Command Centre - Guidance for configuration of non-production systems

Technical Document

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 2021. All rights reserved.

Contents

Background 3
Security Notice 3
Licensing 3
New Licensing Compatibility Rules: Version Table 4
Network Isolation 4
Command Centre Cloud, Mobile Applications and API Gateway 5
Controllers 6
Email and SMS Notifications 7
Scheduled Backups and Archives 8
Macros / Scheduled Macros 9
Enterprise Data Interface (EDI) 9
Multi-Server 9
Active Directory Cardholder Sync 10
Morpho/IDEMIA biometric readers 10
Allegion (Schlage) Engage 11
Reminder/Disclaimer 12

Background

For complex installations of Command Centre, Gallagher recommends that customers have a second system to safely perform testing and validation of configuration changes and software upgrades, before applying them to their production environment.

Such systems may be referred to as "test", "development", "staging", "QA", "integration", "pre-production", "acceptance", "validation" or other similar terms. For the purposes of this document, we shall refer to all such systems as "non-production".

It is common for sites to want to seed the non-production system with a database backup of their production system. This enables a more faithful reproduction of production and can be more valuable than a simple second distinct system, however there are some problems associated with this approach.

The goal of this document is to explain problems that might occur with a cloned system, and outline processes you can take to prevent them.

Disclaimer: This document is non-exhaustive. While we make a best effort to document all known problems and workarounds, we do not guarantee that all possible problems will always be known ahead of time and referenced here.

Security Notice

A database backup of a production Command Centre system **will** contain important sensitive information, such as personal data/PII, encryption keys, passwords, and other such material.

If you are transferring database backups between different servers, please act accordingly. Be careful not to create or leave behind extra copies of the database and transport it securely and carefully.

Licensing

For the non-production system to be able to launch from a copy of the production database, it must have a compatible license file.

Before early 2021, "compatible license file" was defined to be a matching SerialNumber *(along with correct software version)*:

```
[Site]
Name=Gallagher Production
SerialNumber=21769
MultiServerSerialNumber=
OriginalSerialNumber=
Edition=Standard Command Centre
```

The non-production system needed the same license serial number as the production system to launch a copy of its database, however the existence of this cloned license serial number caused significant problems in other areas, such as connecting to the Gallagher Cloud.

In early 2021, Gallagher instituted a process change, such that we will no longer issue license files for different systems with the same serial number. Going forward, non-production systems must have their own license file with a **different** serial number from the production system.

Accordingly, the definition of "compatible license file" has been changed in Command Centre 8.50, to include the OriginalSerialNumber as a possible match to the Serial Number of the production system. This allows a non-production server to launch from a backup of production, whilst retaining its own unique serial number:

Copyright © Gallagher Group Limited

```
[Site]
Name=Gallagher Test
SerialNumber=80235
MultiServerSerialNumber=
OriginalSerialNumber=21769
Edition=Standard Command Centre
```

This change has also been back-ported down through all supported versions.

Important!

If you upgrade Command Centre on an existing non-production system that already had the same license serial number as production, the non-prod system will continue to launch with the duplicate serial number. This is now an unsupported configuration and may lead to problems.

If your existing non-production system connects to the Gallagher Cloud, please obtain a new license for it as soon as possible, which does not share a serial number with production.

If your existing non-production system does not connect to the cloud, there is no immediate requirement to obtain a new license, but it is strongly recommended you do this the next time you upgrade the non-production system.

New Licensing Compatibility Rules: Version Table

Command Centre software versions in the below table use the new compatibility rules. Previous versions use the old rules, requiring an exact match, which Gallagher will no longer be issuing license files for.
If you have a non-production system using a restored database backup, you must upgrade to one of the following releases:

Command Centre 8.50 or newer	Any version
Command Centre 8.40	Maintenance Release **3** or newer
Command Centre 8.30	Maintenance Release **3** or newer
Command Centre 8.20	Maintenance Release **5** or newer
Command Centre 8.10	Maintenance Release **7** or newer
Older versions	Unsupported

Network Isolation

Most problems caused by non-production systems are due to the second system connecting to and interfering with external resources, such as third-party hardware and software. As such, the most effective mitigation is to prevent the second system from establishing network connections.

Network isolation is referenced as a mitigation by many of the features later in this document, so is explained in full here first:

Option 1: Run the non-production system on a separate network ("air-gap")

If there is no physical/logical network path between the non-production system, and other resources, then it cannot connect to them. Thus, it cannot interfere with the operation of the production system.

This is the safest option; however, it may not always be feasible to create a full separate network for the non-production system.

Copyright © Gallagher Group Limited

Option 2: Use a network firewall to stop the non-production system connecting.

If connections are blocked by a network firewall, then the non-production system cannot connect to and interfere with external resources.

This is less safe, as the firewall could be misconfigured, however it may be easier, and can allow partial isolation – for example you could block connections to specific external resources which will be known to cause problems but allow others which are known to be safe.

Command Centre Cloud, Mobile Applications and API Gateway

Please refer to New Licensing Compatibility Rules: Version Table earlier in this document.

If you are running a version of Command Centre prior to the new licensing model, then connecting to the Command Centre cloud, and use of Mobile Credentials from a cloned database is **not supported**:

Important!

You **must** prevent the non-production system from connecting to the Gallagher Cloud. If you do not do this, then the non-production system will interfere with the production system as follows:

- Issuing new mobile credentials on the production system may fail.
- The non-production system can send broadcast notifications to people from the production system, which may be a security policy violation.
- Deleting a mobile credential on the non-production system will result in the production credential being revoked from the end user's phone. This will cause them to be denied access to production.
- Issuing a new credential on the non-production system to a person who also has a production credential will result in the test credential overwriting the production one in the end user's phone. This will cause them to be denied access to production.

Mitigation: Network Isolation/Firewall

If the non-production server cannot connect to the internet, it cannot interfere with the cloud.

After launching Command Centre, you **must** delete the Cloud FT Item, after which point the network isolation can be removed.

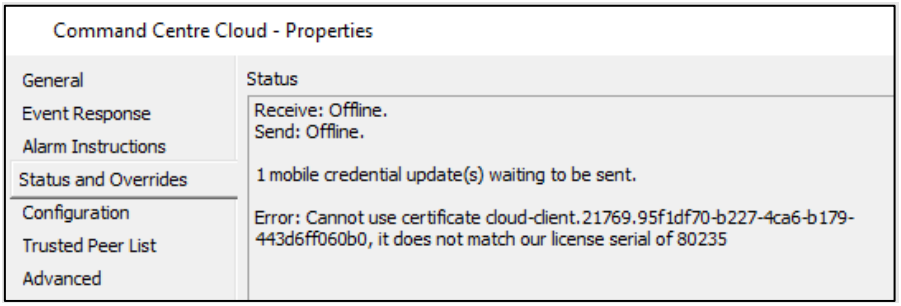
If you are running a version compatible with the new licensing compatibility model, then this is supported, and you do not need to take any additional steps to prevent interference.

Both systems can safely connect to the cloud, but you will need to manually re-establish the cloud connection on the non-production system after a database restore.

Process

The first time you launch the non-production system, after restoring a backup from production, the Cloud Connection will be offline. It will report an incompatible certificate error in the Status and Overrides page of the Cloud FT Item:

Copyright © Gallagher Group Limited



To re-establish the connection, delete the Cloud FT Item, and then create it again.

Gallagher API Gateway, Rest Clients and Command Centre Mobile Clients
Applies to Command Centre 8.60 and newer.

The API Gateway uses the Command Centre Cloud for connectivity and configuration.

If you do not prevent non-production system from connecting to the Gallagher Cloud, it will interfere with the production system in the following ways:

- Rest API clients and Command Centre Mobile clients connecting through the Gateway may have their requests forwarded to the non-production system rather than the production system.
- Alternatively, requests intended for the non-production system may be forwarded to the production system, where they may make unintentional harmful changes.
- Configuration changes (such as de-trusting a Command Centre Mobile device) made on the non-production system may affect the production system, affecting Rest and Mobile connectivity through the Gateway.

Controllers

In versions of Command Centre earlier than 8.50, the Command Centre server would open connections to each controller and push configuration to it.

A restored copy of the production database running on a non-production system will carry with it all the controller configuration information from the production system, and as such, it will also reach out and attempt to connect to production controllers. This has led to various problems in the past, such as changing an access group on the non-production system resulting in access denied for users in production, and so forth.

From Command Centre version 8.50 and later, the server no longer opens connections*; it relies on the controller to do this first. As such a controller configured against the production server should always continue to connect to that server, and a non-production server should no longer be able to interfere with it.

**Note: In the normal course of operation a non-production server running Command Centre 8.50 or later should no longer attempt to connect to controllers and will not interfere with them. However, if you use the "Send Server Address" or "Reset" overrides, then it will connect to the controller and reconfigure it.*

To prevent this from happening in versions earlier than 8.50, or as an additional safety measure against the special overrides in 8.50, you need to stop the non-production server from connecting to controllers carried across from production.

Mitigation Option 1: DB Anonymiser

Copyright © Gallagher Group Limited

The Database Anonymiser utility can reconfigure the database on the non-production system and remove all IP address configuration from controllers, such that when the Command Centre and Controller services are launched, they will not connect to controllers.

1. BEFORE you first launch the Command Centre service, run:

```
CCFTDBAnonymiser.exe ccftcentral -comm
```

2. Launch services as required.

Note: The "-comm" option for CCFTDBAnonymiser will not only clear controller settings, but also many other external communications related settings for other features. Please refer to the anonymiser utility release notes and documentation for more information.

Mitigation Option 2: Network Isolation/Firewall

Network isolation will stop the non-production system from interfering with production servers.

If you have controllers connected to your non-production system, then you can do the following:

1. BEFORE you first launch the command centre service, isolate the non-production server from the network.
2. Launch the configuration client and perform the "Disable Communications" override on all controllers except the specific non-production system controller(s).
3. Disable the firewall or reconnect the non-production system to the network.

Mitigation Option 3: Stop and Disable the Command Centre Controller service

This will prevent Command Centre from communicating with any controllers at all.

If you have controllers connected to your non-production system, then you can do the following:

4. BEFORE you first launch the Command Centre service, disable the controller service using the windows service manager.
   Note: Some non-production environments do not require controllers, or do not otherwise have any which connect to them. If this is the case, you may simply leave the controller service disabled permanently.
   If you do require controllers in your non-production system, proceed to the next step.
5. Launch the main Command Centre service, and the configuration client.
6. Perform the "Disable Communications" override on all controllers except for the specific non-production system controller.
   Note: As a more permanent alternative, in addition to the Disable Communications override, you can enter an invalid IP address (e.g., 0.0.0.0) in the "Controller Address" page in the configuration client.
7. Re-enable the controller service and start it.

(Note that the Controller Service may become re-enabled after a Command Centre upgrade so you should re-check after each upgrade that the Controller Service is still disabled.)

Email and SMS Notifications

The non-production system will have all the configuration needed to send emails and SMS notifications to end users. If not addressed, this can result in duplicate notifications (a competency copied from production expires on a schedule, and both servers notify), or incorrect ones (changing a competency rule in the non-production server causing notifications to real end users)

Copyright © Gallagher Group Limited

Mitigation Option 1: DB Anonymiser
The Database Anonymiser utility can remove any email/sms gateway configuration, such that your non-production system will be unable to send anything.

Run it with the **-comm** argument, as per the instructions for Controllers.

If you do wish to use notifications on your non-production system, then after launching command centre, reconfigure your notification rules to remove the links to production data, and then reconfigure your email/sms gateway.

Mitigation Option 2: Network Isolation/Firewall

If the non-production server cannot connect to the email/sms gateway, it cannot send notifications.

If you do wish to use notifications on your non-production system, then after launching Command Centre in an isolated environment, you can reconfigure the notification rules, and then join the non-production system back to a non-isolated network.

Scheduled Reports

The non-production system will have all the configuration for any scheduled reports. If any of these are configured to send reports via email, or write to a network share, then the non-production system will attempt to perform these actions as well, which may cause duplicate reports to be sent to people expecting production report data.

Mitigation: Network Isolation/Firewall

Launch the non-production system in an isolated network environment, and reconfigure any scheduled reports either to not run, or remove the email/network share information from them.

Scheduled Backups and Archives

If you have configured Command Centre to write backup/archive files to an external network share, then the non-production system will also attempt to use that network share.

This could result in production backups being overwritten, or non-production data being intermingled with production data in reports.

Mitigation Option 1: Use permissions/ACL's so the non-production server cannot access network shares used for production data.

If the non-production server is denied access to the network share, then backup/archive operations will fail, giving you the opportunity to safely reconfigure the non-production server to back up elsewhere.

Mitigation Option 2: Network isolation/firewall

If the non-production server cannot connect to the network, then backup/archive operations will fail, giving you the opportunity to safely reconfigure the non-production server to back up elsewhere.

Copyright © Gallagher Group Limited

Macros / Scheduled Macros

Macro Command Line actions can be configured to run any external program or script. Such scripts may have side effects such as writing files to an external network share, performing HTTP requests, or any other similar thing which could affect the production system.

Mitigation Option 1: Network isolation/firewall

This will stop any macros (in particular, scheduled macros) from affecting other systems. You may then reconfigure the macros to either disable or remove them.

If you do not have scheduled macros, then you will be able to reconfigure the system to remove any manually run macros, or rely on discipline to simply not run them on the non-production system.

Enterprise Data Interface (EDI)

The non-production system will have the same configuration as production.

If you do not do anything, scheduled imports and exports will still run, which may lead to problems such as:

- On file-based import, the non-production system may move or delete data files from the same network shared folder as production before the production system gets to them. This will cause the production system to fail its own import.
- On file-based export, the non-production system may write data files to a network shared folder, which may overwrite data from the production system, or cause two copies of the data to be written.
- On database-based import or export, the non-production system may modify data in the external database, altering what gets imported/exported by the production system.

Mitigation: Network Isolation/Firewall

If the test server cannot connect to external network shares or databases, its EDI runs cannot affect anything.

You should then delete or reconfigure EDI on the non-production system before joining the non-production system back to the wider network.

Multi-Server

If you are running a multi-server configuration, you will likely have a non-production server replicating each production server. Upon database restore, the non-production system will be configured to open connections to all the other **production** servers.

They will not automatically connect back to it, so in theory the non-production server should not be able to modify or damage a production server, however future changes from production -> non-production may propagate which may cause problems for the non-production server.

Mitigation: MultiServerSerialNumber

A multi-server group is defined by the value of the MultiServerSerialNumber in the license file. All servers in a group must have the same value for MultiServerSerialNumber, or they cannot connect to each-other.

As such, test licenses should be issued with a different MultiServerSerialNumber to prevent this. As an administrator of a Command Centre system, you should not need to do anything, as Gallagher should have issued you with correct licenses, however it is prudent to check this before bringing a non-production server online.

Copyright © Gallagher Group Limited

Example: License files for production group

```
[Site]
Name=Gallagher Production A
SerialNumber=21769
MultiServerSerialNumber=21700
OriginalSerialNumber=
```

```
[Site]
Name=Gallagher Production B
SerialNumber=21770
MultiServerSerialNumber=21700
OriginalSerialNumber=
```

License files for test group

```
[Site]
Name=Gallagher Test A
SerialNumber=81769
MultiServerSerialNumber=81700
OriginalSerialNumber=21769
```

```
[Site]
Name=Gallagher Test B
SerialNumber=81770
MultiServerSerialNumber=81700
OriginalSerialNumber=21770
```

Active Directory Cardholder Sync

Because ADSync uses its own configuration, an acceptance clone of the production AD Sync installation will attempt to connect to the production domain controller/s and production Command Centre system and update them both. This will cause problems, so you should change the configuration before starting the AD Sync service on the non-production server. If that does not happen, there are a few safeguards:

- The service will attempt to decrypt the configuration file using the service's client certificate. If the non-production server is based on a database backup, rather than a full server clone, then the certificate may be different or missing and AD Sync will fail to start.
- If the service can decrypt its configuration file, version 8.50 and later will attempt a REST connection to Command Centre. If the Command Centre server is pinning client certificates AD Sync will be configured to search the windows certificate store, which may fail if the non-production server is based on a database backup, rather than a full server clone.
  REST is optional in versions 8.40 and older; systems set up that way will attempt an OPC-UA connection which will have no safeguard.

Morpho/IDEMIA biometric readers

The non-production system may connect to these readers and reconfigure them, including adding and removing fingerprints from the database inside the reader. This could result in people failing to gain access to the production system, or a security breach.

Mitigation Option 1: BiometricDisableCommunication registry key

If you set the `BiometricDisableCommunication` registry key *(in the standard registry location on the server)* to a DWORD value of 1, this will disable all communication with biometric readers. You must do this before you start the Command Centre service, and if you change it back to 0 or remove it, you must restart the service to take effect.

Mitigation Option 2: DB Anonymiser

The Database Anonymiser utility can reset the IP addresses of all biometric readers to 0.0.0.0, such that your non-production system will be unable to connect to them.

Run it with the **-comm** argument, as per the instructions for Controllers.

Copyright © Gallagher Group Limited

Mitigation Option 3: Network Isolation/Firewall

If the non-production server cannot connect to the readers, it cannot affect them.

You should leave the non-production server network isolation/firewall in place; If you cannot do so then you must use another mechanism to disable network communications with morpho readers. E.g., configure their IP addresses to an invalid address such as 0.0.0.0

Note: If you use option 2 or 3, then the system will still contain the readers, and will still make failing attempts to connect to them. With larger numbers of readers, this can cause high CPU usage on the server (this is a limitation of the Morpho/IDEMIA third-party software that Command Centre must use to communicate with the readers).
If you see high CPU usage, or if you otherwise think you may be affected, you can set the `BiometricTaskThreads` registry key to a DWORD value of 1, which will limit the number of concurrent biometric reader connections to 1, thus reducing the CPU usage.

Allegion (Schlage) Engage

The Command Centre Allegion Engage integration is configured via two channels. Engage site and Manager configuration is configured using the Gallagher Cloud, whereas hardware devices are configured on the local network. As such, they are affected differently in a cloned database scenario.

1. Engage Site and Manager Configuration

The non-production system will contain a copy of any Allegion Engage sites from the production system.

If you attempt to modify or delete an Allegion Engage Site record on the non-production server (such as to rename it, or add a site manager), Command Centre will attempt to update the production record in the Allegion cloud.

The Gallagher cloud keeps track of which Allegion Engage sites are associated to which Command Centre systems and enforces a security boundary around each. This will prevent a non-production server from interfering with production cloud data. You will receive an error if you try and do something on a non-production server which might impact production data in the cloud.

Mitigation: None Required

You do not need to do anything for the cloud configuration data to remain safe, and your non-production server may safely configure additional Allegion Engage sites for testing purposes.

2. Local Allegion Engage device connection.

The non-production system will contain a copy of any Allegion Engage hardware from the production system.

If you attempt to modify or delete an Allegion Engage hardware item on the non-production server, then Command Centre will attempt to connect to it via the local network and reconfigure it, which may cause problems such as cardholders getting denied or granted access when they should not and may be a security risk.

Mitigation: Network Isolation/Firewall

Before you launch the non-production server after database restore, you should isolate it from the production network.

Once it has launched, you should reconfigure all the Allegion Engage devices to prevent accidental communication. Engage devices do not have a "Disable Communications" override, but you can approximate this by deliberately configuring an invalid IP address such as 0.0.0.0 against each one – after which point you may remove the network isolation if desired.

Copyright © Gallagher Group Limited

Reminder/Disclaimer

This document is not exhaustive, and there may other systems which may be affected by a cloned system which are not yet documented here. As a general rule, please use network isolation when launching a non-production server, and ensure you have updated the configuration for, or disabled any items which may be affected.

Copyright © Gallagher Group Limited