MorphoAccess Installation

Installation Guide

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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

2 Biometric categories 4

3 Morpho Biometric Readers 5

4 Installation 6
- 4.1 Installing Microsoft Redistributables 6
- 4.2 Installing MSO330 and MSO1300 Drivers 6
- 4.3 Installing the License Manager 7
- 4.4 How to Retrieve Host ID and Install VERIF Software License 8

5 Installing MorphoAccess Readers 9
- 5.1 Configuring a Biometric Reader 9
  - 5.1.1 Configuring Morpho Readers using MBTA application 9
- 5.2 Supported MorphoAccess Readers 13
  - 5.2.1 Supported IDEMIA Devices and Firmware versions 13
  - 5.2.2 Unsupported EOL IDEMIA Devices 13
- 5.3 Upgrading the MorphoAccess Reader Firmware 14
- 5.4 Physically installing MorphoAccess Readers 16
- 5.5 OSDP Wiring 16
- 5.6 MA Sigma, MorphoWave, VisionPass SP and VisionPass Wiring 16
- 5.7 Power Supply Requirements 18
- 5.8 Updating VisionPass SP to VisionPass SP Fingerscan 18
- 5.9 Morpho Extended Database Licenses 18
  - 5.9.1 Morpho Reader Default User Databases 19
  - 5.9.2 Available Morpho Reader Database Extension License 19
  - 5.9.3 Upgrade Database Extension License 19

6 Supported Enrolment Devices 22
- 6.1 Which Firmware and Drivers are required for your enrolment device 23

7 Creating a new Morpho Biometric Card Type 24
- 7.1 Introduction 24
- 7.2 Procedure 24
- 7.3 Result 30

8 Creating a new Morpho Biometric Reader 31
- 8.1 Introduction 31
- 8.2 Before you begin 31
- 8.3 Procedure 31
- 8.4 Result 37

9 Enrolling Users 37
- 9.1 Configuring a Cardholder Biometrics Tile 37
- 9.2 Capturing Biometrics (Fingerprint or Finger Vein) 39
- 9.3 Capturing Biometrics (Hand) 40
- 9.4 Capturing Biometrics (Face) 43
- 9.5 Re-enabling Inactive Biometrics 45

10 Communications Encryption 46
- 10.1 Encryption using Command Centre 46
- 10.2 Encryption using the Biometric Encryption Utility 47
- 10.3 Known Issue 49
- 10.4 Unencryption 50
  - 10.4.1 Unencryption from the Server 50
  - 10.4.2 Unencryption using the Biometric Encryption Utility 51

11 Configuring Biometric Verification 54

12 Encoding Morpho Cards for Verification 55

Copyright © Gallagher Group Limited

13 Performing Overrides on a Morpho Biometric Reader....56
14 Morpho OSDP Configuration....58
14.1 Wiring Morpho Readers for OSDP....58
14.2 Configuring the Controller RS-485 Bus for OSDP....58
14.3 Overrides on Morpho OSDP Readers....61
14.4 Morpho OSDP Reader Display Messages....63
15 QR Code authentication mode at Morpho Readers....67
16 Troubleshooting....70

1 Introduction

The term biometric operation refers to the process of evaluating a biometric sample, (e.g. a person's fingerprint) for the purpose of authenticating a person's identity. Typically, a biometric sample is taken from a person and compared with one or more previously-captured biometric samples, called templates, to determine or verify that person's identity. The Biometric Integration feature provides the ability for Morpho biometric readers to be connected to Gallagher Command Centre and configured as hardware items, for the purpose of biometric identification.

There are several procedures that make up the process for configuring Biometric Integration, both within Gallagher Command Centre and externally from the Gallagher Command Centre system, (e.g. physically installing and configuring MorphoAccess readers).

This document covers the entire configuration process from start to finish.
Notes:

- If your site wants full CAPSS compliance (and has `NPSA=1` in the license file), Morpho should not be installed, otherwise your site will not comply with CAPSS 2024.
- MA2G readers are no longer supported from Command Centre vEL9.30 or later.

2 Biometric categories

Biometric operations fall into one of two different categories depending on how many templates a person's biometric sample is compared with during the operation, as follows:

Biometric Identification:
When a person's biometric sample, (e.g. their fingerprint or finger vein), is compared against all the fingerprints/veins in a database to determine who that person is, the biometric operation is called "biometric identification" because it has been used to identify who that person is.

Biometric Verification:
When a person identifies themselves prior to the biometric operation, (e.g. badging their card), and then the biometric operation is used to verify that the person is in fact who they say they are, this is called "biometric verification". This is done by comparing the biometric sample presented with just one template that has been previously identified as belonging to that person.

If a site chooses to control access by way of biometric identification (as opposed to biometric verification), then there is no need for a Cardholder to carry or use a card. However, if a site chooses to control access by way of biometric verification, then typically these Cardholders will carry a card that they will use to first identify themselves prior to a biometric operation verifying they are who they say they are.

Copyright © Gallagher Group Limited

3 Morpho Biometric Readers

Morpho Biometric Readers can capture a fingerprint from a Cardholder and compare it with a biometric template to determine how closely it matches. The results of that biometric operation can then be used to determine with more certainty that the cardholder is who they say they are.

Biometric Templates
When using biometrics for access control, the enrolment process encompasses three steps:

- Acquisition of the biometric image
- Conversion of the biometric image to a template (a mathematical representation of the biometric image)
- Storage of the template for authentication or identification purposes. Biometric images are not stored at enrollment or matching stations.

The biometric templates are stored as reference templates. A template is a set of 0's and 1's created using a mathematical formula that is patented called a template generator. It is not possible to reverse engineer the 0's and 1's or the mathematical representation of the biometric back to the biometric image. Images are converted to proprietary templates using a proprietary algorithm and are stored in a database located in the Biometric reader. The database of reference templates is encrypted using AES 256.

Display messages
Gallagher's Morpho Biometric Integration allows messages to be displayed on OSDP Morpho Biometric readers with LCD screens. If reader display messages are enabled, the current date and time, and the door's or Access Zone's status, are displayed on the screen when the reader is idle. Additionally, access granted and descriptive access denied messages are displayed when a finger, hand, face or card is presented at the reader. If two readers are assigned to the same Exit Zone or Entry Zone of a Door - one OSDP and one Wiegand - a Cardholder badging at the Wiegand reader will result in the more descriptive access message being displayed on the OSDP reader (as well as the regular message on the Wiegand reader).

Several default messages will display. See ***List of displayed messages*** in the "Open Supervised Device Protocol (OSDP) Integration" chapter of the *Command Centre Configuration Client User Guide* to see the messages that are displayed by default. If your site requires these messages to be changed, including whether the date and/or time are displayed, contact the Gallagher Support Team.

Copyright © Gallagher Group Limited

4 Installation

Note: This section provides step-by-step instructions for installing all the necessary MorphoAccess components. Additional information is available in the *Multiprotect License Protection User's Guide* (**doc-install.pdf**), located in the `'Utilities\Morpho\License Manager\Multiprotect License Manager 6.6.0\doc'` folder of the Command Centre installation files, if required.

4.1 Installing Microsoft Redistributables

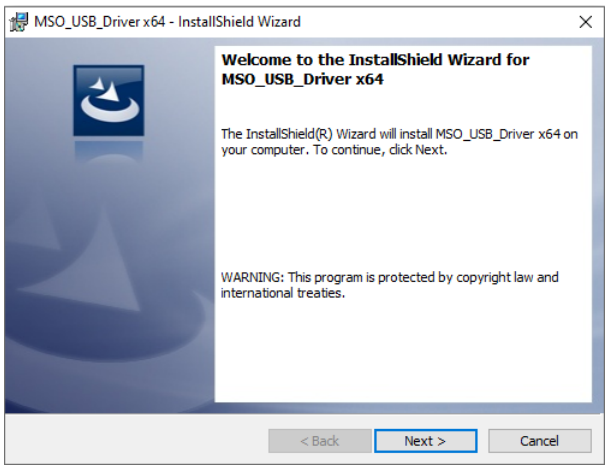
To install the Microsoft Visual Studio Redistributables (32-bit & 64-bit) on the capture workstation and server, follow these steps:

IMPORTANT: The Microsoft Redistributables must be installed on both server and workstation so that they are not affected by newer operating systems that don't have them.

1. Navigate to the `'Utilities\Morpho\Microsoft Redistributables'` folder of the Command Centre installation files.
   Note: VC10redist_x86, VC12redist_x86, VC14redist_x86 and VC14redist_x64 Microsoft Redistributables are required.
2. Open the **vc10redist_x86** folder and run the executable. Work your way through each screen.
3. Open the **vc12redist_x86** folder and run the executable. Work your way through each screen.
4. Open the **vc14redist** folder and run VC_redist.x86 and VC_redist.x64 executables. Work your way through each screen.
5. Once the Microsoft Redistributables have been installed, restart the computer.

4.2 Installing MSO330 and MSO1300 Drivers

1. Navigate to the `'Utilities\Morpho\Device Drivers\MorphoSmart'` folder of the Command Centre installation files.
2. Open the appropriate folder for your operating system, i.e.
   `'x64'` for a 64-bit operating system, OR
   `'x86'` for a 32-bit operating system
3. Run the **Setup.exe** executable as Administrator.
   The Welcome screen of the InstallShield Wizard displays.



4. Click the **Next** button.
   The Destination Folder screen displays.
5. If you want to change installation directory for MorphoSmart Drivers click the **Change…** button and select another directory, otherwise click the **Next** button.
   The Ready to Install the Program screen displays.

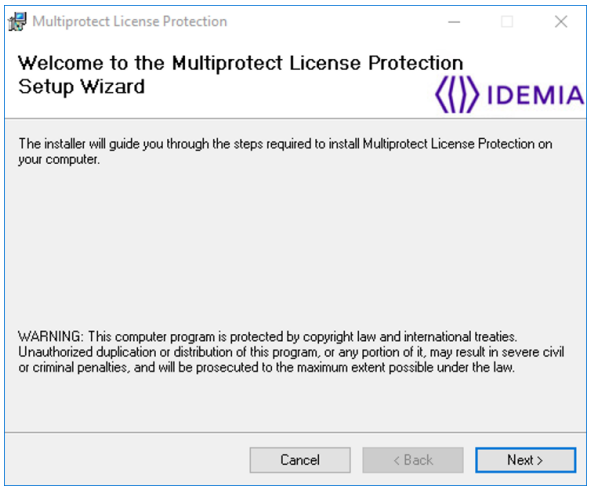
Copyright © Gallagher Group Limited

6. Click the **Install** button.
   Note: You may then be asked to validate installation of driver.
   Once installation has successfully completed, the Completed screen displays.
7. Click the **Finish** button.
   The installation wizard closes and a 'Restart PC' pop-up displays.
8. Click the **No** button.
   A restart of the PC does not need to be done until after you install the License Manager.

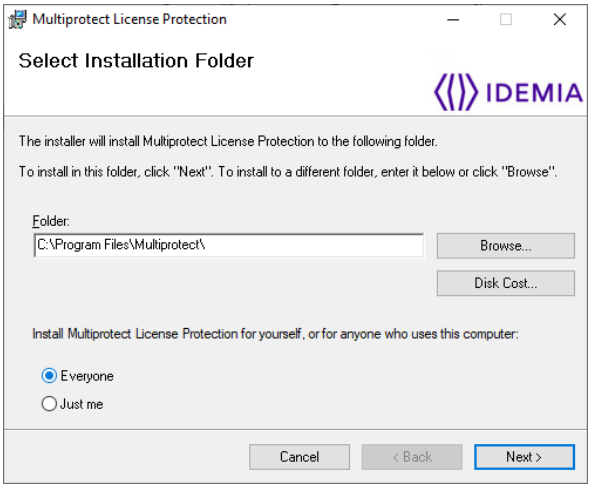
4.3 Installing the License Manager

IMPORTANT: You should install this software with Administrator rights (launch a command prompt as an administrator if you want to use MSI file), otherwise you should manually register. If the service is not registered, no ID or license will be displayed.

1. Path your way to the ''`Utilities\Morpho\License Manager\Multiprotect License Manager`' folder of the Command Centre installation files.
2. Run the **Multiprotect_License_Protection_Installer.exe** executable.
   The Welcome screen of the Multiprotect License Protection Setup wizard displays.



3. Click the **Next** button. The Choose Installation Mode screen displays.
4. Click the **Copy and install service** radio button, then the **Next** button.
   The Select Installation Folder screen displays.



5. Install Multiprotect License Protect for yourself, or for anyone who uses this computer by clicking the **Everyone** or **Just me** radio button as appropriate.

Copyright © Gallagher Group Limited

6. Click the **Next** button.
   The Confirm Installation screen displays.
7. Click the **Next** button.
8. Click the **Close** button.

4.4 How to Retrieve Host ID and Install VERIF Software License

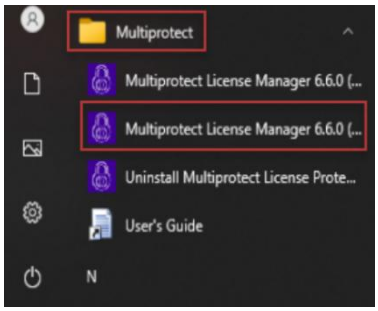
A VERIF license is required on each enrolment workstation that will be capturing biometrics.

IMPORTANT: VERIF Dongles are obsolete, you will need to install a software VERIF License, alternatively you can purchase an MSO enrolment device with an embedded VERIF license.

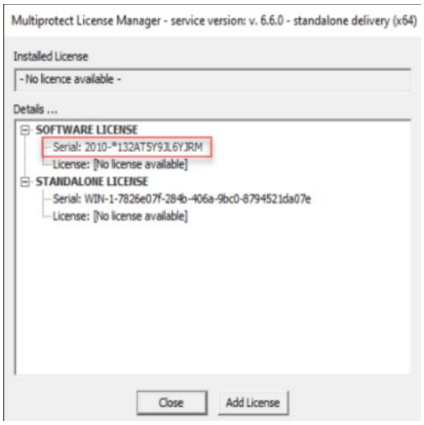
VisionPass & VisionPass SP Enrolment Readers do not require a VERIF License.
C864662 - Idemia Soft Verif License

Software Verif License alternatives:
You can now choose an MSO enrolment reader with a verif license embedded.
C864666 - Idemia 293670375 Bundle: MSO 330 with Verif License
C864667 - Idemia 293670362 Bundle: MSO 1300 with Verif License

1. To retrieve Host ID, click **Start**. Select **Multiprotect** and then select **Multiprotect License Manager (GUI)**.



2. In the Multiprotect License Manager window, the HOST ID is the serial number under SOFTWARE LICENSE. You can right-click the host ID and copy it to the clipboard.
   You can also view what software license is currently available on this machine.



3. Email the host ID to your local Gallagher Customer Service team or local Gallagher Sales team part number: C864662 to have your soft license generated. Soft license is delivered in a license file. The license file has Host ID as file name and file type is .lic.
   For example, 2010-_1BKBRD6DEEBSSEV.lic. (24 hour turnaround time).
4. Save the license file to your machine. Open Multiprotect License Manager (Step 2). Click **Add License** and browse to where the license file is stored and select the license file.
5. Once license is added successfully, you should see message *"License has been correctly set"*, and the license should appear under SOFTWARE LICENSE.

Copyright © Gallagher Group Limited

5 Installing MorphoAccess Readers

5.1 Configuring a Biometric Reader

Readers must be configured with their IP address to be available on the network. Default IP address: 192.168.1.10

Configuring your machine

First, you need to need to set your machine network to be able to communicate with the default IP address of the reader (192.168.1.10), for instance assigning IP address 192.168.1.100 to the PC.

To minimize possible issues in next steps, we recommend checking IP communication between the PC and the reader before proceeding, launch Command prompt and ping the reader.

5.1.1 Configuring Morpho Readers using MBTA application

Note: MorphoBioToolbox (MBTB) has been renamed Morpho Biometric Terminal Administrator (MBTA).

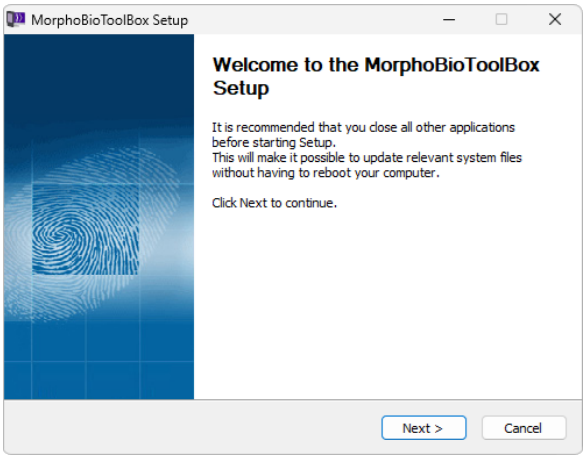
Before you begin

The following components must also be installed on your computer prior to Morpho Biometric Terminal Administrator installation:

- Microsoft Visual C++ 2022 Redistributable Package located `'Utilities\Morpho\Microsoft Redistributables\vc14redist'` folder of the Command Centre installation files.
- Locate and run **VC_redist.x64**
- Locate and run **ndp48-web** .NET Framework 4.8 located `'Utilities\Morpho\dotNet Framework'` folder of the Command Centre installation files.

Morpho Biometric Terminal Administrator installation

1. Copy the executable **MBTA (Terminal Administrator).exe** from the `'Utilities\Morpho\Morpho Biometric Terminal Administrator (MBTA)'` folder to an arbitrary directory on your local hard drive, and execute it. The Welcome screen of the Morpho Biometric Terminal Administrator Setup Wizard displays.



2. Click the **Next** button. The License Agreement screen displays.
3. Click the **I Agree** button. The Choose Install Location screen displays.
4. Choose the **Destination Folder** of MBTA installation, and click the **Install** button to start the proper installation.
   The Completion screen displays when the product is successfully installed.
5. Click the **Finish** button.

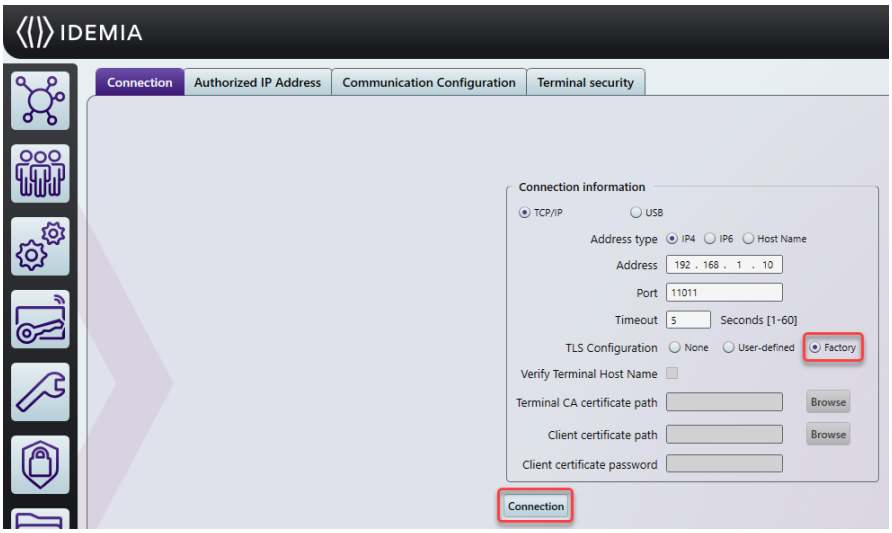
Morpho Biometric Terminal Administrator configuration

Copyright © Gallagher Group Limited

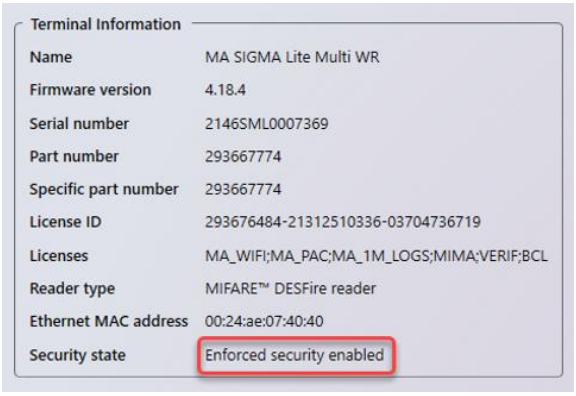
Note: Skip steps 7 to 10 if your device is unlocked. Any Morpho reader with a serial number greater than **2242**xxxxxxxxxx will have 'On-demand Security state' enabled out of the box (must use MBTB v4.6.12 or later for this to work).

6. Double-click the MBTA icon 

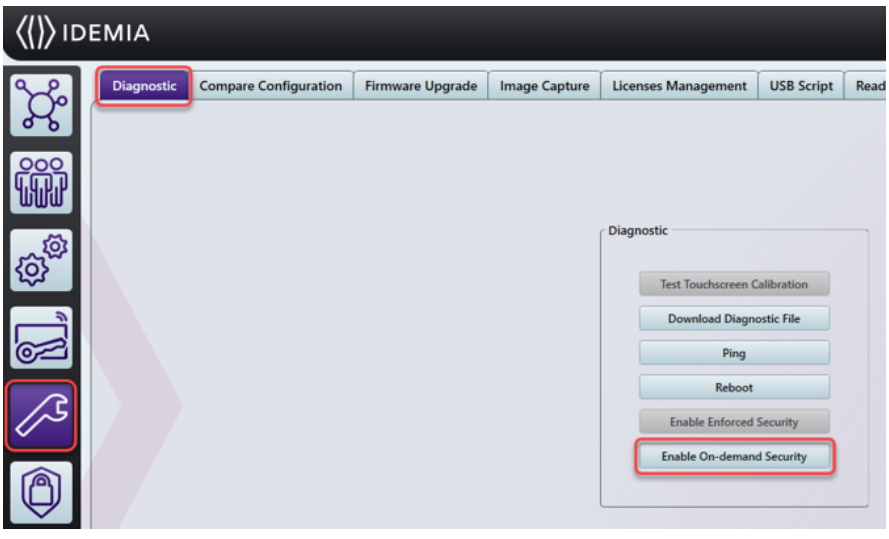
on your desktop.
7. Type in the IP address, click on the TLS Configuration **Factory** radio button and click the **Connection** button.



Note: When the device is in Enforced Security state, the security state Enforced security enabled is displayed.

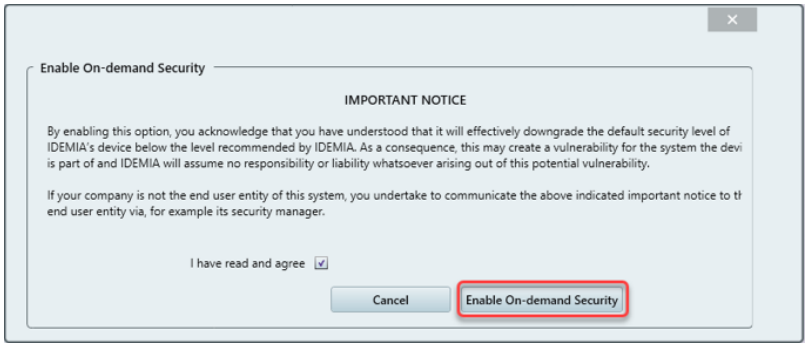


8. Click on the **Tools** icon.



Copyright © Gallagher Group Limited

9. Only one button is available in the **Diagnostic** section, (i.e. Enable On-demand Security). The purpose of this button is to enable the unsecured communication (TCP) on the default port 11010. After clicking this button, the below notice appears:

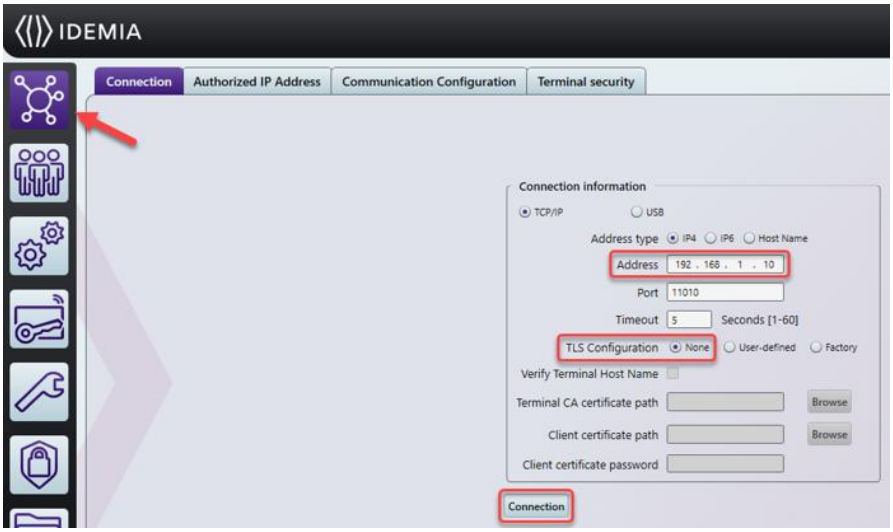


10. Once you have read the important notice carefully, tick the **I have read and agree** checkbox and click the **Enable On-demand Security** button. This message will confirm that your reader has been correctly unsecured:



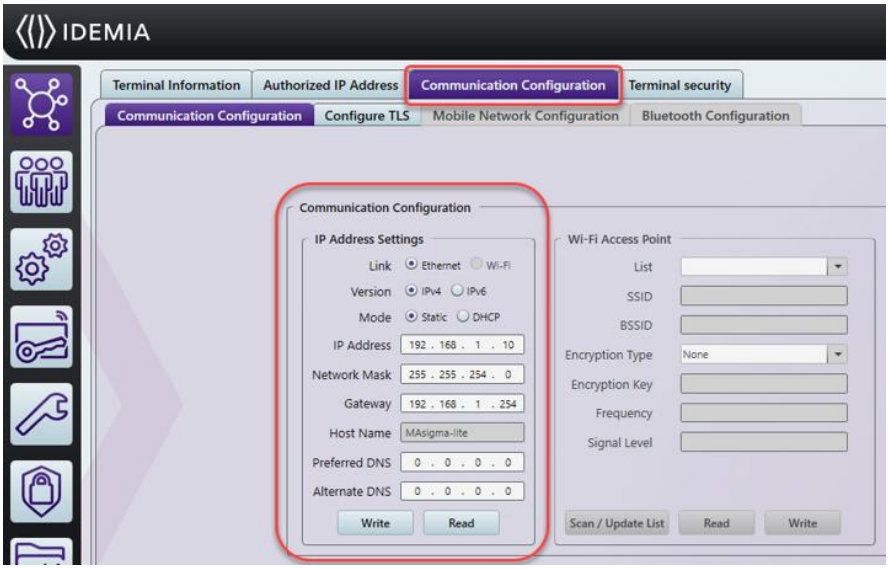
Now your reader is unsecured and you will be able to connect to it on port 11010.

11. Click on the **Network and Secure Communication** button on the left-hand side, type in the IP address of your reader, for the TLS Configuration click **None** and click the **Connection** button.



12. Modify the IP address of the reader. Click the **Communication Configuration** tab and modify the IP address settings as illustrated below:

Copyright © Gallagher Group Limited

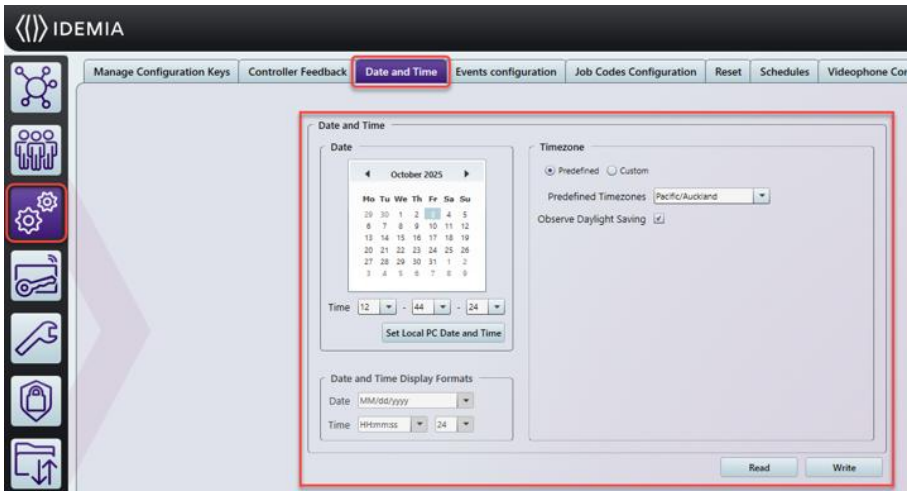


Note: Set the **Preferred DNS** and **Alternate DNS** as above by default (you cannot leave the 0.0.0.0 value).

13. Click the **Write** button to validate the new IP settings; it will disconnect the device.

    In order to reconnect it, modify the IP settings of your current machine or connect the device on your final network and connect it from a machine connected to this network.

14. Click the **Device Settings** button, and then the **Date and Time** tab.
    Set the correct time and Time zone for your site, click the **Write** button.



The message *"Date and time settings written successfully to device"* will appear. Click **OK**.

Copyright © Gallagher Group Limited

5.2 Supported MorphoAccess Readers

The following MorphoAccess readers and associated firmware versions are supported.
Important Notes:

- Gallagher recommends the latest release firmware version for supported devices.
- For site security, it is recommended that the default passwords on all Biometric readers be changed after readers have been configured.
- Changing default reader settings other than those mentioned in this document may adversely impact reader functionality.
- Morpho Biometric Readers have their time synchronised with the Command Centre server daily. By default, it synchronises at 3:30 am.
- IDEMIA ceased support for the Legacy (MA2G) communication protocol for all devices as of January 2022. Consequently, we no longer support MA2G.
- Upgrading to Command Centre v9.30 will not be possible if you have IDEMIA Legacy (MA2G) devices configured.
- All devices shipped from IDEMIA since October 2020 have been preloaded with MA5G firmware.
- IDEMIA recommend keeping device firmware up to date, as they regularly make improvements that protect against potential cyber attacks.
- Device firmware can be downloaded from the IDEMIA Biometric Devices Portal. See the tables below for a summary of supported and unsupported IDEMIA devices and communication protocols, plus recommendations.

5.2.1 Supported IDEMIA Devices and Firmware versions

IDEMIA Device	Communication Protocol	Recommendation	Most recent firmware version available
MA Sigma Light Series, MA Sigma Wide, MA Sigma Extreme	**MA5G** (**MA2G** unsupported from Command Centre v9.30)	Update firmware to Native (MA5G), as required	Latest Firmware available
MA Wave XP	**MA5G** only	Update firmware to latest version, as required	Latest Firmware available
MA Wave XP2			Latest Firmware available
MA Wave SP			Latest Firmware available
MA VisionPass			Latest Firmware available
MA VisionPass SP			Latest Firmware available

5.2.2 Unsupported EOL IDEMIA Devices

These devices will not be supported from Command Centre v9.30:

IDEMIA Device	IDEMIA End of Life (EOL) Date	Recommendations
MA100 Series	January 2013	Replace with MA Sigma Light Series
MAJ Series	Febhruary 2016	Replace with MA Sigma Light Series
MA500 Series	July 2016	Replace with MA Sigma Wide
Finger Vein Print - VP	June 2021	Replace with MA Wave

Copyright © Gallagher Group Limited

5.3 Upgrading the MorphoAccess Reader Firmware

To upgrade the firmware version on the MorphoAccess readers, follow the appropriate steps below:

- If the reader is encrypted, it will need to be unencrypted before upgrading. See ***10.4 Unencryption*** for further detail.
- Do not upgrade the reader via the USB method.

Enforced security firmware upgrade

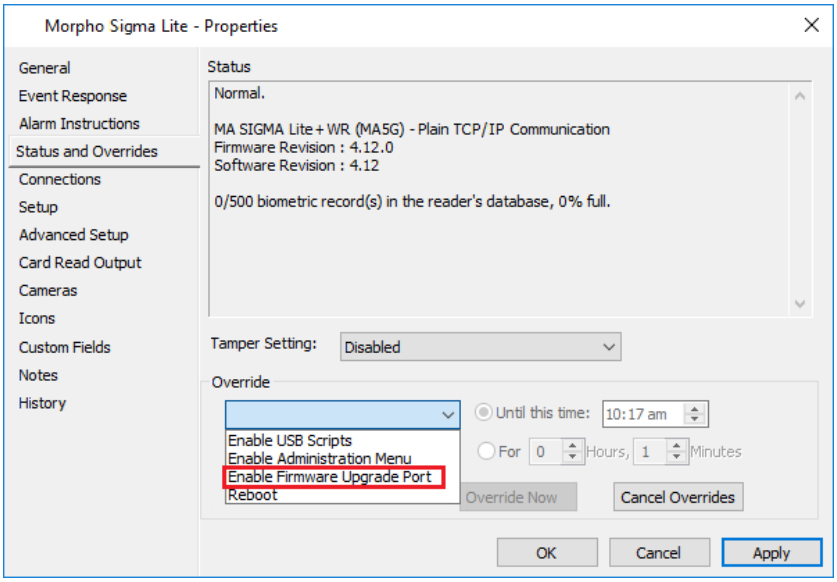
If you upgrade, your device will reboot and enforced security will be enabled.
Enforced security firmware version:
SIGMA Lite and Lite+, from firmware 4.12
SIGMA Wide, from firmware 4.12
SIGMA Extreme, from firmware 4.12
MorphoWave Compact / XP, from firmware 2.9
MorphoWave SP, from firmware 1.1
VisionPass, from firmware 2.9
VisionPass SP, from firmware 2.1.1

Installing the Morpho Biometric Terminal Administrator

Note: See ***5.1.1 Configuring Morpho Readers using MBTA application*** for the components that need to be installed prior to running Morpho Biometric Terminal Administrator.

Upgrading the Firmware

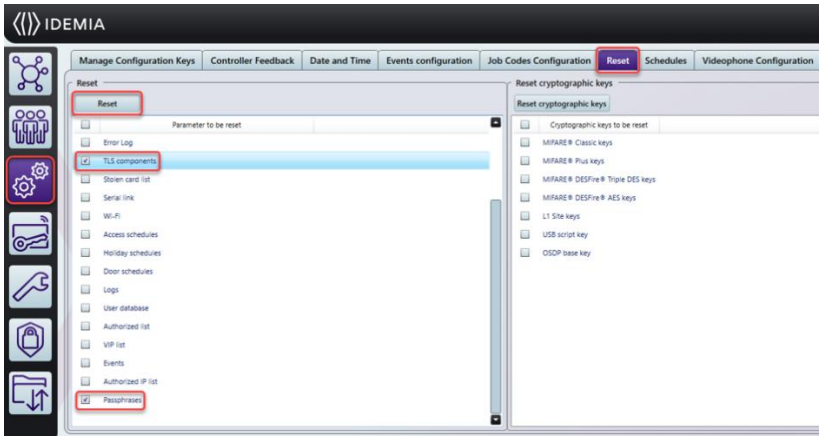
Note: For all Morpho Sigma readers, after Firmware Revision 4.6.0, the "Enable Firmware Upgrade Port" needs to be enabled before the firmware can be updated via the Morpho Biometric Terminal Administrator.



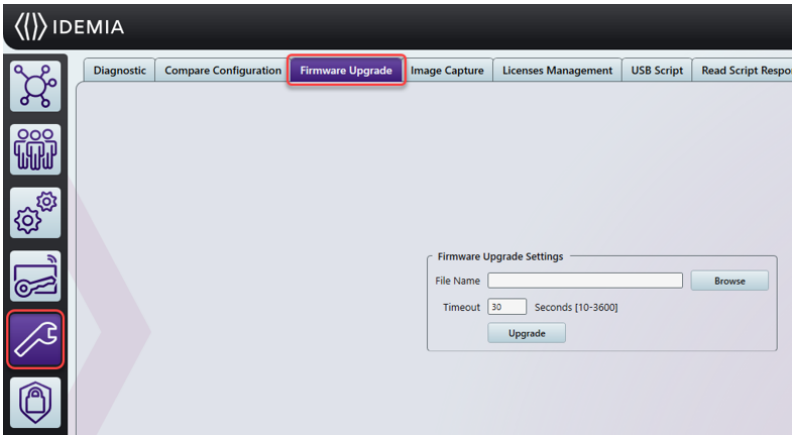
If you are upgrading to an enforced security version of firmware follow Steps 1 to 9. If not, start at Step 4.

1. From the Morpho Biometric Terminal Administrator Connection screen, select the **Device Settings** button, then click the **Reset** tab.

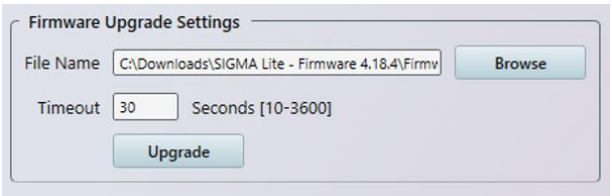
Copyright © Gallagher Group Limited



2. Select **TLS components** and **Passphrases**, then click the **Reset** button.
   The message *"Configuration parameters reset successfully"* displays.
3. Click the **OK** button.
4. From the MorphoBioToolbox Connection screen, select the **Tools** button.
5. Click the **Firmware Upgrade** tab.



6. Go to https://biometricdevices.idemia.com/s/products and download the latest firmware version for your Morpho Reader type. Extract the files to Local PC.
7. Click the **Browse** button, and navigate to the extracted Firmware file downloaded in the previous step.
8. Click the **Open** button.



9. Click the **Upgrade** button.
   Notes:
   - You may get prompted for an interim firmware version if your current version is significantly older than the version you are attempting to upgrade to.
   - **Firmware upgrade stuck during the upgrading process:** Older versions of firmware need to reboot to go into programming mode, if the device does not reboot correctly it will be stuck in this mode.
     1. Check you can ping your device.
     2. Using MBTB 4.4.7 type in IP address and follow the firmware upgrading process (Must use this version as newer versions don't have this feature).
     3. Upgrade firmware.

Copyright © Gallagher Group Limited

5.4 Physically installing MorphoAccess Readers

Install the reader as per the Morpho installation document supplied with the reader.

5.5 OSDP Wiring

Sigma Lite and Sigma Lite+ readers:

Morpho Readers that supports RS485 only	Controller RS485 Port
RS485_A Blue	A
RS485_B Blue / Red	B
RS485_GND Black / Red	-

VisionPass SP, VisionPass, MorphoWave, Sigma Extreme and Sigma Wide readers:

Morpho Readers that supports RS422 & RS485	Controller/OSDP Hub RS485 Port
RS485_TX_Y Green / Black	A
RS485_TX_Z Green / White	B
RS485_GND Black / Red (Black for VisionPass SP)	-

5.6 MA Sigma, MorphoWave, VisionPass SP and VisionPass Wiring

Ethernet (T568A standard)

These readers have an internal RJ45 connector which accepts a standard twisted pair cable. Alternatively, the terminal block can be used:

Reader	Cable Colour (T568A standard)	PIN #	10BaseT Signal / 100BaseT Signal
RX+	White/Green	1	Transmit +
RX-	Green	2	Transmit -
TX+	White/Orange	3	Receive +
TX-	Orange	4	Receive -

HBUS Wiegand Door Module

MA Sigma / MorphoWave / VisionPass Reader 1	HBUS Wiegand Door Module - Reader 1
Wiegand OUT 0 - Green	R1 DATA 0
Wiegand OUT 1 - White	R1 DATA 1
Wiegand LED 1 - Blue	R1 OUT 1
Wiegand LED 2 - Blue/Red	R1 OUT 2
Wiegand Ground - Red/Black (Black for VisionPass SP)	GND -

MA Sigma / MorphoWave / VisionPass Reader 2	HBUS Wiegand Door Module - Reader 2
Wiegand OUT 0 - Green	R2 DATA 0
Wiegand OUT 1 - White	R2 DATA 1
Wiegand LED 1 - Blue	R2 OUT 1
Wiegand LED 2 - Blue/Red	R2 OUT 2
Wiegand Ground - Red/Black (Black for VisionPass SP)	GND -

MA Sigma / MorphoWave / VisionPass Reader	Power Supply *
12V + (Red)	12V +
GND - (Black)	GND -

***** See ***5.7 Power Supply Requirements*** for further details.

Copyright © Gallagher Group Limited

Reader Module 4R / 8R

MA Sigma / MorphoWave / VisionPass Reader 1	Reader Module 4R / 8R
Wiegand OUT 0 - Green	R1 In
Wiegand OUT 1 - White	R2 In
Wiegand LED 1 - Blue	R2 OUT
Wiegand LED 2 - Blue/Red	R1 OUT
Wiegand Ground - Red/Black (Black for VisionPass SP)	GND -

MA Sigma / MorphoWave / VisionPass Reader 2	Reader Module 4R / 8R
Wiegand OUT 0 - Green	R3 In
Wiegand OUT 1 - White	R4 In
Wiegand LED 1 - Blue	R4 OUT
Wiegand LED 2 - Blue/Red	R3 OUT
Wiegand Ground - Red/Black (Black for VisionPass SP)	GND -

MA Sigma / MorphoWave / VisionPass Reader 3	Reader Module 8R
Wiegand OUT 0 - Green	R5 In
Wiegand OUT 1 - White	R6 In
Wiegand LED 1 - Blue	R6 OUT
Wiegand LED 2 - Blue/Red	R5 OUT
Wiegand Ground - Red/Black (Black for VisionPass SP)	GND -

MA Sigma / MorphoWave / VisionPass Reader 4	Reader Module 8R
Wiegand OUT 0 - Green	R7 In
Wiegand OUT 1 - White	R8 In
Wiegand LED 1 - Blue	R8 OUT
Wiegand LED 2 - Blue/Red	R7 OUT
Wiegand Ground - Red/Black (Black for VisionPass SP)	GND -

MA Sigma / MorphoWave / VisionPass Reader	Power Supply *
12V + (Red)	12V +
GND - (Black)	GND -

***** See ***5.7 Power Supply Requirements*** for further details.

Controller 7000 Single Door Wiegand Module

MA Sigma / MorphoWave / VisionPass Reader	7000 Single Door Wiegand Door Wiegand Module
Wiegand OUT 0 - Green	D0 Wiegand Data Input 0
Wiegand OUT 1 - White	D1 Wiegand Data Input 1
Wiegand LED 1 - Blue	LD Wiegand LED
Wiegand LED 2 - Blue/Red	BZ Wiegand Buzz
Wiegand Ground - Red/Black (Black for VisionPass SP)	- Common GND

Copyright © Gallagher Group Limited

5.7 Power Supply Requirements

Note: Morpho Biometric Readers require significantly more current than Gallagher readers. It is strongly recommended that a biometric reader is connected directly to the systems power supply and not to a Gallagher Controller or URI.

Reader	Requirements
SIGMA Lite and **SIGMA Lite+**	Either: • PoE IEEE802.3af, PoE+ IEEE802.3at type 1 compliant, or • 12V to 24V DC (regulated and filtered) 1A min @ 12V
SIGMA Extreme	Either: • POE mode IEEE802.3af, PoE+ IEEE802.3at type 1 compliant, or • 12V to 24V DC (regulated and filtered) 1A min @ 12V
SIGMA Wide	12V to 24V DC (regulated and filtered) 1A min @ 12V
MorphoWave XP / XP2 / Compact / MorphoWave SP and **VisionPass SP**	Either: • POE+ IEEE802.3at type 2 compliant, or • 12 to 24 Volts (regulated and filtered) 2.5 Amp min @ 12V, 1.25A min @ 24V
VisionPass	12V to 24V DC (regulated and filtered) 3A min @ 12V

IMPORTANT: It is important NOT to connect the MorphoWave and VisionPass Terminal to the Gallagher Controller or URI 12VDC output. The current requirements of the MWC exceeds the 12VDC supply from Gallagher hardware. **Failure to connect the Terminal to a suitable power source will damage the terminal and void the warranty.**

5.8 Updating VisionPass SP to VisionPass SP Fingerscan

The VisionPass SP Finger scanner license can be updated as follows:

Is the VisionPass SP device manufactured before or after June 2025?

If…	then…
after June 2025,	install the Fingerscan module (follow the instructions provided by Idemia).
before June 2025,	1. Upgrade the device firmware to version 3.1.5 2. Retrieve the License ID via MBTB or on the back of the VisionPass SP device. 3. Send the License ID and details to order@security.gallagher.com to request the **BT_VIP_FINGER** Fingerscan license (see section ***5.9 Morpho Extended Database Licenses*** next for more details). 4. When the updated license file is received, import and apply it using MBTB. 5. Install the Fingerscan module (follow the instructions provided by Idemia).

5.9 Morpho Extended Database Licenses

A Morpho Reader User Database can be extended by loading an Extended Database License. This may be required for identification from the database on the reader.
Note: The Extended Database License is specific to the Morpho Reader and the Morpho Reader "License ID" is required when purchasing the Extended Database Licence.

The License ID is located on the Morpho Readers label. *For example:*



Copyright © Gallagher Group Limited

5.9.1 Morpho Reader Default User Databases

Reader Model	Default User Database
MA Sigma Lite and MA Sigma Lite + Multi	Default 500 user Database. Reader DB expandable to 10,000 users.
MA Sigma Multi	Default 5000 user Database. Reader DB expandable to 50,000 users.
MorphoWave Compact / XP / XP2	Default 40,000 user Database. Reader DB expandable to 100,000 users.
MorphoWave SP	Default 10,000 user Database. Reader DB not expandable.
VisionPass	Default 20,000 user Database. Reader DB expandable to 100,000 users.
VisionPass SP	Default 10,000 user Database. Reader DB expandable to 50,000 users.

5.9.2 Available Morpho Reader Database Extension License

Reader Extension License	Gallagher Part. No.	Suppliers Part. No.	Extends database size…
Morpho Sigma 3K Upgrade License	C864106	293690335	to 3,000 users
Morpho Sigma 10K Upgrade License	C864107	293589574	to 10,000 users
Morpho Sigma Upgrade License (50K User)	C864114	293654719	to 50,000 users
Morpho Sigma Upgrade License (100K User)	C864115	293654727	to 100,000 users

5.9.3 Upgrade Database Extension License

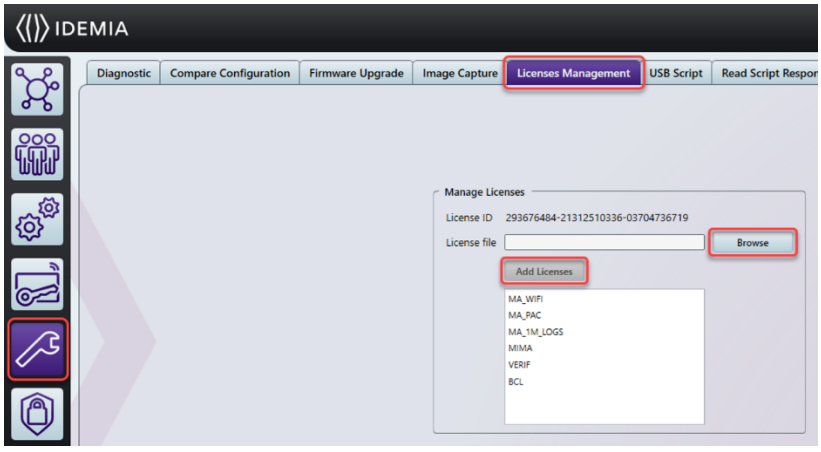
Requirements

- Morpho Licence Manager - Version 4.10.0 to 6.1.0 (located in the Morpho Utilities folder of the Gallagher Command Centre installation media vEL7.80 and above)
- Extended Database license that matches the Morpho Reader License ID
- PC network connectivity to the Morpho readers on port 11010

How to apply the Extensions

License Manager 6.3.0 and above

You need to use the Morpho Biometric Tool Box (MBTB) 4.8.0 and above to add the extended template license directly to the reader.



To add the licenses, select a license file using the **Browse** button and then click the **Add Licenses** button.
After the licenses are added successfully, the licenses are displayed in the list and will be updated immediately.

Copyright © Gallagher Group Limited

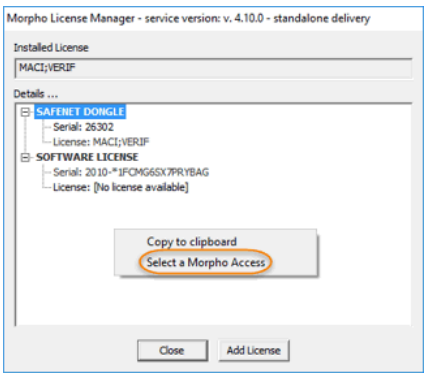
Multi Protect License Manager 4.10 to 6.1.0

Install Morpho License Manager version 4.10.0 on your server (Gallagher Command Centre installation media vEL7.80 and above).

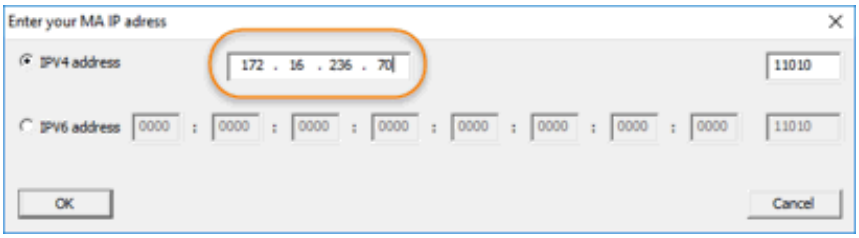
Notes:

- The Morpho Licence Manger can be installed on a laptop or pc, as long as it has network connectivity to the Morpho readers.
- This method is supported until version 6.1.0 of MultiProtect License Manager. Use MBTB 4.8.0 or above to complete this is you are using an unsupported version.

1. Open the Morpho Licence Manager, right-click in the empty white space and click **Select a Morpho Access**.

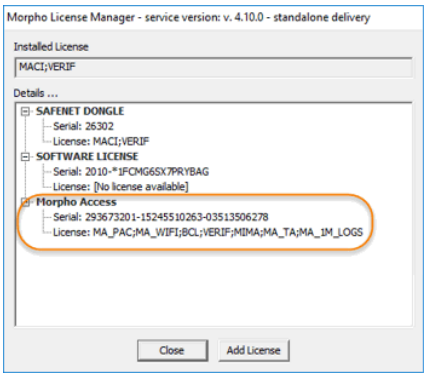


2. Input the IP Address of your Morpho Reader and click the **OK** button.



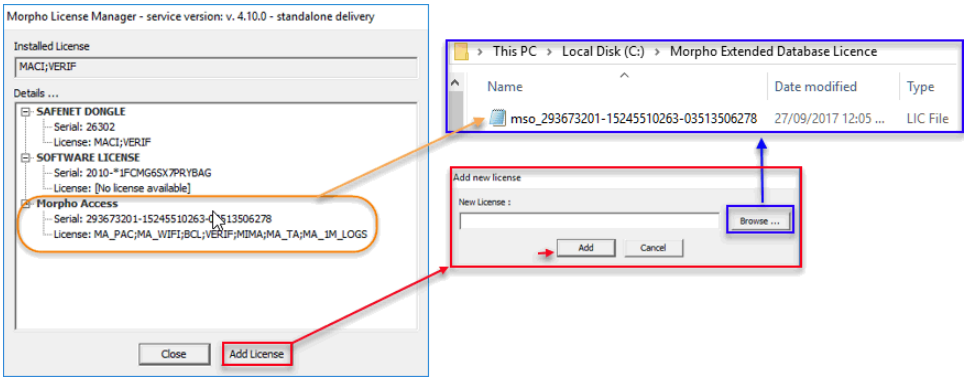
The **Morpho Access** reader serial number displays.

Note: The serial number matches the License ID that is printed on the readers label.

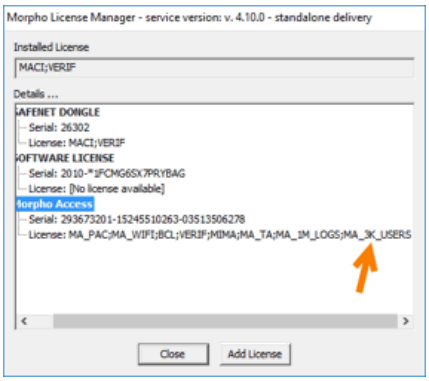


3. Click the **Add License** button. The Add new license window displays.
4. Browse to the Morpho Extended Database License specific to the reader you are connected to. The License number will match the Morpho Access serial and readers License ID.

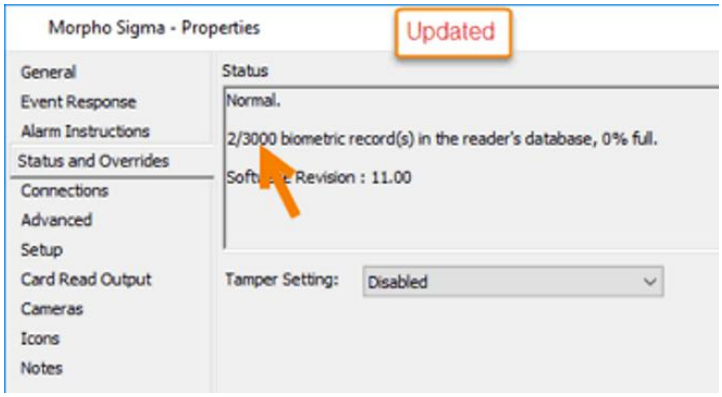
Copyright © Gallagher Group Limited



5. Once the License has been selected click the **Add** button.
   The message *"License has been correctly set"* displays on a confirmation window, and the Morpho Access license will display the new user database size.



   In the Gallagher Command Centre Configuration client, right-click on the Morpho reader and select the **Re-sync Databases** option. Open the Morpho reader properties and on the "Status and Overrides" tab the new user database size will be displayed.



Copyright © Gallagher Group Limited

6 Supported Enrolment Devices

The supported Morpho enrolment devices are:

	**MSO 330/MSO 1300** • Fingerprint enrolment device. • Enrols users Finger templates for use with Morpho Readers. • USB connection to Gallagher enrolment workstation. **Note:** MSO 330 works with vEL8.90 and above.
	**MorphoWave/MorphoWave SP** • Wave enrolment device. • Enrols users Wave templates for use with MorphoWave Readers. • Ethernet connection to Gallagher enrolment workstation.
	**VisionPass/VisionPass SP** • Face detection enrolment device. • Enrols users' facial templates for use with VisionPass Readers. • Ethernet connection to Gallagher enrolment workstation. • No VERIF dongle is required for VisionPass enrolment. **Note:** If your site uses both VisionPass and VisionPass SP access readers, you must use VisionPass for enrolment. However, if the site exclusively uses VisionPass SP readers, then a VisionPass SP enrolment reader will suffice.
	**VisionPass SP Fingerscan** Command Centre vEL9.50 offers support for the VisionPass SP Fingerscan Module. Functionality is limited to: • Biometric face or fingerprint authentication exclusively. • Card plus biometric access is only compatible with face templates stored on the card. • Fingerprint templates on the card are not supported by the VisionPass SP Fingerscan Module.

Copyright © Gallagher Group Limited

6.1 Which Firmware and Drivers are required for your enrolment device

The MorphoSmart MSO enrolment device is shipped with the latest Firmware and USB drivers loaded.

Enrolment device	Firmware	USB Drivers
MSO 300	V11.04.b	V4.6.0.0
MSO 330	V01.00.e	V4.6.0.0
MSO 1300	V05.01.e	V4.8.4
MorphoWave Compact / XP	V1.5.3	n/a (Ethernet connection)
MorphoWave XP2	V3.1.2	n/a (Ethernet connection)
MorphoWave SP	V1.0.0	n/a (Ethernet connection)
VisionPass	V2.14.4	n/a (Ethernet connection)
VisionPass SP	V2.2.3	n/a (Ethernet connection)
VisionPass SP Fingerscan	V3.1.5	n/a (Ethernet connection)

IMPORTANT: VisionPass reader needs firmware version 2.14.4 to enrol face templates.

IDEMIA VisionPass and MorphoWave Readers can be used as enrolment devices OR for access purposes at a door. (It is not recommended to use the access reader as the enrolment reader.)

MorphoWave and VisionPass Readers used for…	
enrolment only,	• are not in Command Centre and are limited to enrolment functionality. • are configured on the enrolment workstation with the special Morpho 'dongle' (a device that allows 'biometric samples' to be transformed into 'biometric templates' for storage in Command Centre). • can be redeployed for access purposes by first removing the enrolment configuration. **Note:** To help protect 'biometric samples' during enrolment, since network communications with enrolment readers are not encrypted, sites may directly connect the reader via a short cross-over cable to a separate (second) network port on the workstation.
access purposes at a door,	• are added to Command Centre as a Morpho Biometric Reader item. • can have encrypted network communications (for access configuration and 'biometric templates').

Copyright © Gallagher Group Limited

7 Creating a new Morpho Biometric Card Type

7.1 Introduction

A Morpho Biometric Card Type needs to be created in Gallagher Command Centre Configuration Client before the readers are added. This procedure describes how to create a new Morpho Biometric Card Type.

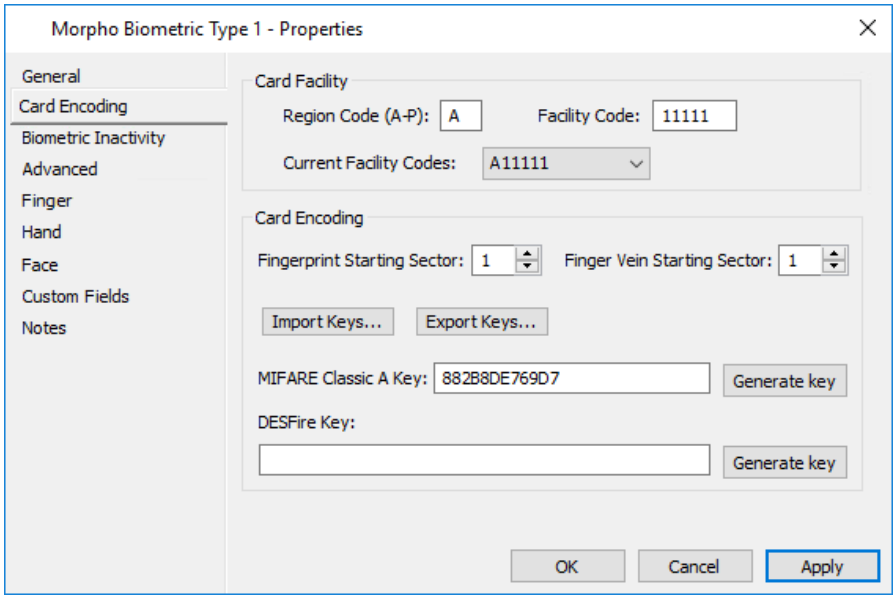
Notes:

- Only **one** Morpho Biometric Card Type is available per Command Centre Server.
- Operators require the "Configure Site" operator privilege to create, edit, view and delete Biometric Types, including the MIFARE Key on the **Card Encoding** tab.
  If an operator has the "View Site" operator privilege, but not "Configure Site", they will be able to view Biometric Type properties, EXCEPT for the MIFARE Key properties.

For multi-server systems, each server needs to have a Morpho Biometric Type set up manually, otherwise cardholders with a Biometric Type from a remote server will not be replicated on the local server. Biometric inactivity is managed by each server independently, using the Morpho Biometric Type configuration unique to each server.

7.2 Procedure

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. **Right click** and select **New...Morpho Biometric Type**.
   By default the **General** tab displays.
   Note: Only one Morpho Biometric Type can exist in the system at any one time.
3. Enter a **Name** and **Description**, and select the appropriate **Division**.
4. Click the **Card Encoding** tab.



5. Configure the settings on this screen as appropriate.

Copyright © Gallagher Group Limited

Field	Description
Region Code	This is the letter representing the **Region Code** for your Facility Code. **Note:** 'A' is the default and should be changed to match the Region Code in your site license. Refer to the **Licensing** tab of the Server Properties for the Region Code.
Facility Code	Although any Facility Code can be used for the Morpho Biometric Card Type, we recommend using the **Facility Code** as listed in the site license. Refer to the **Licensing** tab of the Server Properties for the Facility Code.  Note the Facility Code can only be changed once. If changed, it will require all existing fingerprint templates to be re-captured.
Current Facility Codes	If your site Facility Code has already been entered, then select it from this drop-down list. Adjust the card number allocation of existing Card Type, range needs to be 31 to 8388607.
Capture Type	Options for 'Fingerprint Only' or 'Fingerprint +Vein'. This drives the behaviour within the system for correct templates to capture during enrolment and associated warnings.

6. The **Card Encoding** section is required for card encoding.

Field / Button	Description
Fingerprint Starting Sector and Finger Vein Starting Sector	These fields allow you to select which sector of the MIFARE object will be used. (Range = 1 - 6. Default = 1)
MIFARE Classic A Key	The key entered here will be used to provide protection around reading cards encoded with Morpho biometric templates. This key will provide read access to the Morpho section of encoded cards. **Notes:** • The A Key on the Morpho Card Type should match the A Key on the Card Object. • This key must be unique to sites to prevent cards being used on other sites. Therefore, it is recommended you use the **Generate key** button. • The key is masked with 'X' characters once **Apply** is clicked.
Generate key button	Clicking this button automatically generates a random value that populates the **MIFARE Classic A Key** field.
DESFire Key	The key entered here is used to control access to the Morpho data encoded on a card. **Note:** • In order to prevent cards from another site being used, this key must be unique. To achieve this, it is recommended you use the **Generate key** button. • The key is masked with 'X' characters once **Apply** is clicked.
Generate key button	Clicking this button automatically generates a random value that populates the **DESFire Key** field.

7. If your site is a Multi-Server system, and you need to export a key to send to another system, perform the following steps:
   a) Click the **Export Keys...** button.
   A 'Please choose a password' dialog displays.
   b) Enter a password.
   Note: The password must be at least eight characters long, and can be a maximum of 32 characters.

Copyright © Gallagher Group Limited

c) Click the **OK** button.
A 'Save As' dialog displays with a default filename **MorphoBiometricKeys.txt**

d) Change the default filename if required, and path your way to the location where you want to save the key file.

e) Click the **Save** button.
The message *"Key successfully exported and protected by your password"* displays.

8. If you want to import a key from an exported file, perform the following steps:

a) Click the **Import Key…** button.

b) Path your way to the location where the key file you want to import is located and click on the key file you want to import.

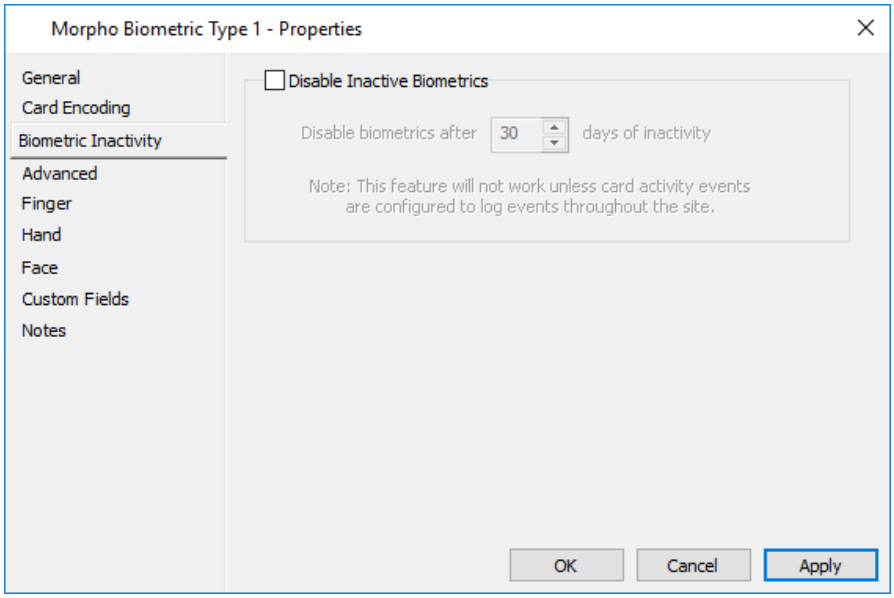
c) Click the **Open** button.
An 'Enter password' dialog displays.

d) Enter the correct password for the selected key file (this password will need to be supplied by the site that exported the key).

e) Click the **OK** button.
The **MIFARE Classic A Key** field displays the text 'IMPORTED KEY', and/or the **DESFire Key** field displays the text 'XXXXXXXXX IMPORTED KEY XXXXXXXXX' to confirm the key has been imported successfully.
Note: Keys exported by earlier versions than vEL8.00 of Command Centre cannot be imported.

f) Click the **Apply** button to save the new key(s).
The key is masked with 'X' characters.

9. Click the **Biometric Inactivity** tab.



10. Do you wish to enable the Inactive Biometrics Expiry feature?

If…	**then…**
yes,	check the **Disable Inactive Biometrics** checkbox, and go to Step 11.
no,	leave the **Disable Inactive Biometrics checkbox** unchecked, and go to Step 12.

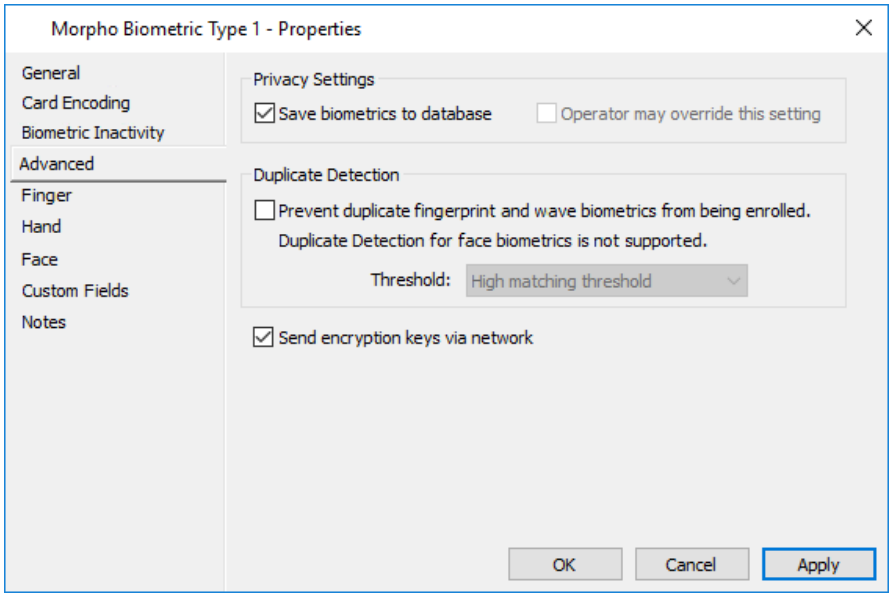
11. Enter a figure to represent the number of days of inactivity that will disable biometrics.
Notes:

- When this feature is first enabled the default timeout = 30 days. The range is 1-999 days.
- If you set the biometrics to disable after 1 day of inactivity, they will become disabled 24 hours to the second after the **Apply** button is clicked.

Copyright © Gallagher Group Limited

- Cardholders will be expired regardless of activity if card activity events are not configured to log events throughout the site (via the **Event Defaults** tab of the Server Properties).

12. Click the **Advanced** tab.



Note: The fields will be populated with any previously configured values for existing biometric types.

13. Configure the **Privacy Settings**, (i.e. Template Storage Mode settings), as required.
    These settings control whether or not biometric templates will be stored in the Command Centre database, and whether or not operators may override this setting for individual Cardholders.
    Note: For privacy reasons, some sites may want to prevent templates from being stored in the Command Centre database, and instead encode them onto cards.

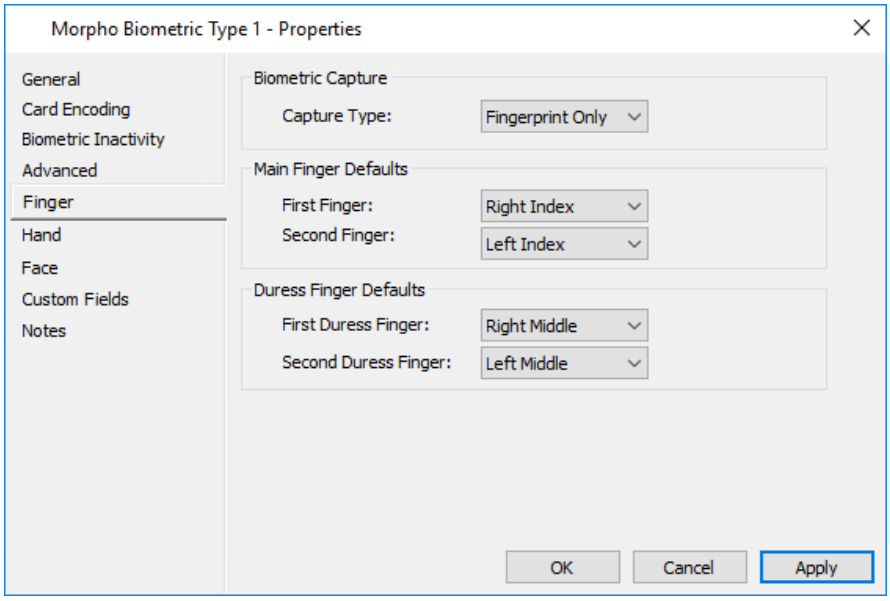
14. The 'Duplicate Detection' option prevents the same fingerprint/vein/Wave template from being enrolled twice.
    Check the **Prevent duplicate biometrics from being enrolled** checkbox if required, and select the appropriate **Threshold** from the drop-down list.
    Notes:
    - The first time this option is selected and applied, the system will check for any duplicate fingerprints and raise an event for each duplicate it finds.
    - For the 'Duplicate Detection' feature to work, an IDENT License and USB Dongle (C864403/ C864405) are required on the server.
    - Duplicate Detection for face biometrics is not supported.

15. Ensure the **Send encryption keys via network** checkbox remains checked, if you require Command Centre to send the encryption keys and certificates to the biometric readers via the network.
    See ***10.1 Encryption using Command Centre*** for further detail.

A non-network solution, (i.e. the **Send encryption keys via network** checkbox is not checked), requires a separate Biometric Encryption Utility that can be used on a laptop or similar in a safe room/network to connect to the readers and assign them the appropriate keys and certificates. This is done from the reader properties.
See ***10.2 Encryption using the Biometric Encryption Utility*** for further detail.

16. Is your site using Morpho Fingerprint or Finger Vein readers?
    If **no**, go to Step 18.
    If **yes**, click the **Finger** tab.

Copyright © Gallagher Group Limited

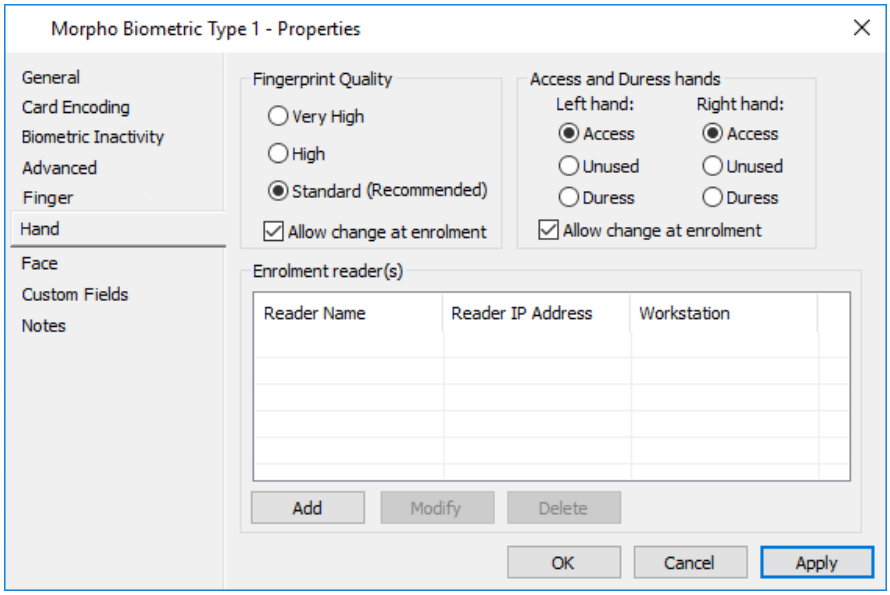


17. Configure the settings on this screen as appropriate.

Field	Description
Capture Type	Options for 'Fingerprint Only' or 'Fingerprint +Vein'. This drives the behaviour within the system for correct templates to capture during enrolment and associated warnings.
Main Finger Defaults *	Select the required fingers from the drop-down lists, to be used for normal day-to-day identification at a reader.
Duress Finger Defaults *	Select the required fingers from the drop-down lists, to be used for identification at a reader when under duress.

* **Note:** All four finger selections on this screen must be unique. If a finger selection is not unique, an error message will display.

18. Is your site using MorphoWave readers?
    If **no**, go to Step 23.
    If **yes**, click the **Hand** tab.



This screen allows you to identify network connected MorphoWave Readers intended for enrolment.
Note: MorphoWave Readers that are used for enrolment do not get added to Command Centre as Morpho Biometric reader items. These readers are only configured on this screen, and are

Copyright © Gallagher Group Limited

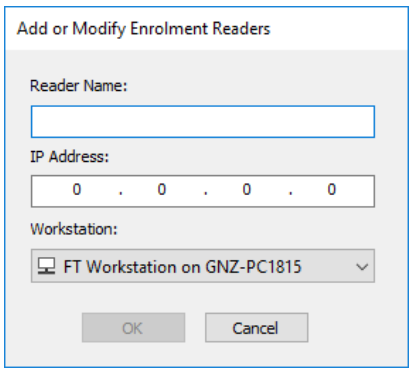
limited to enrolment functionality only. If a site decides it wants to use an enrolment reader for access purposes, they can remove the enrolment configuration and create the reader as a Morpho Biometric Reader item, allowing them to then use the reader for access at a door.

Encrypted MorphoWave readers cannot be used for enrolment. A connection error will be seen when trying to capture.

19. Configure the settings on this screen as appropriate.

Section	Description
Fingerprint Quality	Click the appropriate radio button for a default acceptable fingerprint quality. (Default and recommended option = Standard) If you want operators to have the ability to change the acceptable quality at the time of enrolment, tick the **Allow change at enrolment** checkbox.
Access and Duress hands	Set default access and duress hands. (Default = Both hands for access, therefore none for duress) **Note:** A minimum of one hand must be selected for access. If you want operators to have the ability to change the access and duress hands at the time of enrolment, tick the **Allow change at enrolment** checkbox.

20. Select the network connected MorphoWave readers that will be used for enrolment by clicking the **Add** button.
The Add or Modify Enrolment Readers dialog displays.

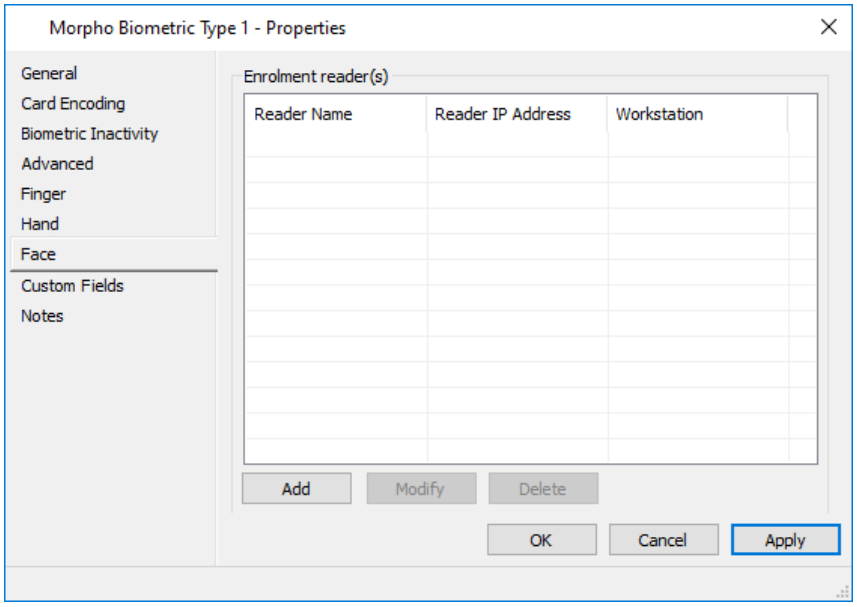


21. Enter the **Reader Name** and **IP Address**, and select the appropriate **Workstation** from the drop-down list.

22. Click the **OK** button.
The Add or Modify Enrolment Readers dialog closes, and the readers details populate the **Enrolment reader(s)** grid.
Notes:
    - The **Modify** button allows existing Enrolment Readers to be modified, and the **Delete** button allows them to be deleted.
    - Enrolment of a cardholder's fingerprints for use by a MorphoWave Reader is done via the **Cardholder Biometrics** tile in the Command Centre client. See *"Cardholder Biometrics Tile actions"* in the Command Centre Client Help file for further detail.
    - From v9.30 onwards, multiple workstations can be linked to the same enrollment reader IP Address, by creating a new Enrolment reader item with a different workstation.

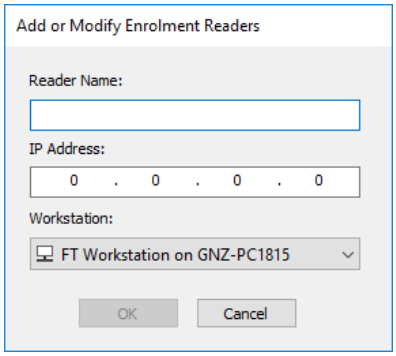
23. Click the **Face** tab.
Configuration on this tab is only required if your site is using VisionPass readers.

Copyright © Gallagher Group Limited



Encrypted VisionPass readers cannot be used for enrolment. A connection error will be seen when trying to capture.

24. Specify the network connected VisionPass readers that will be used for enrolment by clicking the **Add** button. The Add or Modify Enrolment Readers dialog displays.



25. Enter the **Reader Name** and **IP Address**, and select the appropriate **Workstation** from the drop-down.
26. Click the **OK** button. The Add or Modify Enrolment Readers dialog closes, and the readers details populate the **Enrolment reader(s)** grid. **Notes:**
    - The **Modify** and **Delete** buttons only become enabled when a Reader is clicked on in the **Enrolment reader(s)** grid, allowing existing readers to be modified or deleted.
    - From v9.30 onwards, multiple workstations can now be linked to the same enrolment reader IP Address.
27. Click the **Notes** tab if you want to add a note(s) about this Morpho Biometric Type.
28. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

7.3 Result

A Morpho Biometric Card Type has been configured and is ready to use.
To capture fingerprints against cardholders, see ***9 Enrolling Users***.

Note: You cannot delete Morpho Biometric Types if there are any Cardholders enrolled with Morpho Biometrics or any Morpho Biometric Readers configured to be assigned to Gallagher Controllers, Doors, Elevator Cars or HLI Elevator Cars.

Copyright © Gallagher Group Limited

8 Creating a new Morpho Biometric Reader

8.1 Introduction

This procedure describes how to create a new Morpho Biometric Reader, and configure system-wide settings for it.

8.2 Before you begin

Before you begin this procedure ensure that a Morpho Biometric Type has already been created. See ***7 Creating a new Morpho Biometric Card Type*** for the procedure.

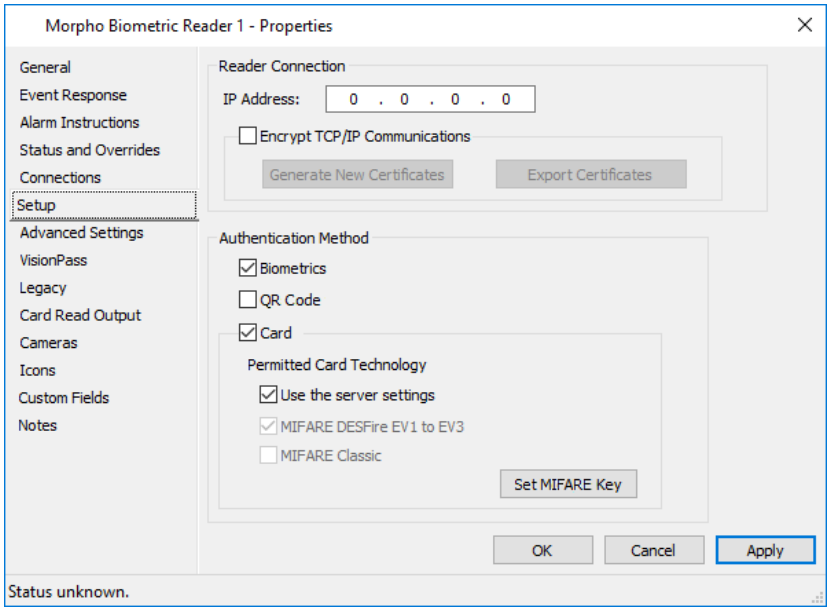
8.3 Procedure

Configuring the Morpho Biometric Reader

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
2. **Right click** and select **New...Morpho Biometric Reader**.
   By default the **General** tab displays.
3. Enter a **Name** and **Description**, and select the appropriate **Division**.
4. Click the **Event Response** tab and assign a primary Alarm Zone for all events.
5. Click the **Alarm Instructions** tab and assign Alarm Instructions to each of the Event Types and/or their Event Group as required.
6. Morpho Biometric Readers have tampers which monitor whether the LCD screen has been removed/ damaged, or the reader has been removed from the wall. By default, if either of these tampers are triggered, an alarm is raised, a buzzer sounds, and an LED flashes.

   If you want to prevent tamper alarms from being generated, click the **Status and Overrides** tab and change the **Tamper Setting** to "Disabled". Alternatively, you can change the **Tamper Setting** to "Send alarm" if you want an alarm to be raised but no buzzer activated.

   Other temporary security override can be performed from the **Status and Overrides** tab.
   See ***13 Performing Overrides on a Morpho Biometric Reader*** for further detail.
7. Click the **Setup** tab.



8. Configure the settings in the **Reader Connection** section as appropriate.
   Note: The fields will be populated with any previously configured values for existing biometric readers.

Copyright © Gallagher Group Limited

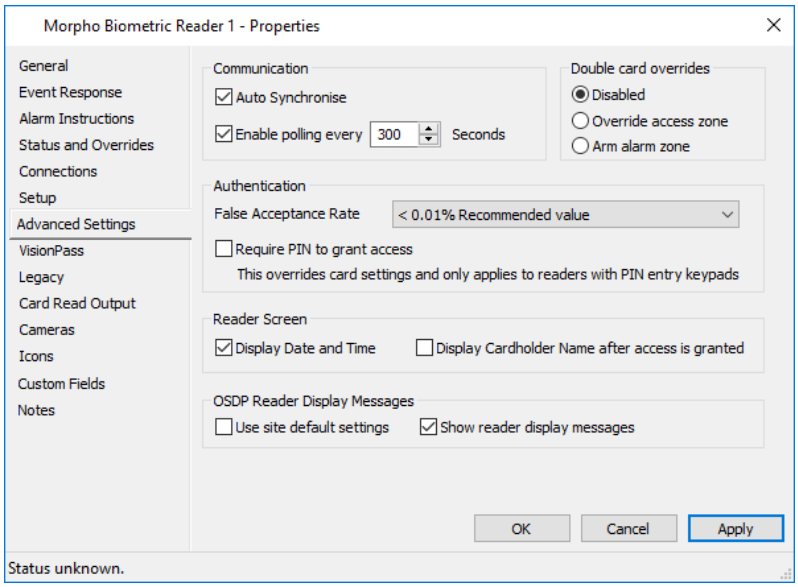
Field/Checkbox	Description
IP Address	Enter the IP Address of this reader (as previously configured in ***6.1 Configuring a Biometric Reader***). **Note:** DHCP is not supported for Morpho Readers' IP Addresses. (Default = 192.168.1.10)
Encrypt TCP/IP Communications	This option is off (disabled) by default. If you want to use encrypted communications for this reader, refer to ***10 Communications Encryption*** for further detail.

9. Configure the settings in the **Authentication Method** section as appropriate.

Field/Checkbox	Description
Authentication Method	This is a flag that determines whether or not the Cardholder has card-only access, or must present their finger, or enter a PIN, (or both), or use a QR Code. The reader has to authenticate a Cardholder using one of these methods. Options are: • **Biometrics** (1-to-many Identification) • **QR Code** (Verification with a QR Code) • **Card** (1-to-1 Verification) **Notes:** • If the Authentication Method is changed the database does not re-sync. • When **Card** mode is selected, and **Require PIN to grant access** (on the **Advanced Settings** tab) is enabled, if there is no PIN number set for the card, the cardholder will be denied access.

10. In the Permitted Card Technology section, **Use the server settings** is selected by default.
    If you want to select other types of cards to be accepted at the reader, uncheck the **Use the server settings** checkbox and select the appropriate checkboxes.

    Note: If you attempt to set a Biometric reader to follow the site default, but the site default does not allow either of the card technologies that the Morpho reader does (MIFARE Classic or DESFire), you get the error message *"The selected permitted card technology settings are not supported by the biometric reader"*. To resolve, you can either change the server settings to allow at least one of those two card technologies, or just not have the Morpho reader follow the site-wide settings.
11. If cards are encoded with Morpho data, the MIFARE data need to be sent down to the Morpho reader. To set the MIFARE Key, click the **Set MIFARE Key** button on each Morpho reader that will be used with the cards. When the **Set MIFARE Key** button is clicked the Reader MIFARE Key is updated.
    IMPORTANT: This needs to be done at least once if your site is planning to use cards with the reader.
12. Click the **Advanced Settings** tab.



13. Configure the **Communication** settings on this screen as appropriate.

Copyright © Gallagher Group Limited

Field	Description
Auto Synchronise	Enabling this checkbox means that this reader will be updated on a 'real-time basis', (i.e. as soon as a change is made in Command Centre). If this checkbox is disabled an operator will still be able to update the reader manually using any of the manual options available, including using macros. (Default = Checked)
Enable polling	If polling is enabled, the reader will be polled as soon as possible after the reader's Poll Time has elapsed since the last connectivity poll, biometric update, database resync, reader configuration or refresh status request has occurred. (Poll Time range = 10 - 300 seconds) **Notes:** • A high polling frequency, (i.e. a low Polling Interval value), might not be achievable on sites that have a lot of readers. For more information, please contact Gallagher Technical Support. • Higher polling rates mean a longer delay before offline alarms occur.
Double card overrides	If you want to configure double card overrides for this reader, click either the **Override access zone** or the **Arm alarm zone** radio button, depending on whether you want the double card override to override the state of the Access Zone or arm the Alarm Zone associated with the Access Zone. Leave the **Disabled** radio button checked if double card overrides are not required.

14. Configure the **Authentication** settings as appropriate.

Field	Description
False Acceptance Rate (FAR)	This value determines the required closeness of a match when comparing two templates for the purpose of verifying captured biometric templates. The False Acceptance Rate (FAR) setting of the reader impacts on the False Rejection Rate (FRR) at that reader, (e.g. the lower the FAR setting, the higher the FRR). **Note:** Selecting a low FAR setting is more secure because there is less chance that the reader will positively authenticate a person that it shouldn't, but there is also a greater chance that the reader could fail to positively authenticate a person when it should, (i.e. a higher FRR). (Default = < 0.01% Recommended value)
Require PIN to grant access	This setting only applies to biometric readers that have pin entry keypads. Enabling it will override the 'Reader ignores PIN' setting on the card layout. The reader will always request a PIN from the cardholder. **Note:** When **Require PIN to grant access** is enabled, **Biometrics** and **QR Code** authentication methods (on the **Setup** tab) cannot be applied.

15. Configure the **Reader Screen** settings as appropriate.

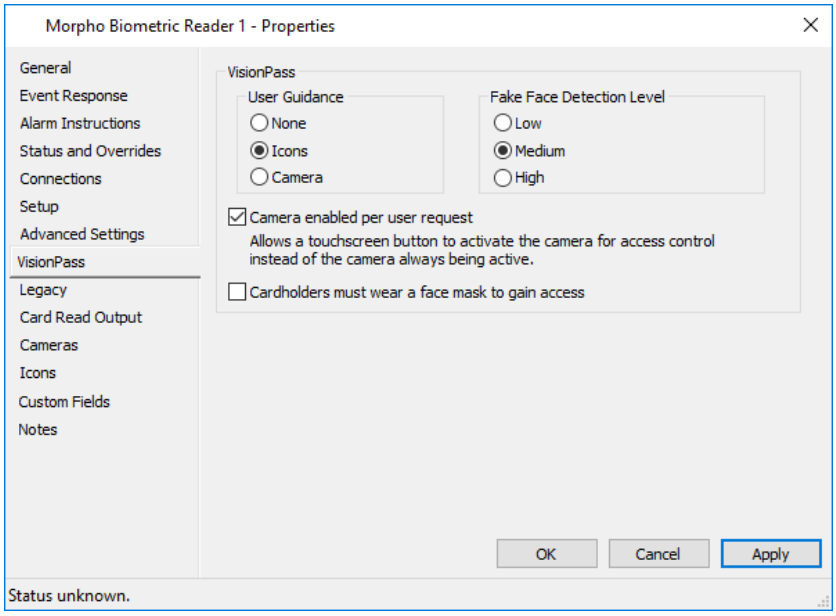
Field/Checkbox	Description
Display Date and Time	Enabling this checkbox means that Morpho Reader models with screens, and in Native Mode (MA5G), will display the date and time.
Display Card-holder Name after access is granted	Enabling this checkbox means the reader will display the cardholders name ("Surname,firstname" and limited to 38-characters) in the welcome message when a biometric is recognised. If cardholders have a **Short Name** (limited to 16 characters), that will be displayed when they enter. However, if they do not have a **Short Name**, their "Surname,firstname" will display. **Note:** This is not supported with OSDP.

16. Do you want access and status messages to be displayed on this reader's screen?

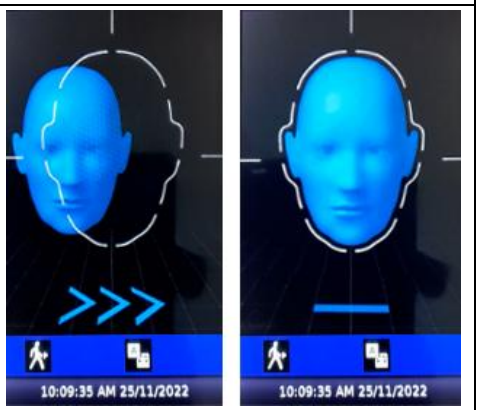
Copyright © Gallagher Group Limited

If…	then if the Server Properties are configured to…
no,	NOT show reader messages, leave the **Use site default settings** checkbox checked; OR if the Server Properties ARE configured to display reader messages, deselect the **Use site default settings** checkbox and ensure the **Show reader display messages** checkbox is unchecked.
yes,	show reader messages, leave the **Use site default settings** checkbox checked; OR if the Server Properties are configured to NOT display reader messages, deselect the **Use site default settings** checkbox and select the S**how reader display messages** checkbox.

17. Click the **VisionPass** tab.



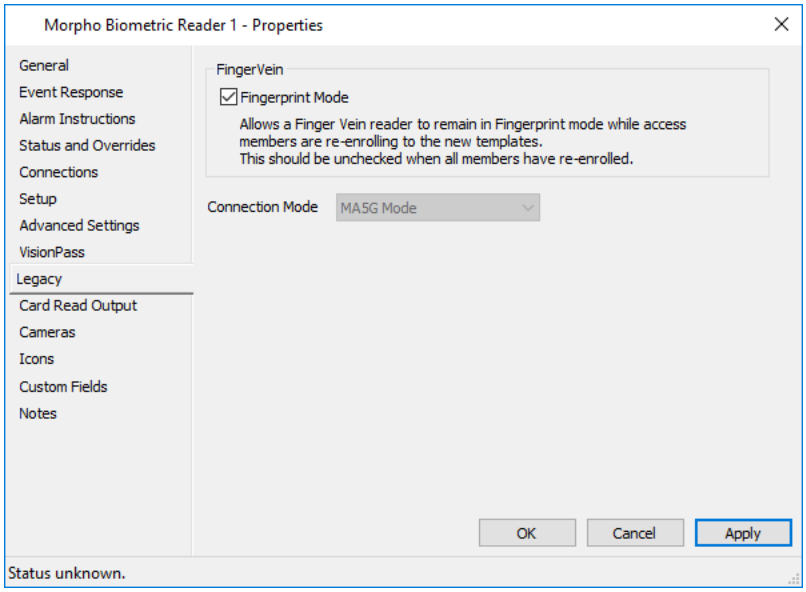
18. Configure the **VisionPass** settings on this screen if this reader is a VisionPass reader.
Note: The fields will be populated with any previously configured values for existing biometric readers.

Field/Checkbox	Description
User Guidance	If you want to configure user guidance for this reader, click either **Icons** or the **Camera** radio button as appropriate. If **Icons** is selected, an icon will appear on the reader and if need be, arrows to show you where to move to be captured. If **Camera** is selected, the camera will briefly show footage of you on the reader. If there is no person there it will stay up for a little longer before timing out and denying access. 

Copyright © Gallagher Group Limited

Field/Checkbox	Description
Fake Face Detection Level	Click the appropriate radio button for a default acceptable fake face detection level. **Low:** detects and manages basic fake face attacks such as pictures presented on paper or smartphone. **Medium:** enhances security controls while providing good user experience. **High:** certified by iBeta as PAD Level 2 with an IAPMR at 0%. **Notes:** • Default = Medium. Recommended option is either Medium or Low if **Cardholders must wear a face mask to gain access** is enabled. • For **High FFD** setting these guidelines must be met: - Enrolment of user on VisionPass - Biometric only (no template on card) - Standard lighting, not recommended outdoor (100 < lux < 5000) - No face mask - No eyewear
Camera enabled per user request	Checking (enabling) this setting will make a "man walking"  icon appear at the bottom left corner of the VisionPass reader. This icon must be pressed for the reader to check your face. This setting is unchecked by default. If you leave it unchecked, then it operates by motion detection. Any movement at the camera will trigger it to try to capture a face.
Cardholders must wear a face mask to gain access	When checked (enabled) it will be mandatory for cardholders to wear a face mask otherwise access will be denied. (Default = Unchecked) **Notes:** • If this checkbox is ticked cardholders are likely to get higher chances of access denied compared to a face mask not being enforced, especially when the **Fake Face Detection Level** (FFDL) is set to high. Therefore, we recommend the FFDL is set to either Medium or Low when wearing face masks is enforced. • This does not apply to VisionPass SP readers.

19. Click the **Legacy** tab.



Copyright © Gallagher Group Limited

20. When checked, the **Fingerprint Mode** checkbox allows a Fingervein or MorphoWave reader to operate on Fingerprints only (for use during biometric enrolment transition from Fingerprint to Fingerprint +Vein). This setting is checked by default. Uncheck it if you do not require this functionality.
21. The **Connection Mode** field specifies the mode of communication that was originally specified for Legacy Readers. This field shows the current configuration but is 'read-only' as Legacy Readers are no longer supported.
22. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Morpho Biometric Reader.
23. Click the **Icons** tab if you want to change the Icon Set for this Morpho Biometric Reader.
24. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Morpho Biometric Reader.
25. Click the **Notes** tab if you want to add a note(s) about this Morpho Biometric Reader.
26. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

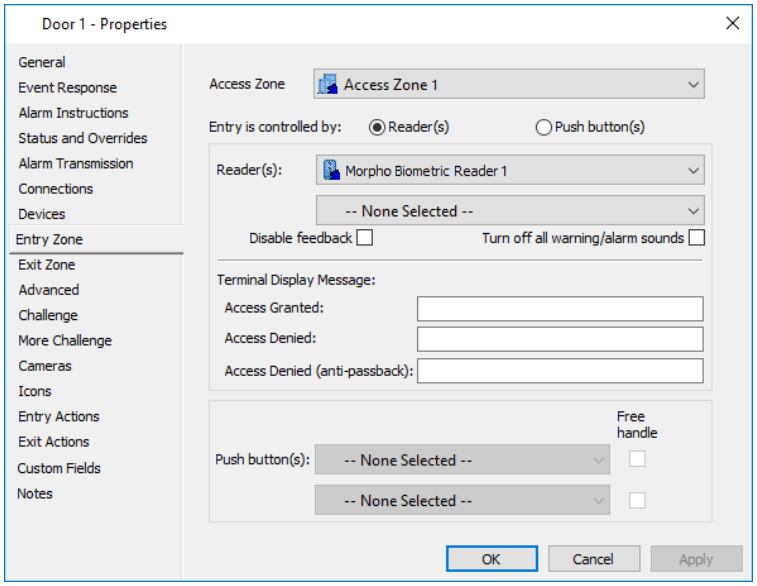
Assigning the Morpho Biometric Reader

Once the configuration work is complete, you need to assign the Morpho Biometric Reader to a Gallagher Controller and other appropriate devices, (i.e. Door, HBUS Wiegand Door Module, Terminal, Elevator Car and/or HLI Elevator Car).

27. Assign this reader to a Controller. See ***14.2 Configuring the Controller RS-485 Bus for OSDP*** for further detail.
28. From either the **Hardware** or **Door** List Window, highlight the device you want to assign this reader to.
29. **Right click** and select **Properties**.
30. What type of device are you assigning the biometric reader to?

If…	**then click the…**
HBUS Wiegand Door Module,	**Readers** tab.
Door,	**Entry Zone** tab.
Terminal, Elevator Car or HLI Elevator Car,	**Connections** tab.

The window displayed will vary depending on the device selected. The example shown is for a Door.



31. Select the appropriate Morpho Biometric Reader(s) from the relevant Reader drop-down list, as follows:

Copyright © Gallagher Group Limited

Gallagher…	can host a maximum of…
Controller 6000, Controller 7000	32 x Morpho readers for OSDP (16 per RS-485) Controller 7000; 16 x Morpho readers for OSDP (8 per RS-485) Controller 6000; 4 x Morpho readers for 8R; 2 x Morpho readers for 4R.
Controller 7000 Single Door (RS-485)	8 x Morpho readers.
Controller 7000 Single Door (Wiegand)	1 x Morpho reader.
HBUS Wiegand Door Module	2 x Morpho readers.

32. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

8.4 Result

A Morpho Biometric Reader has been configured and is ready for use. **Notes:**

- A Morpho Biometric Reader can be synchronised using macros.
- You cannot delete a Morpho Biometric Reader if it appears on a Site Plan.
- It is recommended that encrypted communications be disabled on a Morpho Biometric Reader before it is deleted.

9 Enrolling Users

Capturing Biometric credentials for Cardholders is performed using the Gallagher Command Centre Client.

9.1 Configuring a Cardholder Biometrics Tile

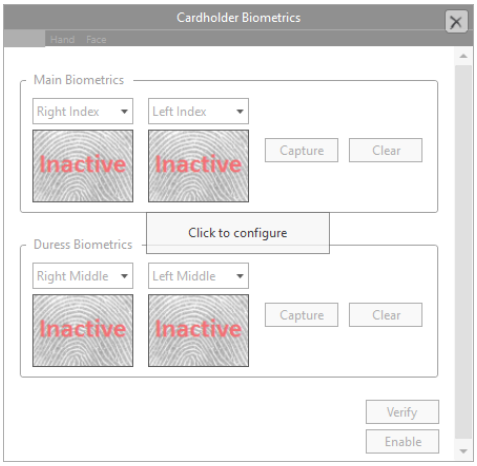
This tile provides the user with the ability to capture and verify biometrics, (i.e. fingerprint, hand and face), and is only used on a Cardholder Viewer.

To…	you need…
view a Cardholder's biometrics,	one of the following privileges in the division of the cardholder: • "View Cardholders" • "Edit Cardholders" • "View Cardholder Notes" • "Edit Cardholder Notes" • "Edit Cardholder Notification" • "Print/Preview & Encode Card" • "Delete Cardholders" **Note:** You only need the privilege to view the Cardholder in order to "Verify" their biometrics.
capture or **remove** a Cardholder's biometrics,	the "Edit Cardholders" privilege in the Division of the Cardholder. **Note:** The above is required to enrol on a MSO device, however when enrolling on Morpho Wave or VisionPass, the "View Site" privilege is also required.

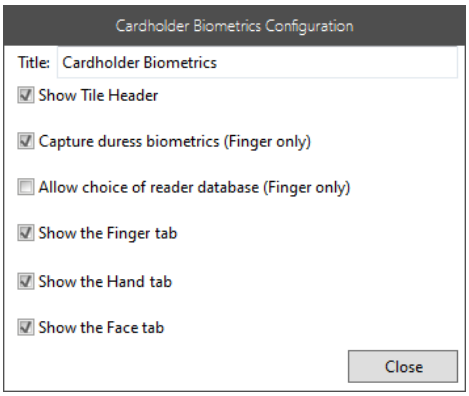
How to configure

1. Double-click on **Cardholder Biometrics** on the 'Tile Toolbox'. The Cardholder Biometrics Tile appears on the Configuration Panel section of the screen in preview mode.

Copyright © Gallagher Group Limited



2. Move the mouse over the Cardholder Biometrics Tile you have added, and click on the **Click to configure** button that appears. The Cardholder Biometrics Configuration pop-up displays.



3. Enter an appropriate **Title** for this Tile.
4. Uncheck the **Show Tile Header** checkbox if you want the tile header to be removed in operational mode.
   Note: While this feature maximises the available screen real estate, be aware that Tile maximise/ minimise can only be achieved using hot keys <**Ctrl**+**M**>.
5. The **Capture duress biometrics** checkbox applies to non-MorphoWave (Finger) biometric only, and controls whether to display the Duress Biometrics capture options or not, and is checked by default. Uncheck it if not required.
6. The **Allow choice of reader database** option applies to non-MorphoWave (Finger) biometric only, and allows an operator to change the Reader Database ID.
   What model of standard Morpho Biometric reader do you have?

If…	**then…**
MA1xx, **MA Sigma**, **MA J**, **MA VP** or **MA5xx** without an IDENTPLUS license	leave the **Allow choice of reader database** checkbox unchecked as these readers only have one database.
MA5xx with an IDENTPLUS license	check the **Allow choice of reader database** checkbox as these are multi-database readers.

7. Check the **Show the Finger tab** checkbox if you intend to enroll cardholder's fingerprints using an MSO enrolment device.
8. Check the **Show the Hand tab** checkbox if you intend to enroll cardholder's fingerprints using a MorphoWave Reader.
9. Check the **Show the Face tab** checkbox if you intend using a VisionPass reader.
10. Click the **Close** button.
    The preview mode of the Cardholder Biometrics Tile now displays the title given.

Copyright © Gallagher Group Limited

9.2 Capturing Biometrics (Fingerprint or Finger Vein)

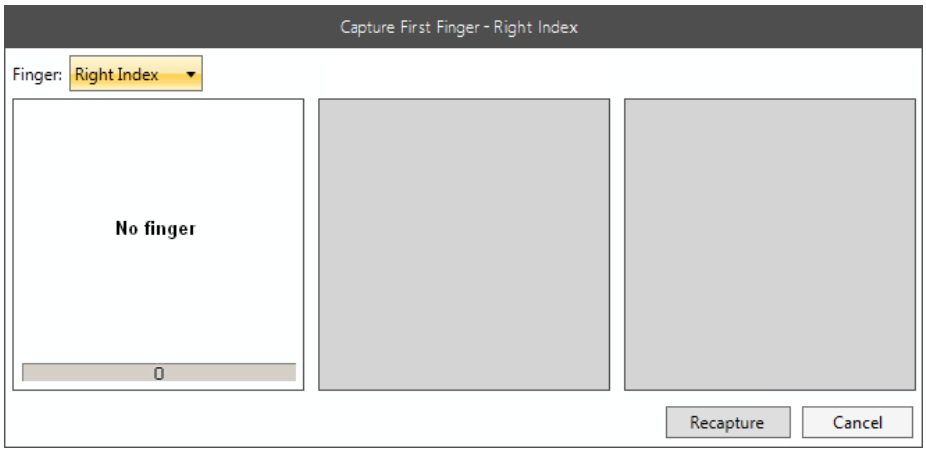
Use the following procedure to enrol a Cardholder for a Morpho Fingerprint or Finger Vein:

1. Click the **Capture** button for either the Main or Duress Biometrics group.
   Note: For fingerprint or finger vein capture to work the following needs to be installed:

For the…	you need…
Server Workstation	+ Microsoft Visual vc10redist_x86 + Microsoft Visual vc12redist_x86 + Microsoft Visual vc14redist_x86 + Microsoft Visual vc14redist_x64
Client Workstation	+ Microsoft Visual vc10redist_x86 + Microsoft Visual vc12redist_x86 + Microsoft Visual vc14redist_x86 + Microsoft Visual vc14redist_x64

   If they are missing, the following error message will display when you click the **Capture** button:
   "Failed to capture fingerprints.
   Reason: Device DLL or one of its dependencies is missing or not registered."

   These files are located in the `'Utilities\Morpho\Microsoft Redistributables'` folder of the Command Centre installation files. See ***4.1 Installing Microsoft Redistributables***.
   The Capture Finger screen displays with instructions on what to do next within the appropriate finger capture area.



2. Select the finger you want to capture biometric templates for from the **Finger** drop-down list.
   As a complete capturing process, both the Main and Duress Biometric groups require fingerprints or finger veins to be captured for two fingers, (e.g. the 'Left Index Finger' and the 'Left Middle Finger'), and three fingerprints/finger veins must be captured per finger.

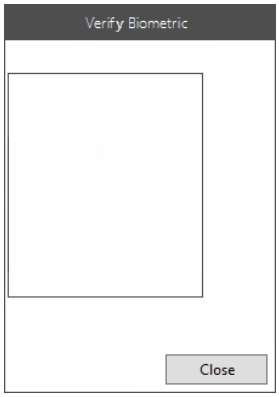
   Note: Biometric captures are stored on the reader and take up quite a bit of space, therefore if duress is not an issue for your site it is suggested that you do not bother capturing 'Duress Biometrics'. Also, duress will only work if a cardholder has been given access to that Morpho Reader.

3. Place the appropriate finger on the enrolment device.
   As each biometric capture occurs the quality of that individual capture is displayed at the bottom of the biometric display area, which remains visible after they have moved on to the next capture.
   Notes:
   - The overall quality (score) of the biometrics that are captured needs to be more than 165 to be validated by the system.
   - At any time the user can click the **Recapture** button to re-start the process for capturing the three samples for the current finger.
4. Repeat Step 2 twice so you have three captures of the same finger.
5. Repeat Steps 2 - 3 for the second finger of that Biometric group.
   On capturing two fingers successfully:

Copyright © Gallagher Group Limited

- an image displays under the appropriate Biometric group on the Cardholder Biometrics Tile to indicate that something has been captured,
- the **Clear** button (used for deleting the captured biometrics) for the group is enabled, and
- the **Verify** button is enabled.
  This button allows you to verify that the Cardholder's fingerprint/finger vein templates that have been captured can actually be used successfully for biometric authentication, (i.e. there is a match between the captured templates and the person's fingerprints/finger veins).

6. Click the **Verify** button.
   The Verify Biometric pop-up displays.

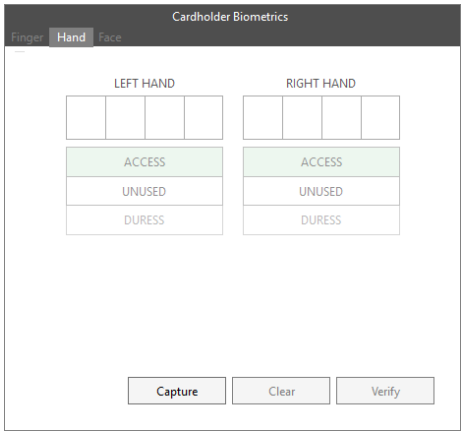


7. Place the appropriate finger on the enrolment device.
   The system verifies whether the captured biometrics match the existing templates already captured, and the appropriate message box displays indicating if there is a match or not. Once a match has been made the finger image is removed and result is displayed at the bottom.
8. Click the **Close** button.

9.3 Capturing Biometrics (Hand)

The following procedure describes how to enrol a Cardholder's fingerprints using a MorphoWave Reader:
Note: Previously used DESFire cards should not be encoded for different cardholders.

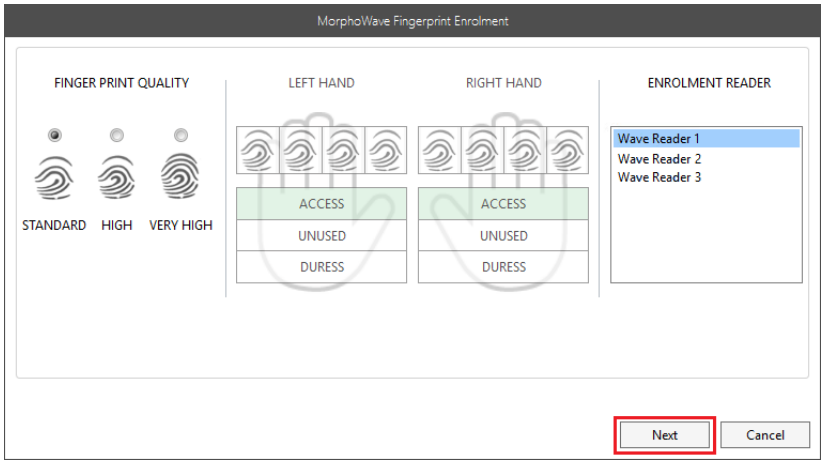
1. Click the **Hand** tab.



   Note: All eight finger locations displaying as 'blank' indicates that the Cardholder is not enrolled for MorphoWave.

2. Click the **Capture** button. The MorphoWave Fingerprint Enrolment screen displays.

Copyright © Gallagher Group Limited



Note: Hand overlays display briefly to demonstrate the order of the fingers.

3. If the Morpho Biometric Card Type (in the Configuration Client) has been configured to allow changes at the time of enrolment, you can change the following default values if necessary:
   - **Fingerprint Quality** by selecting Standard, High or Very High (Default and recommended option = Standard), and
   - 'Access and Duress hands' by selecting Access, Unused or Duress for each hand.
4. If there is more than one **Enrolment Reader** listed, ensure the correct one is selected.
5. Change the status of each fingerprint as required:

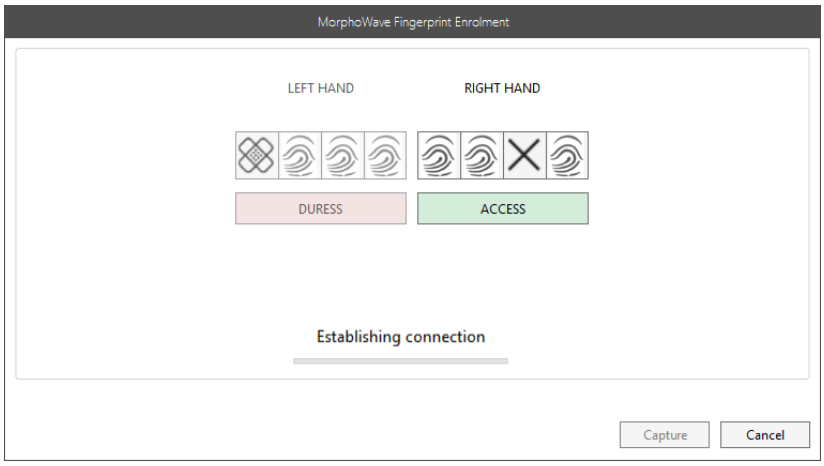
 Active

 Bandaged

 Missing

Note: At least one fingerprint must be active on each hand.

6. Click the **Next** button.
   The wizard displays the enrolment screen for the hand selected as the 'set access' hand. **Notes:**
   - When both hands are selected as "ACCESS" hands, the right-hand enrolment is displayed first.
   - Only "ACCESS" biometrics will be encoded to the card, (e.g. if one hand is selected as "DURESS", then this hand's fingerprints will not be written to the card).



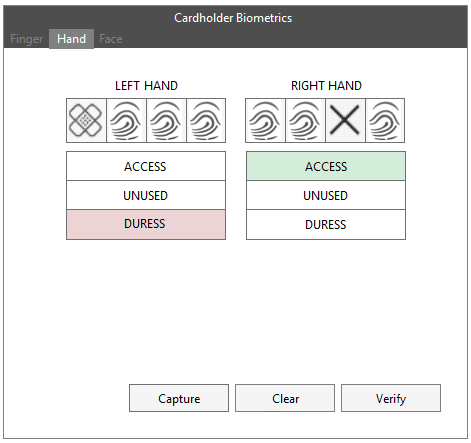
A green light on the MorphoWave Reader indicates connection has been established.

7. Insert the hand to enrol between the cover and optical sensor of the reader, ensuring it is flat, palm down, and fingers are spread slightly apart.

Copyright © Gallagher Group Limited



8. Slide the hand in the appropriate direction for the hand being enrolled, (i.e. from right to left for the right-hand, and from left to right for the left-hand, with the Index finger first).
   Once the hand has enrolled successfully, a message displays indicating that the device is ready to enrol the other hand. **Notes:**
   - After 5 unsuccessful attempts the system times out.
   - If enrolment is unsuccessful, a message indicating the reason will display. *For example:*
     If the hand slides from the wrong direction the message *"Bad hand direction"* displays.
     If the hand is not waving properly between cover and optical sensor the message *"Wave hand in parallel"* displays.
9. Repeat Steps 7 - 8 for the other hand.
   Once that hand has enrolled successfully, another message displays indicating the hand has been enrolled, and the **Accept** button becomes enabled.
10. Click the **Accept** button.
    The MorphoWave Fingerprint Enrolment screen closes, and the **Hand** tab of the Cardholder Biometrics Tile now shows enrolled fingerprints.

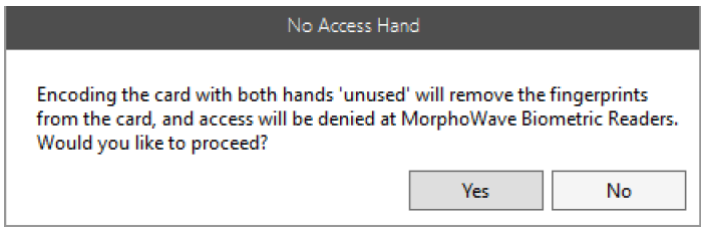


Notes:

- The MorphoWave DESFire object will not encode "UNUSED" and "DURESS" fingerprints to a card. Only "ACCESS" fingerprints will encode to cardholder's card.
- Once fingerprints are enrolled and saved (to either database and card, or database only), any changes to the fingerprints status will result in the following message displaying on the Cardholder Biometrics Tile: *"If these biometrics are encoded to a card, the card will need re-encoding."*
- If a cardholder has had biometrics enrolled previously and the fingerprint status for both hands has changed to "UNUSED", the following message will display on the Cardholder Biometrics Tile: *"At least one hand must be set to Access to use the reader. If these biometrics are encoded to a card, the card will need re-encoding."*

Copyright © Gallagher Group Limited

When the operator starts encoding the card for the cardholder (with "Card Number + Biometrics") the following warning message will display, giving them the option to either proceed with encoding or not.



IMPORTANT: Even if the card is encoded, the cardholder won't be able to access any MorphoWave Biometric Readers. However, if the card has other objects, (e.g. MIFARE DESFire object), it can still be read by Gallagher readers.

11. Click the **Save** button to save the fingerprints to the database, or click the **Revert to Saved** button to undo.
12. Click the **Verify** button.
    Note: A dialog will display if there is more than one enrolment reader available. If so, select the correct reader from the list and click the **Next** button.
    A message displays on the tile indicating which hand to verify.



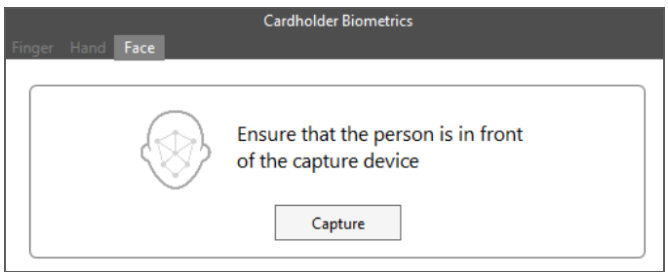
13. Wave the appropriate hand over the enrolment reader to verify the saved fingerprints.
    A message displays indicating the hand was successfully verified, followed by a message indicating it is ready to verify the other hand.
14. Wave the other hand over the enrolment reader.
    A message displays indicating that hand was also successfully verified.
15. Click the **Close** button.

9.4 Capturing Biometrics (Face)

If your site uses both VisionPass and VisionPass SP access readers, you must use VisionPass for enrolment. However, if the site exclusively uses VisionPass SP readers, then a VisionPass SP enrolment reader will suffice.

The following procedure describes how to enrol a Cardholder's face using a VisionPass Reader:

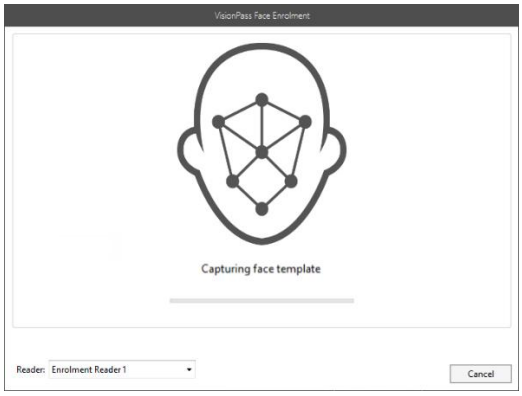
1. Click the **Face** tab.



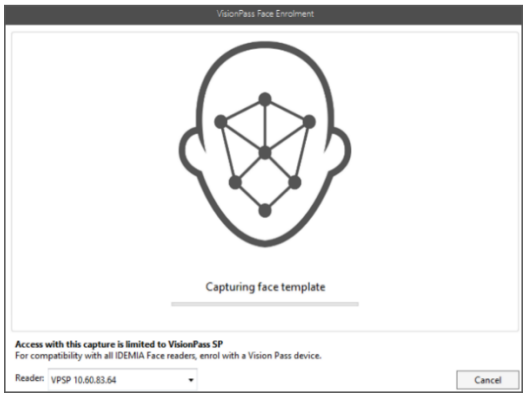
2. Click the **Capture** button. The VisionPass Face Enrolment screen displays.

Copyright © Gallagher Group Limited

*Enrolment with **VisionPass** device:*



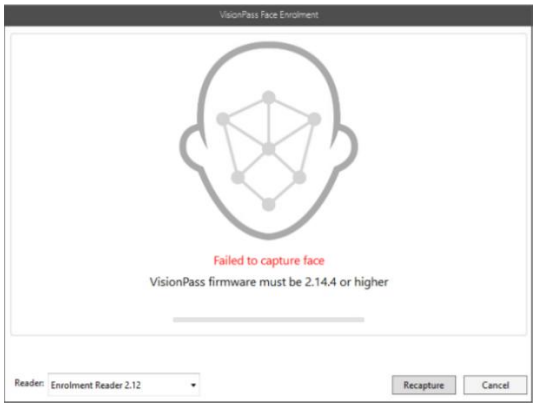
*Enrolment with **VisionPass SP** device:*



3. If there is more than one **Reader** listed, ensure the correct one is selected from the drop-down list.
4. Once enrolment process starts, Command Centre will establish connection with the VisionPass Enrolment Reader and capture a face template. **Notes:**
   - If there is no enrolment reader set up, *"Connection failed"* and *"No biometric capture devices were found."* messages display.
   - We recommend cardholders stand in front of the enrolment device with their face clearly visible, and remove all "non-always on" accessories, (e.g. remove glasses, face masks).

   The *"face captured successfully"* message displays.

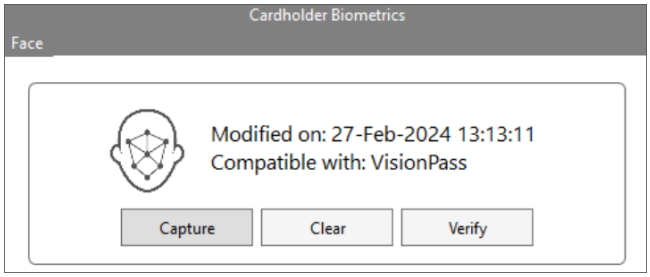
   When the capture process is completed the cardholder picture displays briefly on the screen, so you can ensure the cardholder is the correct person.



   Note: The enrolment reader requires firmware version to be 2.14.4 or higher.
5. When the enrolment process is completed click the **Accept** button to accept the result.
   Note: If the face template isn't satisfactory, the **Recapture** button can be clicked to restart the face capture process.

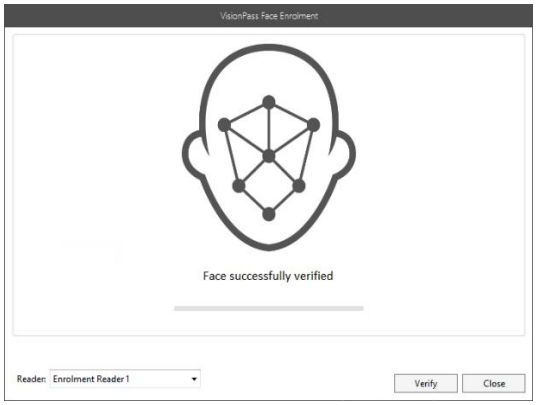
   Once the face template has been accepted, the dummy face displays on the Cardholder Biometrics Tile as solid with the modified time.

Copyright © Gallagher Group Limited



The face template can be modified by clicking the **Capture** button again, or it can be removed by clicking the **Clear** button.
Once the **Clear** button is clicked the *"Ensure that the person is in front of the capture device"* message will display again.

6. Click the **Save** button to save the facial template to the database, or click the **Revert to Saved** button to undo.
7. Click the **Verify** button.
   If there is only one enrolment reader available, the verify process will start immediately, and if the facial template is correct the face will be successfully verified. To verify again, click the **Verify** button.

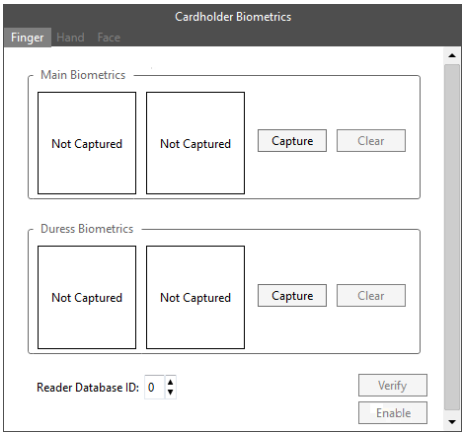


Note: If there is more than one enrolment reader available, a dialog will display. Select the correct reader from the list and click the **OK** button, and then the **Verify** button.

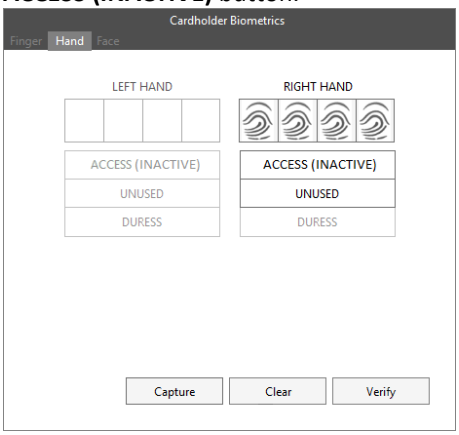
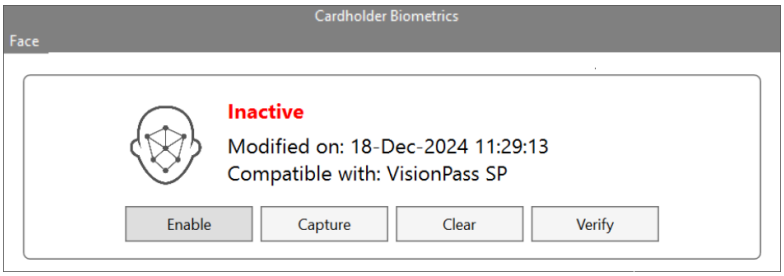
8. Click the **Close** button.

9.5 Re-enabling Inactive Biometrics

The following table describes how to re-enable inactive biometrics from any of the tabs on the Cardholder Biometrics tile:

From the…	click the…
Finger tab,	**Enable** button. 

Copyright © Gallagher Group Limited

From the…	click the…
Hand tab,	**ACCESS (INACTIVE)** button. 
Face tab,	**Enable** button. 

10 Communications Encryption

Native mode allows sites to implement more secure TCP/IP communications for MA Sigma readers if required. Sites can use either of the two methods for securing MA Sigma readers:

- Gallagher Command Centre vEL7.80 (via the network)
  (see ***10.1 Encryption using Command Centre*** next), or
- Biometric Encryption Utility (a non-network solution)
  (see ***10.2 Encryption using the Biometric Encryption Utility***).

Each encrypted Sigma reader will be issued with its own unique certificate, and a unique set of public and private keys.

Notes:

- Readers set to Native Mode (MA5G) will use TLS1.2 encryption. Encryption is RSA2048 with SHA256 hash on certificates.
- Reader encryption is recommended to avoid possible interception and tampering.
- Encrypted communications, which is OFF (disabled) by default, MUST be disabled on Morpho Readers before being removed and/or deleted from Command Centre. The reader will not allow communications outside of Command Centre if the encrypted communications are not disabled. Stateful alarms are generated when a Morpho Readers encrypted communications are disabled.

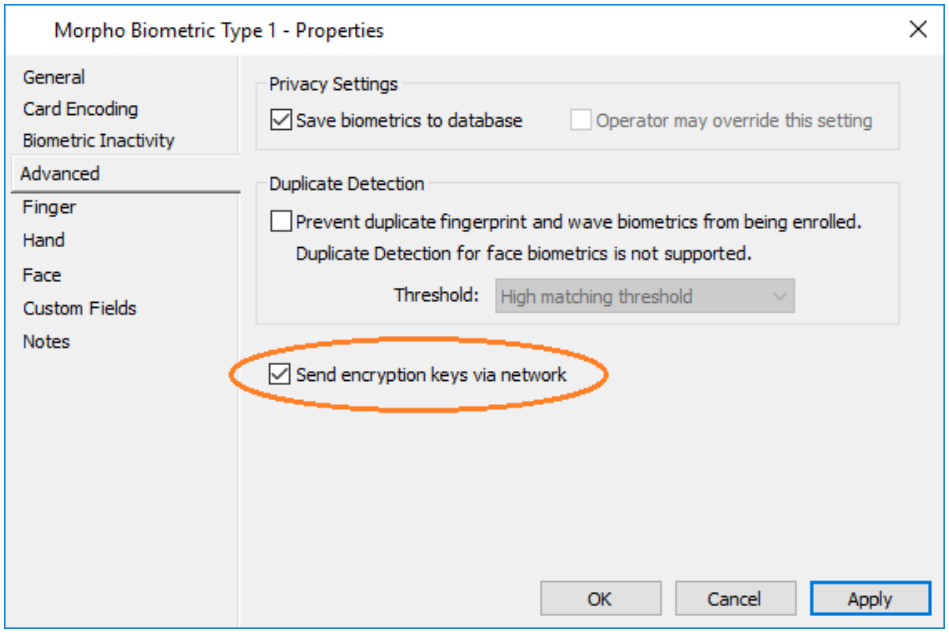
10.1 Encryption using Command Centre

This procedure describes how to send the encryption keys and certificates to the biometric readers via the network.

Copyright © Gallagher Group Limited

Procedure

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Card Types**. The **Card Type** List Window opens.
2. **Right-click** on the Morpho Biometric Type and select **Properties**.
3. Click the **Advanced** tab.



4. Check the **Send encryption keys via network** option.
5. Click the **OK** button. The certificates and keys are processed automatically in the background.
6. Go to each reader and ensure the **Encrypt Communications** checkbox is ticked.
7. Check status and overrides to confirm the reader is in “Secure communication”.

10.2 Encryption using the Biometric Encryption Utility

The Biometric Encryption Utility provides a secure method of encrypting TCP/IP communications on Morpho readers using on a laptop or similar in a safe room/network to connect to Morpho readers and assign them the appropriate keys and certificates. We recommend to directly connect to the readers when using the Biometric Encryptions Utility.

Prerequisites

Before you begin this procedure ensure:

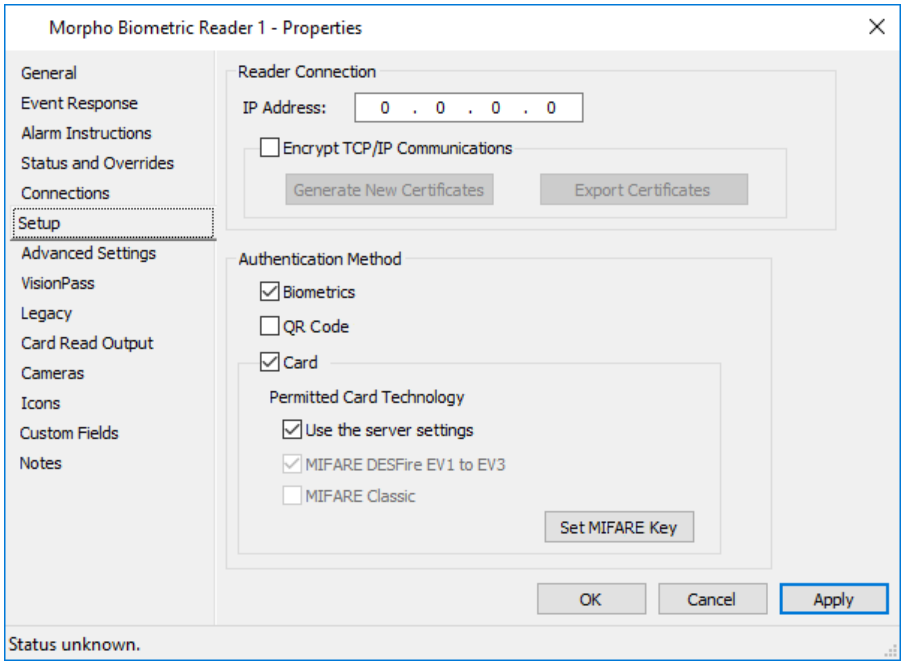
- you are using the Biometric Encryption Utility on a laptop or similar in a safe room/network.
- the **Send encryption keys via network** option is disabled (unchecked) on the **Advanced** tab of the Biometric Card Type.
- the Microsoft Redistributables must be installed on the machine the utility is run on. See ***4.1 Installing Microsoft Redistributables*** for the procedure.

Procedure

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**. The **Hardware** List Window opens.
2. Highlight the Morpho Biometric Reader you want to encrypt communications for.
3. **Right-click** and select **Properties**.

Copyright © Gallagher Group Limited

4. Click the **Setup** tab.



5. Tick the **Encrypt TCP/IP Communications** checkbox.
   Note: This option is OFF (disabled) by default.

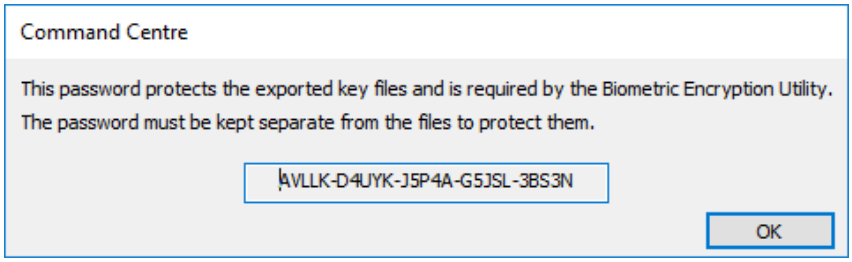
6. Click the **Generate New Certificates** button to generate and export the certificates/keys, and export the Biometric Encryption Utility.
   Notes:

   - This button will be disabled if the **Send encryption keys via network** option is checked on the biometric card type.
   - The **Export Certificates** button is also available for exporting the existing communications certificate.
   - Export Certificate requires "Manage Keys" operator privilege to work.

7. From the displayed **Browse for Folder** dialog, path your way to the directory to export the reader's certificate/key file to, and click the **OK** button. **Notes:**

   - Once the certificate has been generated and you click **Apply**, Command Centre will not communicate with the reader until the certificate and encryption has been applied to the reader.
   - The readers certificate/key files are only valid for seven days.

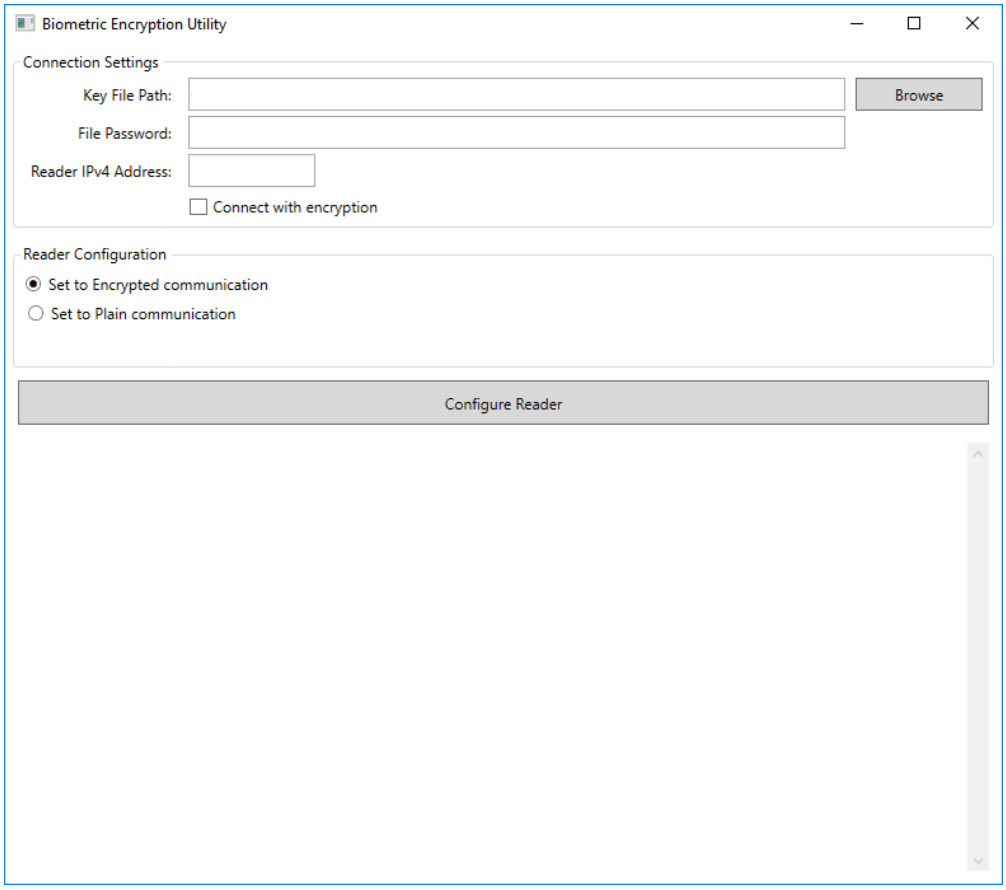
   A pop-up displays the password which is used to protect the exported key files for securing the reader.



8. Transfer the password securely from here into the Biometric Encryption Utility.
9. Take exported files and transfer them to the PC that will be connecting to the reader.
10. Ensure the reader is connected to the PC.

Copyright © Gallagher Group Limited

11. Go to the directory you specified the reader's certificate/key file to be exported to.
12. Run the **BiometricEncryptionUtility.exe** executable. The Biometric Encryption Utility opens.



13. Enter the path to the reader's communication certificate in the **Key File Path** field.
    By default, the directory name will be the same as the name of the reader that you have exported from.
14. Enter the password from the popup at Step 6 into the **File Password** field.
15. Enter the IP address of the reader to connect to in the **Reader IPv4 Address** field.
16. Click the **Set to Encrypted communication** radio button.
17. Click the **Configure Reader** button.
    The utility sends down the key and securely connects to the reader. It then deletes the certificate/key files from disk to prevent accidental re-use on another reader.

Note: The reader will update and reboot after the certificate has been downloaded.

10.3 Known Issue

Cycling the certificates for the reader while in secure mode results in Tamper Alarms and the Reader goes offline.

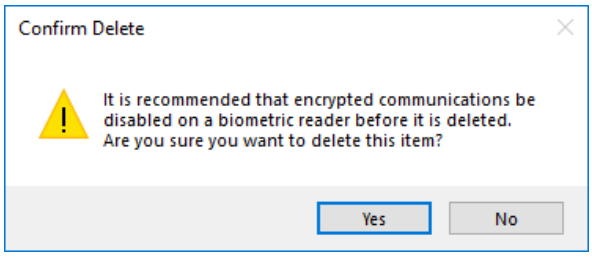
Workaround: Change the reader to "Plain Communication" and then back to "Secure Communication", and the Reader will come online and the alarms will cease.

Copyright © Gallagher Group Limited

10.4 Unencryption

Although there are two methods for unencryption, you should always try to unencrypt from the server first.

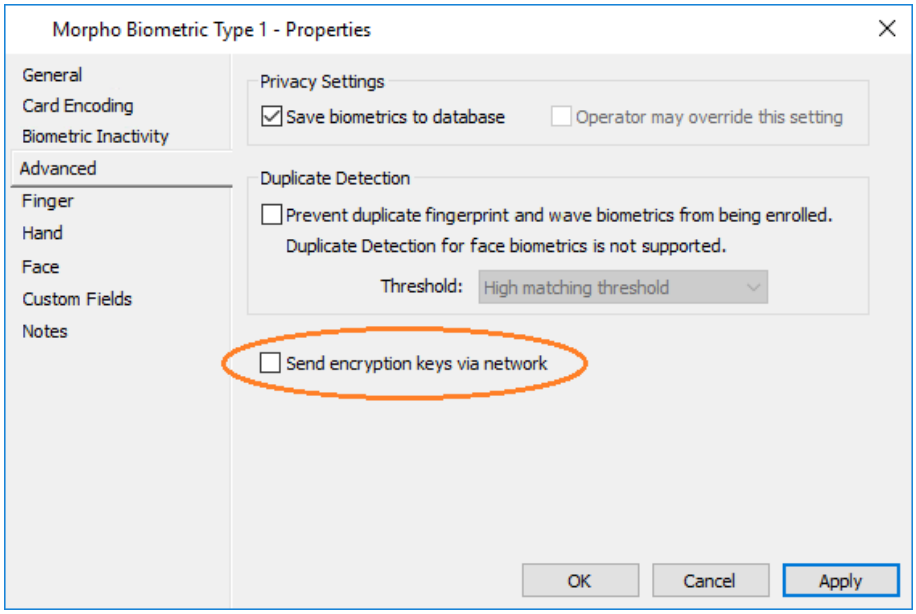
Note: If you try to delete a biometric reader without unencrypting it first, the following message will display.



10.4.1 Unencryption from the Server

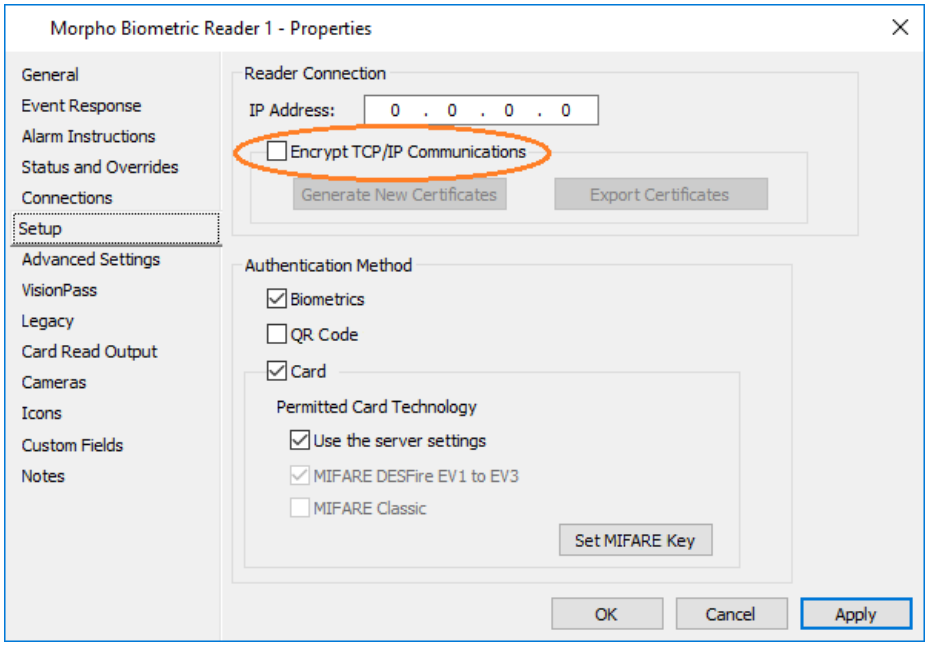
Perform the following procedure to unencrypt a reader from the Command Centre server:

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. **Right-click** on the Morpho Biometric Card Type and select **Properties**.
3. Click the **Advanced** tab and uncheck the **Send encryption keys via network** checkbox.

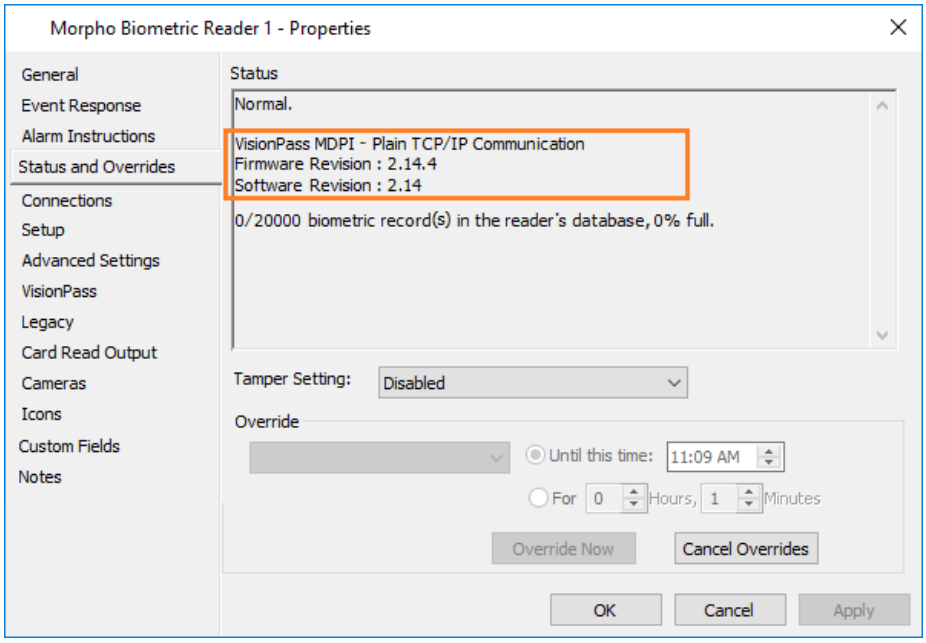


4. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
5. **Right-click** on the Morpho Biometric Reader you want to unencrypt communications for, and select **Properties**.
6. Click the **Setup** tab and uncheck the **Encrypt TCP/IP Communications** checkbox, then click **Apply**.

Copyright © Gallagher Group Limited



7. Click the **Status and Overrides** tab, and make sure the reader has changed to 'Plain Communication'.

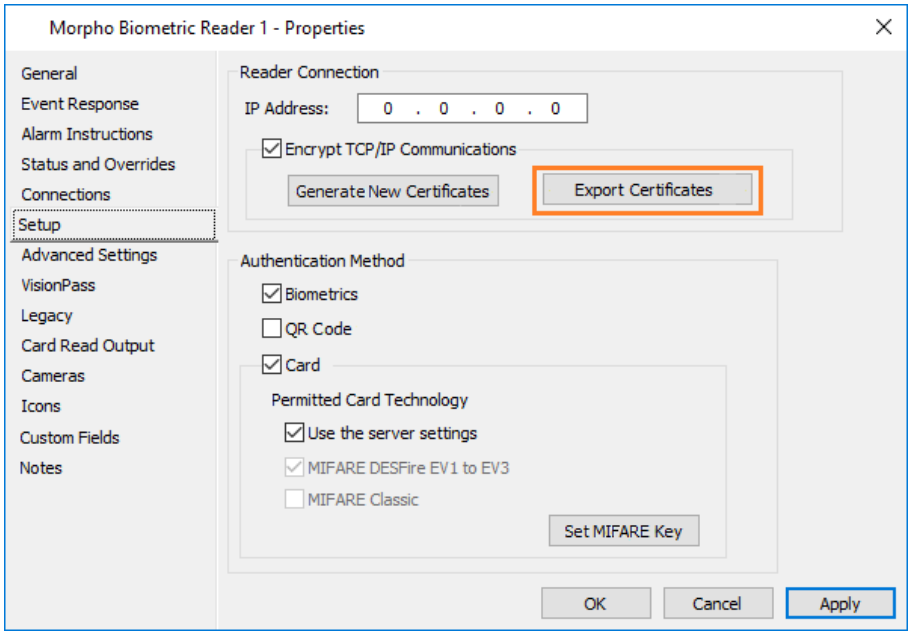


10.4.2 Unencryption using the Biometric Encryption Utility

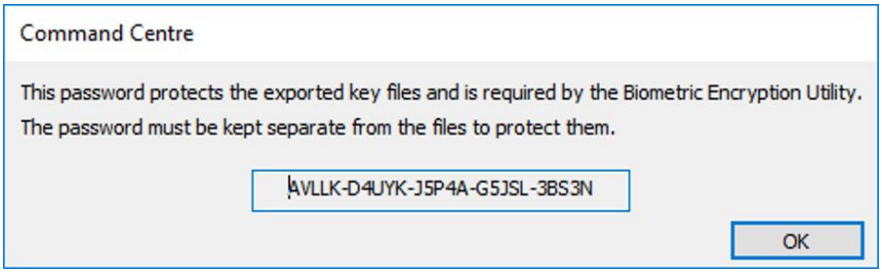
Perform the following procedure to unencrypt a reader:

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**.
   The Hardware List Window opens.
2. Highlight the Morpho Biometric Reader you want to unencrypt communications for.
3. **Right-click** and select **Properties**.
4. Click the **Setup** tab.

Copyright © Gallagher Group Limited

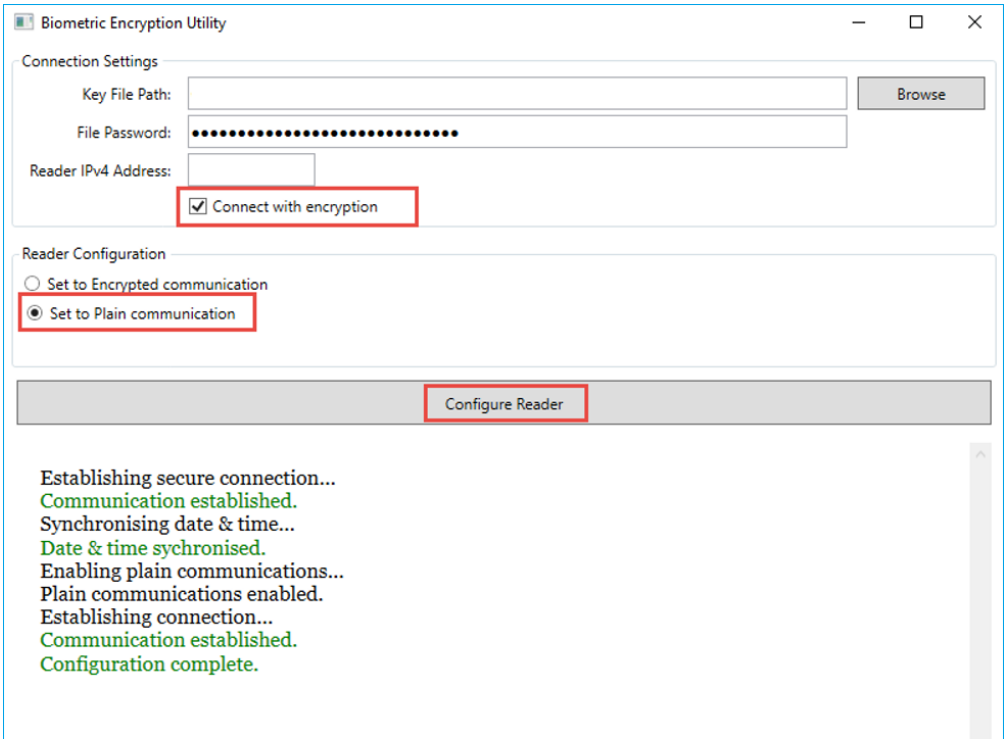


5. Click the **Export Certificates** button to export existing certificates.
   Note: Export Certificate requires "Manage Keys" operator privilege to work.
6. From the displayed **Browse for Folder** dialog, path your way to the directory to export the reader's certificate/key file to, and click the **OK** button.
   A pop-up displays the password which is used to protect the exported key files for securing the reader.



7. Run the **BiometricEncryptionUtility.exe** executable.
   The Biometric Encryption Utility opens.
8. Enter the path to the reader's communication certificate in the **Key File Path** field.
   By default, the directory name will be the same as the name of the reader that you have exported from.
9. Enter the password which is used to protect the exported key files into the **File Password** field. An example of the password is shown in the popup at Step 6.
10. Enter the IP address of the reader to connect to in the **Reader IPv4 Address** field.
11. Tick the **Connect with encryption** checkbox and click the **Set to Plain communication** radio button.
12. Click the **Configure Reader** button.

Copyright © Gallagher Group Limited



The reader will update and reboot after configuration is complete.

Copyright © Gallagher Group Limited

11 Configuring Biometric Verification

Important information when changing the Facility Code of the Morpho Biometric Type

Before changing the facility code of the Morpho Biometric Type, ensure you have taken a backup of the Gallagher Command Centre database.

In version vEL5.20.xxx (or later) of Gallagher Command Centre, there are restrictions on changing the facility code of the Morpho Biometric Type, (i.e. the facility code cannot be changed if cardholders have been assigned cards which use that facility code).

The following procedure should be used after upgrading to avoid having to change the facility code of the Morpho Biometric Type when there are cards using that facility code allocated to cardholders.

After Upgrading

Perform the following steps after upgrading Command Centre:

1. Determine the facility code to use for the Morpho Biometric Type.
   The Command Centre license will enable encoding of MIFARE cards with Gallagher data using 1 or more facility codes.
2. How many facility codes have previously been used to encode MIFARE cards?

If…	**then…**
only 1 facility code	this facility code could also be used when encoding Morpho data on the MIFARE cards.
several facility codes	one of them may be selected as the facility code to use when encoding Morpho data on the MIFARE cards. The facility code that has been used to encode the most cards is recommended, as a cardholder will require a new card to be issued if they need card access using a Morpho reader and have previously been issued a card with a different facility code.

   Note: A facility code that has never been used could also be chosen.
3. Adjust the card number allocation of existing Card Types.
   All Card Types with a facility code matching that chosen in Step 2 must have their card number allocation range changed to be within the range 31 to 8388607 inclusive. Cardholder's fingerprints/veins are allocated card numbers in the range 8388608 to 16777215. Card numbers in the range 1 - 30 are used by Morpho Readers to create events such as Biometric Reader Tampered and can no longer be assigned to cardholders.
4. If necessary, change the facility code of the Morpho Biometric Type.
   If the facility code of the Morpho Biometric Type is not the value selected in Step 2, then change the facility code of the Morpho Biometric Type to the value selected in Step 2.
5. Edit the card layout of all Card Types that need encoding with the Morpho Biometric Type.
   The Morpho MIFARE Object can be added to the card layout using the Card Layout Editor.
6. Encode cards.
   Cards will need to be re-encoded to gain access using Morpho readers in verification mode. Any cards whose card number is not in the range 31 to 8388607, or uses a different facility code to the Morpho Biometric Type cannot be encoded and must be removed from the cardholder, and a new card allocated. The old card can then be re-encoded.

Copyright © Gallagher Group Limited

12 Encoding Morpho Cards for Verification

Introduction

This section describes the overall process for encoding Morpho cards for biometric verification, (i.e. when a person identifies themselves prior to the biometric operation, e.g. by badging their card, and then the biometric operation is used to verify that the person is in fact who they say they are).

When necessary, this process refers to separate step-by-step procedures that are detailed elsewhere, (i.e. either as separate procedures in this section, or in other sections in this document). **Notes:**

- If you are reusing existing cards you will need to contact Gallagher Technical Support for a MIFARE Eraser Utility to blank the cards.
- **Card sizes for DESFire Biometric objects:**
  For Fingerprints (Sigma) only the minimum is 1k.
  For Hand (MorphoWave) only the minimum is 4k.
  For Face (VisionPass) only the minimum is 2k.
  The recommendation is 4k minimum for biometric objects on card.

Process

1. Set up a Morpho Biometric Type.
   Refer to the ***7 Creating a new Morpho Biometric Card Type*** for the procedure.
2. Set up a Card Type with:
   - the same Region and Facility codes used for the Morpho Biometric Type, and
   - the correct card number range that is valid for Morpho.
     Note: Valid range for Gallagher is 31 - 8,388,607, and Morpho it is 8,388,608 - 16,777,215.

   Refer to ***Setting up Card Types*** in the *Command Centre Configuration Client User Guide* for procedure.
3. Create a card layout for the Card Type created in Step 2, and include the appropriate Morpho object in the layout. Refer to the following procedures in the *Command Centre Configuration Client User Guide*:
   - ***Designing Card Layouts*** for full details on configuring a card layout, and
   - the appropriate procedure below for the type of Morpho object you are adding to the card layout and what you want encoded on the card:
     - ***Adding a Morpho MIFARE Classic object,***
     - ***Adding a Morpho DESFire object***,
     - ***Adding a MorphoWave DESFire object***,
     - ***Adding a Morpho FVP DESFire or Morpho VisionPass DESFire object***, and
     - ***Adding a Morpho FVP MIFARE Classic object***
4. Assign the Card Type to a cardholder. Refer to Adding a Card to a Cardholder in the *Command Centre Configuration Client User Guide* for the procedure.
5. Encode the card (via the **Print/Encode** tab of the Cardholder properties). Refer to ***Printing and/or Encoding a card from a cardholder*** in the *Command Centre Configuration Client User Guide* for the procedure. Although this procedure presumes you located the Cardholder via the **Cardholder** List Window, it can still be followed if you used the Find Tool to locate the Cardholder. **Notes:**
   - If a card fails to encode, the encode procedure should be repeated, or the card should be securely discarded.
   - If you haven't enrolled any biometrics when "Card Number + Biometrics" is selected, or any fingerprints/veins when "Card Number + Biometrics" is selected, a warning message will display indicating that these must be captured prior to encoding the card.
   - If the Morpho MIFARE object on the Card Type is set to "Card Number Only", then the card will be encoded normally. However, if it is set to "Card Number + Biometrics", then an additional **Capturing biometrics** dialog MAY display if you have not already captured fingerprints/veins normally. This dialog may allow you to save the fingerprints/veins to the database as well as encode them on the card, depending on the **Privacy Settings** set on the Morpho Biometric Type created at Step 1.
   - The Issue Level is ignored, so changing the Issue Level on a Morpho card has no impact on the Cardholder's ability to gain access through Morpho readers. It is advised that you configure a default Issue Level, (i.e. '1') by checking the Card Issue Level must match default checkbox for all encoded cards.

Copyright © Gallagher Group Limited

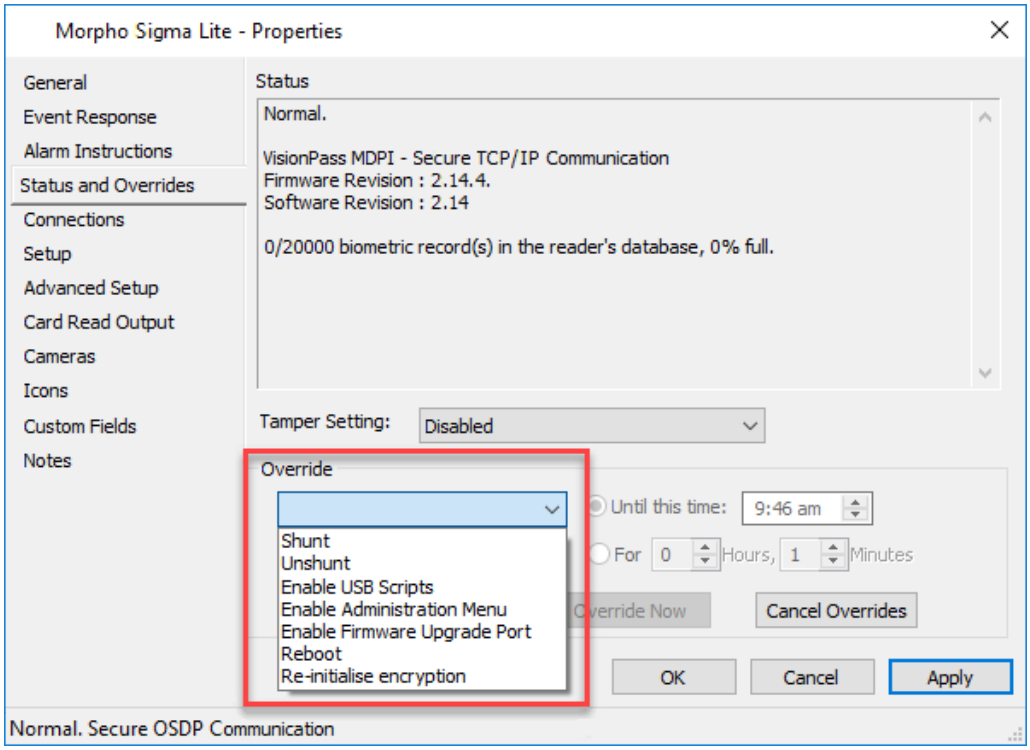
13 Performing Overrides on a Morpho Biometric Reader

Introduction

This procedure describes how to perform a timed override on a Morpho Biometric Reader.

Procedure

1. From the **Hardware** List Window, right-click the Morpho Biometric Reader you want to perform an override on and select **Properties**.
   By default, the **General** tab displays.
2. Click the **Status and Overrides** tab.



Seven options are available in the Override drop-down menu.

Option	Allows users to access the…
Shunt / Unshunt *	This stops OSDP communication to the reader, and all inputs and outputs on that reader will no longer be available by the system. It will remain that way until you "Unshunt".
Enable USB Scripts	USB Port to change configuration settings of the readers.
Enable Administration Menu	Admin menus of the readers with a display.
Enable Firmware Upgrade Port	Unauthenticated port 11010.
Reboot	Reboots the reader.
Re-initialise encryption *	If the reader is replaced, the new one will still be using the previous reader's IP address and OSDP encryption keys. To correct this, a "Re-initialise Encryption" override is required.

* Refer to ***14.3 Overrides on Morpho OSDP Readers*** for further detail on these overrides.

Copyright © Gallagher Group Limited

3. Set the duration for the override to be implemented.
   You can either:
   - select the **Until this time** radio button, and enter the time of day you want the override to occur, or
   - select the **For xx Hours, xx Minutes** radio button, and enter the hours and/or minutes (this is limited to a maximum of 23 hours and 59 minutes).

4. Click the **Override Now** button.
   From this screen you can see the status change as a result of the override.

   Note: From Command Centre v8.90 onwards, overrides can be cancelled by clicking the **Cancel Overrides** button. Also when an override is applied, the override details will be displayed in the Status section.

5. Click the **OK** button.

Result

The Morpho Biometric Reader is overridden for the time specified.

Copyright © Gallagher Group Limited

14 Morpho OSDP Configuration

Introduction

Morpho Biometric Readers can be connected to the Controller either via Wiegand protocol or Open Supervised Device Protocol (OSDP). Gallagher recommends using OSDP as it is more secure.

Morpho readers Firmware support version:

- Sigma family 4.5.0
- MorphoWave SP 1.1
- Morpho XP / XP2, VisionPass and VisionPass SP readers all support OSDP by default

14.1 Wiring Morpho Readers for OSDP

Introduction

This topic describes how to wire Morpho readers for Open Supervised Device Protocol (OSDP).

Configuration

1. On the back of the Morpho Reader, find the bundle labelled RS485 or RS422.
2. Separate three lines on in the bundle.

   Notes:

   - **Controller 6000:** Maximum of 16 OSDP Readers (8 per RS485 port)
   - **Controller 7000:** Maximum of 32 OSDP Readers (16 per RS485 port)
   - Refer to section ***2.4 RS485 cabling*** of the 3E2028 Install Note Gallagher Controller 6000 for further information.

   For Sigma Lite and Sigma Lite+ readers:

Morpho Readers that supports RS485 only	Controller RS485 Port
RS485_A Blue	A
RS485_B Blue / Red	B
RS485_GND Black / Red	-

   For VisionPass SP, VisionPass, MorphoWave, Sigma Extreme and Sigma Wide readers:

Morpho Readers that supports RS422 & RS485	Controller RS485 Port
RS485_TX_Y Green / Black	A
RS485_TX_Z Green / White	B
RS485_GND Black / Red (Black for VisionPass SP)	-

14.2 Configuring the Controller RS-485 Bus for OSDP

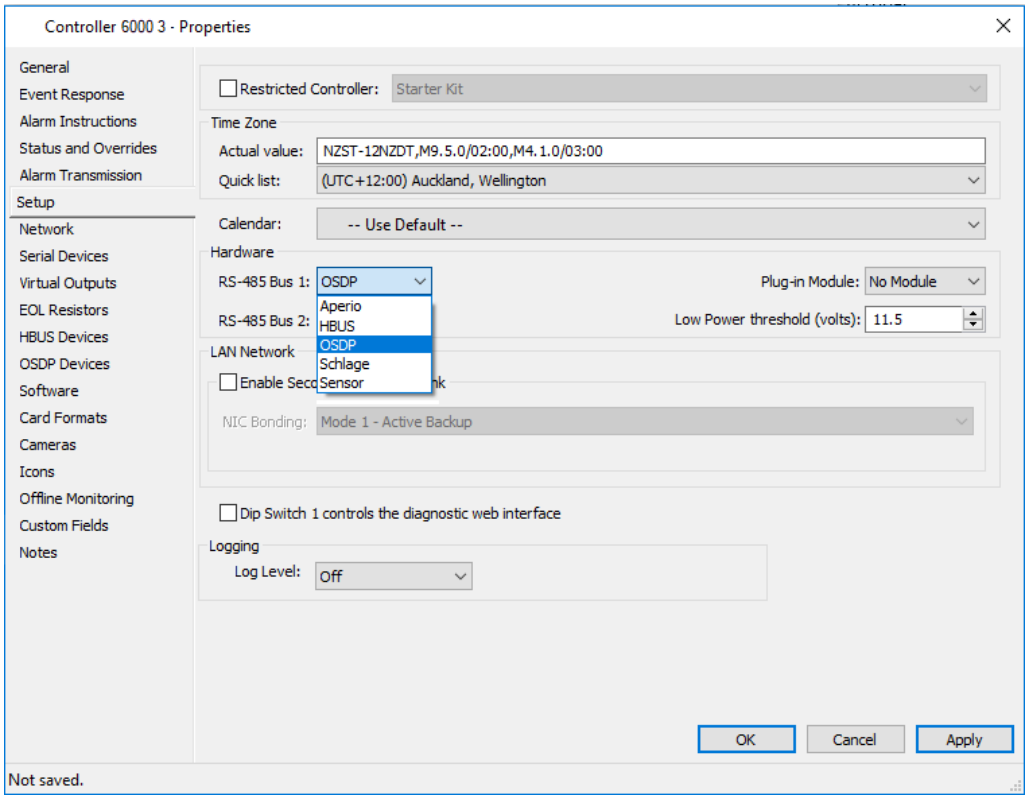
Introduction

This topic describes how to configure the Controller RS-485 Bus for Open Supervised Device Protocol (OSDP) and assign the Morpho reader to the Controller.

Configuration

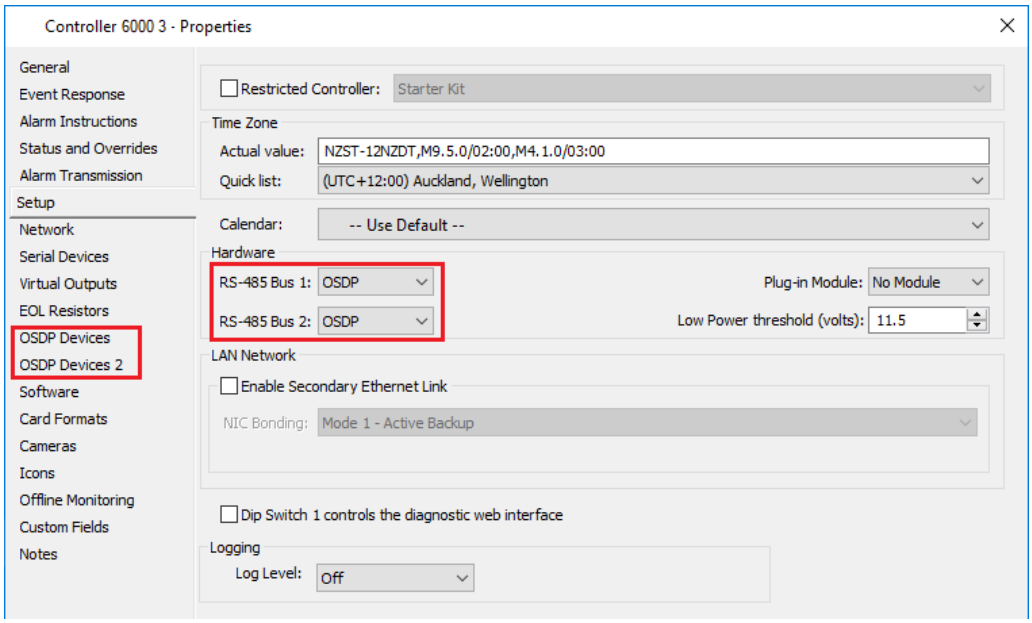
1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**. The **Hardware** List Window opens.
2. Highlight the Controller you want to configure the RS-485 Bus for OSDP.
3. **Right click** and select **Properties**.
4. Click the **Setup** tab.

Copyright © Gallagher Group Limited



5. In the Hardware section of this screen, select the 'OSDP' option form the **RS-485 Bus 1** and/or **RS-485 Bus 2** drop-down lists as appropriate.

   Depending on which RS-485 Bus option(s) you selected 'OSDP' for, an **OSDP Devices** and/or **OSDP Devices 2** tab appears, allowing you to add up to 16 OSDP Readers and/or Morpho Biometric Readers to the Bus port on this Controller.

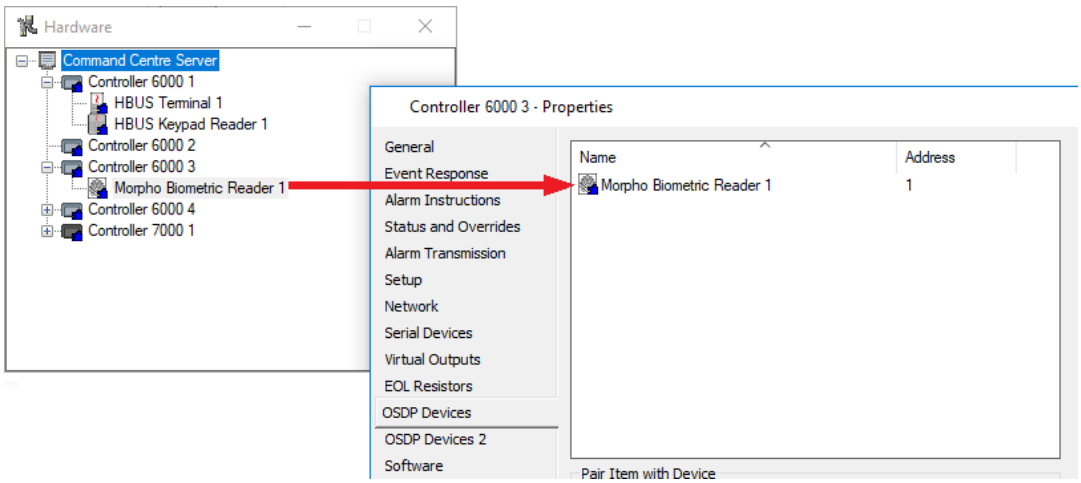


Note:

- **Controller 6000:** Supports up to 16 OSDP and/or Morpho Biometric readers per controller, split across runs (maximum 8 readers per run).
- **Controller 7000:** Supports up to 32 OSDP and/or Morpho Biometric readers per controller, split across runs (maximum 16 readers per run).
- The total number of Morpho readers allowed across the site is determined by the license file.

Copyright © Gallagher Group Limited

6. Click the **OSDP Devices** tab.
7. From the **Hardware** List Window, select the Morpho Readers attached to this Bus.
   Drag and drop each Reader into the grid on the **OSDP Devices** tab.

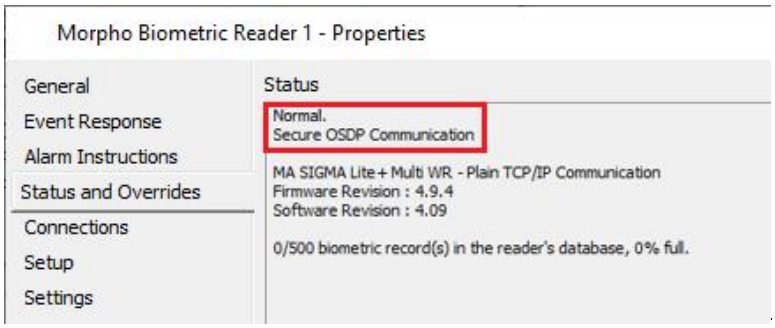


Notes:

- Each Morpho reader that is added receives a unique address (Address Range = 0 - 126). The **Configured Address** automatically increases.
- If readers don't have a unique **Configured Address** and you click **Apply**, the following error message displays:
  "Device addresses on the same bus must be unique."
- The **Change Device Address** section only works for OSDP readers, and is disabled for Morpho readers.

8. If you want to change the **OSDP Bus Baudrate** for communication between the reader and the Controller, select the appropriate **Baudrate** from the drop-down list.
   Note: The default baud rate for newly created Controllers will be "115200", but for existing Controllers it will remain as "9600". We recommend "115200" is used for better performance.
9. Click **OK** to exit and save your changes.
   Click **Cancel** to exit without saving your changes.
   Click **Apply** to save your changes and stay in this window.

The reader status should display as "Secure OSDP Communication" on the reader's **Status and Overrides** tab. By default, the communication between controller and reader is encrypted.



Copyright © Gallagher Group Limited

14.3 Overrides on Morpho OSDP Readers

Introduction

This topic describes how to perform overrides on a Morpho Reader added to an OSDP connection.

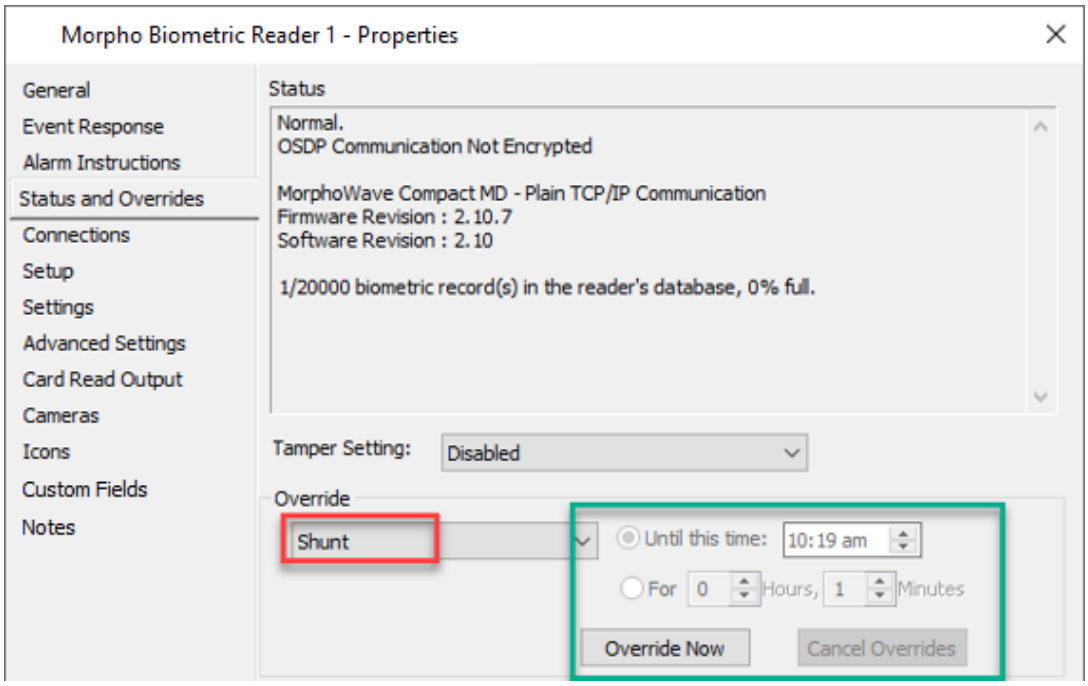
Configuration

Shunt and Unshunt overrides

Shunt overrides stop communication to the reader, and all inputs and outputs on that reader will no longer be available by the system. It will remain that way until you perform an "Unshunt" override.

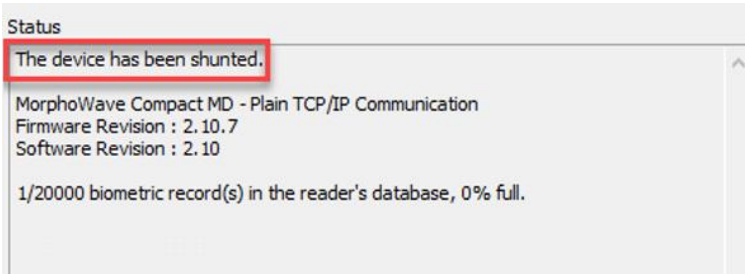
Note: Shunt and unshunt overrides only display for Morpho readers that have been added to an OSDP connection.

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
2. **Right click** on the appropriate Morpho Reader, and click **Override…** from the drop-down menu.
3. Click within the **Override** field and select **Shunt** from the drop-down list.



Note: When the "Shunt" override is selected, the Time setting and **Cancel Overrides** button is disabled.

4. Click the the **Override Now** button.
   From this screen you can see the status change as a result of the override.



5. Click the **OK** button.

Copyright © Gallagher Group Limited

Result

The reader has been shunted, and a "Device Shunted" event is generated. It will remain that way until you perform an "Unshunt" override.

While the "Shunt" override is in place, the system will not monitor the reader, and the reader will not generate alarms or cause event initiated actions.

Re-initialise Encryption overrides

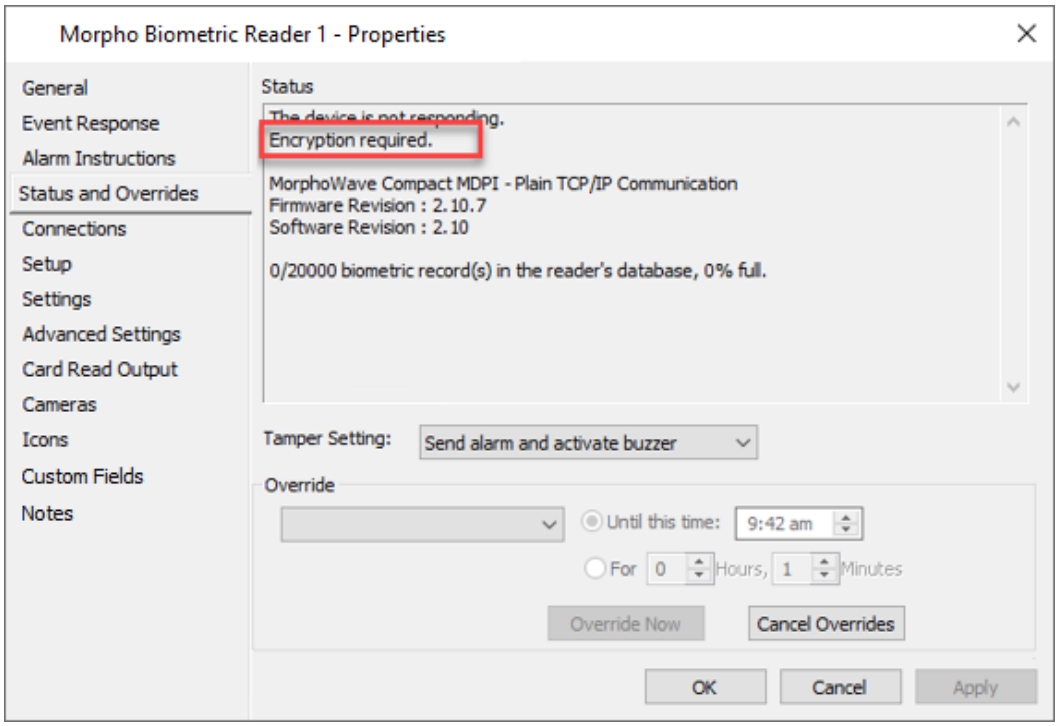
If a reader is replaced, the new one will still be using the previous reader's IP address. To correct this, a "Re-initialise Encryption" override is required.

During the OSDP assignment, if the status shows as "Encryption required" the operator can still use this override to solve this problem.

This override only works if the device is online. Performing the override when the device is offline has no effect.

The override can be performed as follows:

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**. The **Hardware** List Window opens.
2. **Right click** on the appropriate Morpho Reader, and click **Override…** from the drop-down menu. The **Status and Overrides** tab of the Morpho Reader properties displays with the reader status displaying as "Encryption required".



3. Click within the **Override** field and select **Re-initialise encryption** from the drop-down list.
   Note: When the "Encryption required" override is selected, the Time setting and **Cancel Overrides** button is disabled.
4. Click the **Override Now** button.
   From this screen you can see the status change back to "Secure OSDP Communication" as a result of the override.
5. Click the **OK** button.

Copyright © Gallagher Group Limited

14.4 Morpho OSDP Reader Display Messages

Introduction

This topic explains the various OSDP configurations for displaying access and status messages on Morpho readers with screens, and provides a list of the status that can be displayed on them.

Examples of Morpho OSDP Reader configurations

Below are the various configurations available and screenshots as examples of what will display on the Morpho reader screen for that particular configuration.

Notes:

- The example screenshot is for a VisionPass reader, however what displays is the same for MorphoWave, Sigma Lite+, Sigma Extreme and Sigma Wide readers.
- Morpho devices do not support Access Zone PIN modes. "Enter PIN" will appear using OSDP Reader Display Messages, but you are unable to enter PIN using a Morpho device (the only way to support PIN mode is by using Card + PIN).

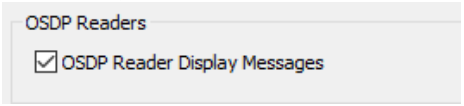
OSDP Reader Display Messages ENABLED

Server Settings ENABLED; Device Show reader messages ENABLED

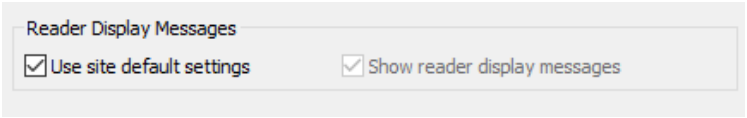
This means that the reader WILL display messages (because the "Use site default settings" is enabled, and Morpho "OSDP Reader Display Messages" is enabled).

Note: The reader setting "Show reader display messages" is enabled but cannot be changed.

Server Properties (Advanced tab)



Reader properties (Settings tab)



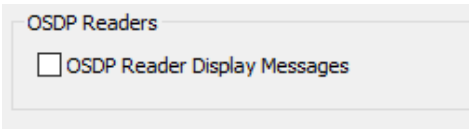




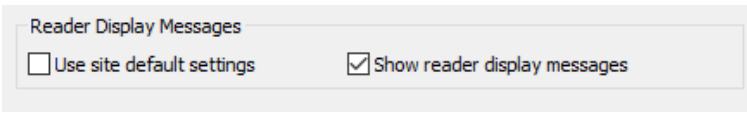
Server Settings NOT enabled; Device Show reader messages ENABLED

This means that this specific reader WILL display messages.

Server Properties (Advanced tab)



Reader properties (Settings tab)







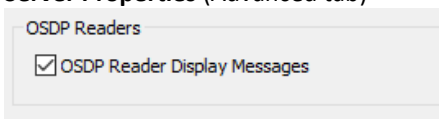
Copyright © Gallagher Group Limited

OSDP Reader Display Messages NOT enabled

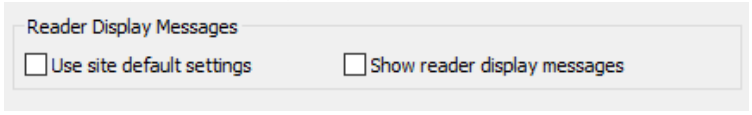
Note: Upon unchecking, a reboot is required for the textbox to go away.

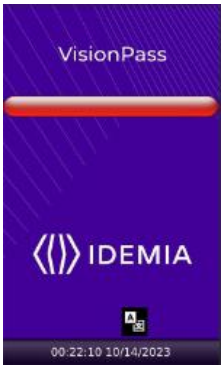
Server Settings ENABLED; Device setting NOT enabled
This means that the readers will NOT display messages (because the READER "Use site default settings" is NOT enabled).

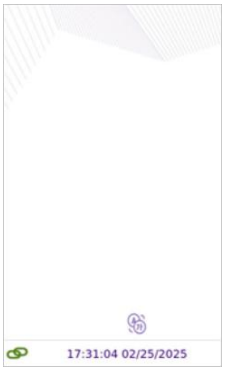
Server Properties (Advanced tab)



Reader properties (Settings tab)



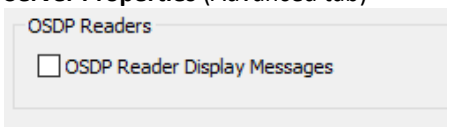




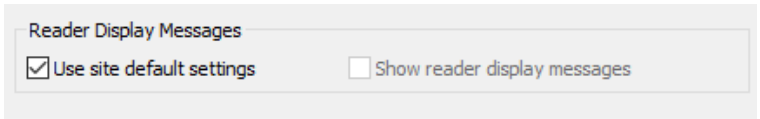
Server Settings NOT enabled; Device setting ENABLED
This means that the reader will NOT display messages (because the "Use site default settings" is enabled, and Morpho "OSDP Reader Display Messages" is NOT enabled).

Note: The reader setting "Show reader display messages" is NOT enabled and cannot be changed.

Server Properties (Advanced tab)



Reader properties (Settings tab)

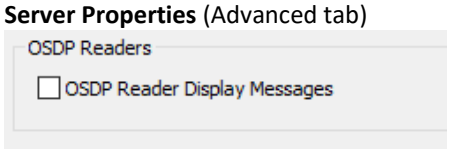




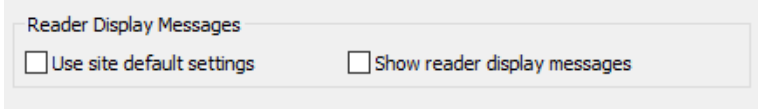


Server Settings NOT enabled; Device setting NOT enabled
This means that the reader will NOT display messages.

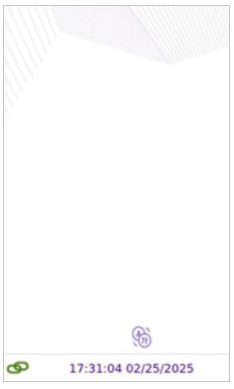
Server Properties (Advanced tab)



Reader properties (Settings tab)





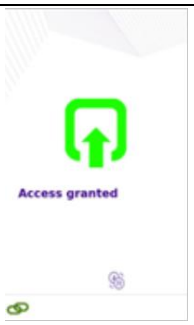
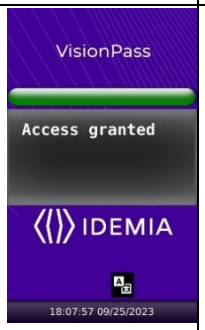
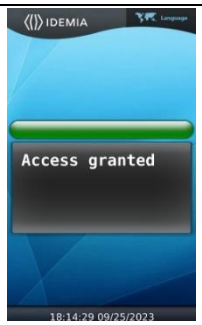
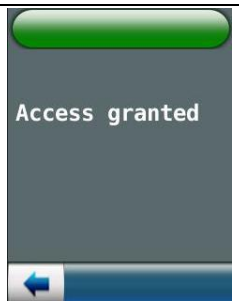
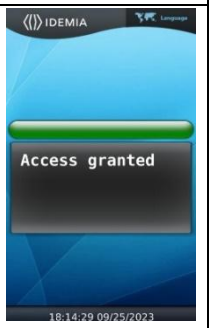
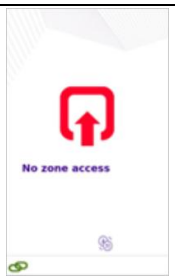
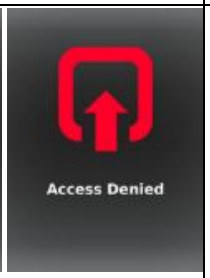
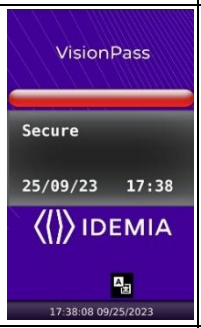
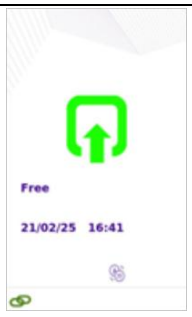
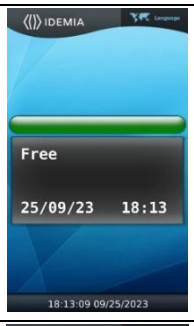
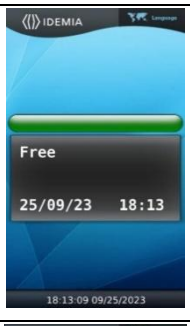


Copyright © Gallagher Group Limited

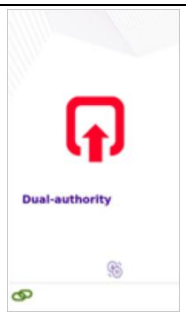
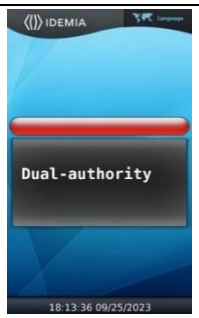
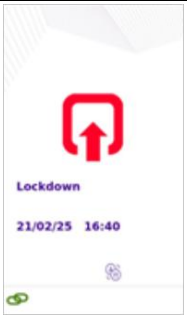
Morpho OSDP Reader status messages

Below is the list of Access Zone status messages that will display on the Morpho reader screen.

Note: Morpho readers do not support any Access Zone PIN modes.

Status or active state	Message displayed on reader screen				
	VisionPass SP reader	**VisionPass reader**	**MorphoWave reader**	**Sigma Lite+ reader**	**Sigma Extreme reader**
Access Granted					
Access Denied					
Secure Secure - PIN					
Free - No PIN Free - PIN					
Code or Card - No PIN Code or Card - PIN					

Copyright © Gallagher Group Limited

Status or active state	Message displayed on reader screen				
	VisionPass SP reader	VisionPass reader	MorphoWave reader	Sigma Lite+ reader	Sigma Extreme reader
Dual Auth - No PIN Dual Auth - PIN					
Lockdown					

VisionPass SP reader with OSDP connection but hasn't been assigned to a door:



Copyright © Gallagher Group Limited

15 QR Code authentication mode at Morpho Readers

Introduction

When configured to do so, cardholders can gain access at MorphoWave, VisionPass and VisionPass SP readers using a QR code. This topic is split into the three parts of this process, as follows:

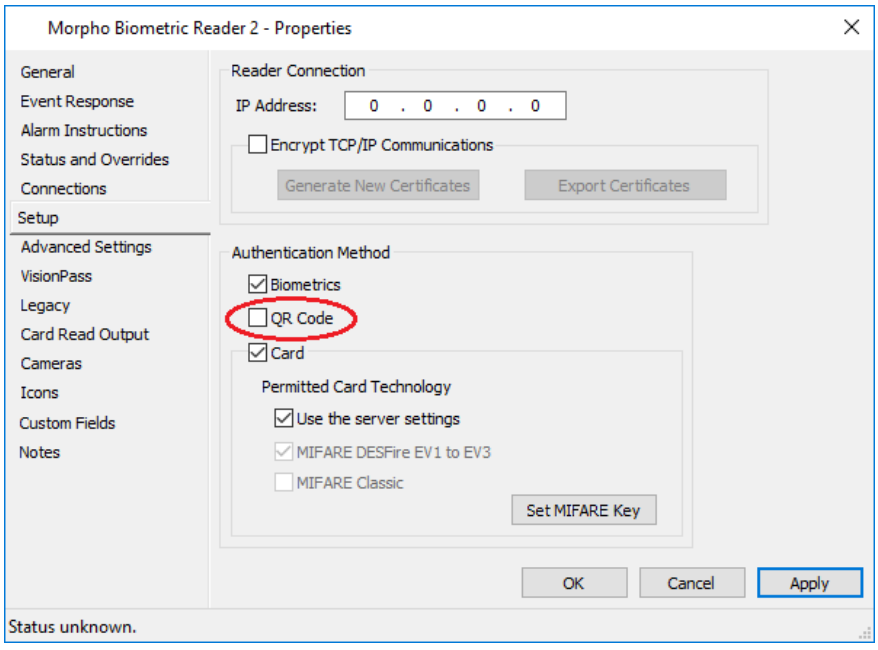
- Configuration of QR codes in Command Centre Configuration Client
  - Setting QR Code as Authentication Mode
  - Creating a card type with "New QR Code Access Token Object"
  - Configuring the Card Type
- QR Code specification recommendations
- Using QR code for access

Important: To ensure the QR Code reading is activated, the following firmware versions should be used:
- for VisionPass SP readers version 2.2.1 or 2.2.3
- for VisionPass readers version 2.8.9 (or later)
- for MorphoWave SP readers version 1.2.7 (or later)

Configuration

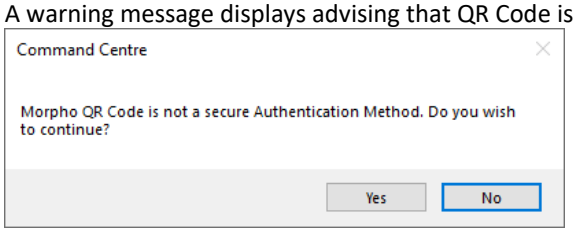
Setting the QR Code Authentication Mode

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**. The **Hardware** List Window opens.
2. **Right click** the MorphoWave or VisionPass reader that you want to support badging of a QR code for access.
3. Click the **Setup** tab.



4. Tick the **QR Code** checkbox.
5. Click **OK** to exit the reader properties and save your changes.

   A warning message displays advising that QR Code is not a secure method.

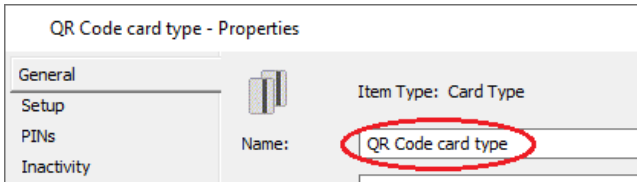


Copyright © Gallagher Group Limited

6. Click the **Yes** button.
   The warning message closes and your changes are applied to the reader properties.

Creating a Card Type

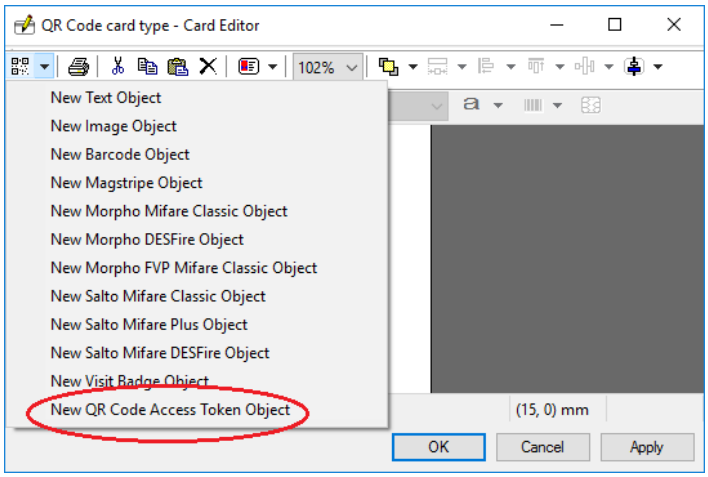
7. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
8. **Right click** and select **New...Card Type**.
   By default the **General** tab displays.
9. Enter an appropriate **Name** for this card type, (e.g. QR Code card type).



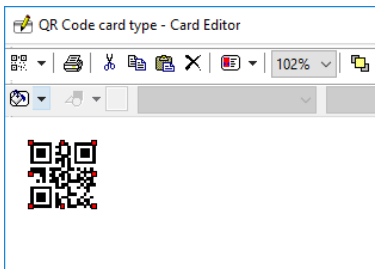
10. Click the **Setup** tab, and enter the correct **Facility Code**.
    Note: It is strongly recommended that you use a different Facility Code from the server, and create a separate QR User Group to avoid security vulnerabilities.
11. Click **OK** to save this card type.

Configuring the Card Type

12. Right click on the newly created **Card Type** and select **Edit Card Layout**.
    The Card Editor window displays.
13. Select **New QR Code Access Token Object** from the drop-down list of objects.



A QR barcode image displays with placeholders around it.

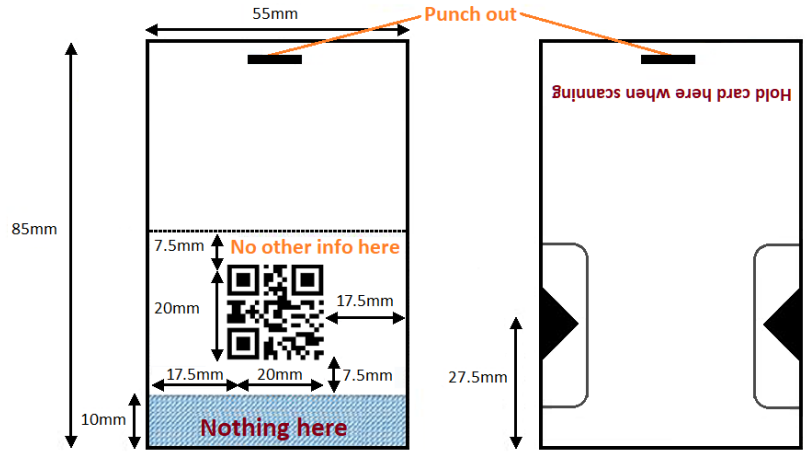


14. Click the **OK** button.
    The Card Editor window closes.
15. Assign the new QR Code card type to the cardholders.
    See ***Adding a Card to a Cardholder*** in the *Command Centre Configuration Client User Guide* for the procedure.

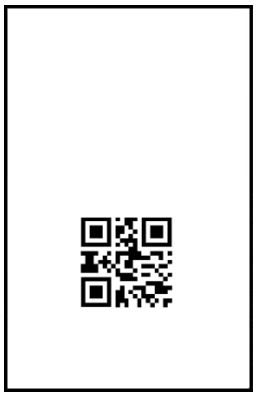
Copyright © Gallagher Group Limited

QR Code specification recommendations

- The QR Code data shall contain an UTF-8 string of 24 characters or less.
- The QR Code shall be printed on paper (not plastic) thick enough to ensure proper rigidity: 10 mil (usual business cards), the paper shall be white (no glossy / shiny) and the QR Code printed in black.
- For VisionPass readers, if you are using a mobile phone or tablet, the background shall be white and QR Code black, with brightness set to high.
- If the QR Code is to be used at a MorphoWave reader, to ensure both a good reading performance and a convenient user guidance while positioning the barcode in the scanning area, please make sure the recommended dimensions below are applied:
  Note: For VisionPass readers 4cm x 4cm barcode size is recommended.



Example: (do NOT resize)



Important: If the QR code size is not followed, this might cause some reading issues. For example, double read the QR code or after reading the QR code, MorphoWave reader asks for hand.

Using QR Code for access

Are you attempting to gain access at a MorphoWave reader or VisionPass reader?

If a…	then…
MorphoWave reader,	place the QR code into the reading area. If the QR code is valid access is granted. Otherwise, an access denied message will display.
VisionPass reader,	place the QR code between 15cm and 25cm away from the top of the reader. If the QR code is valid, and the cardholder is configured correctly with access, access is granted. Otherwise, an access denied message will display.

Copyright © Gallagher Group Limited

16 Troubleshooting

The following table describes some of the known issues that can occur with the installation of Morpho Readers, and possible solutions:

Problem	Possible Cause(s)	Solution
Reader not coming online	Network wiring incorrect	Either: • refer to section ***5.6 MA Sigma, MorphoWave, VisionPass SP and VisionPass Wiring*** for wiring instructions, or • refer to section ***6.1.1 Configuring Morpho Sigma and MorphoWave Readers using MBTA application*** Steps 6-11 for instructions on how to unlock the On-demand Security state.
	No Morpho readers in Command Centre license file	Obtain a new Command Centre license file that includes the Morpho feature. Contact Gallagher Technical Support.
Enrolment reader locks up	No dongle	Obtain a dongle. Uninstall the Sentinel software, and then reinstall it.
Reader generates *"Input parameters are not valid"* errors in the Trace Log file.	Insufficient power to the reader	Either: • connect readers directly to local power supplies (and not to Gallagher Controllers or URIs), or • use thicker power supply wire (allows greater distance between power supply and reader)
Reader appears to be working, but: • 'Access Denied' tone sounds, • the door opens, and • an *'Access Granted'* event is generated.	Incorrect wiring	Refer to section ***5.6 MA Sigma, MorphoWave, VisionPass SP and VisionPass Wiring*** for wiring instructions.
Readers generates *"Re-sync Access Failed*" or *"Updating the configuration failed"* alarm, and shows "The reader has rejected some configuration and a firmware update may be required to ensure correct terminal behaviour" in the status	Wrong firmware on reader	Upgrade reader firmware. Refer to ***5.3 Upgrading the MorphoAccess Reader Firmware***.
	MIFARE Classic and DESFire keys are not initiated	Initialise the keys under **Morpho Biometric Type** > **Card Encoding**.
You get the error message *"The selected permitted card technology settings are not supported by the biometric reader"* when setting permitted card technologies on the Card Reader properties.	If you attempt to set a morpho reader to follow the site default, but the site default does not allow either of the card technologies that the morpho reader does (MIFARE Classic or DESFire).	Either: • change the server settings to allow at least one of those two card technologies, or • have the Morpho reader NOT follow the site-wide settings.

Copyright © Gallagher Group Limited

Problem	Possible Cause(s)	Solution
T20 reader unresponsive when trying to put in the PIN when 'Secure + PIN' mode with VisionPass next to T20 reader.	VisionPass reader does not support 'Secure + PIN' mode and is attempting to grant access through VisionPass reader.	Add VisionPass reader to the same Controller as the T20 reader.
OSDP Morpho reader not coming online with status displaying "The device is not responding".	The reader has been replaced.	Perform a "Push Configuration" override.
OSDP Reader not coming online.	Network disconnection, device offline.	Remove OSDP Reader from the OSDP tab of the Controller and then add it back again.
Bad packet alarm generated Invalid packet type: 0x6B	Using a MorphoWave SP reader with old firmware can cause this scenario when "Show reader display messages" is ticked.	Either: • turn off "Show reader display messages" as the MorphoWave SP does not have an LCD screen, or • update the firmware to the latest version.
Slow read rate when using cards with MorphoWave SP	OSDP Display Messages Turned on	Turn off OSDP Reader Display Messages
VisionPass access reader does not load face templates. VisionPass denies access when badging a VisionPass DESFire card + bio	Enrolled with VisionPass SP	Enrol with VisionPass reader.

Copyright © Gallagher Group Limited