

Gallagher Command Centre

Gallagher Command Centre is the central management tool for the Gallagher security system. The software provides a powerful and versatile feature set.



Gallagher Command Centre leverages client server architecture, enabling system operators to:

- > Configure the site and all system components
- > Manage cardholders, including their access based on the competencies they possess
- > Produce and print photo identification cards
- > Monitor alarms and interact with the system to monitor the status of items or perform overrides
- > Retrieve and report on a variety of stored information including events, cardholders and their access, and site items
- > Communicate via Intercom enabled readers
- > Interface to other third party systems including DVR/NVR systems, intercoms or third party sensors.

The Gallagher system is scalable, with all Gallagher Command Centre server options available regardless of the number of doors, from less than 16 to an unlimited number of doors. It is a powerful yet operator friendly security system.

It can be incorporated into a company's existing Local Area Network, Wide Area Network, or reside on its own dedicated network. Gallagher Command Centre links to Gallagher Controllers and to operator workstations over Ethernet using TCP/IP, a world standard network and internet transmission protocol. Using this protocol means the system communications are internet compatible.

OPERATING PLATFORMS

The Gallagher Command Centre server and workstation software reside on the Microsoft Windows operating platforms.

The database options are Microsoft SQL 2005 (Standard or Express) or SQL 2008 (Standard, R2 or Express) depending on system and customer requirements.

Microsoft SQL is a commonly specified database used globally in a range of applications. Gallagher Command Centre data may be integrated or shared with other systems using the SQL Server database.

Please contact Gallagher for information relating to current operating platforms supported.

DISTRIBUTED PROCESSING

Multi-Server operation is a significant feature of the Gallagher system architecture.

Gallagher Command Centre supports communications between multiple servers, allowing the Gallagher system to operate effectively in a distributed environment. This multi-server environment may include multiple sites separated by large geographical distances and connected via low bandwidth and/or intermittently available networks.

The ability for an operator to view and manage information pertaining to a remote Gallagher Server can be configured via standard Operator Privilege and Division view functionality.

Cross-site Operational Cover

Multi-server architecture allows organisations to provide cross-site operational cover, where operators from one site can temporarily manage security on a remote site when a remote site Operator may be unavailable. This also allows a head office to maintain control of the security at any time on a remote site, should the need arise.



Cardholder Management

If the site experiences network communications problems, full operation of access control and alarms management is still maintained at a local level.

Peer-to-peer communications can be configured to set up relationships between Controllers for flexible and efficient system configuration.

Gallagher Controllers can also be configured for dial-up for the support of remote sites, and for off-site alarm monitoring. Gallagher has a range of industrial switches to provide a solution for redundant Ethernet network communications.

Multi-Server Evacuation Reporting

Any server in a Gallagher Multi-Server network can be configured to act as an 'Aggregation Server' to keep an up-to-date status of the location of all Cardholders over a Multi-Server network.

In the event of a disaster at one of the Multi-Server's sites, the Aggregation Server(s) can provide Evacuation Reports detailing the last known locations of Cardholders at the disaster affected site.

DATA SECURITY

Data over the network between the Gallagher Command Centre and Gallagher Controllers uses up to 256-bit AES encryption; a recognized industry leading level of data protection.

EASE OF CONFIGURATION

Gallagher Command Centre features Configuration Wizards and Templates, tools to support the ease of new system installation. Configuration Wizards enable access controlled doors and new hardware to be quickly and easily configured in Gallagher Command Centre while Database Template functionality allows a standard configuration to be applied to sites with common requirements.

SYSTEM DIVISION

System Division (partitioning) enables a site to be divided into divisions and sub-divisions. It is especially suitable for:

- Multi-tenant buildings where each tenant wishes to manage and monitor their own security
- Very large enterprise-wide systems where it is more practical to divide the site for ongoing management and monitoring, for example, dividing the site into geographic zones

OPERATORS AND WORKSTATIONS

Gallagher Command Centre places no limits on the number of workstations or operators that may be set up. Performance may be limited by the hardware used for the system.

Operators are managed through system division and assigned privileges allowing access only to authorized functions. Smartcard logon to Gallagher Command Centre is also available (Classic only).

MANAGEMENT OF ALARMS

An alarm is a special event that requires urgent operator intervention, for example, when a door is open longer than it should be, a device has been tampered with, an intruder alarm has been activated or a perimeter fence sensor has been triggered.

The alarm configuration in Gallagher Command Centre enables system administrators to define site events to be set up as alarms. Defaults apply system wide ensuring maximum flexibility while minimising the initial setup time.

There are three items to be configured for each alarm:

- The event priority – Up to 10 event



Alarms Management



Alarms Management

priorities can be defined; 8 of these can be assigned to alarms. Alarms can be escalated to higher priorities until they are processed.

- Alarm action plans – To specify the actions that are triggered by the alarm condition.
- Alarm instructions – To provide information and instructions to the operator when the alarm occurs.

Alarm processing is a two stage action. First, the alarm is acknowledged; the operator takes control. Second, it is processed; the cause has been resolved.

Designed for the modern control room, Command Centre's alarm viewers are custom designed to present all the information an operator needs to manage an alarm in one screen. Alarm viewers feature in-built screen designers that allow the installer to select the specific information an operator needs in order to determine the cause and action required for any alarm.

For example, access denied alarms can present selected information about the cardholder to whom access has been denied while a perimeter fence alarm may present only a site plan showing the

location of the alarm as well as video footage, stored or live, from nearby cameras. The information can be targeted to the type of alarm and filtered so that operators see exactly what they need to see and can make informed decisions.

Alarm viewers can include filtered event trails which allow an operator to see exactly what occurred prior to and after the alarm condition. Event trails can be filtered by a number of factors including the alarm source, the related cardholder or all items within the same site plan as the alarm source.

Command Centre also provides options to filter and segregate alarm lists into separate viewers, which can be based on attributes such as escalation status, alarm priority, or geographic location.

These options provide easier cross-coverage of operator workloads and can be used to ensure the most critical alarms, configured in viewers that pop to front on a new alarm occurrence, always retain high visibility. Alarm viewers fully support multi-monitor workstations, allowing differently filtered alarm viewers to be placed on different monitors.

The alarm list is a configurable list, allowing sites to choose the information an operator may want to view or sort by. For example, the operator can sort the alarm list by cardholder name to group together all alarms for the same person. Alternately, sorting by alarm zone or division can be used to group alarms in the list from the same physical location and which may have been triggered by the same event (e.g. an intruder).

Alarm summaries by priority both within the alarm viewer and on the status bar provide an operator with an always visible summary of alarms currently under their management. Alarm summary bars can also be used for quick navigation to the first alarm in the list of the selected priority.



Site Monitoring



Site Monitoring

SITE MONITORING

Gallagher Command Centre provides the ability to build tailored screen layouts bringing together the information and controls a guard needs in one place.

Monitor Site Viewers are extremely versatile and can be used in a number of ways, for example, providing a series of monitoring and control screen layouts, in a tabbed format, each targeted for a specific area of the site, whether that's a perimeter fence, a building, a floor, or even a single high security door. Screen layouts can integrate perimeter, access and intruder alarm information, via site plans, live camera feeds (requires an integration to the DVR/NVR system), status and override tiles, filtered event trails or guard tours. Each of the components can be mixed and matched and the content filtered to provide localised and targeted monitoring and control panels.

Alternately screen layouts can be designed to provide a graphical overview of the site, featuring a collection of site plans or a collection of live video feeds from selected cameras, tiled on screen. User interface design tools allow quick and easy layout of the screen and selection of the content, ensuring operators always have the information

they need at their fingertips. In-built tools to maximise an area of interest ensure viewers can be information rich and single screen with the ability to quickly see more detail when necessary.

SITE PLANS

Site plans show a graphical representation of the site and the real time status of remote field devices and logical entities. An unlimited number of site plans can be stored in the system and used within alarm viewers, monitor site viewers or challenge viewers. An operator can create site plans by importing map images of the site from a range of standard graphics.

Site Items are represented by icons and are placed on these images. The icons placed on the map image show the real time status of the site item, or the full status text for an item can be shown by hovering over its icon on a site plan.

Site plans include configurable elements, which can be associated with Gallagher system Items (macro override buttons and site plan navigation arrows, for example). Fence lines and buildings can be displayed with appropriate alarms, and semi-transparent alarm zone overlays. Site plans also feature touch screen

support and 'free text' objects. Alarm priorities are represented by different background colours for each icon.

Clicking on a site plan icon or clicking and dragging to select a group of items displays the available overrides. Common overrides are presented in the main context menu for quick selection.

It is critical that while operators are monitoring the site or performing other tasks in the system they are aware of alarms occurring. Alarm Viewers can be configured to pop to the front when a new alarm occurs or to trigger alarm sounds, ensuring that new alarms always capture the operator's immediate attention.

Navigation between multiple site plans can be managed easily from a single tile within a viewer, with simple browser-like navigation methods which are familiar to most people and hence easy to pick up.

INTRUDER ALARM MONITORING AND CONTROL

The Gallagher system integrates full intruder alarm functionality eliminating the need for a separate intruder alarm system. Intruder detection zones can be configured to report four different states: arm (set), disarm (unset), and two further



Cardholder Management

states with user definable names. Entry and exit delays can be defined for each zone. This gives cardholders time to enter and leave the site when changing the state of the alarm zone.

Alarm zone state changes can be:

- > Automated via schedules set up in Gallagher Command Centre
- > Initiated from workstations via operator overrides
- > Initiated via Gallagher Remote Arming Terminals
- > Initiated via Gallagher readers
- > Initiated via switch control

Authorised operators monitor alarms at Command Centre workstations. This can be complemented with:

- > Gallagher Remote Arming Terminals for alarms management in the field
- > Offsite alarm monitoring utilising Contact ID transmitted via Gallagher Controllers using a physical PSTN alarms dialler or IP alarms transmission over IP LAN/WAN or cellular network.

CARDHOLDER MANAGEMENT

Command Centre's Cardholder Management Viewers feature an in-built screen designer, allowing sites to design and layout the information an operator needs to search for cardholders and to

view and update their details. Viewers can be tailored for an operator's role, targeting the information displayed to the specific role the person performs, removing any information which is not relevant or useful and making best use of available screen real estate to present and manage all of a cardholder's details from one screen.

Cardholder Viewers can also provide a dynamic event trail for the cardholder, so an operator is able to see additional information about the person's recent activity and any recent changes made to their details or access.

Gallagher Command Centre provides extensive cardholder database features. Each cardholder record includes personal cardholder information and access information:

- > Unlimited personal data fields where personal data can be entered such as an Employee ID, a department, location, email address or mobile information, a photo or signature
- > Access groups to which the cardholder belongs - managing area and time access
- > Competencies (training, licenses, inductions, clearances or medical assessments) the person holds which

can be used to further modify the person's access

- > Detailed information about the card(s) held by the cardholder, for example, card number, facility code, technology type, issue level, and expiry date and time
- > Event and alarm notification filters which determine the notifications this person receives
- > The person's roles and relationships, used for determining who they receive card or competency expiry notifications for
- > Biometric template information for fingerprint identification.
- > Cardholder notes

Searching for cardholders by name is powerful yet straight forward and intuitive. The operator simply starts to type any part of the first or last name; when the third character is entered matching results are automatically returned from the server and are filtered as the operator continues to type. There is no need to know the correct spelling of a cardholder name, as any part of the first or last name, entered in either order will find the correct person. Alternate search fields, such as employee ID, student ID or department, are configurable and are also used to define the search results, allowing operators to quickly and easily pinpoint the person required.



Cardholder Management

As an alternative to standard searches, smartcard technologies (Mifare Classic, Mifare Plus and DESFire) support finding cardholders in the system by presenting the person's card at a Mifare USB encoder connected to the workstation.

Advanced searches provide the greatest flexibility and allow an operator to retrieve a group of cardholders by building multi-statement search criteria, linked by AND/OR. For example, advanced searches can be used to find people in a specific division who have an active and enabled card but have not requested access in the last three months.

Cardholders returned in a search can be viewed on screen or the results can be copied and pasted to Microsoft Excel, providing a simple but immediate reporting option.

Cardholders can use the same cards/fingerprints/PINs across all sites within a Multi-Server network (e.g. a person with appropriate access rights can travel between sites controlled by separate Gallagher Servers, using one card for entry).

Universal Card Formats enable multiple third party Wiegand formats of up to 360 bit to be supported concurrently in the

Gallagher system. Subject to System Division and operator privileges, an operator can create, delete and change cardholder records in the system. Any changes made are recorded as events.

The Gallagher security system provides an easily accessible audit trail of changes made to a cardholder including, what change was made and when it was made, the operator who made the change and the workstation from which the change was made.

The system automatically downloads any changes made to the cardholder record to the relevant field devices. Cardholder data can be shared with third party applications via the XML Interface, or imported via the Enterprise Data Import Interface.

PERSONAL DATA MANAGEMENT

Personal data fields (PDFs) hold the relevant personal data required for a cardholder, for example, the department in which they work or to whom they report.

Personal data fields are created as separate entities and are attached to access groups. Cardholders inherit the personal data fields from the access groups to which they belong.

Personal data fields can be configured to be unique, mandatory, numeric, text, date, text lists or specifically for email, phone or address contact details.

Gallagher Command Centre has a fully integrated photo identification system (Gallagher PhotoID). A personal data field can also contain an image which can then be used for PhotoID and cardholder Challenge.

Each cardholder record can have unlimited personal data field definitions. It is possible to restrict the Personal Data Fields an operator can see and change through their operator privileges and through the selection options within the cardholder viewer.

The Cardholder bulk change feature enables an Operator to make changes to multiple cardholders simultaneously.

ACCESS

Access Groups

Access groups make it possible to define access for groups of cardholders who share the same requirements.

Each access group is named and includes the following information.

- Access – where and when members of the group have access



Alarm Management - Access Denied

- > Members – a list of cardholders who belong to the access group
- > Personal Data Fields – a collection of personal data field definitions attached to individual members
- > Escort – whether the members are allowed to act as escorts for visitors
- > Arm/Disarm alarm zones (areas) – member authorisation to arm and disarm certain alarms
- > Whether members can change the state of the access zones.

Access groups are displayed as a tree with branches having more specific access. A cardholder may belong to one or more access groups to get their full access privileges. For example, there may be an “All Cardholders” group to which all cardholders belong for commonly required access through the entrance and cafeteria. A cardholder acquires additional specific access by joining other groups, for example, “Head Office Managers’ Group”. Information on cardholders’ access groups can be viewed and altered from the cardholder viewer.

Access is defined through access zones and time schedules. Access groups are an efficient cardholder management tool. Access groups also enable bulk

changes to be easily applied to members for the group. Any changes to Access or Personal Data Field properties will automatically apply to all members of the group.

When allocating the required access groups to a cardholder, an operator can use any of the context-sensitive options; searching for the groups by name, by division, by stepping through the access group hierarchy or by selecting their most recent assignment.

Competency Based Access

Access can be based on an individual's competencies, e.g.:

- > Safety (induction, training, licences)
- > Security (clearances)
- > Regulatory Compliance (OH&S policy)

Validity periods and competency expiry can also be factored into the access decision.

Competency based access management delivers:

- > Automatic enforcement of business OH&S rules and policies
- > Reduction of production stoppages due to non-compliant staff being in the wrong areas
- > Tangible evidence of ‘duty of care’ to staff and customers

- > Automatic compliance with government regulations

Controller based decisions based on an individual's competency are delivered via screen feedback on the door reader or display monitor. Once configured, all of this is achieved independent of Server and IT Network connectivity.

Schedules

Gallagher Command Centre enables a site to automate state changes according to a pre-configured schedule, scheduling for example: when a cardholder has access to an access zone, when a zone is secure, when alarms will be automatically armed (set) and disarmed (unset).

The schedule can vary based on the type of day, for example a weekday or a holiday, as well as the time of day. Schedules are highly configurable. A navigable calendar-based view of each schedule enables a system operator to quickly review schedule changes over the coming week or at any future date.

PERSONALISED ACTIONS

Personalised Actions are individually programmed responses which can be configured for individual cardholders or for all cardholders of an access group.



Challenge

The programmed responses – either an output or the running of a macro - are initiated on the cardholder's 'access granted' or 'access granted and taken' event.

There is a wide variety of applications. For example:

- > Switch on lighting or, through a high level interface, trigger lighting or air conditioning managed by a Building Management System for specified access zone(s)
- > On badging a centralized card reader, unlock the cardholder's locker while leaving all other lockers secure.

Up to 250 individual cardholders or access groups can be defined with Personalised Actions for each access zone.

All authentication methods that identify the cardholder entering the access zone are supported including for example, PIN-only access events and access events from third party systems which have been integrated using the Gallagher Controller Application Programming Interface.

REPORTS

A comprehensive range of report templates is available to view and print information held in the system, including four primary report types :

- > Activity Report
- > Cardholder Report – detailed or summary
- > Evacuation Report
- > Exception Report.

The primary reports can be automatically generated on a repeating schedule, for example, automatically generate a weekend activity report at 8am every Monday morning. They can also be scheduled to be generated on specific dates and times in the future.

Where the optional Notifications feature has been deployed these scheduled primary reports can also be automatically emailed to the people who require them, effectively eliminating the manual overhead of generating and emailing reports to the intended recipients.

Other report templates which can be generated from Operator workstations as required include:

- > Access and Access Groups Report
- > ContactID Assignment Report
- > Electric Fence Voltage Report
- > Site Configuration Report
- > Time and Attendance Report
- > Wiring Report

GALLAGHER CHALLENGE

The Gallagher Challenge feature provides the ability to double-check the identity of cardholders passing through a

nominated door via visual comparison of a cardholder image against a live or video image.

This feature is fully integrated with DVR systems and features an in-built screen designer allowing sites to select the specific information to be displayed to the challenge operator. Refer to the Challenge feature datasheet for more information.

USER CONFIGURABLE VIEWERS

For operators managing the day to day security and access to a site, Command Centre introduces new levels of configurability of the user interface. From alarm management to general site monitoring and control; from cardholder administration to challenge; screen layouts can be designed or adapted in minutes with full support provided for multi-monitor workstations.

The in-built screen designer allows the creation of viewers. Viewers ensure the security team sees exactly what you need them to see, with the information sized and placed exactly where you want it.

Viewers are designed to be full screen and contain a navigation area which is customized for the purpose of the viewer (for example, the navigation area is an alarm list within the Alarm Viewer).



Viewer Configuration

Each operator may see multiple viewers or only one viewer in the viewer toolbar, based on their privileges and their particular role and needs. Operators can drag and drop viewers within the toolbar, ensuring these are arranged in an order that makes sense to them.

A panel displays for the item selected in the navigation area and uses the remainder of the screen real estate to display information related to the selected item.

- > Alarm viewers display a list of alarms in the navigation area, the detailed information related to the selected alarm in the panel, and this is all visible in one screen.
- > Cardholder viewers display the cardholders returned in a search in the navigation area, and the specific information for the selected cardholder in the panel, complete with the tools required for cardholder updates.
- > Controlled Challenge viewers display current challenge events in the navigation area, the detailed information related to the selected challenge event in the panel, and this is all visible in one screen.
- > Monitor Site viewers display a list of pre-designed panels (i.e. screen layouts) in the navigation area, as well as the detailed information for the currently selected panel, all visible in one screen.

When an operator selects an item from the viewer navigation area, the configured panel is displayed. Panels consist of tiles and each tile has information or tools related to the item the operator has selected. For example,

- > Within an alarm viewer, a selected alarm displays the panel of information and control options for that alarm. This may consist of tiles displaying, as an example, the related site plan, the alarm instructions, or the video footage for the alarm, all visible in one screen.
- > Within a cardholder viewer, a selected cardholder displays the panel of cardholder information for that person. This may consist of tiles displaying, as an example, the cards, access groups, competencies, personal details and cardholder image, all visible in one screen.

Command Centre's viewers aim to present all the relevant information and controls the operator needs to complete a task in one screen. In some cases, more detail or more screen real estate is needed, and this is supported with single-click animations to maximise a tile, for example maximising a site plan, a video image or a filtered event trail within the panel. Other tiles are minimised, remaining visible in a filmstrip layout on the right hand side of the panel and can still be selected with a single click on the icon.

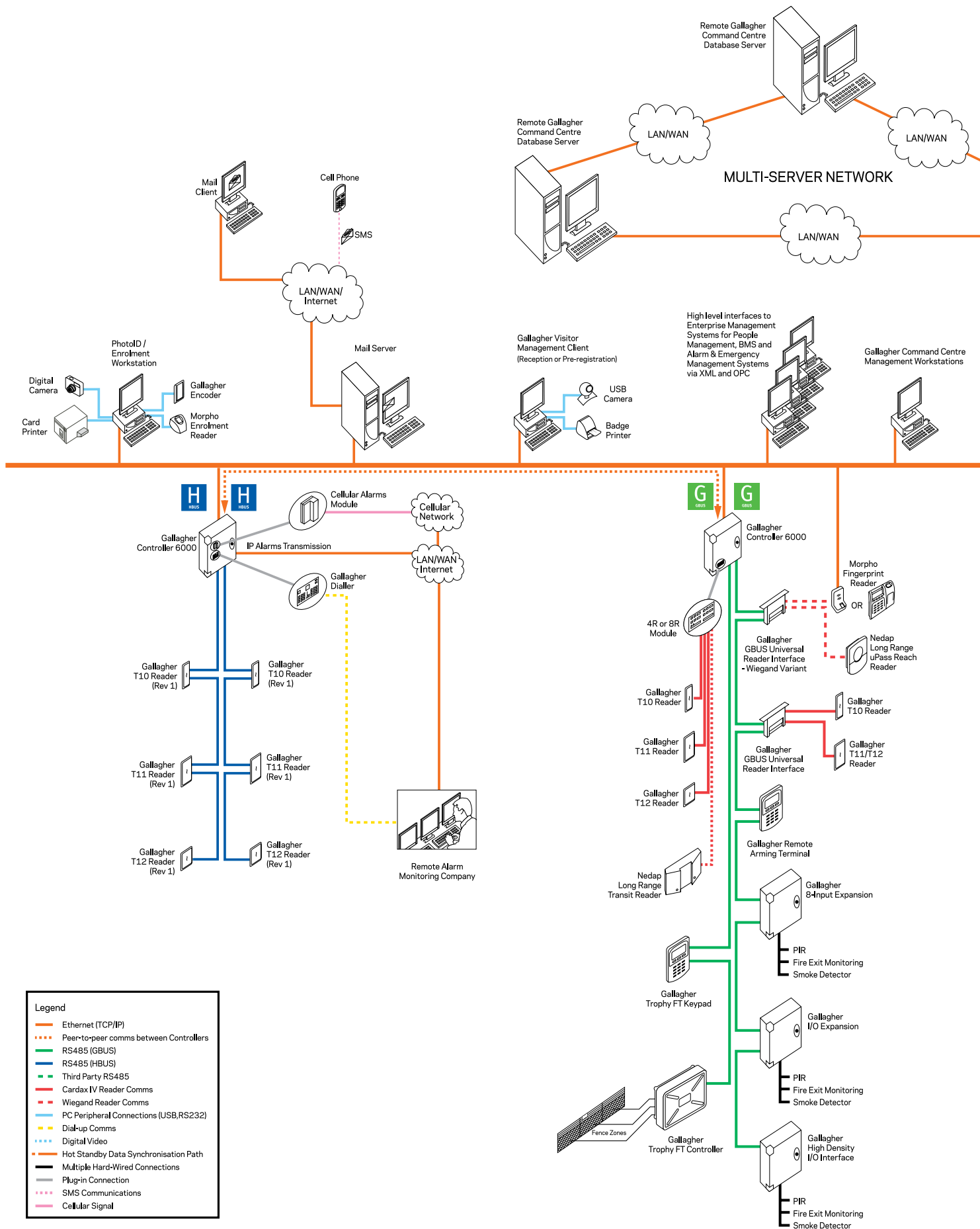
Alternately, an operator can return to the standard or pre-configured panel layout by clicking on the title bar of the maximised tile. With these tools, detailed information is never more than a click away.

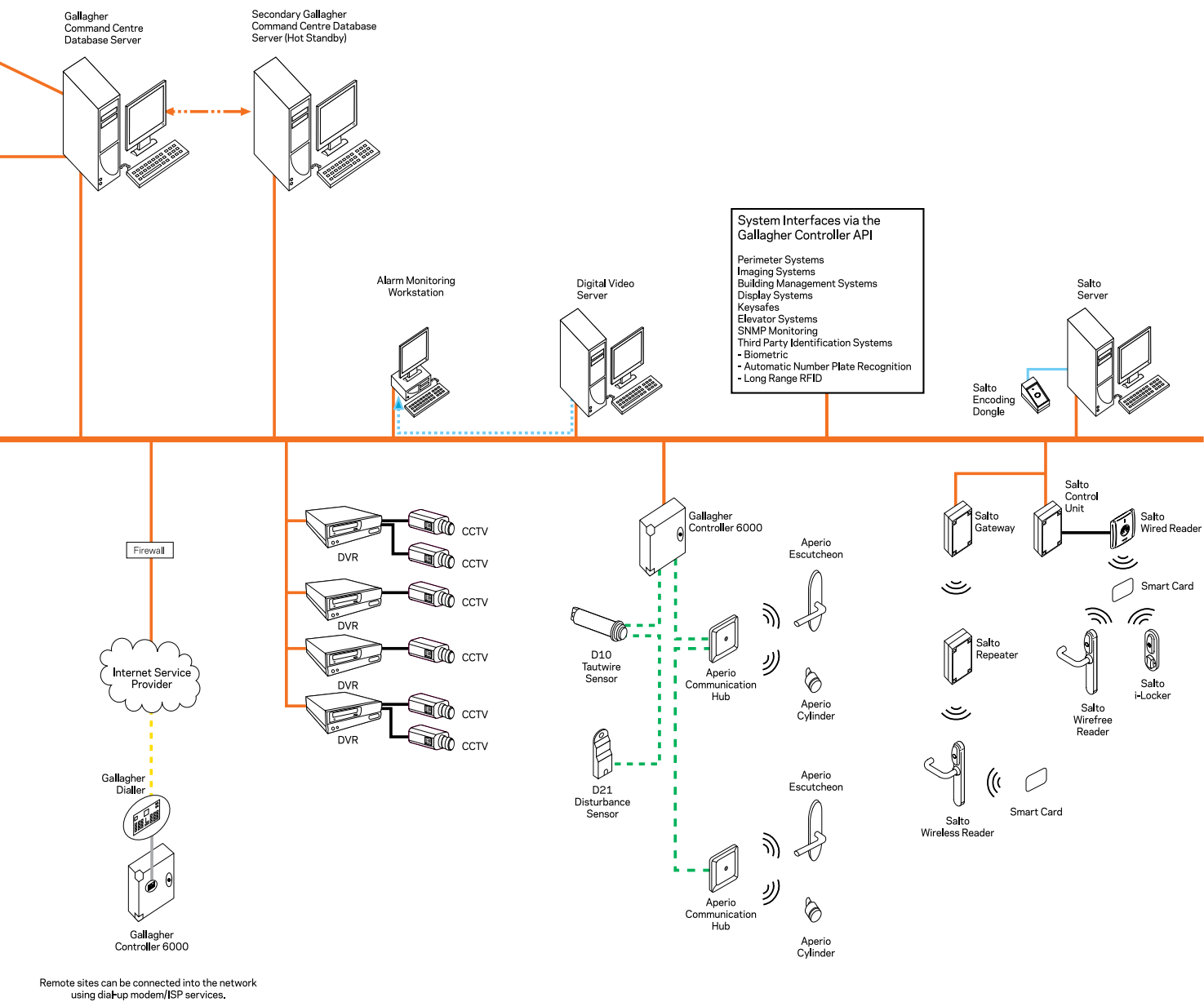
DIGITAL INTERCOM

When a person at the Gallagher Intelligent Door Terminal presses the F3 button on the reader, the operator can use the Integrated Digital Intercom functionality to speak / listen to the person.

SITE LOCKDOWN

Access zones can be configured to enter either partial or full site lockdown during threat or emergency situations. Site lockdown ensures that only selected cardholders (identified via their access group) can enter or exit a zone/s.





The platform for integration

Gallagher Command Centre

The platform for integration

Gallagher Server and Controller Application Programming Interfaces extend the functionality and flexibility of the Gallagher system as the platform for integration.

Gallagher has been designed to readily interface to third party applications. Because this is an ever-changing environment, contact Gallagher Technical Support for the latest information.

XML INTERFACE

Gallagher Cardholder Import and Export provides the ability for cardholder data to be imported from external sources to Gallagher Command Centre using standard software functionality known as XML Interface. Typical sources of data include a student enrolment database, or a company's HR database from a system such as SAP®.

GALLAGHER SCHEDULE IMPORT (XML)

Third party room booking Schedules that are to be reflected in security schedules can also be imported into Gallagher Command Centre using XML Interface.

ENTERPRISE DATA IMPORT INTERFACE

The Enterprise Data Import Interface tool allows configuration and synchronisation of Cardholder data with external enterprise systems. Data maintained in a

primary database (e.g. Human Resources database) can be automatically reflected in the Gallagher database on an ongoing basis, in order to maintain data integrity and reflect business approved changes to Cardholder information and access rights.

The Enterprise Data Import Interface tool also allows sites migrating from an obsolete security system to migrate existing Cardholder details from the legacy system over to the Gallagher system.

GALLAGHER DVR INTERFACE

The Gallagher DVR Interface feature provides the ability to connect to third party DVR (or NVR) systems and provides integration of routine operations for an integrated colour DVR and alarms management solution.

GALLAGHER INTERCOM HIGH LEVEL INTERFACE

The Gallagher Intercom High Level Interface (HLI) feature enables digital intercom systems to be integrated into the Gallagher system.

Using Gallagher Command Centre, the operator can control call connectivity for the TCP/IP Intercom system. Events are logged into the Gallagher database.

OPC (OLE FOR PROCESS CONTROL) INTERFACE

Gallagher Command Centre is OPC enabled, allowing alarms and event data to be interfaced to other OPC enabled applications.

OPC eliminates the need for costly custom software integration, giving customers the freedom to choose a solution based on an open industry standard. Further information can be found at www.opcfoundation.org.

OPC Alarms and Events API

Gallagher Command Centre Server supports the OPC Alarms and Events protocol. This allows external systems (OPC Client) to acknowledge and process alarms and to add comments. It also allows external systems to request extra 'attributes' that a server may make available.

OPC Data Access API - Status and Overrides

Gallagher Command Centre allows Status and Overrides to be shared with third party systems.

An OPC enabled system can also control the state of selected Gallagher Items directly from a third party system by invoking overrides and can report the

Integration delivers cost and time efficiencies, improves data integrity and can help meet your occupational safety and health obligations.

state of selected Gallagher items directly in the third party system.

GALLAGHER ELEVATOR HIGH LEVEL INTERFACE

The Gallagher Elevator High Level Interface (HLI) feature provides the ability for Gallagher to control access to floors from elevator cars.

For more information about each of these features please refer to the Gallagher Feature Information datasheets available from www.gallagher.co.

PROFESSIONAL SERVICES

Gallagher provides a platform for integration. For the development of interfaces to specific third party systems or the development of customized system behaviour, please contact us for more information about our Professional Services.



Monitor Site - Video Wall

Gallagher Command Centre

Optional Features

GALLAGHER TROPHY FT INTEGRATION

The Gallagher Trophy FT Integration is an optional, fully integrated application available for Gallagher Command Centre. It enables the full configuration, control and monitoring of the perimeter system through Gallagher Command Centre.

GALLAGHER PHOTO ID AND ENCODING

Gallagher PhotoID and Encoding is an optional licensed feature available for Gallagher Command Centre. Gallagher PhotoID and Encoding provides the ability to design, produce and encode photo identification cards for cardholders.

Encoding of Gallagher Mifare Classic, Mifare Plus, Mifare DESFire EV1 and Magstripe cards is supported.

The Card Encoding Wizard is specifically designed for efficient card enrolment, printing, and encoding.

GALLAGHER NOTIFICATIONS

Gallagher Notifications is an optional feature which provides the ability to send messages to cardholders via email or SMS (text message) about selected events and alarms the cardholder needs to be informed about, and/or the imminent expiry of a cardholder's Card or Competencies. A very flexible feature, Notifications can also be utilized to email scheduled reports.

GALLAGHER GUARD TOURS

Gallagher Guard Tours is an optional feature which enables the configuration,

live operation and reporting of Guard Tours implemented on site through monitoring the guard's arrival at designated checkpoints in a prescribed order and within specified times. Guard tours can be monitored and controlled from alarm viewers or monitor site viewers.

ENTERPRISE DATA IMPORT INTERFACE

The Gallagher Enterprise Data Import interface is an optional application available for Gallagher Command Centre. Refer to page 12 for further information.

GALLAGHER VISITOR MANAGEMENT

Gallagher Visitor Management is an optional licensed feature for Gallagher Command Centre. Visitor Management delivers extensive visitor pre-registration and Reception functions.

Gallagher Visitor Management employs a client-server architecture for the Gallagher system, allowing the Gallagher Server to communicate with visitor management 'smart' clients via network services over TCP/IP.

GALLAGHER MORPHO FINGERPRINT READER INTEGRATION

The Gallagher Morpho Fingerprint reader integration is an optional integration application available for Gallagher Command Centre. Integration between the Gallagher system and Morpho

MONITOR SITE - PERIMETER FENCE WITH VIDEO



Extend the Gallagher system with the following optional features to meet specific site requirements

biometric fingerprint readers enables seamless fingerprint enrolment and template management within Gallagher Command Centre. Identification (finger only) and verification (fingerprint template stored on a smartcard) are available.

GALLAGHER DATA ON CARD AND WIRELESS DOORS

The Gallagher data on card and wireless doors integration is an optional integration available between Gallagher Command Centre and Salto wire free and wireless reader technologies. It allows Gallagher sites to further leverage their investment in Mifare Classic SmartCard technology for doors which do not require real-time, monitored access control.

APERIO INTEGRATION

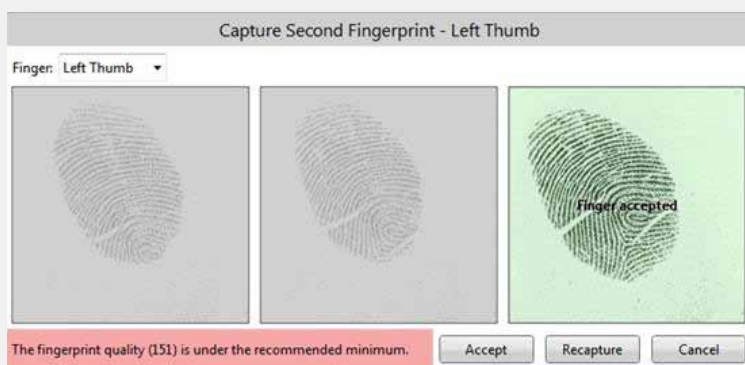
The Gallagher Aperio wire free reader integration is an optional integration available for Gallagher Command Centre. The Aperio integration extends the standard access control capabilities of the Gallagher system to online, unwired Aperio doors, delivering functionality not achievable with mechanical keys.

APPLICATION PROGRAMMING INTERFACES

Gallagher Server and Controller Application Programming Interfaces extend the functionality and flexibility of the Gallagher system as the platform for integration.

For more information about each of these features please refer to the Gallagher Optional Feature datasheets available from www.gallagher.co.

GALLAGHER MORPHO INTEGRATION - BIOMETRIC FINGERPRINT ENROLMENT



Technical Specifications

GALLAGHER COMMAND CENTRE

OCTOBER 2011

Recommended Computer Specifications	A number of variables e.g. event rate, will affect the recommended computer hardware specifications. Please discuss your requirements with Gallagher Technical Support.	
Operating System	Server	Windows 7 Professional/Ultimate* Microsoft Windows 2003 SP2 or 2008 SP2, 2008 Server R2 (64 bit only)
	Workstation	Windows 7 Professional/Ultimate*, Windows XP Professional**
Database Platform	Microsoft® SQL Server 2005 SP2, 2005 Express SP2, 2008 SP1, 2008 R2, or 2008 Express SP1	
Configured Workstations	Maximum Number	Unlimited
Operator Authorisation Level	Fully configurable for each operator	
Configured Operators	Max. number of configured operators	Unlimited
Gallagher Hardware	Gallagher Controllers (6000, 3000 & 5000GL)	Unlimited
	Field Devices	See Controller data sheets
Number of Cardholders	Command Centre	Unlimited*
Event Database	Command Centre	Unlimited*
Card Issue Levels		15
Maximum Access Controlled Doors		Unlimited
Access Control Zones	Max. number of access controlled zones	Unlimited
Controlled Outputs	Max. number of relays	Unlimited
Alarm Inputs	Max. number of inputs	Unlimited
Elevator Control - Low level	Maximum of 2 elevator cars (each with up to 75 levels) per Gallagher Controller Gallagher Technical Support recommends using the Gallagher Controller 6000 architecture for low level elevator control.	
Elevator Control - High Level	Refer to Gallagher Technical Support to determine the number of Gallagher Controllers required for the system.	

System configuration, network capacities and the volume of system activity affect performance.

Please contact Gallagher for advice.

* Maximum number dependant on relevant SQL database limits

* 32 and 64 bit versions are supported

** Conditions apply. Contact your Gallagher Channel Partner for more information.

GALLAGHER WORLD HEADQUARTERS

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

TEL: +64 7 838 9800

EMAIL: sales@security.gallagher.co

REGIONAL OFFICES

New Zealand.....+64 7 838 9800
Americas.....+1 888 430 0770
Asia.....+852 2910 7912
Australia.....+61 2 9412 4477
India.....+91 80 2661 1590
Middle East.....+9615 808728
South Africa.....+27 11 974 4740
United Kingdom / Europe.....+44 2476 64 1234

Disclaimer: System configuration, network capacities and the volume of system activity affect performance. Please contact Gallagher for advice. In accordance with the Gallagher policy of continuing development, design and specifications are subject to change without notice. Gallagher Group Limited is an ISO 9001:2008 Certified Supplier. Copyright © Gallagher Group Limited 2011. All rights reserved.

