter Kit

Time Zone

Actual value: NZST-12NZDT,M9.5.0/02:00,M4.1.0/03:00

Quick list: (UTC+12:00) Auckland, Wellington

Calendar: -- Use Default --

Hardware

RS-485 Bus 1: HBUS

Plug-in Module: No Module

RS-485 Bus 2: HBUS

Low Power threshold (volts): 11.5

Network

Network Type ○ Serial/Dial-up ● LAN

□ Enable Secondary Ethernet Link

● Switch to secondary on failure of primary link

○ Switch to secondary on failure to connect to Command Centre server

□ Dip Switch 1 controls the diagnostic web interface

Controllers upgraded to and beyond vGR8.00 will have the web interface disabled (check box deselected) by default. Newly created controllers will also have the web interface disabled by default (once the controller is configured by the server with controller software post vGR8.00).

4.7 Strict anti-tailgating

Strict anti-tailgating allows the enforcement of the anti-tailgating feature even when a controller is *restarted or power cycled,* ensuring that all Cardholders exiting a zone have previously badged into that zone.

Promotes people management — knowing who is where and when. Improves emergency response capabilities, staff safety and site security.

Background

With standard anti-tailgating, information is lost upon controller restart, and Cardholders cannot be denied until they have first passed through the zone.

With strict anti-tailgating enabled, Cardholders who have not entered the zone (including those who have not previously passed through the zone) are denied exit. The controller persists a list of who is in the zone. This list is also persisted for anti-passback, so a controller restart will no longer forget who has entered. Zone count is also persisted, so a controller restart will not set the zone count back to zero, and outputs triggered by different zone count states will remain in the same state as prior to the restart.

Configuration

When enabling the strict anti-tailgating option, anyone already in the zone will be denied exit.
To mitigate this issue, a site can do any of the following:

- Only turn the option on at a time when the zone is empty

  or

- Enable anti-passback for a day or two prior to enabling strict anti-tailgating, so that the system can determine who is in the zone legitimately and who has tailgated into the zone (anti-passback uses the same persistence list as strict anti-tailgating). If you have anti-passback enabled for a while and then turn on strict anti-tailgating, things should work as intended straight away because the system will have already tracked who is in the zone. However, make sure you do not turn anti-passback off, then apply, and then turn on strict anti-tailgating, because the instant you apply changes with anti-passback off the persistence list will be cleared. So, turn on strict anti-tailgating before switching off anti-passback

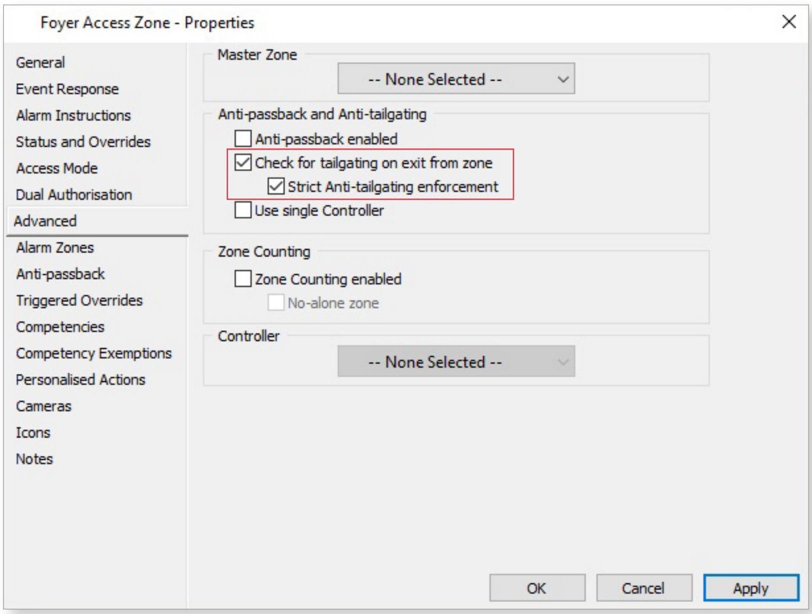
  or

- Change the Access Group's anti-tailgating response to **No action** or **Log an event**, until a day or two has passed, before changing it back to deny access. This is the least preferable option as you need to change all Access Groups that grant access into that zone.

Notes:

1. Strict anti-tailgating has been introduced in Command Centre v8 and back developed to versions v7.70.596, v7.80.894, v7.90.884 and higher.
2. The persistence list is cleared by turning off anti-passback and strict anti-tailgating. Standard anti-tailgating itself does not create a persistence list.
3. The **Anti-passback Forgive All** override does not work for strict anti-tailgating. Cardholders can be forgiven individually.
4. Timed anti-passback forgive, (e.g. at 2:00am) also does not work for strict anti-tailgating.

Configurable on the **Advanced** property page of the Access Zone. The **Strict Anti-tailgating** check box is only editable (enabled) when the **Check for tailgating on exit from zone** is selected.



Foyer Access Zone - Properties

Master Zone: -- None Selected --

Anti-passback and Anti-tailgating
- ☐ Anti-passback enabled
- ☑ Check for tailgating on exit from zone
  - ☑ Strict Anti-tailgating enforcement
- ☐ Use single Controller

Zone Counting
- ☐ Zone Counting enabled
  - ☐ No-alone zone

Controller: -- None Selected --

4.8 Exit Delay tab changes

This enhancement increases the security of an Alarm Zone during Exit Delay. By configuring an exit path, only selected devices are ignored during exit instead of all devices in the Alarm Zone being ignored.

Introduction

Sites can configure an exit path so that personnel can arm an Alarm Zone and then exit securely without triggering an alarm by following a designated exit path.

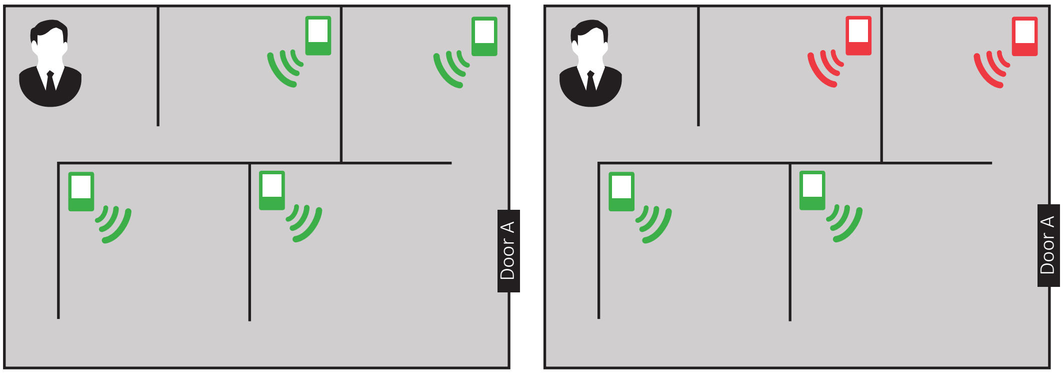
Note: This enhancement is not supported on legacy controllers.

Configuration

The user can specify if the **Ignored Devices** list is ignored only at the time of arming, or if they're ignored during both arming and exit delay.

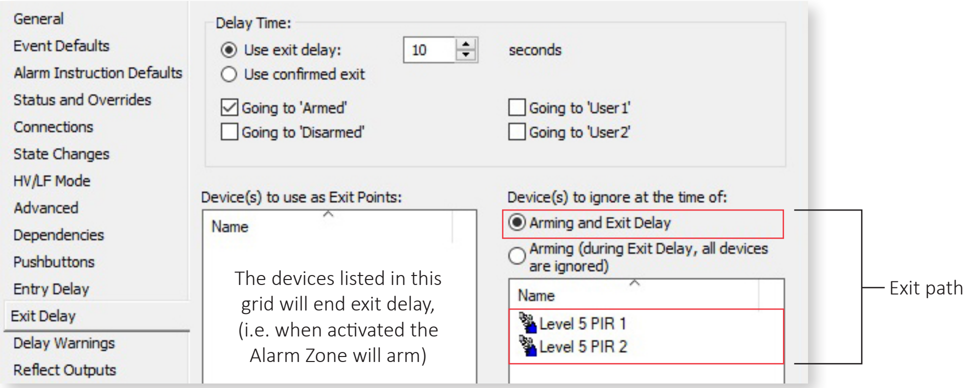
Selecting the **Arming and Exit Delay** option creates an exit path along with any exit points listed in the grid on the left. *Points that are not in either grid are not included in the exit delay and are armed immediately.*

The **Arming only** option retains previous behavior, and is the default selection to maintain existing functionality. If this option is selected and an exit delay has been configured, the listed devices will be ignored during arming, then all devices in the Alarm Zone will be ignored during exit delay.



Previously all devices in the Alarm Zone were ignored during exit delay.

Now only devices on the designated Exit Path are ignored during exit delay.



Delay Time:

● Use exit delay: 10 seconds

○ Use confirmed exit

☑ Going to 'Armed' □ Going to 'User1'

□ Going to 'Disarmed' □ Going to 'User2'

Device(s) to use as Exit Points:

Name

The devices listed in this grid will end exit delay, (i.e. when activated the Alarm Zone will arm)

Device(s) to ignore at the time of:

● Arming and Exit Delay

○ Arming (during Exit Delay, all devices are ignored)

Name
Level 5 PIR 1
Level 5 PIR 2

Exit path

4.9 Alarm Zone dependencies

This enhancement allows more flexibility around the automatic arming and disarming of Alarm Zones, ensuring that core system elements remain protected regardless of the changing states of dependent Alarm Zones.

Introduction

Sites can configure dependencies so that local Alarm Zones aren't automatically armed or disarmed when its dependent Alarm Zone(s) are armed or disarmed.

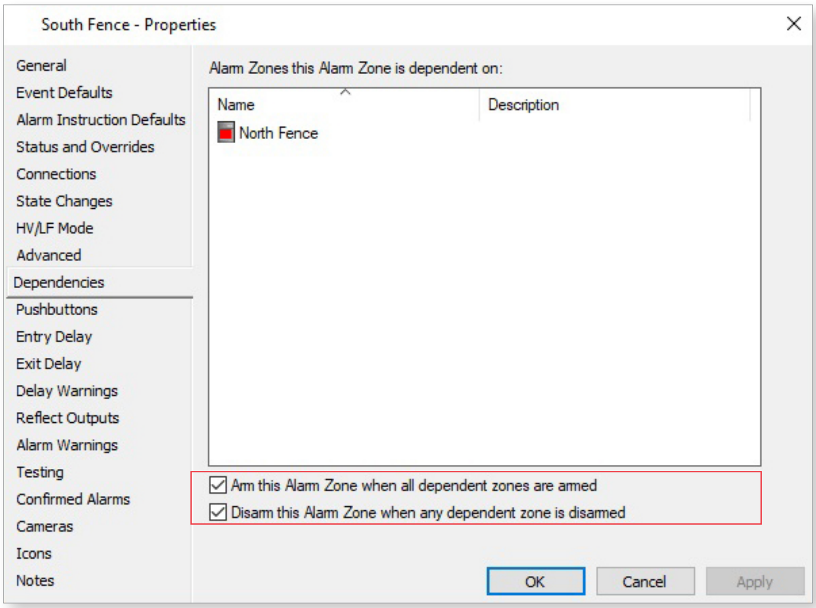
Note: This enhancement is not supported on legacy controllers.

Configuration

The **Dependencies** tab contains two new check boxes that allow the user to specify if the local zone is automatically armed when all dependent zones are armed and/or automatically disarmed when any dependent zone is disarmed.

Both options will be enabled by default to maintain existing functionality. Once deselected, the arming/disarming (as per the configuration) of dependent zones has no effect on the state of the local Alarm Zone. The local zone can still only be armed when all dependent zones are armed, but this will be done by the user.

If dependencies are configured so that the local Alarm Zone is not automatically armed when dependent zones are armed, the local zone will not be checked for points that may prevent arming.



Alarm Zones this Alarm Zone is dependent on:

Name	Description
🟥 North Fence	

☑ Arm this Alarm Zone when all dependent zones are armed

☑ Disam this Alarm Zone when any dependent zone is disarmed

4.10 Reflected Outputs on Fence Zones

This enhancement provides the ability to display the status of a Fence Zone, to satisfy health and safety requirements. Increases staff safety and allows a site to meet compliance standards.

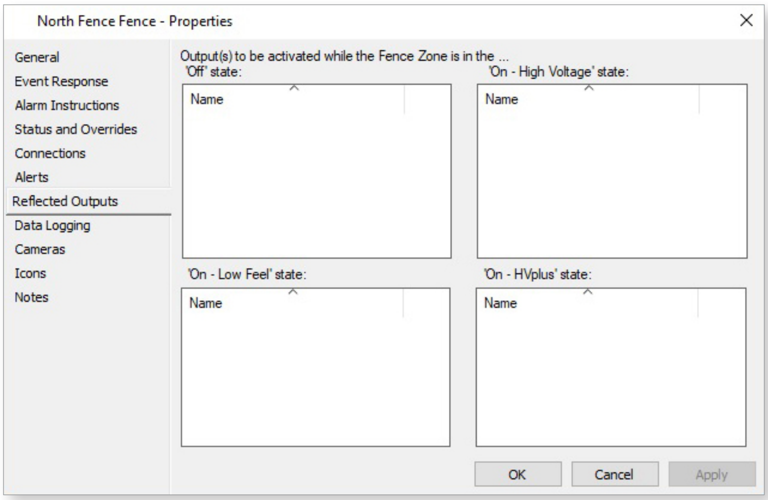
Background

Some health and safety policies require sites to provide a visual indication of a pulse fence status. By providing Reflected Outputs on the Fence Zone, sites will be able to configure indicator lights (or other outputs) to advise people of the fence status.

Configuration

Configuration is simple and requires outputs to be configured and then dragged into the Fence Zone's **Reflected Outputs** properties page.

This enhancement will only work with F-Series Fence Controllers that are connected to a Controller 6000. Note that the escalated state is only applicable to F41 and F42 Fence Controllers that have the ability to increase voltage when an attack is detected.



4.11 Disallow lossless compression of JPEG Personal Data Field

To ensure exported image files are compatible with image viewers all JPEG images are now stored with some level of compression.

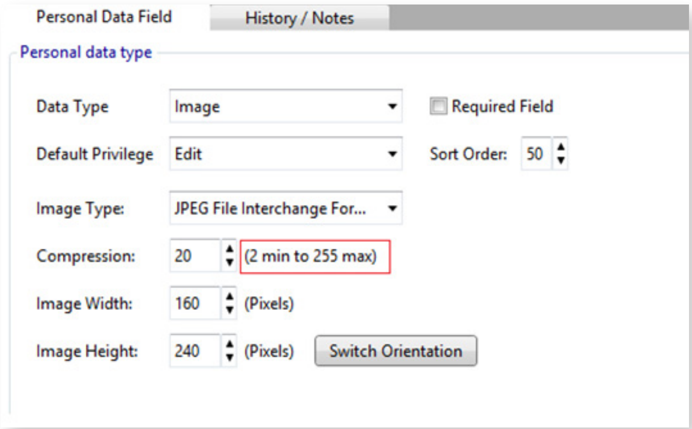
Background

Prior to Command Centre v8 it was possible to store lossless compressed (zero compression value) JPEG Image Personal Data Fields. However, this was causing compatibility issues with most image viewers when exporting the images.

Configuration

In Command Centre v8 it is no longer possible to create a lossless compressed JPEG Image Personal Data Field. An Image Personal Data Field can now only be created with a compression value of 2 or above. It is recommended to use the default compression of 20 to minimize database storage of the images.

Note: Bitmap images ignore the compression setting.



Data Type: Image
□ Required Field
Default Privilege: Edit
Sort Order: 50
Image Type: JPEG File Interchange For...
Compression: 20 (2 min to 255 max)
Image Width: 160 (Pixels)
Image Height: 240 (Pixels)

4.12 Event database backup file extension change

To ensure the Restore Utility does not attempt to restore an event database, the file extensions for the central database and event database have been differentiated — removes complexity, double clicking an Event database no longer launches the Restore Utility.

Background

Changes to the Service Manager in v7.90 allowed the Central and Event databases to be backed up and restored. However the Restore Utility in the Bin directory (CCFTRestore.exe) only supports restore of the central database.

Enhancement

To ensure that double-clicking an event database backup does not launch the Restore Utility, the event database backup file extension has been changed.

From the Command Centre v8 Service Manager:

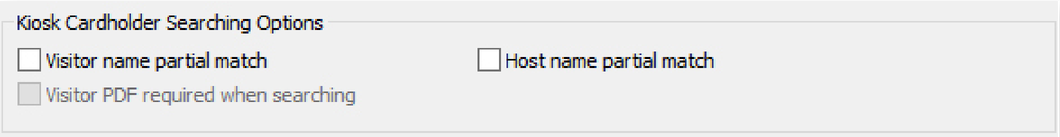
- Backup central creates a backup of the central database with an extension of FTBackup.
- Backup event creates a backup of the event database with an extension of FTEventBackup.

4.13 Visitor Management visitor and host searching

Where visitors registering at the kiosk may not have all the details, the use of partial matching allows for a quicker search to provide them with a choice based on the data entered.

Enhancement

Selecting partial match searching enables the kiosk to provide name options with less details entered. The **Visitor name partial match** and **Host name partial match** options are located on the Kiosk Configuration tab in the Visitor Management Division properties.



Kiosk Cardholder Searching Options

□ Visitor name partial match
□ Host name partial match
□ Visitor PDF required when searching

Note: These options should not be used on sites where visitor and or host name privacy is a concern.

4.14 Changes to Licensing Groups

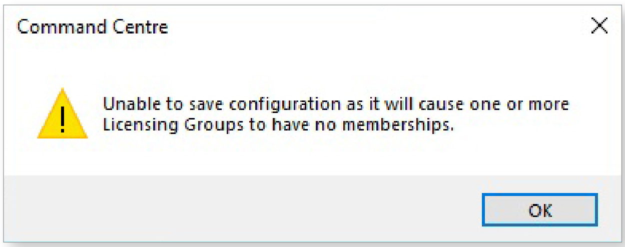
Previously Licensing Groups could be configured in a way resulting in lockout to privileged or occasionally all operators. This configuration restricted the ability to perform important tasks.
In Command Centre v8 this risk is mitigated and to ensure privileged login (the SYSTEM operator) on the server is omitted from Licensing Group restrictions.

Background

The Licensing Group feature introduced in v7.50 allows workstation (and Visitor Management Kiosk) licences to be dedicated to particular workstations or operators. Mis-configuration of this feature however could occasionally result in licences being dedicated to groups with zero members. If all licenses were dedicated in such a manner then it was not possible for any operators to login to Command Centre.

Enhancement

In Command Centre v8 it is *not* possible to save a (non-zero reservation) Licensing Group with zero memberships.



Command Centre

Unable to save configuration as it will cause one or more Licensing Groups to have no memberships.

When upgrading to Command Centre v8 existing Licensing Groups in such a state must be edited (add a workstation or operator) or deleted before the upgrade can continue.

SYSTEM operator exception

If a site gets into a situation where say all operators are dedicated but are all out of the office, or none are able to edit Licensing Groups, the SYSTEM operator is now able to login on the server workstation. This is only possible when there are zero other active sessions against the server across the entire site. Licensing Group rules will be ignored for this SYSTEM operator session.
The SYSTEM operator can then configure the Licensing Group(s) in a manner that solves the issue.

4.15 Restrict ability to view Access Group memberships

This enhancement allows Access Group memberships to be hidden from an operator. When access needs are confidential it is possible to hide the membership from unprivileged operators ensuring confidential zone memberships are not disclosed.

Background

Prior to Command Centre v8 if an operator could view a Cardholder then it was possible to view all Access Group memberships for that Cardholder. If the operator was not privileged to view the Access Group they could still see the Access Group name attached to the Cardholder.

Enhancement

In Command Centre v8 this remains the default behavior. An option **Show all Cardholder Access Group memberships** is added to the **Server Properties Operator Defaults** page so that a site can remove the ability to view these Access Groups.

Configuration

The **Show all Cardholder Access Group memberships** is selected by default (for all new and upgraded sites).

When this control is selected an operator can continue to see all Access Groups assigned to a Cardholder as long as the operator can view the Cardholder. When this control is deselected an operator can only see the Access Groups associated with the Cardholder when they have Modify Access Control, Edit Access Groups, or View Access Groups privilege in the division of the Access Group.

4.16 Cardholder Viewer tracking

Access to Cardholder's personal details can be recorded to allow review of historical operator activity.

This enhancement enables the logging of an event when an operator has accessed a Cardholder record in a Cardholder Viewer, regardless of whether any changes are made to the Cardholder. Access to Cardholder records can therefore be retrospectively audited.

This is a Command Centre only enhancement. Events are not created when operators access Cardholder records in the Configuration Client or Mobile Client. The viewing of Cardholder details through an alarm or through running a report are also out of scope. This enhancement only applies to viewing Cardholder records in a Cardholder Viewer.

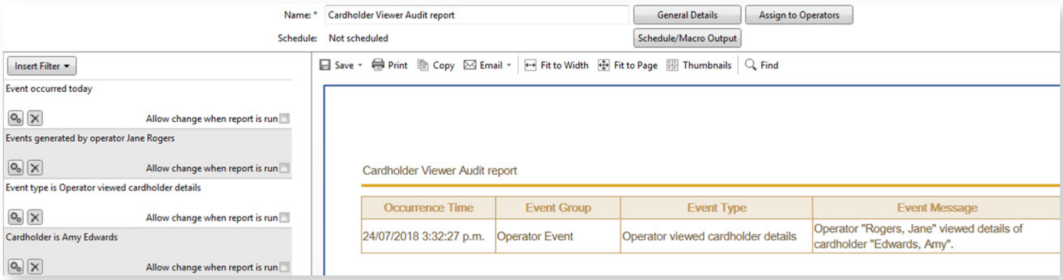
An event will be created for each Cardholder viewed when an operator:

- Queries one Cardholder record in any Cardholder Viewer and that Cardholder record is automatically displayed in the Cardholder panel.
- Queries more than one record and then highlights a record in the Cardholder Navigation Panel to display details in the Cardholder panel below.
- Subsequently clicks on, or down-arrows to further Cardholder records in the Cardholder Navigation Panel to display details in the Cardholder panel below.

Note: These events are created by the Command Centre Client and not by the server.

The event will be delayed for a small amount of time to avoid creation of multiple unnecessary events when down arrowing through a searched list in the Cardholder Navigation Panel. This delay is 250 milliseconds.

The event created displays the Cardholder that was viewed, the operator that viewed the record, and the date and time of the viewing. When a report is run across these events a privileged operator can filter the report by Cardholder viewed, and by which operator performed the viewing.



Name: * Cardholder Viewer Audit report

Schedule: Not scheduled

Event occurred today

Allow change when report is run □

Events generated by operator Jane Rogers

Allow change when report is run □

Event type is Operator viewed cardholder details

Allow change when report is run □

Cardholder is Amy Edwards

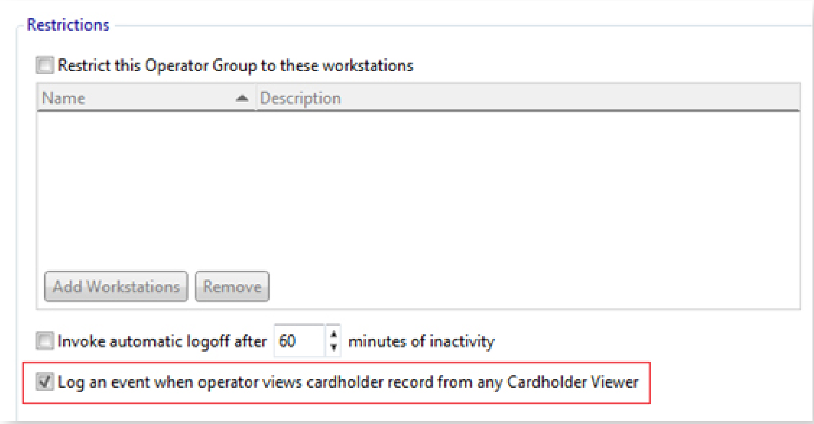
Allow change when report is run □

Cardholder Viewer Audit report

Occurrence Time	Event Group	Event Type	Event Message
24/07/2018 3:32:27 p.m.	Operator Event	Operator viewed cardholder details	Operator "Rogers, Jane" viewed details of cardholder "Edwards, Amy".

Configuration

To allow control over which operator actions create events, configuration of this feature is set at the Operator Group. By default the **Log an event when operator views Cardholder record from any Cardholder Viewe**r check box is off for all Operator Groups.



Restrictions

☐ Restrict this Operator Group to these workstations

Name	Description

☐ Invoke automatic logoff after 60 minutes of inactivity

☑ Log an event when operator views cardholder record from any Cardholder Viewer

Licensing

Cardholder Viewer tracking is a licensed feature of Command Centre.

4.17 Remove Validate Destination from manual backups

Removes complexity — validation of the backup destination now occurs as part of the manual backup process.

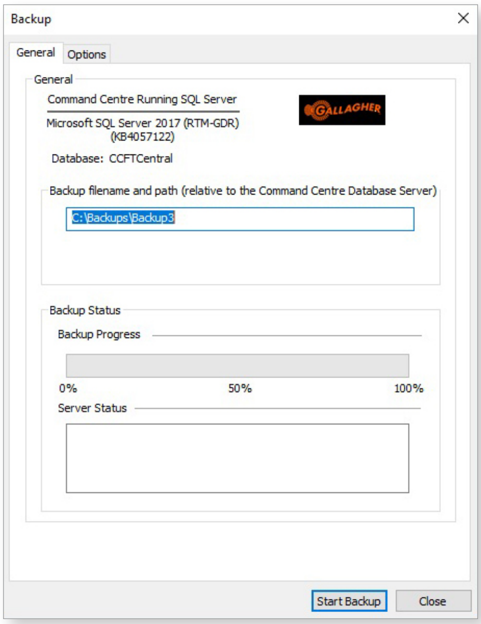
Background

Due to recent security changes and SQL permission issues, the **Validate Destination** button has been removed when manually creating backups.

Enhancement

When configuring a manual backup, the **Schedule Backup** check box must be deselected.

The **Validate Destination** button appears in the **Options** tab when creating scheduled backups, so that the destination can be validated during configuration.



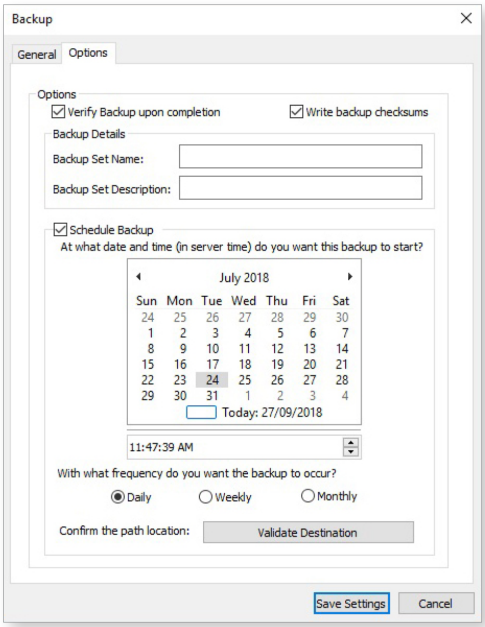
General

Command Centre Running SQL Server

Microsoft SQL Server 2017 (RTM-GDR) (KB4057122)

Database: CCFTCentral

Backup filename and path (relative to the Command Centre Database Server): C:\Backups\Backup3



Options

☑ Verify Backup upon completion ☑ Write backup checksums

Backup Set Name:

Backup Set Description:

☑ Schedule Backup

At what date and time (in server time) do you want this backup to start?

Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Today: 27/09/2018

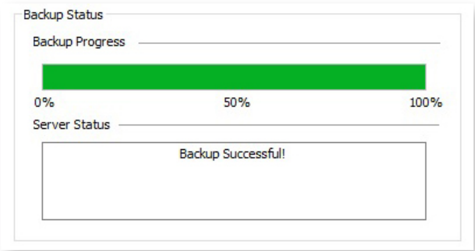
11:47:39 AM

With what frequency do you want the backup to occur?

● Daily ○ Weekly ○ Monthly

Confirm the path location: Validate Destination

Validation of the backup destination occurs as part of the manual backup process:



Backup Successful!

4.18 Disable last operator name at logon

Having Command Centre remember the last Logon Name is a convenient feature introduced in v7.90. However some sites may not want shared workstations to behave this way. An option has been added in Command Centre v8 to disable this feature, and make each logon require the Logon Name to be explicitly typed.

Enhancement

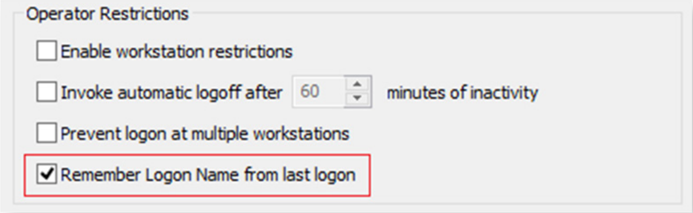
An option exists on the **Operator Defaults Server Properties** page to remember the Logon Name from the last operator logged into Command Centre. This option is selected by default.

When selected, the last operator's Logon Name that logged into Command Centre will be displayed (for both the Command Centre and Configuration Client Logon Windows), and the cursor focus will be on the **Password** field.

When deselected, the Logon Name will be blank (for both the Command Centre and Configuration Client Logon Windows), and the cursor focus will be on the **Logon Name** field.

Configuration

Each time the control is toggled on or off, operators will need to login one additional time before the change takes effect.



Operator Restrictions

□ Enable workstation restrictions

□ Invoke automatic logoff after 60 minutes of inactivity

□ Prevent logon at multiple workstations

☑ Remember Logon Name from last logon

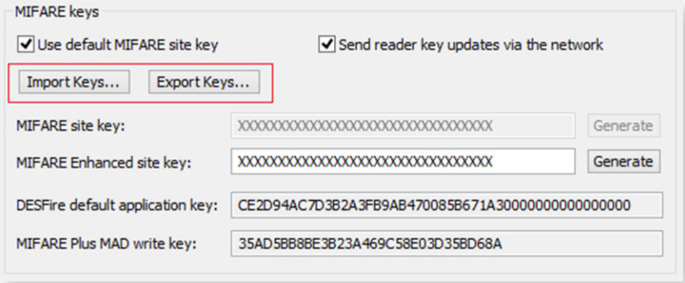
4.19 Minor enhancements

Increased number of controllers that can be upgraded simultaneously

From Command Centre v8 the number of Controller 6000s that can be upgraded via Bulk Change will be increased from 10 to 20. This will allow sites with a large number of controllers to complete their upgrade in a shorter period of time.

Upgraded encryption for MIFARE and Alarm Transmitter key export

- Key export formats upgraded to comply with CAPSS requirements.
- MIFARE site key, MIFARE Enhanced key, and MIFARE Classic key exported in same process.
- Keys exported in previous versions cannot be imported into Command Centre v8.
- Gallagher recommends re-exporting these keys to appropriate media post Command Centre v8 upgrade for sites wishing to store a copy of these keys.
- IP Alarm Receiver configuration utility updated to import new key format.



MIFARE keys

☑ Use default MIFARE site key

☑ Send reader key updates via the network

MIFARE site key: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

MIFARE Enhanced site key: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

DESFire default application key: CE2D94AC7D3B2A3FB9AB470085B671A30000000000000000

MIFARE Plus MAD write key: 35AD5BB8BE3B23A469C58E03D35BD68A

DCOM security

- Most Command Centre installs no longer require DCOM. The Configuration Client was switched to WebSockets by default in v7.90.
- Remote access via DCOM is now disabled by default and encryption is enabled by default. Therefore, DCOM connections from other machines will fail by default, (i.e. BootP, XML import, and OPC AE/DAa0).
- Legacy settings can be restored using the FT DCOM Setup utility, installed here: C:\Program Files (x86)\Gallagher\Command Centre\Bin

Removal of DVR support from the Configuration Client

Integrations built by Gallagher or by anyone using the legacy DVR SDK have not worked in the Configuration Client since v7.50. Support in the Configuration Client for this legacy SDK has been completely removed in Command Centre v8.

Support up to 256 facility codes - extension

Command Centre v7.90 introduced an expansion from 16 to 256 facility codes however the feature was licensed (ExtraFacilityCodes=1) and restricted to use by third party cards. From Command Centre v8 this licence requirement has been removed and the feature has been expanded to now support Gallagher encoded cards.

Note: This extension is not supported on legacy controllers.

GALLAGHER WORLD HEADQUARTERS

Kahikatea Drive, Hamilton 3206
Private Bag 3026, Hamilton 3240
New Zealand

TEL: +64 7 838 9800
EMAIL: security@gallagher.com

REGIONAL OFFICES

New Zealand	+64 7 838 9800
Americas	+1 877 560 6308
Asia	+852 3468 5175
Australia	+61 3 9308 7722
India	+91 98 458 92920
Middle East	+971 4 5665834
South Africa	+27 11 974 4740
United Kingdom / Europe	+44 2476 64 1234

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 2015. All rights reserved.

security.gallagher.com