Gallagher Command Centre

Migrating keys on MIFARE® DESFire cards

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 2025. All rights reserved.

Contents

1 Introduction 4
1.1 Understanding Site-specific Key Migration Modes 4
Migration with All Readers (Default Mode) 4
Migration with Selected Readers 4

2 An Overview of the Migration Process 5
2.1 Before migration 5
2.2 During migration 5
In case of technical difficulties 5
2.3 After migration is stopped or the end date is reached 5

3 Tips 6
3.1 How to tell if a specific user has had any cards migrated 6
3.2 Automatic cloned card detection 6
3.3 Manually detecting cloned cards 6

4 Caveats 8
4.1 Cardax IV Readers 8
Cardax IV readers connected to Wiegand protocol converters 8
4.2 Offline controllers 8
4.3 Card Encoding 8
Cards not migrated during migration period cannot be re-encoded 8
Morpho data 8
4.4 Card sharing scenarios 9
Multi-server 9
Sites entering Facility codes and Card numbers they are not licensed for to make cards work 9
Cards with multiple licensed applications protected by the same key may prevent migration 9
Multiple applications on a card encoded by sites sharing a key seed 9
4.5 Independent sites that share a facility code and key seed 9
Multiple sites with the same licensed facility code have to share key seed also 9
4.6 Multi-tech Cards 9
4.7 Unconfigured HBUS readers may still migrate cards 10
4.8 Restoring from a backup 10
4.9 Pausing migrations using selected readers 10

5 Glossary 10

Copyright © Gallagher Group Limited

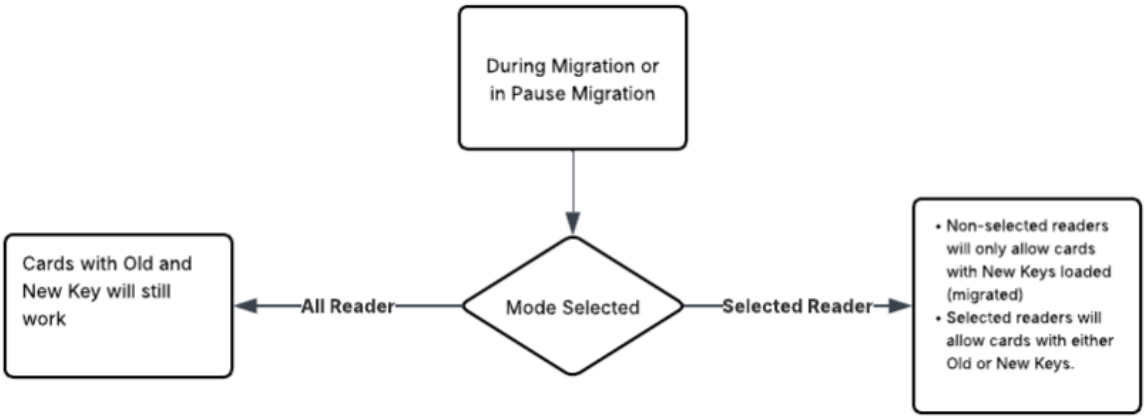
1 Introduction

Sites may want to change their card key if their current key is easily identifiable, (e.g. default key seed), or if the key is compromised. Site-Specific Key (SSK) migration allows sites to do this. There are two modes for SSK migration, as follows:

- **All Readers Mode:** Keys are updated across all readers; cards with old or new keys remain functional.
- **Selected Readers Mode:** Only chosen readers update keys; others enforce new keys, denying access to unmigrated cards. Use cases include enforcing updates at secure entry points to improve card compliance and security.

1.1 Understanding Site-specific Key Migration Modes

When performing a Site-Specific Key migration, or when the process is paused, it's important to understand that there are two distinct migration modes. While the differences may appear subtle, each mode serves a specific purpose and has implications for card functionality across readers.



Migration with All Readers (Default Mode)

In this mode, all readers participate in the migration process. Supported cards that are presented to any reader will have their keys updated. When the migration is paused, cards with either the old or new keys will continue to work across all readers.

Migration with Selected Readers

This mode restricts the migration process to a defined set of readers. Only these selected readers will update the keys on supported cards. Non-selected readers will enforce the new keys, meaning that cards not yet migrated will be denied access. This enforcement applies both during active migration and when the process is paused.

Migration with selected readers is typically used to enforce migration at a designated choke point, such as a high-security entry or exit. This ensures that all cardholders must pass through a specific reader to have their card updated. It also provides a mechanism for sites to address potential security concerns, as any compromised or non-compliant card would be denied access until it passes through the required migration point.

Copyright © Gallagher Group Limited

2 An Overview of the Migration Process

2.1 Before migration

- Command Centre is version 8.30 or later.
- Ensure all controllers and readers are on the latest software.
- It is strongly recommended that there are no readers using the Cardax IV protocol - if this is not possible, see section 4.1 Cardax IV Readers.
- Ensure that only MIFARE® DESFire cards are being used as other MIFARE® card technologies are not compatible with key migration.
- Once ready, change the MIFARE® Plus/DESFire key seed, set the migration end date, and apply the changes.

2.2 During migration

- Once the MIFARE® Plus/DESFire Key Seed has been changed it is strongly recommended that the site keys are exported, and a backup of the system is made and stored in a safe place.
- As MIFARE® DESFire cards are presented at HBUS readers they will be migrated to keys derived from the new key seed.
- Any previously encoded MIFARE® Plus cards will no longer be accepted at HBUS readers.
- New cards that are encoded during this period will be encoded with keys derived from the new key seed.
- If you use Mobile Readers, MIFARE® DESFire cards with both old and new keys will be readable during migration, however a Mobile Reader will not migrate cards.

In case of technical difficulties

- Pause the migration. This will continue to let both migrated and unmigrated cards through doors. Consult Gallagher Tech Support.
  See section 4.9 Pausing migrations using selected readers for further detail.
- Cards that are encoded while the migration is paused will be encoded with keys derived from the new key seed.
- Once issues have been resolved, restart the migration and set a new migration end date.

2.3 After migration is stopped or the end date is reached

Only MIFARE® DESFire cards that have been migrated will be accepted at HBUS readers and Mobile Readers. Any MIFARE® Plus cards will need to be re-encoded in order to function after migration.

After migration has ended, cards that have not been migrated will be incompatible with the Read MIFARE® Card and Search Using Card features.

Copyright © Gallagher Group Limited

3 Tips

3.1 How to tell if a specific user has had any cards migrated

In the Command Centre Client, create an event report with the following filters:

- Event occurred between <insert migration period here>
- Event type is **Card Keys Updated (Confirmed)** and **Card Keys Updated (Unconfirmed)**
- Cardholder is <insert cardholder here>

If there are events in the report, then the cardholder had cards migrated. The different events that show if a card has been migrated or not are as follows:

- **"Card Keys Updated (Confirmed)" event only** - this will probably cover 99% of card key migrations.
- **"Card Keys Updated (Unconfirmed)" event** AND **"Card Keys Updated (Confirmed)" event** - this covers an edge case where the key rolling gets interrupted right at the end of the process, (e.g. card removed from reader too quickly), and the reader can't know for sure if the process completed. In this case, the process **didn't** complete and the next time the card is badged the migration picks up from where it got to last time, and the 'Confirmed' event is sent. Two events for the one card.
- **"Card Keys Updated (Unconfirmed)" event only** - this covers an edge case where the key rolling gets interrupted right at the end of the process, and the reader can't know for sure if the process completed. In this case, the process **did** complete, so the next time the card is badged it already has the right keys and goes straight to the access decision. In this case, the card has been migrated, but no 'Confirmed' event is generated since the server doesn't know that the card completed migration.

3.2 Automatic cloned card detection

The "Detect Duplicate Key Migrations" process is a new feature in vEL8.50 and runs automatically during the Key Migration Period.

It raises a high-priority "Potential Duplicate Card" alarm whenever a Card Keys Updated migration event is repeated for the same card. For each Card Keys Updated migration event, this feature checks for any earlier migration events for the same card.

The details of a "Potential Duplicate Card" alarm indicate that it should be investigated as unauthorised access may be possible using the duplicate card.

3.3 Manually detecting cloned cards

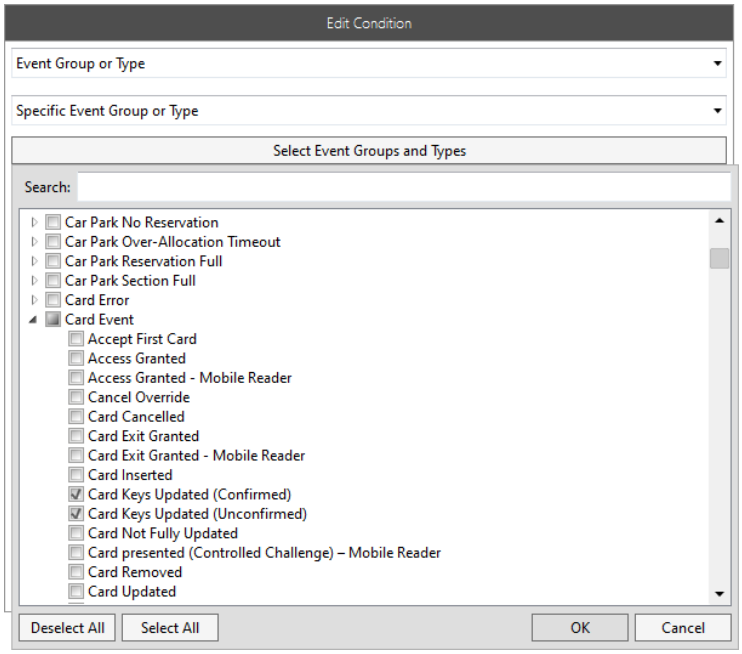
This procedure is relevant for migrations performed prior to vEL8.50.

Note: *This procedure is only reliable for events within a single server. If multi-server event aggregation is turned on this process may produce false positives*.

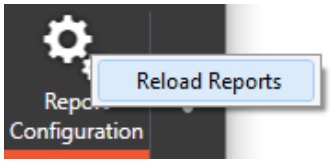
1. Select the **Reports** tab on the Command Centre title bar, and click the **Report Configuration** button on the toolbar.
2. Click the **New Report** button and select **Activity Report**.
3. Click the **Edit this filter** button for the "Event Occurrence Time" filter.
   The Edit Condition pop-up displays.
4. Change the **Report Period** to "User Defined", enter the **Start Date** and **End Date** of your migration, and click the **OK** button.
   The Edit Condition pop-up closes.
5. Click the **Insert Filter** button and select **Event Group or Type**.
   The Edit Condition pop-up displays.

Copyright © Gallagher Group Limited

6. Click the **Select Event Groups and Types** button, and click the arrowhead beside **Card Event**.
7. From the expanded list, tick **Card Keys Updated (Confirmed)** and **Card Keys Updated (Unconfirmed)**, and click the **OK** button.



8. Click the **OK** button.
   The Edit Condition pop-up closes, and the "Event type is one of: Card Keys Updated (Confirmed), Card Keys Updated (Unconfirmed)" filter displays under the "Event Occurrence Time" filter.
9. Click the **Configure Layout** button that appears over the Report Preview to the right of the filters.
   The Report Layout Configuration pop-up displays.
10. In the 'Column Selection' section:
    - remove the **Occurrence Time** and **Event Full Description** columns, and
    - add the **Event Details** column.
11. In the 'Column Configuration' section, click the ▷ beside **Event Details**, and select **Sort descending**.
12. Click the **OK** button.
    The Report Layout Configuration pop-up closes.
13. Click the **Save** button.
14. Right-click on the **Report Configuration** button and select **Reload Reports**.



    The message *"Are you sure you want to reload reports?"* displays.
15. Click the **Yes** button, and run the new report.
16. Click the **Save** button and select **CSV file without headers (*.csv)**.
17. Run the following PowerShell command:
    Get-Content "migration.csv" | Group-Object | Where-Object { $_.Count -gt 1 } | Select { "$($_.Count)`t$($_.Name)" }

    The output will display any cards that have been migrated more than once, with the number of times the card has been migrated, and the card details.

Copyright © Gallagher Group Limited

4 Caveats

4.1 Cardax IV Readers

Cardax IV readers are unable to perform the migration of keys. They also do not receive the new key seed automatically, but rather the new key seed must be set on the readers manually using an admin card. This means that at any one time a Cardax IV reader will only accept either cards that use keys derived from the old key seed, or cards that use keys derived from the new key seed, but not both. As such, it is not recommended to use the key migration feature while still having Cardax IV readers configured.

Cardax IV readers connected to Wiegand protocol converters

There are situations where Cardax IV readers may be connected to a third-party device via a Wiegand protocol converter. In order to continue working after migration, any such readers that have had their key seed changed previously will require connecting to a Command Centre system so that a "use default key" override may be performed before an admin card can change the key seed correctly.

4.2 Offline controllers

If key migration is started, paused or stopped while some controllers are offline, those controllers will continue behaving as if the migration is in the state it was at the time the controllers last connected to the Command Centre server until the controller once again connects to the server. This may cause issues if the key seed is changed a second time before the controller has once again connected to the server, particularly if attempting to migrate to a previous key.

4.3 Card Encoding

Cards not migrated during migration period cannot be re-encoded

Cards that have not been migrated since the key seed was changed will not be able to be re-encoded in Command Centre. In order to re-encode a MIFARE® DESFire card in this situation, present it to an HBUS connected reader to be migrated before attempting a re-encode (migration must be enabled on the reader for the card to be migrated).

Morpho data

Cards that have been migrated to different keys are unable to be re-encoded if the card has already been encoded with Morpho data and the card type has a Morpho DESFire object on the card layout.

Copyright © Gallagher Group Limited

4.4 Card sharing scenarios

Multi-server

Each server in a multi-server setup has its own key seed, independent of the other servers. Performing a key migration on one server will only migrate cards that use keys derived from the key seed for that server. It is recommended to migrate all servers that need to share cards to same new key seed at the same time:

- Generate a new key seed on one server and start the migration.
- Export the keys from this server and import into all other servers.

This will start a migration to the same key seed across all servers in the multi-server setup.

Sites entering Facility codes and Card numbers they are not licensed for to make cards work

Sites that have created a card type with different site's facility code and card number in order to make that site's cards gain access on their site will need to encode their own data onto the card, rather than just reading someone else's once either site migrates their keys (unless all such sites are willing to share a MIFARE® Plus/DESFire Key Seed).

Cards with multiple licensed applications protected by the same key may prevent migration

When a card contains multiple applications linked to licensed facility codes, the first application found on the card will be read and migrated. Other Gallagher access applications on the card with facility codes licensed by the site will not be migrated.

Multiple applications on a card encoded by sites sharing a key seed

A site may migrate a card that has been originally issued by the other site. In this situation, if the sites are both on the same key seed then the card master key may be changed by a site that was not the original issuer. This will not cause a problem with access as the access applications on the card are independent. It will prevent the originally issuing site from changing the default application key on the card via re-encoding.

4.5 Independent sites that share a facility code and key seed

If sites are using the same facility code and key seed (and that facility code is in their license file) then key migration on one site can affect access to other sites, both for its own users visiting those other sites and for those other site's visitors to the key migration site. Unless all sites are migrating to the same key seed at the same time, cards that get migrated on one site will no longer work on the others.

Multiple sites with the same licensed facility code have to share key seed also

If multiple sites share a licensed facility code, they will have to share their key seed also. Otherwise, when one site migrates the other site will no longer be able to read cards.

4.6 Multi-tech Cards

If multi-tech cards are presented to Multi-tech readers that have all technologies enabled the migration may take a few hundred milliseconds longer.

Copyright © Gallagher Group Limited

4.7 Unconfigured HBUS readers may still migrate cards

If an HBUS reader has been configured against a controller but has not been assigned to a door or configured as an alarm terminal, it will still migrate keys on cards presented to it, despite showing as unconfigured.

4.8 Restoring from a backup

If restoring from a backup that was taken prior to changing the key seed, the old key seed will be restored, and any cards that were using keys derived from the new key seed will no longer work. It is recommended to both take a backup after changing key seeds, and export the site keys whenever they are changed, and store them securely.

4.9 Pausing migrations using selected readers

If key migration is running on selected readers and you pause the migration, the migration will only be paused on the selected readers. Any non-selected readers will continue only accepting cards on the new key.

If you are having technical difficulties and wish to make all cards work while performing a migration on selected readers, you may want to pause the migration on all readers, as follows:

1. Click the **Pause** button.
   A message indicating what happens while the migration is paused displays.
2. Click the **Yes** button to proceed.
3. Change the readers to be used for migration by clicking the **All Readers** radio button.
4. Click the **Apply** button.

Refer to section 2.2 During migration for further detail.

5 Glossary

- **MIFARE® Plus/DESFire Key Seed** - This is a value that is used to derive the keys that protect each card.
- **MIFARE® DESFire Default Application Key** - This is the value that all keys for the applications on a card are set to when the application is created, after which they are typically changed to custom values.

Copyright © Gallagher Group Limited