Gallagher Command Centre vEL9.40

Release Note

Upgrade Procedures

Copyright © Gallagher Group Limited

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2026. All rights reserved.

Contents

1 Introduction 4
- 1.1 Compatibility 4
- 1.2 Supported SQL Server versions 5
- 1.3 SQL Database Installation on a separate server 5
- 1.4 Command Centre database integrity recommendations 6
- 1.5 SMTP library update 6
- 1.6 Windows Performance Counters 7
- 1.7 Maintaining DCOM connections from other machines 7
- 1.8 Gallagher Controller compatibility 7
- 1.9 OneLink 7
- 1.10 Controller Global Default Server Address 7
- 1.11 Salto Lock Interface 8
- 1.12 Multi-server system sites 8
- 1.13 Gallagher Mifare Encoders 8
- 1.14 OPC Bridge 8
- 1.15 Gallagher Controller API compatibility 8
- 1.16 Morpho Biometric Integration 8
- 1.17 Schlage AD Series locks 9
- 1.18 Key Device alarm changes 9
- 1.19 Visitor Management 9
- 1.20 Customisations 9
- 1.21 IP Alarms Receiver compatibility 10
- 1.22 Jacques Video Stream 10
- 1.23 MIP Plugin Feature 10
- 1.24 UL Installations 10
- 1.25 Managing keys for MIFARE credentials 10
- 1.26 Commend Intercoms 10
- 1.27 Other files installed 10

2 Upgrading to vEL9.40 from a previous version 11
- 2.1 Before you begin 11
- 2.2 Upgrading the Server 12
- 2.3 Upgrading Workstations 15
- 2.4 Upgrading Gallagher Controller 6000s to vCR9.40.xxxx 18

3 Gallagher Command Centre Rollback Procedure 20
- 3.1 Downgrading the Server, Workstations and Controllers to a previous version 20

Appendix A: Alternative Client Deployment Options 22

Appendix B: SQL Database Installation on a separate Server 24

Appendix C: Upgrading from ScanShell 1000B to SnapShell Passport Scanners 27

Appendix D: Client Authentication 28

Appendix E: Migrating SQL Server from 32-bit to 64-bit 32

Appendix F: Implementation of Controller Global Default Server Address Upgrade 33

Copyright © Gallagher Group Limited

1 Introduction

This version of Gallagher Command Centre is supported on upgrades from any release version of Gallagher Command Centre from vEL9.00 onwards (see *Upgrading to vEL9.40 from a previous version* for further detail regarding upgrades).

IMPORTANT:

- **A number of enhancements made to this version of Gallagher Command Centre may affect how some of the existing features now operate. For further details refer to the *Gallagher Command Centre Version 9.40 Feature Summary* located at Feature Summaries - Resources | Security Hub (gallagher.com).**
- **Gallagher recommend sites run the Pre-Upgrade Validation Tool before upgrading, to evaluate site compatibility with the upgrade. For instructions refer to the *Gallagher PreUpgrade Validation Tool Release Note* (located in the 'Utilities\PreUpgradeValidationTool_v9.xx.xx' directory of the Command Centre installation files).**
- **The Gallagher Command Centre Installation software is available from SharePoint.**

1.1 Compatibility

This version of Gallagher Command Centre (vEL9.40) supports the following Microsoft Operating Systems and follows Microsoft Windows lifecycle. Please refer to https://support.microsoft.com/en-nz/help/13853/windows-lifecycle-fact-sheet

	Operating Systems Supported
Gallagher Command Centre Server	Windows Server 2025
	Windows Server 2022
	Windows 11 Pro / Enterprise *(64 bit versions only)*
	Windows 10 Pro / Enterprise
	Windows Server 2019
	Windows Server 2016
Gallagher Command Centre Workstation, Visitor Management and Kiosk	Windows 11 Pro / Enterprise *(64 bit versions only)*
	Windows 10 Pro / Enterprise

Notes:

- Windows 10 Pro N and 11 Pro N are NOT supported operating systems.
- Gallagher Command Centre installation is **not** supported on a Windows Domain Controller PC.
- Your Server can be on a different operating system to your workstations, as long as they are any of those listed.
- Windows Accessibility Options are not supported.
- Gallagher Command Centre is supported on English and non-English language versions of Microsoft Windows.
- Sites who want to use a translated version of Gallagher Command Centre may encounter problems with non-English characters not displaying correctly, (e.g. in Reports), if they do not have the Arial Unicode MS font installed.
  This font is only available with the set of approved translation files. To install it simply copy the file **Arialuni.TTF** from the “Resources” folder and place it in the C:\Windows\Fonts folder on every workstation which will run the Command Centre client.

Copyright © Gallagher Group Limited

- **Scheduled Reports:** Scheduled reports may fail if the Network Service account does not have permissions to write to the output location. There are also issues surrounding printing scheduled reports using macros. The issues you encounter will depend on the type of printer being used, (i.e. local or network), and the operating system the "FT Command Centre Service" is running on. For further detail refer to the "Configuring Printers for Reports automatically generated via Macros" in v9.40 of the *Gallagher Command Centre Configuration Client User Guide* (part number C209000).

1.2 Supported SQL Server versions

Gallagher Command Centre currently supports the following databases:

Gallagher Command Centre Database Server Systems Supported	**Minimum Service Pack**
Microsoft SQL Server 2022 / 2022 Express	n/a
Microsoft SQL Server 2019 / 2019 Express	n/a
Microsoft SQL Server 2017 / 2017 Express	n/a
Microsoft SQL Server 2016 / 2016 Express	SP2

Notes:

- The Command Centre database naming schema does not support changing the defaul schema name from dbo.
- If your existing SQL Server version is not supported by the Command Centre upgraded version, a window will pop up and the installation will not continue. You will need to upgrade SQL Server instance to a supported version (see table above).
  Note: Native SQL compatibility level is set according to the version of the SQL installed. When SQL is upgraded to a newer version after Command Centre is upgraded, this won't change the compatibility level causing potential performance issues with Command Centre. Gallagher recommends that SQL is upgraded prior to Command Centre upgrade or Command Centre installer is run after the SQL server is upgraded which changes the CCFTCentral and CCFTEvents DB to recommended compatibility level for the installed SQL version.
- Gallagher Command Centre does not support 32-bit SQL Server versions. Refer to *"Appendix E: Migrating SQL Server from 32-bit to 64-bit"* for the procedure.
- Gallagher Command Centre will support any combinations of the server operating systems (mentioned on page 4) and SQL server versions that are supported by Microsoft. The only exception to this is for any third party peripheral devices that do not support the listed operating system.
- Server collation should be set to **SQL_Latin1_General_CP1_CI_AS** or **Latin1_General_CI_AS**
- The Command Centre service can be run under a Group Managed Service Account.

1.3 SQL Database Installation on a separate server

Command Centre offers the option to connect to SQL databases installed on a separate server from Command Centre. This allows a company's IT team to more efficiently manage databases and other IT resources.

IMPORTANT:

- This feature requires a site to take full responsibility for all management of their SQL databases.
- When SQL is installed on a separate computer from the Command Centre server, it is imperative that communication links between these computers are reliable. It is also critical that latency between these machines is as small as possible, less than 1ms is recommended as anything higher than this can cause performance issues for some operator initiated actions. Should the Command Centre server be unable to connect to the database for any reason the Command Centre services, and therefore all workstations, will be restarted.

Copyright © Gallagher Group Limited

- If your Command Centre SQL databases are hosted on an Always On Availability Group, first remove the databases from the Availability Group, then upgrade Command Centre, then put the databases back on the Availability Group. Alternatively you can change your collation before the upgrade and change it back again afterwards, please consult Gallagher if you do this. You need only to perform either action the first time you are upgrading to vEL9.40 or later version.

If your site wishes to use this feature, refer to *"Appendix B: SQL Database Installation on a separate Server"* for the procedure.
IMPORTANT: Please check the prerequisites of *Appendix B* at the time of installation.

1.4 Command Centre database integrity recommendations

Sites have full access to the Command Centre databases. This means administrators can grant local and/or domain Windows users access to edit, manage and maintain the SQL Instance and attached Gallagher (CCFT) databases.

Customer Responsibilities

As per the Software License and Maintenance Terms and Conditions accepted upon installation of Command Centre, Gallagher will not be liable in any circumstances for the loss or corruption of data.

It is the responsibility of the customer to:

- Not modify any Data, Metadata or Schemas in the Gallagher Command Centre databases by any method other than via the Gallagher Command Centre Application.
- Not share the database instance with other services.
- Not upgrade the databases while in Availability groups.
- Implement appropriate measures to ensure adequate levels of data security.
- Manage, monitor and maintain their Gallagher Command Centre databases, this includes backups (scheduled and manual), archiving and database transaction log files.
- Accept full responsibility for any data loss or corruption associated with the unauthorized modification of data or schemas within the Gallagher system.
- Accept that if the event data is required for legal purposes, Gallagher will be unable to verify that the data has not been altered by an unauthorized method, or software outside the Gallagher Command Centre application.
- Communicate promptly and completely in response to all issues and requests for information from Gallagher.

Support Approach

Support requests resulting from the tampering, corruption, failure to maintain transaction log files or unauthorized modification of any Gallagher system Data or Schema will be at the Customers full cost where possible.

1.5 SMTP library update

Command Centre 9.40 has an updated SMTP library which supports Microsoft Office 365 and enables customers to opt in for an additional layer of security when sending emails. There is now an option that allows validation of the email certificate provided by the SMTP server, strengthening the authentication process, and protecting against any unauthorised access.

The updated library also requires a stronger method of approving access to the SMTP server. Due to this existing configuration may impede the ability to send emails from Command Centre. In the event that the SMTP server does not support authentication and Command Centre notifications are configured with a user account and password, emails will fail to send. To resolve this, the account and password need to be removed completely. This configuration is under Server Properties, Outgoing Email.

Copyright © Gallagher Group Limited

1.6 Windows Performance Counters

Real-time performance counters can now be deployed into Windows Performance Monitor as part of Gallagher Command Centre for detailed monitoring of your system. Such monitoring can be useful for finding bottlenecks, assist with fault-finding, or just working out system loads at any given time of the day to plan downtimes. For further details refer to the *Gallagher Windows Performance Counter Release Note* (located in the 'Utilities' directory of the Command Centre installation files).

1.7 Maintaining DCOM connections from other machines

Most Command Centre installs no longer require DCOM, so remote access via DCOM is disabled by default and encryption is enabled by default. Therefore, DCOM connections from other machines will fail by default, (i.e. XML import, BootP, or OPC AE/DA). Legacy settings can be restored using the 'FT DCOM Setup' utility. Refer to the "DCOM Setup Utility" topic in v9.40 of the *Gallagher Command Centre Configuration Client User Guide* (part number C209000) for instructions.

1.8 Gallagher Controller compatibility

Command Centre v9.40 supports the Controller 6000 firmware vCR9.40. No configuration changes should be made on Controller 6000 running pre-version v9.40 once Command Centre has been upgraded.

IMPORTANT: Legacy Controllers, (i.e. Controller 5000GL, 5000, 3000-8R and 3000-4R) are no longer supported from version vEL8.30. If your site has a Legacy Controller as a key device in the license file, you will need to request a new license file with one of your site's Controller 6000s/7000s as a replacement key device.

Notes:

- The installer will block an upgrade for sites with pre-vEL7.10 controllers. Therefore, sites that are upgrading controllers running firmware earlier than v7.10, and require those controllers to communicate with each other during upgrading, should upgrade the group of controllers to a version later than v7.10 first before upgrading to the latest version.
- If you receive "Controller Incompatible configuration" alarms the Controllers need to be upgraded to v9.40.

1.9 OneLink

OneLink utilises Gallagher Cloud Services to enable Controller 7000s to connect to the on-premises Command Centre Server over the internet.
Note: Controller 6000s do not support OneLink connection.
Refer to the "OneLink Configuration" topic in v9.40 of the *Gallagher Command Centre Configuration Client User Guide* (part number C209000) for further detail.

Known Issue: The Random Selection feature will not function reliably on Controllers connected via OneLink. This issue will be addressed in a future Maintenance Release.

1.10 Controller Global Default Server Address

From v9.00, a Global Default Server Address can now be set for Controllers.
An upgrade step will be executed the first time a site upgrades from v8.90 (or earlier) to v9.00 (or later), i.e. If Controllers have a commonly used custom server address (custom hostname or ip address) it will become the Default Global Server Address, and any Controllers using that address will be changed from "custom" to "default" server address.

Refer to *"Appendix F: Implementation of Controller Golbal Default Server Address Upgrade"* for further detail.

Copyright © Gallagher Group Limited

1.11 Salto Lock Interface

The Salto Lock Interface for Command Centre v9.40 supports Salto ProAccess SPACE 6.10.4.3. To upgrade your Salto installation, refer to the "Salto Lock Interface" chapter in v9.40 of the *Gallagher Command Centre Configuration Client User Guide* (part number C209000).

Important: Please contact your Gallagher representative if using RF mode 1 devices. Salto ProAccess SPACE 6.10.4.3 supports Salto RF2 and RF3 modes only. Salto RF mode 1 devices are not supported and will need to be replaced.

1.12 Multi-server system sites

- Sites with legacy devices cannot be upgraded to v8.40 or later versions. 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 a database backup after the legacy devices are removed, but before the upgrade to v9.40.
- Before upgrading a multi-server system, it is important to disable the communications between the servers to prevent changeset corruption and "out-of-sync" issues. On a workstation at every server, go to the **Services and Workstations** Master List Window and override all remote servers to "Disable Communication".

1.13 Gallagher Mifare Encoders

The combinations of firmware/drivers that work together depend on the version of Command Centre you have installed. For further details refer to the *Gallagher Mifare Encoder Installation Note* (**3E0774 Install Note Mifare Encoder.pdf**) located in the "Utilities\Mifare Encoder Drivers" directory of the Command Centre installation files.

1.14 OPC Bridge

Sites already using the OPC Bridge should upgrade the OPC Bridge to version vOB7.0.0.3, located in the "OPC\OPC Bridge 7.0.0.3" folder of the Command Centre installation files.

In addition to upgrading OPC Bridge to vOB7.0.0.3, sites will need to apply a patch, as instructed in **OPCBridge.dll Release Note.pdf**, also located in the "OPC" folder.

1.15 Gallagher Controller API compatibility

Version vEI8.10.019 of the Gallagher Controller API (FTCAPI) is compatible with version vEL9.40 of Command Centre and vCR9.40 of Controller 6000.

1.16 Morpho Biometric Integration

A CompressFingerprints Utility, providing the ability to compress and store biometrics on the server, is now available. If required, refer to **CompressFingerprints Utility Release Note.pdf** (in the **Morpho Utilities.zip** of the Command Centre installation files) for further details.
Notes:

- Upgrading to Command Centre vEL9.40 will not be possible if you have IDEMIA Legacy (MA2G) devices configured. MA2G readers are no longer supported from Command Centre vEL9.30 or later.
- If your site wants full CAPSS compliance, (and has `NPSA=1` in the licence file), Morpho should not be installed, otherwise your site will not comply with CAPSS 2024.

Copyright © Gallagher Group Limited

1.17 Schlage AD Series locks

Schlage AD Series door modes are supported on AD devices from v9.00. To make sure this feature works correctly:

1. Update Command Centre to vEL9.40.
2. Update the Controller software to the latest version.
3. Once all updates are complete, right-click on the AD Lock and click **Push Configuration**.
4. Right-click on the Alarm Zone and click **Push Configuration**.

1.18 Key Device alarm changes

From version vEL7.00, for sites with two key devices in the license file, if either key device is removed an alarm will be generated after 6 hours, and thereafter every hour until either the key device is returned or the licence file updated. The same alarm is used for removal of either the first or second key device. This alarm is hard-coded and cannot be altered via Action Plan configuration. The alarm details will indicate whether the alarm being generated is for the first or last key device. The site will only go into 'read-only' mode when both key devices have been removed for 30 days.

1.19 Visitor Management

Visitor Management Service was merged into Command Centre Service on vEL8.20 (or later) Command Centre upgrade. Sites using Visitor Management will have the FT Visitor Management item reported offline and this can be manually removed from the Services and Workstations Master List Window.

Note: Cardscan components will not be available if your site installs Command Centre with `NPSA=1` in the licence file.

1.19.1 Visitor Management OCR Passport/Drivers License Interface

The 'Visitor Management OCR Passport/Drivers License Interface' allows the Gallagher Visitor Management Client to support an interface to both the ScanShell 1000B and SnapShell Passport Scanners. The "Visitor Management Passport/Drivers License Scanning Process" topic in v9.40 of the *Gallagher Command Centre Configuration Client User Guide* (part number C209000) covers the procedure for installing these scanners. However, for sites already using the ScanShell 1000B Scanner that want to move to the newer SnapShell Passport Scanner, refer to *"Appendix C: Upgrading from ScanShell 1000B to SnapShell Passport Scanners"* for the procedure.

1.20 Customisations

If your site currently has a Gallagher Command Centre customisation installed, you will need to uninstall the customisation before installing this version (vEL9.40), and then reinstall the customisation after the upgrade if it is still required. Likewise, you need to remove any Controller customisations, (**dlls**) from your Controllers before upgrading.

Note: Check with Gallagher Security Technical Support to ensure there is a new version of the customisation available before upgrading.

If your site currently has a customisation installed, upgrade Gallagher Command Centre as follows:

1. If the customisation has Controller DLLs, remove them from the Controller(s).
2. Use CCFTServiceManager to stop the Command Centre Services.
3. Uninstall the customisation using the Windows **Programs and Features** utility.
4. Upgrade Gallagher Command Centre to version vEL9.40 from the installation files, using the *Upgrading to vEL9.40 from a previous version* procedure on page 10.
5. Upgrade the Controller 6000 software to vCR9.40.
6. Install the new version of the customisation you have been provided.
7. For any of the Elevator HLI customisations, select the type of elevator system protocol on the **Advanced** tab of the Elevator HLI. Refer to the "Configuring High Level Elevator Interfaces"

Copyright © Gallagher Group Limited

topic in v9.40 of the *Gallagher Command Centre Configuration Client User Guide* (part number C209000) for the procedure.

8. Re-run the Click-Once builders (Command Centre Client and Configuration Client).

Note: Refer to the specific customisation release note regarding methods for upgrading the clients.

1.21 IP Alarms Receiver compatibility

Monitoring stations running v1.0.1.9 of Gallagher IP Alarms Receiver Software will not be able to import keys from vEL9.40 of Command Centre. Please ensure the monitoring stations have upgraded to the latest version of IP Alarms Receiver. Refer to the "IP Alarms Receiver Software Release Note vx.x.x.pdf" for further details.

1.22 Jacques Video Stream

If you are upgrading Jacques Video to vEL9.40, and you have been using VLC 1.11.1, please uninstall VLC 1.11.1 unless you are using that VLC instance for another purpose.

1.23 MIP Plugin Feature

The Gallagher Milestone MIPS Extension must be uninstalled before upgrading to Command Centre vEL9.40. For more information about upgrading the MIP Plugin feature to vEL9.40, refer to the *"Release Note MIP Plugin (v2.0)"*.

1.24 UL Installations

Refer to the document *"Gallagher Command Centre Underwriters' Laboratory Inc. - Configuration Requirements"* (part number 3E2793) for details covering specific requirements needed to meet the specified UL Licenses. Installers must ensure these instructions are followed to ensure the installed system is UL compliant.

1.25 Managing keys for MIFARE credentials

A new "Manage Keys" operator privilege was introduced in vEL8.40 to perform the following:

- Change/import/export site keys
- Start/stop migration
- Encode admin cards
- Change/import/export Morpho biometric type keys
- Change Salto keyset and Configure Encryption Override

Any operators currently with the "Edit Site" operator privilege needing to perform these actions will need the new "Manage Keys" privilege added to them, as the ability to perform these actions has been removed from "Edit Site". Operators with the "Edit Operator" privilege in the Root Division (or Advanced User, or the System Operator) will be able to grant the new "Manage Keys" privilege.

1.26 Commend Intercoms

Once you upgrade to v9.40, any previously configured Commend Intercom Viewer(s) will be converted to new Intercom Viewers, (i.e. if your site had two Commend Intercom Viewers prior to upgrading you will end up with two Intercom Viewers).

1.27 Other files installed

Other files included with the Command Centre installation files are:
Gallagher Controller - vCR9.40.251031b.gglsec

Copyright © Gallagher Group Limited

2 Upgrading to vEL9.40 from a previous version

This version of Gallagher Command Centre is supported on upgrades from any full release version of Gallagher Command Centre from vEL9.00 onwards.

This version of Command Centre no longer supports GBUS devices. All GBUS devices need to be replaced with HBUS devices to allow upgrading to vEL9.40

Notes:

- All legacy Controllers, (i.e. 5000GL, 5000, 3000-8R and 3000-4R) and local bus devices, (e.g. Relay Interface, Prox Readers) are unsupported from version vEL8.50 onwards.
- Serial/Dial-up network connection is unsupported for all Controllers from vEL8.50 onwards. Ensure all Controllers communicate via a LAN before upgrading.
- The license file will be placed in the C:\ProgramData\Gallagher\CommandCentre directory.
- If you have a pre-vEL8.50 license file, when you upgrade to vEL9.40 Command Centre will not restart. A valid license file must be ready before upgrading.
- The Gallagher Command Centre CA certificate is copied from the Gallagher Database into the Trusted Root certificate store for New Installs, Upgrades and when the Recovery tool is used. The Gallagher Command Centre CA certificate is used for Mobile Client authentication and can be safely removed if the Mobile Client is not utilised on site.

IMPORTANT:

- **To ensure a complete Gallagher Command Centre Server installation, be sure to run the installation directly from the Command Centre installation files, and do not do a Server install of Gallagher Command Centre over the network.**
- **The Command Centre Installer (setup.exe) now supports command line parameters. For further details refer to *Release Note Command Centre Installer Command Line Support* (located in the 'Release Notes' directory of the Command Centre installation files).**

2.1 Before you begin

IMPORTANT:

- Sites using workstation or operator restrictions will need to generate a code to authenticate their workstations after upgrade. Sites using Click-Once will need to run the workstation certificate utility. Refer to *"Appendix D: Client Authentication"* for further detail.
  Note: If this has been done on a previous upgrade, you do NOT need to do it again, (i.e. it only needs to be done once).
- From v8.20 onwards, Controller 6000s use a Linux operating system and there is no option to opt out or downgrade to pre-v8.20 WinCE version. Refer to the "Controller 6000 Release Note" for further detail on upgrades.
- Command Centre version vEL9.40 requires .NET version 4.8 or later to be installed.
  .NET requires Windows administrative permission to be installed on the workstation or server. For the server and workstation upgrade, the Command Centre installer will install .NET 4.8 if there is not a .NET existing already or the .NET is older than 4.8. For Click-Once Deployment users that don't have Windows administrative permission on their workstation it is advised to install .NET 4.8 prior to upgrade.
  .NET 4.8 can be found on the Command Centre installation media at:
  \Setup\SQLInstall\ ndp48-x86-x64-allos-enu.exe

- Ensure your server machine has one of the supported Windows operating systems, with the appropriate Service Packs, installed before upgrading.
- You must be logged on as an Administrator.
- All Command Centre clients (including those logged on via terminal services) should be shut down prior to upgrading the server.
- We highly recommend you perform an Archive, and then perform a backup of the Central database after the Archive.

Copyright © Gallagher Group Limited

- Check that your **Power Options** (from the Control Panel) have system 'standby' and 'hibernate' set to "Never".
- Ensure that the Windows Event Viewer (via **Control Panel** > **Administrative Tools**) is closed before upgrading.

2.2 Upgrading the Server

Note: The client authentication feature was introduced in v8.20. If you have Workstation Restrictions enabled then you will need to spend extra time upgrading the workstations to ensure they are properly registered to the Server. These actions will only need to be performed once, and an additional step is required for Click-Once workstations to install a client certificate. Refer to *"Appendix D: Client Authentication"* for further detail.

Running the certificate utility on all of the restricted Click-Once workstations prior to upgrading the server can reduce down time and inconvenience, (i.e. if the certificate exists prior to upgrading the server then only the registration code needs to be done).

1. Ensure all applications are closed before beginning an upgrade, and stop the multi-server communication within Command Centre.
2. Backup the databases using 'Backup Central' and 'Backup Event' in CCFTServiceManager.
3. Exit CCFTServiceManager before running **Setup.exe**.
4. Locate and run **Setup.exe**.
   The installation wizard will show you that an upgrade is taking place.
   Note: If you **Exit** the installation wizard at any point, Command Centre Services might go into a 'Disabled' state. This is normal behaviour for a system upgrade.
5. After the Install initialises click the **Next** button to proceed.
   Note: The following screen will display if the installer detects that files which need to be shut down as part of the install are currently in use by processes running in the system.



If this screen does display, we recommend you restart the machine. However, if feasible, you can try closing the application(s) listed and then click the **Refresh** button.
Once there are no application(s) using Command Centre files the status message at the top changes to *"There are no applications using files which will be installed by Command Centre. The installation can proceed".* Click the **Next** button.

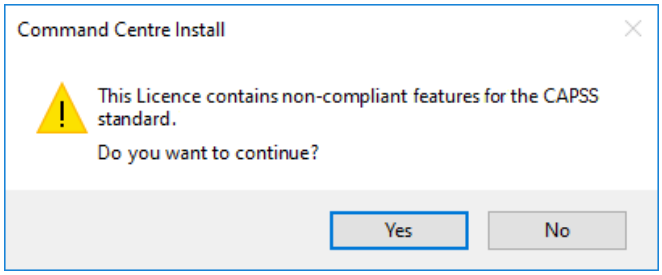
Copyright © Gallagher Group Limited

6. Check the tick box to accept the Master Software License and Maintenance Agreement and click the **Next** button.
   Note: A softcopy of the Master Software License and Maintenance Agreement is available in the `'Documentation'` folder of the Command Centre installation files.
7. Ensure you fully understand that Controllers will be restricted to a maximum of 10 connected doors, and that upgrading without the correct license may affect the system. Once reviewed, check the box to accept, and click the **Next** button.
8. Check the right **Server Components** are selected for a Server upgrade.
   Note: Only check the "Intercom Server" option if your site is going to use this feature. Likewise, only check the "Visitor Management Server, Client and Kiosk" option if your site is going to use the Visitor Management feature. Cardscan components will not be available if your site installs Command Centre with NPSA=1 in the licence file.
9. Gallagher Command Centre consists of two clients, (i.e. Configuration Client and Command Centre Client). The **Create network share for client setup** checkbox applies to both clients.
   Do you want a network share for Command Centre Client created as part of the upgrade?

If…	then ensure the 'Create network share for client setup' checkbox is…
no	unchecked. This allows you to create the network share manually with the privileges you want. Refer to *"Appendix A: Alternative Client Deployment Options"* for the procedures. **Note:** Choose this if you will always use the Workstation Installer.
yes	checked. This automatically installs server and client components and runs the Click-Once Builder so that the client is ready to be installed from a network share on the Command Centre server machine.

10. Select your new license file for version vEL9.40, and click the **Next** button.
    Note: The license file MUST be vEL8.10 or later, otherwise Command Centre will not restart until the license file is updated.

    Does the following message pop-up display?



If…	then…
yes,	this is because your license file contains both `NPSA=1` and `Sagem Fingerprint Readers=nn` (for Morpho components). Go to Step 11.
no,	the Windows Firewall Configuration screen displays. Go to Step 12.

11. If your site wants full CAPSS compliance, Morpho components (which are not CAPSS compliant) should not be installed.
    Does your site want full CAPSS compliance?

If…	then…
no,	a) Click the **Yes** button. The message pop-up closes. b) Click the **Next** button until the installation starts.
yes,	a) Click the **No** button. The message pop-up closes.

Copyright © Gallagher Group Limited

If…	then…
	b) Replace the license file with one that has `NPSA=1` but no `Sagem Fingerprint Readers` defined. c) Click the **Next** button until the installation starts.

12. Click the **Next** button on the Windows Firewall Configuration screen.
13. On the Service Account screen, click the appropriate radio button to define the Windows account which Command Centre services will run as.



Notes:

- If you select **Use a custom service account**, you must enter a Username and Password of an active Windows account, and the account must have privileges to run as a service.
- When using a custom service account, if you are installing and using the BootP server, the account must be a member of "Network Configuration Operators" or local administrator, otherwise BOOTP will fail and the Controller will not come online.
- EDI imports may fail if the service account does not have permissions to move the file out of the incoming folder.

14. Click the **Next** button to proceed with the installation and wait while Command Centre installs.

Notes:

- A restart of the PC may occur. If so, the install should continue once the PC restarts, however if not, you will need to re-run the Installer.
- The upgrade of the databases occurs at this point. Therefore, it can take a significant amount of time depending on the size of your databases.
- A warning message may display if your site has a large amount of redundant change sets that will affect your system performance. If so, complete the upgrade and contact Gallagher Tech Support so they can run the **CleanupCardholderPDFChangeSet** utility for you.

15. Once Command Centre has finished installing, the Completion screen of the Install wizard displays.

Note: What appears on the Completion screen can differ, as follows:

- there will be either a **Finish** or a **Restart Computer** button depending on whether a restart is required or not, and
- if your site has customisations installed, the following message will display along with a list of the customisation(s):
  The version of Command Centre that you are upgrading was customised. Please install all licensed

Copyright © Gallagher Group Limited

Customisations before restarting the Command Centre services.
In this scenario, install the customisations and then restart the system.

Important: If a BETA warning message appeared during the upgrade, the word BETA will now appear on the title bars of the Command Centre Client and the Configuration Client. Please contact Gallagher Tech Support as BETA versions are only intended for installation on test sites.

2.3 Upgrading Workstations

Upgrade all workstation PCs using one of the following methods:
Notes:

- Command Centre version numbers comprise a major build version and a minor build version, (e.g. for version vEL9.40.nnnn, 9.40 is the major build and nnnn is the minor build).
  Server and workstation major builds must always match, however the minor build on the workstation can be equal to or lower than the server minor build. When Command Centre is launched, if the minor build number is newer than the server, logon will fail and the message "*The client version is incompatible with the server. Startup failed!*" will display.
- There are alternative methods of installing the Command Centre Workstation. Refer to *"Appendix A: Alternative Client Deployment Options"* for details of the other options.
- Client Authentication verifies that a Workstation is what it claims to be, using a Client Certificate installed on the Workstation machine. If your site is using Workstation Restrictions, all Workstations except for the server workstation will need to be registered with a registration code after installation. Refer to *"Appendix D: Client Authentication"* for further detail.

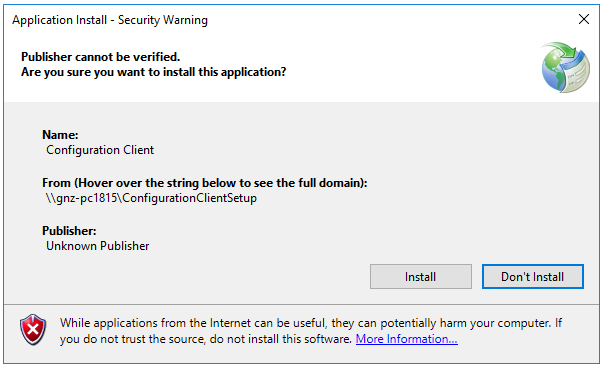
Upgrading Command Centre or Configuration Client via Click-Once Application

Notes:

- **Important:** Ensure you have .NET version 4.8 or later installed before upgrading Command Centre or Configuration Client on workstations using Click-Once.
- When upgrading any Command Centre applications with version vEL8.00 and below and the Click-Once method is preferred; previous fully installed applications will need to be manually un-installed as the Click-Once deployment will not remove/replace the old application.
- The Click-Once share folders must be accessible to the Windows users before deployment/re-deployment.
- When running up any Click-Once applications, Click-Once will automatically update any previously deployed applications and include customisations, patches, upgrades, etc, provided the Click-Once clients have been rebuilt at the server (see *"Appendix A: Alternative Client Deployment Options "* for further details).
- The Click-Once applications must deploy and install/update for every user on the same workstation. Each deployment takes approximately 300-400Mb.

1. If upgrading Configuration Client applications from version vEL8.00 and below, manually un-install the old applications.
2. From the client machine, browse to the appropriate server share:
   '\\ServerName\CommandCentreSetup', OR '\\ServerName\ConfigurationClientSetup'
   Note: If the server's full name differs from its short name, the short name has to be used to access the server's shared deployment folder.
3. Run the Command Centre or Configuration Client Click-Once Application **setup.exe**.
   An Application Install Security Warning screen displays.

Copyright © Gallagher Group Limited



4. Click the **Install** button.
   The Command Centre Client or Configuration Client installs.

The Click-Once installation places a shortcut to the runtime files in the users application directory with a shortcut in the Start Menu. Upon opening the shortcut the Click-Once application checks the files on the server vs the local files. If it finds a change it will re-download the server files, otherwise it just runs the local files.

Upgrading Command Centre or Configuration Clients via Workstation MSI

Notes:

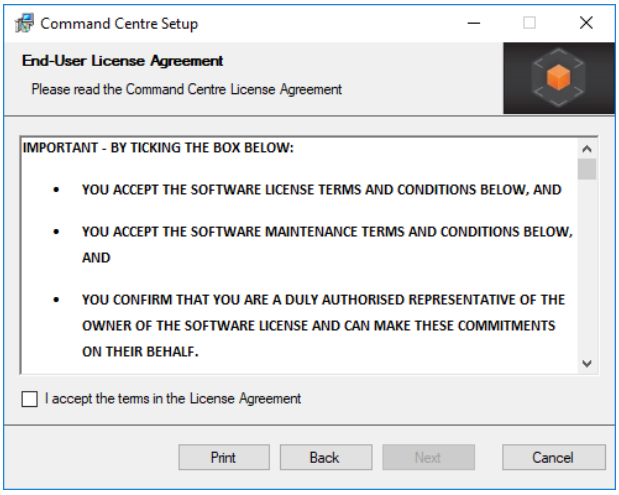
- The Server automatically includes the workstation clients, so this procedure is only needed for installing on other workstation machines.
  Important: This procedure cannot be performed on the machine the Server is installed on.
- Any customisations, patches, etc will need to be manually applied to each workstation after the applications have been installed.
- Using MSI installer means that Command Centre applications only need to be installed once and then it is available for all users to the same PC. This is unlike the Click-Once application which requires the client to be installed for every user on the same workstation.

1. Copy the 'Workstation' folder from the server onto the Workstation PC, and run **Setup.exe**
   Note: This will automatically remove any previously installed workstation on upgrade.
   The Welcome screen of the Command Centre Setup Wizard displays.

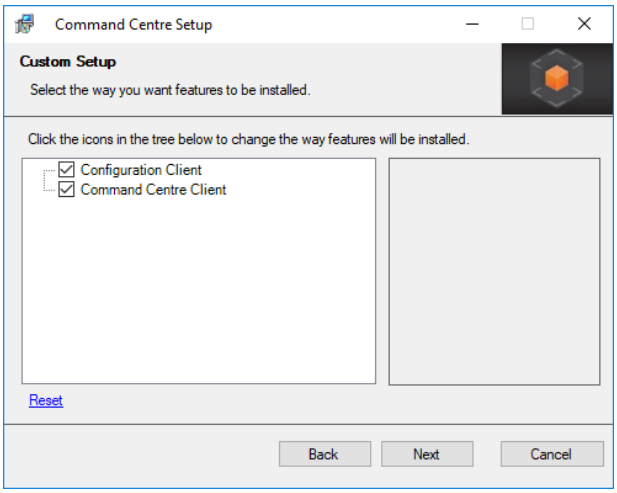


2. Click the **Next** button.
   The End-User License Agreement screen of the wizard displays.

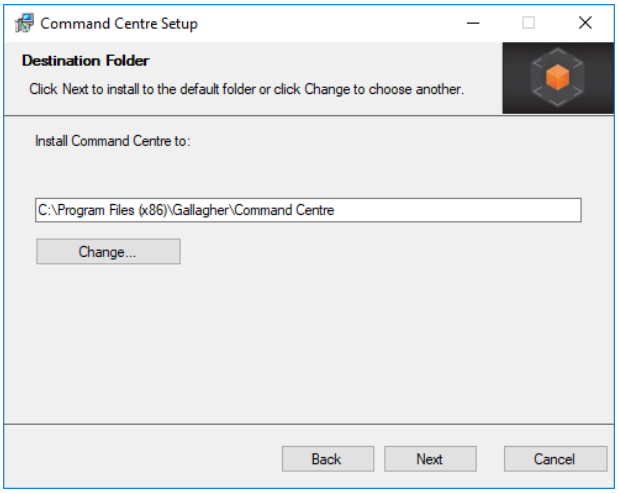
Copyright © Gallagher Group Limited



3. Ensure you fully understand the terms and conditions listed in the License Agreement you are about to enter into, and check the box to accept.
4. Click the **Next** button.
   The Custom Setup screen displays.

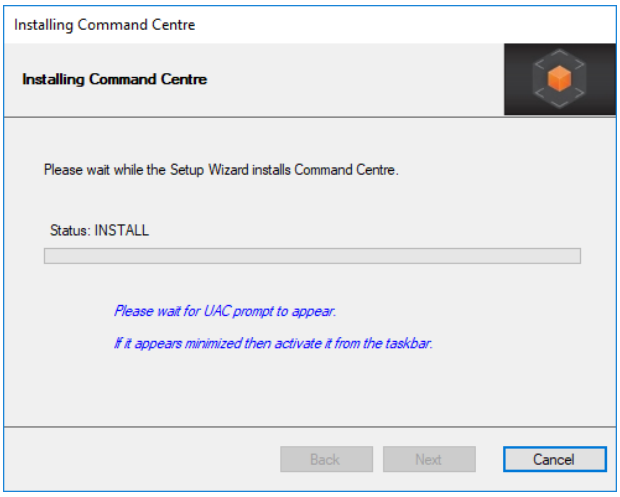


5. By default, both the Command Centre Client and the Configuration Client will be installed. Deselect a Client if you do not want to install it.
6. Click the **Next** button.
   The Destination Folder screen displays.

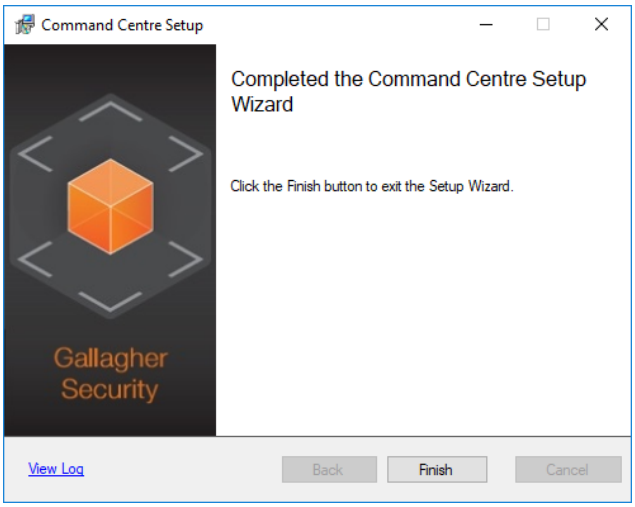


Copyright © Gallagher Group Limited

7. The **Change…** button can be used if you want to change the location of where Command Centre will be installed. Otherwise, use the default location and click the **Next** button.
   An install screen displays indicating the progress of the install.



   Once the installation is complete, the Completed screen of the wizard displays.
8. Click the **Finish** button.
   A shortcut for the clients selected on the Custom Setup screen appear on the desktop.



9. Run any customisation upgrades and/or apply any necessary patches, etc.
10. Repeat Steps 1 - 8 as necessary for all other workstations.

2.4 Upgrading Gallagher Controller 6000s to vCR9.40.xxxx

It is possible that the Controller 6000s that have been installed on your site will have a different version of software loaded on them. The version of Controller code you use needs to be compatible with the version of Gallagher Command Centre you have running, (e.g. vEL9.40.xxx of Command Centre requires vCR9.40.xxxxxx of Controller code).

The installer will block an upgrade for sites with pre-vEL7.10 controllers. Therefore, sites that are upgrading controllers running firmware earlier than v7.10, and require those controllers to communicate with each other during upgrading, should upgrade the group of controllers to a version later than v7.10 first before upgrading to the latest version.

To get your Gallagher Controller 6000s running the latest version of code, perform the upgrading procedure described in the *Gallagher Controller 6000 Release Note* (for version vCR9.40.xxxxxx).

Copyright © Gallagher Group Limited



Important Controller 6000 v9.40 upgrade note

Controller 6000s running vGR8.10.179 onwards can be migrated directly to Linux which could take up to 4 minutes. Controllers with older than vGR8.10.179 software will go through a two-step upgrade which could take up to 7 minutes.

Rollback a partial upgrade for any reason:

Gallagher has extensively tested the Controller Linux OS upgrade process and is confident the majority of sites will not require a rollback of Controller code back to WinCE OS if they follow the upgrade instructions. However, Gallagher Technical Account Managers can be engaged to help manage sites with special requirements, (e.g. sites with test systems upgrading and downgrading physical Controllers as part of a test process) to meet their process needs.

Dual authorisation and anti-passback behaviour:

From 7.70 onwards, dual authorisation and anti-passback are based on cardholders, not credentials. This is to ensure a cardholder using more than one credential, (e.g. a card and mobile credential), will be seen as a single person.

Copyright © Gallagher Group Limited

3 Gallagher Command Centre Rollback Procedure

The following assumes that the site upgraded from a previous version using the procedure entitled "Gallagher Command Centre Upgrade Procedure to vEL9.40". It is also assumed that the site after a short period of time has decided to rollback to the previous version of Gallagher Command Centre. Any changes made to the configuration of the site whilst running vEL9.40 WILL BE LOST from the head-end configuration database when this rollback is performed. Any events that occur during this period will also be lost. It is recommended to run an Activity Report on all events to file so they can be searched for this period if required. This is because the last backup taken under the previous version will be used as the starting point for future configuration after this procedure is completed. Unfortunately, any changes made to the configuration of the site whilst running vEL9.40 WILL NOT BE LOST from the Gallagher Controllers and this creates an inconsistency. Gallagher suggest that the decision to rollback is made prior to any configuration changes being made.

IMPORTANT: Controller rollback to a WinCE operating system is not possible. Refer to the "Controller 6000 Release Note" for further detail.

3.1 Downgrading the Server, Workstations and Controllers to a previous version

1. Shutdown all workstations ensuring CCFT.exe is no longer in the task manager process page. To get to the process page:
   a) Press '**Ctrl-Alt-Del**' on your keyboard.
   The Windows Security dialog displays.
   b) Click the **Task Manager** button.
   The Window Task Manager dialog displays.
   c) Click the **Processes** tab.
2. Stop all the Command Centre Services using either Command Centre Service Manager or the Services window, via **Control Panel** > **Administrative Tools** > **Services**, i.e.
   - FT Bootstrap Protocol Service
   - FT Command Centre Service
   - FT Controller Service
   - FT Import - Export Service
   - FT Intercom Service
3. Using the Windows **Add or Remove Programs** utility, remove "Gallagher Command Centre" and "Visitor Management Server".
4. Choose to delete the databases and restart the PC when requested.
5. Delete the Visitor Management Click-Once folder, (usually in c:\Program Files\Gallagher\ Visitor Management\VM Client\VM Client Update).
6. Install the required previous version of Gallagher Command Centre Server software by following the instructions in the appropriate Release Note, (e.g. vEL7.40).
7. Once you have completed the install and closed the install wizard, (i.e. either by clicking the **Finish** or **Restart Computer** button, the Gallagher Command Centre services will have restarted. These need to be shutdown using the same procedure as used in Step 2.
8. Did you detach and copy the databases during the upgrade to vEL9.40?

If...	**then...**
no	a) If required, install Visitor Management and run the VM Click-Once executable, (i.e. **ClickOnceVisitorManagementSetup.exe**). b) Run the CCFT Restore and point it to your backup of the Central database.

Copyright © Gallagher Group Limited

If...	then...
yes	a) If required, install Visitor Management and run the VM Click-Once executable, (i.e. **ClickOnceVisitorManagementSetup.exe**). b) Use CCFTServiceManager to detach all databases from the original location, by clicking **Database** > **Detach** from the context menu. c) Copy the database files (CCFT*.mdf and CCFT*.ldf) from the backup location and paste them to the active "Data" directory for the site (this may be in "C:\Program Files\Gallagher\ Command Centre\DATA" depending on the site). d) Use CCFTServiceManager to attach all databases from the original location, by clicking **Database** > **Attach** from the context menu (ensure this batch file has been edited to point to the same active "Data" directory as used above). e) If after running and attaching the database, ccft service does not start, then: 1. Run "CCFTRecoveryCode" from the BIN folder and use the recovery code that you have previously saved before upgrading to a Command Centre version. 2. Import the old recovery code using the **Enter a code for command center to use** button. 3. Restart the services again.

9. Restart all the Command Centre Services.
10. Start-up the Gallagher Command Centre Configuration Client workstation software on the server and logon. Check the hardware window shows your correct site name and that your Gallagher Controllers are all online.
11. On each workstation on the network, uninstall the vEL9.40 workstation software using the Windows **Add or Remove Programs** utility and remove "Gallagher Command Centre".
12. Restart each workstation when requested and then install the required previous version of Gallagher Command Centre Workstation software by following the instructions in the appropriate Release Note, (e.g. vEL7.80).
13. Restart the workstation PC when requested and logon to the system.
14. Reinstall Visitor Management from the Click-Once directory.

Copyright © Gallagher Group Limited

Appendix A: Alternative Client Deployment Options

These alternative client deployment options apply only to the Gallagher Command Centre client and the Configuration Client. Use the option suitable for your requirements:

- File Server as a Deployment
- MSI Installation
- XCOPY Deployment
- Installing using Command Prompt (intended for SysAdmins)

Note: It is important you only install using **one** of the client deployment options, otherwise you could end up with two copies of the application installed.

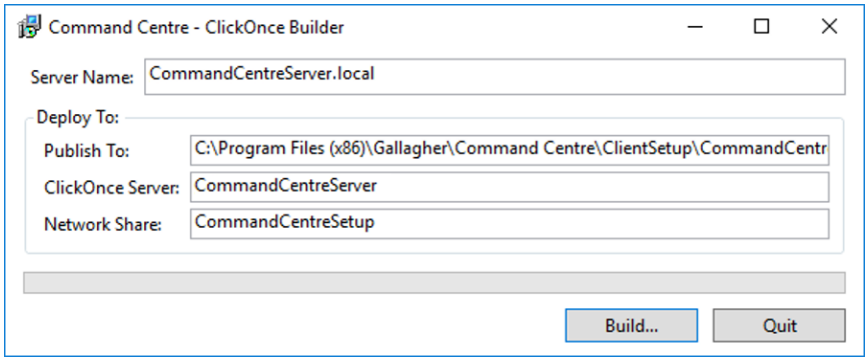
File Server as a Deployment

This option allows the client deployment to be setup on either the Command Centre Server or any other file server, as follows:
Note: This option can be used on the Command Centre Server if you want to control privileges and share location.

1. Browse to the Command Centre server's appropriate setup folder for the client you want to install, as follows:

For…	go to C:\Program Files (x86)\Gallagher\Command Centre\…
Command Centre Client,	ClientSetup
Configuration Client,	ConfigClientSetup

2. Run the Click-Once executable, (i.e. **Click-OnceBuilder.exe**).
The Click-Once Builder screen displays. The example below is for the Command Centre Client.



3. The following fields should auto-populate. If they do not, or if you wish to have a file server other than the Command Centre Server for deployment of the application then modify as appropriate.

Server Name: Fully qualified domain name of deployment server - *CommandCentreServer.local*

Publish To: Full local path of the folder that will host the deployment files - *C:\Program Files (x86)\Gallagher\Command Centre\ClientSetup\CommandCentreSetup*

Click-Once Server: Short name of server – *CommandCentreServer*
Note: Click-Once supports deployment via a file server. You can specify a URL instead of a machine name for the **Click-Once Server** name.

Network Share: The folder that the Click-Once runtime files are built up in - *CommandCentreSetup*

4. Click the **Build** button.
The application may take a few minutes. Once finished, a message displays at the bottom of the Click-Once Builder screen to indicate that it built successfully.

Copyright © Gallagher Group Limited

5. Ensure the folder in the **Network Share** field is shared.
   Modify the properties of this folder directly so it is accessible by using the UNC path derived from 'Click-Once Server' and 'Network Share' e.g. *\\CommandCentreServer\CommandCentreSetup*.
6. Click the **Quit** button.
   A shortcut for the client you installed appears on the desktop and the Logon screen displays.

Note: To upgrade the file server you simply perform the same steps as for a clean install. Once the files in the network share location are updated the client will be automatically upgraded the next time it starts.

MSI Installation

The Command Centre clients can be installed after first installing the server.

The installation files can be found in the Workstation folder of the server installation:
'Program Files (x86)\Gallagher\Command Centre\Workstation'

Copy that folder to your workstation machine, and run **Setup.exe** inside the Workstation folder.

XCOPY Deployment

This option allows you to install the client manually, (i.e. without using the Command Centre Installer or Click-Once), as follows:
Note: In a multi-server environment, this is the appropriate option as it allows you to have multiple copies of the client on a workstation, all pointing to different servers.

1. Install .NET 4.8 (located in the 'SQLInstall' folder of the Command Centre Installation files) on the client.
2. Copy the 'Client' and/or 'ConfigClient' folder from the server's install folder, (e.g. C:\Program Files\Gallagher\Command Centre), to the client machine.

   Note: The 'Client' folder is also located in the 'ClientSetup' folder of the Command Centre installation files. However, if you copy the folder, you will need to replace the 'localhost' with the name of the server in the client's configuration file (**CommandCentreClient.exe.config**) before the client will be able to connect.
3. Double-click the **CommandCentreClient.exe** in this folder to start the client.

Notes:

- For convenience, you might want to create a shortcut to **CommandCentreClient.exe** so you do not have to locate it each time.
- The client must be manually upgraded by replacing the old client files with the ones from the upgraded server, (i.e. upgrade the server and repeat Step 2 above).

Installing using Command Prompt (Intended for SysAdmins)

This option allows you to install a Command Centre workstation without user interaction, which may be useful for automated installs, as follows:

1. Copy the 'Workstation\Setup' folder from 'Program Files(x86)\Gallagher\Command Centre'.
   Note: If deploying MSI, configuration files need to be included.
2. Run the appropriate command line for the client(s) you want to install. For example:

   Command Centre client only:
   msiexec /q /i Workstation_8.10.946.msi ADDLOCAL=PremierClient

   Configuration client only:
   msiexec /q /i Workstation_8.10.946.msi ADDLOCAL=ConfigClient

   Both clients:
   msiexec /q /i Workstation_8.10.946.msi ADDLOCAL=PremierClient,ConfigClient

Copyright © Gallagher Group Limited

Appendix B: SQL Database Installation on a separate Server

Prerequisites

- Command Centre requires SQL Server 2016 SP2 or later.
- SQL Server must be configured to allow remote connections.
- Firewall settings on the SQL Server computer must allow a networked computer to connect to SQL Server (see *"How To: Configure a Windows Firewall for Database Engine Access"* at http://msdn.microsoft.com/en-us/library/ms175043.aspx).
- Server collation should be set to **Latin1_General_100_CI_AI**.
  Note: Server collation should previously have been set to **SQL_Latin1_General_CP1_CI_AS** or **Latin1_General_CI_AS**, but was changed in vEL8.90 MR2.

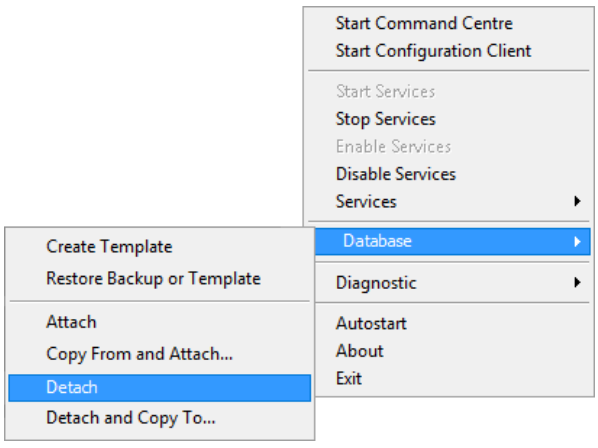
Restrictions

The following restrictions apply when Command Centre and SQL Server are run on separate servers:

- Restoring a database from within Command Centre is not supported.
- The Database Attach/Detach menus are unavailable in the Command Centre Service Manager.
- Archives are not impacted; the path of Archives is still relative to the Command Centre Server.

Moving SQL Database to a separate Server

1. On the Command Centre server, run the Command Centre Service Manager executable, (i.e. **CCFTServicemanager.exe**).
   By default it is installed under Program Files\Gallagher\Command Centre\Bin.
   The Command Centre Service Manager displays a small icon in the Windows System Tray with one of the following overlays to indicate its current state:
    Services Starting (blue arrow overlay)
    Services Started (green arrow overlay)
    Services Stopped (red square overlay)
2. Left mouse click on the Command Centre Service Manager icon and select **Stop Services**.
   Note: If the Command Centre services are not running then **Stop Services** will be disabled and this step can be skipped.
3. Left mouse click on the Command Centre Service Manager icon and select **Database** > **Detach**.



   Once the databases have been detached the message *"Database detach successful"* displays.
4. The Command Centre databases are now ready to be copied to another server. By default the

Copyright © Gallagher Group Limited

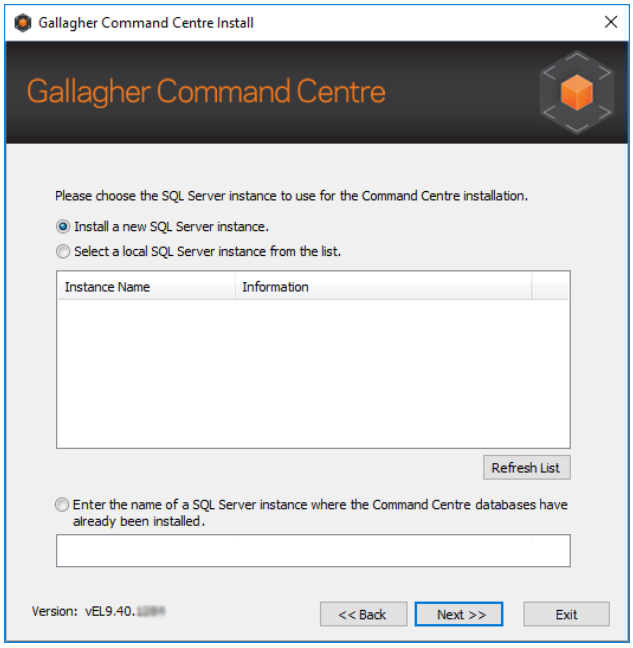
database files are stored under Program Files\ Gallagher\Command Centre\Data.
Copy **CCFTCentral.mdf** and **CCFTEvent.mdf** to your database server.

5. On your database server, start SQL Server Management Studio and login with an account that is capable of attaching databases. Alternatively, use the **sqlcmd.exe** or **osql.exe** command line utilities.
6. In SQL Server Management Studio, either:
   a. Right mouse click the Databases folder in the Object Explorer and select **Attach**.
   b. Use the **Add** button in the Attach Databases dialog to locate and select the **CCFTCentral.mdf** database file.
   c. Under the Database Details section, (i.e. the lower half of the Attach Databases dialog), select the log file entry and click the **Remove** button.
   d. Click the **OK** button to attach the database.
   e. Repeat steps a. through d. for the **CCFTEvent.mdf** database.

   OR

   a. Open a new query.
   b. Run the following command to attach the **CCFTCentral.mdf** database (modify the file path as required):
      Create Database CCFTCentral on (Filename = 'C:\Program Files\Gallagher\Command Centre\Data\CCFTCentral.mdf') For Attach
   c. Run the following command to attach the **CCFTEvent.mdf** database (modify the file path as required):
      Create Database CCFTEvent on (Filename = 'C:\Program Files\Gallagher\Command Centre\Data\CCFTEvent.mdf') For Attach
7. Uninstall Command Centre from the PC (including removing the Databases), and restart the PC.
8. From the Command Centre installation files, locate and run the Command Centre installer, (i.e. **Setup.exe**) on the computer where you wish to install the Command Centre Server.
   Note: The account under which SQL Server is running must also have “read/write” permissions to these files. During Command Centre installation, this account requires “sysadmin” privileges. Once the installation has completed this can be reduced to “read/write” permissions.
9. Accept the license agreement and click the **Next** button.
10. Select the **Server Components** option, enter the path and name of your valid Command Centre License File, and click the **Next** button.
11. Check the option on the Windows Firewall Configuration screen if appropriate, then click the **Next** button.

Copyright © Gallagher Group Limited



12. Click the **Enter the name of a SQL Server instance…** radio button and enter the name of your SQL Server instance (where the Command Centre databases have been installed) in the text box below this option, as follows:

    <ComputerName>\<InstanceName>

13. Click the **Next** button, and go to Step 13 of the *Upgrading the Server and Workstations from a previous version* (earlier in this document) for the remainder of the installation procedure.
14. Continuing on the Command Centre server, left mouse click on the Command Centre Service Manager icon and select **Start Services**.
15. Once the Command Centre services are running, start the Command Centre Workstation to confirm that the system is operational.

Troubleshooting

If the Workstation is unable to connect to the Command Centre server, then check the following:

1. Open the Windows Services Console and look for the FT Command Centre Service.
2. Check the status of this service.
3. If the service is not running then start the service manually. If the service starts successfully then re-try the Workstation.
4. If the service was already or now remains in the Starting state for some time, then it is likely that Command Centre cannot communicate with or access SQL Server.
5. To verify this, open the Windows Registry and go to the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Gallagher\Command Centre key.
6. Set the StartupTraceOn and TraceOn entries to 1.
7. Wait for 30 seconds to allow the server to make further attempts to communicate with SQL Server.
8. Open Windows Explorer and navigate to the C:\ProgramData\Application Data\Gallagher\Command Centre folder.
9. Open the **Command_centre.log** file.

Copyright © Gallagher Group Limited

Appendix C: Upgrading from ScanShell 1000B to SnapShell Passport Scanners

Introduction

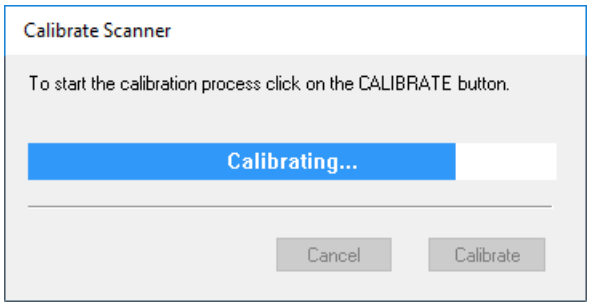
The ScanShell 1000B Passport Scanner is already supported by the 'Visitor Management OCR Passport/Drivers License Interface'. As of v7.60, the SnapShell Passport Scanner is now also supported.

For sites replacing their ScanShell 1000B Scanners with SnapShell Passport Scanners, this procedure describes how to perform the upgrade.

Procedure

1. Exit Command Centre and stop the Command Centre Services.
2. Uninstall the ScanShell SDK, (i.e. **CSSN SDK Version nn.nn.nn.nn**), using the Windows **Programs and Features** utility.
3. Browse to the `'Utilities\Visitor Management Drivers\Snapshell'` folder of the Command Centre installation files.
4. Run **SnapShellSilentInstallerForVMClient.bat**, and then click the **Install** button on each of the screens as they display.
5. Plug the SnapShell Passport Scanner into the PC.
   The Driver Software Installation screen displays.
6. Manually start the Visitor Management Client.
7. Go to the Visitor window and click the **Scan** button.
   Note: You require the "Edit Visits" operator privilege to scan.

   A message displays indicating that the scanner needs to be calibrated.
8. Place the calibration sheet provided with the scanner into the scanner.
   A Calibrate Scanner screen displays.
9. Click the **Calibrate** button.
   Calibration starts.



When the progress bar reaches 100% calibration is complete, and a pop-up message *"Calibration done successfully"* displays.

Note: The scanner needs to be calibrated before being used for the first time, and may need recalibrating if unplugged.

Copyright © Gallagher Group Limited

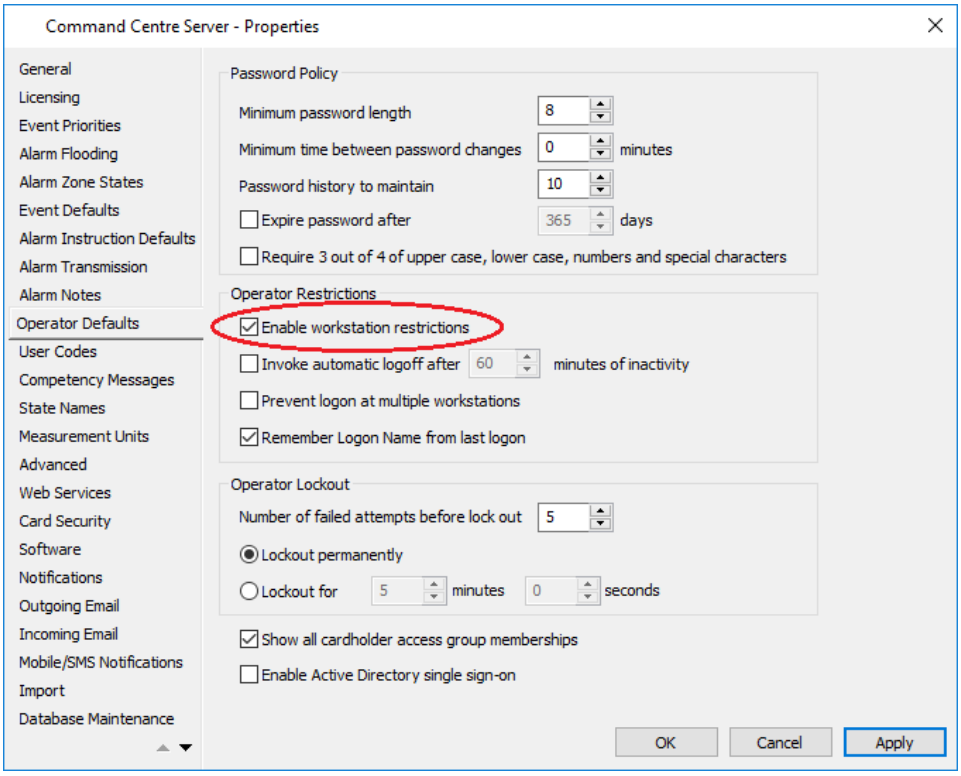
Appendix D: Client Authentication

Introduction

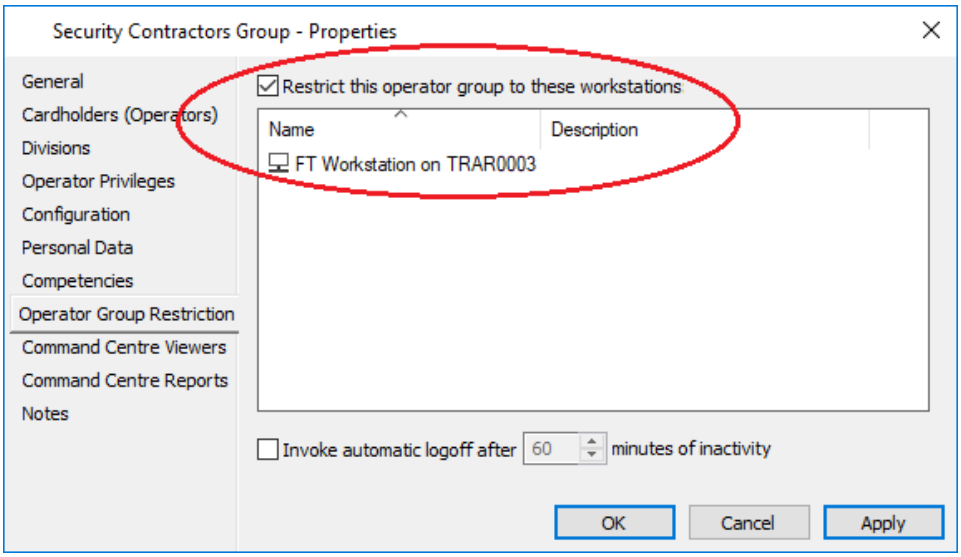
Client Authentication verifies that a connecting Workstation is what it claims to be, using a Client Certificate installed on the Workstation machine. This appendix provides a "step-by-step" guide to authenticating a workstation.

Note: This is only required if either:

- the Server Properties have been configured with workstation restrictions (on the **Operator Defaults** tab), OR



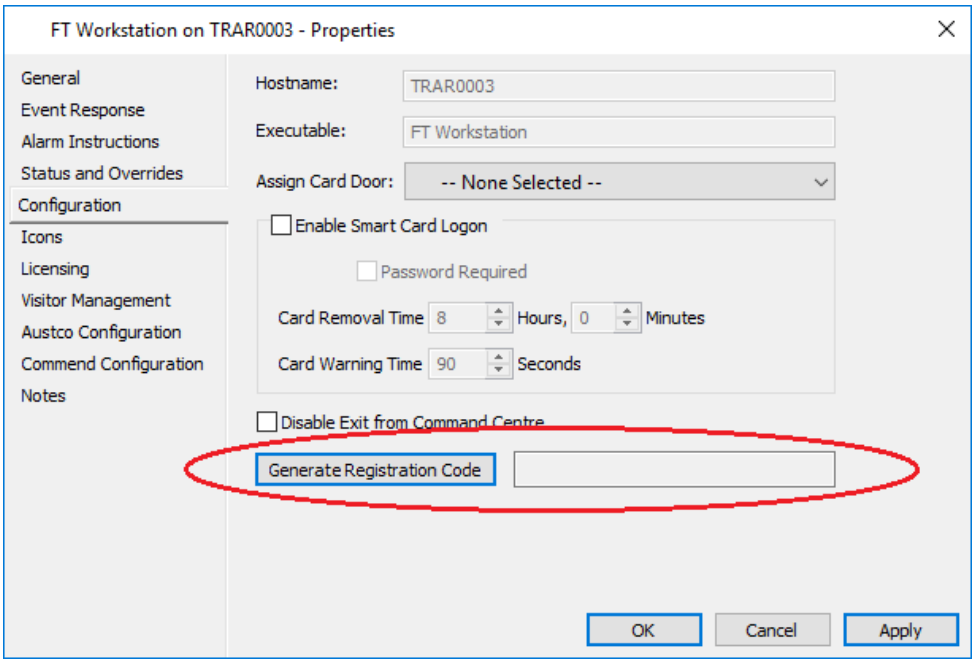
- the Operator Group has workstation restrictions enabled (on the **Operator Group Restriction** tab).



Copyright © Gallagher Group Limited

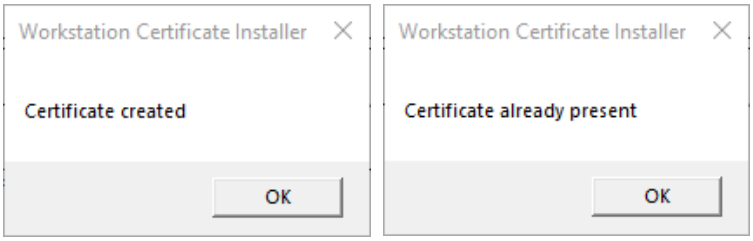
Click-Once all deployments

1. Logon to the Command Centre server and logon to the Configuration Client.
2. Click **Configure** from the menu bar, then **Services & Workstations**.
   The Services and Workstations Master List Window opens.
3. Open the Workstation and click the **Configuration** tab.
4. Click on **Generate Registration Code**.
   A random 5-digit code is created and stored on the server.



5. Note down the code (securely) as it will be used at the workstation itself.
6. Copy the **WorkstationCertificateInstaller.exe** from the "Utilities\Workstation Certificate Installer_8_20_5" folder of the Command Centre installation files to the respective workstation.
7. Run the **WorkstationCertificateInstaller.exe** as an administrator.
   A certificate will be applied in the newly created "Gallagher Applications > Certificate" folder.

   A pop up will appear to say it has been created. If there is a certificate already there then the app will pop up a message saying there is one already there.

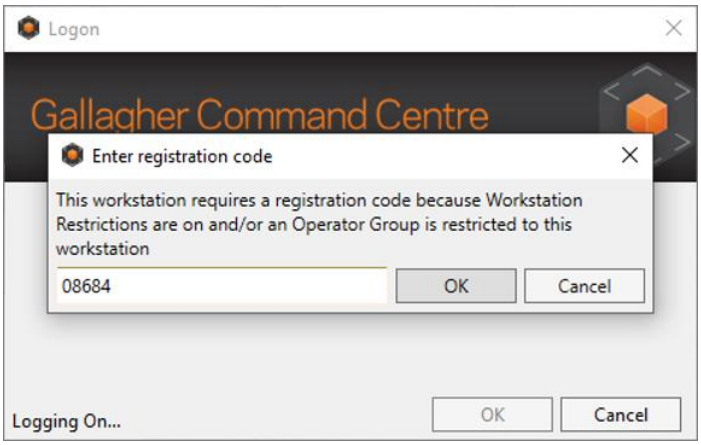


   Note: Running the Workstation Certificate installer on the Workstation will only need to be done once, as the Click-Once installer does not have the correct permissions to install a certificate itself.

8. Locate the shared ClickOnce installers. Located in \CommandCentreSetup for Command Centre Client and for Configuration Client setup.
   Run **ClickOnceCommandCentreSetup.exe** or **ClickOnceConfigClientSetup.exe** in the respective folders.
   The ClickOnce installers will successfully download and install to each user on the pc.

Copyright © Gallagher Group Limited

9. When you attempt to logon to either the Command Centre Client or the Configuration Client for the first time it will pop up a message (shown below).
   Enter the saved code generated from the server into the field and press **OK**.

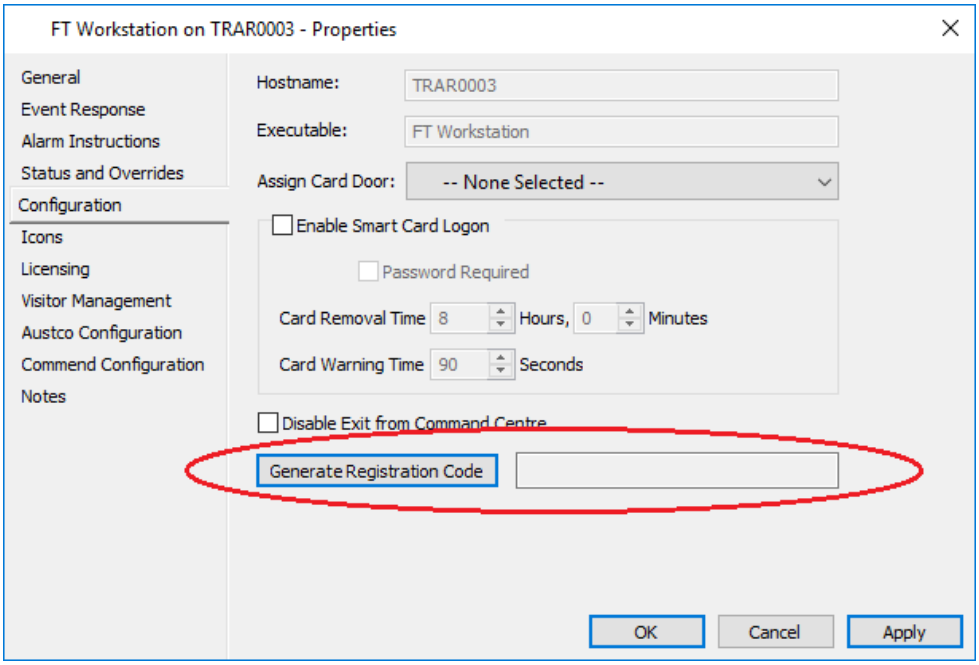


   Note: If an invalid code is entered 3 times then the generated code will become invalid and a new code will need to be re-generated on the server.

10. You can now log into the software as per normal.
    Note: This process only needs to happen on the first time you attempt to logon. It will not be needed thereafter.

Workstation installations

1. Logon to the Command Centre server and logon to the Configuration Client.
2. Click **Configure** from the menu bar, then **Services & Workstations**.
   The Services and Workstations Master List Window opens.
3. Open the Workstation and click the **Configuration** tab.
4. Click on **Generate Registration Code**.
   A random 5-digit code is created and stored on the server.



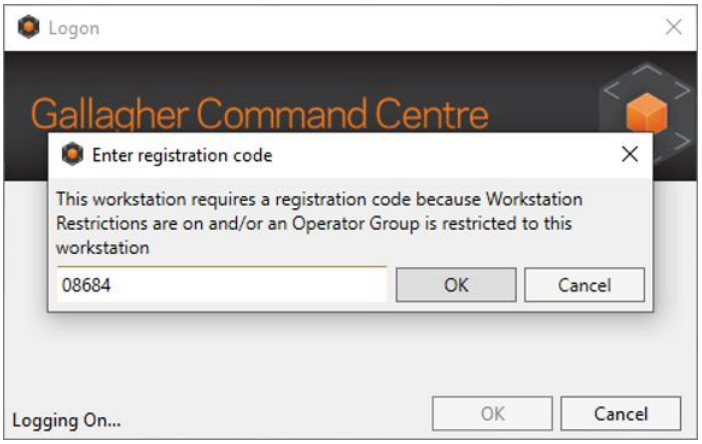
5. Note down the code (securely) as it will be used at the workstation itself.

Copyright © Gallagher Group Limited

6. The installation files can be found in the Workstation folder of the server installation, (i.e. 'Program Files (x86)\Gallagher\Command Centre\Workstation').
   Copy that folder to your workstation machine, and run **Setup.exe** inside the Workstation folder.

   Note: The Installer installs the select applications and creates a certificate as part of the Installer.

7. When you attempt to logon to either the Command Centre Client or the Configuration Client for the first time it will pop up a message (shown below).
   Enter the saved code generated from the server into the field and press **OK**.



   Note: If an invalid code is entered 3 times then the generated code will become invalid and a new code will need to be re-generated on the server.

8. You can now log into the software as per normal.
   Note: This process only needs to happen on the first time you attempt to logon. It will not be needed thereafter.

The workstation **Status and Overrides** tab is useful for determining if the workstation has been registered successfully. You can also De-register a workstation if the workstation has been physically changed or the client is re-installed; this allows a new workstation to be re-registered.

Status messages

This Workstation is offline	=	Workstation has previously been able to log into the server.
Normal	=	the workstation is currently logged in.
Not registered	=	Workstation has not successfully registered their certificate to the server.
Registered	=	Workstation has successfully registered their certificate to the server.
Waiting for registration code	=	The server is waiting for the generated registration code to be applied to the workstation.

Copyright © Gallagher Group Limited

Appendix E: Migrating SQL Server from 32-bit to 64-bit

Introduction

Command Centre no longer supports 32-bit SQL Server. This procedure describes how to migrate from 32-bit to 64-bit SQL Server.

Procedure

1. Exit Command Centre and stop the Command Centre Services.
2. Detach and backup the database.
3. Remember the Gallagher instance, "GALLAGHER" by default Command Centre install.
4. Uninstall 32-bit SQL from the Control Panel - Programmes and Features.
5. Install 64-bit SQL using the same instance name above (Step 3).
6. Attach the database using **CCFTServiceManager**.
7. Restart the Command Centre Services.

Copyright © Gallagher Group Limited

Appendix F:
Implementation of Controller Global Default Server Address Upgrade

From v9.00 there is a new **Controller Defaults** tab in the Server Properties. The Global Default Server Address setting on this tab will affect the server address of all new and existing controllers on the site.

The upgrade step will be executed the first time a site upgrades from v8.90 (or earlier) to v9.00 (or later). It will not be executed on any subsequent upgrades.

- If any controllers have a custom server address (custom hostname or ip address) then whichever is the most commonly used address will become the Default Global Server Address. Any controllers using that address will be changed from "custom" to "default" server address. Any controllers that have a different custom server address will not have their settings changed.

  For example:
  100 controllers have "gallagherserver.com" custom server address.
  1 controller has "gallagherserver2.com" custom server address.
  The site default server address will be set to "gallagherserver.com" and the 100 controllers will be changed to "default" server address. The last controller will not be changed - it will stay as "gallagherserver2.com" custom server address.)

- If any existing controllers are configured to use "default" server address before the upgrade, then the site default server address setting will not be changed.

  For example:
  100 controllers have "gallagherserver.com" custom server address.
  1 controller uses the "default" server address setting.
  The site default server address setting will remain blank. No controller setting will be changed.
  This is because setting the Global Default Server Address would affect the 1 controller using the "default" server address, potentially causing it to go offline.

- If no controllers use a custom server address then the Global Default Server Address setting will not be changed.

- If the Global Default Server Address setting is not blank then no changes will be made. This won't be possible in production, but it could occur on some Dev/Test environments if they're already using the Global Default Server Address setting.

Copyright © Gallagher Group Limited