

Command Centre v7.70

Feature Summary



GALLAGHER

COMMAND CENTRE v7.70

FEATURE SUMMARY

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 2017. All rights reserved.

Introduction.....	5
PURPOSE OF THIS DOCUMENT	5
General Command Centre v7.70 Notes.....	5
UPGRADING TO VERSION 7.70	5
OPERATING SYSTEM SUPPORT	6
MOBILE SUPPORTED DEVICES - COMMAND CENTRE MOBILE.....	6
MOBILE SUPPORTED DEVICES - MOBILE CONNECT	6
MONITOR RESOLUTION SUPPORT	7
DATABASE SUPPORT	7
COMMAND CENTRE SERVER SOFTWARE LICENSING CHANGES.....	7
<i>Key device policy</i>	7
<i>Command Centre licensing</i>	7
<i>Key Device Failure</i>	7
<i>License updates</i>	8
COMMAND CENTRE UPGRADE PATHS	8
Command Centre Security Changes	9
IMPROVEMENTS TO DATABASE ENCRYPTION	9
WINDOWS AUTHENTICATION TO SQL SERVER.....	11
REDUCED DATABASE PRIVILEGES	11
REDUCED SERVICE PRIVILEGES	11
RUNNING VISITOR MANAGEMENT KIOSK OVER HTTPS	11
Mobile Connect	12
PERFORMING ACTIONS	12
RE-PROVISIONING BLUETOOTH CREDENTIALS.....	14
MOBILE CREDENTIAL STATUS	15
MOBILE CONNECT - TIPS	15
MOBILE CONNECT - ADDITIONAL ENHANCEMENTS.....	15
Command Centre Mobile.....	16
BARCODE READER.....	16
READER BLUETOOTH CONFIGURATION.....	17
CONNECTING TO COMMAND CENTRE THROUGH A REVERSE PROXY	18
Personalised Notifications	19
HTML Email Notification Templates.....	21
PIV Cardholder Registration	22
Cardholder PIN management options	24
Visitor Management Kiosk	25
SUPPORT FOR PASSPORT & DRIVERS LICENSE SCANNING.....	25
<i>Licensing</i>	25
Minor Enhancements	26
RESIZING CONFIGURATION CLIENT PROPERTY PAGES	26
TRACKING THE PERSON, NOT THE CREDENTIAL.....	26
PLAYING A TONE ON T-SERIES READERS WHILST THE DOOR IS RELEASED	26
Third Party Interfaces	27
APERIO V3.....	27

<i>General Functionality</i>	27
<i>Privacy Mode</i>	27
<i>Aperio Door</i>	27
<i>Access Group Options</i>	29

New Product.....30

MIFARE DESFIRE EV2 CREDENTIAL SUPPORT	30
T-SERIES NXP INTEGRATED CIRCUIT UPGRADE	31
T15 READER.....	32
T21 PIV READER	33
HBUS 8 PORT HUB.....	35

Coming Soon.....36

CLASS 5 INTRUDER ALARM SYSTEM	36
<i>Gallagher Class 5 Power Budget Calculator</i>	37
<i>Class 5 Compliant - Independently Tested</i>	37
T15 MOUNTING BLOCK.....	37
VERIDT STEALTH BIO PIV READER.....	38
<i>Veridt Stealth Bio Reader - Configuration</i>	38
<i>Veridt Stealth Bio Reader - Installation</i>	39
COMMEND INTERCOM INTEGRATION.....	39
CONTROLLER 6000 DHCP SUPPORT	39

Introduction

PURPOSE OF THIS DOCUMENT

The purpose of this document is to provide Gallagher Certified Channel Partners and end users with an overview of new features and products released with Gallagher Command Centre v7.70. Please note this document is not intended to be the single source of information regarding v7.70 but rather a guide to the improvements and additions.

General Command Centre v7.70 Notes

This section provides an overview of information that must be understood when considering Command Centre v7.70.

UPGRADING TO VERSION 7.70

Sites upgrading to Command Centre v7.70 from a previous version of Command Centre (v7.60 or earlier) will require an updated Gallagher Command Centre license file. To obtain an updated license file a Command Centre software upgrade or software maintenance must be purchased. Refer to the Gallagher access policy documents for information regarding software maintenance and upgrades.

Changes in Command Centre v7.70 may impact on the configuration of sites upgrading from earlier versions. Refer to the Command Centre v7.70 new features / enhancements release note for full details on the impact of these features before upgrading.

Important Controller 6000 v7.70 upgrade note

When upgrading Controller 6000 devices to v7.70, from a version prior to v7.30 the upgrade time will be longer than usual. This is to resolve an issue where a Controller 6000 may fail after upgrading that was resolved in v7.30.

- The Controller is expected to be **offline for approximately 9 minutes 30 seconds**: The normal offline time is approximately 2 minutes 15 seconds
- While the Controller is offline the Run LED will enter a slow flash rate, this is expected and should not be interrupted
- A version of this fix will also be provided in v7.20 (vGR720685.fts) and v7.10 (vGR710401.fts) controller code and are available on our FTP Server. Sites that are on v7.20 or v7.10 may apply the appropriate upgrade 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 v7.70 will return to normal timings. For further information, please contact Gallagher Security Technical Support.

CONTROLLER VERSION COMPATIBILITY

Command Centre v7.70 is compatible with the firmware version vBT/GR 7.70 of the Gallagher Controller. It is also compatible with previous versions of Controller code for upgrade purposes only. No configuration change should be done on pre-version vBT/GR 7.70 Controllers once Command Centre has been upgraded.

Important Note

There are no software controls in place to check Controller versions during peer-to-peer communications; a site will simply get unpredictable behavior.

It is recommended that sites upgrading from a version prior to Command Centre v7.40 upgrade all Controllers as soon as is practical for the site.

OPERATING SYSTEM SUPPORT

Support for the following Operating Systems/Service Packs is included in Command Centre v7.70:

Gallagher Command Centre Server Operating Systems Supported	Minimum Service Pack	Supported	Tested
Windows 10 Pro	n/a	✓	✓
Windows 8.1 Pro	n/a	✓	✓
Microsoft Windows 2016 Server	n/a	✓	✓
Microsoft Windows 2012 Server	n/a	✓	✓
Microsoft Windows 2012 Server R2	n/a	✓	✓
Microsoft Windows 2008 Server	SP2	✓	✓
Microsoft Windows 2008 Server R2 (64 bit only)	SP1	✓	✓
Microsoft Windows 7 Professional/Ultimate*	SP1	✓	✓

Gallagher Command Centre Workstation Operating Systems Supported	Minimum Service Pack	Supported	Tested
Windows 10 Pro	n/a	✓	✓
Windows 8.1 Pro	n/a	✓	✓
Microsoft Windows 7 Professional/Ultimate*	SP1	✓	✓

Note: 32 and 64 Bit versions of the above Operating Systems are supported*. Command Centre is supported on Virtual Server environments. 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 PC

MOBILE SUPPORTED DEVICES - COMMAND CENTRE MOBILE

iPhone: 4S/ 5 / 5C / 5S / 6 / 6 Plus/ 7 / 7 Plus iPad & iPad Mini Android	iOS 8.0 and above iOS 8.0.2 and above 5.0 and above
---	---

MOBILE SUPPORTED DEVICES - MOBILE CONNECT

iPhone: 5S and above Android	iOS 9.0 and above 5.0 and above
---------------------------------	------------------------------------

MONITOR RESOLUTION SUPPORT

Gallagher Command Centre, from v7.00, is fully supported on monitors with a minimum vertical resolution of 720px and above. While most Command Centre screens will display correctly on lower resolution monitors some lightboxes, such as the 'Assign Access' lightbox, have a fixed resolution which requires a monitor with a minimum vertical resolution of 720px. Monitors with a lower resolution than this will cause the bottom of some lightboxes to be removed from view.

DATABASE SUPPORT

Command Centre v7.70 currently supports the following databases:

Gallagher Command Centre Database Server Systems Supported	Minimum Service Pack	Supported	Tested
Microsoft SQL Server 2016	SP1	✓	✓
Microsoft SQL Server 2014	SP2	✓	✓
Microsoft SQL Server 2014 Express	SP2	✓	✓
Microsoft SQL Server 2012	SP2	✓	✓
Microsoft SQL Server 2012 Express	SP2	✓	✓
Microsoft SQL Server 2008 R2	SP3	✓	✓
Microsoft SQL Server 2008 R2 Express	SP3	✓	✓
Microsoft SQL Server 2008	SP4	✓	✓
Microsoft SQL Server 2008 Express	SP4	✓	✓

Note: *SQL Server 2014 Express is the default freely available database for Gallagher Command Centre. 32 and 64 Bit versions of the above databases are supported.*

COMMAND CENTRE SERVER SOFTWARE LICENSING CHANGES

From Command Centre v7.30 the core Gallagher Command Centre Server License (part number C201311) and associated translated version (part number C201411) now includes three licensed Gallagher Networked Perimeter Integration Licenses (part number 2A8945). Sites receiving new or upgraded licenses for Gallagher Command Centre v7.30 will automatically receive these Networked Perimeter licenses within their CommandCentre.Lic file.

Key device policy

In Command Centre v7.00 Gallagher introduced a new key device policy. The policy is described below and relates to the process for changes to key devices in a Command Centre license file.

Command Centre licensing

Gallagher licenses the use of its Command Centre product via key devices. 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 Gallagher Command Centre.

Note: *Prior to Command Centre v7.00, only the last key device being removed from the system causes an alarm. From Command Centre v7.00 and later versions, any key device being 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.

COMMAND CENTRE UPGRADE PATHS

The following upgrade paths to Command Centre version 7.70 are fully supported:

Version 7.20.xxx to version 7.70

Version 7.30.xxx to version 7.70

Version 7.40.xxx to version 7.70

Version 7.50.xxx to version 7.70

Version 7.60.xxx to version 7.70

Command Centre Security Changes

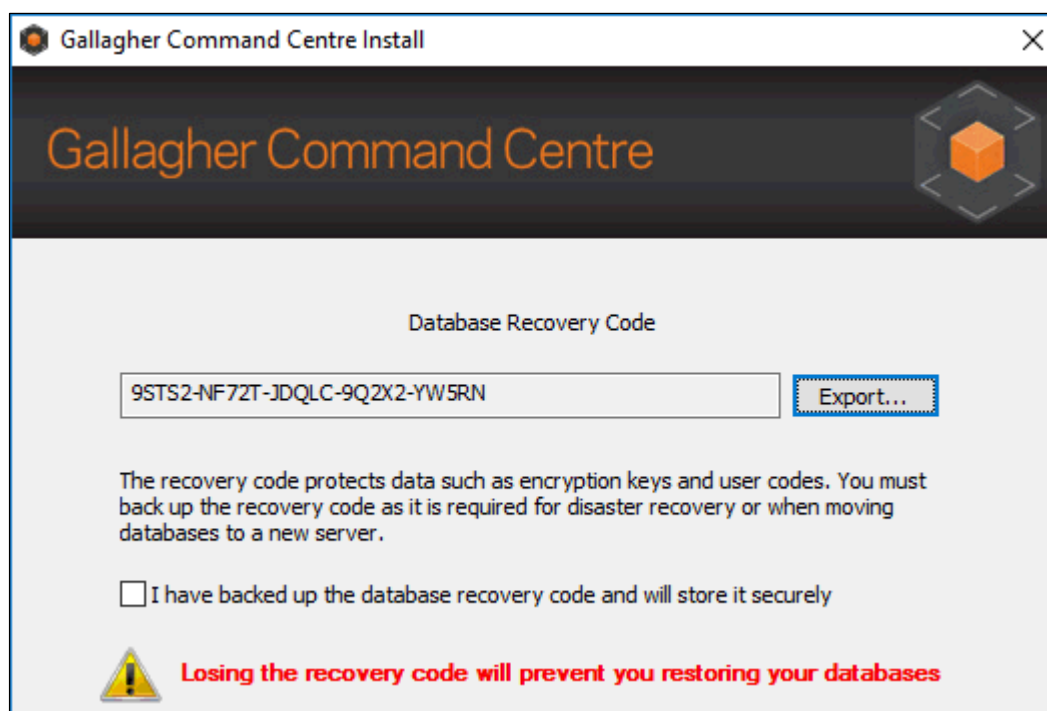
Command Centre v7.70 includes a number of security best practice improvements to ensure systems are as secure as possible. Threats evolve constantly, and Gallagher's extensive research, development and testing programs allow us to evolve our defenses accordingly.

IMPROVEMENTS TO DATABASE ENCRYPTION

To improve the encryption of sensitive database information, at time of installation of v7.70 (or upgrade to, or any versions beyond) a random system-generated code is generated. This code is a mixture of alpha and numeric characters long enough to ensure it can't be easily guessed. **The code must be exported or manually recorded** as any restore of the database on another machine will require import or manual entry of the code. The code will be used on that machine to "unlock" the database in relation to the sensitive information.

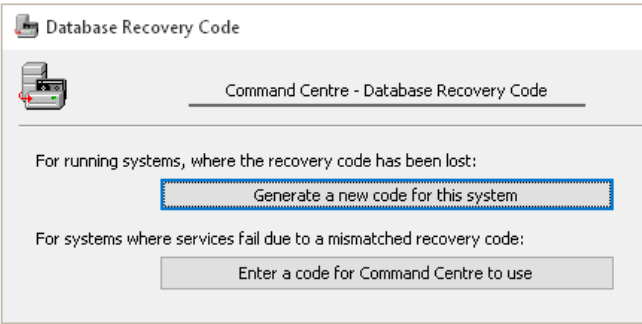
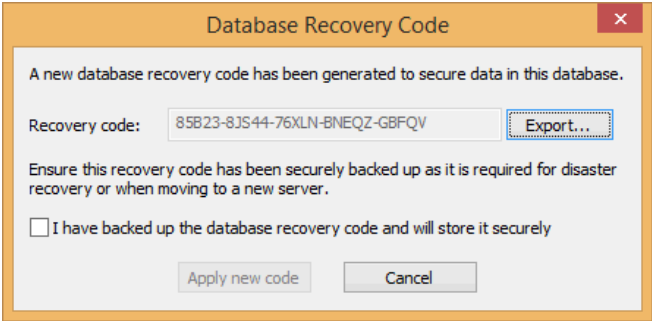
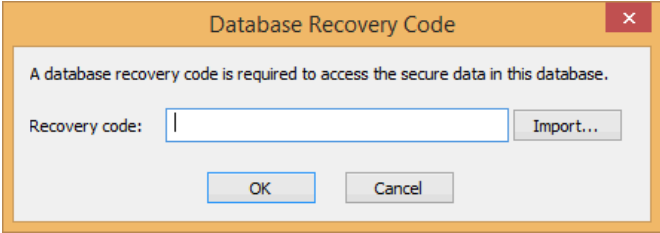
Standard upgrade from v7.70 on the same machine will not require entry of the code.

Losing the system-generated code would mean that the encrypted data in the database would become permanently unavailable when restoring on a new machine. It will be possible to restore the database as a template without the code, but doing so will erase the encrypted sensitive data. Hence sites need to make sure that the code is backed up appropriately.



A database recovery utility CCFTRecoveryCode.exe is provided to allow a new recovery code to be generated, however the code cannot be regenerated while restoring a database to a new machine.

If you are upgrading or changing the system and cannot locate the current database recovery code, stop and regenerate a new database recovery code before backing up the system and proceeding.

Scenario	Steps/Notes
<p>Start-up of the utility (requires services not running)</p>	<ol style="list-style-type: none"> Run CCFTRecoveryCode.exe 
<p>A site has lost their recovery code and wants to generate a new code on the same machine</p>	<ol style="list-style-type: none"> Run CCFTRecoveryCode.exe Click 'Generate a new code for this system' button.  <ol style="list-style-type: none"> Either copy and paste the code or export it Check the box to confirm 'I have backed up the database recovery code and will store it securely' and enable the 'Apply new code' button. Click 'Apply new code' button.
<p>Reasons:</p> <ol style="list-style-type: none"> A site has changed the network service account, and needs to re-enter their existing recovery code for the database in order to get the Command Centre services working again, or Where a database (from another machine) has been "attached" rather than restored via our CCFTRestore utility, or Where customers have a redundant server setup, where the database files are swapped between two machines, the following will be needed when upgrading to v7.70 	<ol style="list-style-type: none"> Run CCFTRecoveryCode.exe Click 'Enter a code for Command Centre to use'.  <ol style="list-style-type: none"> Import or enter the recovery code. Click 'OK'.

WINDOWS AUTHENTICATION TO SQL SERVER

Moving to Windows Authentication when connecting to SQL Server is considered best practice and meets Microsoft certification requirements. From v7.70, Windows Authentication is the only method of Command Centre connecting to SQL Server. The 'ccftsa' user account is deprecated and the DBAdminEnabled licence string is unnecessary.

New sites will use Windows Authentication to connect to SQL Server. Existing sites will use Windows Authentication after upgrade. The 'ccftsa' account will not be created in SQL Server when a new site is installed. This account will be deleted from SQL Server when an existing site upgrades. Machine administrators will be added to the SysAdmin role, if they have not already been. Sites will be required to run Command Centre utilities under a Windows Administrator account. We recommend that sites follow industry best practice regarding use of appropriate Windows privileges for Windows user accounts within their organisation.

REDUCED DATABASE PRIVILEGES

The account used to access the SQL database has been reduced to require only 'DB Owner' for the CCFT databases. To test backups, you will also need the 'Create Database' privilege for the SQL instance.

REDUCED SERVICE PRIVILEGES

A Windows account with Administrator rights is no longer required to run the Command Centre services. The default service account for v7.70 (and later) is now the "Network Service" account. The use of the "Local System" account (NT Authority\System) is discouraged. When an existing site upgrades to v7.70, they will be prompted to confirm whether they wish to retain the existing "Local System" service account, and encouraged to change to the new default of "Network Service". There are situations where the "Network Service" account is not ideal however, and these are documented in the installation and upgrade Release Notes available on the v7.70 installation DVD.

RUNNING VISITOR MANAGEMENT KIOSK OVER HTTPS

You can now run Gallagher Visitor Management Kiosk over HTTPS, allowing you to use an off-the-shelf web proxy between the Kiosk and your Command Centre server. This configuration helps to meet various compliance requirements including New Zealand government installations. For more information refer to the VM Kiosk OPCUA over HTTPS document available on the v7.70 installation DVD.

Mobile Connect

PERFORMING ACTIONS

Allows users of Mobile Connect to trigger a macro, effectively opening up a world of possible interactions with building management systems, lights, alarms, air-con and more.

The Mobile Connect app was introduced in v7.60 and allows users with a mobile credential to use smartphones to gain access at Bluetooth® enabled Multi Tech Readers in place of a traditional Access Card or Fob. The Mobile Connect app has been enhanced for v7.70 making it possible for a privileged user to perform a number of tasks such as arming an Alarm Zone or changing the Access Mode for the door. It will even be possible to turn on lights and air conditioning. This is achieved by allowing outputs to be toggled on or off from the reader and means that from v7.70 this is available for iOS and Android phones on any site that upgrades to v7.70. For the 'Actions' feature to work, the reader must be configured for manual connect:

The screenshot shows the 'HBUS Reader 1 - Properties' dialog box. On the left is a sidebar with various tabs: General, Event Response, Alarm Instructions, Status and Overrides, Connections, Advanced, Audio Visual, Bluetooth Settings (selected), Bluetooth Actions, Card Read Output, Cameras, Icons, and Notes. The main area displays the 'Bluetooth Settings' configuration. It includes a 'Use site default Bluetooth settings' checkbox which is checked. Below this are three unchecked checkboxes: 'Turn on Bluetooth low energy technology', 'Second factor authentication always required', and 'Advertise reader name'. The 'Transmit Power' section shows a value of -26 dBm. The 'Auto connect range' section has 'Enable' checked and a 'Path Loss' of 45 dBm. The 'Manual connect range' section is highlighted with a red box; it also has 'Enable' checked and a 'Path Loss' of 64 dBm. Below this section, a note states: 'A greater path loss value will increase the connection distance.' At the bottom, there is a 'Configuration' section with a note: 'For accurate configuration per reader, consult the reader's path loss values via the app to determine the required dBm values.' At the very bottom are 'OK', 'Cancel', and 'Apply' buttons.

For users to perform Actions such as Arming or Changing the Access Modes, they will need to be privileged to perform overrides. It is now possible to assign up to 10 outputs to Bluetooth® enabled multi tech readers. In the screenshot overleaf it is a simple process of dragging and dropping the desired output onto the Bluetooth Actions tab. The output can be assigned a label that will be displayed in Mobile Connect.

HBUS Reader 1 - Properties

General

Event Response

Alarm Instructions

Status and Overrides

Connections

Advanced

Audio Visual

Bluetooth Settings

Bluetooth Actions

Card Read Output

Cameras

Icons

Notes

Users require the "Lock and unlock access zones" privilege for the Door's Access Zone to trigger an Output, unless the "Available to All" checkbox is ticked.

Actions are only available in the Gallagher Mobile Connect App when Bluetooth manual connect is enabled.

Output	Label	Available to ...
Air con	Air conditioning	<input checked="" type="checkbox"/>

↑
↓

Label:

OK
Cancel
Apply

The outputs can be triggered by any Cardholder with valid access through the door (when 'Available to all' is checked). Or they can be restricted to users with the 'Lock and unlock access zones' privilege on their Access Group. The system will know and record who triggered what and when to provide a complete audit trail.

Demo Access Group - Properties

General

Lineage

Cardholder Membership

Membership Defaults

Access

Privileges

Terminal Access

Alarm Zones

Personal Data

Anti-Passback Response

Salto Access

Event Notifications

Notes

Access Privileges

☐ Visitor

☐ Escort visitors

☒ Lock and unlock access zones

☐ Entry allowed during lockdown

☐ First Card Unlock

☐ Aperio Privacy Override

☐ Aperio Offline Access

Alarm Zone Privileges

☒ Change to the Disarmed state

☒ Change to the Armed state

☒ Change fence HV/LF mode

Terminal Privileges

☒ View alarms and items

☒ Shunt items

☒ Acknowledge all alarms

☐ Acknowledge alarms below high priority

☒ Lock out fence zones

☒ Cancel others lock out

☒ Prompt for alarm zone selection

☒ Force-arm alarm zones

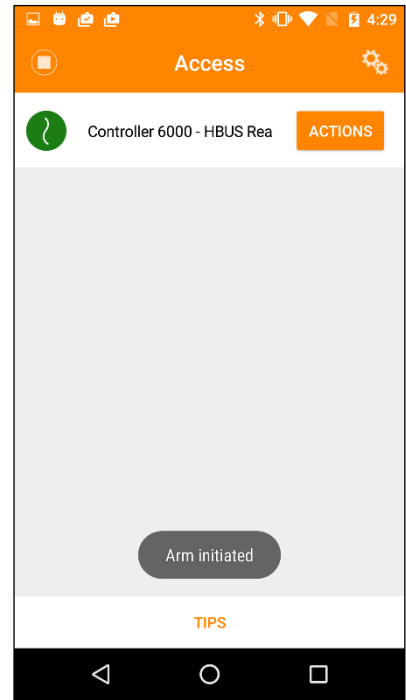
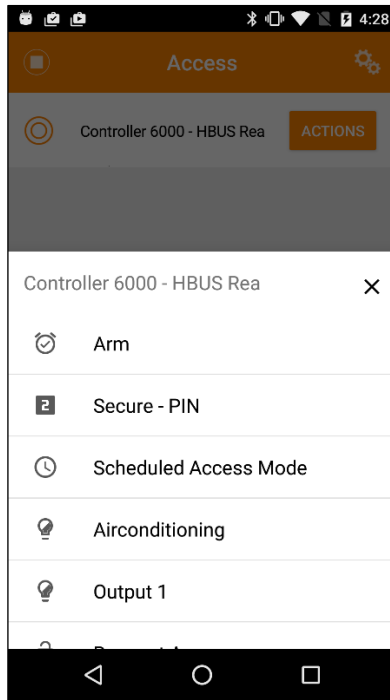
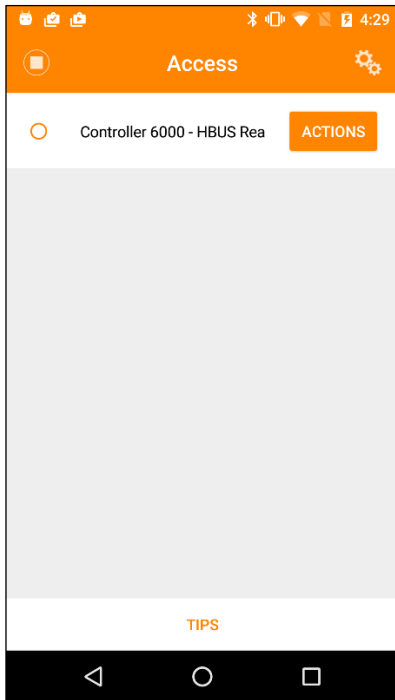
☒ Auto-isolate alarm zones

OK
Cancel
Apply

A new 'Actions' button has been added to the Door on Mobile Connect.

Pressing this button will bring a list of actions that the user can perform.

And confirmation is given that an action has been requested.



Note: It will now be possible for a cardholder to Arm and Change the Access Zone to secure with one button press via the Mobile Connect Actions feature.

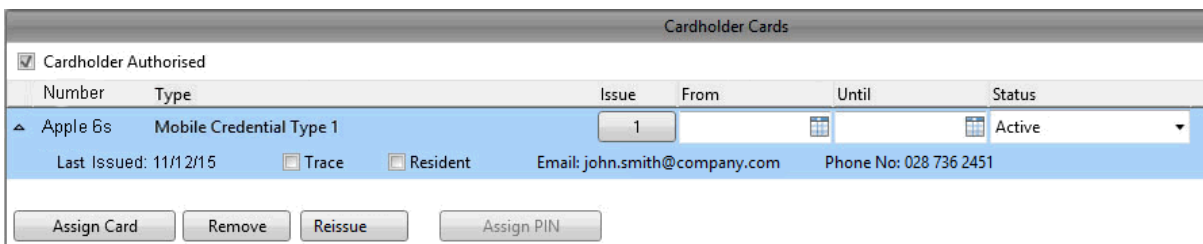
RE-PROVISIONING BLUETOOTH CREDENTIALS

Helps security managers re-issue credentials easier and faster (users get new phones, troubleshooting etc)

When a cardholder changes mobile phones or when a mobile credential needs reissuing v7.70 provides an improved operator experience for reissuing the credential.

A new 'Reissue' button exists in the Cardholder Cards tile to resend credential details to the last used email address and mobile phone number.

When an operator has the 'View Mobile Credential Email and Mobile' privilege in the division of the cardholder, and the card record is expanded using the 'Show More' arrow, the Email Address and the Mobile Phone number entered at the time the credential was issued are displayed.



The Cardholder History tile will now show the Phone ID if populated (or else the Mobile Credential ID), the email address used by the registration server when sending the email, and the phone number used by the registration

server when sending the SMS. If the operator does not have the 'View Mobile Credential Email and Mobile' privilege, this information will not be displayed.

The term 'reissue credential' is used to describe the process. It should be noted that the old credential is not actually reissued. The old credential is effectively deleted in the Cards tile and a new credential is issued. The user may be required to manually delete the old credential from the mobile device. This enhancement is primarily targeted at speeding up the process of manually deleting of old and assigning of a new credential, with the additional benefit of retaining the last used email address and phone number.

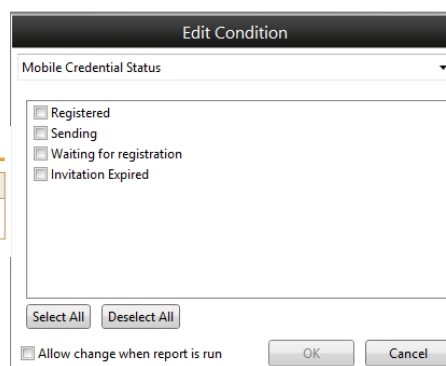
MOBILE CREDENTIAL STATUS

The Cardholder Report now includes a Mobile Credential Status column to view the status of mobile credentials.

Mobile Credential Status Report

First Name	Last Name	Card Type	Card Number	Mobile Credential Status
John	Smith	Mobile Credential	7c213013-3a5d-471b-82b3-9110173ef909	Sending

The report also includes a Mobile Credential Status filter allowing easy identification of outstanding credentials. This filter is also available in the Cardholder Viewer advanced search and in Cardholder Bulk Change.



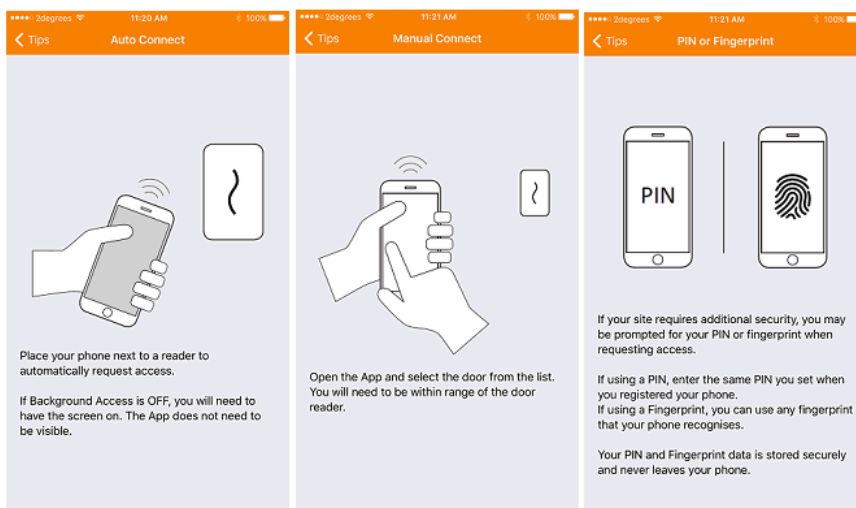
MOBILE CONNECT - TIPS

Provides people with useful hints and tips while using the Mobile Connect App

From the main Access screen and the Settings screen, a Tips screen can be accessed that provides concise information regarding:

- Auto Connect
- Manual Connect
- PIN and Fingerprint use
- Background Access use and recommendation (different for iOS and Android)

Tips can be toggled on/off from the Settings screen.



MOBILE CONNECT - ADDITIONAL ENHANCEMENTS

The following usability improvements enhance the experience of interacting with the Mobile Connect App:

- Email icon and text points the user back to the registration email when no credentials are installed
- Manual Registration link has been added to the main Access screen.
- Previous series of pop-up configuration requirements (e.g. Enable Bluetooth, Set a Passcode) are now displayed in a list.
- The registration email clarifies the two-step process 1) download app, and 2) accept credential.
- The button size for Two Factor authentication is increased, and keypad and fingerprint icons added.

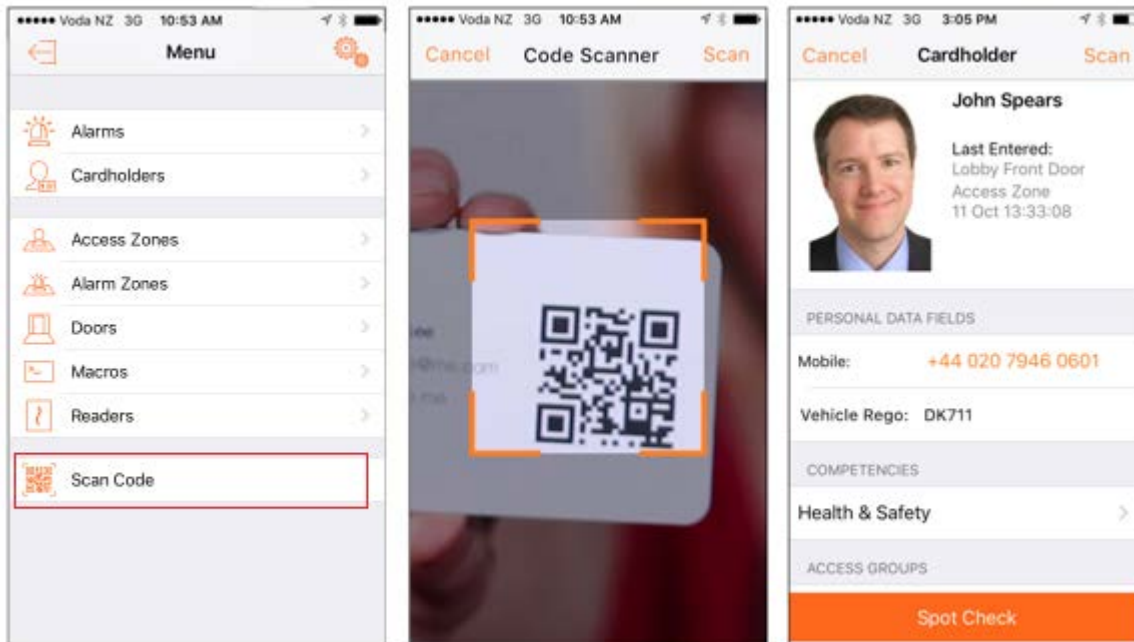
Command Centre Mobile

BARCODE READER

Command Centre Mobile can now be used to scan QR or Barcodes to check people (or items) to ensure they are who (or where) they should be, uses include:

- Enable parking wardens to check the validity and status of parking permits.
- Provide temporary ID for a corporate gala or seminar.
- Enable validation of exam participant identification.

The Barcode/QR code scanner is a recent customization merged into the core mobile client, enabling users to search for a cardholder via a barcode. The feature is available on both iOS and Android phones. The barcode is attributed to the cardholder by assigning them an additional card in Command Centre which is linked to the barcode number. A scan of the code will display the cardholder's details in the Command Centre Mobile app.



Gallagher has successfully tested this feature with the following barcode formats:

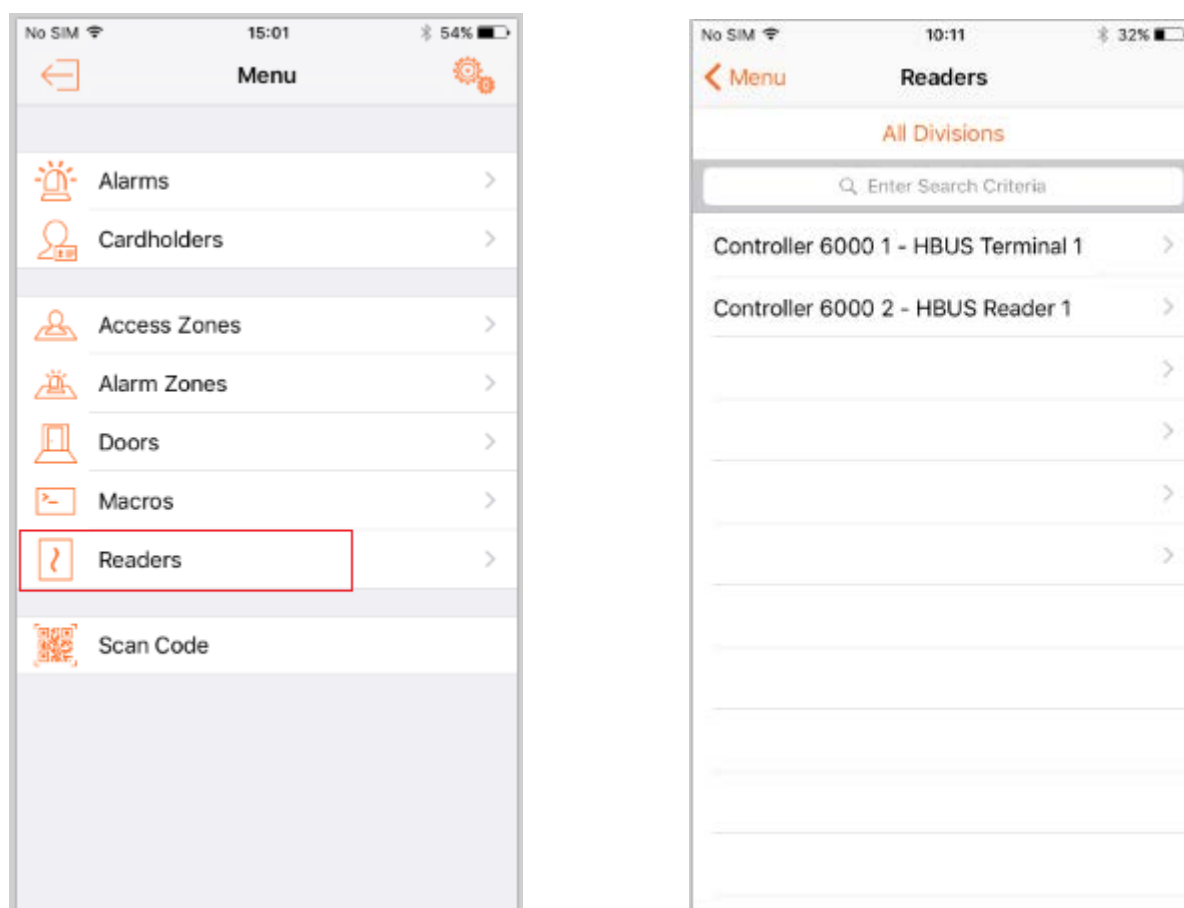
- Aztec Code 2D
- DataMatrix 2D
- PDF417 2D
- QR Code 2D
- Macro PDF417 2D
- Semacode 2D
- Code 128 1D
- Code 32 1D
- Code 39 1D
- EAN-13 1D
- EAN-8 1D
- ISBN 1D
- EAN-99 1D
- EAN-Velocity 1D
- Interleaved 2 of 5 1D
- UPC-A 1D

READER BLUETOOTH CONFIGURATION

Configuration of BLE readers is now quicker and easier with Command Centre Mobile, the installer can simply stand where they want the access transaction to take place and let the calibration feature automatically assign the values.

Prior to v7.70 the configuration of Bluetooth Low Energy (BLE) settings was exclusive to the Bluetooth Settings property page of the reader. Configuration of your BLE capable readers is now fast and easy, removing complexity from the installation. An installer can configure each reader's BLE settings using Command Centre Mobile. Rather than recording the Path Loss and Transmit Power values to manually enter them into the Configuration Client, the installer stands where they want the access transaction to take place and the calibration feature automatically assigns the values.

The main menu contains a 'Readers' option that when selected allows a search of any configured reader. The operator must have at least the 'View Site' privilege in the reader's division to see the reader, and the 'Edit Site' privilege in the reader's division to edit the BLE settings in the Configuration screen.

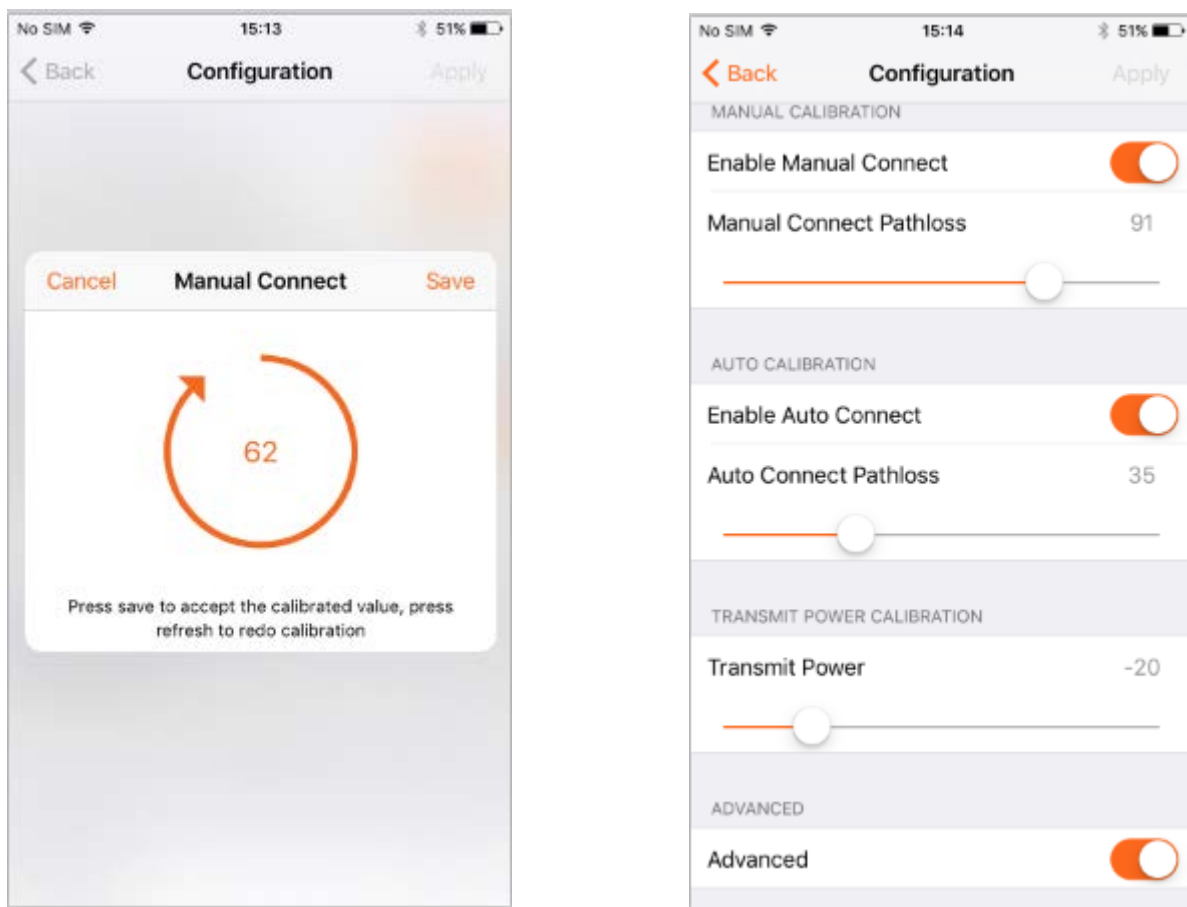


BLE controls are shown in an intermediate Readers screen (not shown in examples) to control:

- Use of Site Defaults
- Enabling Bluetooth
- Forcing Second Factor authentication
- Advertising Reader Name
- Configuring BLE range (as described below)

An operator can calibrate the Manual Connect range (Path Loss value) by tapping the Calibrate circle. Visual feedback will display as the read range is adjusted. Similarly, the Auto Connect range can be determined using the same process. The Transmit Power level can also be calibrated using this method and should be set at a

distance beyond the Manual Connect range. Under most operating scenarios, the transmit power will not need adjusting. An advanced option presents sliders to manually configure the values.



CONNECTING TO COMMAND CENTRE THROUGH A REVERSE PROXY

Provides secure deployment options to set-up Command Centre Mobile on secure networks.

From v7.70, the new "Signed Token" device identification mode has been added. This mode allows traffic to be intercepted by a reverse proxy server which can inspect requests, absorb malicious traffic, and other such features. The mode is designed to be compatible with existing reverse proxy solutions, such as the widely-used Nginx linux web server, so customers can use their existing preferred security appliances.

Prior to v7.70, Command Centre Mobile used TLS client certificates for identification of mobile devices. Connections using TLS client certificates require a direct TCP network connection to the Command Centre server, and thus it was not possible to insert an HTTPS proxy as a line of defense in front of the Command Centre server.

Using Command Centre to change the device identification mode, or the TCP port numbers used by the mobile client API's no longer requires a server restart.

Personalised Notifications

This feature is now available without separate license, and allows timely notification to selected users of card related info - card expiry, competency expiry etc.

Whereas original or standard event notifications send any event to a dedicated cardholder, Personalised Notifications allows cardholder related events to be sent to the related cardholder and/or their supervisor (or other role).

Notification filters are normally configured against cardholder records and send event notifications to those cardholders (e.g. guards). Personalised Notifications are configured by placing the notification filters against access groups and send cardholder related events only to the related cardholder if that cardholder is a member of the access group (or a child access group).

To send event email or SMS to:	Configure Notification Filter against:
Guard (or non-related cardholder)	Each particular guard/cardholder
Related cardholder	Access Group

In Configuration Client, a Personalised Notifications property page has been added to the Access Group item. This page behaves in the same manner as the Event Notification property page on the Cardholder record with the addition of the text "Cardholder related events only sent to Access Group (and child group) members". The notification filter will only send notifications to access group (and child group) members while the notification status and filter status are enabled.

In Command Centre, Notification Filters along with a notification schedule and method can be assigned to an Access Group in the Personalised Notifications tab.

Filter	Schedule	Method	Enabled
High pri and above	Default Notifications Disabled	Email and SMS	<input checked="" type="checkbox"/>

An operator must have at least the View Site privilege (in the appropriate division) to view a Notification Filter, and the Configure Site privilege (in the appropriate division) to edit a Notification Filter.

The Edit Cardholder Notification privilege is required to:

1. enable/disable notifications on the Access Group, and
2. change the Notification Method assigned to each Notification Filter.

An operator with the 'Edit Cardholder Notification' privilege must have the 'View Site' privilege in the Notification Filter's division before that Filter can be added or removed from the Access Group (would still allow enabling/disabling the filter with 'Edit Cardholder Notification' alone).

An operator with the 'Edit Cardholder Notification' privilege must have the 'View Schedules' privilege in the Schedule's division before that schedule can be added (alongside the notification filter) to the Access Group.

The Role properties have been extended so that these cardholder related events can exclusively or additionally be sent to cardholders filling a relationship/role (e.g. Supervisor).



☒ Card Expiry Warnings
☒ Competency Expiry Warnings
☒ Cardholder related events (Personalised Notifications)

The following table shows the required configuration for the possible notification features:

To send email or SMS for:	Configure the following:
Selected events to a guard (or other cardholder)	Email and/or Mobile PDFs against the guard/cardholder As per table above Notification Filter against guard/cardholder
Selected events to guard's (or the cardholder's) supervisor (or other Role)	Not applicable. To achieve this, set the same Notification Filter against the supervisor (or other Role) cardholder record
New: Cardholder related events to the cardholder	As per table above Notification Filter against Access Group Email and/or Mobile PDFs against the cardholders
New: Cardholder related events to the supervisor (or other Role)	Email and/or Mobile PDFs against the Role cardholders 'Cardholder related events' notification flag set for Role
Card or Competency expiry warnings to the individual cardholder	Email and/or Mobile PDFs against the cardholders Card Type and/or Competency advanced warning set
Card or Competency expiry warnings to the supervisor (or other Role)	Email and/or Mobile PDFs against the Role cardholders Card Type and/or Competency advanced warning set Card or Competency Expiry Warnings notification flags set for Role

This enhancement does not change the way Notification Filters are configured. Changes are made only to the assignment of the notification filters (to the Access Groups) and the 'Cardholder related events' notification flag available on the Role.

Notes:

1. If a Cardholder has been assigned a Notification Filter directly, as well as belonging to an Access Group containing the filter, or if they belong to multiple Access Groups that contain the filter, then the Cardholder will receive only one notification event for each event matching the filters.
2. When a Notification Filter is assigned to an Access Group, events that are not related to a Cardholder, (e.g. Tamper) will not be sent to Cardholders assigned to the Access Group.

HTML Email Notification Templates

Look and feel enhancements to emails templates allowing users to personalize their communications

Command Centre v7.70 comes with three custom and four standard (default) HTML email templates, located at C:\Program Files (x86)\Gallagher\Command Centre>EmailTemplates. The custom templates provide examples of how the feature can be used to customize notification email output. We recommend that before importing new templates, you back up existing templates to a location of your choosing. This is to prevent users from accidentally editing the default templates. To revert the templates back to their original versions you can import a backup template or re-install them from the Command Centre DVD. HTML templates support the following email notification features:

- Event Notifications (includes original/standard event notifications and the newly introduced Personalised Notifications)
- Individual Card and Competency Expiry Warning Notifications
- Role Card and Competency Expiry Warning Notifications
- Broadcast Notifications

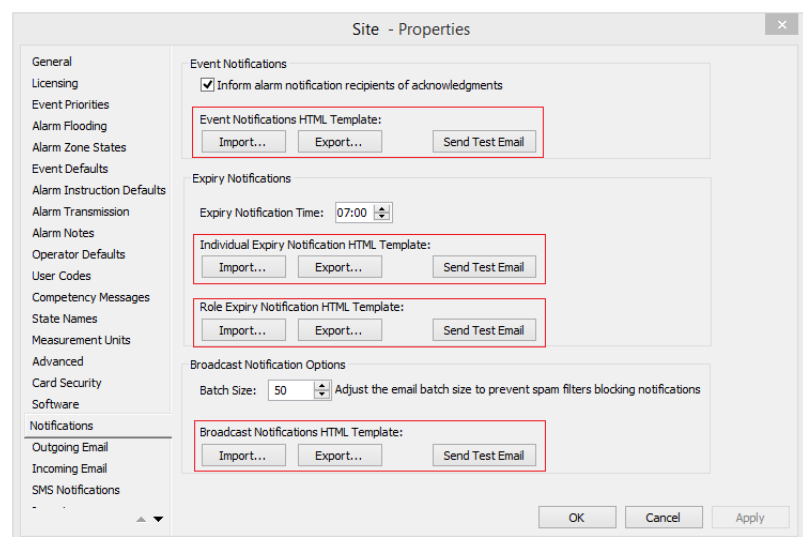
HTML templates are able to be created or edited by sites independently to allow the following enhancements to email notification subject line and body:

- Logos and other images
- Corporate standard fonts and colours
- Instructions for what a cardholder needs to do when they receive notification of a card or competency warning or expiry
- Embed URLs so that a form can be downloaded or filled in online for card or competency renewal
- Further cardholder PDF details for each expiry, and each cardholder related event notification
- Customised subject line

The feature allows sites to:

- Send different e-mail Expiry Notifications for different Card Types or Cardholders (e.g. by Division or Personal Data Field value)
- Send different e-mails for different Broadcast Notifications
- Send different e-mails for different kinds of Event Notifications (by Event Type, Event Group, Event Source)

Once you have imported a template, you can send a test email to a designated email address (e.g. your own, by setting up an Email Personal Data Field for the logged in operator's cardholder record and ensuring the Notification flag selected), to check the look and feel of the email before sending it to its intended recipients. Test emails all contain dummy data. An export feature is provided to allow a site to export (and then save) an existing HTML template which is helpful when the file is misplaced.



For more details (including how HTML inserts and conditions can be used to include or exclude email content) see the *Gallagher Command Centre HTML Help document* - available on the v7.70 installation DVD.

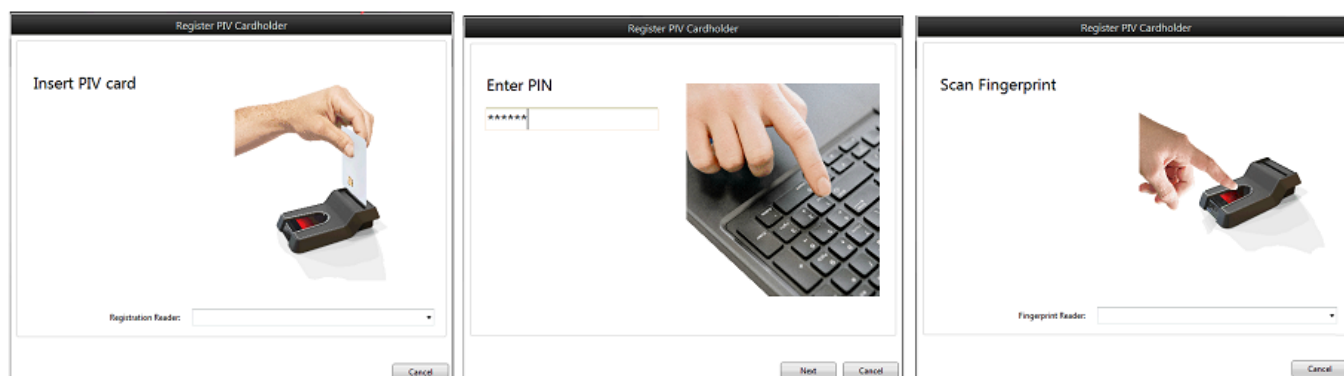
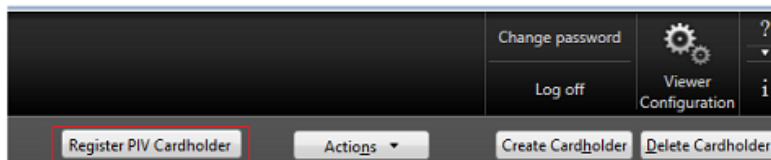
PIV Cardholder Registration

Now a native part of PIV Command Centre, making installation and use simpler. It is a more cost-effective solution as users do not need to purchase or maintain separate PIV card enrollment software.

Gallagher Command Centre v7.70 now enables PIV Cardholder registration directly from within PIV Command Centre, without the need for third party PIV cardholder enrolment software. Gallagher's PIV cardholder enrolment is designed to be compliant as a FIPS 201-2 product component under the GSA Approved Product List (APL)

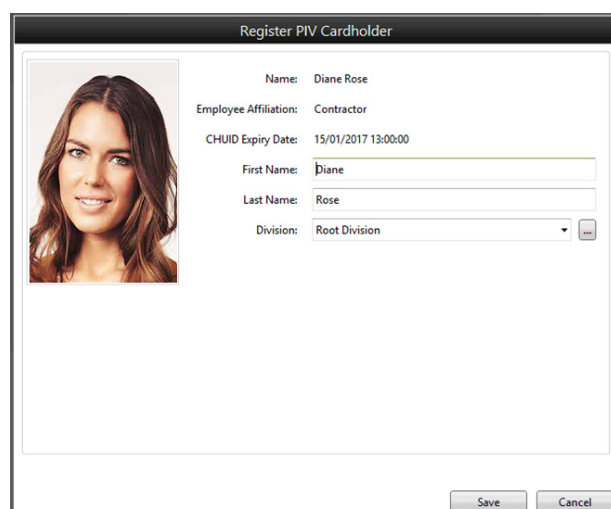
If an Operator has the privileges to create and edit a cardholder then the 'Register PIV Cardholder' button will become active.

This button will invoke the registration workflow prompting for insertion of the PIV card into the selected registration reader (USB Smart Card Contact Reader). The screen will then prompt for successful entry of the PIV card PIN and presentation of the cardholder's fingerprint, prior to the harvesting of the PIV card data into Command Centre. Certificate validation, fingerprint verification and card integrity checks are performed at the time of card registration.



When the cardholder registration has succeeded the cardholder details become visible in the Register PIV Cardholder light box. The Name, Employee Affiliation and CHUID Expiry Date are non-editable fields as read from the card. The First Name, Last Name and Division are editable fields representing the details that will exist in the Command Centre database when saved.

Once saved, the newly created cardholder appears behind the light box in the Cardholder Viewer, providing confidence to the operator that the registered details have been committed to the database. At this stage the light box returns to the 'Insert PIV Card' dialogue.



It is also possible to register a PIV card directly against a cardholder from the Cardholder Cards tile by selecting the 'Assign PIV Card' button. This method is only recommended when the cardholder is known to already exist in Command Centre, and they have been re-issued a replacement PIV card with a different card number.

Cardholder Cards						
<input checked="" type="checkbox"/> Cardholder Authorised						
Number	Type	Issue	From	Until	Status	Last Validation Time
3201-0295-759494-116464979587132011	PIV Card	1	30/03/2017 10:48	31/12/2030 13:00	Active	

Configuration

Prior to registering a PIV card, an 'Image' type Personal Data Field should be created and linked to the PIV Card type in the Registration Options property page. This link allows the image to be stored in the Command Centre database and displayed against the cardholder. To display the image in the Cardholder Images tile, the image PDF is assigned to an Access Group to which the cardholder is a member.

PIV Card - Properties

Personal Data Field used to store the facial image read from PIV cards

Photo

To streamline this process, Gallagher Command Centre allows Access Groups to be automatically assigned to PIV cardholders during registration. This is easily configured in the Registration Access property page for the PIV Card type.

PIV Card - Properties

Default Access Groups added to PIV Cardholders

Access Group	Description
Access Group 1	
Access Group 2	Includes the PIV Card Type Image PDF

The Registration Options property page is also home to the registration client's certificate validation options:

Client side Certificate Validation Option	Default	Description
Validate optional certificates	Unchecked	If checked, the two optional certificates (Key Management Certificate and Digital Signature Certificate) will be validated.
Validate the content signing certificate	Checked	If unchecked the content signing certificate will not be validated. This is used to digitally sign the PIV objects and is issued to the issuer of the card and not for the cardholder. If you choose to trust this issuer then you may be happy to not validate this certificate
Ignore end-entity certificate revocation unknown	Unchecked	If checked you are allowing entity certificate with unknown revocation status to be enrolled. This may be of benefit when experiencing network problems or the CA server is down, to allow enrolment immediately
Ignore certificate authority revocation unknown	Unchecked	If checked you are allowing intermediate certificate with unknown revocation status to be enrolled. This may be of benefit when experiencing network problems or the CA server is down, to allow enrolment immediately
Enforce CHUID expiration nesting	Unchecked	If checked, all certificate expiry dates need to be on or before (not after) CHUID expiry date
Ignore time not valid	Unchecked	If checked, validation will ignore expired certificates and certificates not yet active

Licensing

The PIV Cardholder Registration feature is a standard feature of a PIV Command Centre license, and does not require any additional licensing.

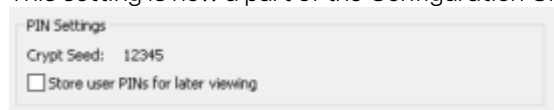
Cardholder PIN management options

Command Center Version 7.70 restores the “View PIN’s privilege”, and also provides the option to determine as to whether the (manual allocated User) PIN’s will be encrypted and stored for operators that have the View PIN’s privilege.

In Command Center version 7.40 a process was introduced to provide an additional layer of security for cardholder PIN (personal identification number) data. Through the use of encryption and a hashing procedure to further obscure discoverability of Access Card PIN’s within the system, the manual allocation procedure was changed and the ability to view PIN’s was removed.

Feedback from a number of customers suggested that this level of security was not needed for some sites and that there was a need to view the PIN for some trusted operators, especially if the site had cards encoded and issued in bulk. (Automatically allocated System PIN’s).

This setting is now a part of the Configuration Client - Server Properties.



Note: An operator can only see User PIN's if they have the privilege and the checkbox is checked in the server properties. An operator can see System PIN's if they have the privilege and the PIN hasn't been changed, if it has changed it then becomes a User PIN and the rule above applies. User PIN's changed prior to the checkbox being checked are not retrievable and will need to be reallocated if the cardholder has forgotten it.

On upgrade

For sites changing from Command Center v7.30; there are no noticeable changes, check the checkbox if the desire is to extend the View PIN’s privilege to see user PIN’s as well as System PIN’s.

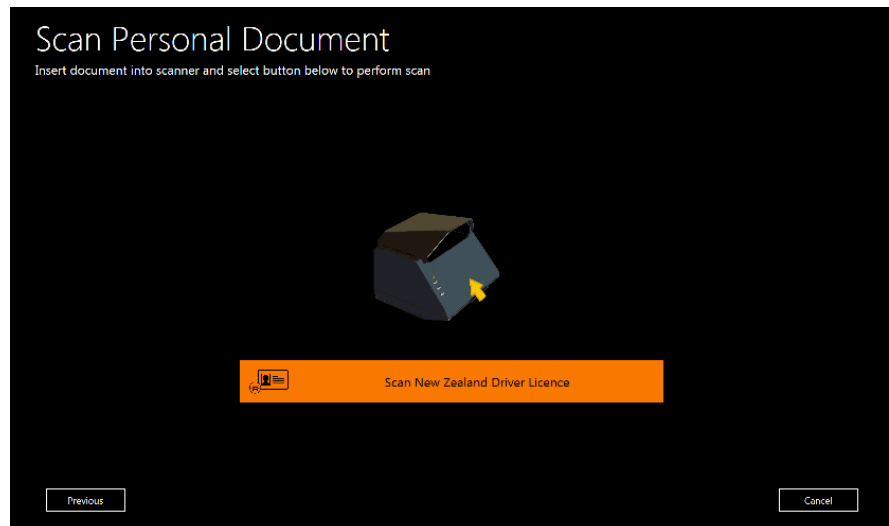
Command Center v7.40 onwards; if this functionality is required, the View PIN’s Privilege will need to be allocated to the trusted operator groups. The system PIN’s will be visible; However, the above check box will need to be checked if the desire is to see User PIN’s (from that point on).

Visitor Management Kiosk

Allows users to incorporate driver's license & passport scanning into 'sign in' processes at our visitor management kiosks, capturing the information and enabling auto-fill for text fields during sign in.

SUPPORT FOR PASSPORT & DRIVERS LICENSE SCANNING

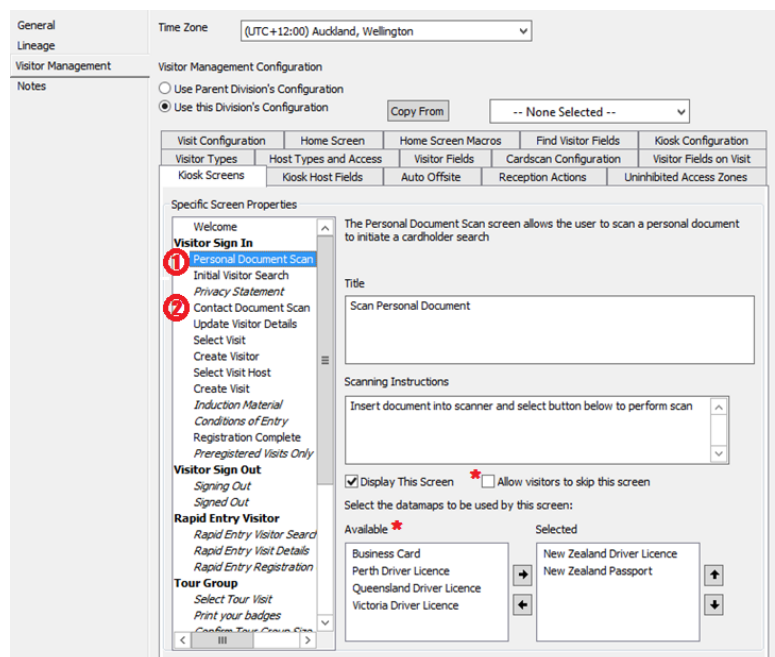
The types of customer needing this functionality tend to be those requiring some officially recognized form of identification. This enhancement adds the ability to scan Identification documents (in addition to business cards) as a part of the Visitor management kiosk process. Support is provided using the Acuant Snapshell Scanner.



Configuration options have been provided to:

1. Allow the scanning details to appear in a separate screen prior to the initial search screen (personal details scan) and the additional information screen (contact details scan).
2. Allow the second document type (for example business card) to provide contact details on the additional details information screen.

Note: Sites have the option to enforce that an official document be scanned, or skipped. A global list of Passports and Drivers Licenses is supported, Documents specific to a region are set up as a part of the configuration within the Command Center Administration Data Maps.



Licensing

Visitor Management is a licensed feature, adding to a growing list of Visitor Management Integrations and customizable configuration options for customers.

Minor Enhancements

RESIZING CONFIGURATION CLIENT PROPERTY PAGES

Allows easier visibility of pages containing large amounts of detail

Configuration Client property pages can now be resized, allowing easier visibility of pages containing large amounts of detail. This minor improvement will especially help when viewing grid pages with many columns or item names that are unusually long.

TRACKING THE PERSON, NOT THE CREDENTIAL

Tightens security when people have more than one credential in use

With the implementation of Mobile Connect, it is now more likely that Cardholders will own two or more credentials. Prior to v7.70, Command Centre tracked credentials in order manage the Dual Authorization, Anti-passback and Zone Counting features. From 7.70, Command Centre will now track the cardholder regardless of which credential they use. It is no longer possible for a cardholder to share one of their credentials and potentially violate Anti-passback or similar features.

PLAYING A TONE ON T-SERIES READERS WHILST THE DOOR IS RELEASED

Lets people know audibly when a door is unlocked remotely, useful to alert the person at the door that they can now gain access.

From v7.70, there will be a new setting on the Doors Advanced Properties page that allows a site to configure their T-Series readers to play a tone whenever the door lock is released. This will play if the door is released by a remote release button, Command Centre Override or an exit button.

Category	Property	Value	Unit
Advanced	Lock type	Mortise	
	Access is via turnstile	<input type="checkbox"/>	
	Door is confirmed as closed after	200	Milliseconds
	If lock attempt fails, alarm after	20	Seconds
	Retry the lock	<input checked="" type="checkbox"/>	
	Door unlock time	5	Seconds
	Second card (for two-card entry) must be swiped within	10	Seconds
	PIN (for PIN entry) failed if not entered correctly within	99	Seconds
	Door warns 'Open Too Long' if still open after	20	Seconds
	Door is 'Open Too Long' if still open after	20	Seconds
	Door is 'Forced Open' if opened while still locked	<input checked="" type="checkbox"/>	
	Door lock status follows entry zone only	<input type="checkbox"/>	
	Play tone on HBUS readers while door is unsecured	<input type="checkbox"/>	
	Play tone on HBUS readers when door is released	<input checked="" type="checkbox"/>	
	Extended access time	25	Seconds

There are several use cases that this will address. Firstly, it will alert someone standing outside of the door that they have been buzzed in and can open the door. Secondly, it meets a health and safety requirement to alert a person on the other side of the door that it is being opened.

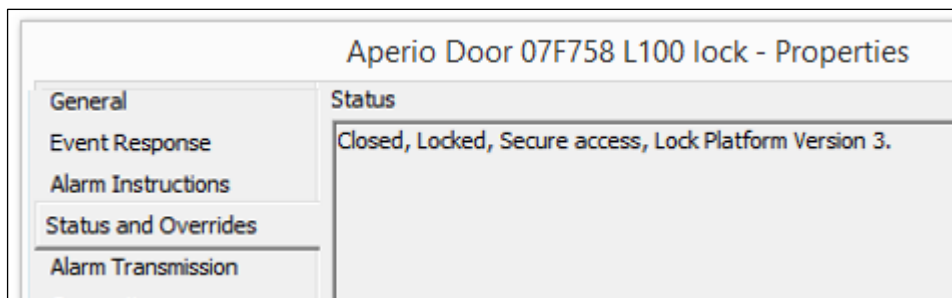
Third Party Interfaces

APERIO V3

Aperio v3 hardware and software are now supported with Command Centre v7.70. Key new features supported with this upgrade are listed below.

General Functionality

- The access mode of Dual Authorization is now fully supported for Aperio doors.
- The Aperio door supports the new Non-diversified Mifare Plus Object as well as the existing Non-diversified Mifare DESFire Object. Pre-encoded HID iCLASS 26/8 cards are supported with high frequency Aperio readers. HID 125 KHz cards are supported with low frequency Aperio readers.
- Aperio doors can now be overridden to open using the Open Door override from the Master List Window.
- A mini-poll between the Hub and Aperio door enables lock state changes to be sent from the Hub without a card badge. Command Centre operators can now action timely overrides and remote emergency lockdown. The defined polling time is configured within the PAP configuration tool (5 or 10 seconds) and this defines the latency duration between the lock and hub.
- The Aperio Lock version can now be identified from within the status and overrides tab. Aperio locks will report the Platform version used by the lock. Aperio Hubs will report the platform and firmware version that is supported by the hub.



Privacy Mode

A Privacy Mode with optional Privacy Override is introduced, where a cardholder can press a button on a lock to ensure other cardholders cannot gain access. An 'Aperio Privacy Override' check box will appear as an access privilege on the Access Group's Privileges tab. The checkbox will be unticked by default. When Privacy Mode is on for any room, cardholders with access to the room and in an Access Group with the privacy override flag selected, can enter the room.

The privacy button is not available on all Aperio Lock hardware.

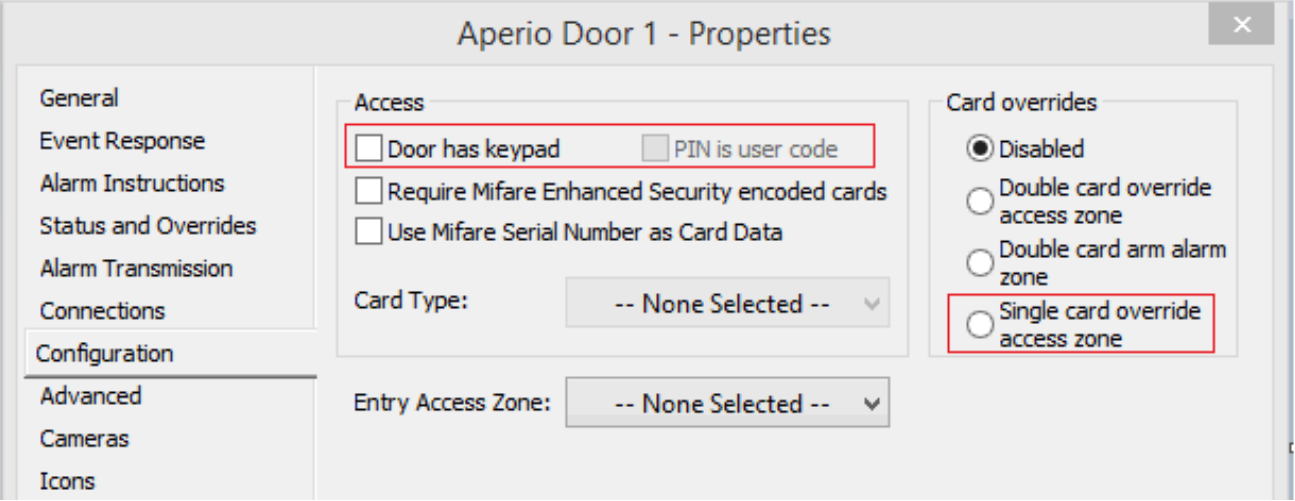
Aperio Door

It is possible for up to 1000 cardholders to be cached at the lock to enable the door to open without wireless connectivity. The Aperio cache will only accept card credentials i.e. user PIN and key code cannot be cached for off line access. An option 'Clear dynamic cache' exists in the door override menu to clear the cache of cardholders (Configuration Client only). The maximum duration a cardholder will remain in the Aperio door cache is 30 days (PAP tool configuration) from date of last access.

A new 'Door has keypad' option exists on the Aperio Door item to allow a second factor of authentication. It is recommended that this checkbox is ticked whenever the associated door has a keypad. If the door has a keypad

and this is not ticked, then Command Centre may deny access without waiting for a PIN to be entered, when the Access Zone is in PIN mode. When this checkbox is ticked, it enables the 'PIN is user code' option. When ticked this allows the cardholder to enter their cardholder User Code as the PIN number.

A new single card override option is introduced. A common use case exists to allow the cardholder to use escutcheons in the same manner as Aperio cylinders. Rather than badging every time to get access, and potentially getting into the situation where the card is accidentally left in the room, the card can be used to unlock the door, and then have the door remain in free access until the card is again used to lock the door. To achieve this, use the 'Single card override access zone' on the Aperio Door item. When this option is ticked a single badge at the door will override the zone into 'Mode 2' e.g. a typical scenario would be to have a zone in 'Secure - No PIN' and Mode 2 set to 'Free - No PIN'. In this example, a single badge will open the door and leave the door free. A subsequent badge at the door will set the access mode back to the scheduled state. The double card access and alarm zone overrides have been renamed for clarity.



Aperio door properties are extended to include a 'Door unlock time' and 'Extended Access time' controls

Option	Details
Door unlock time	The maximum time the door is unlocked
Extended Access time	The period of time the door will remain unlocked in addition to the Door unlock time for those cardholders who require more access time

General

Event Response

Alarm Instructions

Status and Overrides

Alarm Transmission

Connections

Configuration

Advanced

Cameras

Icons

Notes

Aperio Door 1 - Properties

Second card (for two-card entry) must be swiped within10Seconds

Door warns 'Open Too Long' if still open after20Seconds

Open warning-- None Selected --

Door is 'Open Too Long' if still open after20Seconds

Door is 'Forced Open' if opened unexpectedly

Door unlock time5Seconds

Extended Access time25Seconds

Access Group Options

When licensed for Aperio, 'Aperio Privacy Override' and 'Aperio Offline Access' check boxes will appear as access privileges on the Access Group's Privileges tab. Both check boxes will be off by default.

Privilege	Details
Aperio Privacy Override	When Privacy Mode is On for any room, cardholders with access to the room and in an Access Group with the Aperio Privacy Override privacy flag selected can enter the room
Aperio Offline Access	Cardholders in an access group with this privilege enabled will have their card details held at the Aperio door/lock, hence enabling the lock to open for these cardholders without wireless connectivity

The screenshot displays the 'Access Group 1' configuration page. At the top, there are fields for 'Name' (set to 'Access Group 1') and 'Description'. Below these are tabs for 'Access', 'Cardholders', 'Alarm Zone', and 'History / Notes'. The 'Access' tab is active, showing an 'Access Zone' section with a 'Schedule' button. On the right, the 'Access Privileges' section lists several options with checkboxes: 'Visitor', 'Visitor Escort', 'Lock/Unlock Access Zones', 'Entry During Lock Down', 'First Card Unlock', 'Aperio Privacy Override', and 'Aperio Offline Access'. The last two options are highlighted with red boxes, indicating they are the focus of the document.

New Product

MIFARE DESFIRE EV2 CREDENTIAL SUPPORT

Mifare DESFire EV2 credentials combine with the latest credential security features with quicker and more user-friendly performance at the reader.

NXP, the manufacturer of Mifare credential semi-conductors, has released its new generation of physical access smartcard technology, Mifare DESFire EV2. Mifare DESFire EV2 is the successor to Mifare DESFire EV1 and Mifare Plus credentials, and is now available for use on Gallagher T Series Readers.

Mifare DESFire EV2 key benefits include:

- Longer read range - DESFire EV2 features a significantly improved read range over Mifare DESFire EV1 and Plus credentials. Gallagher's DESFire EV2 card testing has shown read ranges of up to 60mm with Gallagher T Series card only reader, and up to 100mm on the Gallagher T20 Terminal.
- Enhanced Security - Mifare DESFire EV2 builds upon already strong DESFire EV1 and Plus security. MIFARE DESFire EV2 is Common Criteria EAL5+ security certified, which is the same security certification level as demanded for banking smartcards and electronic passports.
- Backwards Compatible - Mifare DESFire EV2 backwards compatibility means Gallagher can encode DESFire EV2 in the same manner as DESFire EV1 credentials. This means all sites with Gallagher T Series readers and Command Centre v7.00 and above can immediately begin to roll out Mifare DESFire EV2 credentials, at a pace which suits the site.
- Cost Effective - Gallagher is able to provide Mifare DESFire EV2 at a substantially lower price than DESFire EV1 credentials, delivering immediate cost savings to customers moving over to the new credentials.



Gallagher has tested Mifare DESFire EV2 for compatibility assurance with third party solutions currently offered by Gallagher on Command Centre v7.60 and beyond.

Parts:

C297472 - Mifare DESFire ISO Card, 2K, EV2

C297474 - Mifare DESFire ISO Card, 4K, EV2

C297478 - Mifare DESFire ISO Card, 8K, EV2

C297404 - Mifare DESFire EV2 Keyfob, 4K

Availability

Gallagher expects to have Mifare DESFire EV2 cards available for order, along with optional encoding service, from mid May 2017. Availability of the DESFire EV2 Keyfob is pending final validation testing, and will be announced via Gallagher's monthly communications.

T-SERIES NXP INTEGRATED CIRCUIT UPGRADE

Significant improvements to credential read range

All Gallagher T-Series Readers and Terminals now include NXP's latest Mifare Integrated Circuit for reader hardware. Applied to both Mifare only and Multi Technology variants of T10, T11, T12, T15 and T20 Readers, NXP's latest technology delivers exceptional read range performance for Mifare Classic, DESFire EV1, and DESFire EV2 credentials.

Technical Specifications

					
T-Series Readers	T10	T11	T12	T15	T20
Maximum Read distance - Mifare Classic	75mm	75mm	75mm	75mm	100mm
- DESFire EV1	50mm	50mm	50mm	35mm	95mm
- DESFire EV2	60mm	60mm	60mm	50mm	100mm
- Mifare Plus	30mm	30mm	30mm	25mm	65mm
- 125kHz	-	95mm	95mm	60mm	95mm
- Mobile Connect (BLE) ***	-	Configurable	Configurable	Configurable	Configurable

Table note: *Read range may reduce when Readers are mounted upon metal surfaces. Where Readers are mounted on metal, Gallagher recommends the use of optional Gallagher Reader Spacers to provide improved read range performance. Card manufacturing tolerances, installation environments, and user card orientation can impact read range; values should be considered as approximate. Read ranges are tested on Gallagher supplied Mifare Classic, Plus and DESFire EV1/EV2 cards, optimized for performance on Gallagher T Series readers; non-Gallagher supplied cards may exhibit lower read ranges.*

There is no change to part numbers or pricing following the implementation of the new Mifare IC from NXP.

T15 READER

The T15 reader has undergone comprehensive testing procedures to prove it is the best choice for outdoor use. Ideal for use in tough environmental conditions.

The latest addition to Gallagher’s range of T-Series Readers, the T15 Reader provides a mullion mountable reader option available in both Mifare only and Multi Technology variants. With the inclusion of Bluetooth Low Energy Technology componentry, all non-PIV T15 Multi Technology Readers also provide support for the Gallagher Mobile Connect solution.



Dimensions (Including Bezel) 140mm (L) x 44 (W) x 23mm (H)

Engineered to withstand the most challenging environmental conditions, the T15 features a thermoset potting compound with exceptional resilience to water and temperature variation that is new to the T Series Reader range. Designed to work well when installed upon metal without the need for a spacer, the T15 is also complemented by the following accessories:

- Black and white reader colour options
- Black, white, gold and silver bezel options
- Custom dress plate for retrofits

Parts

C300470	T15 Mifare Reader, Black	C300471	T15 Mifare Reader, White
C300480	T15 Multi Tech Reader, Black	C300481	T15 Multi Tech Reader, White
C305470	T15 PIV Reader, Black	C305471	T15 PIV Reader, White
C305480	T15 PIV Reader, Multi Black	C305481	T15 PIV Reader, Multi White
C300296	T15 Bezel, Black pk 10	C300297	T15 Bezel, White pk 10
C300298	T15 Bezel, Silver pk 10	C300299	T15 Bezel, Gold pk 10
C300324	T15 Dress Plate, Black pk 10		

Availability

All variants of the T15 Reader are now available for purchase

T21 PIV Reader

The Gallagher T21 PIV Reader houses a USB contact reader, and users only need to remember one PIN for a dual authorization PIV solution. The reader is fully compliant to the NIST SP-800-116 specification for dual factor authentication for access to 'Limited' security areas.

The Gallagher T21 PIV Reader provides site running the Gallagher PIV Solution with contact PIV card plus PIN authentication for security areas requiring dual factor authentication for access. The Gallagher T21 PIV Reader meets the requirements of the NIST SP-800 specification for dual factor authentication for access to 'Limited' security areas. The Gallagher T21 PIV reader has been designed to meet the FIPS 201-2 standards, and has been submitted for GSA Approved Product List (APL) compliance.

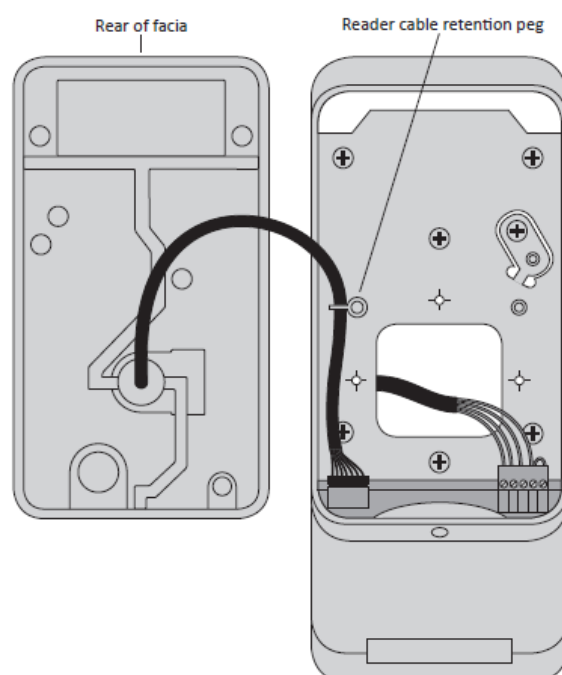


T21 PIV Reader Access

The T21 PIV Reader can be set to operate in single factor (card only – either contact or contactless) or dual factor (contact card + PIN) modes. When operating in dual factor mode, the reader requests the user to insert their PIV card into an insertion slot at the bottom of the reader, then enter their PIV card PIN. Before an access decision is made, the user is required to remove their card, ensuring the card is not left accidentally in the reader. The reader's card insertion slot features a blue illuminated strip, allowing users to easily locate the insertion point in low light conditions.

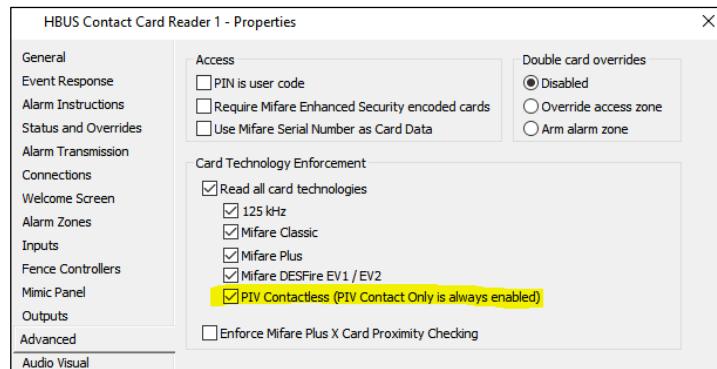
T21 PIV Reader Installation

Installation of the T21 is similar to the standard T series readers, with a reader bezel first mounted to the wall, with the field wiring fed through a central hole in the bezel. Unlike other T Series readers, the field wiring is then terminated at HBUS power and data connector screw terminals built into the bezel. The T21 fascia is then connected to the bezel via a plug-in connector, with the fascia inserted into the bezel and secured in place with a standard T Series Reader security screw.



T21 PIV Reader Configuration

The T21 PIV Reader is configured in the Command Centre Configuration client by creating a new HBUS Contact Card Reader item. The reader's PIV contactless card reading functions can be turned off, along with other supported contactless card technologies, for sites that wish to mandate a PIV contact card read as part of the door access process.



T21 Reader Parts

The Gallagher T21 PIV reader is available in black and white color variants, and with the option of standard and multi-technology variants. Gallagher has also produced both black and white bezel parts, as a cost-effective bezel replacement should the T21's card insertion slot become fouled or wear from card use over time.



C305500	T21 PIV Reader - Black
C305501	T21 PIV Reader - White
C305510	T21 PIV Reader - Multi, Black
C305511	T21 PIV Reader - Multi, White
C305280	T21 Bezel, Black
C305281	T21 Bezel, White

Availability

All Gallagher T21 PIV Reader parts are now available for order. Sites wishing to install the T21 PIV Reader must be running Command Centre v7.60 or beyond to configure the reader.

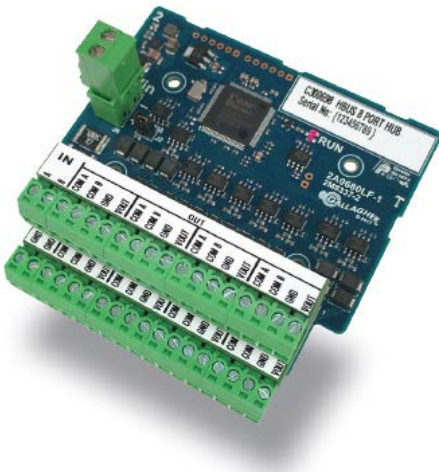
HBUS 8 PORT HUB

Gives installers the flexibility to re-use existing wiring on site, allowing combinations of star / home run and daisy chain wiring to be used when connecting HBUS devices back to the Controller.

The Gallagher HBUS 8 Port Hub provides a means of consolidating up to 8 x HBUS RS-485 wiring runs into one HBUS RS-485 run. The HBUS 8 Port Hub provides installers with the flexibility to re-use existing wiring on site, allowing combinations of star / home run and daisy chain wiring to be used when connecting HBUS devices back to the Controller. The HBUS 8 Port Hub can also act as an HBUS RS-485 repeater, extending the distance of HBUS devices from the controller far beyond the standard HBUS 500m/1,600ft.

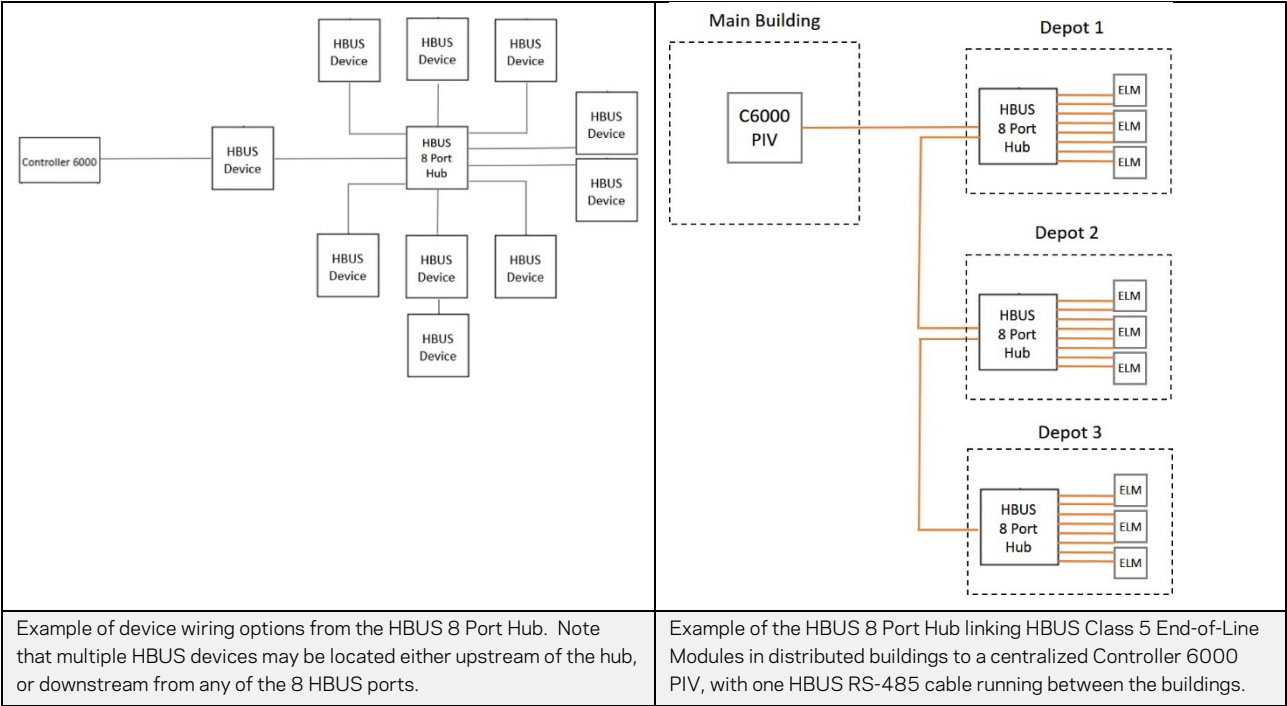
Features of the HBUS 8 Port Hub include:

- Consolidation of data from up to 8 downstream HBUS RS-485 data wires into one upstream run
- Supports multiple HBUS devices on all 8 downstream RS-485 runs, and additional HBUS devices further upstream from the hub.
- ¼ footprint PCB, allowing up to 4 HBUS 8 Port Hubs to be mounting on a single Gallagher hardware footprint
- HBUS RS-485 signal regeneration, allowing the hub to act as a repeater where additional distance is required beyond the standard HBUS 500m range (up to 1,200m/4,000ft when using 2 HBUS in series on the same wiring run)
- No Command Centre configuration required



HBUS Device wiring flexibility

The HBUS 8 Port Hub allows an installer to use a combination of wiring architectures to link HBUS devices back to the controller. The below diagrams describe two scenarios where this may be useful.



Part

C300698

HBUS 8 Port Hub

Availability

The HBUS 8 Port Hub is now available for order. The Hub does not require Command Centre configuration, as such it will work on all existing HBUS device installations.

Coming Soon

CLASS 5 INTRUDER ALARM SYSTEM

Gallagher's Class 5 Intruder Alarm System protects high value assets and information from emergent threats to successful intruder detection and alarms transmission. The Gallagher Class 5 Alarm System provides customers with a compliant AS/NZS 2201 Class 5 level Alarm System, the highest level of this intruder alarm system standard.

AS/NZS 2201 Intruder Alarm Systems Standards - Class 5

The AS/NZS 2201 Intruder Alarm Systems standards define requirements that intruder alarms are required to meet for various security level requirements. The standard covers all elements of an intruder alarm system, such as system product design and performance, installation, maintenance, and alarms monitoring specifications. The standards outline several alarm system performance levels, from low security alarms systems (Class 1), up to high security and performance intruder alarm systems (Class 5).

In mid-2016, Gallagher developed an HBUS Class 5 End-of-Line Module (ELM), a key component of a Class 5 compliant AS/NZS 2201 system. The HBUS ELM eliminates a viable attack against most existing alarm system sensor communications (4 state balanced input protection), effectively rendering the alarm sensor blind to intruder detection. Gallagher has now developed a Class 5 compliant cabinet and power supply, providing customers with a turn-key solution for AS/NZS 2201 Class 5 compliance.



New Class 5 Cabinet and Power Supply (PSU)

The Class 5 Cabinet, Controller and PSU (C306105) comprises of the base elements for a Class 5 compliant alarm system installation.

The Class 5 Cabinet is a deeper version of the Gallagher Dual Cabinet, catering for the larger Class 5 PSU and allowing for increased battery space. The ability to sense physical attacks to the cabinet is mandated in the Class 5 specification, which is provided by a vibration sensor pre-mounted in the cabinet. The AS/NZS 2201 Class 5 standard also mandates that the enclosure be secured via a restricted locking system. This is delivered via a bi-lock installed on the Class 5 Cabinet, with 2 keys provided with the cabinet delivery.

Gallagher's Class 5 PSU is a 100W PSU specifically chosen and tested for compliance to the AS/NZS 2201 Class 5 alarm system requirements. The PSU mounts on the side wall of the Class 5 Cabinet, and meets Class 5 requirements for battery charging and monitoring. The PSU supports several features, such as a battery temperature sensor for optimized PSU battery management performance, and battery alarm outputs for mains fail, battery low and no battery alarms.



The Controller 6000 HS PIV is required as the HBUS Class 5 ELM is equipped with a high grade secure cryptographic chip, to which only the PIV variant of Gallagher's controllers are capable of communicating. The Controller 6000 HS PIV supports up to 30 HBUS Class 5 ELMs per controller.

Beyond the Class 5 Cabinet, Controller and PSU (C306105), sites will add appropriate HBUS End-of Line modules, HBUS I/O Boards and T20 Terminals as their specific site needs require. Gallagher's Class 5 Intruder

Alarm System only requires standard Command Centre site licensing, with all standard licensed features available. The Gallagher Class 5 Cabinet (C306104) and Class 5 PSU (C306440) are available as individual parts, should these be required for an installation.

Gallagher Class 5 Power Budget Calculator

The ASNZ 2201 standard specifies that intruder alarm systems must provide a mandated amount of battery backup, and must recharge batteries within a defined period of time. Gallagher has produced a Class 5 Power Budget Calculator, which allows Channel Partners to work out the power budget for devices powered from the Class 5 PSU, to ensure the site remains within Class 5 specified tolerances.

The Gallagher Class 5 Power Budget Calculator is available for Gallagher Channel Partner use on the Gallagher Security Support Website.

Gallagher Class 5 Power Supply and Battery Calculator				V7.2.6
System parameters				Help
System size				
Required backup time	16	Hours		
Battery capacity	36	Hrs		
Total power supply capacity				
Equipment items				Help Enter the load items here. The "Total Load Current" is the load connected to the power supply.
	Current	No. of units	Load (Amps.)	
C6000 HS PIV	0.800	1	0.8	
T20 Terminal	0.200	1	0.20	
HBUS End of line module	0.015	16	0.24	
HD I/O board	0.650	1	0.65	
HBUS 8 Input board	0.050			
PIR	0.015			
LED Indicators				
Buzzer				
Electronics				
1				1.89
Battery details				Help The "Effective capacity" and "Time to discharge" values are the derated battery details resulting from the required system load, according to Peukert's Law.
Effective capacity, or	29.8	A-Hrs		
Time to discharge	15.8	Hours		
Time to charge				8.8
Disclaimer Gallagher Group Ltd, nor its subsidiaries, accept any liability for the data generated from the use of this spreadsheet. Calculations are provided as a guide only, the responsibility remains with the user to verify data and calculation accuracy.				

Class 5 Compliant – Independently Tested

Gallagher's Class 5 Intruder Alarm System is being fully tested to the ASNZ 2201 Class 5 specification, with the results verified independently by an IANZ accredited test laboratory. IANZ (International Accreditation New Zealand) is New Zealand's premier accreditation body, and is a full signatory member of the International Laboratory Accreditation Cooperation (ILAC) and the regional body, Asia Pacific Laboratory Accreditation Cooperation (APLAC). On the launch of our Class 5 Intruder Alarm System, Gallagher will provide Channel Partners and Consultants with proof of this test compliance, assuring all stakeholders that the installed system meets the exacting demands of this standard.

Parts

C306105	Class 5 Cabinet, Controller & PSU
C306104	Class 5 Cabinet, Cool Grey
C306440	Class 5 PSU, 100W

Availability

The above Class 5 parts are due for release May, 2017.

T15 MOUNTING BLOCK

The T15 Reader is able to be mounted on standard electrical flush boxes, with the addition of the T15 Dress Plate (C300324) to cover any exposed flush box area. However, mounting the T15 reader on external surface mount boxes (i.e. where external conduit fed wiring is run to the box) can present a challenge, due to the height of the reader creating an overhang.

The T15 Mounting Block, Side Cable Entry is a custom-made conduit mounting block for surface mount applications requiring a conduit wire feed to the T15 reader. The mounting block allows for conduit entry from all sides of the box, and is proportional to the size of the T15 reader.

Parts

C300951	T15 Mounting Block, Side Cable Entry
---------	--------------------------------------

Availability

Gallagher expects the T15 Mounting Block, Side Cable Entry to be available late calendar Q2, 2017.

VERIDT STEALTH BIO PIV READER

With Command Centre V7.70, Gallagher has integrated the Veridt Stealth Bio PIV reader, a reader which enables triple factor authentication for sites using the Gallagher PIV Solution.

The Veridt Stealth Bio reader meets requirements of the NIST SP-800 specification for three factor access to 'limited' security areas, allowing Gallagher to offer a complete PIV reader solution for all site areas. The Veridt Stealth Bio reader currently features on the GSA Approved Product List, and has been integrated with Gallagher PIV Command Centre v7.70 to gain full APL compliance with Gallagher's PIV Solution.

The Veridt Stealth Bio reader integrated with Gallagher PIV Command Centre delivers the following customer benefits:

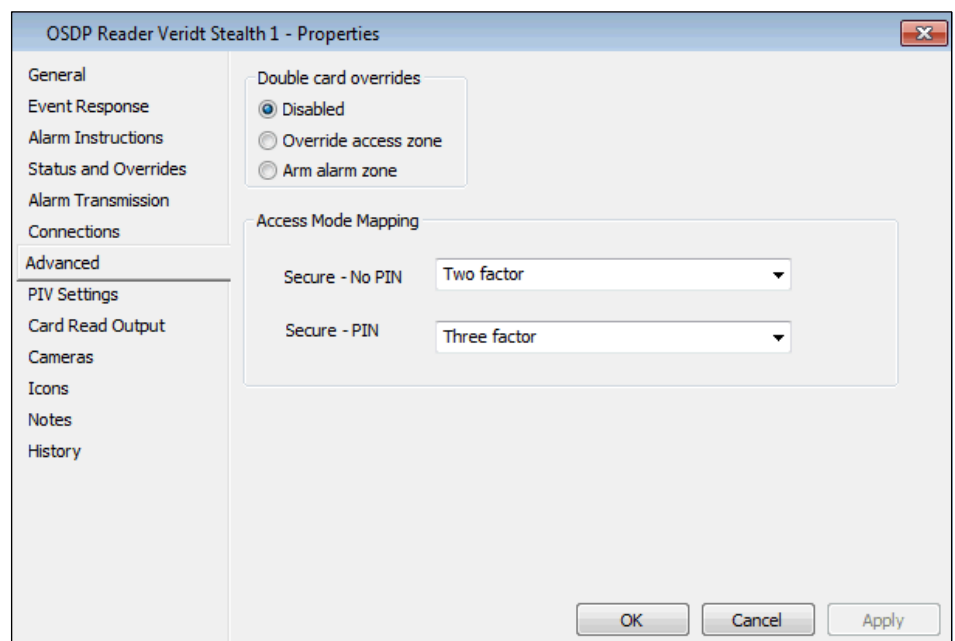
- Security - The Veridt Stealth Bio reader delivers triple factor authentication options for areas of a site requiring a high level of physical access control security.
- Compliance - The Veridt Stealth Bio reader integration with Gallagher PIV Command Centre has been designed for compliance to the FIPS 201-2 standard, backed up by GSA APL independent test results.
- Standards Based - Gallagher has integrated the Veridt Stealth Bio reader via the Open Supervised Device Protocol (OSDP), an open standard reader to controller protocol. A site with existing Veridt Stealth Bio readers can connect these readers via OSDP directly to the Gallagher Controller 6000 - PIV.
- Flexibility - The Veridt Stealth Bio reader can be scheduled to operate in either single factor (card only), dual factor (card + PIV card PIN), or triple factor modes (card + PIV card PIN + fingerprint), depending on the site's needs.



Veridt Stealth Bio Reader - Configuration

The Veridt Stealth Bio reader can operate in One Factor (Card Only), Two Factor (Card and PIN) or Three Factor (Card, PIN and Fingerprint) modes. It is possible to schedule these modes by using the Access Mode Mapping feature on the Advanced Setting of the reader's 'Properties' page:

Depending on the mode of access, the cardholder is guided through these steps by intuitive LEDs on the reader advising the user when to enter their PIN or place their finger on the fingerprint scanner. When configured for triple factor authentication, the reader scans a Cardholder's fingerprint and compares it to the one stored on their PIV card.

A screenshot of the 'OSDP Reader Veridt Stealth 1 - Properties' dialog box. The 'Advanced' tab is selected in the left sidebar. The 'Double card overrides' section has 'Disabled' selected. The 'Access Mode Mapping' section shows two rows: 'Secure - No PIN' mapped to 'Two factor' and 'Secure - PIN' mapped to 'Three factor'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

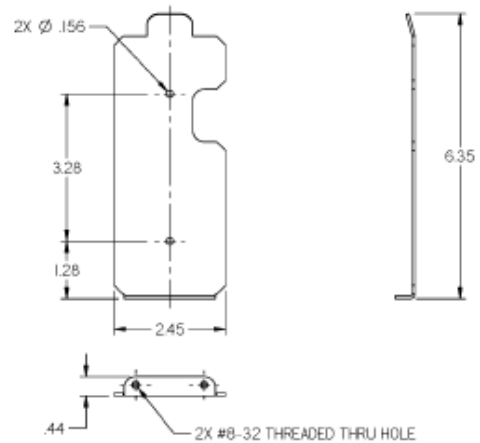
OSDP Reader Veridt Stealth 1 - Properties	
General	Double card overrides
Event Response	<input checked="" type="radio"/> Disabled
Alarm Instructions	<input type="radio"/> Override access zone
Status and Overrides	<input type="radio"/> Arm alarm zone
Alarm Transmission	
Connections	
Advanced	Access Mode Mapping
PIV Settings	Secure - No PIN Two factor
Card Read Output	Secure - PIN Three factor
Cameras	
Icons	
Notes	
History	
OK Cancel Apply	

Veridt Stealth Bio Reader - Installation

Installation simply requires attaching a metal backing plate to the wall, connecting the field wiring to the reader, then attaching the reader to the backing plate. The reader is then secured to the backing plate through the insertion of two screws into the bottom of the unit.

Parts

TBC Veridt Stealth Bio PIV Reader



Availability

The Veridt Stealth Bio PIV reader is being submitted with Gallagher PIV Command Centre v7.70 for GSA APL testing. Gallagher anticipates this testing will be completed during calendar Q2, 2017, at which point the Veridt PIV reader will be available for order from Gallagher. Sites wishing to use this reader will need to be running Gallagher PIV Command Centre v7.70 or higher.

COMMEND INTERCOM INTEGRATION

Intercom systems are an important part of security on many sites. While they have many benefits, they are yet another system that an operator must become familiar with and use on a daily basis. This integration will bring the day to day functionality from Commend into Command Centre, giving operators a single platform from which to manage access throughout their site.



Availability

Available with Command Centre v7.80.

CONTROLLER 6000 DHCP SUPPORT

Bringing Controllers online for the first time requires a technician on site, and can be a tedious process. As of v7.80 it will be possible to assign IP addresses to Controller 6000's from a DHCP server. This means that the responsibility of properly configuring Controllers moves from an Installer to a Network Administrator. Once a DHCP server is properly configured with the correct permissions, Controller 6000 DIP switches can be used to set the Controller to accept an IP from the DHCP server automatically. Once connection is established, the DHCP server will be capable of updating the Controller's IP address whenever the network requires it. This is particularly useful during network restructuring as technicians will not need to visit the site in order to physically access each controller individually, saving time and money.

Availability

Available with Command Centre v7.80.

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 80 2676 2084
Middle East.....	+971 4 2602145
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.

3E1361 - 03/17

