Gallagher Command Centre

Recovery Code

Technical Information Paper

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 2019. All rights reserved.

Document History

Edition	Date	Author	Comment
1.0	07/05/2018	G Thompson	-
1.01	21/05/2018	G Thompson	Minor changes.
1.02	07/02/2019	G Thompson	Minor changes.

Contents

1 Introduction 4

2 Background 4

3 Purpose 4

4 How the Recovery Code works 5

5 Management of the Recovery Code 6

6 Generating a new Recovery Code 6

7 When the Recovery Code may need to be re-entered 7
- 7.1 Changing the service account will require the recovery code to be re-entered 7
- 7.2 Shared Database on High Availability Systems 7
- 7.3 Microsoft updates that inadvertently delete sections of the service account registry 7
- 7.4 Restoring or attaching an older database which used an earlier recovery code 7
- 7.5 Other Command Centre utilities may request the recovery code 7

8 Questions and Answers 8

Copyright © Gallagher Group Limited

1 Introduction

This document addresses questions regarding the Recovery Code, which was introduced in Command Centre 7.70.

In the content that follows, various cryptography terms may be used without in-depth explanation. It is assumed the reader is either already familiar with these terms, or is able to research the applicable standards if further details are required. This document focuses on Command Centre's use of these technologies.

2 Background

Due to the increasing number of cyber threats, and the need for software to comply with various cyber security standards, Command Centre has been updated to ensure that it uses the best technology available.

Command Centre 7.70 improved the way that keys, passwords and other sensitive data is stored in the database. It was through this development that the Recovery Code was introduced.

Command Centre is used by a wide range of customers, both in situations where there is a dedicated IT department with various policies and management processes, through to other environments where this IT support is not on site. Command Centre continues to be developed to be as flexible as possible as to how Gallagher's customers wish to run their systems.

Command Centre is also developed to be "secure by default". This is to both reduce the time for hardening a system after installation, and to ensure an "out of the box" installation of Command Centre is less vulnerable to attack. The Command Centre setup does this with as minimal user interaction as possible.

3 Purpose

Command Centre's configuration is stored within an SQL Server database, which makes the backup and restoring of a Command Centre server a straight-forward process. Some of this stored configuration includes passwords, keys and codes which Command Centre needs access to, in order to operate. Examples of these are:

- Mifare Card Encryption keys
- Encryption and Authentication keys used for:
  - Controller communications
  - Alarm Transmitter communication
  - Third party device communication, (e.g. Morpho)
  - Client communication, (e.g. Configuration Client and Command Centre Client)
- Cardholder User codes and PINs
- Passwords for network shares for Event Archives
- Account credentials used by Command Centre's notification feature.
- External database passwords, used in EDI Imports
- REST Client API keys
- Proxy passwords for Gallagher Cloud access
- Command-line macro credentials

Copyright © Gallagher Group Limited

Even if a site has rigorous IT security policies in place, it is widely accepted that private keys and passwords should be encrypted, and never be visible in the clear. The extra layer of protection prevents the chance of this data becoming a target for a hacker or malicious software. Disk Encryption and TDS Encryption (SQL connection encryption) would not protect this data from misuse if the attacker managed to gain access to the SQL database engine.

The Command Centre databases are sometimes accessed directly by third-party integrations, which are often given read-only access to the database in order to operate. Command Centre's encryption of data within the database provides protection for sensitive data when fine-grained access permissions may not be applied.

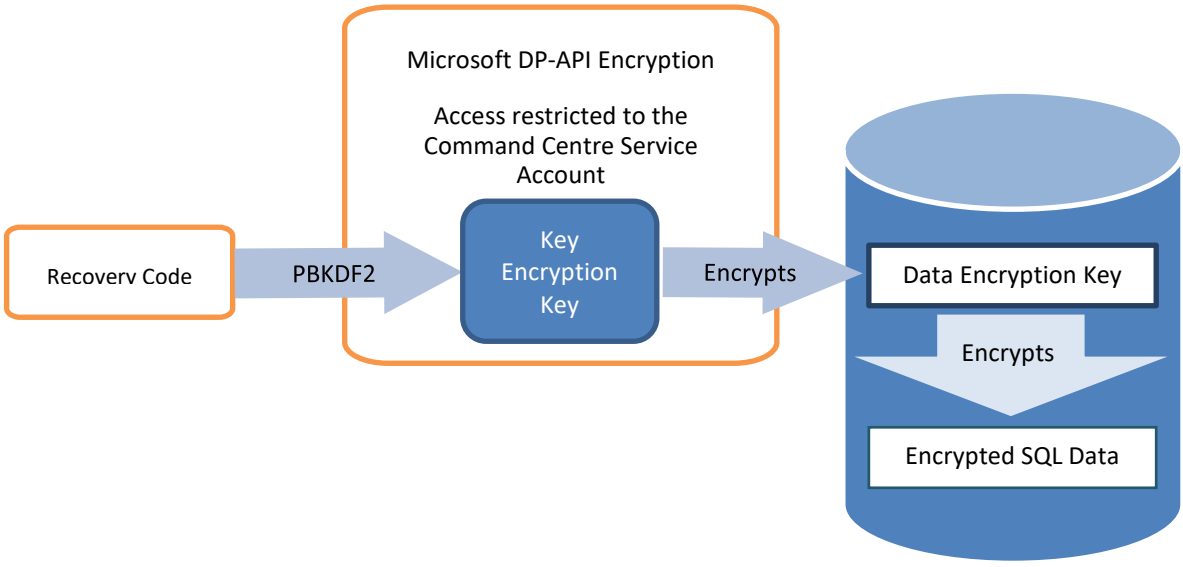
The keys that are used to encrypt the data need to be reproducible, so that server migrations and restoring of backups is possible (e.g. disaster recovery). However, these keys needed to be different for each site to prevent data being copied and decrypted on another machine. Prior to Command Centre 7.70, these keys were derived by algorithms that are proprietary and hidden to try and keep customer data safe. These unpublished algorithms do not comply with modern cryptography standards. There had also been requests from customers who wanted to be in control of their own encryption keys.

The solution is to have a customer controlled key to secure the data within the database, which could be used to recover and migrate a systems when needed. This key could not be packaged within the software or supplied by Gallaghers, and also needed to be unique to the Command Centre installation.

4 How the Recovery Code works

An ideal encryption key is very difficult to guess, and is truly random. The stronger encryption algorithms require longer keys which are not user-friendly. Command Centre currently uses AES-256 to encrypt data within the database, which requires a 256 bit key (32 bytes). To avoid installers having to deal with these keys, Command Centre creates a recovery code from a cryptographic random number generator, and then uses a "key derivation function" to produce a strong encryption key from the recovery code. This ensures that a strong and un-guessable encryption key is used, and avoids predictability issues that would come from user supplied passwords.

The key derivation function used is PBKDF2, and is configured to perform 100,000 rounds of the SHA512 hashing algorithm. This process is irreversible, so it is not possible to get the recovery code out of an existing Command Centre system.



Copyright © Gallagher Group Limited

The resulting Key Encryption Key (KEK) is needed by the system during start-up, so that the Command Centre service can access information in the database. This key also has to be stored outside of the database in a secure manner. For this, Gallagher chose Microsoft's DP-API (Windows Data Protection) which encrypts data to a specific Windows User Account. For the Command Centre service, this is the service account that is chosen when Command Centre is installed (Network Service by default). More information about Microsoft's DP-API can be found at:

https://www.passcape.com/index.php?section=docsys&cmd=details&id=28

This encrypted KEK is then stored within the service account's registry which further limits access to the encrypted key.

As the Command Centre service starts, it will decrypt the KEK using DP-API, and in turn use that key to decrypt the Data Encryption Key (DEK) that is stored in the database. The Data Encryption Key is used to encrypt and decrypt the sensitive configuration data. This indirection (key to encrypt a key) allows the recovery code to be changed, without needing to decrypt and re-encrypt all of the data within the database.

5 Management of the Recovery Code

Because the recovery code is the source data for an important encryption key for Command Centre, it should be handled with care. The following practices should be used:

- Don't store the recovery code in the same location as database backups. Obtaining the recovery code and a database backup gives all the details needed to recreate a system elsewhere.
- Don't leave the recovery code on the Command Centre server machine. The recovery code will be needed to restore the Command Centre system if the server fails. Also if the recovery code is left on the Command Centre server, it negates the protections put in place for the Key Encryption Key.

6 Generating a new Recovery Code

Because loss of a recovery code could be a disastrous situation for a site, an option to "generate a recovery code" for a running system has been provided in the Command Centre Recovery Code Utility (CCFTRecoveryCode.exe). This is only intended to be used when the recovery code has been lost, and where the Command Centre server is still operational. Generating a recovery code is not intended to be used for where it is inconvenient to obtain the recovery code from its secure storage location. Access to the recovery code utility should be restricted, and by default, it requires administrative rights on the Command Centre server.

If a new recovery code is generated for a system, then that new recovery code is what will be needed to restore a system from any backups made from that point onwards. In order to keep track of which backups require which recovery codes, installers and customers should be cautious of generating new recovery codes too frequently.

Generating a new recovery code for a system goes through the process of creating a new recovery code, deriving a new Key Encryption Key from that code, and re-encrypting the stored Database Encryption Key with that new KEK. This relies on Command Centre being able to decrypt the Database Encryption Key with the old Key Encryption Key. A new recovery code cannot be generated on a non-functioning system.

Changing the key encryption key stored within the service account is made via service control commands issued to the Command Centre service. This requires the user running the Recovery Code utility to have service control privileges on the server, and requires the Command Centre services to be stopped.

Copyright © Gallagher Group Limited

7 When the Recovery Code may need to be re-entered

There a number of situations when a recovery code may need to be re-entered for a Command Centre installation. Aside from the backup recovery and server migration, the recovery code may also be needed for the following reasons. The Recovery Code utility's "Enter a code for Command Centre to use" option is what should be used for these cases.

7.1 Changing the service account will require the recovery code to be re-entered

Because the Key Encryption Key is securely stored within the service account registry, altering the account that the Command Centre service runs under will require the recovery code to be entered using the Recovery Code utility (CCFTRecoveryCode.exe).

7.2 Shared Database on High Availability Systems

If the Command Centre databases are shared between multiple servers in a high availability / SQL Cluster environment, then each server that may start the Command Centre service and require access to the same database will have to have the recovery code entered. In situations where the High Availability software clones the entire machine, the Key Encryption Key will be mirrored automatically by that software.

7.3 Microsoft updates that inadvertently delete sections of the service account registry

Early in 2018, Microsoft released an update that cleared sections of user registry. We have not been able to identify which specific update this was, but the solution was to re-enter the recovery code to place the encrypted Key Encryption Key back into the registry.

7.4 Restoring or attaching an older database which used an earlier recovery code

If a system has had the recovery code re-generated, and then an earlier database backup restored or a database file re-attached, then the recovery code for that earlier database will need to be re-entered. This is due to the Key Encryption Key stored in the system not matching the recently restored / attached database file.

7.5 Other Command Centre utilities may request the recovery code

Utilities that require access to the encrypted data, but are run outside of the Command Centre service account, will need the recovery code in order to gain access to that encrypted data. The utility should be checked for authenticity before providing it with the recovery code.

Copyright © Gallagher Group Limited

8 Questions and Answers

Q: What is protected by the Recovery Code?

A: The following configuration is protected by the recovery code encryption

- Mifare Card Encryption keys
- Encryption and Authentication keys used for:
  - Controller communications
  - Alarm Transmitter communication
  - Third party device communication, (e.g. Morpho)
  - Client communication, (e.g. Configuration Client and Command Centre Client)
- Cardholder User codes and PINs
- Passwords for network shares for Event Archives
- Account credentials used by Command Centre's notification feature.
- External database passwords, used in EDI Imports
- REST Client API keys
- Proxy passwords for Gallagher Cloud access
- Command-line macro credentials

Operator Password hashes are also further encrypted by the recovery code to prevent dictionary password attacks being ran over the database or one of its backups.

Q: Can Gallaghers find my recovery code?

A: The recovery code is generated on the server machine from random data, and then passed through a one-way function to generate the Key Encryption Key. Gallaghers is unable to reverse engineer the recovery code out of your system. If you have misplaced your recovery code and still have a functioning server, a new recovery code can be generated using the Recovery Code utility, but this will mean the old recovery code will not be able to be used when restoring any future backups. If you have lost your server and the recovery code, then you may have to restore your backup as a template, which will result in the loss of some configuration.

Q: Can I install Command Centre without a recovery code?

A: It is important to have a unique recovery code for your installation for the security of the data that the recovery code protects. The Command Centre installer does not provide a fixed / pre-canned recovery code option.

Q: When should I change my recovery code?

A: Only if the previous recovery code has been lost, or if the existing recovery code has been compromised. Be aware that you will need to track which database backups are using which recovery code. One way of doing this is by comparing the date and time that the recovery code was generated to the date and time of the backup. See "Generating a new Recovery Code" above.

Q: Where should I store the recovery code?

A: In a secure location that is not in the same place as the database backups, or on the Command Centre server machine. See "Management of the Recovery Code" above.

Q: Who should have access to the recovery code?

A: Only authorised and trusted personnel should have access to the Recovery Code. Because of the security implications of access to the data it encrypts, the Recovery Code should be treated as sensitive information.

Copyright © Gallagher Group Limited