Gallagher Database Anonymiser Utility

Release Note

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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

1 Introduction

The Gallagher Database Anonymiser Utility is a command line utility that supports various options to clear secure data in customer databases.

IMPORTANT: The Gallagher Database Anonymiser Utility must not be run on the site server as Command Centre data will be lost. Setup a Test Server and restore/attach a backup/database of your site Command Centre server on to your test system on an isolated network and run this Anonymiser Utility to clear secure data in customer databases.

Refer to section ***4. Setting up a test system*** for details.

2 Usage

```
Usage: CCFTDBAnonymiser.exe ccftcentral [-all] [-rename] [-key] [-pdf] [-bio] [-card]
[-comm] [-changeset] [-cloud] [-misc] [-serial <serial>] [-cardholder] [-report]

       -all                Clear all data.
       -rename             Rename FT item names.
       -key                Clear all encrypted data.
       -pdf                Rename string or integer PDFs and clear image PDFs.
       -bio                Clear all biometric data
       -card               Reset all card numbers.
       -comm               Clear communication details, e.g. IPs.
       -changeset          Clear all changesets.
       -cloud              Clear all cloud-related data.
       -misc               Randomise any other misc data e.g. Site Plans.
       -serial <serial>    Sets the site serial number to <serial>.
       -cardholder         Clears cardholder related data.
       -report             Clears report schedules and output paths.

Usage: CCFTDBAnonymiser.exe ccftevent [-all] [-rename] [-event]
       -all                Clear all data.
       -rename             Rename FT item names in RelatedItems.
       -event              Clear event information.
```

CCFTCentral

[-all]

This will run all options at one go.

[-rename] Rename Items

Item names are renamed using the template “ItemType ItemID”

Currently items of the following types are renamed:

- Cardholder
- Access Group
- Access Zone
- Alarm Zone
- Input
- Output
- Door
- Site Plan
- Division
- Fence Zone
- Workstation
- Alarm Notes

Cardholders have their own FirstName and LastName fields as well as their FTItem name. These are updated similarly to Item names: FirstName = “cardholder”, LastName = “ItemID”.

Copyright © Gallagher Group Limited

[-key] Clear All Encrypted Data

Clears or resets encrypted data, such as keys and passwords configured in the system. A new Command Centre recovery code will be generated and will need to be copied using “Mark” > “Copy” in the command prompt, and then pasted into a text file and saved.

The keys and passwords cleared or reset:

- MIFARE keys and Enhanced MIFARE site keys
- Cardholder user Code
- Macro password to shared folder
- Archive password to shared folder
- Alarm transmitter encryption key
- Card PIN
- EDI Passwords
- RestClient encryption
- Commend Intercom system
- DESFire Default AppKey
- REST Client Certificate Thumbprint (can be re-populated with original thumbprint)
- GovPass keys

Note: From v9.00, the API Key is changed to all zeros *except* the last numbers which use the REST Client’s FTItemID.

[-pdf] Randomise String and Integer PDFs, delete image PDFs

String PDFs are replaced using the template “PersonalDataFieldID – CardholderID”

Integer PDFs are set to PersonalDataFieldID + CardholderID.

This ensures unique values across a given PDF, which is required for some PDFs.

Image PDFs cannot be reasonably replaced, so they are deleted.

Text PDFs are given values like "String-<pdfid>-<cardholderid>"

Text List PDFs are given values like "StrList-<pdfid>-<random4byteinteger>"

Cardholder PDF values from a Text List PDF are assigned a value from the above list (even if the restrict to list option is not used).

Date PDFs are now given a random date between 1970-01-01 and 2019-12-28, based on the PDF ID and Cardholder ID.

The PDF names will be retained but all their information is in these anonymised values.

Values also anonymised in the ChangesetItemField table.

[-bio] Clear Biometric Data

Clears or resets all biometric data, (e.g. fingerprints) from cardholder records.

[-card] Change Card Numbers

Randomises all card numbers in the Card table.

The MifareCSN column in the Card table has and CSNs replaced with random values.

Copyright © Gallagher Group Limited

Decimal card numbers are reassigned a random unique number per facility code, whilst also making significant effort to ensure that the card number ranges of Card Type are not violated.

Text format card numbers have no range and in this case are given decimal strings beginning with "1", "2", "3", etc.

PIV cards are given sequential values starting from 1111-1111-111111-111111111111111111 and incrementing just the last portion.

Mobile card numbers are reset back to just their GUID as a string.

[-comm] Disable Communications among Site Items

Resets communication settings for the Site Items, such as IPs, host names, BUS number, etc.

[-changeset] Delete Changesets

The changesets contain the entire history of the database, so they will be deleted.

If the site uses multiserver, this step will need to be skipped for the multiserver configuration to keep working.

[-cloud] Clear Cloud related data

Clears or resets all Cloud related configuration data.

- The Bluetooth Facility code used for Mobile Credentials
- All Mobile Credentials waiting for Registration
- The Cloud FTItem is deleted
- All Cloud Queues are deleted
- The Apple Wallet Configuration is cleared (Keys, TCI, and Artwork ID)

After this argument is used, the Cloud FT item will need to be recreated, and all Mobile Credentials on this system will need to be re-issued, if required.

Any REST API Clients and Mobile Clients that use the API Gateway will nned to be deleted and recreated.

[-misc] Randomise miscellaneous data

Randomise any other miscellaneous data, (e.g. Site Plans).

[-serial <serial>] Set Site Serial Number

Sets the site serial number in the database to <serial>.

[-cardholder] Clear Cardholder related data

Clears all Cardholder related data.

[-report] Clear Report Schedules and Output paths

Clears all Report Schedules and Output paths.

Copyright © Gallagher Group Limited

CCFTEvent

[-all]

This will run all options at one go.

[-rename] Rename Historical Item Names

The CCFTEvent database stores historical Item names in the RelatedItems table. When this argument is used, these are reset to the newly generated name for the related Item.

The item names are also renamed in the ChangesetField table.

[-event] Delete Event Info

Deletes event messages and details fields.

Redacted fields are replaced with the string “REDACTED”. This is currently not configurable.

The 'message' field for all events will be wiped out.

The 'Details' field for some events will be wiped out; but some will be re-filled with updated messages.

3 Safety

The program will not run when the database is being used or Command Centre services are running.

4 Setting up a test system

IMPORTANT: The Gallagher Database Anonymiser Utility must not be run on the site server.

Perform the following procedure to set up a test system:

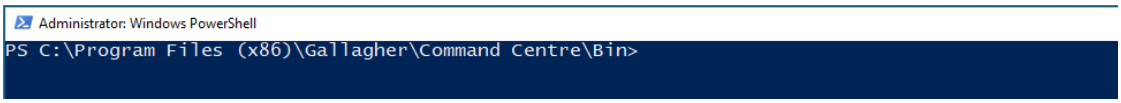
1. Contact Gallagher Technical Support to get a test license with site serial entered as original serial number.
2. Copy databases from production server to test server.
   Note: If Customisations are in the license, they must be installed on the test system prior to restoring/ attaching the site database.
3. Restore/attach the database.
   Note: The services won't start as Recovery code is not applied.
4. Apply the site server recovery code or run the Anonymiser as instructed to clear encrypted data and generate a new recovery code for the test system.
5. Use commands as required to clear secure data in customer databases, as explained in the previous section ***2. Usage***.

Copyright © Gallagher Group Limited

5 Running the utility

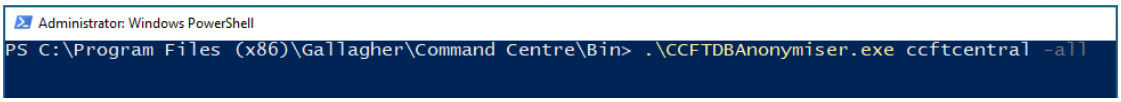
Perform the following procedure to run the Gallagher Database Anonymiser Utility:

1. Ensure a test system is set up as described above in section ***4. Setting up a test system***.
2. Close Command Centre and stop the Command Centre Services.
3. Copy **CCFTDBAnonymiser.exe** into the 'C:\Program Files (x86)\ Gallagher\Command Centre\Bin' folder.
   Note: The Utility should only be run from the Bin folder.
4. <**Shift**> and right-click on empty space in the 'Bin' folder, and click either **Open command window here** or **Open PowerShell window here**.

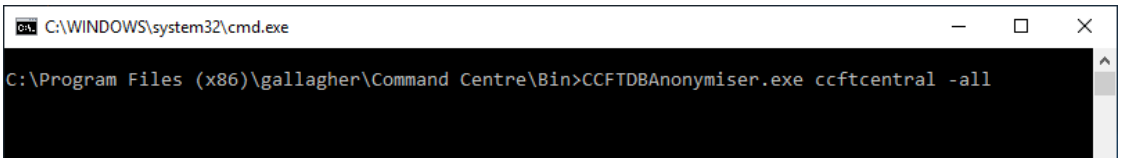


5. Run the utility by entering the appropriate command line parameter according to the options available in the previous section ***2. Usage***.
   Note: The command line parameter will differ depending on whether you are using Command window or PowerShell, as follows:

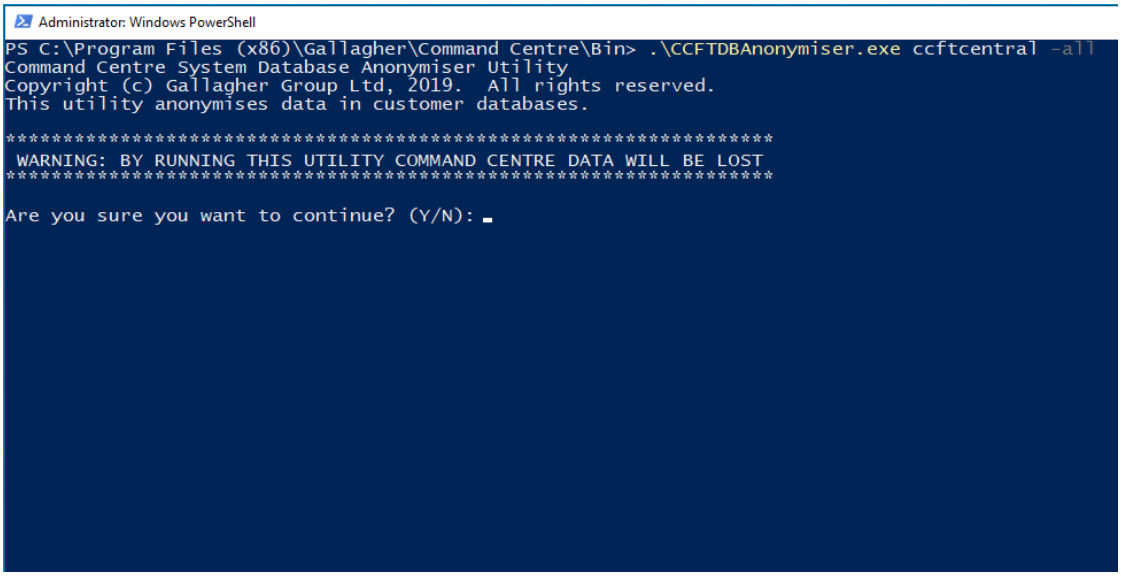
   PowerShell requires **`.\`** at the beginning of the command line parameter.
   For example, **`.\CCFTDBAnonymiser.exe ccftcentral -all`**



   Command window does not require **`.\`** at the beginning of the command line parameter.
   For example, **`CCFTDBAnonymiser.exe ccftcentral -all`**



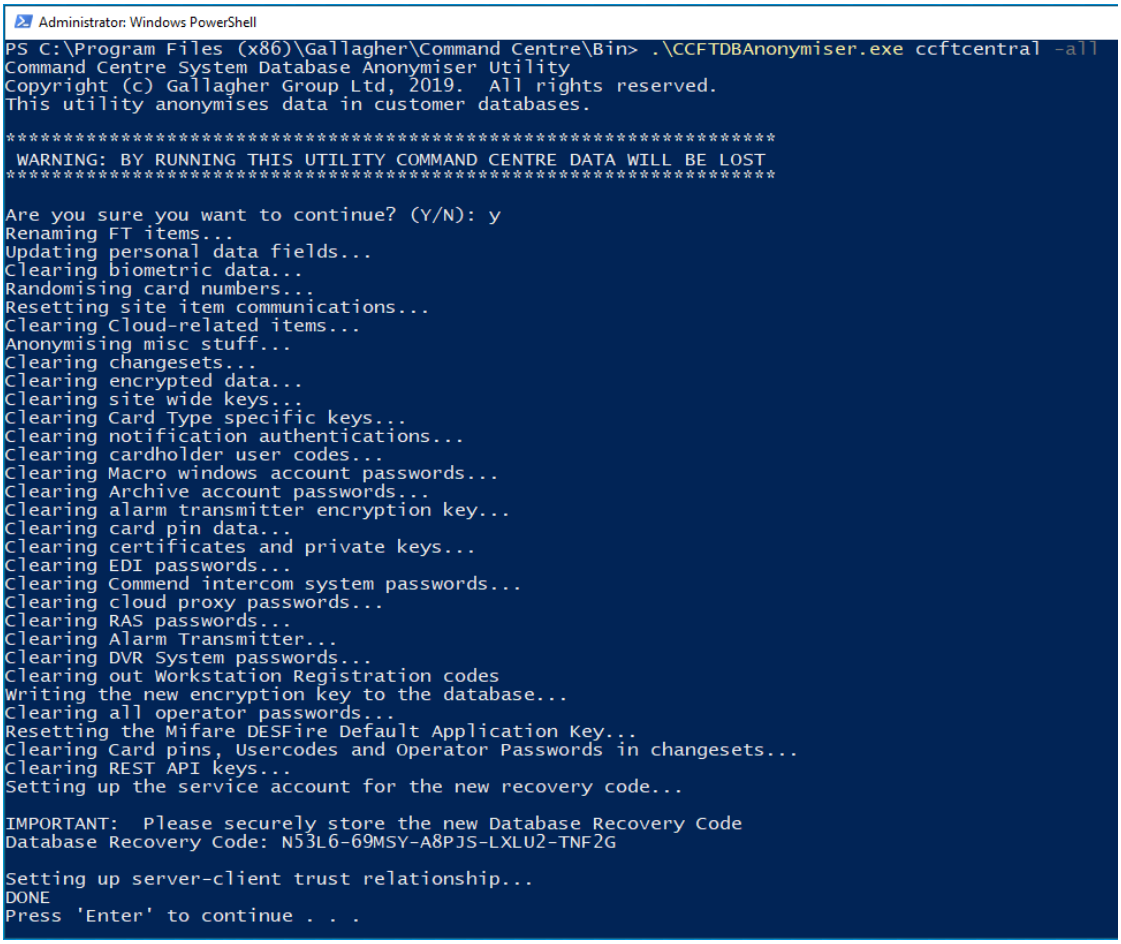
6. Press <**Enter**>.
   The utility launches with a warning message, indicating that data will be lost by running the utility.



7. Type **Y** or **Yes**, and press <**Enter**>.
   The data is anonymised according to the option selected.

Copyright © Gallagher Group Limited

In this example, all the **ccftcentral** options have been run in one go, (i.e. **[-rename] [-key] [-pdf] [-bio] [-card] [-comm] [-changeset]** and **[-serial <serial>]**).



Note: The **ccftcentral [-all]** or **[-key]** options generate a new Database Recovery Code. If you selected either of these options, it is important that the new code gets stored securely.

8. Restart the Command Centre Services, and run Command Centre.

   The **ccftcentral [-all]** or **[-key]** options also clear operator passwords, therefore on the Command Centre Logon screen enter your Logon Name and click the **Logon** button.
   The Change Password screen displays, allowing you to enter a new password.

Copyright © Gallagher Group Limited