Gallagher Command Centre

Multi-Server User Guide

Version: 9 .50
Date: May 2026

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 Limited 2026. All rights reserved.

Gallagher Group Limited
Private Bag 3026
Hamilton
New Zealand
+64 (7) 838 9800
Internet E-Mail: security@gallagher.com
Website: http://www.gallagher.com

Table of Contents

Definitions **5**

Multi-Server Overview **6**

Supported Systems **9**

Multi-Server Setup **10**
- Architecture 11
- Licensing 12

Command Centre General **13**
- Change History 14
- Find Tool 15
- Operators 16
- Reporting 17
- Cardholder Location Data 18
- Remote Items 19
- Functionality across multi-server systems 23
- Limitations of multi-server systems 24
- Exceptions 25

Access Control and Multi-Server **26**

Alarms and Events **27**

Multi-Server Communications **31**
- Connectivity 32
- Site Autonomy 33
- Trusting Servers 34
- Time Clock Synchronisation 35
- Workstation and Controller Communications 36
- Communications Security 37
- Network disconnection and/or remote server off-line 39

Multi-Server Installation **40**
- Install 41
- Upgrade 42
- Example: Setting up a Multi-Server System 43
- Remote Server Status 46
- Initialising communications and replication 50
- Splitting Existing Server 51
- Merging Servers 52
- Divisions 53
- Contact ID local to a server 54
- Restoring a Server From Backup 55
- Globally unique logon name 56

Administration **57**
- Backups and Archives 58
- Replacing a Server 59
- Applying Custom Certificates 60

Third Party products in a Multi-Server environment **61**

Conflict Resolution 66
Conflict - Default Behaviour 68
Conflict - Concurrent Updates 69
Conflict - Dependency on Unknown Item 70
Conflict - Dependency on Deleted Item 72
Conflict - Duplicate Card Numbers 74
Conflict - Duplicate User Codes 75
Conflict - Duplicate Operator Logon Name 76
Conflict - Duplicate Value in Unique Personal Data Field 77
Conflict - Value Invalid According to Configuration 78
Conflict - Controller Capacity Exceeded 79
Conflict - Licence Limit Exceeded 81
Conflict - Item Locked for Editing 82

Index **83**

Definitions

Local A relative term that describes the server an item is connected to. When discussing a particular Gallagher multi-server system this term refers to the one server to which your workstation is directly connected or which your hardware is connected to and configured on.

With reference to a particular server, Local Configuration refers to the items that belong to Divisions on that server. With reference to that server, these items are referred to as Local Items and the server is referred to as the "home server".

With the exception of Cardholders, Local Items are only editable from workstation connected to their home server. Some Local Items can be viewed from other servers (where they will be known as Remote Items).

Remote A relative term that describes the server an item is connected to. Every server in a Gallagher multi-server system is a remote server other than your local server.

With reference to a particular server, a Remote Item refers to an item that belongs to a Division on a different server, known as the item's "home server".

With the exception of Cardholders and Access Groups, Remote Items are only editable from workstations connected to their home server. Some Remote Items can be viewed from servers other than their home server.

Global A global item describes a Command Centre item that is the same on all servers. It can edited on any server in a multi-server system.

Server * A single installation of the Command Centre server application.

Site * A location where a Command Centre server application has been installed.

* *The terms server and site are used interchangeably in this document.*

Multi-Server Overview

Key Functionality

- Global cardholder configuration and replication.
- Event and alarm management between sites.
- Status transfer between sites.
- Overrides on remote items.
- Reporting on data from multiple sites (Evacuation report only).
- Allow servers to operate independently.
- Efficient use of the network.
- Increased reliability – sites can continue to operate if a server at another site, or the network, goes down.
- Improved performance – load is distributed amongst the servers, and workstations don't need to run across a WAN.

General Approach

Each server maintains a copy of the entire configuration needed by its clients. The copy is kept up to date by subscribing for relevant configuration changes from the other servers in the system. Having a local copy of the entire necessary configuration allows each server to continue to operate with full functionality while the rest of the system is unavailable.

Local Items and Global Items

A multi-server system's configuration can be divided into local and global components. Local configuration belongs to a particular server (the "home server") and is only editable when connected to that server, although some local configuration is viewable at other servers. Local items cannot be moved to other servers or assigned to divisions on other servers. Global items (initially just cardholders) do not belong to a particular server and can be edited while connected to any server and assigned to divisions on any server.

Each server maintains a copy of its entire local configuration as well as all global configuration. Servers also maintain some information about other servers' local configuration - just enough to allow for remote monitoring, (e.g. Icon Sets) and to provide support for global items, (e.g. Card Type facility codes). This means that clients connected to a server will not be able to see the full configuration of local items from other servers - for most items only the **General**, **Status and Overrides** and **Notes** property pages are shown.

Proxy Command Centre Items

A server's local items will be represented by a proxy Command Centre item at other servers. These Command Centre items provide a subset of the normal functionality of the Command Centre item. For most items this will only include the following:

- Viewing basic configuration, (e.g. name and description)
- Viewing status
- Performing overrides
- Viewing alarms and events

Replication

When a client modifies configuration that may be relevant to other servers, the local server sends the change to each of the other servers. This is not complicated in principle but a number of guarantees are required to ensure that servers maintain a consistent view of the system's configuration:

Changes made get to every server by adding each change to the database as part of the transaction that applies the original configuration change. Other servers then retrieve each change from this list in order, only moving on to the next change after the previous change has been stored in its own database.

A full list of conflicts and how they are resolved can be found in the conflict resolution section.

Resynchronising Servers

The rules described previously ensure that server consistency is maintained unless something exceptional happens, (e.g. a server is restored from backup). If servers do get out of sync for any reason then a resync mechanism is provided to sort out the inconsistencies. Resyncs are initiated by selecting a source server (one that is up-to-date). The source server then sends the global configuration and the local configuration to the operator's server in a series of messages.

Gallagher multi-server minimises any increase in network traffic due to resynchronising servers by sending only the data that has changed since the previous resync. The resync operation will run as a low-priority background task.

System performance

Overall performance of a Gallagher Multi-Server system should be better than an equivalent single server Command Centre system because each server is only responsible for part of the system.

Load partitioning

Gallagher Multi-Server makes use of load partitioning to eliminate unnecessary traffic between sites which enables it to operate effectively over a WAN connection. Load partitioning also improves overall reliability by enabling all sites to continue operating in isolation if necessary. This has been implemented by:

- Sharing full details across all servers of only certain key item types, such as cardholders.
- Sharing a subset of data for other specific site items so that overrides can be performed on them from other servers.
- Maintaining hardware configuration at local servers only.

Multiple servers on one site

In general we do not recommend having multiple servers on a single site as this will limit functionality and will duplicate a large amount of configuration.

Supported Systems

Supported Operating Systems for Gallagher Server

Supported Microsoft Operating systems will be the same for Multi-Server systems as it is for single server systems.

Supported Database Systems

Supported SQL database versions are the same for multi-server systems as it is for single server systems.

Note: If SQL Server Express is used on any server then the total database size for the Command Centre central database on every server is limited to the maximum database size for SQL Server Express (4Gb).

Running different operating systems and database versions

It is possible for the multi-server system to comprise of servers running different operating systems and different databases, as long as the database and OS are supported by this version of Command Centre.

Running different Gallagher Server versions

For version vEL6.01 all servers need to be on the exactly the same version and build of Command Centre.

From version vEL6.02 and above if any of the servers are not running exactly the same version and build then an alarm is generated and configuration changes are not transferred between the servers. Other cross-server functionality such as alarm management, status, overrides and Evacuation Reports are still available if the servers are running different software versions.

Note: An upgrade of your servers may fail if they are on different versions of Command Centre, due to incorrect certficates. If this occurs, perform an 'Accept Certificate' override on all servers and restart the services so the multi-servers come online.

Multi-Server Setup

In this section:

- ***Architecture*** (on page 11)
- ***Licensing*** (on page 12)

Architecture

- Controllers and workstations connect to a single server.
- Servers connect directly to each other.
- Inter-server communication uses a single port.
- Confidentiality (encryption) and server authentication is based on per-server private keys and certificates.
- Cardholders are replicated to all servers.
- Other configuration is only partly replicated.
- Replication conflicts are resolved automatically where possible and/or an alarm is raised.
- Status, events and alarms are forwarded from the source server to workstations via the workstation's server.
- Overrides and alarm acknowledgements are forwarded to the source server via the workstation's server.
- Each server in a multi-server system will have its own system operator account which should always be disabled in a production environment (Note: All servers in a multi-server system are considered as a single system with no trust boundary between the individual servers).

Servers off-line for extended periods

Gallagher Multi-Server is optimised for systems which aim to have all servers on-line at all times. If your WAN is not up and running for an extended period then changes may take a long time to replicate and data conflicts are much more likely.

Workstation connection

In a Gallagher Multi-Server system, workstations only connect to local servers (via a LAN) to access remote server information (assuming the operator is suitably privileged). It is strongly recommended that this is done rather than connecting directly to remote servers over a WAN because performance is significantly better. If direct connection of a workstation to a remote server is vital (i.e. because the local server is down) then Terminal Server or other thin client should be used.

Licensing

Licensing Multi-Server

1. Multi-server functionality is provided as a licensed feature. A server will not be able to participate in a multi-server system if its Licence File does not have multi-server enabled.
2. Licensing is used to control which multi-server system, (i.e. which other servers) a server can be connected to. A server will not be allowed to be connected to another server unless the licence files of both servers dictate that they can communicate to each other.
3. Each server in the multi-server environment will have its own licence file. This means that licence limits will only be applied locally on each server. The system will prevent two servers in a multi-server system from running with the same server's licence file.
4. License restrictions for Command Centre Items only apply to the local items on the server to which the licence file applies. Remote Items are not counted when determining how many instances of a Command Centre Item exist for the purpose of licensing.
5. It is possible for different servers in a multi-server set up to have different license options and customisations.

License File Contents

[Site]	
Name=Cardax Demo	
SerialNumber=10001	Unique
MultiServerSerialNumber=12345	This value should be the same for all servers in a multi-server environment
OriginalSerialNumber=90021	Used when splitting a site into a multi-server environment
Version=6.01	Must be 6.01 or later
[Features]	
MultiServer=1	

Command Centre General

In this section:

- ***Change History*** (on page 14)
- ***Find Tool*** (on page 15)
- ***Operators*** (on page 16)
- ***Reporting*** (on page 17)
- ***Cardholder Location Data*** (on page 18)
- ***Remote items*** (on page 19)
- ***Functionality across multi-server systems*** (on page 23)
- ***Limitations of multi-server systems*** (on page 24)
- ***Exceptions*** (on page 25)

Change History

Each server in the multi-server system maintains a change history of its local configuration. The change history only contains changes that other servers in the system will need to know about. It includes information such as:

1. What the change was, (e.g. name was changed to "Bob").
2. When the change was made.
3. Who made the change, (i.e. the operator).
4. Where the change was made, (i.e. the workstation).

For Cardholders this information will be available on the **History** tab.

Find Tool

1. In the Find Tool, a operator is able to search for all servers, by selecting a "Servers" option in the **Look In** drop-down.
2. Both local and remote items are displayed in the results of the Find Tool. All local and remote Command Centre items can be found by searching the type of the item they represent.
3. Operators can drag any global or remote item they can see into the **Related To** tab of the Find Tool.

Operators

1. Password restrictions apply from the server where the password is being created or modified. This means that an operator may be able to log onto a workstation where the format of their password does not match the local server's password restrictions.
2. The Allow maximum of one login per logon name Operator Restriction setting is applied on a per server basis, (i.e. if this setting is set to **YES** on a local server, it does not prevent the operator from being logged onto another remote server at the same time).
3. Operator Preferences are specific to individual servers, (i.e. an operator has a different set of preferences for each server in the multi-server system).
4. All System Operators in a multi-server system have full privileges on all servers.

Reporting

When generating reports on a server, only data available at that server is used. As most data used in reporting is not replicated across servers, each server is only able to generate reports containing information relating to Command Centre Items that belong to that server.
Since cardholders are shared globally across a multi-server system this means that the Cardholder Report is global. Although technically the records are still only coming from the local server therefore it may be that recent cardholder changes made on a remote server may not be reported if they have not yet been transferred.

The only exception is for evacuation reporting. This data is replicated to servers that have been configured as aggregation servers and allows operators to run an Evacuation Report for Access Zones associated with a remote server. The report covers all Cardholders in the entire system for all selected local or remote Access Zones. Each server is able to be configured as an aggregation server so it receives cardholder location updates. Appropriate server selections must be made to ensure that in the case of a server being destroyed there is at least one other with the relevant cardholder location information.

Cardholder Location Data

Cardholder location status updates have the potential to have the largest impact on network traffic and database growth. The Gallagher Multi-Server System uses data aggregation to minimise this impact

Cardholder Location data is copied to other servers when they are configured as aggregation servers so that it is possible to run Evacuation Reports from the aggregation server. This allows for the production of an accurate and current Evacuation Report listing all cardholders to be evacuated.

It is possible to change an aggregation server to a non-aggregation server. Whenever this happens an appropriate warning message will be displayed advising that turning off the aggregation setting could cause inaccuracies in the evacuation reports run on that server.

Scenario for displaying cardholder location data:

1. The first time a cardholder badges at a server, cardholder location data is sent to all other servers. Subsequent badges are not sent to other servers (unless they are aggregation servers).
2. If you open a cardholders properties window:
   a) If the last location is at the local server, the location will be correct and updated in real time.
   b) If the last location is at a remote server, the location from 1 above will be displayed. The remote server will then be queried for the current location and will then be updated in real time.
3. If the cardholder is in the Status Viewer, its last location is updated in real time.
4. If the workstation is on an aggregation server, the cardholder location data is updated for cardholders that are on servers that this server is an aggregation server for in real time.

Remote Items

Viewing Remote Items

1. As a general rule remote items are not visible in local Master List Windows. However, there are a number of exceptions to this rule detailed below.
2. The visibility of a remote item is not affected when the items home server is offline. For example, if the remote item were visible before the server was offline then it will still be visible if the remote server is offline.
3. A remote Command Centre item is displayed using the Icon Set defined on that items home server.
4. Local and Remote Command Centre Items of the same Command Centre Item Type will be distinguishable by the server field on the general tab of each remote item
5. Any remote item that belongs to a hierarchy and is displayed in a Master List Window is displayed showing its full hierarchy. For example Access Groups, Divisions, and Site Plans
6. The following remote Items are visible in the local Master List Windows
   a) Remote Access Groups *
   b) Remote Card Types
   c) Remote Divisions
   d) Remote Macros
   e) Remote Operator Groups
   f) Remote Personal Data Fields (Note: Personal Data Fields should have unique names across servers.)
   g) Remote Servers
   h) Remote Site Plans
   i) Remote Workstations

   * Some access group properties are editable remotely. Local access can be assigned to remote access groups in the same way as for local access groups. Any access assigned on other servers are visible but cannot be modified.
7. Any other items not listed above are not visible in the local Master List Window. For example:
   a) Remote Access Zones
   b) Remote Alarm Instructions
   c) Remote Alarm Zones

d) Remote Doors
e) Remote Elevator Cars
f) Remote External Systems
g) Remote Hardware
h) Remote Insertion Tags
i) Remote Interlock Groups
j) Remote Operator Privileges
k) Remote Salto items

To be able to view remote items in remaining Master List Windows that support the display of remote items (typically grids), it can optionally be enabled in the registry as follows:

Key	Type	Values	Where	Purpose
ShowAllRemote	DWORD	0 (disabled) 1 (enabled)	Client	**v6.0+** If set to 1 then items from remote servers will be shown in Master List Windows that support the display of remote items (typically grids).

Remote Item Status

Remote Command Centre Items show the same status information (icon, overlay, text, etc.) for the status of that item as they would show on the home server, except for when the remote Command Centre Item is off-line, the status text will show as "Offline". The icon in this case will be the unknown state, if the icon set has such an icon, otherwise it will be the first icon in the icon set. The icon's overlay in this case will be the red off-line circle with a slash through it.

Examples:
A macro only has two states, normal operation or macro running. It can now also be off-line when the macro is viewed remotely. The icon under the overlay in this case will be that of a macro that is in normal operation(the first icon) rather than an unknown icon.

e.g. 

A remote site plan, unlike a remote macro, will not show an off-line status when the remote server is off-line. This is because site plans are represented by the real Command Centre Item on both servers, and also there is nothing that the user can't do with an off-line remote Site Plan that they can do with an on-line remote Site Plan. Other examples are : Access Groups and Operator Groups.

Remote Item Properties

For remote items only the following property page tabs are visible:

1. **General** tab
2. **Status and Overrides** tab
3. **Icons** tab
4. **Notes** tab

Remote Card Types

Remote Card Types can be assigned to cards on local servers.

Editing Remote Items

1. It is not possible to create or delete remote items. It is not possible to create or delete a new Command Centre item and assign it to a division on a remote server unless it is a global Command Centre item. Items must be deleted from their local server only.
2. It is not possible to edit any properties of any remote items. Editing an item includes assigning other items (local or remote) to it. Currently the only exception to this is operators are able to assign a cardholders, local access or local Alarm Zones to a remote Access Group.

Overrides on Remote Items

1. Overrides operate in a multi-server system the same way as for a single-server system. The following rules will apply:
   a) If a local server receives an override request from a Remote Server and the override request is more than one minute old it is considered expired at the originating server and ignored.
   b) When a local server receives an override request from a remote server, the override request is treated as though it was triggered at the time it was received at the local server.
   c) When performing overrides, local and remote overrides are given equal priority.
   d) Overrides are performed in the order that they are received.
2. Operators are able to trigger a remote override. Privilege checks are done at the server where the override is requested from and no further privilege checks are done by the server performing the override.
3. An operator cannot request or cancel any override or operation on an item that is off-line for any reason. This includes not being able to schedule a remote macro when the server it belongs to is offline.

Operations on Remote Items

1. Remote items cannot be duplicated.
2. A Bulk Change of Division cannot be run on any remote items.
3. Operators can refresh the Status shown for any Remote Item in the same way as a local item, (i.e. via the **Force Status Request** option on the item's context menu).
4. Operators can force a configuration update for any remote item in the same way as a local item, (i.e. via the **Push Configuration** option on the item's context menu).
5. Operators can stop/resume polling of remote hardware items in the same way as local items.

Using and Assigning Remote Items

1. It is not possible to associate local items with remote items. This restriction greatly reduces the number of conflict scenarios that need to be dealt with.
2. There are a few exceptions where remote items can be assigned to local items and these exceptions will be covered below.
3. It will not be possible to select a remote item as the parent of a local item.

Functionality across multi-server systems

1. View alarms associated any remote items that generate alarms.
2. All Overrides on Access Zones (including anti-passback for cardholders).
3. Override the Alarm State for a remote Alarm Zone (and cancel if required).
4. Force a remote Controller to refresh its alarms in Command Centre, dial-up one of its Controllers (and hang up), resynchronise its database.
5. Reset remote Controllers, Digital Cameras, IO Boards, IDT and remote Reader Interfaces, (i.e. reboot the device).
6. Open a remote Door.
7. Override a remote Access Zone.
8. Allow a remote Site Plan to be opened from within the Event's Properties Window (if there is a related event).
9. Shunt and unshunt Fence Zones, (i.e. disable/enable any alarms associated with the Fence Zone).
10. Switch Fence Zones ON and OFF.
11. Shunt and unshunt remote Inputs.
12. Override remote Interlock Groups, Logic Block outputs, remote Outputs (and cancel if required).
13. To reset the logic for a remote Logic Block.
14. To run and schedule remote Macros
15. Perform all synchronisation operations on remote Sagem Fingerprint Readers.
16. Preview remote card layouts of cardholders.
17. Open and view the plans and alarms associated with a remote Site Plan.
18. Printing and encoding of cards.

Limitations of multi-server systems

The following will not work across multi-server systems:

1. Starting and stopping remote Archives and Backups.
2. Running remote Cardholder Bulk Changes.
3. Running a remote Bulk Change of Division.
4. Edit remote Card Layouts.
5. View live video footage from remote Gallagher Digital Cameras.
6. Open and run remote Enrolment Wizards.
7. Work with remote Intercoms.
8. Call remote IDT Reader intercoms.
9. Configure remote Sagem Fingerprint Readers.
10. Run remote reports.
11. Edit plans (drawings/images) associated with remote Site Plans.
12. Template utility when the database includes remote items.
13. Salto Resynchronisation.
14. Local Salto Doors or Zones cannot be added to an Access Group that contains remote Salto Doors or Zones. The workaround is to create separate Access Groups for the Salto items from each server.
15. Each server has its own unique Morpho Biometric Type configurable for biometric inactivity that does not get replicated across servers. As a result, biometric inactivity is managed by each server independently, using the Morpho Biometric Type configuration unique to each server.
16. Card states and their properties must be replicated in a multi-server environment, so that card states configured in a local server are available to use at a remote server.
17. Custom card state assignments need to be replicated, (e.g. A card that is marked as Lost on one server will need to replicate to other servers).

Exceptions

1. It is possible for a remote Access Group to be:
   a) assigned to a Cardholder.
   b) used in a Bulk Change to give new access rights to, or remove access rights from, a Cardholder(s)/Access Group(s).
   c) assigned to a Personal Data Field.
   d) Use remote Access Groups to group cardholders anywhere it is currently possible to use a local Access Group to group them, (e.g. Cardholder Reports, Bulk Change).
   e) Assigned local Access Zones, Schedules and Alarm Zones.
2. A remote Card Type can be assigned to a Cardholder's card.
3. A remote division will not be allowed to be assigned to any local item except for cardholders.
4. A remote Operator Group can be assigned to a Cardholder.
5. A remote Personal Data Field can be assigned to any local items.
6. A remote Site Plan can be placed on a local Site Plan.
7. Remote Access Zones and remote Divisions can be selectable for inclusion in the output of the Evacuation Report only when it is run on an aggregation server.
8. A remote competency can be assigned to a Cardholder.

Access Control and Multi-Server

Gaining Access

For gaining access at any site in the entire multi-server system, a Cardholder can use:

- the same card
- the same PIN
- the same User Code
  Note: These need to be unique across the entire multi-server system.
- their biometric data

Assigning Cards

1. When a Card is disabled it is disabled for the entire multi-server system.
2. When determining if a Card should be disabled due to inactivity, the Cardholder's activity throughout the entire system must be taken into account.
3. When servers are offline it is technically impossible to meet all the access control requirements on a real-time basis. However, when the servers are back online, any inconsistencies that were introduced as a result of the servers being offline will be corrected or conflict alarms are raised.
4. Conflicts between assigned card numbers can, and should, be avoided by good card management practices as these can directly impact access security. Separate card types should be used for each card-issuing site to avoid problems with overlapping card number ranges.
5. Command Centre can support up to 256 Facility Codes on Gallagher Controller 6000s, however legacy Controllers, (i.e. 3000/5000/5000GL) only support up to 16 Facility Codes. Therefore, if your site is using legacy Controllers, we recommend that you use one facility code for all servers, unless different facility codes are absolutely necessary, (e.g. when merging existing systems that have large numbers of cards already in circulation).

Alarms and Events

Viewing remote alarms and events

1. Operators can view alarms and events associated with all Remote Items.
2. When an alarm or event occurs any workstation in the multi-server system, where a suitably-privileged operator is logged on, are updated to show the alarm/event.
3. Events generated by a remote server when it is off-line do not appear at a local workstation. When the remote server does come back on-line, it does not show, at the local server, any events generated while the remote server was off-line.
4. When a remote server is off-line, alarms raised by that server do not appear at a local workstation until the remote server comes back on-line. When it does any unprocessed alarms it generated while being off-line appear for suitably-privileged operators at local server workstations.

Preventing Duplicate Cardholder Events

In order to prevent duplicate events being raised, membership activated / expired events will be logged by the Access Groups server only.

Likewise, card activated / expired events will be logged by the cardholder's Division's server only.

Alarm Sounds and Colours

When a remote alarm is presented at a local workstation, the accompanying sound and display colour is from the local configuration for event priorities, (i.e. alarm sounds will not be replicated between sites). This means that the alarm sounds played for remote alarms are the local server's sounds.

Viewing Alarm Instructions

1. Operators will be able to view the Alarm Instructions for alarms associated with remote items.
2. The same Alarm Instructions (including the same Insertion Tag values) that would be displayed if the operator was logged onto a workstation connected to the server that generated the alarm.
3. Alarm instructions and Insertion Tags are replicated to all servers using the standard replication mechanism. The alarm's source server determines the Alarm Instruction that is displayed for the alarm and includes its ID with the event notification. The alarm property page looks up the Alarm Instruction specified by the server.

4. Remote Alarm Instructions cannot be assigned to local items.

Viewing Remote Item properties from alarm details

When viewing remote alarm and event properties, an operator can navigate from the alarm or event's property page to any related remote item's property page in the same manner they are able to for local alarms and events.

Viewing the last 500 events

The Event Viewer displays the 500 previous events whenever an operator first logs on or changes their system view. Within a Multi-Server installation, these are local events from the local server.

Processing Remote Alarms

An operator can perform any of the usual operations on alarms associated with remote items.

Processing Remote Alarms when the remote server is off-line

If a local server loses communications with a remote server after it has raised an alarm, no actions can be performed on this alarm until the server the alarm originated from is back online. The process request will be available for processing as soon as it is back on-line.

When a remote server is off-line, a user cannot acknowledge process or enter details against the alarm. All other remote alarms from that remote server will also appear as off-line and read only. The indication that an alarms remote server is off-line is for each alarm a black off-line circle with a slash through it over the bell location.

Removing Processed Alarms

When an alarm is processed by an operator, that alarm will be removed from all alarm viewers in the multi-server system.

Generating events for remote overrides and operations

1. When an override or operation on a Remote Item is requested from a local server it generates and logs a *"Remote override requested"* operator event to record the fact that the override was requested.
2. When an override or operation is performed on a Local Item as a result of a request from a remote server, events are generated and logged by the item's home server as normal, (i.e. the same as when the override is triggered locally). The remote server does not generate an event to record the fact that the override was performed.

3. No event is generated to record the fact that a remote override request did not occur.

Configuration Conflict Alarm

"Configuration Conflict" alarms are raised when configuration replication conflicts occur. For more information see ***Conflict Resolution*** (on page 66).

Server Off-line Alarm

A *"Remote Server Off-Line"* event is raised by a server when its connection to a remote server in the multi-server system cannot be made. By default, this event must raise an alarm.

New Events for Multi-Server

The following table lists the new events added for Multi-Server, and how to raise them:

Event Group	Event Type	Event Text	Event Source	When Raised
Command Centre Comm Interrupted	Remote Server Offline	Remote Server 'A' Offline	Remote Server	Raised when the Remote head-end is closed whilst it i online with Command Centre, after about one minute has passed.
Command Centre System	Remote Server Online	Remote Server 'A' Online	Remote Server	Raised when the Remote head-end is started up again after being closed.
Operator Event	Operator requested Remote Override	The operator "X" requested that a remote override be performed on "Server Name"	Any Item	When an operator selects to perform an override from a Remote Command Centre Item. Note that the exact type of override selected is not shown in this event.
Operator Event	Operator Stopped Communication	Operator "X" stopped communication wit "Server Name"	Workstation	When an operator performs the 'Stop Communication' override on a remote server
Operator Event	Operator Starte Communication	Operator "X" starte communication wit "Server Name"	Workstation	When an operator performs the 'Start Communication' override on a remote server
Operator Event	Operator Reset Replication	Operator "X" reset replication with "Server Name"	Workstation	When an operator performs the 'Reset Replication' override on a remote server

Event Group	Event Type	Event Text	Event Source	When Raised
Operator Event	Operator Accepted Certificate	Operator "X" accepted new certificate for "Server Name"	Workstation	When an operator performs the 'Accept Certificate' override on a remote server

Events and alarms related to replication conflicts are described in the ***Conflict Resolution*** (on page 66) section.

OPC Alarms and Events

Existing event clients (including third party OPC AE clients) continue to operate.

Existing OPC alarms and event clients manage events and alarms from local server only.

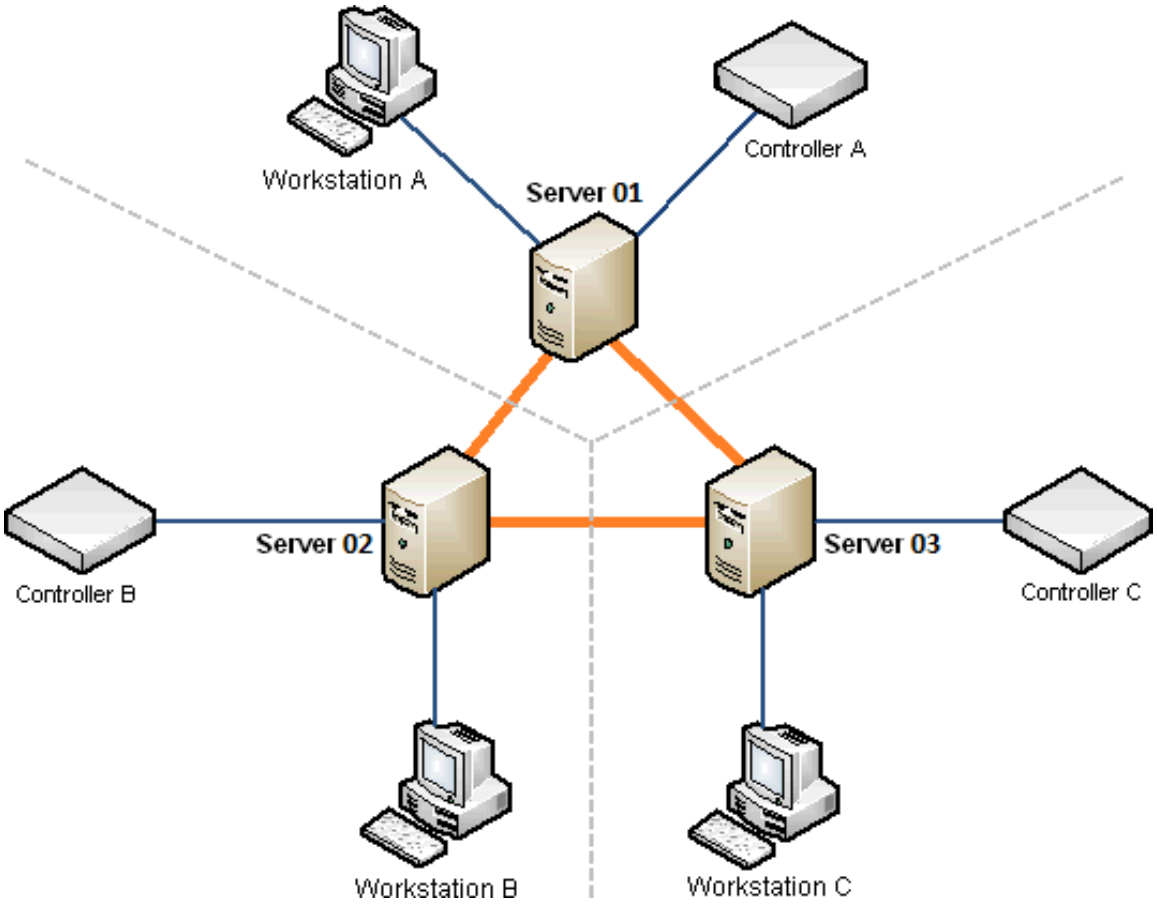
Multi-Server Communications

In this section:

- ***Connectivity*** (on page 32)
- ***Site Autonomy*** (on page 33)
- ***Trusting Servers*** (on page 34)
- ***Time Clock Synchronisation*** (on page 35)
- ***Workstation and Controller Communications*** (on page 36)
- ***Communications Security*** (on page 37)
- ***Network disconnection and/or remote server off-line*** (on page 39)

Connectivity

1. Servers are to be connected over LANs or WANs or both.
2. Servers communicate with each other using OPC UA.
3. The multi-server system does not use dynamic port-allocation technology. Installers will be able to configure the port that each server in the system will communicate on. By default, this will be set to TCP port 4840.
4. Servers communicate with other 'authorised' servers, (i.e. appropriately licensed and installed).
5. All communications between servers is encrypted.
   See ***Communications Security*** (on page 37) for further detail.
6. Each server in the multi-server system communicates directly with every other server in the multi-server environment. No server can communicate with another server via an intermediate server. See below:



Site Autonomy

When one or more servers are disconnected from other servers in the system, all servers in the system continue to operate autonomously. This means:

1. Local access control would be unaffected.
2. Local configuration is not affected.
3. Status functionality continues to work as normal for all local items.
4. Alarms and events continue to work normally for all local items.
5. Performing all overrides and actions on all local items.
6. Editing of global items.

Trusting Servers

1. A new server is authenticated as belonging to the Gallagher multi-server system before any messages received from it are accepted and applied.
2. Servers within the system are trusted. If a new server is authenticated, its messages are considered by the other servers to be valid and they are accepted and applied without any further validation.
3. The server performs all relevant operator privilege checks before sending a message to other servers in the system.

Time Clock Synchronisation

All servers in the multi-server system are required to have their time clocks synchronised. It is the responsibility of the IT System Administrator to implement this.

Workstation and Controller Communications

1. No change has been made to the way servers and workstations communicate with each other. Each workstation in the multi-server system communicates with one local server.
2. No changes have been made to the way servers and controllers communicate with each other. Each controller in the system communicates with one local server.

Bandwidth consumption

The following design principles aim at minimising bandwidth consumption in the multi-server system.

Minimising the number of communication targets

Servers only talk to other servers of interest and avoid talking to every other server, unless it is absolutely necessary. For instance:

- Override requests on a remote item are only sent to the item's home server.
- Status updates on a local item are only sent to other servers of which their workstations have registered interest on the status changes on the item.
- Local events are only sent to other servers of which their workstations are monitoring the events.
- Updates on cardholder locations are only sent to report aggregation servers or the cardholders home server when cardholders travel between sites.

Sending original changes only

Servers only send changes automatically to other servers if the changes originally happened locally. For instance:

- Cardholder changes made by an operator are only replicated to other servers automatically by the server to which the operator's workstation is connected. Servers that have received the replication do not try to replicate the changes to other servers again.

Avoiding injecting unnecessary traffic into the network

Out-of-date changes are not sent to their destinations. For example:

- Expired override requests on a remote item are not sent to the item's home server
- If an item's status has changed and its previous status has not been sent to the registered servers, the previous status update is discarded

Communications Security

Communication between servers is protected by OPC UA security. The default security policy is 'Basic256' which consists of the following algorithms:

- RSA-OAEP for asymmetric encryption and key exchange. Command Centre defaults to using 2048 bit RSA keys.
- AES with 256 bit keys for symmetric encryption.
- SHA-1 for hashing.

Server Authentication

Servers are authenticated using "instance certificates". Each server has its own instance certificate and this is stored in the other servers' databases when the server is added to the system. When a connection is established between two servers, each server verifies that the other server's certificate matches the stored certificate.

If the server is replaced then a new instance certificate and private key will be generated when Command Centre is installed on the new machine. These keys have to be marked as trusted by one of the other servers in the system before any other servers communicate with the new machine.

Default Certificate

When a server is installed, a default self-signed certificate is generated and stored in the "Personal" section of the "local machine" certificate store. The private key is marked as "not exportable" to prevent users on the machine copying the private key. By default the private key will be available for use by the account that added the certificate to the store (i.e. the user who installed Command Centre) and server administrators. Note that this means that if the "Command Centre Service" account is not an administrator then it needs to be granted access to the private key.

The automatically generated certificate will have the following properties:

Property	Value
Friendly Name	Command Centre
Subject	DC=<machine>, CN=Command Centre
Issuer	DC=<machine>, CN=Command Centre
	The certificate is self-signed.
Valid From	January 1, 2000

Property	Value
Valid To	Time of install + 20 years
Subject Alternate Names	URN-style URL based on machine name Fully qualified DNS name IP addresses (IPv4 and IPv6)
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment
Enhanced Key Usage	Server Authentication, Client Authentication

Protecting the Server's Private Key

As the private key never leaves the server machine it should not be possible for someone to copy or use the key without access to the server.

Users on the server who are not administrators are not able to use or copy the private key as Windows restricts access to administrators and the user who created the key (also an administrator). As the private key will not be marked as exportable users who can make use of the key are not able to copy it.

Network disconnection and/or remote server off-line

The multi-server system is designed to be running in an environment with continuous network availability between servers. It is not designed for an environment with frequent and continuous network outage. Intermittent network disconnections are handled so that they have minimum impact on the running of the whole multi server system.

Limiting the scope of impact on network disconnection

When the network connection between two servers goes down, the disconnection should only have impact on the communication between the two servers and should not have any impact on the communication between any other servers.

To limit the impact on network disconnections, servers will talk to each other directly. This makes communication between two servers only dependent on the network connection between them, and resistant to any other network disconnections in the system.

Servers keep functioning when networks between servers are disconnected

When the network between two servers is disconnected, each server should keep functioning independently:

Operators can still make changes on each server. Changes made by operators are not lost and when the connection is resumed the changes made on each server are replicated to the other, and any conflicts will be resolved.

Operators on each server can still perform operational task on local items. However, they cannot perform operational tasks on items on the off-line servers. For instance, an operator cannot perform an override on a remote item when the item's home server is off-line.

Cardholder location updates will be stored so that when the off-line aggregation servers come back on-line, they will receive the update.

The last status update on a local item is stored so that when the remote server that has registered interest on the status of the item comes back on-line, it receives the update.

Multi-Server Installation

In this section:

- ***Install*** (on page 41)
- ***Upgrade*** (on page 42)
- ***Example: Setting up a Multi-Server System*** (on page 43)
- ***Remote Server Status*** (on page 46)
- ***Initialising communications and replication*** (on page 50)
- ***Splitting Existing Server*** (on page 51)
- ***Merging Servers*** (on page 52)
- ***Divisions*** (on page 53)
- ***Contact ID local to a server*** (on page 54)
- ***Restoring a Server from Backup*** (on page 55)
- ***Globally unique logon name*** (on page 56)

Install

1. An installer can configure Command Centre to add one or more servers to an existing implementation to create a multi-server installation. The Gallagher install program provides installers an option to automatically configure the Windows Firewall to allow communications between Command Centre servers in the multi-server system. (Current Firewall checkbox – no change from existing versions).
2. If the licence is not enabled for multi-server, the "New/Remote Server" option is not available.
3. If the server has already been added to the multi-server environment a duplicate item pop-up will occur.
4. If the installer does not have suitable logon privileges the "New/Remote Server" option is either not available or read-only.
5. The licence cannot be used on more than one server in this multi-server system.
6. If an Unhandled Exception appears when creating a Remote Server, it is probably due to the licence file being installed or swapped after the FT Command Centre Service is started.

   If this does occur, it should only happen the first time the FT Command Centre Service is started. Therefore, a second attempt to create a Remote Server should succeed.

Upgrade

Sites with any of the following legacy devices cannot be upgraded to v8.30 or later versions:

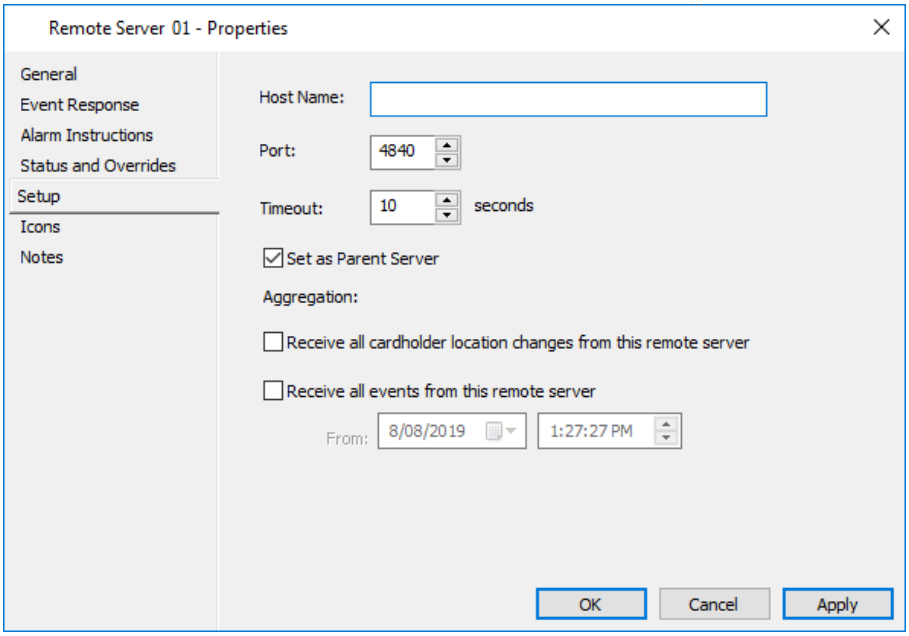
- Legacy Controllers: C3000, C5000 and C5000GL
- Local Bus devices: I/O Interface, Relay Interface, Reader I/O Interface, Universal Reader Interface, Strike Controller, IDT Tiris Reader, IDT MIFARE Reader, IDT 125 Reader and Prox Reader

On a Multi-Server site, all servers are required to be online when legacy devices are removed to allow replication between servers before communications are disabled for Command Centre upgrade. A Server that hasn't received the deletion update won't be allowed to upgrade. Gallagher recommends sites to take database backup after the legacy devices are removed, but before the upgrade to v8.30.

Error messages will display if either local or remote server obsolete device(s) are present when upgrading to v8.30. If this occurs, revert the upgraded server back to it's previous version and database, ensure all legacy devices are deleted and with all servers online to each other, ensure all changesets are replicated using Reset Replication.

Example: Setting up a Multi-Server System

1. The general idea is that an operator sets up a connection between the new server and one of the existing servers (described as "Server A" and "Server B" in this document) and the system will ensure that the information about the new server is distributed to any other servers in the system. The connection can be configured in either direction so Server A could be either the new server or the existing server.
2. Prerequisites:
   - You must be logged on to Server A as an operator with privileges to create a Remote Server Command Centre Item.
   - You must be logged on to Server B as an operator with privileges to create a Remote Server Command Centre Item.
   - Server A and Server B must have compatible licence files.
3. Configure a "Remote Server" Command Centre Item for Server B on Server A, as follows:
   a) Open the **Services and Workstations** Master List Window on Server A and create a new "Remote Server" Command Centre Item.



   b) Enter the Host Name or IP address of Server B on the **Setup** property page, and click **Apply**.
   Notes:
   - The **Host Name** can be specified in any form that can be resolved by the operating system, (e.g. host name, fully qualified domain name or IP address). However, the host name should be entered in a form that can be resolved by other servers as they will need to connect to the new server.

- The **Port** number that a server talks on is configured via the **Setup** tab, whereas the port number that a server listens on is configured via a registry key on the server.
- The **Aggregation** settings are not replicated to other sites, as it is up to those operators of those other sites to decide if they also wish to receive cardholder location information and all events from the new server. If so, check the **Receive all cardholder location changes from this remote server** and/or **Receive all events from this remote server** checkboxes, as appropriate.

Server A will now attempt a connection to Server B. This will usually fail as Server A and Server B do not trust each other.

If Server B's certificate is not trusted you will be asked if you want to trust Server B's certificate. If the certificate is correct then select "Yes".

4. Configure a "Remote Server" Command Centre Item for Server A on Server B.
   Note: Follow the procedure described in Step 3 from Server B's workstation to create a Remote Server Command Centre Item for Server A.
5. Wait for replication to complete.
   Once the servers trust each other they should come online and start replicating their configuration. This can take quite a while. You can monitor the progress of the replication from the Remote Server's **Status and Overrides** property page.
6. Configure operator privileges.
   Operators can be assigned privileges to remote servers in the usual way, (i.e. by adding them to an Operator Group that has privileges in the remote server's divisions). However, initially only System Operators will have any remote privileges so the initial configuration of operator privileges will need to be performed by a System Operator.
7. When a server is added into a multi-server system then the other servers automatically create the remote server items for this newly created server.

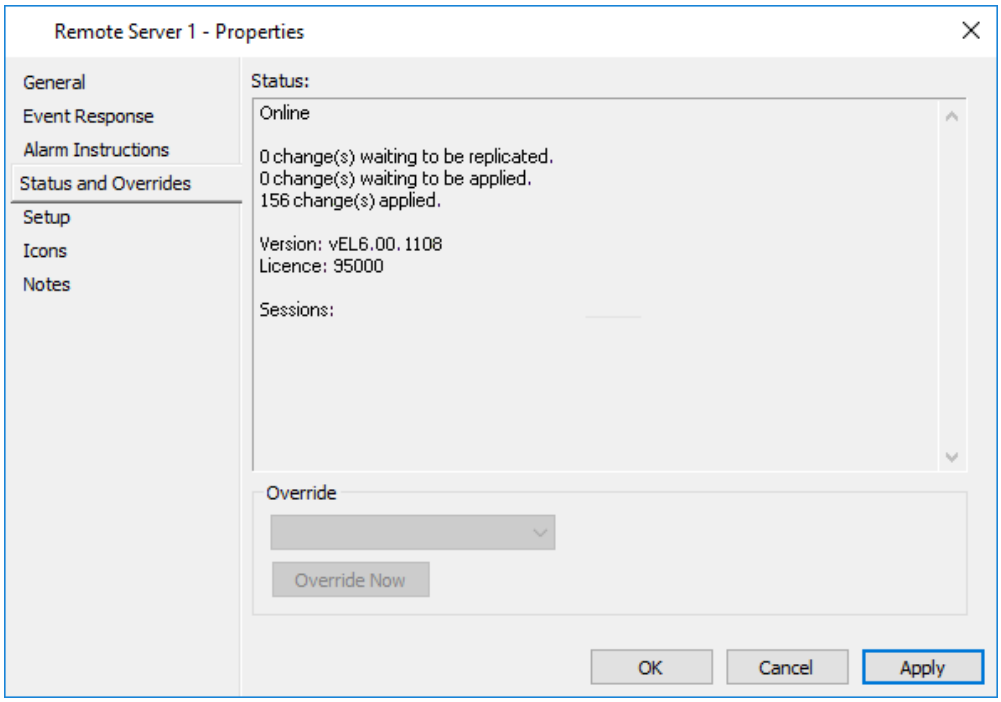
The first time (and only the first time) the Remote Server is saved the system will attempt to connect to the server using the specified connection information. If a connection cannot be established then one of the following messages will be displayed:

Message	Reason
"The Remote Server is not currently trusted. *The server's certificate was issued to Gallagher Command Centre by Gallagher Command Centre.* *Do you want to start trusting this server? [Yes] [No]*	The system was able to connect to the Remote Server but the Remote Server's certificate was no trusted by the system. The operator can select "Yes" to start trusting the Remote Server.

Message	Reason
"The Remote Server did not respond within the configured timeout period"	The system was not able to connect to the Remote Server for some reason. There are a number of possible reasons for this: • The host name or port number is incorrect or the timeout is too short. • The Remote Server is not running. • The Remote Server is inaccessible because of some firewall or network configuration. • The Remote Server is not running a "multi-server capable" version of Command Centre. • The Remote Server rejected the connection for some reason. etc...
"The Remote Server has already been added to this system"	The Remote Server has already been added to this system. A server is identified by a unique ID stored in its database so attempting to add a clone of an existing server to the system will result in this error message. Similarly, attempting to add a remote server representing the local server, (e.g. by entering "localhost" as the host name) will result in this error message.

Remote Server Status

The Remote Server's **Status and Overrides** property page behaves the same way as the standard **Status and Overrides** property page with behaviour specific to the Remote Server described below.



Status Messages

Icon	Status Text	What it means
	Online	The remote server is online.
	Offline	A remote server is considered offline if the local server has not received any responses to requests for a period of time (the offline timeout). Incoming requests are not considered when determining if a server is offline.
	Communication Disabled	An operator has disabled communication with the remote server using the "Disable Communication" override.
	The Remote Server refused the connection. This server may need to be configured on the Remote Server.	The Remote Server has refused the connection. Typically this means that the remote server has not been configured to trust the local server.

Icon	Status Text	What it means
	The Remote Server does not have the correct certificate.	The Remote Server is not using the expected instance certificate. This can occur if Command Centre is re-installed on the remote server or if its instance certificate is replaced. To resume communication the new certificate must be explicitly accepted.
	The Remote Server does not have the correct database.	The Remote Server is not using the expected database. This can occur if the Remote Server Command Centre item is configured to connect to the wrong machine. It can also occur if Command Centre is re-installed on the remote server or if the remote server restores another server's backup.
	The Remote Server does not have a compatible licence.	The "MultiServerSerialNumber" in the Remote Server's licence file is not the same as that of the local server.
	The Remote Server does not have a unique licence.	The Remote Server is using a licence file that has the same "SerialNumber" as this server.
	The Remote Server is not running a compatible version of Command Centre.	The Remote Server is running a version of Command Centre that is known to be incompatible with the version installed on the local server.
	The Remote Server's time is not synchronised with this server.	The Remote Server's clock is sufficiently different from the local server's clock to interfere with communication.
	The Remote Server is not using a compatible security configuration.	There was a security-related problem connecting to the remote server that may be related to the server's security configuration (e.g. an unsupported encryption algorithm).
	Communication with the Remote Server failed.	There was some other problem connecting to the remote server.

Replication Status

The **Status and Overrides** property page displays the replication progress:

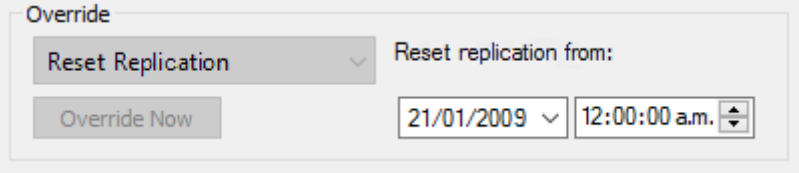
"<number> change(s) waiting to be replicated."	This is the number of changes on the remote server that have not yet been replicated to the local server. It may be greater than zero after servers are reconnected after being off-line if changes were made.
"<number> change(s) waiting to be applied."	This is the number of changes that have been replicated to the local server but have not yet been applied. It may be greater than zero due to temporary delays in replication, or dependencies on not yet replicated changes, etc.
"<number> change(s) applied."	This is the number of changes that have been replicated to the local server and have been successfully applied. This will start at zero when the server is first configured and will increase over time as configuration changes arrive from the remote server.

Server Information

The **Status and Overrides** property page will also display the version number and licence serial number of the remote server.

Reset Replication

If 'Reset Replication' is selected from the **Override** list, then the following 'Restart replication' controls appear to the right of the **Override** list:



The time displayed by default is today at midnight. If the operator starts the override then all changes since that date and time will be re-retrieved from the remote server. Any changes that had not previously been received will be applied.

1. Operators can reapply remote configuration to a local server. The option to do this is via the Remote Server property page, (e.g. on the **Status and Overrides** tab – **Override** menu).
2. When choosing this option, the operator will be able to specify a date and time in the past when the remote configuration is to be reapplied at the local server.

3. At the time this option is chosen, the local server behaves as though it has not yet received any remote changes on or after the time specified, and it will reapply all remote configuration changes that occurred anywhere in the system on or after the specified time.
4. The remote configuration changes to be reapplied are collected in the same manner as for the normal replication of configuration changes. There is no option for the operator to specify one particular server from which all remote configuration should be sourced.

Accept Certificate

If 'Accept Certificate' is selected from the **Override** list, then a **View Certificate** button appears to the right of the **Override** list. Clicking this button will display the remote server's certificate using a standard Windows certificate dialog.

Starting the override causes the local server and any other servers trusted by the local server to start trusting the remote server's current certificate. It is not be possible to start the 'Accept Certificate' override if the local server already trusts the remote server's certificate.

Note: An upgrade of your servers may fail if they are on different versions of Command Centre, due to incorrect certficates. If this occurs, accept both certificates and restart the services so the multi-servers come online.

Initialising communications and replication

As soon as a new Remote Server has been configured in the system, it starts to communicate with, and be updated by, all the other servers in the multi-server system.

Notes:

- The new server is updated with all required configuration information from existing servers in the system.
- The existing servers are updated with all configuration information from the new server. Typically, the new server only contains the default data found in a new Command Centre system. However, where the new server has a Command Centre installation that has already been used in operation, all its existing data is replicated to the existing servers.
  Note: It is acknowledged that in some cases this could pose problems with regard to duplicates, (e.g. Cardholders, Card Types and PDFs), in which case steps would need to be taken by the installer/operator to resolve this.

Splitting Existing Server

There is a utility available to split existing single server systems into multi-server systems.
The solution will need to take into account the following:

- The actual splitting of individual sites will be performed by Technical Account Managers(TAMS) as a Professional Service.
- The single server events database will not be split. After the split, this database is recommended to be moved to both servers. The ability to run activity reports from the individual servers will not be affected as long a new division is created prior to the splitting of the server. This new division should reside at a level above the division that is planned to be split.
- The splitting tool will be run against a back up copy of the live database in order to allow testing before implementation.
- Sites are split by division.
- If the site splitting tool detects any errors, the split will fail. A progressively growing list of errors will be returned to the user with an option to cancel the split.
- It is possible to easily import the list of errors to an excel spreadsheet.
- It is possible to undertake a split without the need to physically restart any of the controllers.

This utility only detects some of the issues that could cause problems for the post-split configuration. The output from the splitting tool should never be deployed to production without extensive testing in an isolated environment.

Merging Servers

1. When merging a new server into a multi-server system, regardless of whether or not the new server has already been in operation in another environment, its data is replicated across all servers (and vice-versa), so that, after any conflicts have been resolved, the result is the same as if the newly-added server had always been a part of the multi-server system.
2. Any conflicts that emerge as a result of adding a new server into a multi-server system must be handled in the same manner as they would be in a normal system where all servers are on-line and running normally. This applies regardless of whether or not the new server has already been in operation in another environment.

Note: Where two currently-operational systems are merged into one multi-server system, it is highly likely that duplicate Cardholders and Card Numbers will emerge and conflict resolution could be a major operation. However, there is currently no special requirement for handling these cases (other than by the normal means).

Divisions

Every Division in the multi-server system is permanently linked to the server it is created on and cannot span across other servers, (i.e. it cannot be assigned to any server other than the one it is created on).

Contact ID local to a server

Contact ID CCC codes are local to each server.

Restoring a Server From Backup

This procedure describes the behaviour of a multi-server system when a server (the "restored server") is restored from backup:

Configuration

The restored server will:

1. recover any configuration changes made on the other servers since the backup.
2. recover any edits or deletions performed on the restored server since the backup. Only changes that were replicated to the other servers will be able to be recovered.
   Note: Only configuration that was replicated to the other servers will be able to be recovered. For example, access groups will be recovered but they will not have any access as the access is not replicated to other servers.
3. delete other items created on the restored server since the backup, from the other servers.
4. recover changes automatically, unless a newer backup is restored on top of an older backup. If this happens it may be necessary to manually reset replication to ensure that any changes made between the restores are recovered correctly.

Example:

1. Server A is restored from a week-old backup.
2. Server A creates a cardholder (C1).
3. Server A is restored from a day-old backup.
4. Server A will not recover C1 from the other servers unless replication is reset to a time before the week-old backup.

Cardholder Location

The restored server will recover any cardholder location changes that have occurred on other servers since the backup.

The restored server will not recover any cardholder location changes that have occurred on the restored server since the backup.

Globally unique logon name

When setting or changing an Operator's Logon Name, the system will ensure that it is unique throughout the entire set of local and replicated data on the Operator's server.

Administration

In this section:

- ***Backups and Archives*** (on page 58)
- ***Replacing a Server*** (on page 59)
- ***Applying Custom Certificates*** (on page 60)

Backups and Archives

Backups

Regular backups are just as important for servers that are part of a multi-server system as they are for standalone servers. Each server can be backed up independently on a separate schedule, however if possible the schedules should be synchronised so that the set of backups provides a consistent snapshot of the overall system state in case it is necessary to roll back the entire system to a "known good" state.

Restoring Backups

There are two main reasons for restoring a server from backup:

- Server problems, (e.g. hard drive failure), or
- Configuration problems, (e.g. cardholders deleted incorrectly)

To recover from a server failure the last backup should be restored onto that server (or a replacement server if the original is not available). Once the server has been restored the other servers will automatically resynchronise with it. In general, cardholder changes made since the last backup will be recovered from the other servers but site configuration changes will not.

To roll back the system's configuration it will be necessary to restore all servers from the last backup before the incorrect configuration change. The servers should be disconnected from each other until all restores are complete to prevent them attempting to synchronise the restored and unrestored servers. This may be impractical in a system with a large number of servers; if so, it might be more efficient to reapply the changes, (e.g. recreate the cardholders that were deleted).

Archiving

Archiving and restoring from archive is similar to archiving and restoring in a standalone system, except that archiving must be configured separately on each server.

Replacing a Server

The process is identical to replacing a standalone server except that the other servers need to be informed about the new server's host name and certificate.

1. Install Command Centre on the new server.
2. Stop and disable the services on the original server.
   The services should never be started after this point as they can interfere with inter-server or controller communication.
3. Move the databases from the original server to the new server.
   Ideally this should be done by detaching the databases from the original server and attaching them to the new server. However, if the original server is not available then the last backup from the original server should be restored onto the new server instead.
4. Start the services on the new server.
5. Inform the other servers about the new server, as follows:
   a) Log on to one of the other servers in the system.
   b) Change the host name of the replaced server to the new host name.
   c) Execute an 'Accept Certificate' override to accept the new server's certificate.

Applying Custom Certificates

These instructions are included for completeness only. Applying a custom certificate is unlikely to provide any benefits and can reduce security.

1. Generate a new certificate for the server.
   The certificate must be valid for the following uses:
   - Digital Signature,
   - Non-Repudiation,
   - Key Encipherment,
   - Data Encipherment,
   - Server Authentication,
   - Client Authentication

   Note: Every server (including test or replacement servers) should have a different certificate.
2. Add the certificate to the Windows certificate store.
   The custom certificate may be stored against either the computer account or the service account used by the Command Centre services. The default certificate generated by the Command Centre installer is stored in the 'Personal' section of the computer account's certificate store.
3. Stop the Command Centre services.
4. Identify the certificate to use. Add the following values under "HKEY_LOCAL_MACHINE\SOFTWARE\Gallagher\Command Centre" in the registry:
   a) I**nstanceCertificateStoreLocation:** "CurrentUser" or "LocalMachine" (default = "LocalMachine")
   "CurrentUser" means the certificate store for the FT Command Centre Service service account.
   b) **InstanceCertificateStoreName:** Name of the store that contains the certificate (default = "My")
   c) **InstanceCertificateSubjectName:** Subject name of the certificate (default = "Command Centre")

   For example, if the subject name of the custom certificate was "CARDAXSERVER" and the certificate was stored in the "Cardax" certificate store of the domain account used to run the Command Centre services, the registry keys would be:
   InstanceCertificateStoreLocation: "CurrentUser"
   InstanceCertificateStoreName: "Cardax"
   InstanceCertificateSubjectName: "CARDAXSERVER"
5. Restart the services.
6. Tell the other servers to accept the new certificate.
   If the server is already part of a multi-server system then you will need to perform an 'Accept Certificate' override from one of the other servers so the rest of the system will accept the new certificate.

Third Party products in a Multi-Server environment

Salto Lock Interface

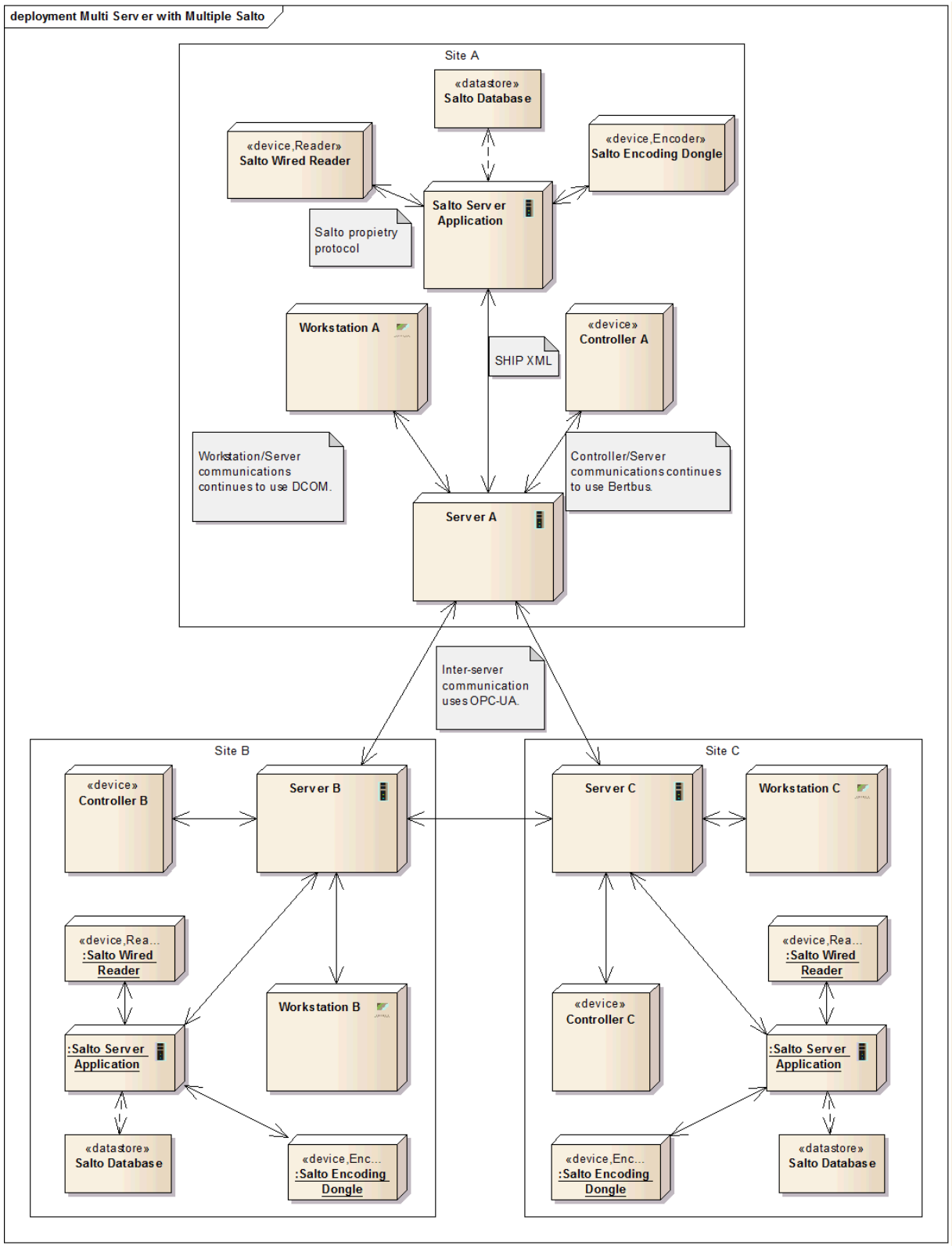
There are two possible scenarios when using Salto products in a Multi-Server environment, as follows:

Note: There are advantages and disadvantages with both scenarios to be taken into consideration.

Scenario 1: Every Command Centre server has its own Salto server and talks only to that local Salto application

This scenario is essentially the same as having separate Gallagher Command Centre server systems. There would be no ability at all to use Salto cards from one site at another site.

No changes would be required to Command Centre because the Salto Access from Remote Access Groups is not replicated and thus it cannot create confusion with the local Salto access.



Advantages

- No changes are required in Command Centre.
- Any problems with one Salto server do not affect other sites.
- Doors appear as local only on the site they actually exist on.

Disadvantages

- It completely prevents sharing cards between sites for Salto doors, (i.e. a cardholder would need separate cards for each site where they access Salto doors).
- A Salto Encoding Dongle is required per site.

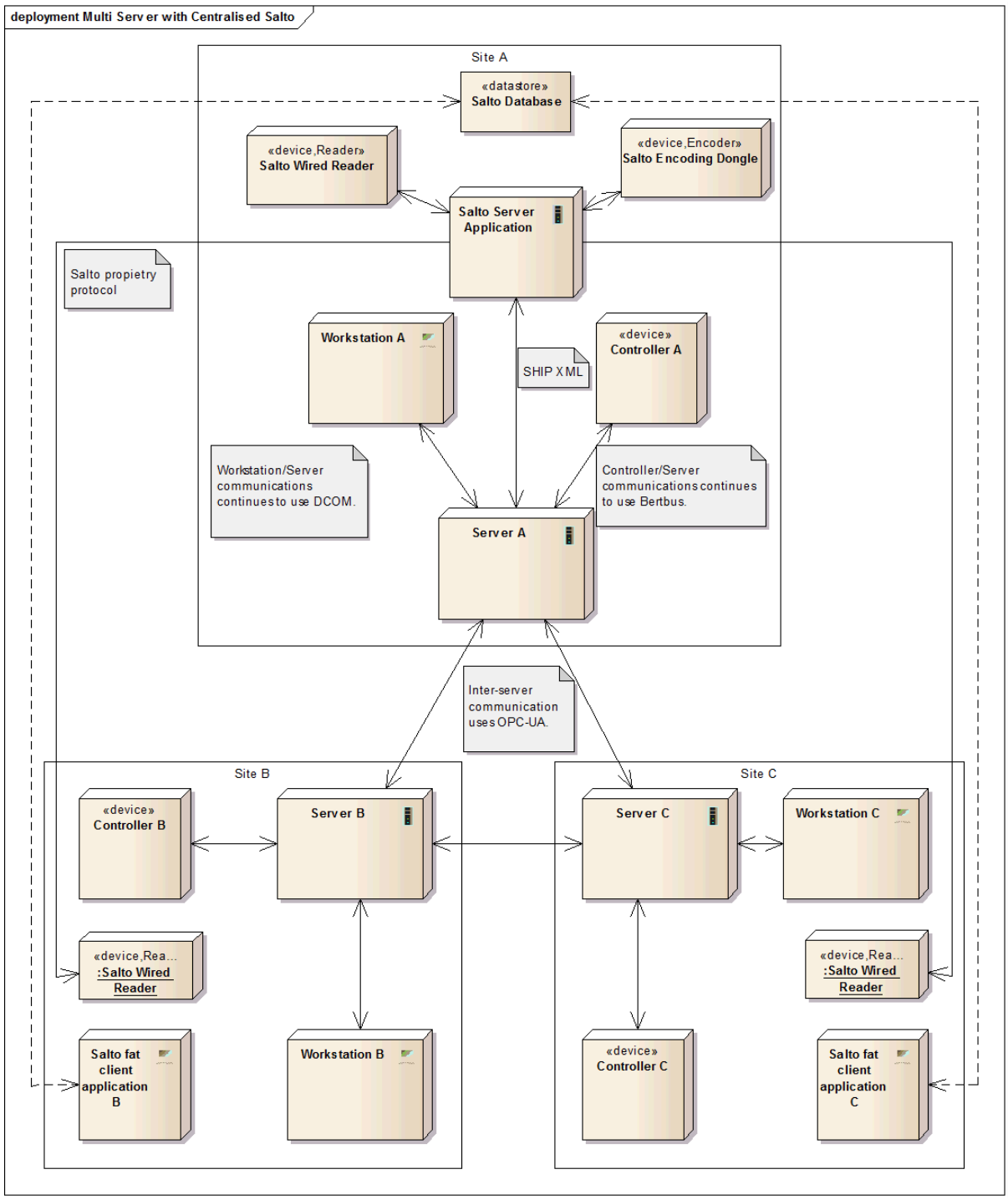
Scenario 2:
There is only one Salto server and only one Command Centre server talks to this Salto application

Only one Gallagher Command Centre server can connect to Salto and requests events and card encoding data.

When a card is used at a wired reader, only one of those systems will be contacted by Salto, and that system would be responsible for providing the access for all Salto doors. Cards can thus be shared between sites.

The Salto server FTItems created automatically on the remote server(s) would be visible but would not be used under this scenario, and cannot be deleted.

Updating unwired doors on a remote site via a PPD can be done by running a Salto application as a workstation only, connecting back to the other site's Salto database, but not the hardware.



Advantages

- Cards can be shared between sites.
- Only one Salto Encoding Dongle would be required for the whole multi-server system.

Disadvantages

- All doors appear as local to only one server (though they can be put in the different divisions to help distinguish them).

- Single point of failure for all sites Salto access.
- Wired readers communicate with Salto over the WAN.
- Card encoding will currently only work from the Command Centre Server connected to the Salto Application designated as the Online Peripheral Manager, or a change is required to make it work from any workstation on any server.
- Superfluous local Salto Server FTItems are untidy.
- All sites need to be in the same time zone.

Conflict Resolution

Configuration Conflict - Definition

Refers to a remote configuration change that should not or cannot be applied at a local server because it either breaks a constraint or definition in Command Centre, (e.g. a uniqueness or maximum limit constraint) or because dependent items do not exist. This can occur when changes made at one server do not always instantly appear at all other servers - delays in the network are inevitably involved.

Configuration conflicts can be divided into two broad categories:

1. **Configuration conflicts:**
   These include:
   a) Uniqueness constraints
   b) Required value constraints
   c) Limit constraints, e.g. maximum Facility Code limit, (i.e. 256 Facility Codes on Gallagher Controller 6000s, or 16 Facility Codes on legacy Controllers)
2. **Dependency Violations:**
   These occur when a dependent item does not exist, i.e. the configuration change (made at a remote server) involves an item that does not exist at the local server. This can happen when, for example, an item is edited on one server while the same item is being deleted on another server. Or similarly, because the order in which updates arrive at a server can't be guaranteed, it is possible for a server to receive an update for an item before it even knows that the item itself has been created.

Note: Two operators "simultaneously" changing the same property of an item is not in itself considered to be a configuration conflict. It is assumed that, as long as server time-clocks are synchronised, it will always be possible to determine the order in which changes were saved in real-time, and that one of the changes will be more recent than the other (even if only by one thousandth of a second). The most recent change is the one that should be applied (on each server).

Raising and Processing Alarms

- A Configuration Conflict Alarm will be raised by the server as soon as it becomes apparent that a conflict has been created, (e.g. duplicate Card Numbers have been used).
- A Configuration Conflict Alarm will be raised regardless of whether or not the configuration changes concerned have been applied. Remote configuration changes may or may not be applied at a local server even

though the change comprises of data that causes the conflict. This will depend upon the type of change.

- A Configuration Conflict Alarm will be raised by a server whenever a remote configuration change cannot be applied at that server due to a dependency violation, (e.g. the item to be updated doesn't exist).
- Configuration Conflict Alarms will be stateful.
- All Configuration Conflict Alarms are viewable via the Alarms window.

Conflict - Default Behaviour

Unless otherwise specified in the operational specification for a specific conflict, replication conflict alarms will have the following properties.

Event Type	Conflict Detected
Event Group	Maintenance Warning
Event Source	Command Centre item ("Server Properties")
Division	Root division of the server that detected the conflict
"Stateful"	No

Conflict - Concurrent Updates

Summary

A value is simultaneously modified at more than one server.

Scenario

- Server A changes a cardholder's name to "Alice".
- Server B changes the same cardholder's name to "Bob".
- Server A receives the cardholder update from Server B
- Server B receives the cardholder update from Server A

The name of the cardholder will be different on each server if both servers blindly apply the last change they received.

Resolution

Servers only apply a new update if:

- The update's timestamp is more recent than the timestamp of the last update applied OR
- Both updates occurred at the same time and the update's unique ID ("ChangeSetID") is larger than the ID of the last update.

The "timestamp" is the time of the change according to the server that initiated the change.

Alarms

None

Conflict - Dependency on Unknown Item

Summary

An update references an item that is not known on a server.

Scenario

- Server A creates a division
- Server B assigns a cardholder to the new division
- Server C receives the cardholder update from Server B

Server C cannot apply the division change because it does not know about the existing of the cardholder's new division.

Resolution

The update is not applied until the item that the update is dependent on arrives. If it never arrives then the update will never be applied. A resync would be required to clear any redundant data.

Alarms

None. The conflict will usually be resolved automatically when the relevant update arrives.

Cardholder Examples

- Cardholder arrives before the division
- Card arrives before the cardholder
- Card arrives before the Card Type
- Biometrics arrive before the biometric type
- Biometrics arrive before the cardholder
- PDF value arrives before the PDF definition
- PDF value arrives before the cardholder
- Access Group membership arrives before the Access Group
- Access Group membership arrives before the cardholder
- Operator Group membership arrives before the Operator Group
- Operator Group membership arrives before the cardholder

Non-Cardholder Examples

- Child arrives before the parent.
  This should only happen if a message is lost, which means a resync will be required to fix the problem.
- Item arrives before the icon set.
  This should only happen if a message is lost, which means a resync will be required to fix the problem.
- Site Plan arrives before the items.
- Workstation restriction arrives before the Operator Group.
- Workstation restriction arrives before the workstation.

Conflict - Dependency on Deleted Item

Summary

An update introduces a dependency on a deleted item.

Scenario

- Server A deletes a card type
- Server B adds a card of that type to a cardholder
- Server A receives the card update from Server B
- Server B receives the card type deletion from Server A

Server A cannot create the card because the card type has been deleted.

Server B cannot delete the card type because a card is using it.

If the item can normally be deleted while assigned then this scenario is not considered a conflict and the item will be deleted without any alarms being generated. For example, cardholders can be deleted while assigned to access groups so deleting a cardholder at one server while the cardholder is being added to an access group at another is not considered a conflict.

Resolution

Server A does not create the card as the card type has been deleted.

Server B delays the deletion of the card type until all cards of that type have been deleted.

It will not be possible to undo the deletion so all items using the deleted item must be manually reconfigured so they no longer depend on the deleted item.

Alarms

Message	[Item] "[Name]" deleted while in use *e.g. Card Type "Student Card" deleted while in use*
Details	None
Event Type	Deletion Conflict Detected

Examples

- Assigning a deleted Card Type to a card
- Assigning a deleted division to a Command Centre item
- Assigning a deleted Icon Set to a Command Centre item

- Assigning a deleted Personal Data Field to an Access Group / deleted Access Group to a Personal Data Field
- Assigning a deleted Operator Group to an operator / deleted operator to an Operator Group
- Assigning a deleted division to an Operator Group (for granting privileges in that division)
- Assigning a deleted Personal Data Field to an Operator Group
- Assigning a deleted workstation to an Operator Group
- Assigning a deleted Operator Group to an Operator Group

Conflict - Duplicate Card Numbers

Summary

More than one card exists with the same card number and facility code.

Scenario

- Server A creates a card (facility code A1, number 1)
- Server B creates a card (facility code A1, number 1)
- Server B receives the card update from Server A
- Server A receives the card update from Server B

Server B cannot create the card as it already has an existing card with the same facility code.

Server A cannot create the card as it already has an existing card with the same facility code.

Resolution

The destination server allows the second card to be created with the same card number and facility code. Both cards are considered disabled until the duplication is manually resolved. The reason the card is disabled is displayed in the card's properties.

Alarms

The following alarm will be generated by a server when it applies a change that causes a card to have the same card number and facility code as another card. If there is more than one existing card with the card number and facility code then a separate alarm will be generated for each existing card.

Message	Duplicate Card: "<cardholder name 1>" and "<cardholder name 2> *<cardholder name 1> is the name of the cardholder associated with the replicated change that caused the conflict.* *<cardholder name 2> is the name of the existing cardholder with a card that conflicts with the replicated change*
Details	Card Number: <card number> Card Types: "<card type 1>" and "<card type 2>" *<card type 1> is the name of the replicated card's card type. <card type 2> is the name of the existing card's card type.*
Event Type	Duplicate Card Detected
Stateful	Yes

Conflict - Duplicate User Codes

Summary

A cardholder's user code conflicts with the user code or duress code of another cardholder.

Scenario

- Server A assigns user code 1234 to a cardholder
- Server B assigns user code 1234 to a different cardholder
- Server B receives the cardholder update from Server A
- Server A receives the cardholder update from Server B

Server A cannot apply the update as it already has an existing cardholder with that user code.

Server B cannot apply the update as it already has an existing cardholder with that user code.

Resolution

The destination server allows cardholders to have conflicting user codes or duress codes, however the cardholders' user codes and duress codes are non-functional until the duplication is manually resolved. The reason the user code and duress codes are disabled is displayed in the cardholder's properties.

Alarms

The following alarm will be generated by a server when it applies a change that causes a cardholder to have the same user code as another cardholder. If there is more than one existing cardholder with the user code then a separate alarm will be generated for each existing cardholder.

Message	Duplicate User Code: "<cardholder name 1>" and "<cardholder name 2>" *<cardholder name 1> is the name of the cardholder associated with the replicated change that caused the conflict.* *<cardholder name 2> is the name of the existing cardholder with a user code that conflicts with the replicated change*
Details	None
Event Type	Duplicated User Code Detected
Stateful	Yes

Conflict - Duplicate Operator Logon Name

Summary

The same logon name is assigned to multiple operators.

Scenario

- Server A assigns the logon name "admin" to an operator
- Server B assigns the logon name "admin" to a different operator
- Server B receives the update from Server A

Server B cannot apply the update as it already has an existing operator with that logon name.

Resolution

The destination server allows both operators to have the same logon name. If an operator attempts to log on using a logon name that is assigned to more than one operator then the server will assume that the operator is attempting to log on as a "local" operator. If none of the operators are "local" then the logon will fail.

Alarms

The following alarm will be generated by a server when it applies a change that causes an operator to have the same logon name as another operator. If there is more than one existing operator with the same logon name then a separate alarm will be generated for each existing operator.

Message	Duplicate Logon Name: "<operator name 1>" and "<operator name 2>" *<operator name 1> is the name of the operator associated with the replicated change that caused the conflict.* *<operator name 2> is the name of the existing operator with a logon name that conflicts with the replicated change*
Details	None
Event Type	Duplicate Logon Name Detected
Stateful	Yes

Note: If both servers are online and a duplicate logon name is entered and applied, a digit is appended to the logon name to create a unique logon name.

Conflict - Duplicate Value in Unique Personal Data Field

Summary

The same Personal Data Field (PDF) value is assigned to more than one cardholder, but the PDF is configured to be unique.

Note: Personal Data Fields should have unique names across servers.

Scenario

- Server A assigns the value "A" to a cardholder's PDF
- Server B assigns the value "A" to a different cardholder's PDF
- Server B receives the cardholder update from Server A

Server B cannot apply the change as the PDF value is already assigned to a cardholder.

Resolution

The destination server allows the duplicate value to be saved. Multiple cardholders end up with the same value in the unique PDF.

If the personal data field is being used as the "Third Party ID" in a cardholder import then the import will fail for any cardholders that share an ID.

Alarms

The following alarm will be generated by a server when it applies a change that causes a cardholder to have the value in a unique personal data field as another cardholder. If there is more than one existing cardholder with the same value in the unique PDF then a separate alarm will be generated for each existing cardholder.

Message	Duplicate "<personal data field name>": "<cardholder name 1>" and "<cardholder name 2>" *<cardholder name 1> is the name of the cardholder associated with the replicated change that caused the conflict.* *<cardholder name 2> is the name of the existing cardholder with a personal data value that conflicts with the replicated change*
Details	None
Event Type	Duplicate Personal Data Detected
Stateful	Yes

Conflict - Value Invalid According to Configuration

Summary

A value is invalid according to the system's configuration.

Scenario

- Initially the personal data field is not configured as "Required"
- Server A creates a cardholder but does not assign a value to the personal data field
- Server B marks the personal data field as "Required"
- Server B receives the cardholder from Server A
- Server A receives the personal data field update from Server B

Server B cannot save the cardholder as they do not have a value in the "Required" PDF.

Server A cannot make the PDF "Required" as there is a cardholder without a value in the PDF.

Resolution

Both servers allow the changes to be applied. In the example the cardholder ends up with no value in the "Required" PDF.

Alarms

None

Examples

- No value in a "Required" Personal Data Field.
- Value in a "Restricted Text - List" Personal Data Field is not in the list.
- Card number is not in the Card Type's configured card number range.
- Alarm notes are not optional for an Operator Group but there are no alarm notes configured.

Conflict - Controller Capacity Exceeded

Summary

An update causes a Gallagher Controller capacity limit to be exceeded.
Important: Command Centre can support up to 256 Facility Codes on Gallagher Controller 6000s, while legacy Controllers, (i.e. 3000/5000/5000GL) only support up to 16 Facility Codes. Therefore, this scenario is for a site using legacy Controllers.

Scenario

- Initially the system contains 15 facility codes
- Server A creates a card type with a new facility code
- Server B creates a card type with a new (but different) facility code
- Server B receives the card type from Server A

Server B cannot save the card type as it would exceed the controller's limit of 16 facility codes.

Resolution

Facility Code Limit Exceeded: The destination server saves the remote card types and their facility codes and assigns a facility code index to each of the excess remote facility codes. These indexes are greater than or equal to the facility code limit. All the cards created using the excess remote facility codes cannot be downloaded to controllers. If a facility code with an index less than the facility code limit is deleted, another remote facility code with an index greater than or equal to the facility code limit will be activated to use the index of the deleted facility code. All cards using that activated remote facility code are then sent to controllers.

Other Limits Exceeded: The destination server will not apply the change immediately. An operator will need to resolve the issue manually before the change will be applied, (e.g. by removing an access group from the cardholder).

Alarms

Message	Conflict Detected for [item type] "[item name]" *e.g. Conflict Detected for Card Type "Student Card".*
Details	The maximum number of facility codes has been reached. *The exact text will depend on the limit that was exceeded. It will generally be the same as the message that would have been displayed if the change had been applied by an operator.*
Event Type	Conflict Detected

This is an example of the generic "Conflict Detected" event that will be used for any conflicts that are important enough to require an alarm but not likely enough to warrant the creation of a specific event.

Examples

- Limit of 16 facility codes exceeded
- Limit of 255 Access Groups per Controller per cardholder exceeded

Conflict - Licence Limit Exceeded

Summary

Licence limits are exceeded because items are created on separate servers.

Scenario

- Each server is licenced for 1000 cardholders and 999 are currently configured.
- Server A creates a cardholder
- Server B assigns one of its cardholders to a division on Server A
- Server A receives the cardholder from Server B

Server A cannot save the cardholder as the licence limit would be exceeded.

Resolution

The destination server ignores licence limits when applying changes from other servers. The system currently checks the licence limits at runtime and expires the licence after a grace time if the limits have been exceeded.

Alarms

The existing "Licence Limit Exceeded" alarm will be generated if the licence limit is exceeded.

Conflict - Item Locked for Editing

Summary

A change arrives while an item is being edited by another operator.

Scenario

- Server A operator starts editing a cardholder
- Server B modifies the same cardholder
- Server A receives the cardholder update from Server B

Server A cannot apply the change as the cardholder is locked while it is being edited.

Resolution

The destination server queues the update for processing later when the cardholder is not being edited.

Alarms

None

Index

A

Access Control and Multi-Server • 26
Administration • 57
Alarms and Events • 27
Applying Custom Certificates • 60
Architecture • 11

B

Backups and Archives • 58

C

Cardholder Location Data • 18
Change History • 14
Command Centre General • 13
Communications Security • 37
Conflict - Concurrent Updates • 69
Conflict - Controller Capacity Exceeded • 79
Conflict - Default Behaviour • 68
Conflict - Dependency on Deleted Item • 72
Conflict - Dependency on Unknown Item • 70
Conflict - Duplicate Card Numbers • 74
Conflict - Duplicate Operator Logon Name • 76
Conflict - Duplicate User Codes • 75
Conflict - Duplicate Value in Unique Personal Data Field • 77
Conflict - Item Locked for Editing • 82
Conflict - Licence Limit Exceeded • 81
Conflict - Value Invalid According to Configuration • 78
Conflict Resolution • 66
Connectivity • 32
Contact ID local to a server • 54

D

Definitions • 5
Disclaimer and Copyright Notice • 2
Divisions • 53

E

Example: Setting up a Multi-Server System • 43
Exceptions • 25

F

Find Tool • 15
Functionality across multi-server systems • 23

G

Globally unique logon name • 56

I

Initialising communications and replication • 50
Install • 41

L

Licensing • 12
Limitations of multi-server systems • 24

M

Merging Servers • 52
Multi-Server Communications • 31
Multi-Server Installation • 40
Multi-Server Overview • 6
Multi-Server Setup • 10

N

Network disconnection and/or remote server off-line • 39

O

Operators • 16
Overrides on Remote Items • 19

P

Preventing Duplicate Cardholder Events • 28

R

Remote Items • 19
Remote Server Status • 46
Replacing a Server • 59
Reporting • 17
Restoring a Server From Backup • 55

S

Salto Lock Interface • 61
Server Off-line Alarm • 28
Site Autonomy • 33
Splitting Existing Server • 51
Supported Systems • 9

T

Third Party products in a Multi-Server environment • 61
Time Clock Synchronisation • 35
Trusting Servers • 34

U

Upgrade • 42

W

Workstation and Controller Communications • 36