Gallagher Command Centre

Configuration Client User Guide

Volume 4

Version: vEL9.50
Date: April 2026
Part number: C209000

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 Limited 2026. All rights reserved.

Open Source Licenses

Command Centre includes software code developed by third parties. The open source code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors.

Command Centre installs a comprehensive list of the third party licenses (**ThirdPartyLicenses.txt**) in `C:\Program Files(x86)\Gallagher\Command Centre\ConfigClient`. Refer to this text file for full license details.

Copyright Notice

The software contains proprietary information of Gallagher Group Limited; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Gallagher Group Limited and the client and remains the exclusive property of Gallagher Group Limited. If you find any problems in the documentation, please report them to us in writing. Gallagher Group Limited does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Gallagher Group Limited.

Copyright notices of third party components:

- Barcode technology provided in this product is copyrighted by TAL Technologies, Inc.
- Report Print Preview in this product is provided by Portions Copyright © ComponentOne, LLC 1991-2002. All rights reserved.
- Portions of this product were created using LEADTOOLS © 1991-1999, LEAD Technologies, Inc.
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)
- This product includes cryptographic software written by Eric Young (eay@cryptosoft.com) and Tim Hudson (tjh@cryptosoft.com)

Gallagher Group Limited
Private Bag 3026
Hamilton
New Zealand
+64 (7) 838 9800
Internet E-Mail: security@gallagher.com
Website: http://www.gallagher.com

Table of Contents - Volume 1

Part 1: Introduction to Command Centre

Chapter 1: Introduction 1-1

Chapter 2: Getting Started 2-1
Logon 2-2
Restricting System View 2-9
Logoff 2-11
Automatic Logoff 2-12
Exit 2-13
Help 2-14
Operator Passwords 2-15
Dual Monitors 2-24
Magnetic window snapping 2-25
Using the advanced drag and drop feature 2-26

Chapter 3: Knowing your way around 3-1
List Windows 3-2
Generic Properties configuration 3-14

Chapter 4: Utilities 4-1

Part 2: Site Installation

Chapter 5: Setting up your Site 5-1
Recommended Site Configuration Process 5-2
Wizards 5-5

Chapter 6: Server Properties 6-1
Opening the Server Properties window 6-3
Licensing 6-4
Event Priorities 6-7
Alarm Flooding 6-9
Alarm Zone States 6-11
Event Defaults 6-12
Alarm Instruction Defaults 6-14
Alarm Transmission 6-15
Alarm Notes 6-17
Operator Defaults 6-19
User Codes and PINs 6-23
Competency Messages 6-24
State Names 6-26
Measurement Units 6-28
Advanced 6-30
Web Services 6-33
Card Security 6-37
Notifications 6-47
Outgoing Email 6-49
Incoming Email 6-52
Mobile/SMS Notifications 6-53
Import 6-55
Database Maintenance 6-56
Controller Defaults 6-58

Controller Web Server 6-60
Reserved Input Defaults 6-62
Challenge and More Challenge 6-63
Standards 6-64
Data Retention 6-72
Mobile Connect Settings 6-73
HBUS Terminals Defaults 1 and 2 6-76
SIP Settings 6-79
Icons 6-80
Custom Fields 6.81
Notes 6-85

Chapter 7: Card Types 7-1
Setting up Card Types 7-2

Chapter 8: Enrolment Wizard and Templates 8-1
Configuring Enrolment Templates 8-2
Using the Enrolment Wizard 8-7

Chapter 9: System Division 9-1
Divisions and Lineage 9-2
Setting up System Divisions 9-3
Cardholder Management across Divisions 9-5

Chapter 10: Access Zones 10-1
Understanding Access Zones 10-2
Adding a new Access Zone 10-3
Access Zone Lockdown 10-9
Anti-Passback 10-14
Configuring Strict Anti-tailgating 10-20
Enabling Zone Counting 10-22
Configuring No-Alone Zones 10-28
Manually Resetting Zone Counts 10-32
Configuring Pushbutton Overrides 10-34
Configuring Personalised Actions for Access Zones 10-36

Chapter 11: Day Categories 11-1
Adding a new day category 11-2
Changing the day category colour 11-3

Chapter 12: Schedules 12-1
Creating a new Schedule 12-2

Chapter 13: Calendars 13-1
Viewing/Editing the Default Calendar 13-2
Creating a Special Calendar 13-3
Assigning Days to Day Categories 13-5
Resetting Dates 13-7

Chapter 14: Alarm Zones 14-1
Setting up Alarm Zones 14-3
Adding multiple items to Alarm Zones 14-18

Chapter 15: Action Plans 15-1
Creating a new Action Plan 15-4
Assigning Action Plans to Events 15-10

Chapter 16: Alarm Instructions 16-1
Creating a new Alarm Instruction 16-2

Chapter 17: Insertion Tags 17-1
Creating an Insertion Tag 17-2
Adding an Insertion Tag to an Alarm Instruction 17-3
Chapter 18: Site Plans 18-1
Pop-up Menu 18-3
Creating a New Site Plan 18-4
Site Plan "Edit" and "View" modes 18-6
Editing a Site Plan 18-8
Drawing on Site Plans 18-12
Navigating between linked Site Plans 18-23
Removing Icons from Site Plans 18-24
Chapter 19: Icon Sets 19-1
Creating a new Icon Set 19-2
Modifying an existing Icon Set 19-5
Chapter 20: Macros 20-1
Creating a new Macro 20-2
Scheduling a Macro 20-7
Editing/Removing Actions for a Macro 20-10
Editing/Removing Scheduled run times for a Macro 20-12
Adding Command Lines for Macros 20-13
Placing a Macro on a Site Plan 20-17
Running a Macro 20-18
Duplicating a Macro 20-20
Chapter 21: Hardware 21-1
Creating Controller 7000s or 6000s 21-2
Creating a Controller 7000 Single Door 21-9
Configuring a Controller 7000 or 7000 Single Door for 802.1x 21-22
Upgrading a Controller 6000 to a Controller 7000 21-27
Creating Devices 21-45
Assigning Device Software to devices 21-45
Configuring EOL Resistors for devices 21-46
Linking devices to Controllers 21-48
Creating Inputs and Outputs 21-50
Linking Inputs and Outputs to devices 21-56
Creating Readers 21-57
Configuring HBUS Devices 21-65
Configuring an HBUS Keypad Reader 21-68
Configuring HBUS Terminals 21-74
Configuring an HBUS Contact Card Reader 21-109
Configuring an HBUS I/O Interface 21-127
Configuring an HBUS QuickSwitch Board 21-132
Chapter 22: Doors 22-1
Creating Doors 22-2
Configuring extended access time for a Door 22-11
Interlocking Doors 22-13
Challenge 22-19
Action on Access 22-31
Chapter 23: Elevator Cars 23-1
Low Level Interface Elevator Cars 23-2
High Level Interface Elevator Cars 23-7

Chapter 24: External Systems 24-1
The External System List Window 24-3
Configuring an External System Server 24-5
Configuring an External System 24-8
Configuring a DVR System 24-14
Configuring FTCAPI Trigger Strings and Reflected Outputs 24-22
SchindlerID 24-26
Adding external systems to a Site Plan 24-69

Chapter 25: Logic Blocks and Virtual Outputs 25-1
Scenarios using Logic and Virtual Outputs 25-4
Creating a new Logic Block 25-15
Creating a new Virtual Output 25-21

Chapter 26: Universal Card Format 26-1
Adding a new Universal Card Format 26-2
Deleting a Universal Card Format 26-10
Universal Card Formats for 'Use MIFARE Serial Number as Card Data (CSN mode) 26-11

Chapter 27: Device Software 27-1
Adding a new version of Device Software 27-2
Assigning Device Software to devices 27-5
Loading Device Software to a Controller 6000 or 7000 using a USB stick 27-9
Upgrading Multiple Controllers 27-11

Chapter 28: Services and Workstations 28-1
Creating a new Workstation Item 28-2
Editing a Service or Workstation Item 28-5
Deleting a Service or Workstation Item 28-6
Connecting to the Cloud 28-7
Server Migration 28-12
Creating a REST API Client Item 28-13

Chapter 29: External Alarm Monitoring 29-1
Setting up Contact ID 29-4
Setting the Country Code 29-6
Configuring an Alarm Transmitter/Dialler 29-10
Assigning the Alarm Transmitter/Dialler to a Controller 29-25
Configuring Items for Contact ID 29-27
Sample Messages 29-33
IP Alarms Receiver Software 29-34

Chapter 30: Licensing Groups 30-1
Creating a new Licensing Group 30-2

Chapter 31: Mobile Connect 31-1
Setting up Mobile Credential Types 31-3
Setting up Digital ID Types 31-6
Configuring a reader for Mobile Connect 31-8
Performing Bluetooth® Actions 31-14
SALTO Mobile Access Integration 31-19
Aperio Mobile Access Integration 31-21

Table of Contents - Volume 2

Part 3: Site Management

Chapter 32: Cardholders 32-1
Adding a New Cardholder 32-2
Copying Cardholder details 32-7
Adding a Card to a Cardholder 32-9
Removing a Card from a Cardholder 32-13
Editing Card details 32-15
Enabling Card Trace 32-16
Reactivating Expired or Disabled cards 32-17
Re-issuing a Card for a Cardholder 32-19
Editing a Cardholders PDF data 32-20
Configuring a User Code for Terminal Access 32-23
Configuring User Codes for access at Card Readers with keypads 32-25
Audit Trail of Cardholder changes 32-28
Running a Cardholder Report from a Cardholder 32-30
Reading MIFARE Cards using a MIFARE USB Encoder 32-31
Disabling the System Operator 32-34

Chapter 33: Personal Data Fields 33-1
Creating a new Personal Data Field 33-2
Capturing an Image 33-10

Chapter 34: Access Groups 34-1
Access Groups and Lineage 34-2
Setting up Access Groups 34-4
Configuring Access Group Privileges for Terminal Access 34-13
Temporary Access 34-17

Chapter 35: Notifications 35-1
Overall Process - Setting up Notifications 35-3
Creating a Notification Filter 35-5
Setting Cardholder "Email" and "Mobile" PDFs 35-9
Enabling Event/Alarm Notifications for a Cardholder 35-10
Setting Expiry Notification Threshold Values 35-14
Setting up Roles 35-17
Assigning Cardholders to Roles via Bulk Change 35-20
Copying all Cardholders under a Role 35-23
Notification Examples 35-25
Acknowledging alarms via SMS or email 35-28

Chapter 36: Operator Groups 36-1
Setting up Operator Groups 36-5
Configuring Operators 36-14

Chapter 37: Operator Privileges 37-1
Which Operator Privileges you require 37-2

Chapter 38: Bulk Changes 38-1
Initiating a new Cardholder Bulk Change 38-3
Initiating a new Division Bulk Change 38-15
Initiating an Inactive Cardholder Bulk Purge 38-19
Editing and Running a saved Cardholder Bulk Change 38-24
Initiating a new Alarm Zone Bulk Change 38-26
Initiating a new Controller 6000 Bulk Change 38-30
Initiating a new Reader Bulk Change 38-34
Initiating a new Door Bulk Change 38-37

Chapter 39: Reports 39-1
Creating a new report 39-2
Automatically Generated Reports 39-63
Printing an existing report 39-73
Customising Report Printouts 39-75
Editing settings of an existing report 39-77
The Report Print Preview window 39-78
Advanced Reports 39-81

Chapter 40: Archives, Backups and Restores 40-1
Configuring Archives 40-3
Performing Archives 40-8
Restoring Archives 40-11
Performing Backups 40-14
Restoring Backups 40-19

Part 4: Site Monitoring

Chapter 41: Find Tool 41-1
Using the Find Tool 41-2

Chapter 42: The Event and Alarm Viewers 42-1
Opening the Event Viewer window 42-2
Viewing event details 42-3
Events with Restorals 42-5
Alarm Viewers 42-6
Opening the Alarm Viewer window 42-8
Collapsing the alarm groups 42-10
Viewing alarm details 42-11
Viewing images associated with an alarm 42-15
Acknowledging an alarm 42-16
Processing an alarm 42-17
Quick Processing an alarm 42-18
Processing numerous alarms 42-20
Alarm sounds 42-23
Mute Alarm 42-25
Changing the Alarm Viewer behaviour 42-26
Notify Restoral 42-29

Chapter 43: Site Plans 43-1
Viewing an Existing Site Plan 43-2
Viewing Alarms from Site Plans 43-4

Chapter 44: Operator Sessions 44-1
Opening the Operator Sessions Viewer 44-2
Terminating an Operator Session 44-4

Chapter 45: Status and Overrides 45-1
Understanding Status and Overrides 45-2
Opening the Status Viewer 45-3
Adding items to the Status Viewer 45-5
Removing an item from the Status Viewer 45-6
Performing Overrides 45-7
Open a Door Request 45-13
Configuring Local Overrides at Card Readers 45-14

Chapter 46: Alarm Input Test Modes 46-1
Functionality provided by Alarm Input Test Modes 46-2
Configuring Inputs for Test Modes 46-5
Configuring Alarm Zones for Test Modes 46-7
Configuring Access Groups for Test Modes 46-9
Configuring Cardholders for Test Modes 46-11
Configuring Terminals for Test Modes 46-12
Configuring Event/Alarm Notifications for Test Modes 46-13

Table of Contents - Volume 3

Part 5: Licensable Features

Chapter 47: Card Layouts - Designing / Printing / Encoding 47-1
Overall Process 47-2
Designing Card Layouts 47-13
Printing/Encoding Cards 47-55
Batch Printing and/or Encoding 47-64

Chapter 48: Perimeter Fence Controllers 48-1
Creating a Fence Zone 48-2
Assigning a Fence Zone to a Terminal 48-6
Configuring an F3x/F4x/F5x/F6x Fence Controller 48-9
Configuring an F22 Fence Controller 48-19
Monitoring Fence Zone Status 48-27
Monitoring Fence Controller Status 48-28
Monitoring Fence Alarms and Events 48-29
Overriding a scheduled Fence Zone state 48-30
Overriding a Fence Controller 48-32
Creating a Voltage Report 48-34
Creating a Temperature Report 48-36
Using Server mode 48-38
Using HVplus mode 48-40

Chapter 49: Multi-Server systems 49-1
Important Issues 49-4
Remote Command Centre items 49-6
Creating a Remote Server 49-9
Switching from Peer-to-Peer structure to Star structure 49-13
Switching from Star structure to Peer-to-Peer structure 49-14
Adding a new server to a Star structure 49-15
Overriding a Remote Server 49-17
Event Aggregation 49-19
Deleting a server from a Peer-to-Peer structure 49-22
Deleting a child server from a Star structure 49-24

Chapter 50: Visitor Management 50-1
Visitor Management Application Installation Instructions 50-3
Command Centre Site Configuration 50-6
Using Visitor Management 50-66
Visitor Management Barcode Scanner Process 50-148
Visitor Management Passport/Drivers License Scanning Process 50-170

Chapter 51: Visitor Management Kiosk 51-1
Visitor Management Kiosk Installation Instructions 51-3
Visitor Management Kiosk Configuration 51-7
Configuring Visitor Management Kiosk 51-15
Visitor Management Kiosk Document Scanning Process 51-36
Visitor Management Kiosk screens 51-39

Chapter 52: Cardholder Competencies 52-1
Scenario: Accessing a zone restricted by cardholder competencies 52-3
Configuring Competencies 52-5
Assigning Competencies to cardholders 52-12
Adding Competencies to Access Zones 52-15
Overriding Operator Group Competencies 52-20
Reporting on Cardholder Competencies 52-23
Competency Bulk Changes 52-31

Chapter 53: Guard Tours 53-1
Creating a new Guard Tour 53-2
Running a Guard Tour 53-6
Creating a Guard Tour Report 53-10

Chapter 54: Enterprise Data Interface 54-1
Configuring operators 54-2
Configuring an interface 54-3
Manually running an interface 54-77
Stopping an interface 54-78
The log file 54-79
The failed file 54-80
Cardholder Interface configuration example 54-81
Booking Interface configuration examples 54-83
Troubleshooting 54-86

Chapter 55: Perimeter Sensors 55-1
Configuring a Z10 Tension Sensor Group 55-3
Fence Configuration Example 55-8
Performing a Maintenance Mode Override 55-9
Performing a Walk Test Mode Override 55-12
Tension Overload 55-14
Configuring a Z20 Disturbance Sensor 55-15
Configuring a D10 Tautwire Sensor 55-18
Assigning Z20 and D10 sensors to a Controller 6000 or 7000 55-20
Performing a 'Log Tuning Data' override on a Z20 Disturbance Sensor 55-22

Chapter 56: PIV Card Support 56-1
Installing the necessary applications/tools 56-3
Editing the PIV Card Type 56-7
Configuring the PIV Card Reader 56-18
Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Readers 56-21
Supporting custom OCSP URLs for PIV certificate validation 56-30
Enrolling PIV and PIV-I cards 56-32
PIV cards in Command Centre 56-33

Chapter 57: Active Directory Single Sign-on 57-1
Configuring Single Sign-on and Automatic logon 57-2
Linking operators to their Active Directory account 57-3

Chapter 58: Austco Intercoms 58-1
Configuring an Austco Intercom System 58-3
Configuring an Austco Intercom Item 58-4
Assigning an Austco Console to a Workstation 58-5
Locating an Austco Symbol 58-6

Chapter 59: Jacques Intercoms 59-1
Configuring an Intercom System 59-3
Configuring an Intercom 59-5
Opening the Intercom window 59-7
Placing a call 59-10
Answering a call 59-11

Chapter 60: Commend Intercoms 60-1
Configuring a Commend Intercom System 60-4
Configuring a Commend Intercom Item 60-6
Assigning a Commend Console to a Workstation 60-8
Using Commend Intercoms 60-9

Chapter 61: Class 5 End-of-Line Module (ELM) 61-1
Configuring a Class 5 ELM 61-2
Configuring Class 5 ELMs for Test Modes 61-6
Performing Overrides for Class 5 ELMs 61-8

Chapter 62: Locker Management Solution 62-1
Configuring a Locker Bank 62-4
Locker Bank Status and Overrides 62-16
Configuring a Locker 62-17
Locker Status and Overrides 62-19

Chapter 63: REST API 63-1

Chapter 64: UK GovPASS Card Support 64-1
Enrolling a UK GovPASS configuration card 64-2
Rolling configuration on a UK GovPASS card 64-5
UK GovPASS cards in Command Centre 64-6

Chapter 65: Prepay Car Parking 65-1
Understanding the Prepay Car Parking feature 65-3
Configuration examples 65-4
Configuring the Prepay Car Parking feature 65-5
Configuring a low credit warning signal 65-14

Chapter 66: Tag Tracking 66-1
Configuring the Tag Tracking feature 66-3
Setting up Tracking Tag Types 66-7

Chapter 67: SIP Integration 67-1

Chapter 68: PII Redaction 68-1
Redaction Configuration in Command Centre 68-3
Requesting a Cardholder Event Redaction 68-6
Requesting a Cardholder Information Redaction 68-7
Redacted Cardholders 68-8
Redaction events 68-9

Chapter 69: Apple Employee Badge 69-1
1. Configure Apple Keys 69-4
2. Configure Mobile Wallet Readers 69-5
3. Configure the Apple Employee Badge Type 69-7
4. Enable In-app Apple Employee Badge Provisioning 69-9
5. Manage Apple Employee Badges 69-11
6. Report Apple Employee Badge Assignments 69-14

Chapter 70: Shifts 70-1
Configuring a Shift 70-3
Purging Shift history 70-6
Chapter 71: CipherToken 71-1
Enrolling a CipherToken configuration 71-2
Rolling configuration on a CipherToken card 71-5
Configuring and printing CipherToken card layouts 71-6
Chapter 72: Entra ID Single Sign-on 72-1
Configuring Entra ID Single Sign-on and Automatic logon 72-3
Entra ID admin center configuration 72-4
Linking operators to their Entra ID account 72-5
Migrating from Active Directory Single Sign-on 72-7

Table of Contents - Volume 4

Part 6: Integrated Systems

Chapter 73: Morpho Biometric Integration 73-1
Installation 73-3
Installing MorphoAccess Readers 73-8
Supported Enrolment Devices 73-25
Creating a new Morpho Biometric Card Type 73-27
Creating a new Morpho Biometric Reader 73-35
Enrolling Users 73-44
Communications Encryption 73-56
Configuring Biometric Verification 73-65
Encoding Morpho Cards for Verification 73-67
Performing Overrides on a Morpho Biometric Reader 73-69
Morpho OSDP Configuration 73-71
QR Code authentication mode at Morpho Readers 73-82
Troubleshooting 73-86

Chapter 74: Salto Lock Interface 74-1
Space Compatibility 74-3
Space Installation 74-5
Space Site Configuration 74-31
Command Centre Site Configuration 74-71
Troubleshooting - Salto Lock Interface 74-112
Salto to Command Centre Event Mapping 74-113

Chapter 75: Nedap Readers 75-1

Chapter 76: Aperio Integration 76-1
Aperio Communication Hubs 76-4
Connecting the communication hubs to a Gallagher Controller 76-7
Aperio Site Configuration 76-10
Gallagher Command Centre Site Configuration 76-29
Configuring the Aperio Locks/Readers 76-42
Troubleshooting - Aperio Integration 76-78

Chapter 77: Schlage Lock Interface 77-1
Schlage Device Setup and Configuration 77-5
Configuring a Gallagher Controller for Schlage RS485 Devices 77-11
Creating a Schlage PIM (Panel Interface Module) 77-12
Creating a Schlage Door 77-15
Assigning Devices 77-20
Configuring a Universal Card Format to support different Schlage Credential Formats 77-23

Chapter 78: Allegion Engage Interface 78-1
Creating an Engage Site in Gallagher Configuration Client 78-3
Allegion Engage configuration 78-8
Command Centre configuration 78-19

Chapter 79: Open Supervised Device Protocol (OSDP) Integration 79-1
Configuring an OSDP Reader 79-3
Assigning an OSDP Compliant Reader to a Gallagher Controller 79-7
Moving OSDP Readers between Controllers 79-9

Chapter 80: QR Code Readers 80-1

Chapter 81: ThyssenKrupp Insight Elevator Systems 81-1
Configuring a ThyssenKrupp Insight Elevator System 81-2
Configuring a ThyssenKrupp Elevator Group 81-5
Configuring a ThyssenKrupp Elevator 81-10
Creating an Elevator Kiosk Control Schedule 81-12
Configuring a ThyssenKrupp Kiosk 81-14

Chapter 82: HALO Smart Sensor Integration 82-1

Appendices
Appendix A: Country Codes ..... Appx A-1
Appendix B: XYZ Event Mappings ..... Appx B-1
Appendix C: CCC Identifiers ..... Appx C-1

Glossary of Terms G-1

Index I-1

Part 6: Integrated Systems

This part of the User Guide provides detail on the systems that are currently integrated with Gallagher Command Centre, and how to use them, in the following chapters:

- **Chapter 73: Morpho Biometric Integration**
- **Chapter 74: Salto Lock Interface**
- **Chapter 75: Nedap Transit Readers**
- **Chapter 76: Aperio Integration**
- **Chapter 77: Schlage Wireless Lock Interface**
- **Chapter 78: Allegion Engage Interface**
- **Chapter 79: Open Supervised Device Protocol (OSDP) Integration**
- **Chapter 80: QR Code Readers**
- **Chapter 81: ThyssenKrupp Elevator Systems**
- **Chapter 82: HALO Smart Sensor Integration**

Chapter 73: Morpho Biometric Integration

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 chapter 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.

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.

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*** (on page 79-2) 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.

This section covers the following:

- ***Installation*** (on page 73-3)
- ***Installing MorphoAccess Readers*** (on page 73-8)
- ***Supported Enrolment Devices*** (on page 73-25)

- ***Creating a new Morpho Biometric Card Type*** (on page 73-26)
- ***Creating a new Morpho Biometric Reader*** (on page 73-35)
- ***Enrolling Users*** (on page 73-44)
- ***Communications Encryption*** (on page 73-56)
- ***Configuring Biometric Verification*** (on page 73-65)
- ***Encoding Morpho Cards for Verification*** (on page 73-67)
- ***Performing Overrides on a Morpho Biometric Reader*** (on page 73-69)
- ***Morpho OSDP Configuration*** (on page 73-71)
- ***QR Code authentication mode at Morpho Readers*** (on page 73-82)
- ***Troubleshooting*** (on page 73-86)

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.

- ***Installing Microsoft Redistributables*** (on page 73-4)
- ***Installing MSO330 and MSO1300 Drivers*** (on page 73-4)
- ***Installing the License Manager*** (on page 73-5)
- ***How to Retrieve Host ID and Install VERIF Software License*** (on page 73-6)

Installing Microsoft Redistributables

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

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.

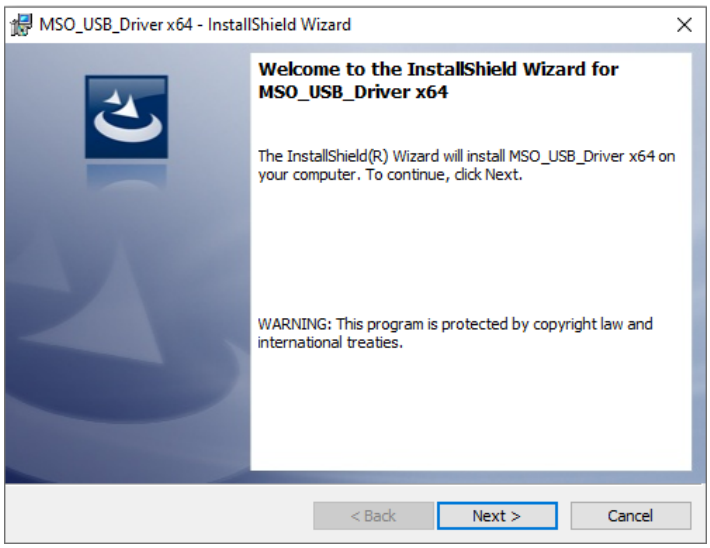
1. Navigate to the **`'Utilities\Morpho\Microsoft Redistributables'`** folder of the Command Centre installation files.

   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.

   Once the Microsoft Redistributables have been installed, restart the computer.

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.

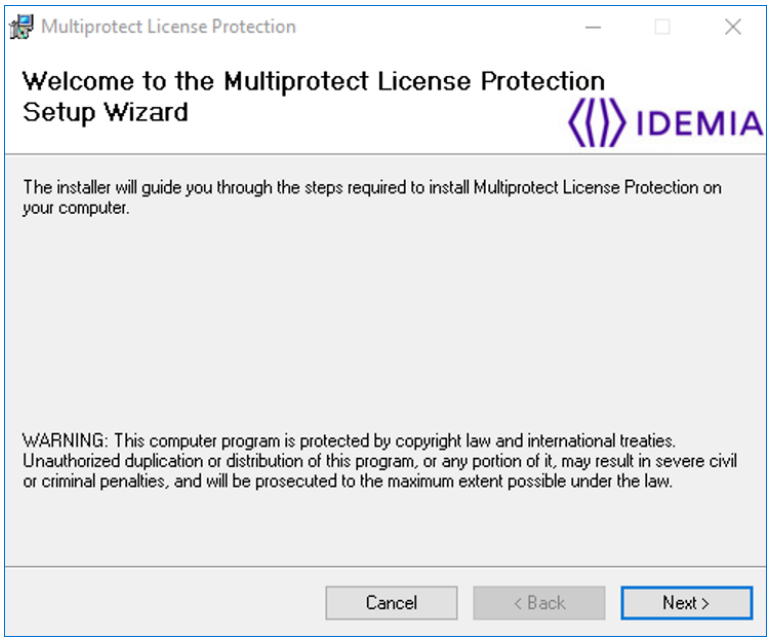


4. Click the **Next** button. The Destination Folder screen displays.
5. If you want to change installation directory for MorphoSmart Drivers click the **Change…** button and select another directory, otherwise click the **Next** button.
   The Ready to Install the Program screen displays.
6. Click the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

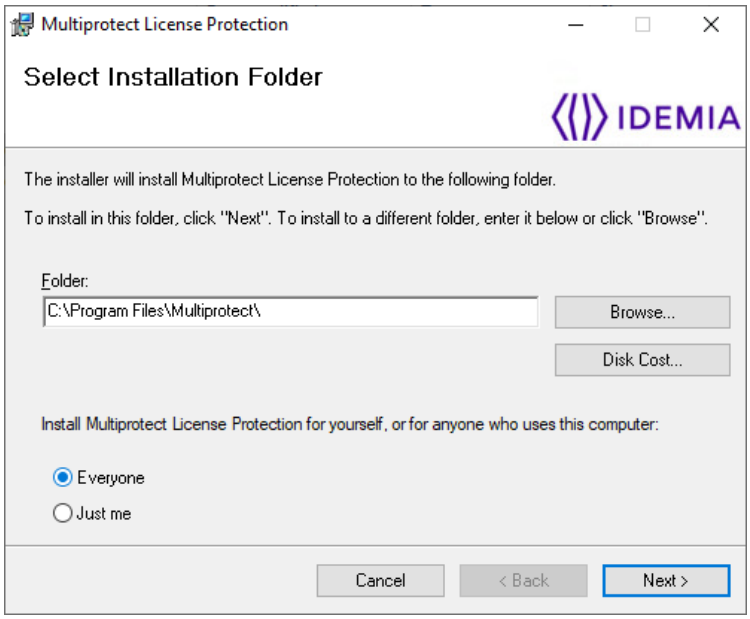
Installing the License Manager

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

How to Retrieve Host ID and Install VERIF Software License

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

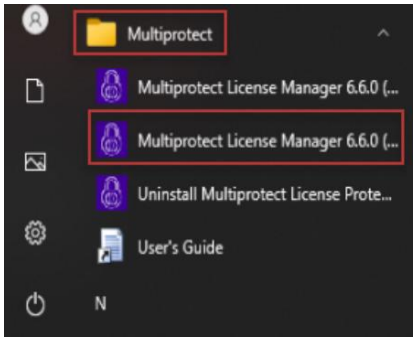
IMPORTANT: Verif dongles are obsolete. You will need to install a software VERIF License, alternatively you can purchase an MSO enrolment device with an embedded VERIF license.

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

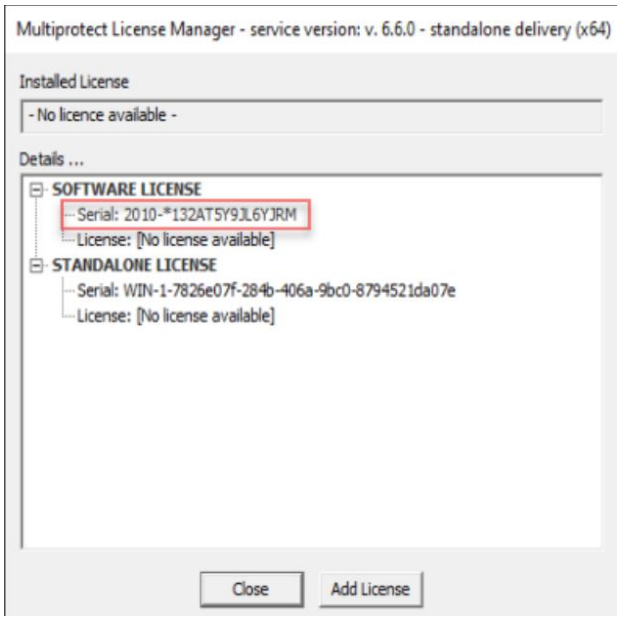
Software Verif License alternatives:
You can now choose an MSO enrolment reader with a verif license embedded.

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 **Multiproterct 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.

Installing MorphoAccess Readers

This section covers the following topics:

- ***Configuring a Biometric Reader*** (on page 73-9)
- ***Supported MorphoAccess Readers*** (on page 73-14)
- ***Upgrading the MorphoAccess Reader Firmware*** (on page 73-16)
- ***Physically installing MorphoAccess Readers*** (on page 73-18)
- ***OSDP Wiring*** (on page 73-18)
- ***MA Sigma, MorphoWave and VisionPass Wiring*** (on page 73-18)
- ***Power Supply Requirements*** (on page 73-20)
- ***Morpho Extended Database Licenses*** (on page 73-21)

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 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.

- ***Configuring Morpho Readers using MBTA application*** (next)
- ***Configuring Morpho Reader IP Address via Web Browser*** (on page 73-12)

Configuring Morpho Readers using MBTA application

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

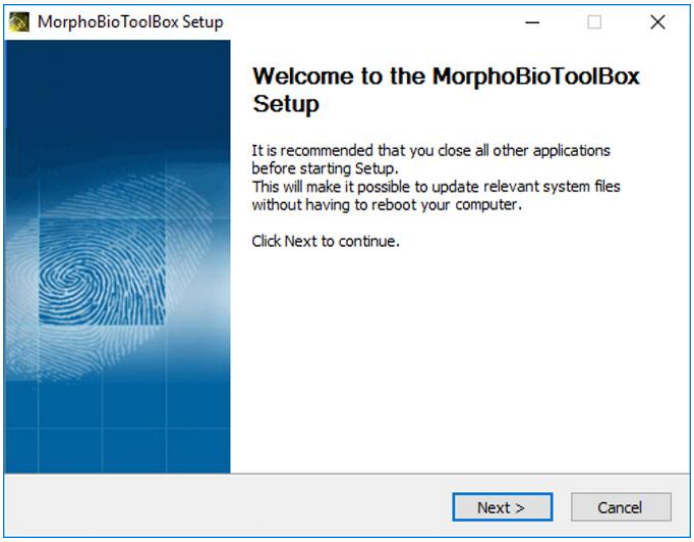
Before you begin

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 arbitary directory on your local hard drive, and execute it.
   The Welcome screen of the Morpho Biometric Terminal Administrator Setup Wizard displays.



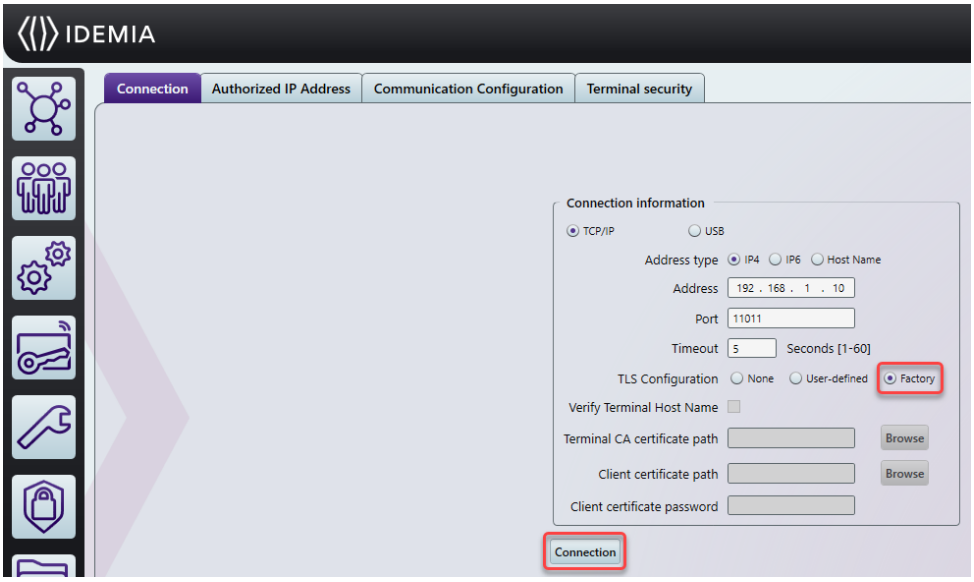
2. Click the **Next** button. The License Agreement screen displays.
3. Click the **I Agree** button. The Choose Install Location screen displays.
4. Choose the **Destination Folder** of MBTA installation, and click the **Install** button to start the proper installation. The Completion screen displays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

Morpho Biometric Terminal Administrator configuration

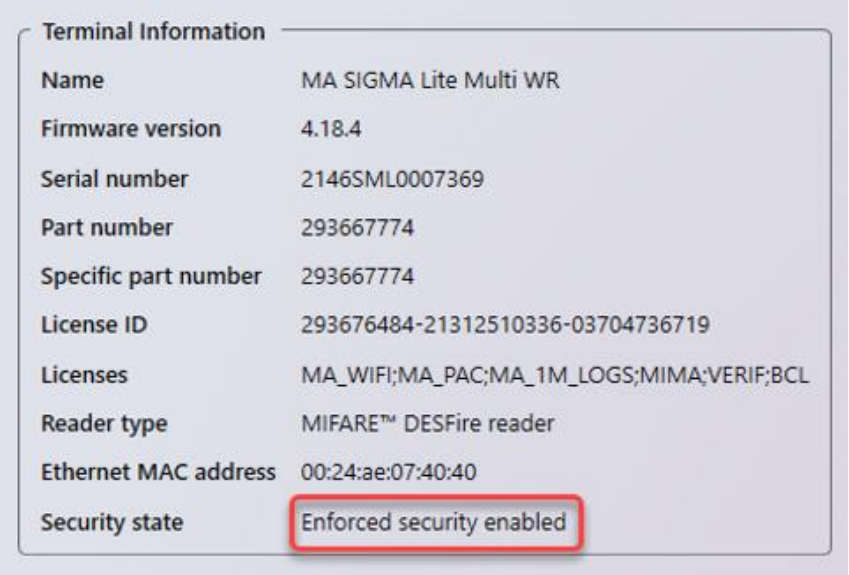
Note: Skip steps 7 to 10 if your device is unlocked. Any Morpho readers with a serial number greater than **2242xxxxxxxxx** will have 'On-demand Security state' enabled out of the box (must use MBTB v4.6.12 or later for this to work).

6. Double-click the **MBTA** icon 

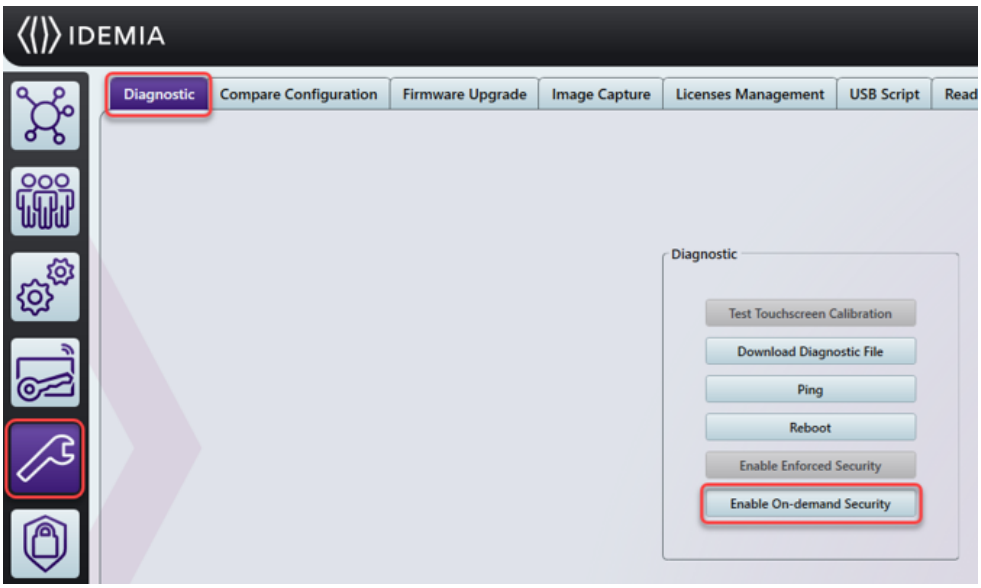
on your desktop.
7. Type in the IP address, click on the TLS Configuration **Factory** radio button and click the **Connection** button.



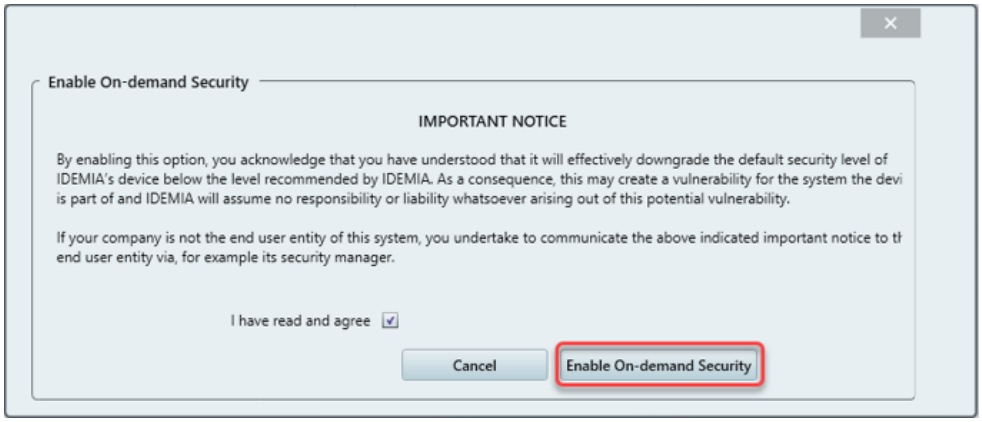
Note: When the device is in Enforced Security state, the security state Enforced security enabled is displayed.



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



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:

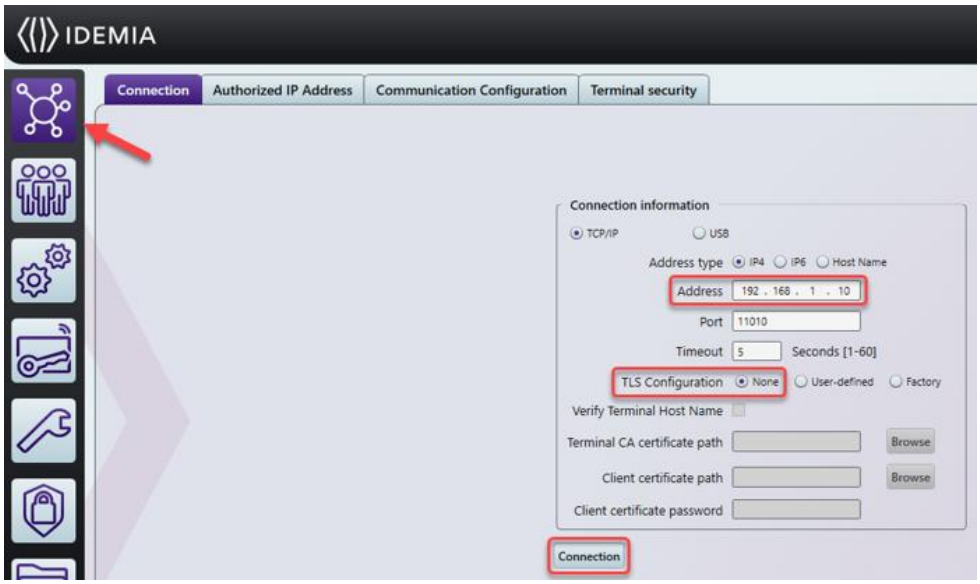


10. Once you have read the important notice carefully, tick the **I have read and agree** checkbox and click the **Enable On-demand security** button. This message will confirm that your reader has been correctly unsecured:

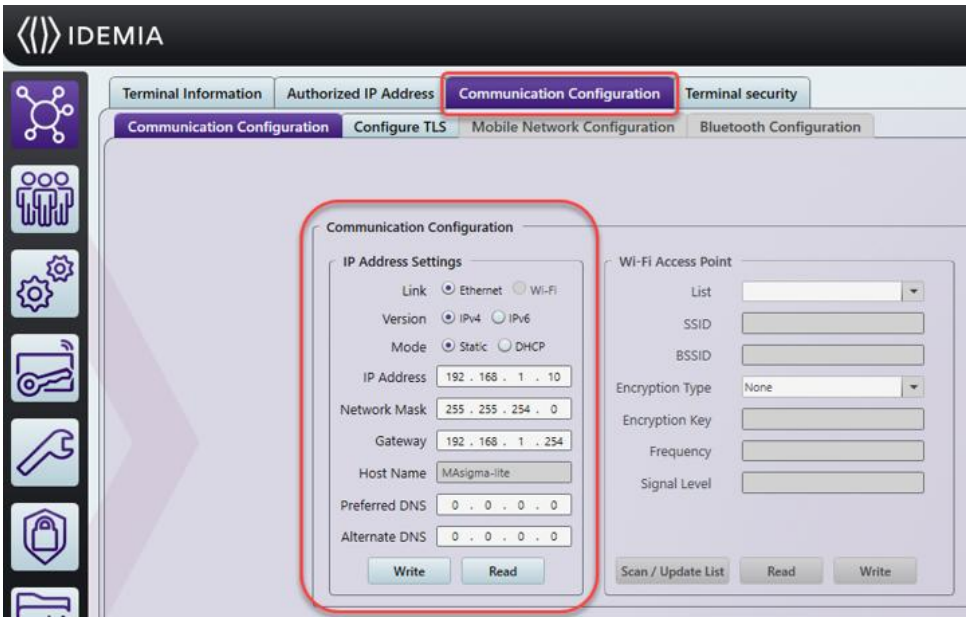


Now your reader is unsecured and you will be able to connect to it on port 11010.

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 the **Connection** button.

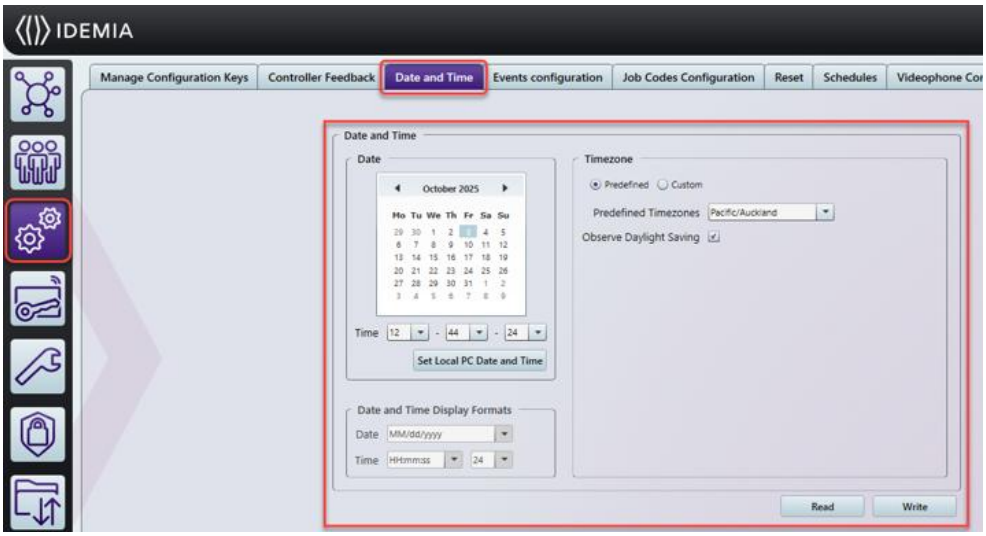


12. Modify the IP address of the reader. Click the **Communication Configuration** tab and modify the IP address settings as illustrated below:



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**.

Supported MorphoAccess Readers

The following MorphoAccess readers and associated firmware versions are supported.

- ***Supported IDEMIA Devices and Firmware versions*** (on page 73-14)
- ***Unsupported EOL IDEMIA Devices*** (on page 73-15)

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.

Supported IDEMIA Devices and Firmware versions

IDEMIA Device	Communication protocol	Recommendation	Most curent 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

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	February 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

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 ***Unencryption*** (on page 73-61) for further detail.
- Do not upgrade the reader via the USB method.

Enforced security firmware upgrade

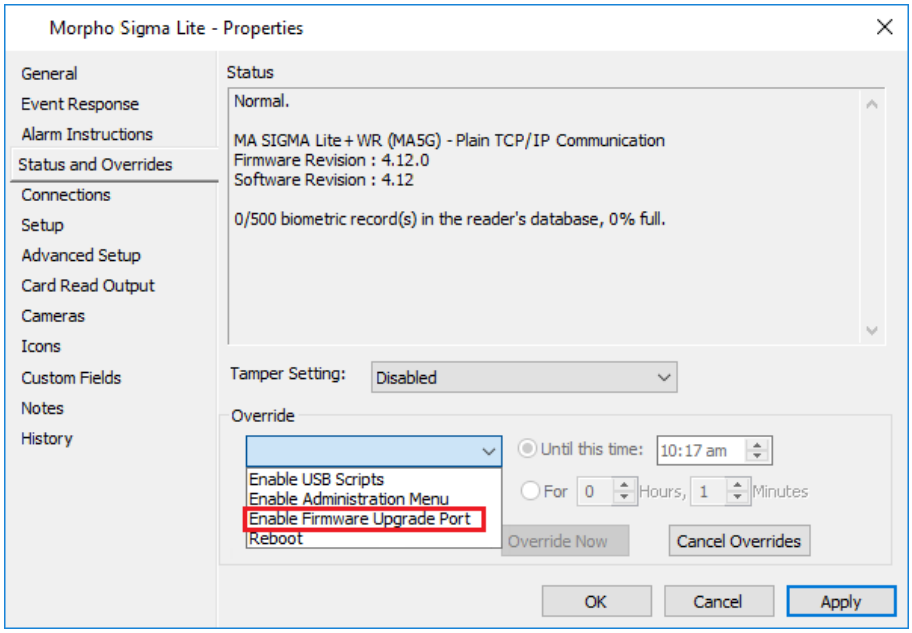
If you upgrade your device will reboot and enforced security will be enabled.
Enforce security firmware version:
SIGMA Lite and Lite+, from firmware 4.12
SIGMA Wide, from firmware 4.12
SIGMA Extreme, from firmware 4.12
MorphoWave Compact / XP, from firmware 2.9
MorphoWave SP, from firmware 1.1
VisionPass,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

Installing the Morpho Biometric Terminal Administrator

Note: See ***Configuring Morpho Readers using MBTA application*** (on page 73-9) for the components that need to be installed prior to running Morpho Biometric Terminal Administrator.

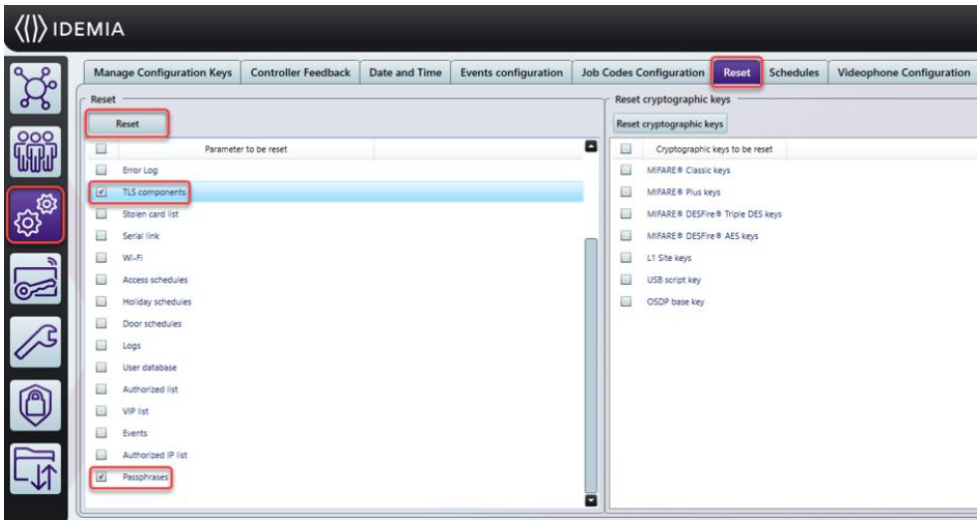
Upgrading the Firmware

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.

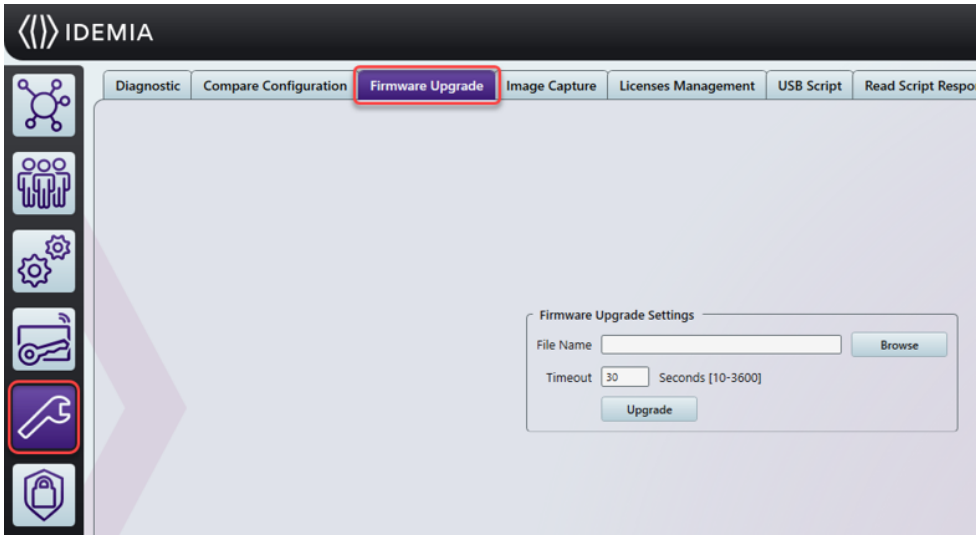


If you are upgrading to an enforced security version of firmware, follow Steps 1 to 9. If not, start at Step 4.

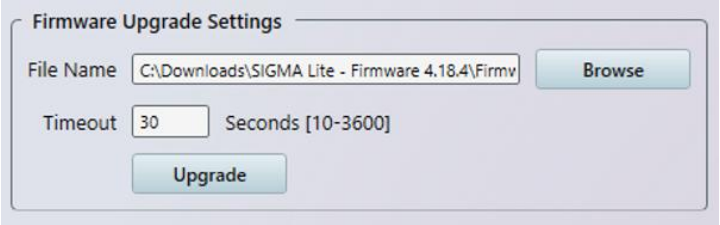
1. From the Morpho Biometric Terminal Administrator Connection screen, select the **Device Settings** button, then click the **Reset** tab.



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.

Physically installing MorphoAccess Readers

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

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)	-

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 ***Power Supply Requirements*** (on page 73-20) for further details.

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 ***Power Supply Requirements*** (on page 73-20) 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

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.**

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 ***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).

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:*



- ***Morpho Reader Default User Databases*** (next)
- ***Available Morpho Database Extension License*** (on page 73-21)
- ***Upgrade Database Extension License*** (on page 73-22)

Morpho Reader Default User Databases

Reader	Requirements
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.

Available Morpho Reader Database Extension License

Reader Expansion 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

Upgrade Database Extension License

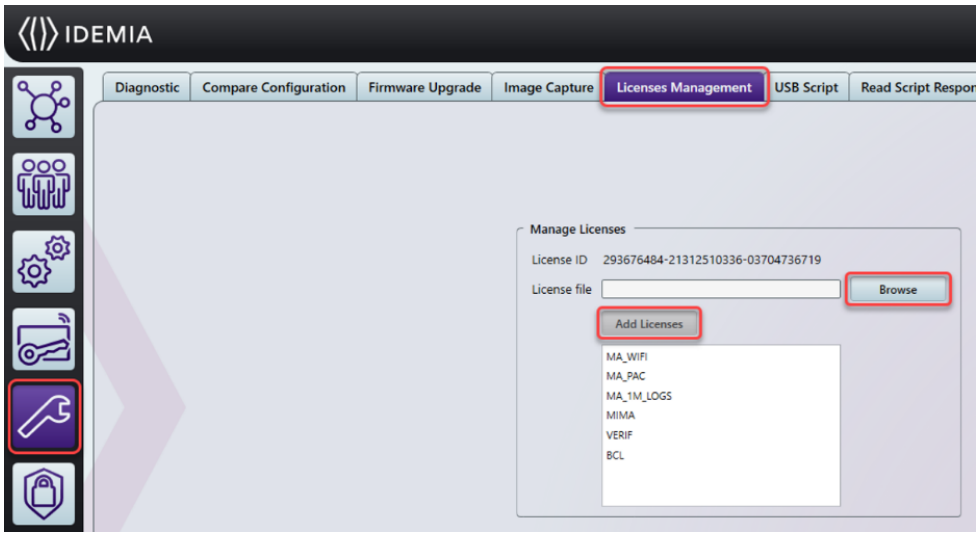
Requirements

- 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.



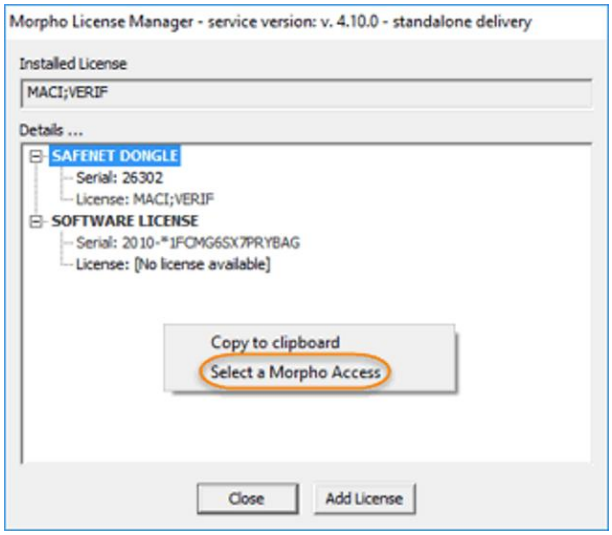
To add the licenses, select a license file using the **Browse** button and then click the **Add Licenses** button.
After the licenses are added successfully, the licenses are displayed in the list and will be updated immediately.

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 Manager 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.

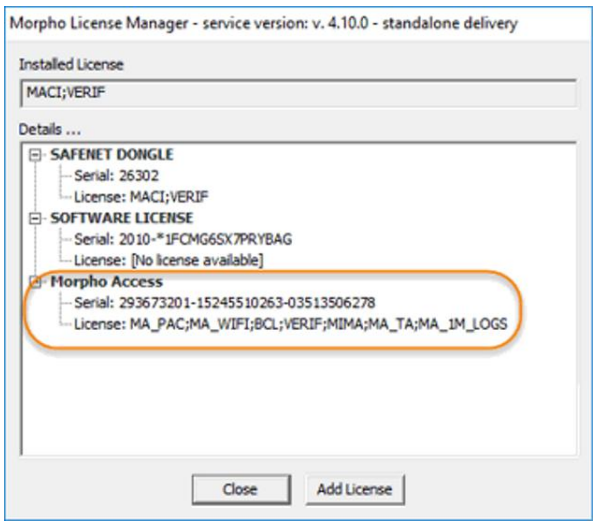
1. Open the Morpho Licence Manager, right-click in the empty white space and click **Select a Morpho Access**.



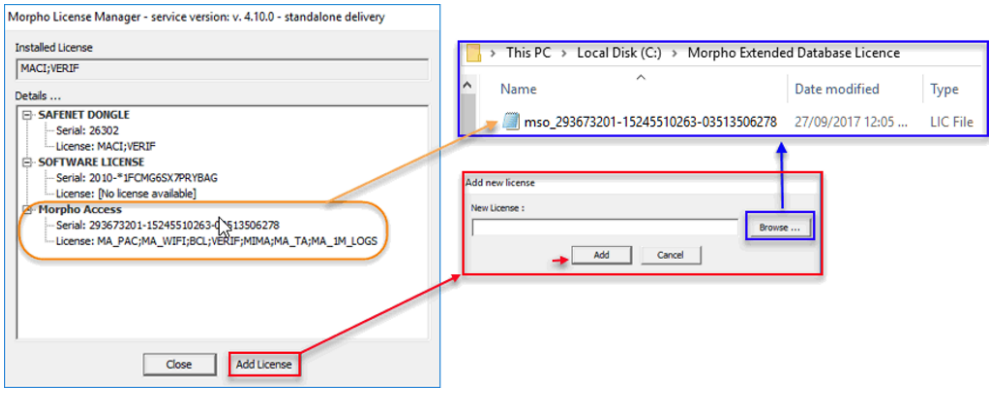
2. Input the IP Address of your Morpho Reader and click the **OK** button.



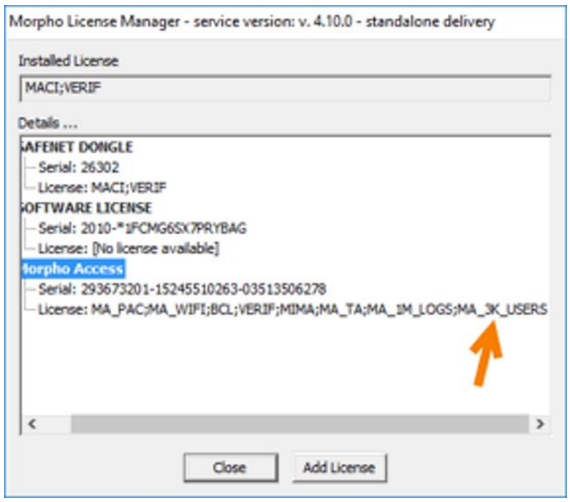
The **Morpho Access** reader serial number displays.
Note: The serial number matches the License ID that is printed on the readers label.



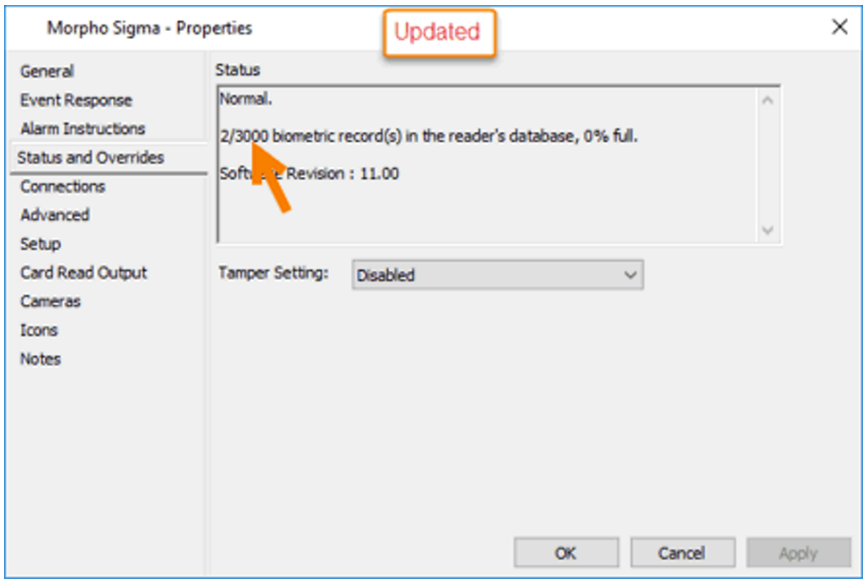
3. Click the **Add License** button.
   The Add new license window displays.
4. Browse to the Morpho Extended Database License specific to the reader you are connected to. The License number will match the Morpho Access serial and readers License ID.



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.



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.

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').

Creating a new Morpho Biometric Card Type

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.

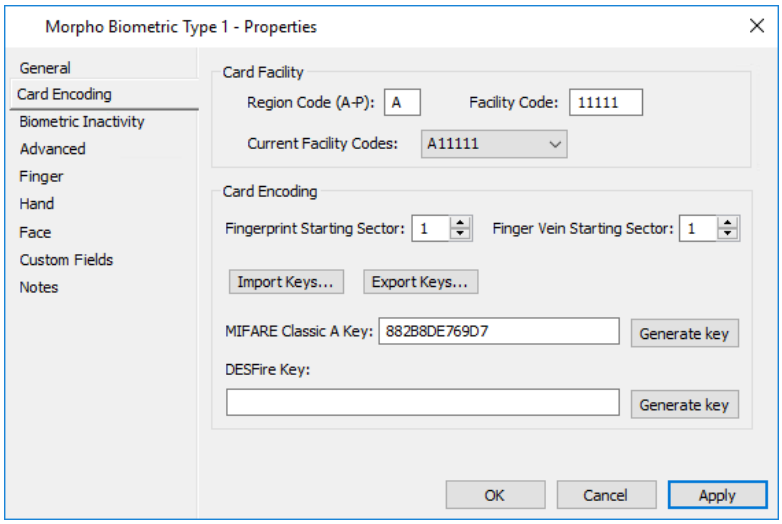
Notes:

- 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.

Procedure

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Card Types**. The **Card Type** List Window opens (in grid view).
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.

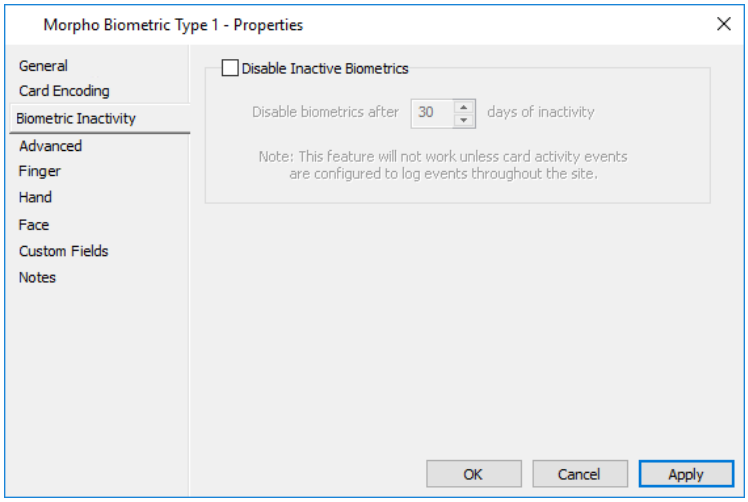
Field	Description
Region Code	This is the letter representing the **Region Code** for your Facility Code. **Note:** 'A' is the default and should be changed to match the Region Code in your site license. Refer to the **Licensing** tab of the Server Properties for the Region Code.
Facility Code	Although 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	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.

Field	Description
DESFire Key	The key entered here is used to control access to the Morpho data encoded on a card. **Notes:** • 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.
   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.



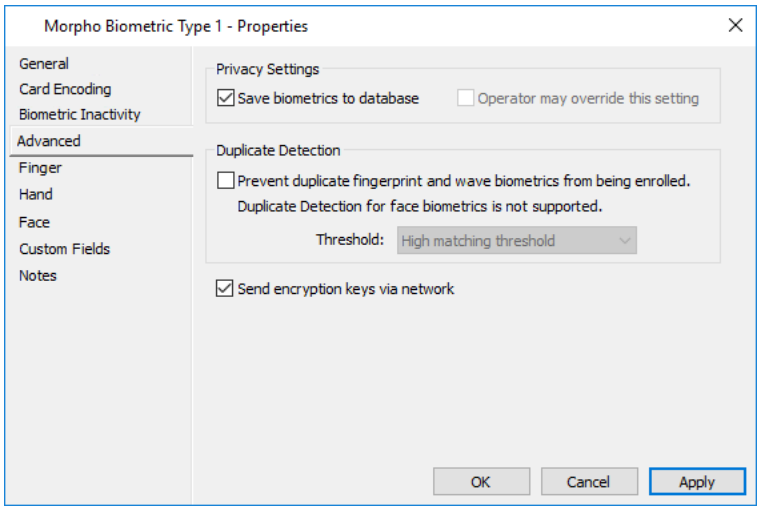
10. Do you wish to enable the Inactive Biometrics Expiry feature?

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

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

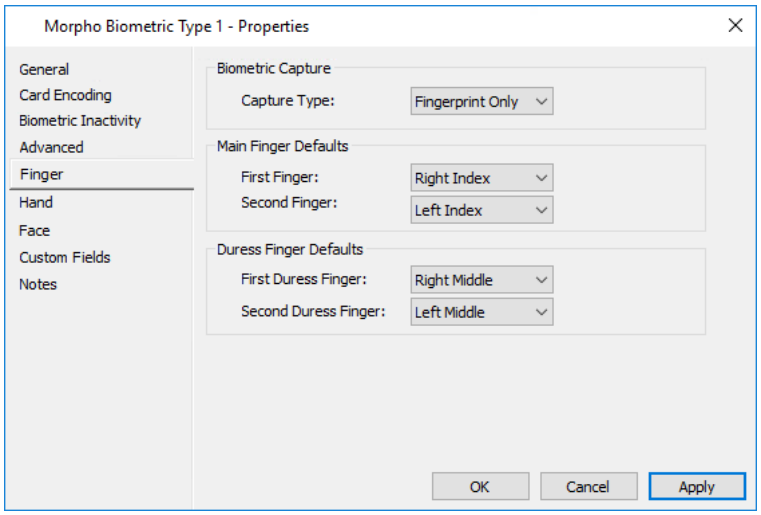
    - When this feature is first enabled the default timeout = 30 days. The range is 1-999 days.
    - If you set the biometrics to disable after 1 day of inactivity, they will become disabled 24 hours to the second after the **Apply** button is clicked.
    - Cardholders will be expired regardless of activity if card activity events are not configured to log events throughout the site.
      (Refer to ***Event Defaults*** on page 6-12 for further detail.)

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 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 ***Encryption using Command Centre*** (on page 73-57) 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 ***Encryption using the Biometric Encryption Utility*** (on page 73-58) 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.

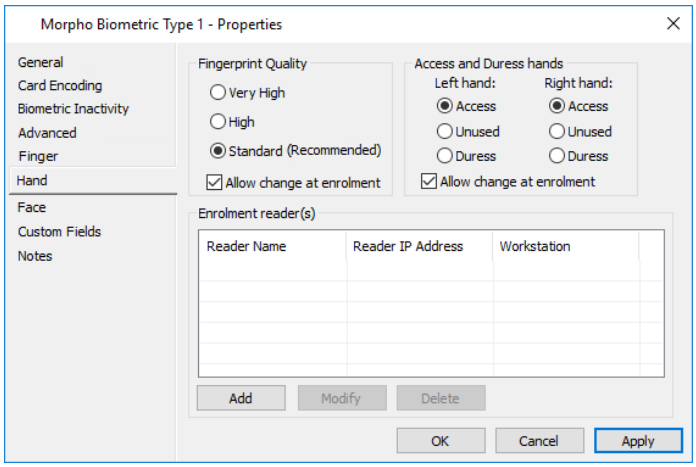


17. Configure the settings on this screen as appropriate.

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 20. 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 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.

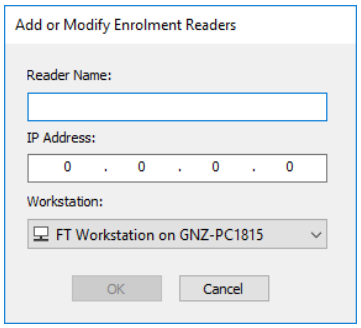
Encrypted MorphoWave readers cannot be used for enrolment. A connection error will be seen when trying to capture.

19. Configure the settings on this screen as appropriate.

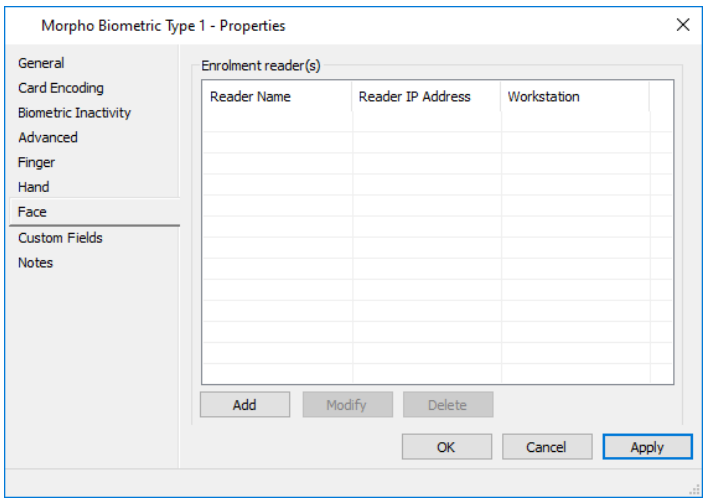
Section	Description
Fingerprint Quality	Click the appropriate radio button for a default acceptable fingerprint quality. (Default and recommended option = Standard) If you want operators to have the ability to change the acceptable quality at the time of enrolment, tick the **Allow change at enrolment** 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.

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



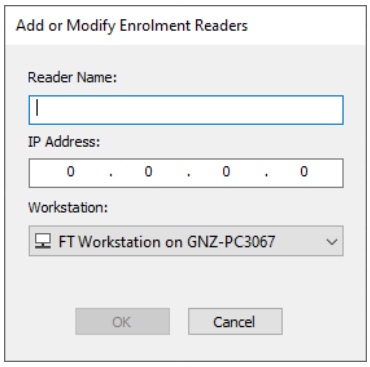
21. Enter the **Reader Name** and **IP Address**, and select the appropriate **Workstation** from the drop-down list.
22. Click the **OK** button.
    The Add or Modify Enrolment Readers dialog closes, and the readers details populate the **Enrolment reader(s)** grid. **Notes:**
    - The **Modify** 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 if your site is using VisionPass readers.





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 list.
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, by creating a new Enrolment reader item with a different workstation.
27. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Morpho Biometric Type.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
28. Click the **Notes** tab if you want to add a note(s) about this Morpho Biometric Type.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
29. 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.

Result

A Morpho Biometric Card Type has been configured and is ready for use. To capture fingerprints against cardholders, see ***Enrolling Users*** (page 73-44).

Hint

Editing and Deleting Morpho Biometric Types
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Morpho Biometric Types.
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.

Creating a new Morpho Biometric Reader

Introduction

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

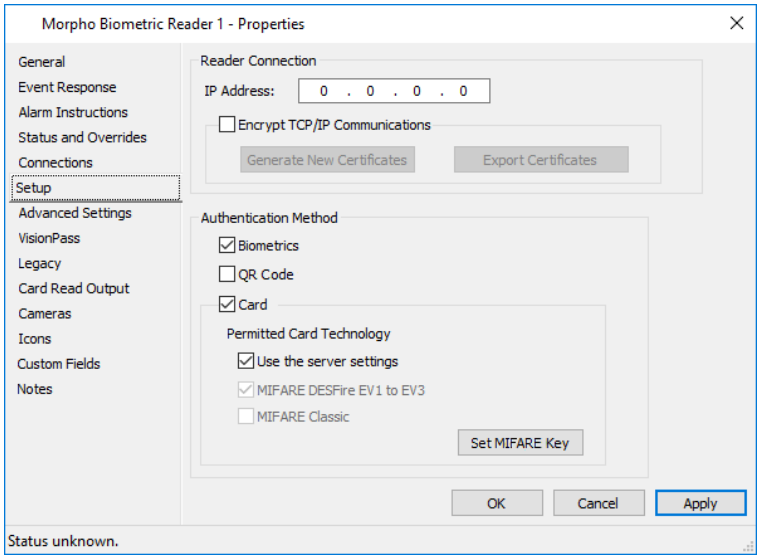
Before you begin

Before you begin this procedure ensure that a Morpho Biometric Type has already been created. See ***Creating a new Morpho Biometric Card Type*** (on page 73-26) for the procedure.

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 (in tree view).
2. **Right click** and select **New...Morpho Biometric Reader**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
5. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
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 overrides can be performed from the **Status and Overrides** tab. See ***Performing Overrides on a Morpho Biometric Reader*** (on page 72-69) 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.

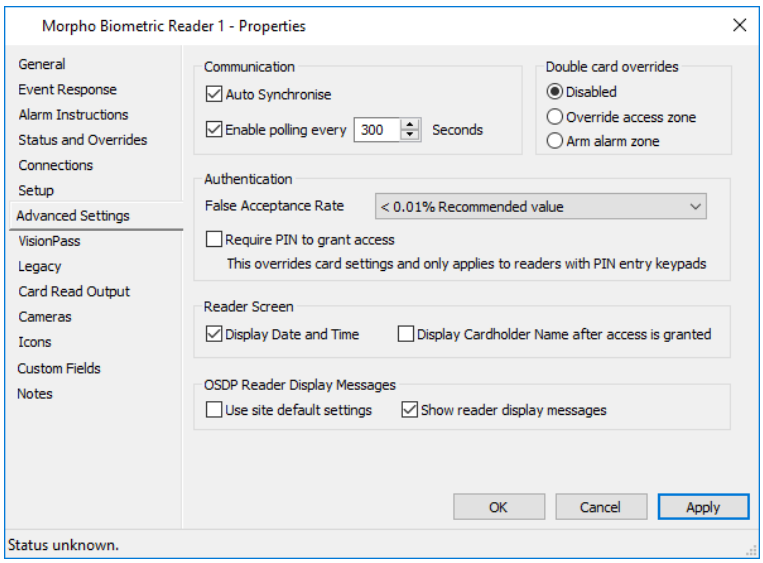
Field/Checkbox	Description
IP Address	Enter the IP Address of this reader (as previously configured in ***Configuring a Biometric Reader*** on page 73-9). **Note:** DHCP is not supported for Morpho Readers' IP Addresses. (Default = 192.168.1.10)
Encrypt TCP/IP Communications	This option is off (disabled) by default. If you want to use encrypted communications for this reader, refer to ***Communications Encryption*** (on page 73-56) 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.

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

Field	Description
	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** section as appropriate.

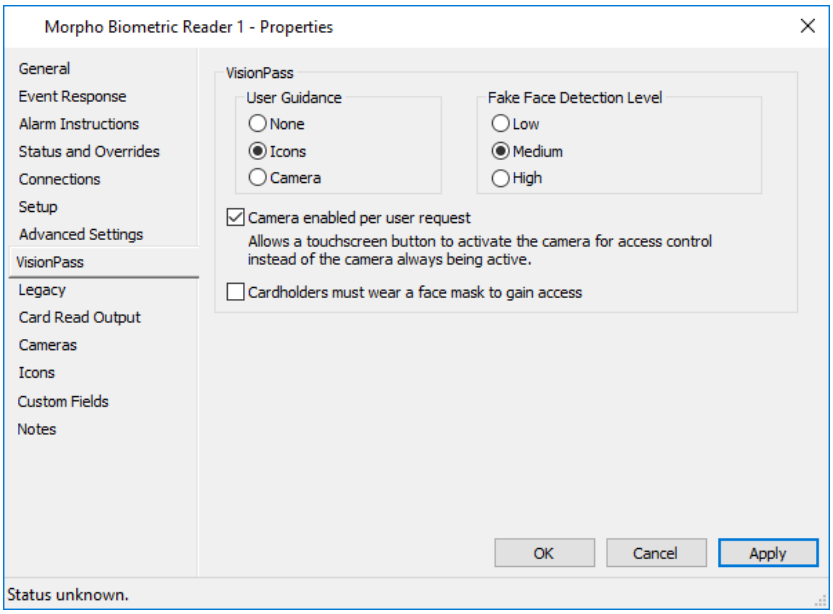
Field/Checkbox	Description
Display Date and Time	Enabling this checkbox means that Morpho Reader models with screens, and in Native Mode (MA5G), will display the date and time.

Field/Checkbox	Description
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 ODSP.

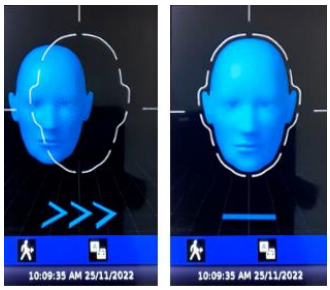
16. Do you want access and status messages to be displayed on this reader's screen?

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 **User 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 **Show reader display messages** checkbox.

17. Click the **VisionPass** tab.

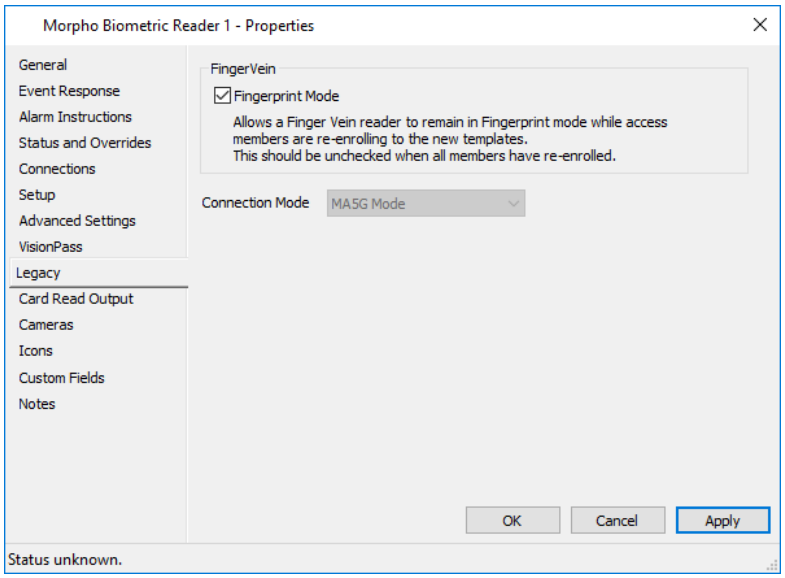


18. Configure the the **VisionPass** settings on this screen if this reader is a VisionPass reader.
Note: The fields will be populated with any previously configured values for existing biometric readers.

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.
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 un-checked by default. If you leave it unchecked, then it operates by motion detection. Any move-ment at the camera will trigger it to try to capture a face.

Field/Checkbox	Description
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.



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 however are no longer supported.
22. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Morpho Biometric Reader.
    For further details see ***Cameras tab*** (on page 3-24).
23. Click the **Icons** tab if you want to change the Icon Set for this Morpho Biometric Reader. For further details, see ***Icons*** (on page 6-80).
24. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Morpho Biometric Reader.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).

25. Click the **Notes** tab if you want to add a note(s) about this Morpho Biometric Reader. For further details, see ***Notes*** (on page 6-85).
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.

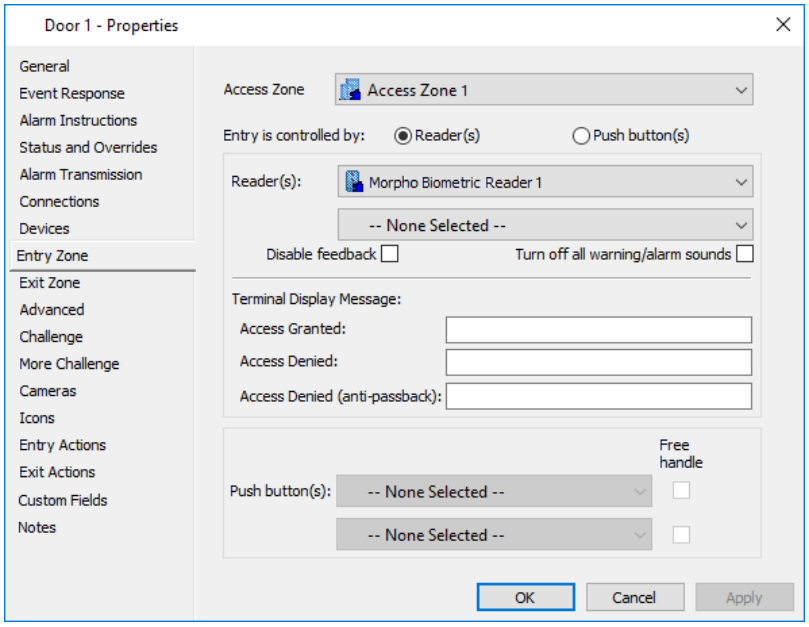
Assigning the Morpho Biometric Reader

Once the configuration work is complete, you need to assign the Moprho 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 ***Configuring the Controller RS-485 Bus for OSDP*** (on page 73-73) 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 you selected. The example shown below is for a Door.



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

Gallagher…	can host a maximum of…
Controller 6000, Controller 7000	32 x Moprho readers for OSDP (16 per RS-485) Controller 7000; 16 x Morpho readers for OSDP (16 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.

Result

A Morpho Biometric Reader has been configured and is ready for use.
Note: A Morpho Biometric Reader can be synchronised using macros.

Hint

Editing and Deleting Morpho Biometric Readers
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Morpho Biometric Readers.
Notes:

- 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.

Enrolling Users



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

- ***Configuring a Cardholder Biometrics Tile*** (next)
- ***Capturing Biometrics (Finger print or Finger Vein)*** (on page 73-46)
- ***Capturing Biometrics (Hand)*** (on page 73-48)
- ***Capturing Biometrics (Face)*** (on page 73-52)
- ***Re-enabling Inactive Biometrics*** (on page 73-55)

Configuring a Cardholder Biometrics Tile

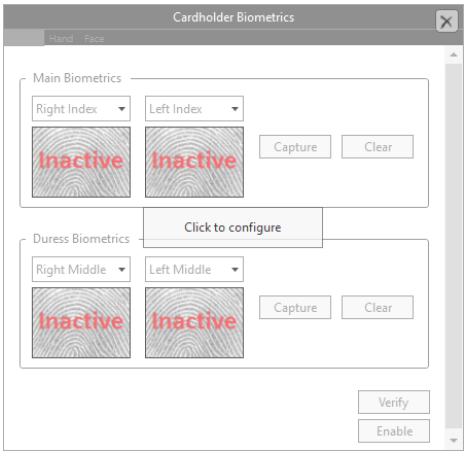
This tile provides the user with the ability to capture and verify biometrics, (i.e. fingerprint, hand and face), and is only used on a Cardholder Viewer.

Operator Privileges

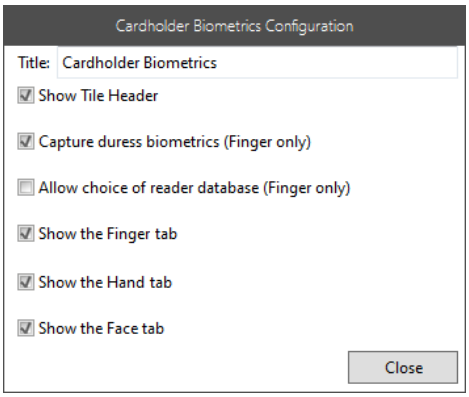
To...	You need...
view a Cardholder's biometrics,	one of the following privileges in the division of the cardholder: • "View Cardholders" • "Edit Cardholders" • "View Cardholder Notes" • "Edit Cardholder Notes" • "Edit Cardholder Notification" • "Print/Preview & Encode Card" • "Delete Cardholders" **Note:** 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.



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 Data-base ID. What model of finger Morpho Biomertric 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.

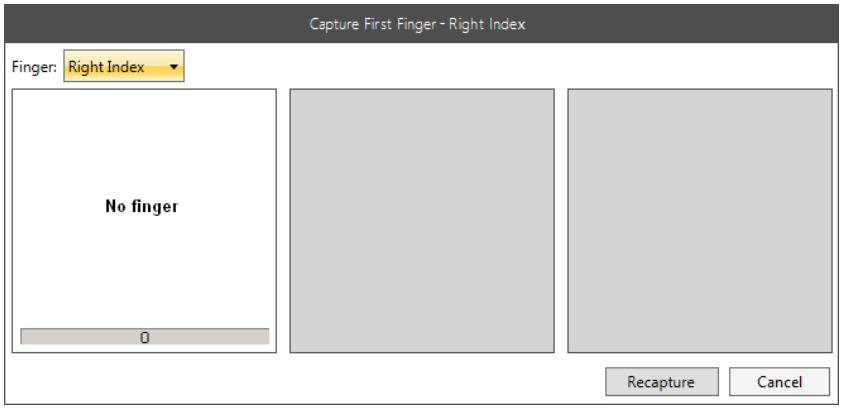
Capturing Biometrics (Fingerprint or Finger Vein)

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

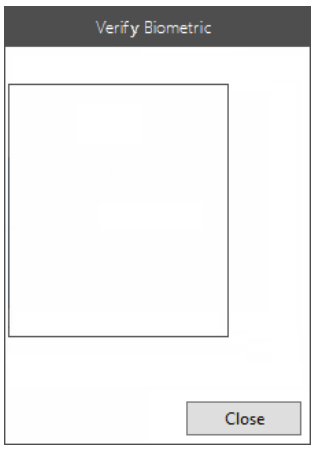
For the…	You need…
Server workstation	+ Microsoft Visual vc10redist_x86 + Microsoft Visual vc12redist_x86 + Microsoft Visual vc14redist_x86 + Microsoft Visual vc14redist_x64
Client workstation	+ Microsoft Visual vc10redist_x86 + Microsoft Visual vc12redist_x86 + Microsoft Visual vc14redist_x86 + Microsoft 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 ***Installing Microsoft Redistributables*** (on page 73-4).
   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:
   - 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.

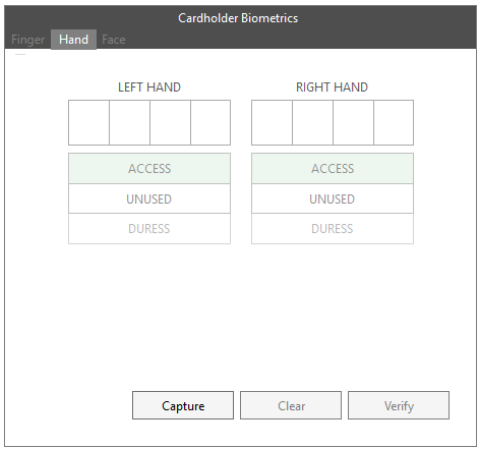


7. Place the appropriate finger on the enrolment device.
   The system verifies whether the captured biometrics match the existing templates already captured, and the appropriate message box displays indicating if there is a match or not. Once a match has been made the finger image is removed and result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

Capturing Biometrics (Hand)

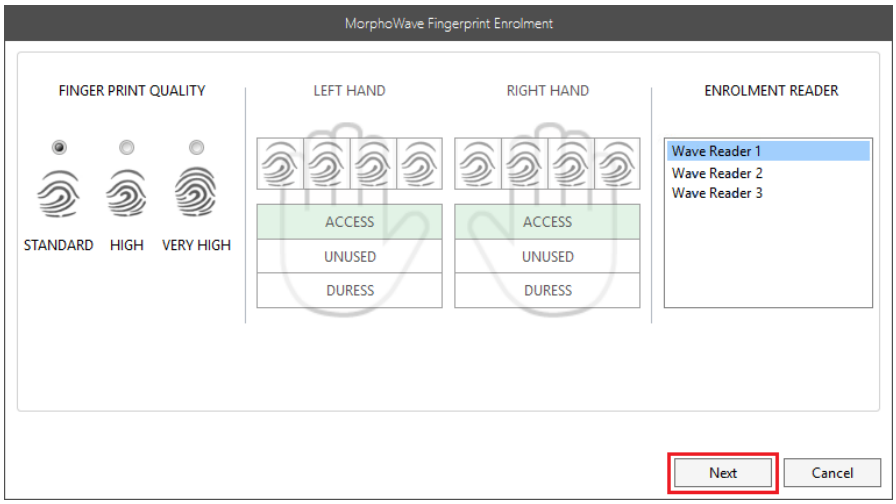
The following procedure describes how to enrol a Cardholder's fingerprints using a MorphoWave Reader:
Note: Previously used DESFire cards should not be encoded for different cardholders.

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.



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

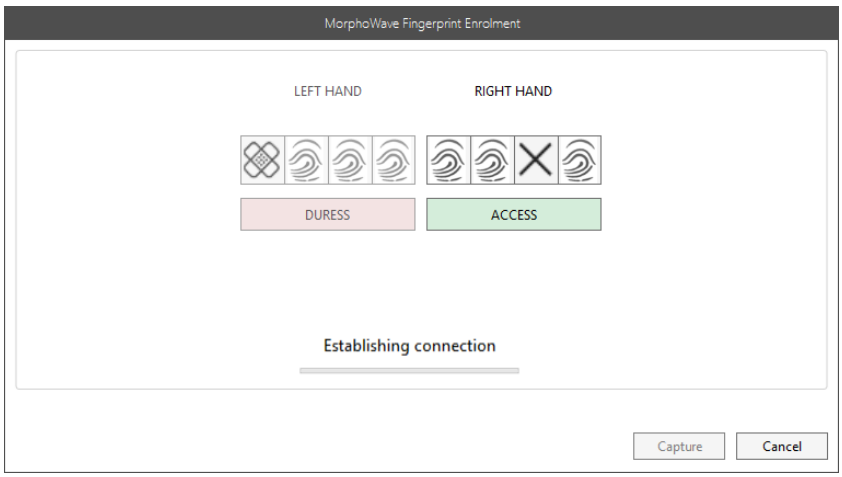
3. If the Morpho Biometric Card Type (in the Configuration Client) has been configured to allow changes at the time of enrolment, you can change the following default values if necessary:
   - **Fingerprint Quality** by selecting Standard, High or Very High (Default and recommended option = Standard), 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.



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.

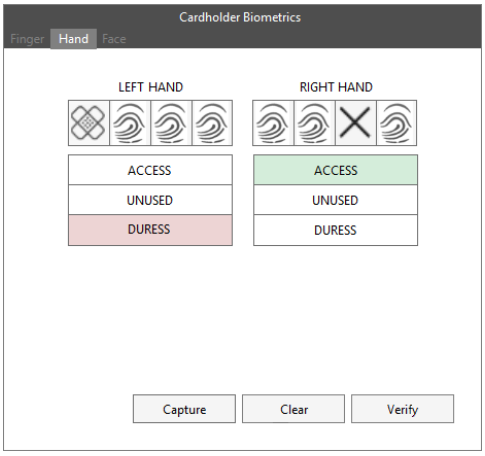
   Notes:

   - 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.

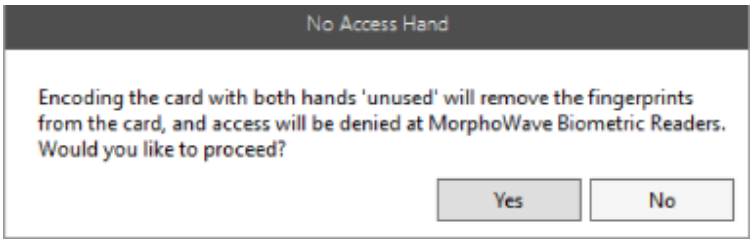
10. Click the **Accept** button.
    The MorphoWave Fingerprint Enrolment screen closes, and the **Hand** tab of the Cardholder Biometrics Tile now shows enrolled fingerprints.



Notes:

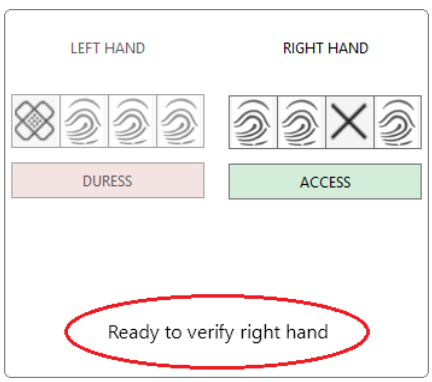
- The MorphoWave DESFire object will not encode "UNUSED" and "DURESS" fingerprints to a card. Only "ACCESS" fingerprints will encode to cardholder's card.
- Once fingerprints are enrolled and saved (to either database and card, or database only), any changes to the fingerprints status will result in 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."*

  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.

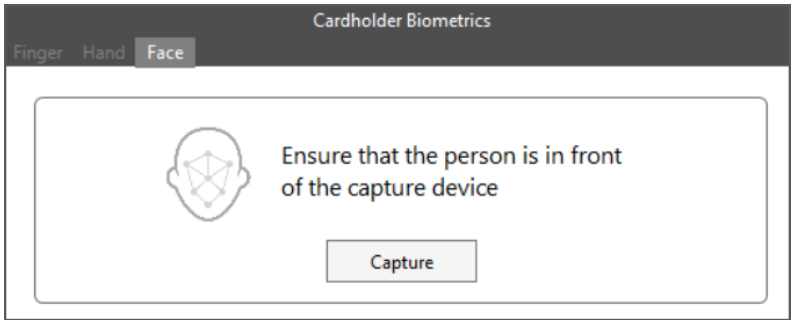
14. Wave the other hand over the enrolment reader.
    A message displays indicating that hand was also successfully verified.
15. Click the **Close** button.

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.

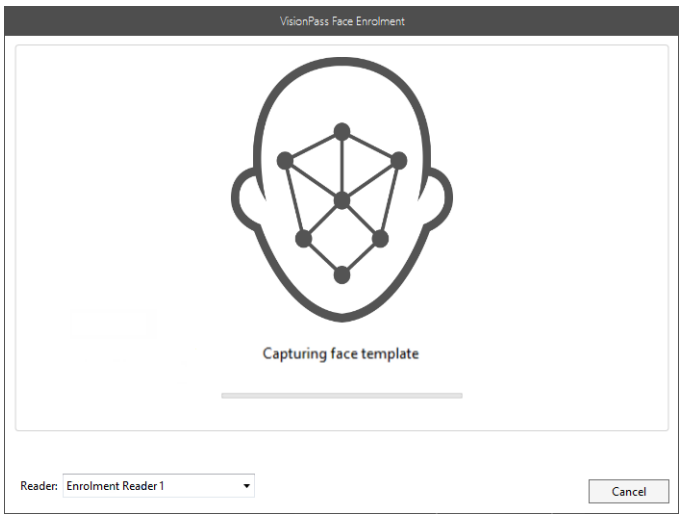
The following procedure describes how to enrol a Cardholder's face using a VisionPass Reader:

1. Click the **Face** tab.

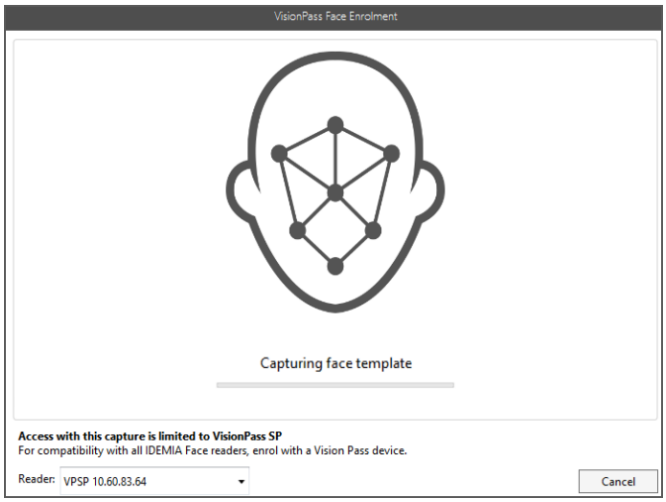


2. Click the **Capture** button.
   The VisionPass Face Enrolment screen displays.

   *Enrolment with **VisionPass** device:*



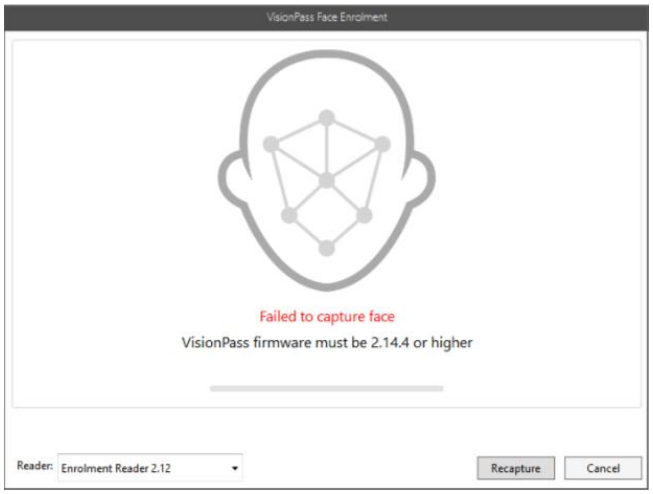
*Enrolment with **VisionPass SP** device:*



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.

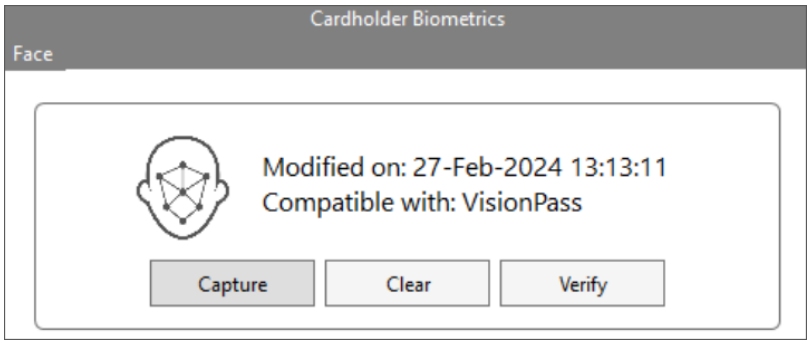
   When the capture process is completed the cardholder picture displays briefly on the screen, so you can ensure the cardholder is the correct person.



   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

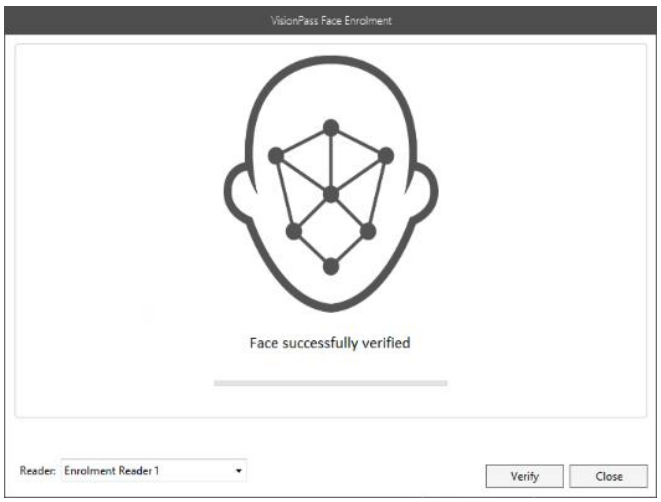
Recapture button can be clicked to restart the face capture process.

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



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.



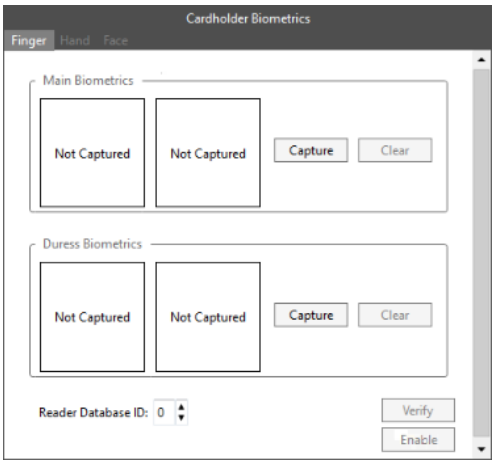
Note: If there is more than one enrolment reader available, a dialog will display. Select the correct reader from the list and click the **OK** button, and then the **Verify** button.

8. Click the **Close** button.

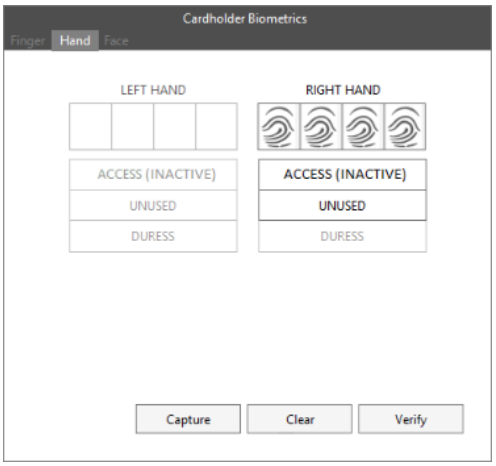
Re-enabling Inactive Biometrics

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

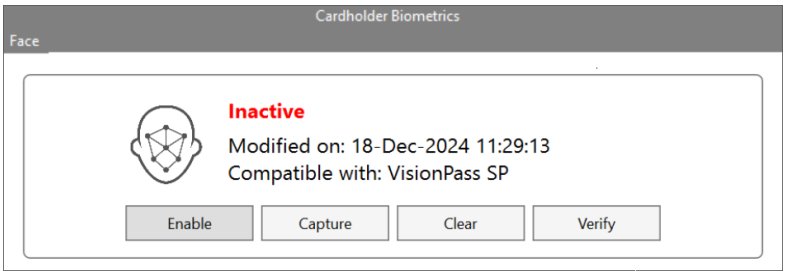
From the…	click the…
Finger tab,	**Enable** button.



Hand tab,	ACCESS (INACTIVE) button.



Face tab,	**Enable** button.



Communications Encryption

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

- Gallagher Command Centre vEL7.80 (via the network)
  (see ***Encryption using Command Centre*** on page 73-57), or
- Biometric Encryption Utility (a non-network solution)
  (see ***Encryption using the Biometric Encryption Utility*** on page 73-58)

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.

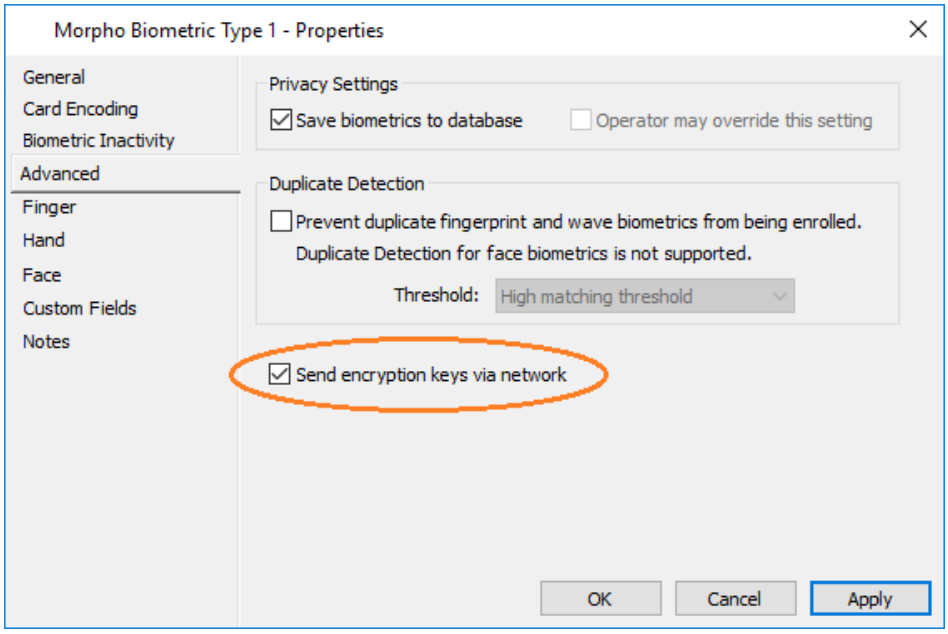
- ***Encryption using Command Centre*** (on page 73-57)
- ***Encryption using the Biometric Encryption Utility*** (on page 73-58)
- ***Known Issue*** (on page 73-60)
- ***Unencryption*** (on page 73-61)

Encryption using Command Centre

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

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".

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.

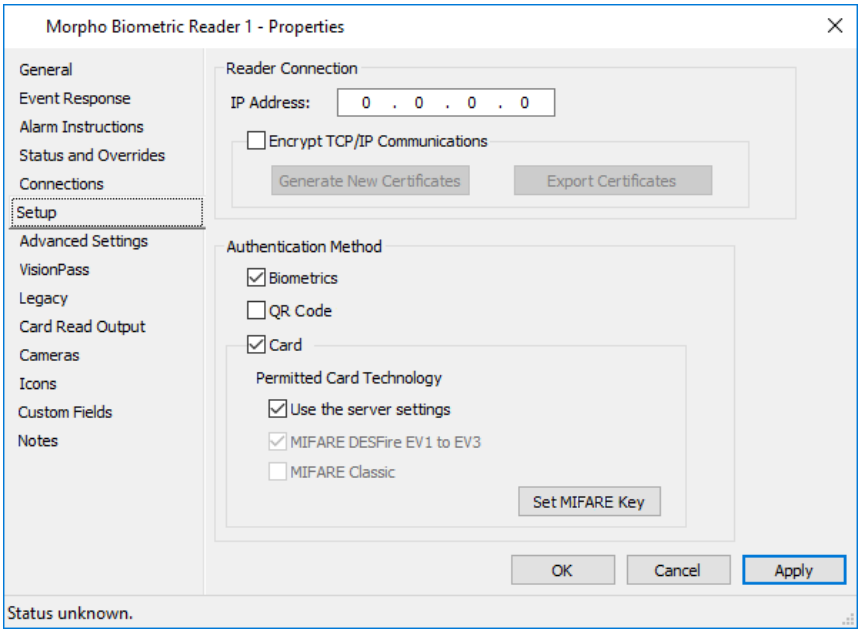
Prerequisites

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 ***Installing Microsoft Redistributables*** (on page 73-4) for the procedure.

Procedure

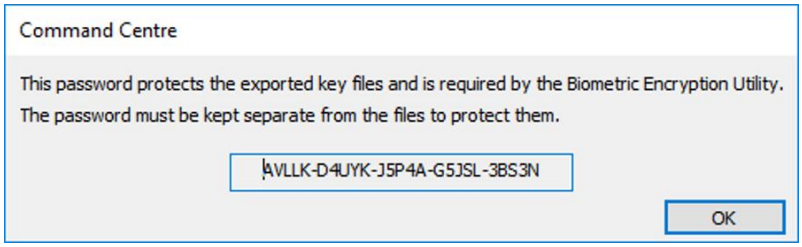
1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**. The Hardware List Window opens.
2. Highlight the Morpho Biometric Reader you want to encrypt communications for.
3. **Right-click** and select **Properties**.
4. Click the **Setup** tab.



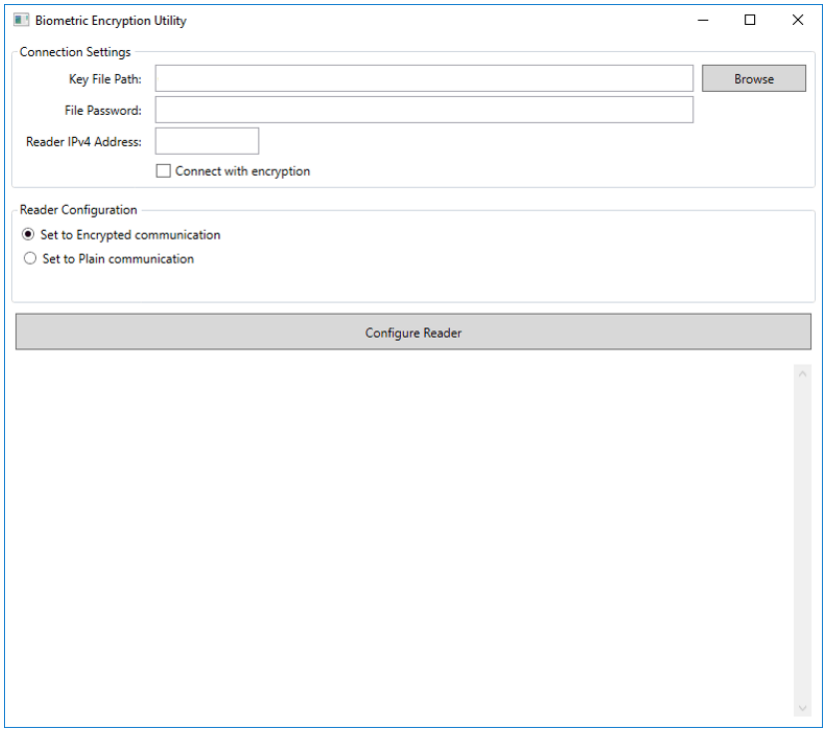
5. Tick the **Encrypt TCP/IP Communications** checkbox.
   Note: This option is OFF (disabled) by default.

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.
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.

Known Issue

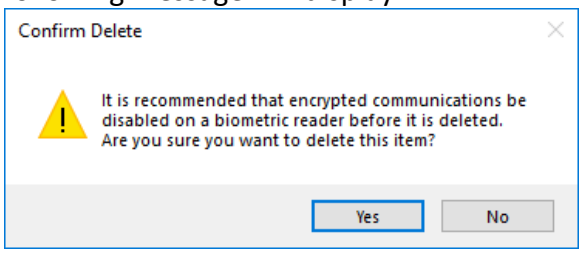
Cycling the certificates for the reader while in secure mode results in Tamper Alarms and the Reader goes offline.
Workaround: Change the reader to "Plain Communication" and then back to "Secure Communication", and the Reader will come online and the alarms will cease.

Unencryption

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

- ***Unencryption from the Server*** (next)
- ***Unencryption using the Biometric Encryption Utility*** (on page 73-62)

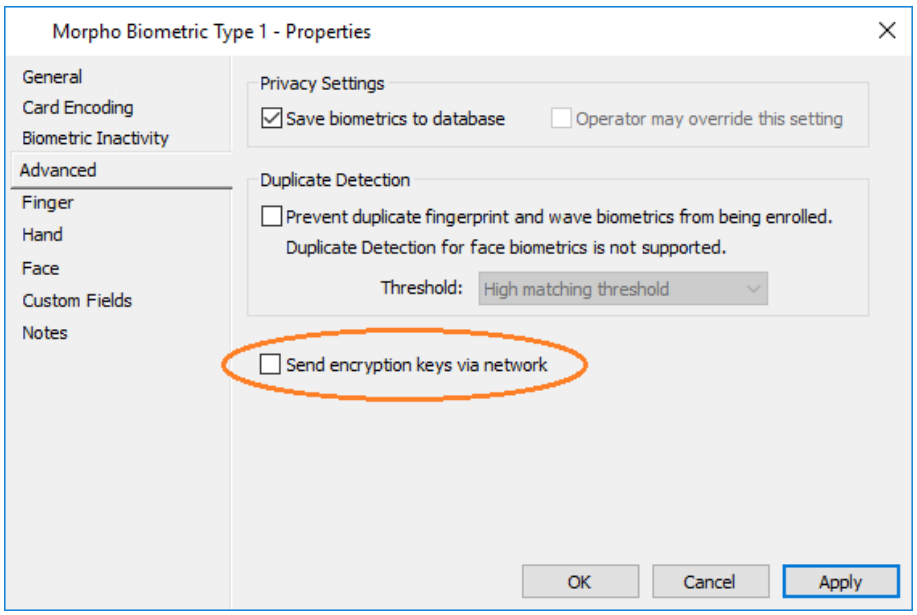
Note: If you try to delete a biometric reader without unencrypting it first, the following message will display.



Unencryption from the Server

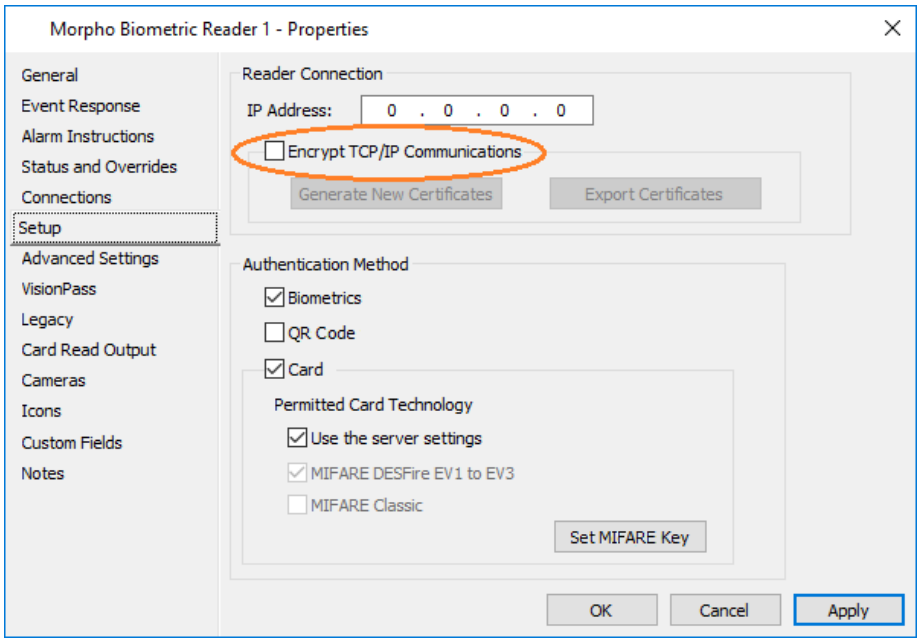
Perform the following procedure to unencrypt a reader from the Command Centre server:

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Card Types**. The **Card Types** 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.

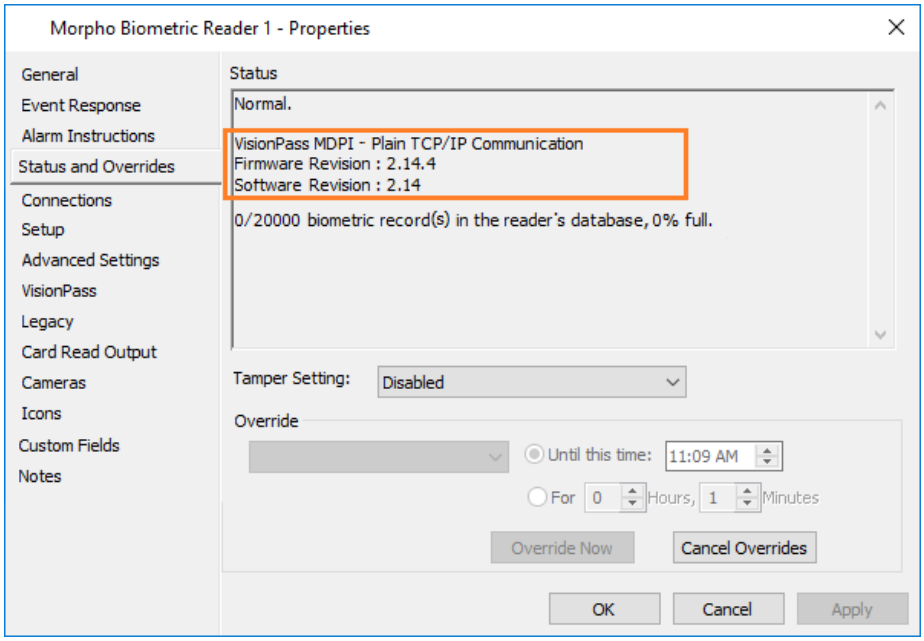


4. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
5. **Right-click** on the Morpho Biometric Reader you want to unencrypt communications for, and select **Properties**.

6. Click the **Setup** tab and uncheck the **Encrypt TCP/IP Communications** checkbox, then click **Apply**.



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

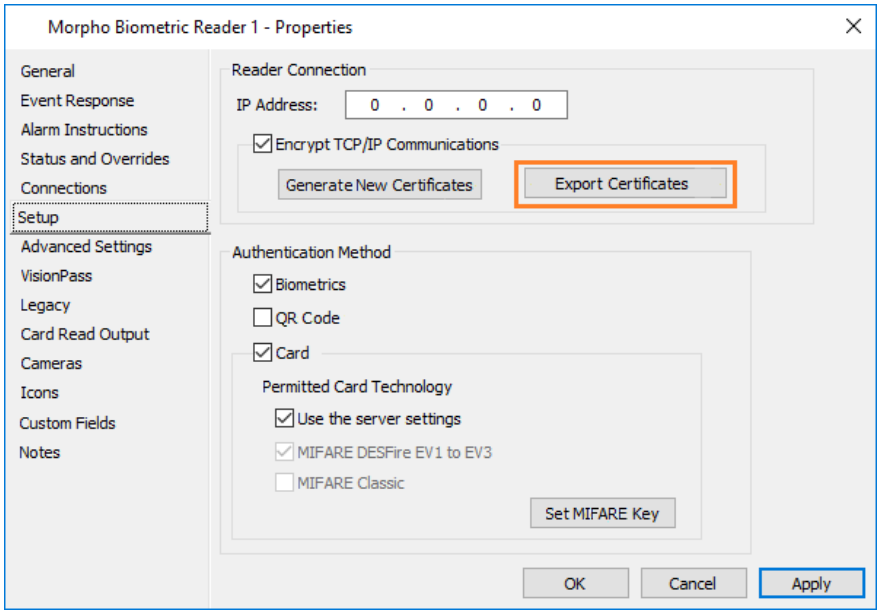


Unencryption using the Biometric Encryption Utility

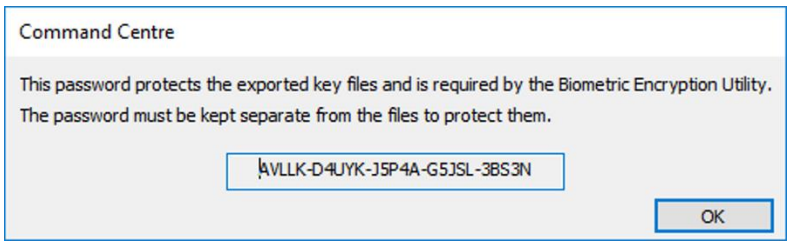
Perform the following procedure to unencrypt a reader:

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.

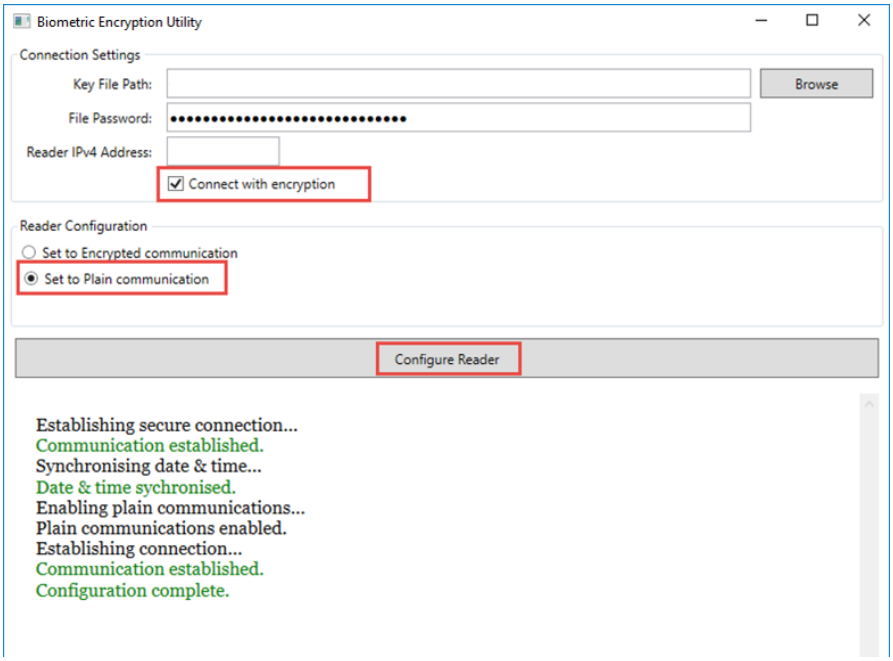


5. Click the **Export Certificates** button to export existing certificates.|
   Note: Export Certificate requires "Manage Keys" operator privilege to work.
6. From the displayed **Browse for Folder** dialog, path your way to the directory to export the reader's certificate/key file to, and click the **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.



The reader will update and reboot after configuration is complete.

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.

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 chapter, or in other sections in this user guide).

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 ***Creating a new Morpho Biometric Card Type*** (on page 73-26) 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: The valid range for Gallagher is 31 - 8,388,607, and for Morpho it is 8,388,608 - 16,777,215.

   Refer to ***Setting up Card Types*** (on page 7-2) for the 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:
   - ***Designing Card Layouts*** (on page 47-13) 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*** (on page 47-28),
     - ***Adding a Morpho DESFire object*** (on page 47-29),
     - ***Adding a MorphoWave DESFire object*** (on page 47-30),
     - ***Adding a Morpho FVP DESFire or Morpho VisionPass DESFire object*** (on page 47-31), and
     - ***Adding a Morpho FVP MIFARE Classic object*** (on page 47-32)

4. Assign the Card Type to a cardholder.
   Refer to ***Adding a Card to a Cardholder*** (on page 32-9) 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*** (on page 47-58) 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.

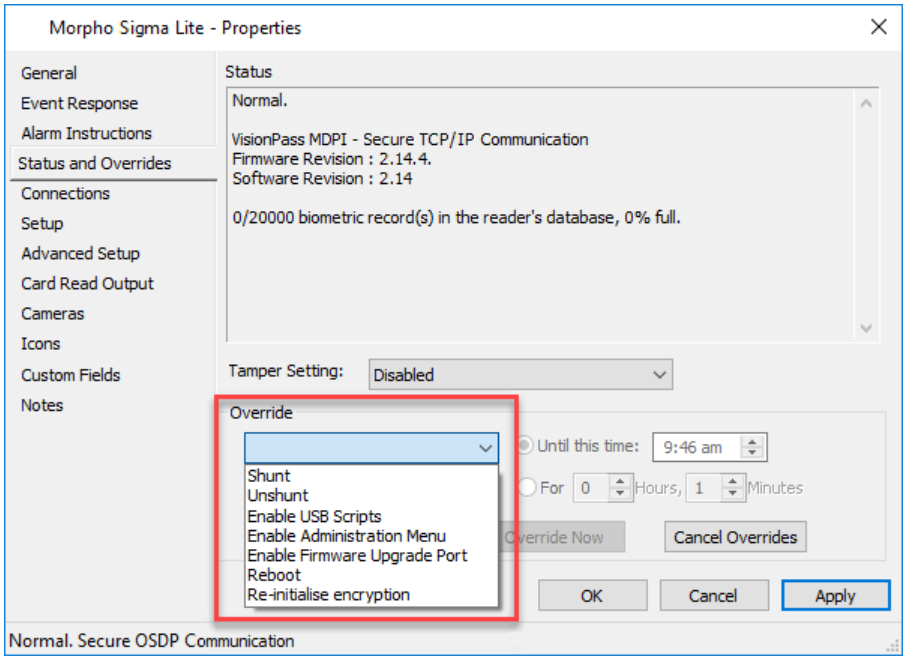
Performing Overrides on a Morpho Biometric Reader

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.

Option	Allows users to access the...
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 ***Overrides on Morpho OSDP Readers*** (on page 73-76) for further detail on these overrides.

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.

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 1.2.7
- MorphoWave XP / XP2, VisionPass and VisionPass SP readers all support OSDP by default

This section covers the following:

- ***Wiring Morpho Readers for OSDP*** (on page 73-72)
- ***Configuring the Controller RS-485 Bus for OSDP*** (on page 73-73)
- ***Overrides on Morpho OSDP Readers*** (on page 73-76)
- ***Morpho OSDP Reader Display Messages*** (on page 73-78)

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 (16 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)	-

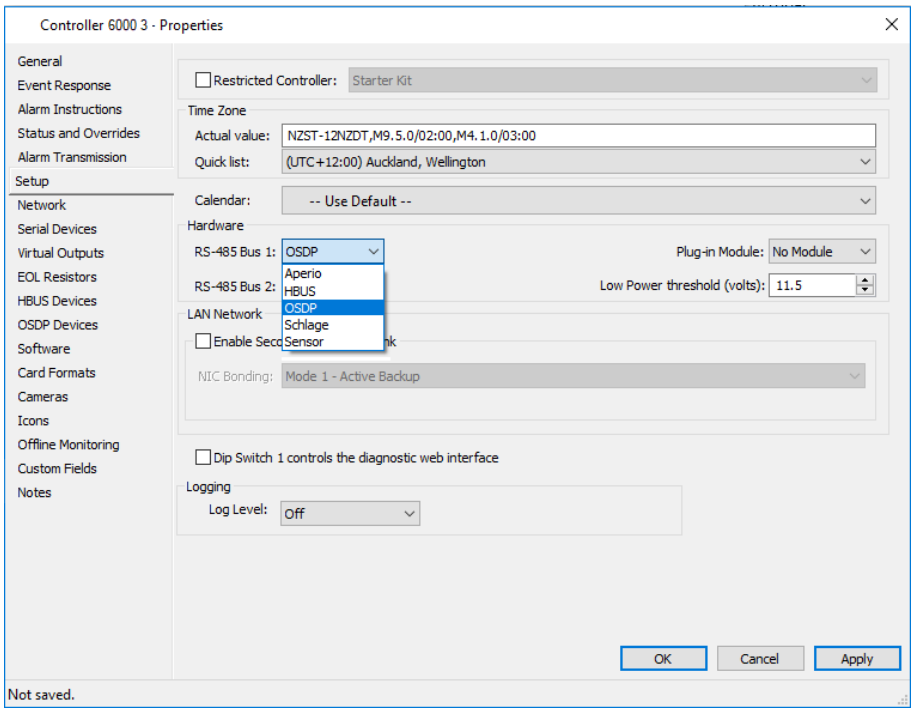
Configuring the Controller RS-485 Bus for OSDP

Introduction

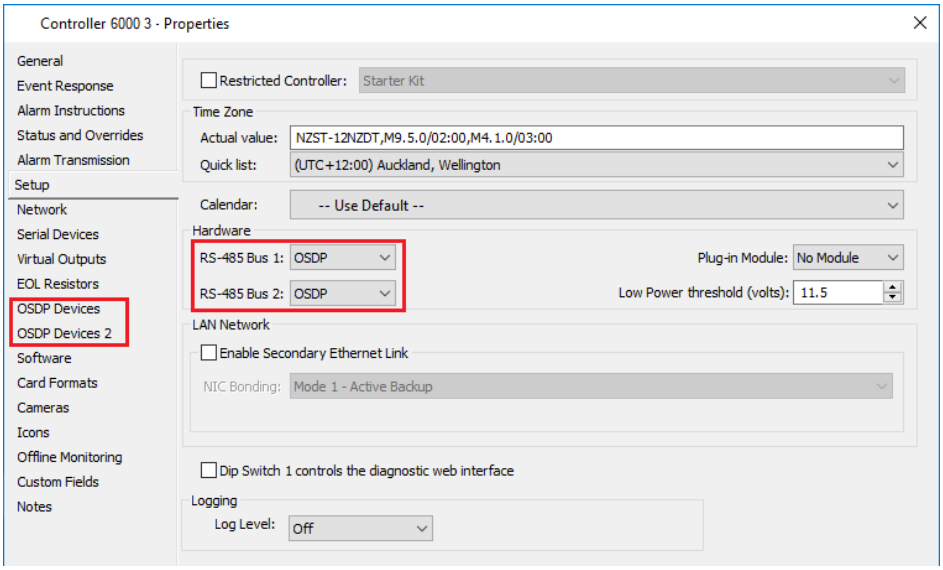
This topic describes how to configure the Controller RS-485 Bus for Open Supervised Device Protocol (OSDP) and assign the Morpho reader to the Controller.

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.



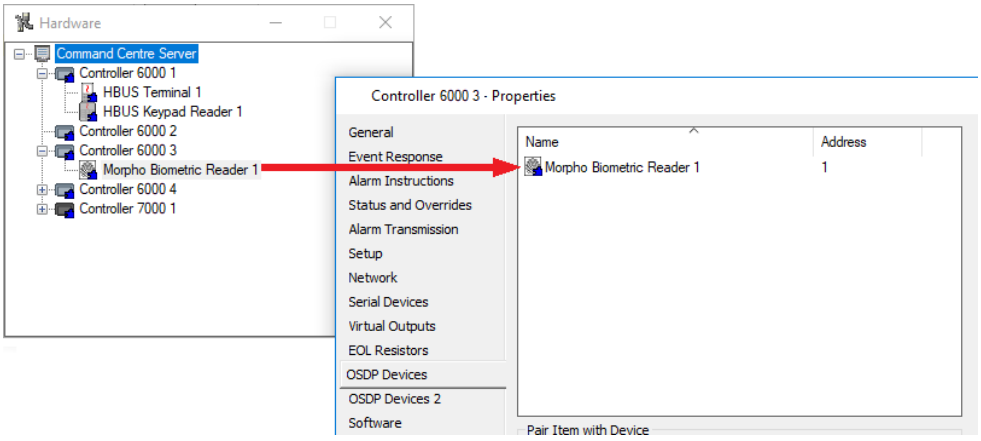
5. In the Hardware section of this screen, select the 'OSDP' option form the **RS-485 Bus 1** and/or **RS-485 Bus 2** drop-down lists as appropriate. Depending on which RS-485 Bus option(s) you selected 'OSDP' for, an **OSDP Devices** and/or **OSDP Devices 2** tab appears, allowing you to add up to 16 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 16 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.

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:

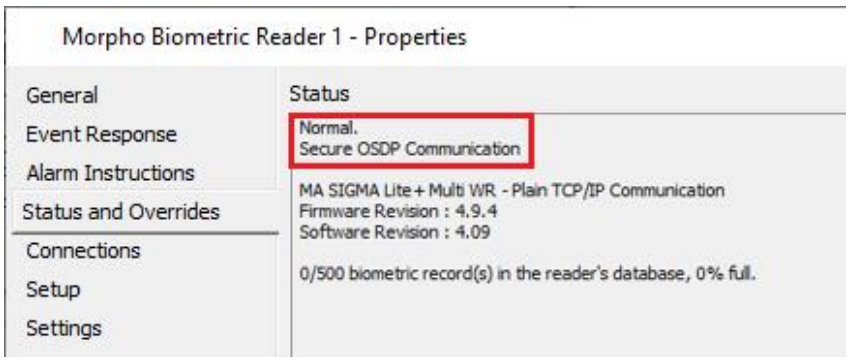
- Each Morpho reader that is added receives a unique address (Address Range = 0 - 126). The **Configured Address** automatically increases.
- If readers don't have a unique **Configured Address** and you click **Apply**, the following error message displays:
  "Device addresses on the same bus must be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



Overrides on Morpho OSDP Readers

Introduction

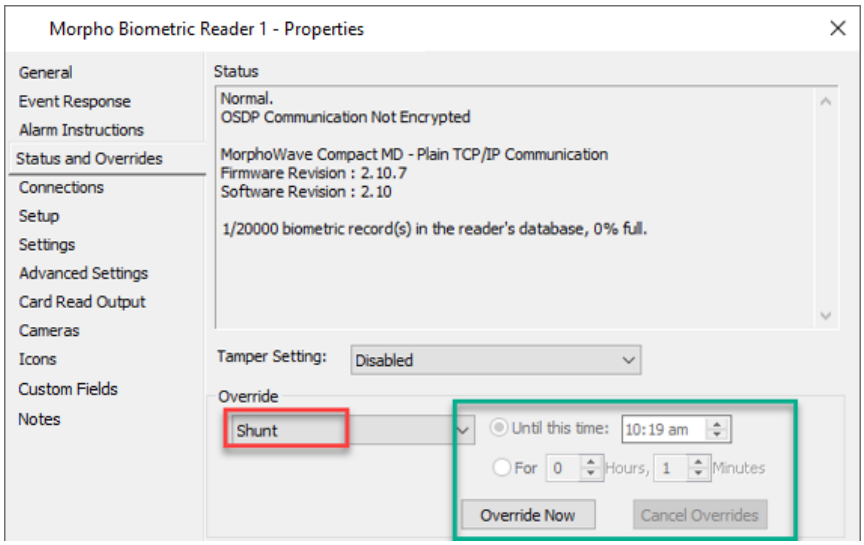
This topic describes how to perform overrides on a Morpho Reader added to an OSDP connection.

Configuration

Shunt and Unshunt overrides

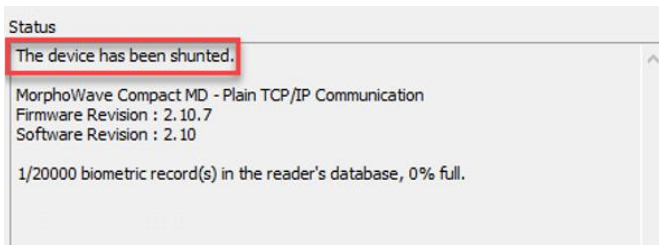
Shunt overrides stop communication to the reader, and all inputs and outputs on that reader will no longer be available by the system. It will remain that way until you perform an "Unshunt" override.
Note: Shunt and unshunt overrides only display for Morpho readers that have been added to an OSDP connection.

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.
   The **Status and Overrides** tab of the Morpho Reader properties displays.
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.



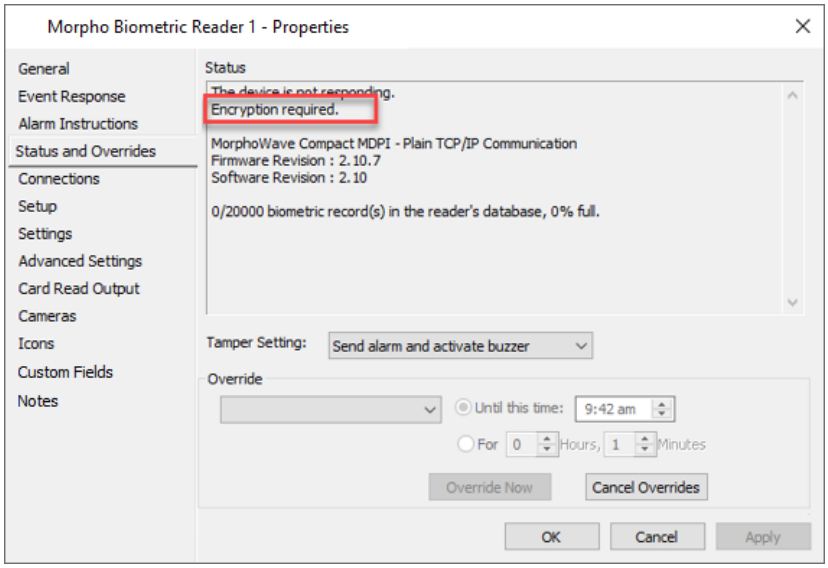
5. Click the **OK** button.

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 the 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.

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

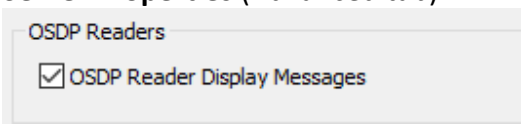
Below are the various configurations available and screenshots as examples of what will display on the Morpho reader screen for that particular configuration. **Notes:**

- 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).

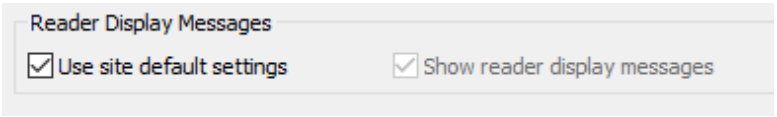
OSDP Reader Display Messages ENABLED

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)

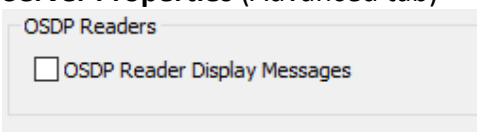




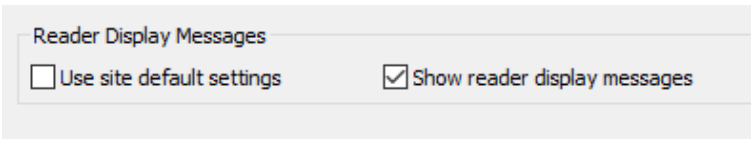


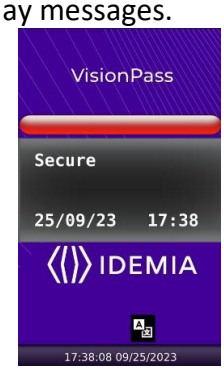
Server Settings NOT enabled; Device Show reader messages ENABLED
This means that this specific reader WILL display messages.

Server Properties (Advanced tab)



Reader properties (Settings tab)







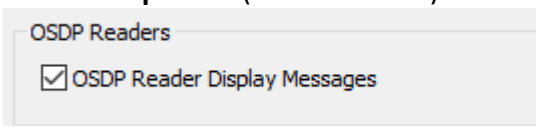
OSDP Reader Display Messages NOT enabled

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

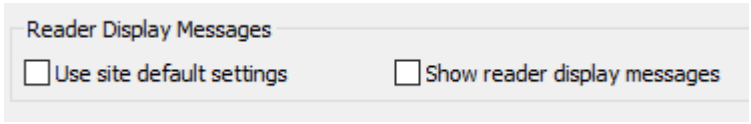
Server Settings ENABLED; Device setting NOT enabled

This means that the readers will NOT display messages (because the READER "Use site default settings" is NOT enabled).

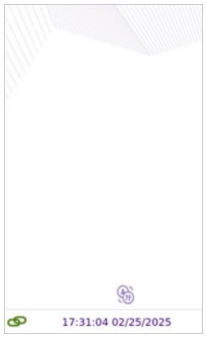
Server Properties (Advanced tab)



Reader properties (Settings tab)





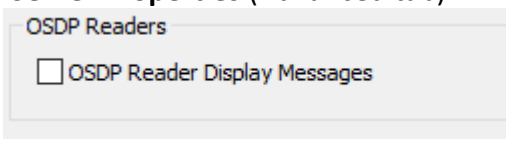


Server Settings NOT enabled; Device setting ENABLED

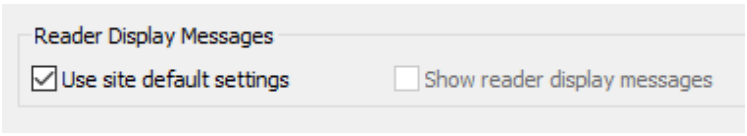
This means that the reader will NOT display messages (because the "Use site default settings" is enabled, and Morpho "OSDP Reader Display Messages" is NOT enabled).

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

Server Properties (Advanced tab)



Reader properties (Settings tab)



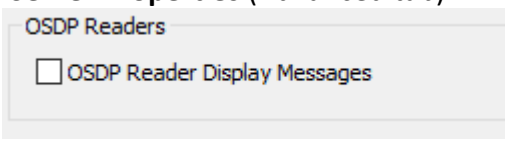




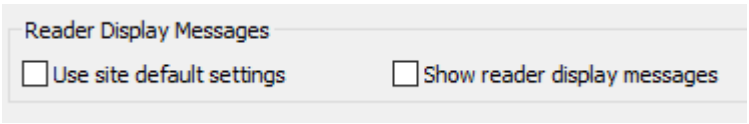
Server Settings NOT enabled; Device setting NOT enabled

This means that the reader will NOT display messages.

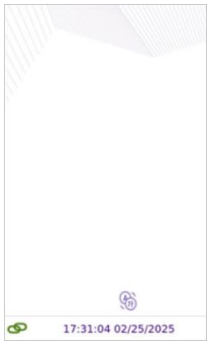
Server Properties (Advanced tab)



Reader properties (Settings tab)



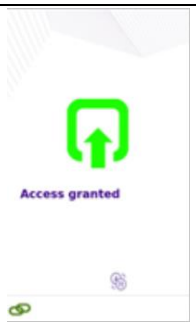
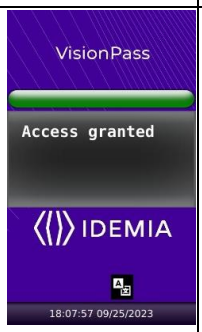
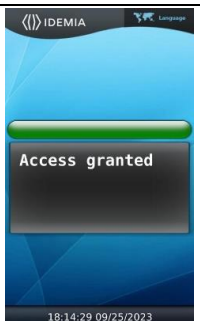
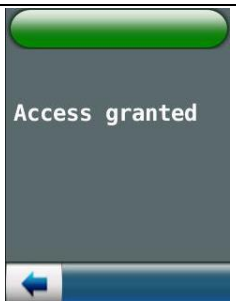
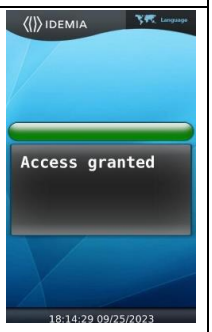
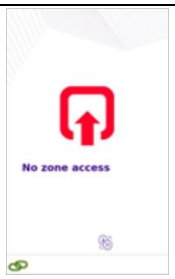
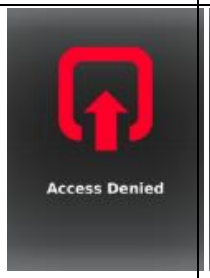
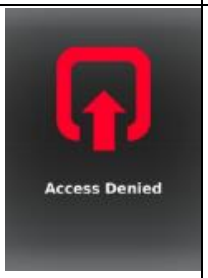
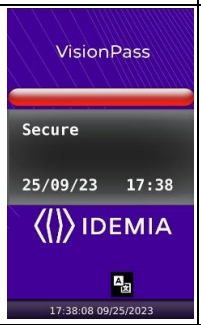
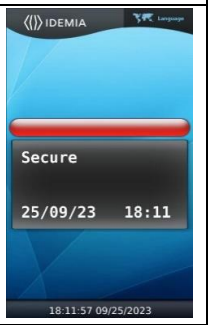
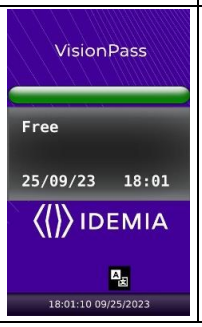
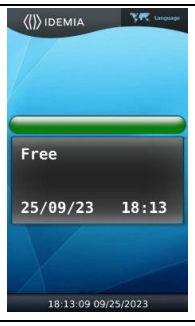
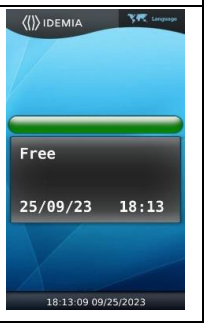


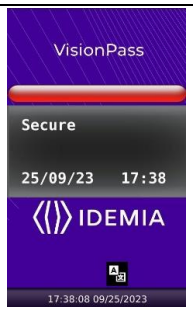
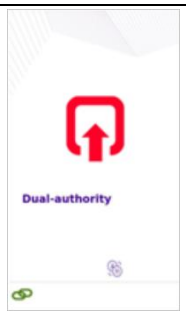
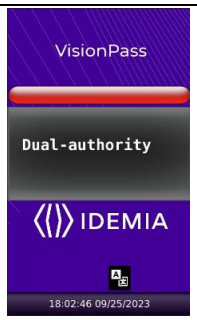
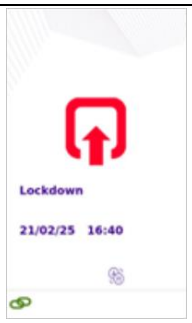
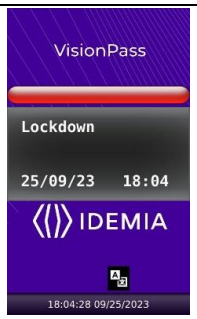


Morpho OSDP Reader status messages

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					

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

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



QR Code authentication mode at Morpho Readers

Introduction

The 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:

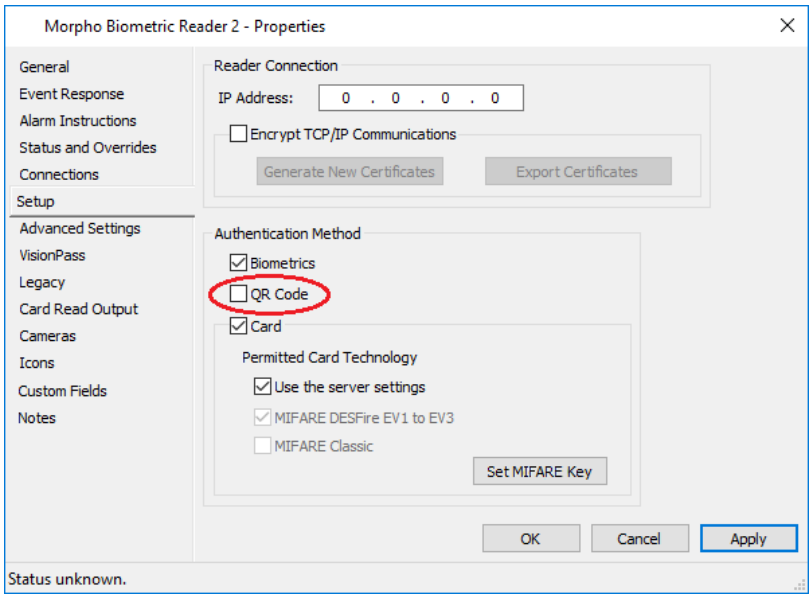
- Configuration of QR codes in Command Centre Configuration Client
  - Setting QR Code as Authentication Mode
  - Creating a card type with "New QR Code Access Token Object"
  - Configuring the Card Type
- QR Code specification recommendations
- Using QR code for access

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 verison 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.



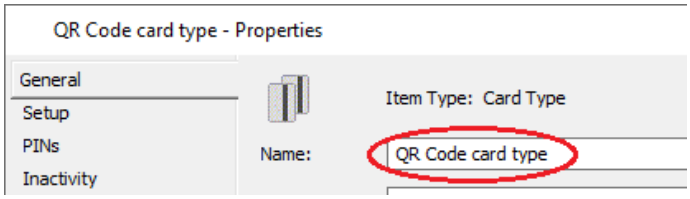
4. Tick the **QR Code** checkbox.
5. Click **OK** to exit the reader properties and save your changes.
   A warning message displays advising that QR Code is not a secure method.



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

Creating a Card Type

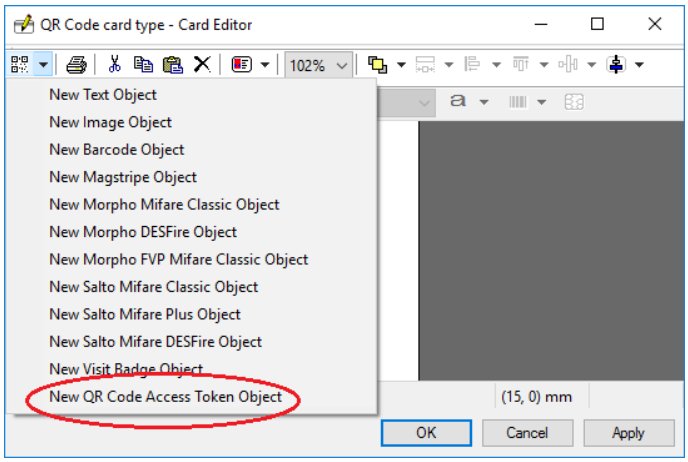
7. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
8. **Right click** and select **New...Card Type**.
   By default the **General** tab displays.
9. Enter an appropriate **Name** for this card type, (e.g. QR Code card type).



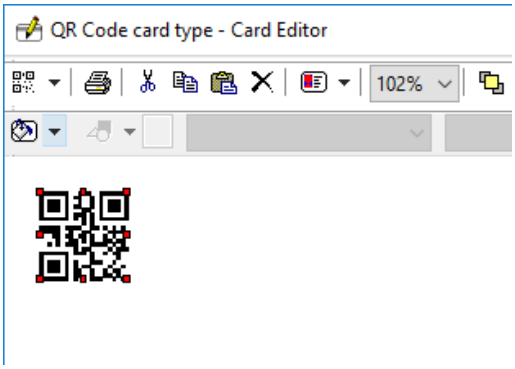
10. Click the **Setup** tab, and enter the correct **Facility Code**.
    Note: It is strongly recommended that you use a different Facility Code from the server, and create a separate QR User Group to avoid security vulnerabilities.
11. Click **OK** to save this card type.

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.



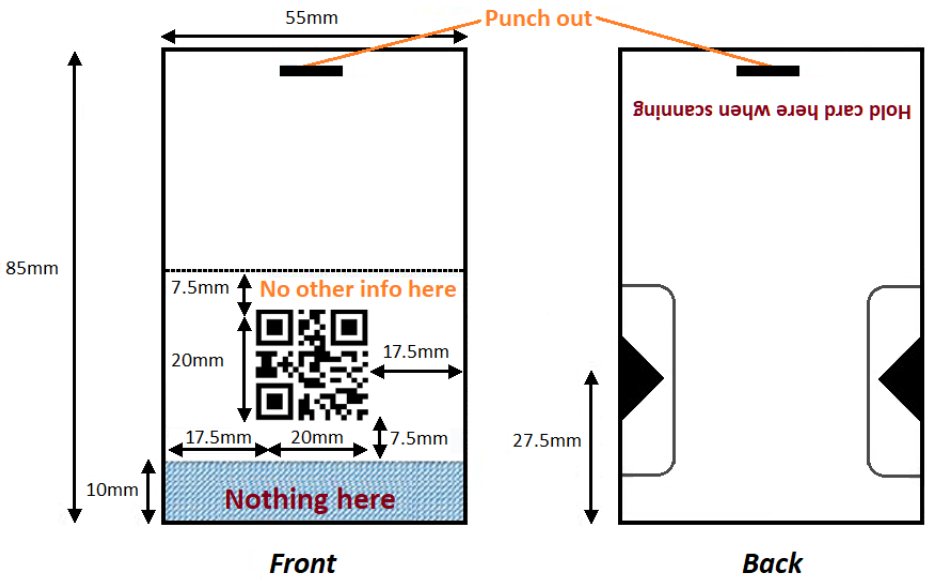
A QR Code image displays with placeholders around it.



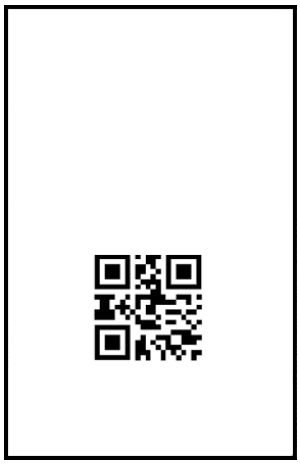
14. Click the **OK** button.
    The Card Editor window closes.
15. Assign the new QR Code card type to the cardholders.
    See ***Adding a Card to a Cardholder*** (on page 32-9) for the procedure.

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.

Troubleshooting - Morpho Biometrics

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 ***MA Sigma, MorphoWave and VisionPass Wiring*** (on page 73-18*)* for wiring instructions, or • refer to ***Configuring Morpho Readers using MBTA application*** (on page 73-9) 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 ***MA Sigma, MorphoWave and VisionPass Wiring*** (on page 73-18*)* for wiring instructions.
Reader generates *"Re-sync Access Failed*" or *"Updating the configuration failed"* alarm, and shows "The reader has rejected some configuration and a firm-ware update may be requir-ed to ensure correct terminal behaviour" in the status	Wrong firmware on reader	Upgrade reader firmware. Refer to ***Upgrading the MorphoAccess Reader Firmware*** (on page 73-16).
	MIFARE Classic and DESFire keys are not initiated	Initialise the keys under Morpho Biometric Type > Card Encoding.

Problem	Possible Cause(s)	Solution
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 techno-logies 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.
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.

Chapter 74: Salto Lock Interface

Introduction

Command Centre supports Salto ProAccess SPACE 6.10.4.3. Command Centre no longer supports Salto HAMS For Service v12.2.2.205.

The Salto Lock Interface provides an interface between Command Centre and the Salto ProAccess SPACE 6.10.4.3 software.

Salto are world leaders in non-wired door locking mechanisms and Gallagher provides a seamless integration to Salto Proximity MIFARE Classic, MIFARE Plus SL3 and DESFire EV1 to EV3 readers. Salto BLE readers can be accessed through Gallagher Mobile Connect.

The Gallagher Salto integration provides a single user interface for cardholder enrolment, card encoding and management of cardholder access, allowing a single card to be used for access at both Gallagher and Salto readers on site.

The Salto system incorporates online wired, online wireless, non-wired offline and wireless doors. Wired online door readers/wireless online door readers write access changes received from Command Centre to a Cardholder's card which is then used to gain access at non-wired offline and wireless doors.

Non-wired offline and wireless doors are connected to the Salto Virtual Network (SVN) for continuous event monitoring.

Salto Native Mode facilitates secure communication between the Gallagher Command Centre and Salto Space, enhancing user functionality and improving the overall customer experience. Customers benefit from additional features, such as access during lockdown. **Key benefits of upgrading to the SALTO Native Interface include:**

- End-to-end encryption between the Gallagher Command Centre and SALTO Space.
- Enhanced user experience with additional features.

Upgrade steps for existing sites are found in section ***6. Salto Server Connection*** (on page 74-24).

The Salto Space installation instructions below have been updated for Native Mode since vEL9.30. **If Legacy Mode Salto Space installation instructions are required, please see older installation documents.**

Licensing

The Salto Lock Interface integration is a licensed feature of the Gallagher Command Centre, and therefore the following license is required:

- 2A8953 - SALTO Integration License. Required for each SALTO Control Unit /Escutcheon/i-Locker/Energy Saving Device integrated with Command Centre.

Note: If the SALTO Control Unit/Escutcheon/i-Locker/Energy Saving Device is not purchased through Gallagher please order 2A8996.

Functionality

The Salto Lock Interface provides the following functionality:

- Sharing of Cardholder, card, door and access-related data between the Command Centre and Salto systems such that installers are not required

to dual configure the same item within each system and changes in either system are communicated between the systems.

- The ability for a Cardholder to use a single card to access a Command Centre door or a Salto door.
- Encoding of the card used for accessing a Command Centre door or a Salto door to be managed solely from Command Centre, (i.e. preventing any need for dual encoding of cards separately from within each system).
- Allowing a Cardholder's access to a Salto door to be assigned or restricted from within Command Centre.
- Events from a Salto door, (e.g. Cardholder access events or low battery warnings) are transferred to and stored in the Command Centre event log. These events are configurable from Command Centre as an event only or as an alarm that is visible in the Alarm Viewer. Non-wired offline and wireless doors report events at the time a Cardholder's card is presented at an update point (wired online door).
- Using Salto's CUADAP functionality which allows a Salto Control Unit to pass Wiegand data to a third-party system.
  Note: All cards that use this feature need to be re-encoded, so the Wiegand data gets added to the cards.
- A Salto Output number can be assigned to an Access Zone in Command Centre. When a Cardholder's card is encoded with Salto data by Command Centre, the Salto Output numbers for any Access Zones the Cardholder is required to access are added to the card. When a Cardholder presents their card at a Salto wired reader located within a lift, the Salto Outputs for which the Cardholder has access will be activated, thus enabling the Cardholder to access one or more floors.
- Salto Door and Zone status can be viewed in Command Centre.
  Note: Salto Zones are merely groups of doors and hence there is no need to show them as offline.
- The following Salto online door overrides can be performed from Command Centre: Open Door, Emergency Closing, Emergency Opening and End of Emergency Opening. If required, a Command Centre operator can configure a Macro to perform an override for all doors on site (both Salto online and Command Centre doors).
- Online wireless battery monitoring. Battery low alarm raised at 20% battery level. Battery critical alarm raised at 10% battery level.
- Online ESD monitoring with window open sensor and event monitoring.
- Card update via online wireless readers reduces the need for wired update points.

Select the item below that you require further detail on:

Space Compatibility (on page 74-3)

Space Installation Instructions (on page 74-5)

Space Site Configuration (on page 74-31)

Command Centre Site Configuration (on page 74-71)

Troubleshooting - Salto Lock Interface (on page 74-112)

Salto to Command Centre Event Mapping (on page 74-113)

Space Compatibility

The Salto Space Lock Interface has been tested using:

- Command Centre (Windows Server 2019 64-bit using Microsoft Internet Explorer 11 and Microsoft Silverlight) with Microsoft SQL Server 2019, and
- Salto ProAccess SPACE 6.10.4.3 (on Windows Server 2019 64-bit) with Microsoft SQL Server 2019.

The Salto Space Lock Interface has been tested using the following card technologies:

- Salto encoded Guest cards: MIFARE Ultralight C and MIFARE Classic cards.
- Gallagher encoded Staff cards: MIFARE Classic, MIFARE Plus Security Level 3 (SL3), and MIFARE DESFire EV1 to EV3 cards. MIFARE Plus X and S card types are supported.

The Salto Space Lock Interface has been tested using the following Salto hardware:

- Salto Wireless Gateway 2, part number GATEWAYW2C with mini node
- Salto Node, part number RFNODE
- Salto Expansion Relay Board, part number EB5008
- Salto Control Unit CU42E0
- Salto Control Unit CU4200
- Salto Relay Board CU4EB8
- Salto UBOX4000
- Salto Wired Reader WRDB0E0
- Salto Wired Reader with keypad WRDB0E0K
- Salto XS4 BLE Escutcheon AB650 (offline)
- Salto AElement RF2 Wireless Reader with Privacy
- Salto XS4 BLE RF2 Wireless Escutcheon with Privacy
- Salto Escutcheon E9450U00IM38-03
- Salto XS4 Locker Lock (offline)
- Salto E450 RF3 Escutcheon
- Salto ESDs ESD92UC (offline) and ESD92UIC (online)
- Salto Control Unit (CU5000) - firmware version 01.52, 2.21 and 5.03
- Salto Portable Programming Device PPD firmware version 02.18
- Salto RF3 Gateway, part number GATEWAYW3CAU with RF3 mini node

- Salto AElement Fusion
- Salto Neo Cylinder (RF3 BLE)
- Salto RF3 Repeater, part number REPEATER03AU

Considerations

- Salto ProAccess SPACE 6.10.4.3 supports Salto RF2 and RF3 modes only. Salto RF mode 1 devices are not supported and will need to be replaced.
- Command Centre polls the Salto application every 10 seconds, this means a delay of up to 20 seconds may occur (allowing for network latency) before an event generated at a Salto online wireless reader is displayed in Command Centre.
- If a Salto device is disconnected from the network, the device and the wireless doors connected will go offline. No offline event is reported in the Salto audit trail, hence the corresponding Command Centre Salto doors continue to display as online. In this scenario, the events are stored on the Salto lock. The Salto events will be transferred to the Salto server when wireless connectivity is restored.

Space Installation Instructions

Introduction

The process for installing Salto ProAccess SPACE v6.10.4.3 is split into the following procedures:

1. Installing Microsoft SQL Server for use with the Salto application (below)

2. Register Salto ProAccess SPACE (on page 74-10)

3. Install Salto ProAccess SPACE (on page 74-12) *****

4. Install Salto Local IO Bridge (on page 74-19) *****

5. Checking the Salto ProAccess SPACE Configuration (on page 74-20)

6. Salto Server Connection (on page 74-24) *****

*** IMPORTANT:** If you are **upgrading** Salto from a previous version, (e.g. ProAccess SPACE v5.7.3.2), only ***3***, ***4*** and ***6*** need to be performed.

Before you begin

- Salto ProAccess SPACE 6.10.4.3 requires Dot Net v4.6 to be installed as part of its installation pack.
- The installation must be performed by a Windows operator with admin rights.
- Prior to installing Salto ProAccess SPACE v6.10.4.3, a new SQL Instance must be installed. This needs to be a separate Instance of SQL from Command Centre, and must be installed prior to starting the Salto application. The Salto application can be run on the same PC as the Command Centre server or on a separate networked PC. When installed on a separate PC, care should be taken to avoid network delays which could affect access to Salto doors.

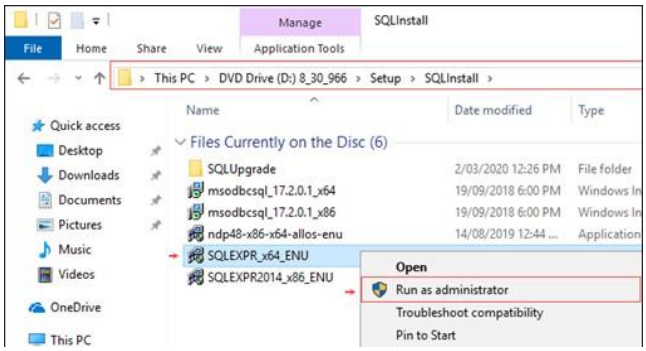
Important:

- The Salto ProAccess SPACE v6.10.4.3 application supports Microsoft SQL Server 2017, 2019 and 2022.
- The Salto application and Command Centre are supported on Windows 10, Windows 11 (64-bit versions only), Windows Server 2016, 2019 and 2022.

1. Installing Microsoft SQL Server for use with the Salto application

To install Microsoft SQL Server for use with the Salto application, perform the following procedure:

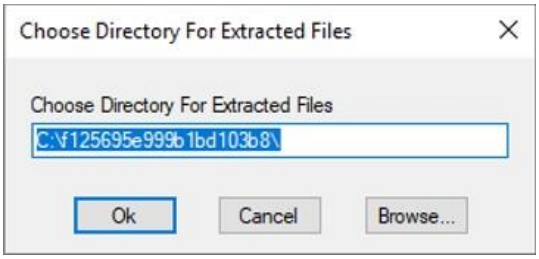
1. Open the Command Centre installation media and navigate to the SQL Express 2019 application setup files. Located in the `'vELx.xx.xxx\Setup\SQLInstall'` folder.
2. Run the **SQLEXPR_xxx_ENU.exe** (32-Bit) installer as administrator.
   - SQLEXPR_x86_ENU.exe for 32-Bit Windows operating systems
   - SQLEXPR_x64_ENU.exe for 64-Bit Windows operating systems



3. Does the following screen display?



If…	then…
no,	the 'SQL Server Installation Centre' application displays. Go to Step 4.
yes,	a) Click **Yes**. The Choose Directory For Extracted Files dialog box displays.

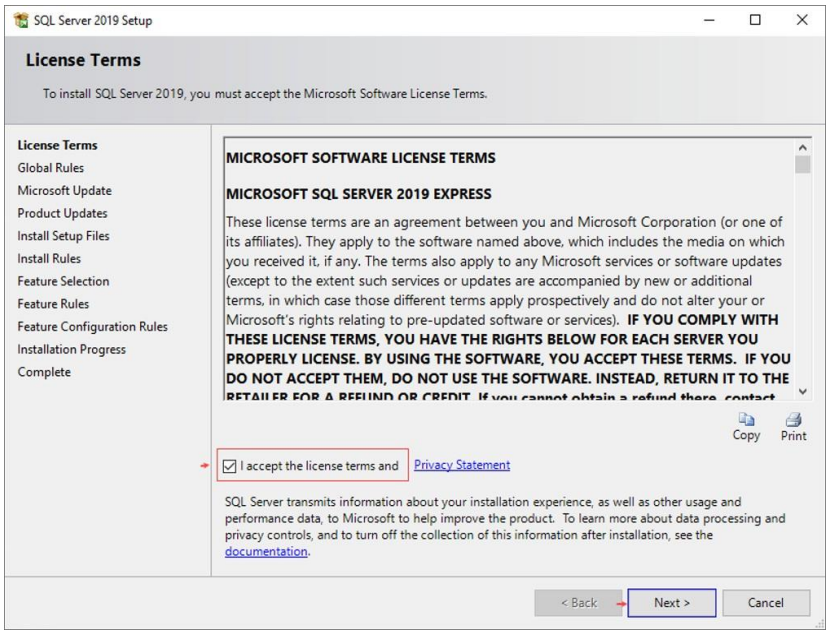


b) Choose a directory to extract files to and click **Ok**.
The Microsoft SQL Server 2019 Express file extraction starts.
Once complete, the 'SQL Server Installation Centre' application displays.

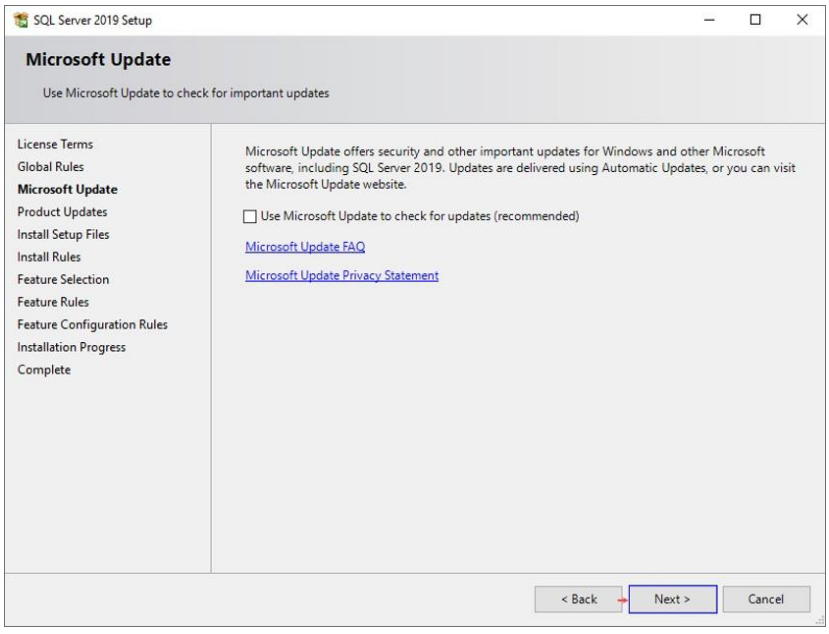
4. Click **Installation** on the left side of this screen, then click the **New installation or add features to an existing installation** option.



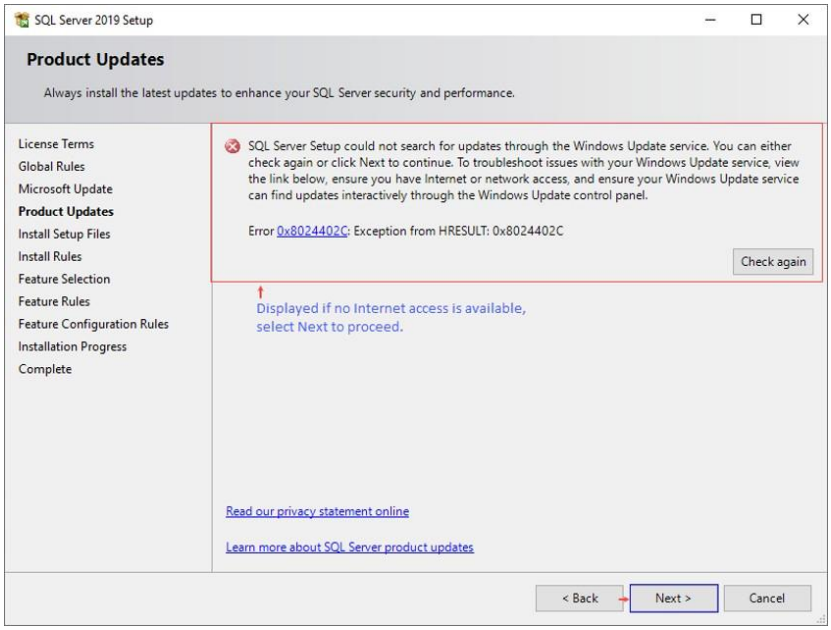
The 'Licence Terms' screen of the SQL Server 2019 Setup wizard displays.



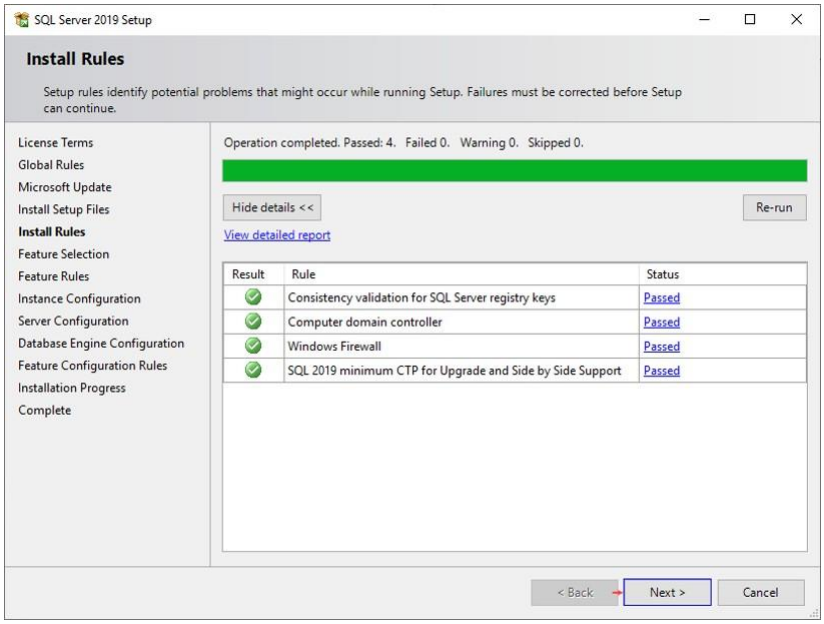
5. Ensure you fully understand the terms and conditions listed in the licensing agreement you are about to enter into, then tick the box to accept and click the **Next** button.
   The 'Microsoft Update' screen displays.



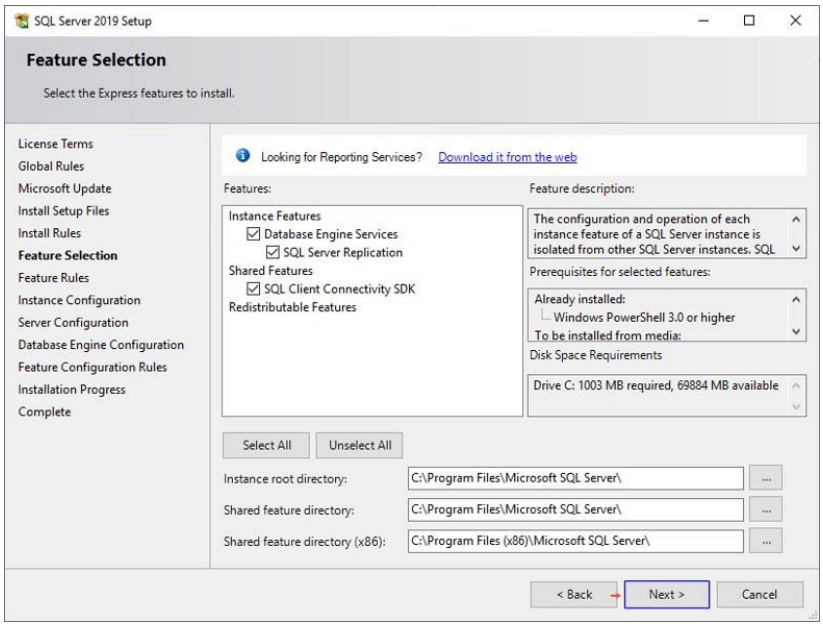
6. Choose whether you want to **Use Microsoft Update to check for updates**, by checking the checkbox or leave it unchecked if you do not. Click the **Next** button.
   The 'Product Updates' screen displays.



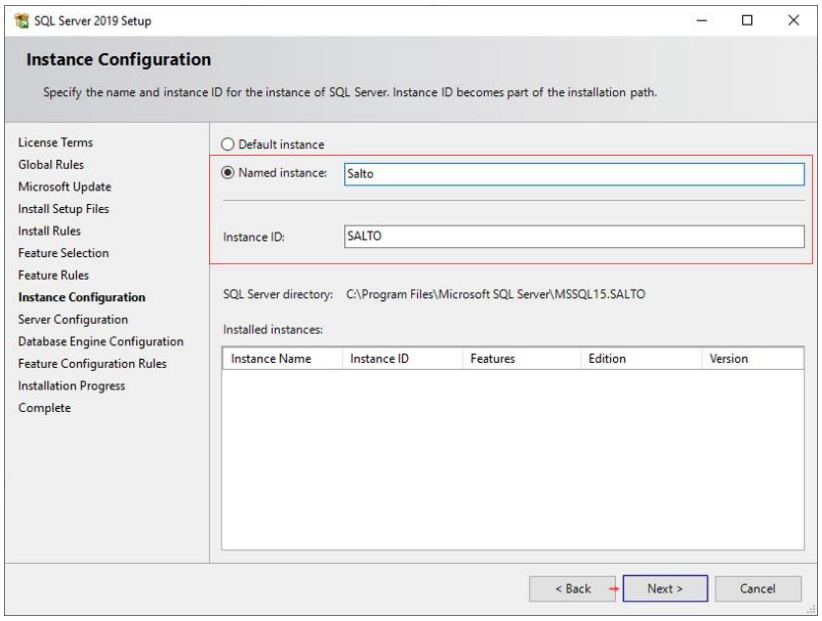
7. Click the **Next** button.
   The 'Install Rules' screen displays.



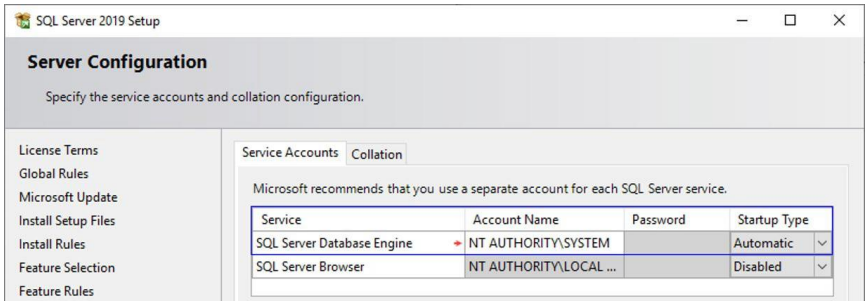
8. Click the **Next** button.
   The 'Feature Selection' screen displays.



9. Ensure all the checkboxes are checked and click the **Next** button.
   The 'Instance Configuration' screen displays.



10. Enter the name "Salto" for your instance in the **Named instance** field.
    Note: As you enter the Instance Name, the **Instance ID** field automatically populates also.
11. Click the **Next** button.
    The 'Server Configuration' screen displays.



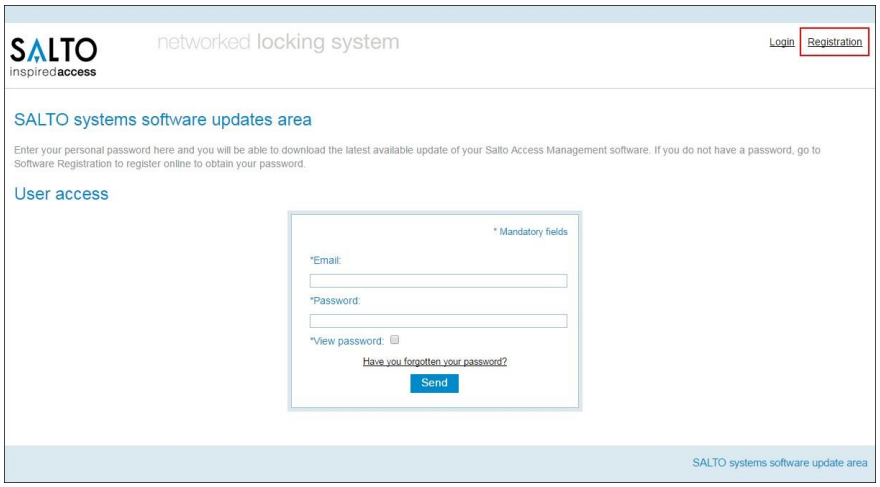
12. Change the Account Name for the SQL Server Database Engine to "NT AUTHORITY\SYSTEM", and click the **Next** button.
    The 'Database Engine Configuration' screen displays.
13. **Windows Authentication Mode** should be selected by default. Leave these settings as they are and click the **Add Current User** button if the current user is not displayed in the **Specify SQL Server administrators** list.
14. Click the **Next** button.
    The 'Installation Process' screen displays. This may take a while to complete.
15. Wait while the installation process runs through the installation automatically.
    Once the progress bar reaches the end, the 'Complete' screen displays.
16. Ensure the Status of each feature is "Succeeded" and click the **Close** button.
    The Setup wizard closes.
17. Close the 'SQL Server Installation Centre' application.

2. Register Salto ProAccess SPACE

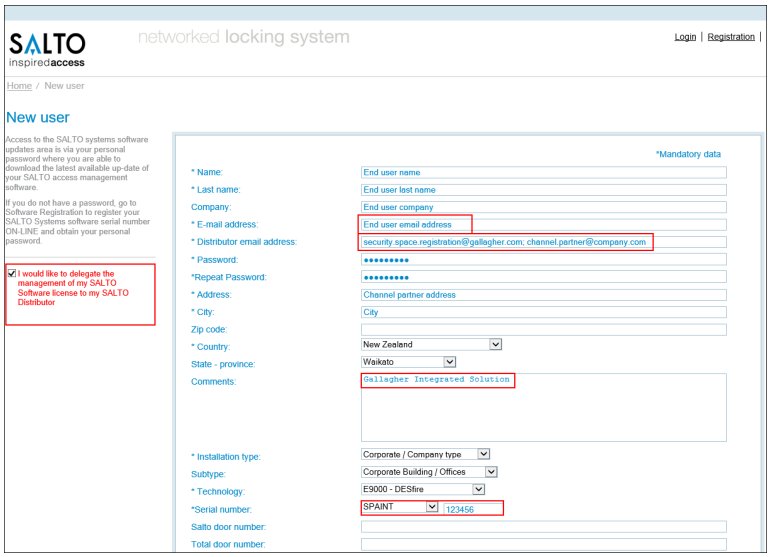
Before you install Salto ProAccess SPACE v6.10.4.3, you must register the software. The following procedure covers the registration process.

Note: The SPAINT number provided by Gallagher Tech Support or SOM (Sales Order Management) must be registered with Salto. Upon completion of this process Salto will send a validation email to the email address(es) specified during the registration process. This validation email contains log on details and further instructions which outline the steps required to log in to the Salto portal, active the software and download the licence **.DAT** file. This licence file is required to install SPACE, it is **not possible** to proceed without it.

1. Using a web browser, navigate to the Salto software area ***https://softwarearea.saltosystems.com/***
   The web browser opens the SALTO systems software updates area.



2. Click the **Registration** button, located on the top right of the screen.
   The New user screen is displayed.



3. **IMPORTANT:** Check the **I would like to delegate the management of my SALTO Software license to my SALTO Distributor** checkbox, located on the left of the screen. This will allow Gallagher and yourself (the Channel Partner) management rights for this installation. Failure to select this checkbox will limit Gallagher or yourself the ability to provide technical support for this installation.

   Note: Failure to select this checkbox will limit Gallagher Tech Support and the Channel Partner (yourself) the ability to provide support for this installation. When the delegate management option is used a confirmation email (**but no validation**) is sent to the email address specified in 'E-mail address'. A validation email is sent to all the emails specified in the 'Distributor email address'. This validation email is **required** to complete the process.

   If the delegate management option is not selected the validation email will be sent to email address specified in 'E-mail Address' only. Validation and activation are not carried out by Gallagher, this is the responsibility of the channel partner, our email should be included as a backup only. If not included Gallagher have no special access to Salto systems and will be unable to assist in the event of a problem.

4. Create a new user.
   - In the **E-mail address** field, enter the end user's email address. This address must be unique for each site.

     Important: Ensure that 'I would like to delegate the management of my SALTO….' is selected, enter at least one generic channel partner email, and 'security.space.registration@gallagher.com' is in the 'Distributor email address' section.
   - In the **Distributor email address** field, enter the email address **security.space.registration@gallagher.com** followed by your Channel Partner email address. Email addresses must be separated using a semi colon (;) character. An email will be sent to each address in order to validate the installation.
   - In the **Password** field, enter a password that will be used by you, the Channel Partner.

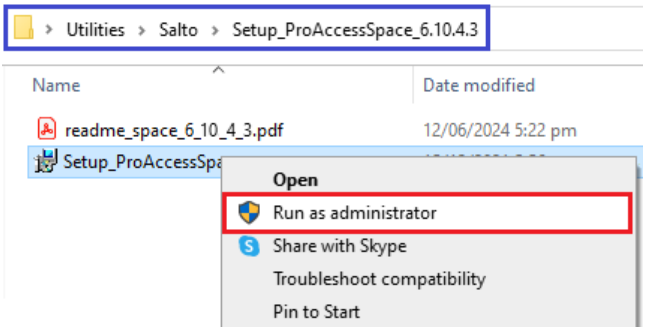
- In the **Comments** field, enter the comment **Gallagher Integrated Solution**.

5. In the **Serial number** field, select **SPAINT** as the product type and enter the SPAINT serial number provided by Gallagher for your customer into the corresponding field, (e.g. SPAINT 197660). This serial number will be unique for each site.
6. Complete all mandatory fields required to create a new user.
7. Click the **SEND** button. You will receive an email with a validation link.

3. Install Salto ProAccess SPACE

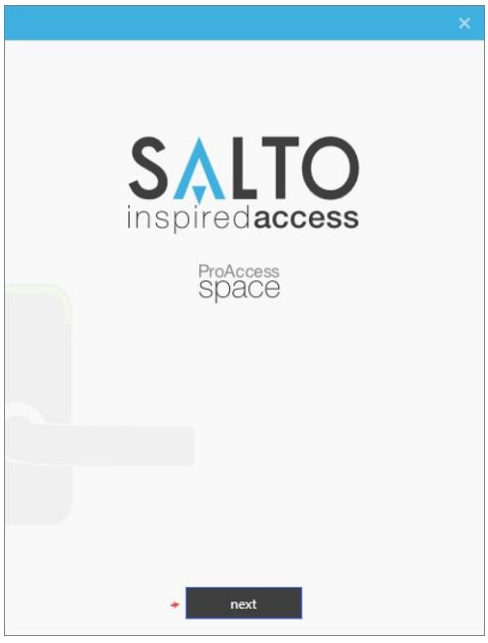
Salto ProAccess SPACE v6.10.4.3, the Salto Service and the Salto ProAccess SPACE Configurator are installed together from the one installation file. The following procedure covers the installation of these items.

1. Path your way to the **`'Utilities\Salto\Setup_ProAccessSpace_6_10_4_3'`** folder on the Command Centre installation media.
2. Right-click the **Setup_ProAccessSpace.exe** file, and select **Run as administrator**.

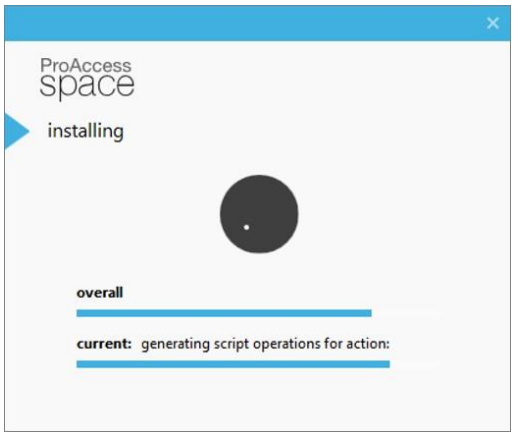


Note: If Windows User Account Control is enabled, you will be prompted with the message: *"Do you want to allow the following program from an unknown publisher to make changes to this computer?"* Click **Yes**.

The initial installation dialog box displays.



3. Click **next**.
   The license agreement dialog box displays.
4. Ensure you fully understand the terms and conditions in the license agreement you are about to enter into, then select **I agree to the terms and conditions** and click **next**.
   The destination folder dialog box displays.
5. Choose a different location or accept the suggested installation destination folder and click **next**.
6. Wait while the installation process runs through the installation automatically.



Is this a new install of Salto or an upgrade?

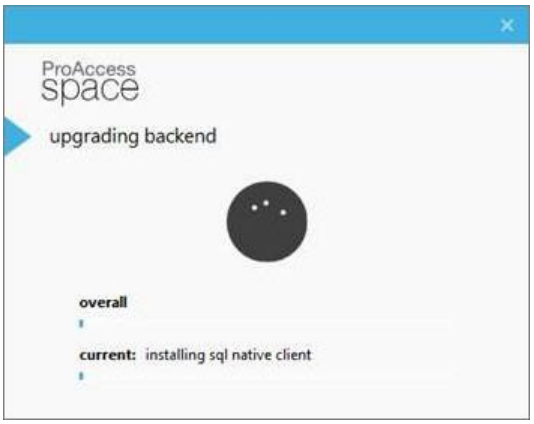
If…	then…
a new install,	go to Step 7.
an upgrade,	the following configure data backend dialog displays.



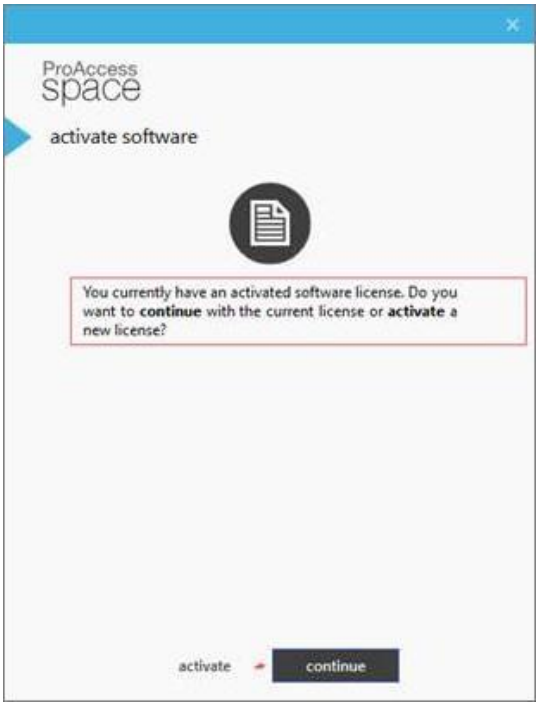
a) Select **Use existing** and click **next**.
   The upgrading backend dialog box displays.
b) Wait while the upgrade process completes

If…	then…

automatically.



The activate software dialog box displays.



c) Click **continue**.
The starting up dialog box displays.



d) Wait while the starting process completes automatically.

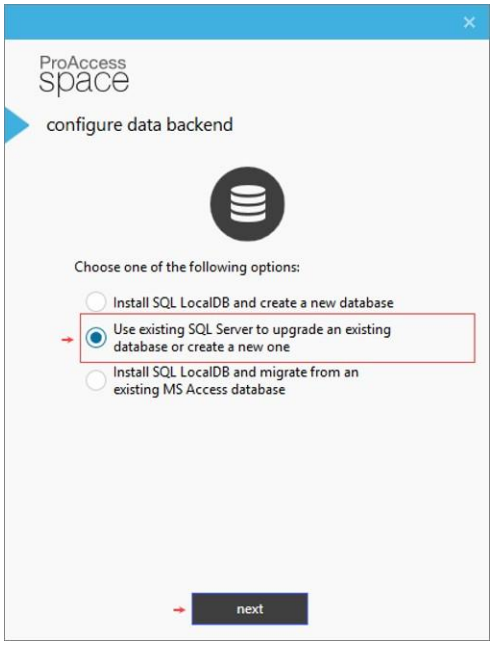
If…	then…
	The Well done! screen, confirming that Salto ProAccess SPACE is upgraded displays.



Note: You can click the quick-access tile to start using Salto ProAccess SPACE.

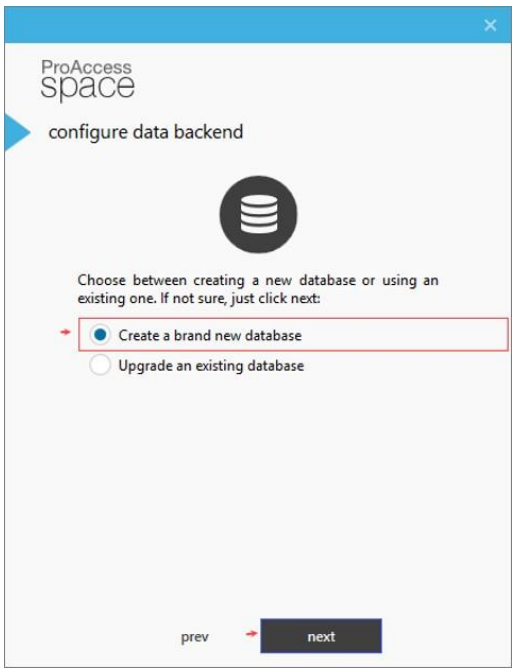
e) Go to ***4. Install Salto Local IO Bridge*** (on page 74-19)

7. The first configure data backend dialog box displays.

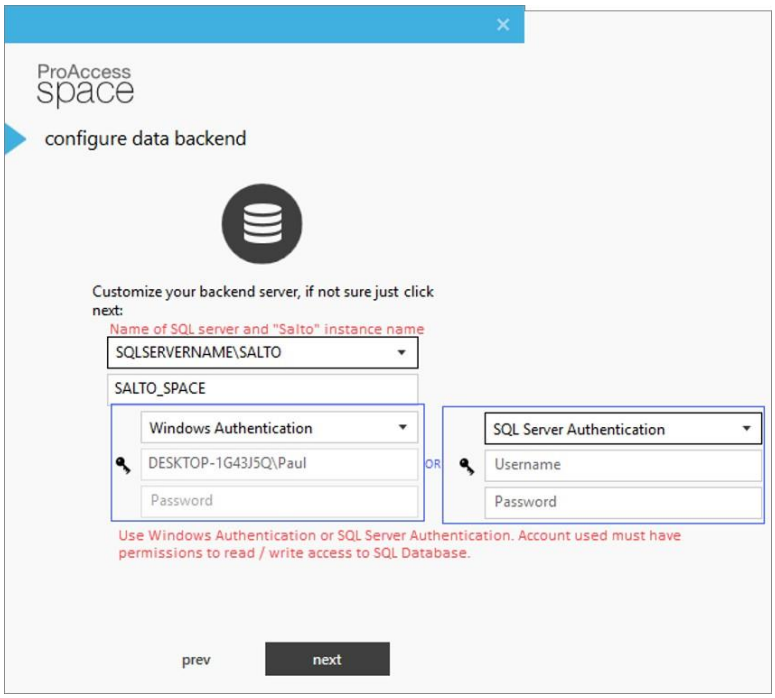


Select **Use existing SQL Server to upgrade and existing database or create a new one** and click **next**.
The second configure data backend dialog box displays.

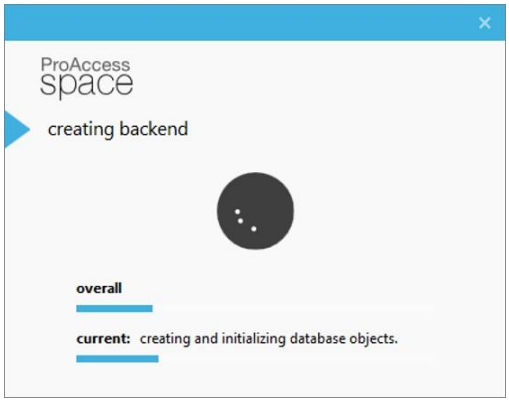
Note: This option is selected, because the SQL instance "SALTO" has already been created as per the section *"Installing Microsoft SQL Server for use with the Salto application"* above. SQL LocalDB is not supported.



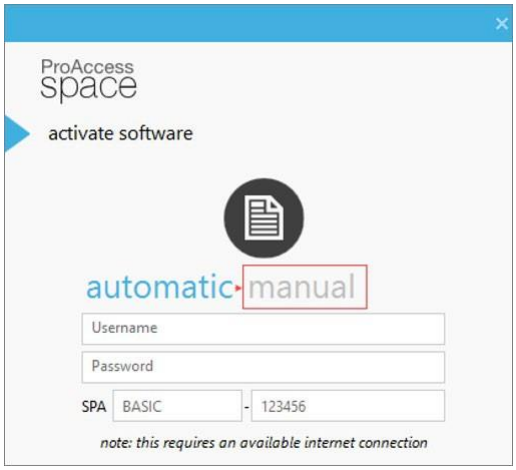
8. Select **Create a brand new database** and click **next**.
   The third configure data backend dialog box displays.



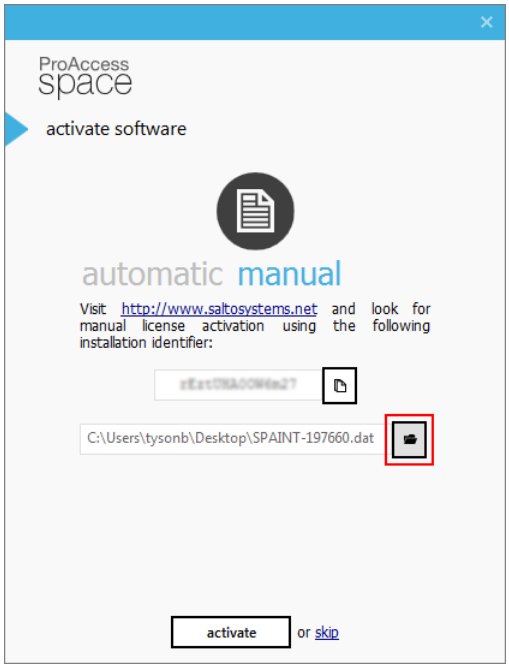
9. Add the SQL server name, the "Salto" instance name, and a Windows account that has read/write access to SQL databases.
10. Click **next**.
11. Wait while the creating backend process runs through the installation automatically.



The activate software dialog displays.



12. Select **manual**.
    The manual activation options display.

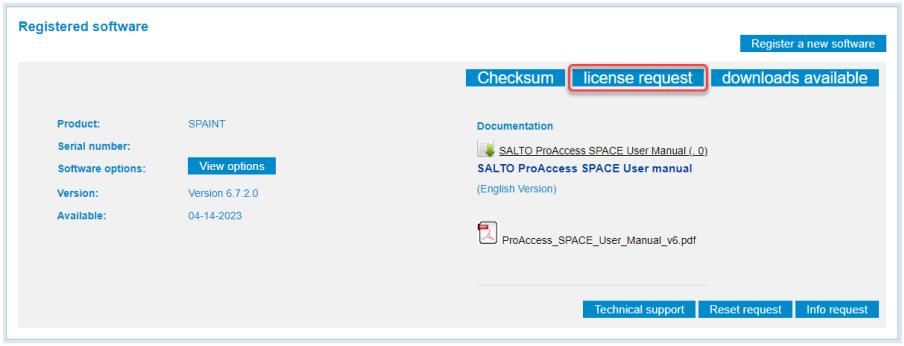


13. Click the **Copy** button to copy the installation identifier.
    The installation identifier is saved to the clipboard.

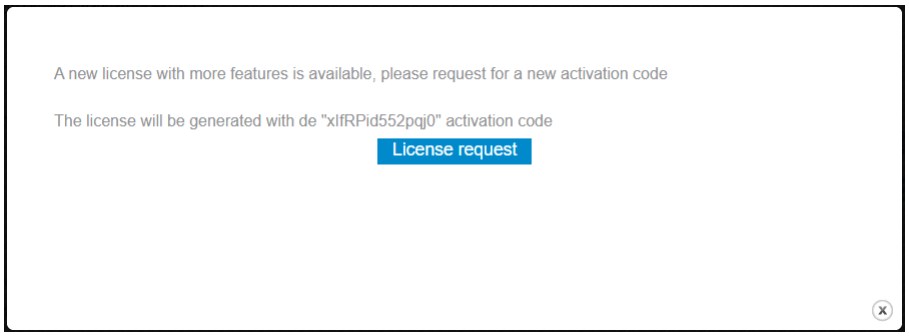
    The identifier is required later in order to activate your installation. Click

on the provided www.saltosystems.net on the manual activation screen.

14. Check your email (Distributor's email address entered during the registration process) and click the Salto registration validation link.
The Registered software screen displays within your internet browser.

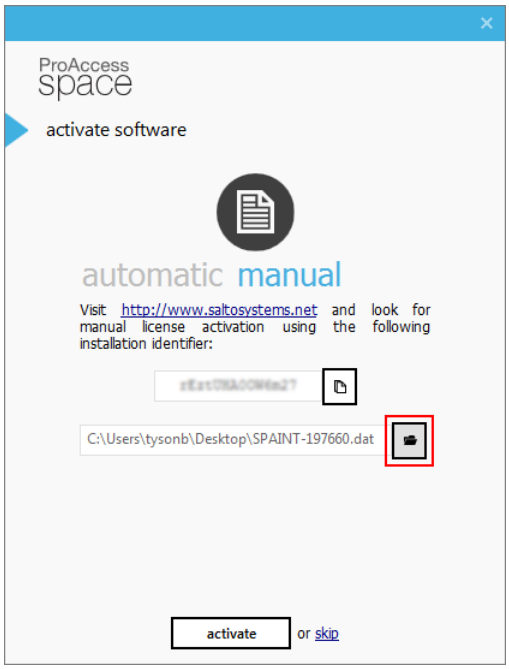


15. Click the **license request** button.
The License request screen displays.

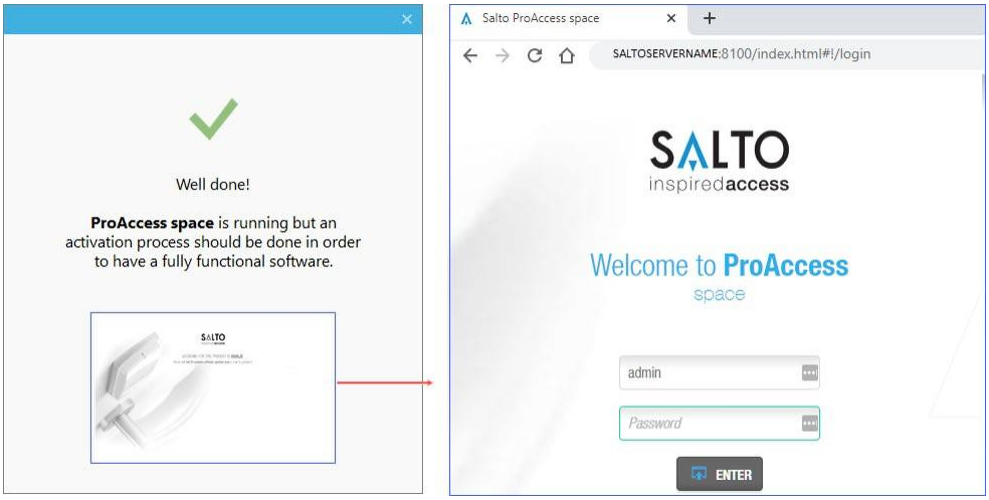


16. Paste your installation identifier (previously copied) into the **Activation code** field, and click the **License request** button. The Salto license data (.dat) file will be downloaded.
Note: It is recommended that you backup this license data file and store it in a secure location.

17. Navigate to the Salto ProAccess SPACE installer.



18. Click the **Folder** button and navigate to the Salto license data (.dat) file (previously downloaded).
19. Click **activate**.
    The Well done! screen, confirming that Salto ProAccess SPACE is installed displays.



Note: You can click the quick-access tile to start using Salto ProAccess SPACE. Default username is **admin** with a **blank** password. When you select enter, you'll be prompted to select a password.

4. Install Salto Local IO Bridge

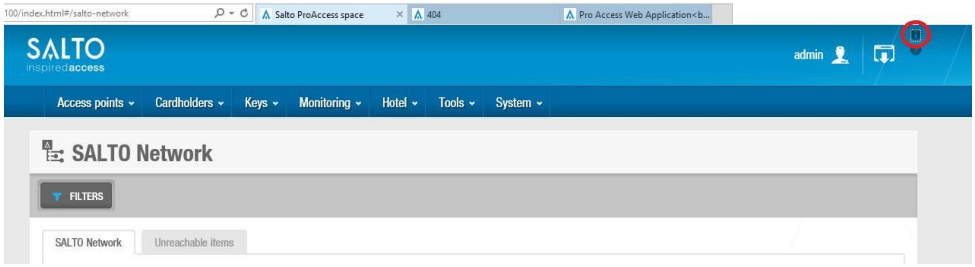
The Salto Local IO Bridge software allows USB devices to be used with Salto ProAccess SPACE by creating a link between the USB device (such as a Salto PPD) and the browser.

Notes:

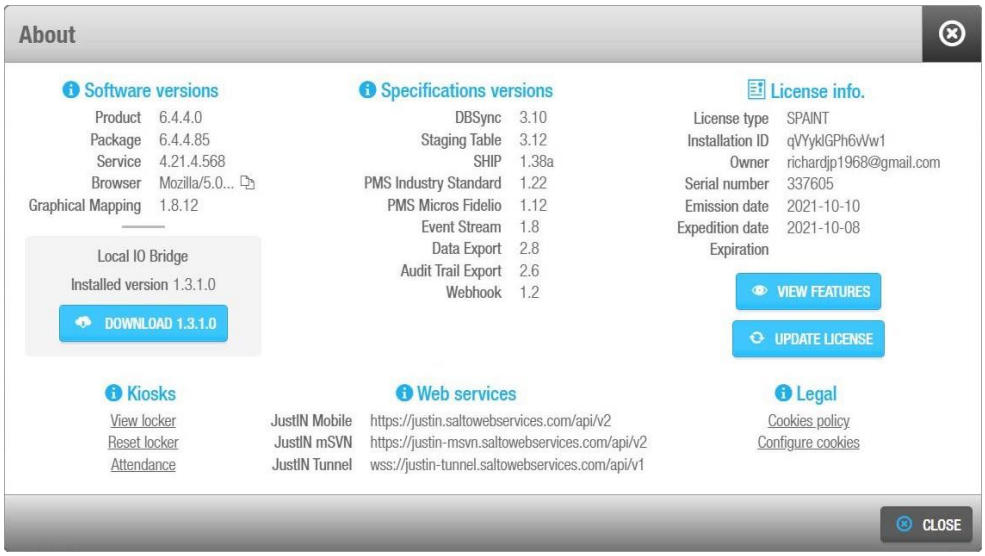
- Salto Local IO Bridge is not required on the Salto server, but must be installed on any machine that requires the connection of Salto USB devices.
- If the Salto Local IO Bridge software can be installed from the internet when a USB device is connected to Salto ProAccess SPACE, if not already installed.

To install the Salto Local IO Bridge, you must first log into Salto ProAccess SPACE as an operator with admin rights. The following procedure covers the installation of the Salto Local IO Bridge.

1. Open Salto ProAccess SPACE, and click the **About** button (**i**) located at the upper right corner of the Salto software.



2. On the **About** screen, click the **DOWNLOAD 1.3.1.0** button to download the Local IO Bridge executable.



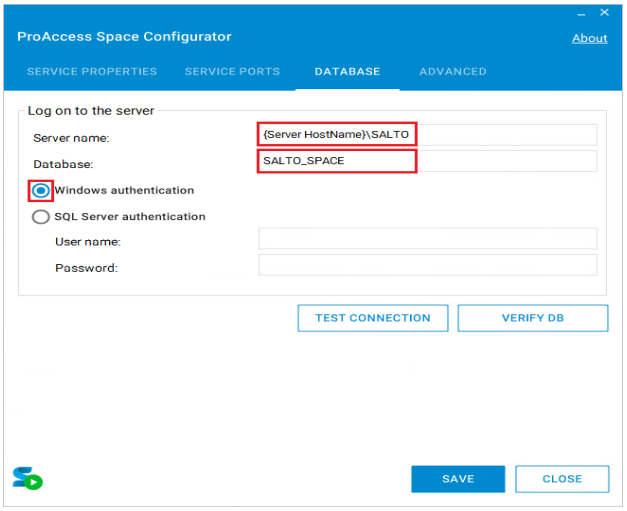
3. Right-click the **Setup_SaltoLocalIOBridge.exe** executable file.
4. Select **Run as administrator**.
   Note: If Windows User Account Control is enabled, you will be prompted with the message: "Do you want to allow the following program from an unknown publisher to make changes to this computer?" Click the **Yes** button.
5. Click **next**. The license agreement dialog box is displayed.
6. Select **I agree to the terms and conditions**.
7. Click **next**. The destination folder dialog box is displayed.
8. Choose a different location or accept the suggested installation destination folder.
9. Click **next**. The succeeded dialog box, confirming that the Local IO Bridge is installed is displayed.
10. Click **quit**.
11. Is this for a new install of Salto or an upgrade?

If…	then…
a new install,	go to 5. Checking the Salto ProAccess SPACE Configuration (next).
an upgrade,	go to ***6. Salto Server Connection*** (on page 74-24).

5. Checking the Salto ProAccess SPACE Configuration

To check the configuration settings for Salto ProAccess SPACE, perform the following steps:

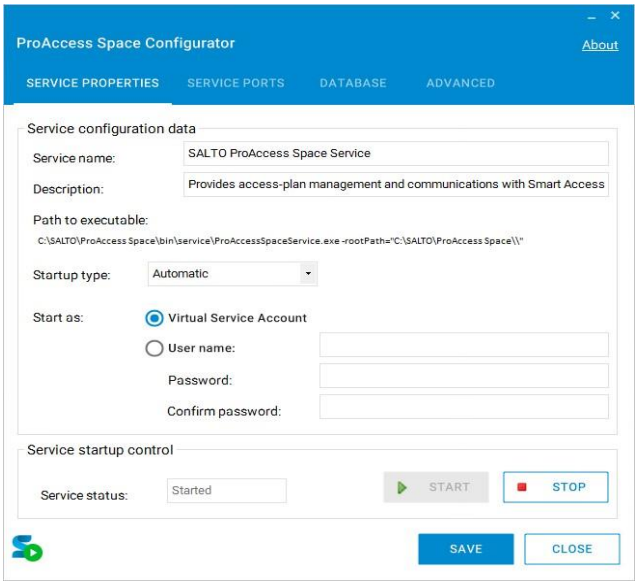
1. Ensure that the appropriate database has been set up in Salto ProAccess SPACE.
2. Double-click the **Salto ProAccess SPACE Configurator** icon on your desktop. The Salto ProAccess SPACE Configurator launches and the **DATABASE** tab is displayed.



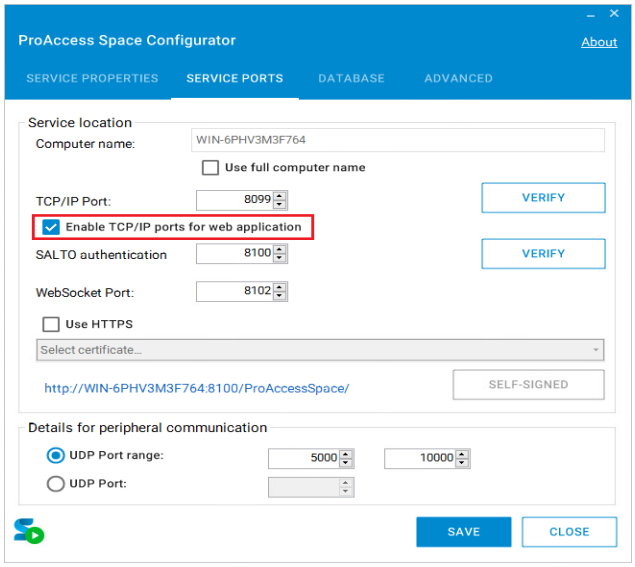
3. Ensure the server name in the **Server name** field is correct. You can verify the data in Microsoft SQL Management Studio if installed.
4. Ensure the database name in the **Database** field is correct. You can verify the data in Microsoft SQL Management Studio if installed.
5. Ensure the **Windows authentication** option is selected if you are working in a Windows domain.

   If you are not working in a Windows domain, select the **SQL Server authentication** option. You must enter the appropriate SQL Server username and password.
6. Click **SAVE**.

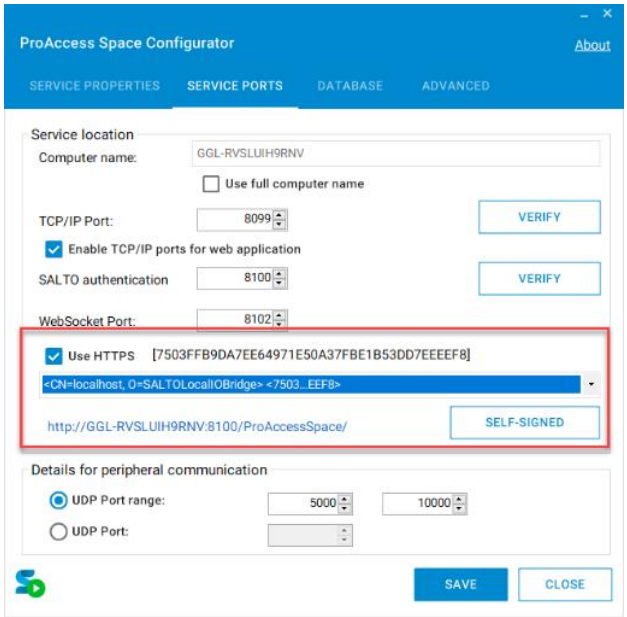
   Note: The SALTO Service must be stopped to save any change on the **Service properties** tab and then restarted.
7. Click the **SERVICE PROPERTIES** tab.



8. Ensure that **Automatic** is selected as the **Startup type** option.
   This value is selected so that when the PC reboots, the SALTO Service starts automatically.
9. Ensure that the **Virtual Service Account** option is selected.
   If you select this option, it means that the SALTO Service starts with local rights. If you select the **User** option, the SALTO Service starts with that particular user's rights. The **User** option might be required if the SALTO Service has to perform tasks with files located on a different PC.
10. Click **SAVE**.
11. Click the **SERVICE PORTS** tab.

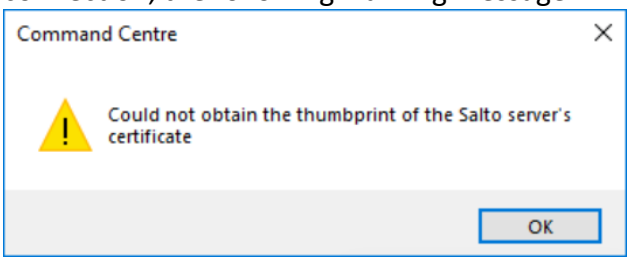


12. Select the **Enable TCP/IP ports for web application** checkbox.
    The default ports can be changed in accordance with your requirements. In some cases, ports can be limited to one rather than a range.
13. Select the **Use HTTPS** checkbox.
    Choose the correct certificate from the drop-down list.



Notes:

- Please consult your IS department for the certificate to be installed.
- If you skip this step, when Command Centre establishes a HTTPS connection, the following warning message will display:

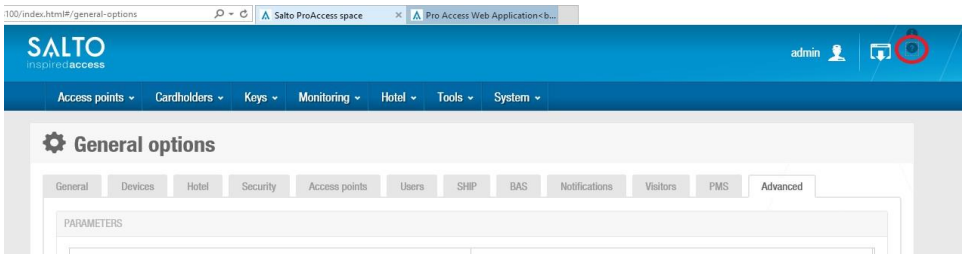


- If the certificate has changed from the Salto side, the Command Centre will lose connection with the Salto Server.

14. Click **SAVE**.
    The ProAccess SPACE link on this tab should now become active. If required, add the Salto ProAccess SPACE URL to a ***URL Tile*** (see ***Adding Salto to the URL Tile*** on page 74-105) in Command Centre.

Notes:

- The latest firmware for Salto devices is provided with the Salto ProAccess SPACE software. Download the new firmware to the Salto PPD. Using the PPD, update the firmware on all Salto devices.
- If Command Centre is installed and licensed for Salto doors, the Salto server in Command Centre should come online.
- If the Salto server is on a different PC, then in Command Centre change the settings of the Salto Server Command Centre item to match the IP address of the Salto server and Port numbers used.
- If the SALTO ProAccess Space Service is stopped, no access information will be transferred from Command Centre to the card via the Salto server.
- Salto has introduced a security feature that enables Salto to only accept communications from one IP. Refer to the topic ***Editing the Salto Server*** (on page 74-73) for details.
- Once Salto ProAccess SPACE is installed, the Salto user manual is available by clicking the **?** button located at the upper right corner of the Salto software.



6. Salto Server Connection

Introduction

If your site is not able to immediately upgrade to HTTPS + Salto Native integration (encrypted communication is desired), it is recommended to setup a secure tunnel between the Salto server and Command Centre server.

Procedure

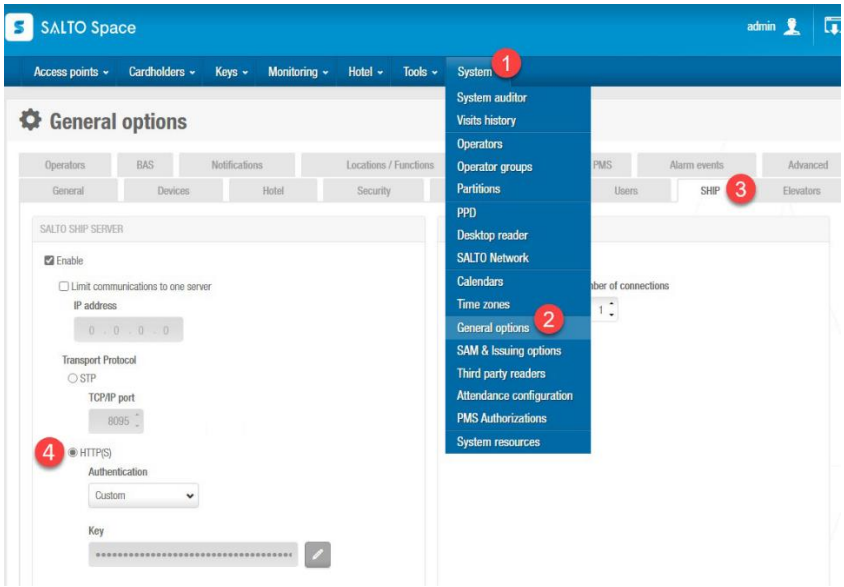
This procedure is split into three parts, as follows:

1. Changing settings in Salto Space
2. Changing to HTTPS connection in Command Centre
3. Enabling Salto-Native Users Mode

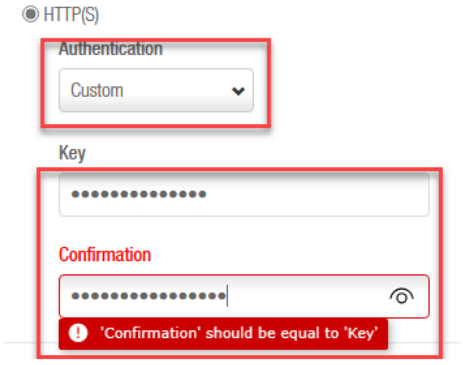
1. Changing settings in Salto Space

Before changing connections to HTTPS in Command Centre Configuration Client, settings from the Salto server side need to be changed, as follows:

1. Log on to Salto Space.
2. Select **System > General options > SHIP**.



3. Change Transport Protocol to **HTTP(S)**, and select "Custom" from the **Authentication** drop-down list.

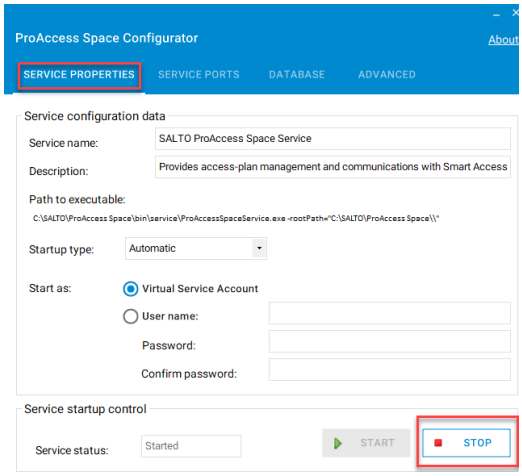


4. Create a unique key in the **Key** field, then re-type it in the **Confirmation** field- and click **Save**.

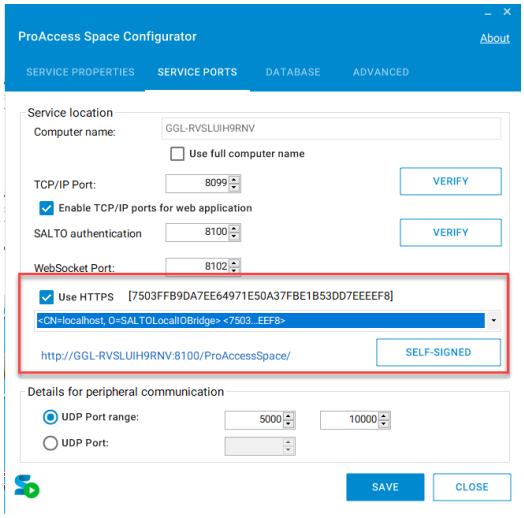
Notes:

- This key is based on a custom token that a client provides when making HTTP requests. API keys are supposed to be a secret that only the client and server know.
- Once the key is populated, it won't be able to see anymore from Salto Space.

5. Double-click the **ProAccess SPACE Configurator** icon on your desktop.
6. From the **Service Properties** tab, click the **STOP** button to stop the Salto services.

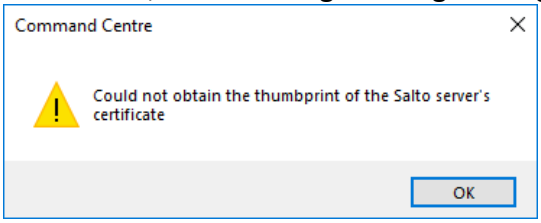


7. Select the **Service ports** tab and tick "Use HTTPS" checkbox.
8. Choose the correct certificate from the drop-down list, and click **Save**.
Note: Please consult your IS department for the certificate to be installed.



Notes:

- If you skip Steps 5 - 7, when Command Centre changes to HTTPS connection, the following warning message will display:

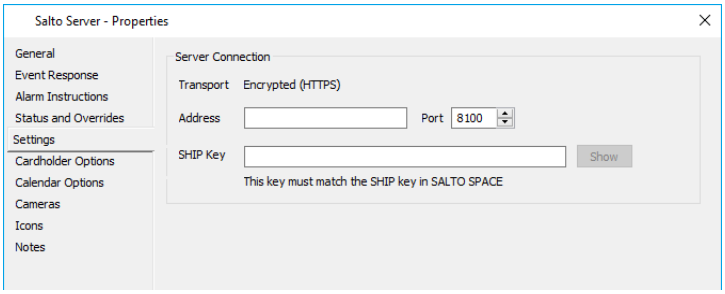


- If the certificate has changed from the Salto side, the Command Centre will lose connection with the Salto Server.

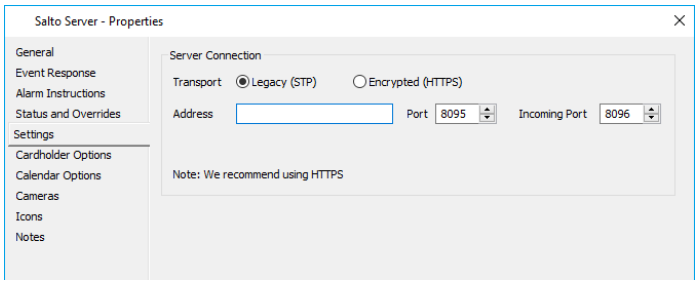
9. Click the **Start** button to start the Salto services.
10. Click **VERIFY** for Salto authentication Port to check your port is working, and then click **SAVE**.
11. Return to Salto Space and select **System** > **General options** > **Users**.
12. Within the 'Settings' section, select the **Discarded openings are also included in the key's auditor** check box.
    This setting is required for unauthorised events with offline doors to be raised in Command Centre.
13. Within the 'Tracks of user key section', Gallagher recommends ensuring the **Wiegand code** checkbox is selected and **Profile code** is selected.
    This is required for when you create third party doors using UBOX4000 or other wired door controllers.
14. Click **Save**. If a Warning window displays, click **Yes**.

2. Changing to HTTPS connection in Command Centre

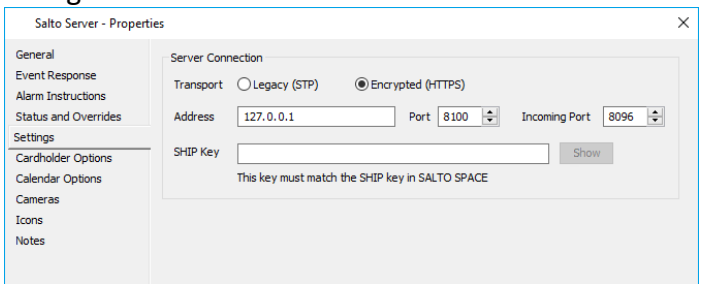
1. In Configuration Client, click **Configure** from the menu bar, then **Salto**.
   The **Salto** List Window opens.
2. **Right click** on the Salto Server and select **Properties**.
   By default the **General** tab displays.
3. Click the **Settings** tab.
   How this screen looks depends on whether this is a new or an existing site.

If…	then…
a new site,	**Encrypted (HTTPS)** is the default "Transport" connection. If your site chooses to use Salto Native Mode, settings from the Salto server side need to be changed. 
an existing site,	there are two "Transport" options to choose from, i.e. **Legacy (STP)** and **Encrypted (HTTPS)**. Select the appropriate "Transport" radio button: • **Legacy (STP) Transport with Legacy Mode:** This option is available for STP (TCP/IP) connection, however it is recommended to use the **Encrypted (HTTPS)** option to secure communication.

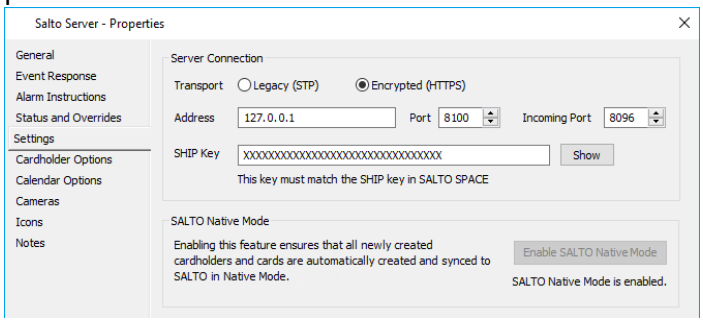
If...	then...



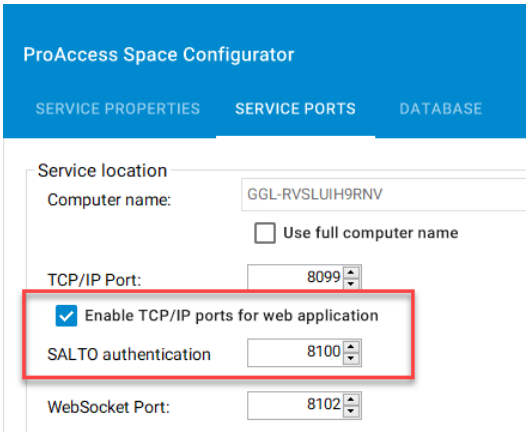
- **Encrypted (HTTPS) Transport with Legacy Mode:**
  If your site chooses to use Salto Native Mode, this option must first be selected. Before changing connections to HTTPS, settings from the Salto server side need to be changed.



- **Encrypted (HTTPS) Transport with Native Mode:**
  After the site enabled Native Mode, the Server Connection page will still display the incoming port so that existing Legacy Mode cards can use the STP connection. Completing Native Mode card migration will allow this port to be closed.

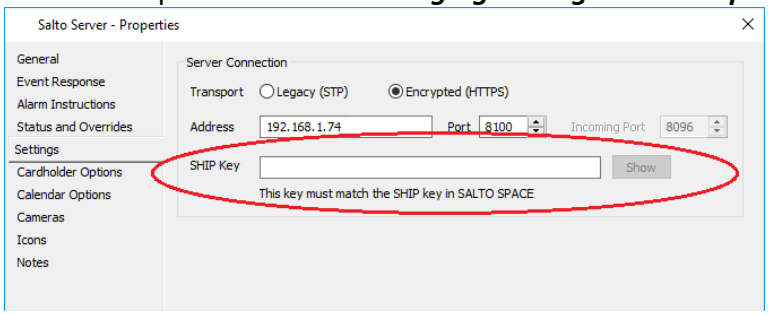


4. The single Salto Server Command Centre item has the following properties which are valid for the Server only:
   - **Address** of Salto Server (default = empty). This needs to be changed to the Server name or IP Address for the Server running the Salto application, if the Salto Server does not reside on the same PC as the Command Centre Server. It can take up to approximately ten seconds for the Salto server to come online after configuring or re-configuring the Name / IP-Address.
   - **Port** is the port for outgoing requests to Salto Server (Default to 8100). The port comes from the "SALTO authentication" field on the **Service Ports** tab in the ProAccess SPACE Configurator.



. **Incoming Port** is for legacy Salto card updating its access information from Command Centre. Native Salto cards don't require this.
Command Centre will automatically open or close this connection according to whether or not legacy cards exist. Communication on this port is not encrypted (Default to 8096).

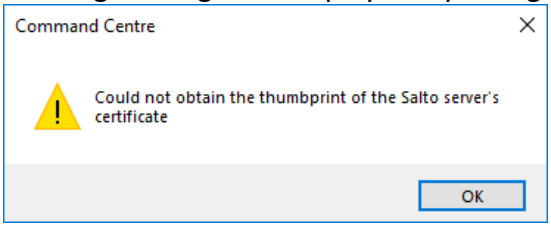
5. Type or paste the **SHIP Key** that you created for Salto Space and click the **Apply** button.
Refer to Steps 3 and 4 of ***1. Changing settings in Salto Space*** (earlier).



Command Centre is now connected to the Salto Space Server. **Notes:**

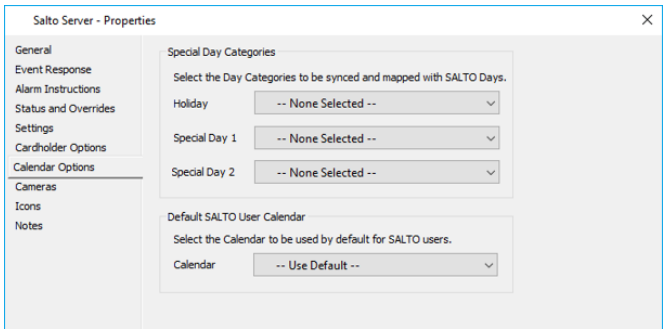
- Clicking the **Show** button will display the key that you have entered. Clicking the **Apply** button changes the text back to X's and the Show button is enabled again. An operator event is also logged.
- A "SALTO Native Users" section displays, and once HTTPS connection is successfully created, the Legacy (STP) connection is still available to switch back to. However, the **Enable SALTO Native Users** button will be disabled if the **Legacy (STP)** radio button is selected.
Note: Existing sites need to be licensed for Salto Native User Mode for the "SALTO Native Users" section to display.

  Once HTTPS connection is established, if you want to change the Server Connection settings, (i.e. IP Address, Port and SHIP Key), they must be changed in Salto first, and then replicated in Command Centre. The following warning message will display if any changes are made:

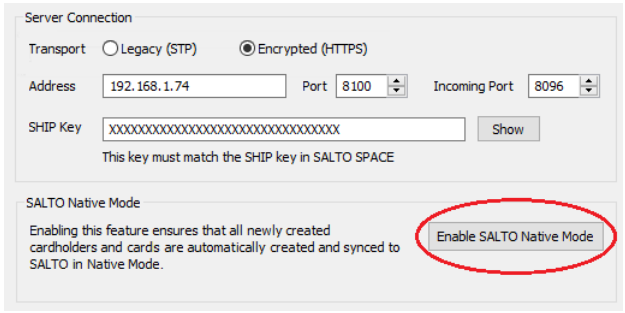


3. Enabling Salto-Native Users Mode

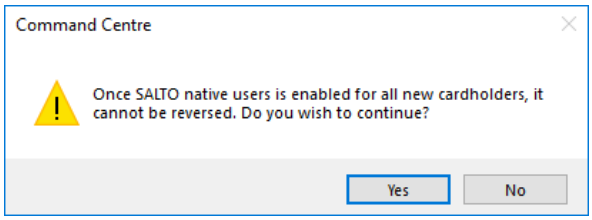
1. Click the **Calendar Options** tab.
   This tab allows you to select three special Day Categories and a Calendar which will be reflected in Salto.
   Note: If you have enabled Native Mode, once Day Categories and Calendars are selected in Command Centre they are reflected in Salto.



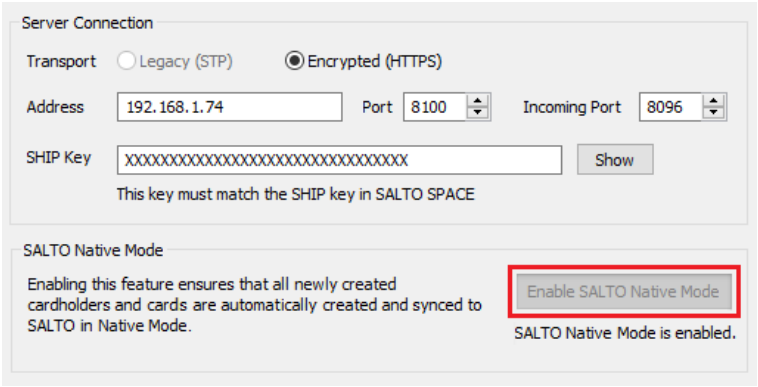
2. The **Special Day Categories** section allows different access times to be configured for special days so that cardholders can have different access depending on the day.
   Select the appropriate options from the **Holiday**, **Special Day 1** and **Special Day 2** drop-down lists.
   Note: Each drop-down list shows the available Special Day Categories and Calendars within an operator's divisional privileges.
3. Select the appropriate 'Calendar' from the drop-down list to be used as the **Default SALTO User Calendar**.
   Note: If **Calendar** is not selected, the system will use the "Default Calendar" as the Salto User Calendar.
4. Click the **Apply** button to save your changes.
5. Once HTTPs communication is established, in Configuration Client, click the **Enable SALTO Native Users** button on the **Settings** tab of the Salto Server properties.
   Note: Salto Native license is required to Enable SALTO Native Users.



   The following prompt displays:



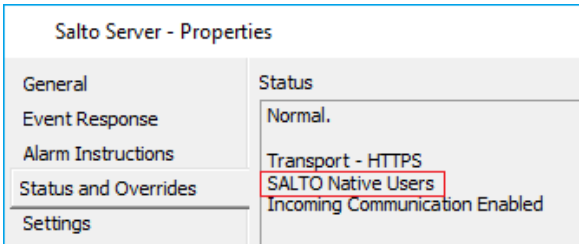
6. Click the **Yes** button.



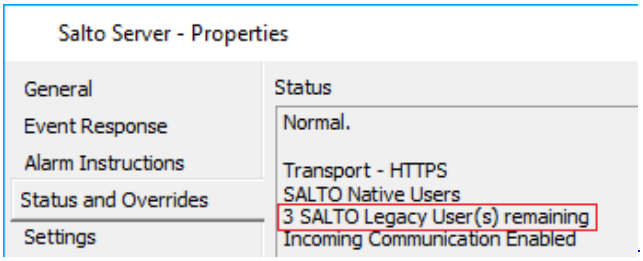
After moving to "Salto Native Users" mode:

- the **Enable SALTO Native Users** button is disabled and an event is generated.
- a "GallagherCommandCentre" partition is created in Salto Space which will be used to separate Command Centre created/used items from other items in Salto. The partition protects all Command Centre used Salto Users, Access Levels, Cardholder Timetables and Calendars in Salto Space. It is important to leave this data untouched because they are managed by Command Centre. Any Salto Space operator other than the default system operator should be restricted from accessing the "GallagherCommandCentre" partition.

  How long it takes to sync cardholders and access privileges is dependant on the number of cardholders and Salto doors, (e.g. up to 10,000 cardholders can take up to 15 minutes).
- the Salto Server status will be changed to *"SALTO Native Users"* on the **Status and Overrides** tab.



If the site is updated from Legacy to Salto Native Users mode, then the status message will display if there are any Salto Legacy User(s) remaining, and how many.



Space Site Configuration

You will need to configure your Salto hardware using Salto ProAccess SPACE.

Note: For details on how to install the Salto hardware, (i.e. relay board wiring, DIP switch settings, termination, etc.) refer to the Salto installation documents provided with the Salto hardware.

In the first instance, you should consult the Salto documentation, however the following topics have been provided to assist in the Salto hardware configuration process:

- ***Salto User and SHIP settings*** (on page 74-32)
- ***Salto Advanced Parameter Options*** (on page 74-34)
- ***Salto Native Mode Migration*** (on page 74-35)
- ***Salto Ethernet Encoders/Dongles*** (on page 74-37)
- ***PPD Status*** (on page 74-40)
- ***Salto Doors or ESDs*** (on page 74-41)
- ***Salto Lockers*** (on page 74-46)
- ***Salto Rooms*** (on page 74-48)
- ***Salto Suites*** (on page 74-51)
- ***Salto Zones*** (on page 74-54)
- ***Salto Outputs*** (on page 74-56)
- ***Salto wired (online) devices*** (on page 74-57)
- ***Salto wireless RF devices*** (on page 74-59)
- ***Initialising a door using the PPD*** (on page 74-64)
- ***Audit Trail (collecting door opening data using the PPD)*** (on page 74-66)
- ***Enable mobile audit trail for Salto offline doors/locks*** (on page 74-67)
- ***Emergency Opening*** (on page 74-68)
- ***Other Salto Configuration*** (on page 74-70)

Notes:

- When naming your Salto items '@' and '(X)' should not be used in the name field.
- You will need to perform an ***Update Access Points*** (on page 74-82) each time you modify the properties of a Salto hardware item.

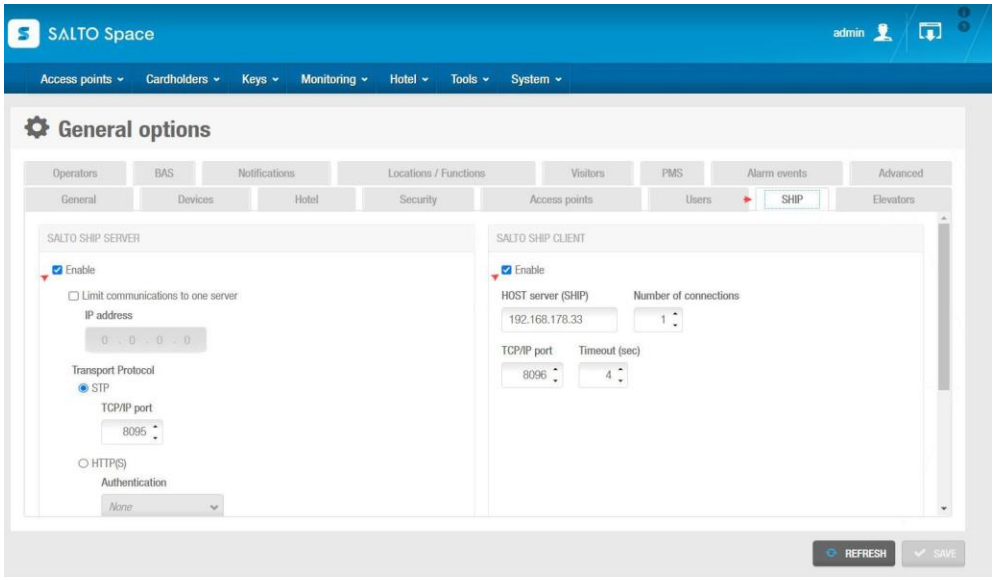
Salto User and SHIP settings

Introduction

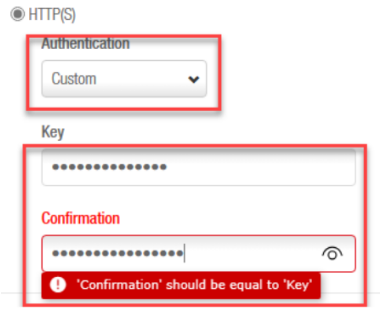
You must configure the SALTO Host Interface Protocol (SHIP) option by using the SHIP tab. When SHIP integration is performed, only doors are managed by the SALTO system. Users are managed in Gallagher Command Centre, and synced with Salto Space.

Procedure

1. Select **System** > **General Options** > **Users**.
   The Users tab displays.
2. Within the 'Settings' section, select the **Discarded openings are also included in the key's auditor** checkbox.
   This setting is required for unauthorised events with offline doors to be raised in Command Centre.
3. Within the 'Tracks of user key' section, Gallagher recommends ensuring the **Wiegand code** checkbox is selected and **Profile code** is selected.
   This is required for when you create third party doors using UBOX4000 or other wired door controllers.
4. Select **System** > **General Options** > **SHIP**.
   The SHIP tab displays.
5. Enable the SALTO SHIP SERVER to communicate with Gallagher Command Centre.



6. Configure as appropriate.

Checkbox/Field	Description
Enabled *for SALTO SHIP SERVER*	Enables the SALTO SHIP server.
Limit communications to one server	Limits communications to one server in the network. When you select this option, you must enter the IP address for the third-party server you have selected for the communications in the **IP address** field underneath the checkbox. This means that the SALTO software will only communicate with that server (using SHIP protocol). If you do not select this option, other servers in the network will be able to send commands to the SALTO server.
Transport Protocol	Native mode uses **HTTP(S)**. Select "Custom" from the **Authentication** drop-down list.  Create a unique key in the **Key** field, then re-type it in the **Confirmation** field. **Notes:** • This key is based on a custom token that a client provides when making HTTP requests. API keys are supposed to be a secret that only the client and server know. • Once the key is populated, it won't be able to be seen anymore from Salto Space.

Salto Advanced Parameter Options

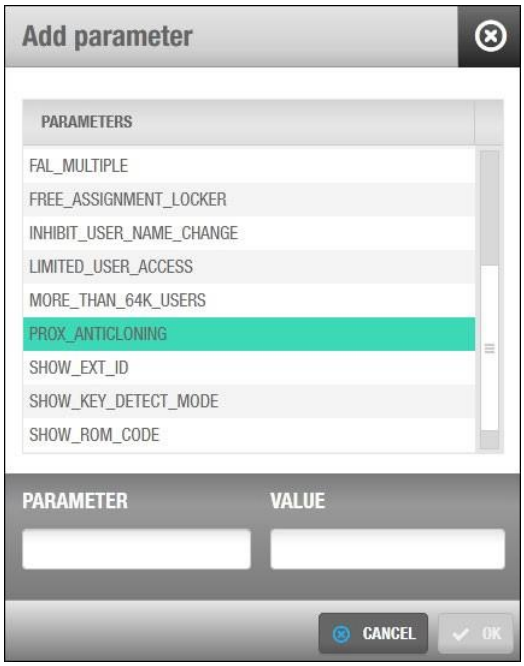
Introduction

You will need to disable the advanced parameter PROX_ANTICLONING to your Salto ProAccess SPACE installation. This parameter allows the data written on proximity cards to be mixed with the key ROM codes.

For information regarding other parameters that can be enabled, refer to the topic "Advanced Parameter Options" in the Salto ProAccess SPACE documentation.

Procedure

1. Select **System > General options > Advanced**.
   The Advanced tab displays. This tab shows a list of available parameters. Any parameters you have enabled are displayed in the **Advanced Parameters** field.
2. Click the **Add parameter** button.
   The parameters list is displayed in the Add parameters screen.



3. Double click the parameter PROX_ANTICLONING.
   The PROX_ANTICLONING parameter needs to be disabled, so set the **Value** field to '0'.

   Note: The **Value** field is a Boolean data type, having two values (usually denoted true=1 and false=0). In some cases, a different value will be requires such as DISCARD_PERSONAL_EVENTS_OLDER_THAN=7 or AUTO_LOGOFF_TIMEOUT=120.
4. Click **OK**.

Salto Native Mode Migration

Introduction

This section is intended to provide a set of instructions for the migration of a Legacy Mode integration into Native Mode. If your site is already in Native Mode, this section can be skipped.

Salto's Native Interface enhances cyber security and user functionality, and future-proofs the Salto integration with Command Centre, allowing extended functionality in the future. It also ensures Gallagher Command Centre will work with future Salto features. Salto's legacy interface does not support end-to-end encryption. By migrating to Salto Native Interface, encryption is enabled between Command Centre and Salto Space. Operators will benefit from additional features, for example, Access during lockdown, improving the user experience.

Native Mode versus Legacy Mode

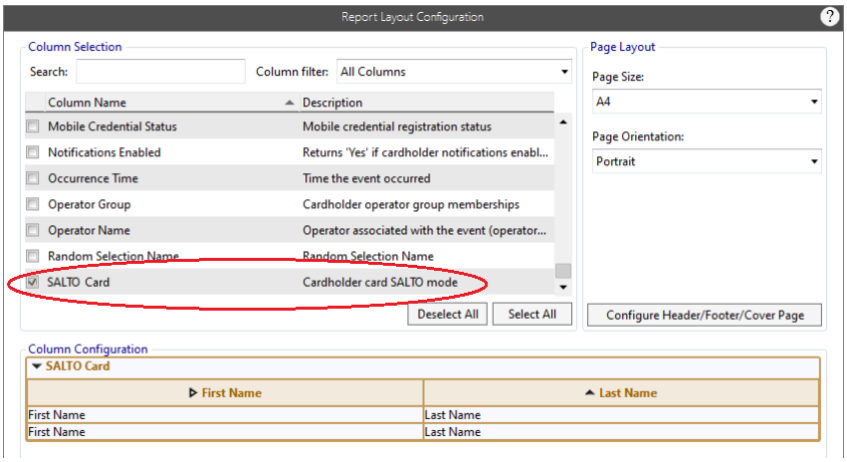
Native - Salto-managed users (access managed by Command Centre)	Legacy - Host-managed users
Command Centre Cardholders are the Users in Salto's database	Command Centre Cardholders do not exist as Users in Salto's database
Communication between Gallagher Command Centre and Salto Space is encrypted (HTTPS)	Communication between Gallagher Command Centre and Salto Space is unencrypted (STP)
New user access features are available	User access features are limited

Lockdown overrides

The Lockdown override only works for Native Mode. When the **Entry allowed during lockdown** access privilege (on the **Privileges** tab of the Access Group) is enabled, a Lockdown override can be performed to allow members to enter Access Zones contained in the Access Group, when those Access Zones are in lockdown mode.

Reports

Cardholder Reports can be configured in Command Centre Client that show whether a cardholder has a Salto Native encoded card, Salto Legacy card or no Salto card.



Refer to these sections to ensure you have configured Salto to encode cards in native mode, if you are using 26 bit cards configuration is required in Salto Space:

- ***Reason for using 64-bit Wiegand format*** (on page 74-93)
- ***Configuring Key to support Space CUADAP 64-bit integration*** (on page 74-94)
- ***26 bit Wiegand Setup*** (on page 74-96)

Migrating Salto Legacy Cards to Salto Native Mode

The Salto Legacy Card Migration Tool enables a smooth transition from Salto Legacy Cards to Salto Native Mode, simplifying the upgrade process.
Note: You must be in Salto Native Mode to use this tool.

For further detail refer to the document **"Salto Migration Tool_Release Note.pdf"** located in the `'Utilities/Salto'` directory of the Command Centre installation media.

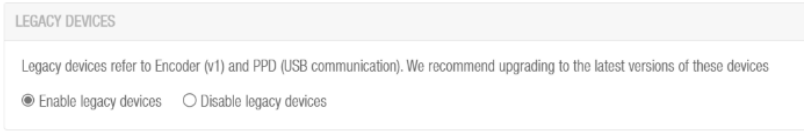
Salto Ethernet Encoders/Dongles

Introduction

Every site requires a Salto Ethernet encoder/dongle, regardless of whether they will be encoding. To encode cards with Salto data from Command Centre, you will need a Command Centre USB encoder and/or a printer, (e.g. Fargo HDP5000 Printer) connected to Command Centre. The Salto Ethernet encoder is used by the Salto system for card encryption, but is not used when encoding cards from Command Centre.
The Salto Ethernet encoder must be connected to the Salto server. The Command Centre USB encoder and/or printer must be connected to the Command Centre server or a Command Centre workstation.
Note: If cards are encoded off-site, then the off-site bureau connects to the Salto server on the site, which then connects to the Salto Ethernet encoder.

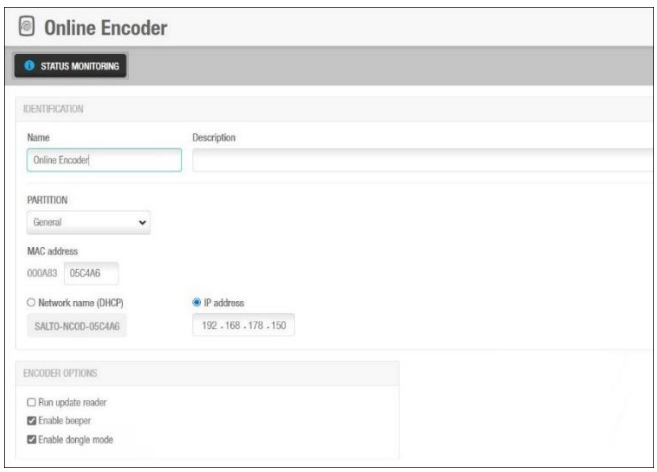
Procedure

1. If your site is using an old encoder, select **System** > **General Options** > **Devices**.
2. Within the 'LEGACY DEVICES' section, select the **Enable legacy devices** checkbox.



Note: Sites using an old Encoder will not be able to encode cards with the **Disable legacy devices** checkbox ticked. The **Disable legacy devices** setting is on by default with new installations.

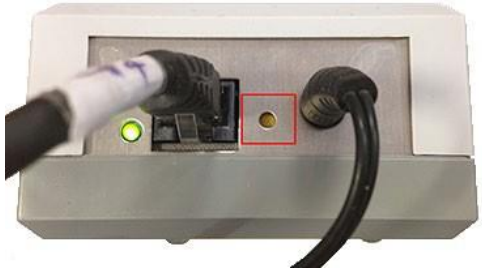
3. Select **System > SALTO Network**. The SALTO Network screen is displayed.
4. Click **Add**. The Add network device dialog box is displayed.
5. Select **Encoder** or **Ncoder** as applicable from the drop-down list, and click **OK**. The Encoder information screen is displayed.
   This screen will differ depending on the type of encoder you selected. The example below is the screen for the **Ncoder**, and includes some additional fields that don't appear on the screen for the **Encoder**:



6. Type a name for the encoder in the **Name** field.
7. Type a description for the encoder in the **Description** field.
8. Select the appropriate **Partition** from the drop-down list.
9. Type the media access control (MAC) address in the **MAC address** field. **Note:** This field only appears for the Ncoder, (i.e. it does not appear for the encoder).
10. Did you select **Encoder** or **Ncoder**?

If…	then…
Ncoder,	select either the **Network name (DHCP)** or **IP address** option. If you select **Network name (DHCP)**, an IP address is automatically assigned to the RF gateway. A Dynamic Host Configuration Protocol (DHCP) server and a DNS are required for this option. If you select **IP address**, you must type a static IP address in the field.
Encoder,	type the **IP address** you are going to assign to this Ethernet encoder in your local area network. **Note:** Consult your LAN Administrator if you are not sure which IP address should be given to this device. Ensure the IP address is a valid one that is not already in use by another device.

11. Select the **Run update reader** checkbox, if required.
    This option is used to configure an Ethernet encoder to update user keys automatically when users present their keys to it. If you select this option, the encoder runs continuously but it can only update keys. It cannot be used to encode keys with access data from the Salto software.
12. Select the **Enable beeper** checkbox, if required.
    If you select this option, the encoder emits beeps when in use.
13. Select the **Enable dongle mode** checkbox. The encoder will be used by the SALTO service to encrypt data using a third-party reader.
14. Click the **Save** button.
15. On the physical Ethernet encoder, use a pen or pencil to push the **Address** button (shown below) for three seconds until it starts flashing. Once flashing, click the **Address** button on the Encoder information screen (in the Salto application).



Encoder



Ncoder

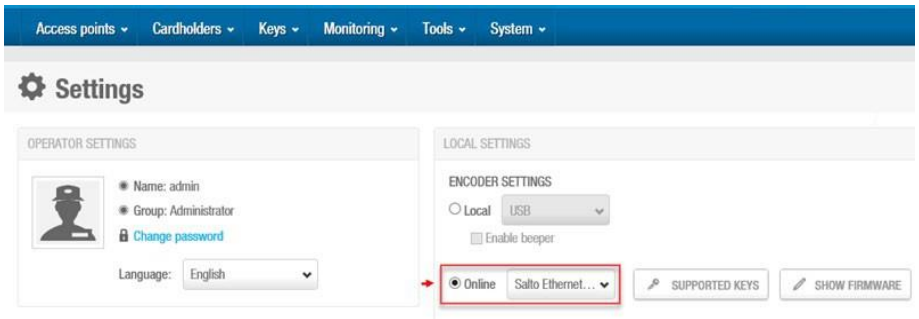
The Address dialog box disappears and the Encoder will be available.

16. Click the **Back to Salto Network** button.
    The Encoder information screen closes and you are returned to the SALTO Network screen, with the newly created Ethernet Encoder appearing in the list.

17. Select the **admin** tab.



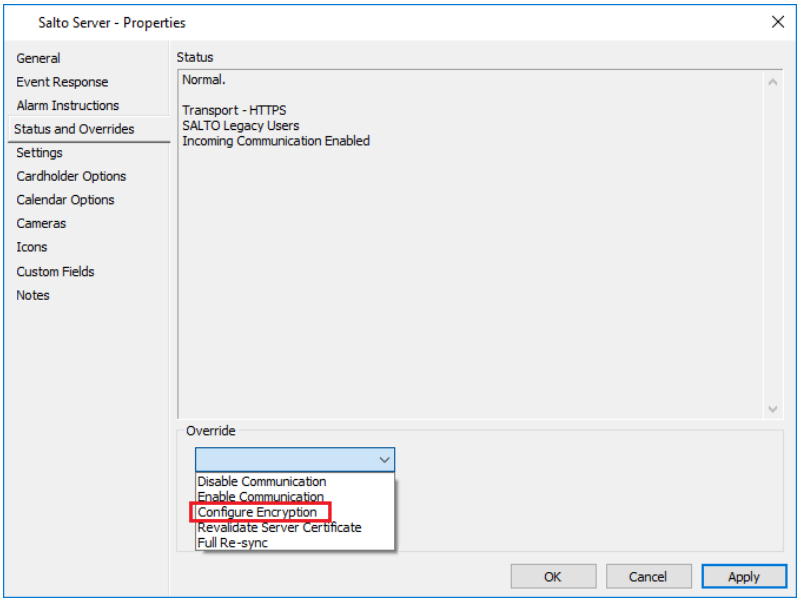
18. Change the ENCODER SETTINGS to "Online" and select the **Salto Ethernet network encoder** from the drop-down list.



Sending MIFARE keys from Command Centre to Salto

By default, Salto Space has no Mifare SAM keys set. The Mifare keys need to be sent from the Command Centre to Salto.

An override exists on the Salto Server **Status and Overrides** property page to send the MIFARE keys that are used for Salto data on cards, from Command Centre to Salto, in order for the keys to be put onto Salto locks. This allows the locks to read cards that are encoded with Salto data.



This override option only appears on the Command Centre server machine while logged in with an operator that has "Manage Keys" privilege. If you log in on a workstation machine with the same operator, the override option will not appear.

Apply the override “Configure Encryption” the Mifare SAM keys are sent from Command Centre to Salto. This should preferably be done before connecting the PPD to any of the Salto devices. If the PPD is plugged into the Salto devices before applying the Mifare SAM keys, the devices will be set with has no Mifare SAM keys and this will then have to be applied at a later stage.

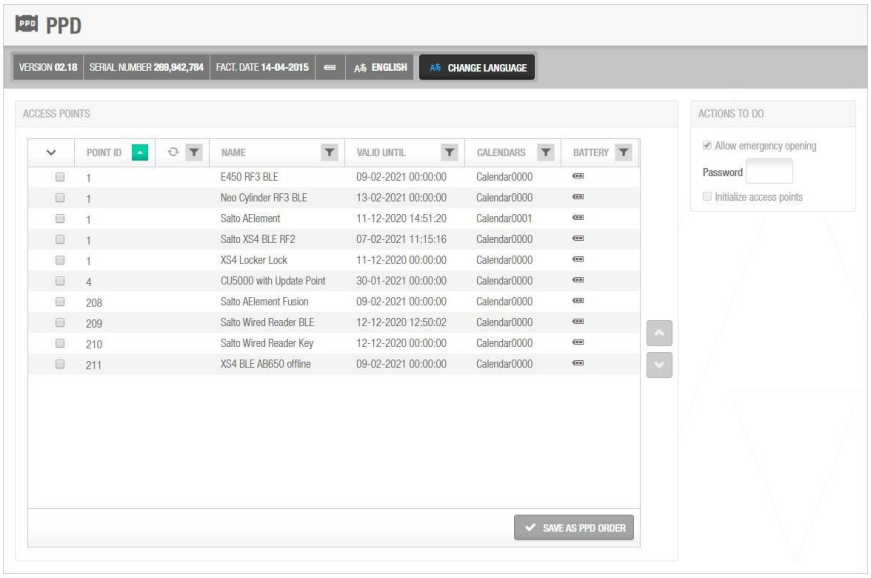
PPD Status

Introduction

This procedure describes how to specify some operating features for Salto Portable Programming Devices (PPDs).
Note: Ensure 'Enable legacy devices' is ticked if you want to use USB communication with your PPD, refer to ***Salto Ethernet Encoders/Dongles*** (on page 74-37).

Procedure

1. In the Salto application, select **System > PPD**.
   The PPD information screen is displayed.



   The PPD information screen displays the Version, Serial number, Factory date (or date of manufacture), Battery status and Language.

2. Configure the fields on this screen for the required set up.

Field / Checkbox	Description
Allow emergency opening	By checking this option, 'Emergency opening' will now be one of the options available on the main menu of the PPD, even after data expiration. **Note:** When this option is selected the **Password** field is enabled. Enter the password required when enabling emergency opening using the PPD. If a password is not entered, the PPD could be misused, if in the possession of an unauthorised person, to open all doors on site.
Initialize locks	By checking this option, 'Initialize locks' will now be one of the options available on the main menu of the PPD.

Salto Doors or ESDs

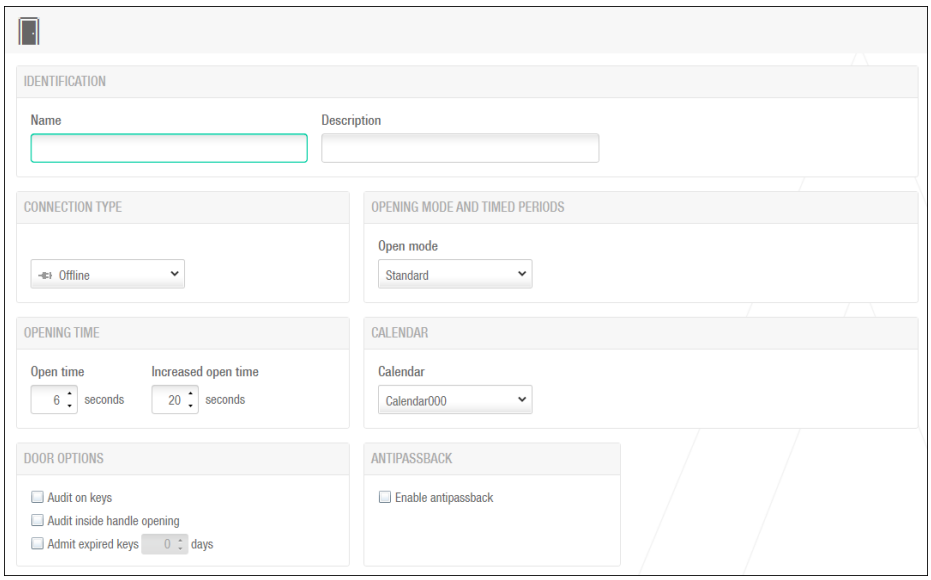
Introduction

This procedure describes how to create the access control for Doors (wired online, non-wired offline and wireless locks) and offline Energy Saving Devices (ESDs) within the Salto application.

Note: Salto Doors and offline ESDs are represented as Salto Door items in Command Centre. Changes made to Salto Door names and descriptions in Command Centre update automatically in Salto without performing an 'Update Access Points', when Salto is online or comes online after being offline. Likewise, Salto Doors can be deleted from Command Centre and the deletion occurs automatically in Salto when Salto is online.

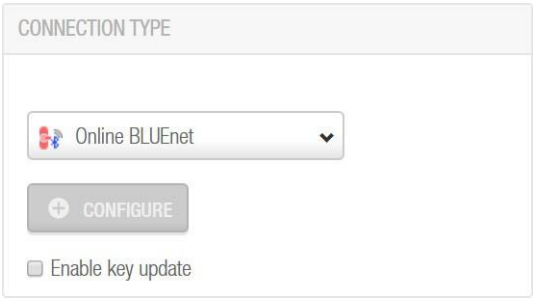
Procedure

1. Select **Access points > Doors**.
   The Doors screen is displayed.
2. Click **Add Door**.
   The Door information screen is displayed.



3. Type in the name of the Door or offline ESD in the **Name** field.
   Notes:
   - Doors and offline ESDs are represented as Salto Door items in Command Centre, so it is recommended that you clearly identify this item, (e.g. Door 1 wired). Characters '@' and '(X)' should not be used in the name field.
   - The Salto Door or offline ESD name must match the Command Centre name. If the names do not match, card events will not show the source and the next 'Update Access Points' will cause the Command Centre item to be deleted.

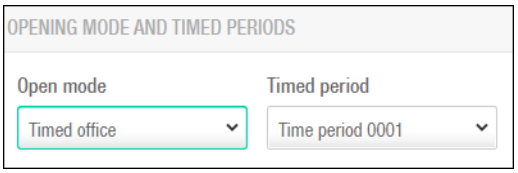
4. Type in a description for the Door or offline ESD in the **Description** field, if required.
   Note: If a description is entered, it will not be replicated to Command Centre during an 'Update Access Points'.
5. Check that the remainder of the fields contain the required set up.

Field / Checkbox	Description
Connection Type	This drop-down provides a list of connection types for the door. The default option is Offline. When you select any other (wireless) connection types from the **Connection Type** drop-down list, a **Configure** button is displayed on the Door information screen. Additional panels are also displayed on the Door information screen, depending on the connection type selected. Connection types are: Offline, Online IP (CU5000), Online IP (CU4200), Online RFnet, Online BLUEnet and Online BAS. **Note:** If you select "Online BLUEnet" as the connection type, an additional **Enable key update** option appears which only applies to BLE locks/readers. Setting this configures the door as an update point. 
Open time	This field determines the time passed from the moment access is granted, until the electronic system locks it again. **Salto Default** = 6 **Command Centre Equivalent** = Door unlock time **Command Centre Default** = 5
Increased open time	Defines a longer opening time. This option is designed for disabled or 'hands full' users. The default time value is 20 seconds. The value can be increased or decreased in the range 0 to 255 seconds. You must enable this option in the user's profile. If extended access time is used in Command Centre, it is then used in Salto as the increased open time. **Salto Default** = 20 **Command Centre Equivalent** = Extended access time **Command Centre Default** = 25

Field / Checkbox	Description
Audit on keys	Allows monitoring of when and where keys are used. You must enable this feature on both the access point and the user's key. When this option is selected, the door is enabled to write or stamp the audit on the key as long as the key's memory is not full. **Salto Default** = Off (should be changed to ON for non-wired offline locks) **Command Centre Equivalent** = Automatic in Command Centre
Audit inside handle opening	Allows monitoring of when a user exits a door. For RF doors, this data is automatically transferred and displayed in the audit trail.
Admit expired keys	The door can be configured to admit cards already expired for a certain amount of days.
Open mode *	This determines the electronic locks working mode. You can select one from the drop-down list provided. **Salto Default** = Standard (can be changed if needed) **Command Centre Equivalent** = Secure - Card and no PIN **Command Centre Default** = Secure - Card and No PIN
Calendar	This drop-down provides a list of the calendar configurations that have been created. This is useful when there are doors in different geographical areas with different calendar configurations. **Salto Default** = Calendar000 **Command Centre Equivalent** = Access Mode in Access Zone **Command Centre Default** = User selected
Enable antipassback	This feature is not supported in Command Centre.

* The options available in the **Open mode** drop-down list are described below, along with the nearest Command Centre equivalent:

Mode	Description
Standard	The lock will only open if you use an authorised key card, within its allowed Timezones. **Command Centre Equivalent** = Secure
Office	The door is unlocked. Access does not require an authorised key card whilst the door is in this mode, however: when using SOLID spindles on Salto door escutcheons, (e.g. Standard European Mortise locks) enabling this mode requires an authorised key card to be presented whilst holding down the INTERNAL door handle. To disable office mode, repeat this procedure. when using SPLIT spindles on Salto door escutcheons (e.g. Australian ANSI Mortise locks), enabling this mode requires an authorised key card to be presented whilst

Mode	Description
	holding down the EXTERNAL door handle. To disable office mode, repeat this procedure. **Command Centre Equivalent** = Override to free
Timed office	This is the same as "Office" mode (above), except that it can only be enabled within specified Time periods. Note that the lock will automatically revert to "Standard" mode at the end of the Timed period. When this option is selected, a new **Timed periods** field appears with a default value of “Time period 001”. You need to select one of the opening periods available from the drop-down list, and then define a period using the **Timed Periods** tool (from the main Salto menu bar).  **Command Centre Equivalent** = Override to free within time-frame
Automatic opening	This is similar to "Timed office" mode (above), but the door can switch to and from office mode automatically without any manual user operation. In this mode, it is also necessary to set a time period (defined with the **Timed Periods** tool). **Command Centre Equivalent** = Scheduled change, (i.e. when a door is scheduled to be secure sometimes and free at others).
Toggle	In this mode, presenting an authorised key card will set the door in "Office" mode, without needing to hold down the inner handle. The next authorised key card presented will cancel "Office" mode. It continues "toggling" the office setting on presentation of each authorised key card. **Command Centre Equivalent** = Free/Secure Double card override
Timed toggle	This mode works in the same way as "Toggle" mode (above), except that you can only toggle the door within a set 'Timed Period'. **Command Centre Equivalent** = No equivalent
Automatic opening + office	This mode is the same as "Automatic opening" mode, except that out of the opening periods, the escutcheon can be left in "Office" mode by a user with this attribute enabled. **Command Centre Equivalent** = Override to free within time-frame.

Mode	Description
Keypad only	Supported in Command Centre. A lock can be opened at any time by entering a valid code on the keypad. The keypad code must contain between one and eight digits and is the same for every user. When you select the **Keypad only** option from the **Open mode** drop-down list, a keypad code field is displayed in which you can define the code. The lock can also be opened with a valid key. A "Code only access granted entry at [Salto Door]" event is raised in Command Centre.
Timed keypad	Not supported in Command Centre.
Key + PIN	Not supported in Command Centre.
Timed Key + PIN	Not supported in Command Centre.
Automatic opening + Office	This mode works in the same way as the Automatic opening mode. However, outside of the timed period, the lock reverts to Office mode rather than Standard mode.
Automatic opening + Toggle	This mode is the same as Automatic + Office mode except that outside of the timed period the lock reverts to the Toggle mode.
Automatic changes	This 'mode' acts as an indication that the lock will work with a mixture of modes during certain time periods throughout the day. The combination of modes is defined in an automatic changes entry, for example, Automatic change#001. You can select an automatic changes entry using the drop-down list in the **Automatic changes** field.

6. Click **Save**.

What happens next?

You will now need to associate a Salto zone with the Door or offline ESD. Command Centre Cardholder access to the Salto zone will provide access to the Door or offline ESD. Salto guest access to the Salto zone will provide access to the Door or offline ESD.

Salto Lockers

Introduction

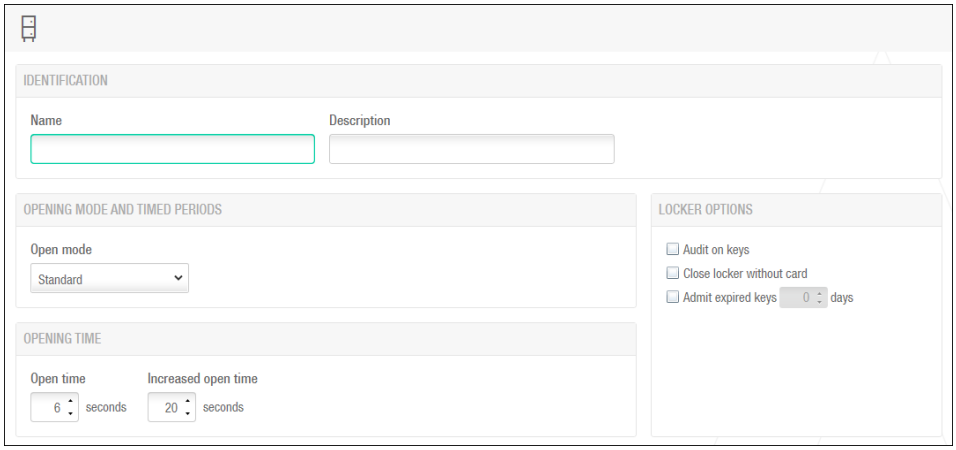
This procedure describes how to create the access control for Lockers within the Salto application.

Notes:

- Salto Lockers are represented as Salto Door items in Command Centre.
- The advanced parameter FREE_ASSIGNMENT_LOCKER allows users to choose any locker from a number of available lockers within a Salto zone. Locker events are mapped through to Command Centre.

Procedure

1. Select **Access points > Lockers**.
   The Lockers screen is displayed.
2. Click **Add Locker**.
   The Locker information screen is displayed.



3. Type in the name of the Locker in the **Name** field.
   Notes:
   - Lockers are represented as Salto Door items in Command Centre, so it is recommended that you clearly identify this item, (e.g. Locker 1). Characters '@' and '(X)' should not be used in the name field.
   - The Salto Locker name must match the Command Centre name. If the names do not match, card events will not show the source and the next 'Update Access Points' will cause the Command Centre item to be deleted.
4. Type in a description for the Locker in the **Description** field, if required.

   Note: If a description is entered, it will not be replicated to Command Centre during an 'Update Access Points'.
5. Check that the remainder of the fields contain the required set up.

Field / Checkbox	Description
Open mode	This determines the electronic locks working mode. **IMPORTANT:** Do not change the default mode of Standard, as the other mode in the drop-down list, (i.e. Automatic opening), is not supported. **Salto Default** = Standard **Command Centre Equivalent** = Secure - Card and no PIN **Command Centre Default** = Secure - Card and No PIN
Open time	This field determines the time passed from the moment access is granted, until the electronic system locks it again. **Salto Default** = 6 **Command Centre Equivalent** = Door unlock time **Command Centre Default** = 5
Increased open time	Defines a longer opening time. This option is designed for disabled or 'hands full' users. The default time value is 20 seconds. The value can be increased or decreased in the range 0 to 255 seconds. You must enable this option in the user's profile. If extended access time is used in Command Centre, it is then used in Salto as the increased open time. **Salto Default** = 20 **Command Centre Equivalent** = Extended access time **Command Centre Default** = 25
Audit on keys	Allows monitoring of when and where keys are used. You must enable this feature on both the access point and the user's key. When this option is selected, the locker is enabled to write or stamp the audit on the key as long as the key's memory is not full. **Salto Default** = Off (should be changed to ON for non-wired offline locks) **Command Centre Equivalent** = Automatic in Command Centre
Close locker without card	Allows a user or a group of users to secure the locker without a key. This is a useful feature for common lockers that are used by a small number of users, for example, medicine cabinets or store cupboards.
Admit expired keys	The locker can be configured to admit cards already expired for a certain amount of days.

6. Click **Save**.

What happens next?

You will now need to associate a Salto zone with the Locker. Command Centre Cardholder access to the Salto zone will provide access to the Locker. Salto guest access to the Salto zone will provide access to the Locker.

Salto Rooms

Introduction

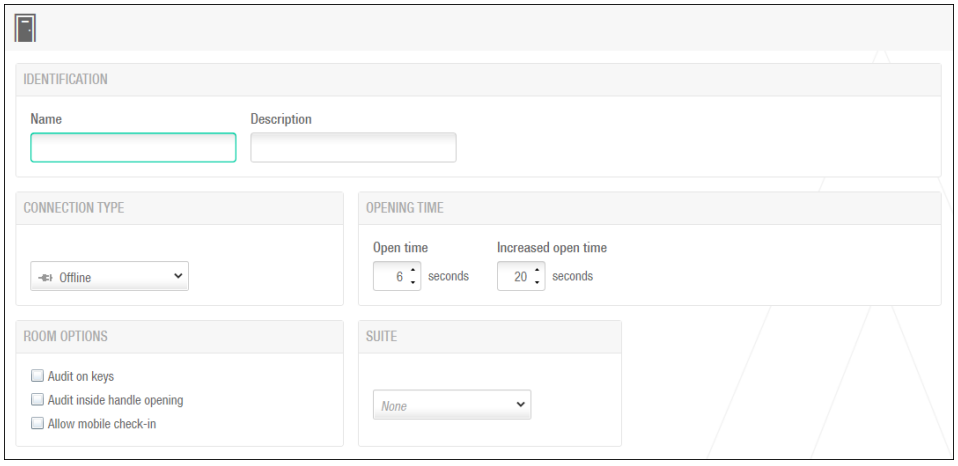
This procedure describes how to create the access control for Rooms (wired online, non-wired offline and wireless locks) within the Salto application.

Rooms are used for hotel guests only. These access points are then made visible to hotel check in operators within the Salto application.

Note: Salto Rooms are represented as Salto Door items in Command Centre.

Procedure

1. Select **Access points > Rooms**.
   The Rooms screen is displayed.
2. Click **Add Room**.
   The Room information screen is displayed.



3. Type a name for the Room in the **Name** field.
   Notes:
   - The Room naming convention must be the same as that used in the hotel PMS system.
   - Rooms are represented as Salto Door items in Command Centre, so it is recommended that you clearly identify this item, (e.g. #808 - Room 8, Floor 8). Characters '@' and '(X)' should not be used in the name field.
   - The Salto Room name must match the Command Centre name. If the names do not match, card events will not show the source and the next 'Update Access Points' will cause the Command Centre item to be deleted.
4. Type a description for the Room in the **Description** field.

Note: If a description is entered, it will not be replicated to Command Centre during an 'Update Access Points'.

5. Select the appropriate configuration options.

Note: The default opening mode for Rooms and Suites is Standard. However, you can change this to Toggle mode in the General options if required. To do so, select the **Toggle** option from the **Open mode** drop-down list in **System > General options > Hotel**. The selected opening mode applies to all external room doors in the hotel. However, it does not apply to doors in sub-suites.

Field / Checkbox	Description
Connection type	This drop-down provides a list of connection types for the room. The default option is Offline. When you select any other (wireless) connection types from the **Connection Type** drop-down list, a **Configure** button is displayed on the Room information screen. Additional panels are also displayed on the Room information screen, depending on the connection type selected. Connection types are: Offline, Online IP (CU5000), Online IP (CU4200), Online RFnet, Online BLUEnet and Online BAS.
Audit on keys	Allows monitoring of when and where keys are used. You must enable this feature on both the access point and the user's key. When this option is selected, the door is enabled to write or stamp the audit on the key as long as the key's memory is not full. **Salto Default** = Off (should be changed to ON for non-wired offline locks) **Command Centre Equivalent** = Automatic in Command Centre.
Audit inside handle opening	Allows monitoring of when a guest exits a room. For RF doors, this data is automatically transferred and displayed in the audit trail.
Allow mobile check-in	Allows mobile guest keys to be used to access a room. Mobile guest keys allow guests to access a room by using the JustIN key app on their mobile phone (instead of a separate physical credential). When you select this option, a **Send key to guest's mobile** checkbox and a **Notification message** field are displayed on the Hotel check-in screen for the room. This option is currently only compatible with smartphones using iOS or Android operating systems.

Field / Checkbox	Description
Open time	This field determines the time passed from the moment access is granted, until the electronic system locks it again. **Salto Default** = 6 **Command Centre Equivalent** = Door unlock time **Command Centre Default** = 5
Increased open time	Defines a longer opening time. This option is designed for disabled or 'hands full' guests. The default time value is 20 seconds. The value can be increased or decreased in the range 0 to 255 seconds. You must enable this option in the user's profile. If extended access time is used in Command Centre, it is then used in Salto as the increased open time. **Salto Default** = 20 **Command Centre Equivalent** = Extended access time **Command Centre Default** = 25
Suite	Selecting a suite from the drop-down list.

6. Click **Save**.

What happens next?

You will now need to associate a Salto zone with the Room. Salto guest access to the Salto zone will provide access to the Room.

Salto Suites

Introduction

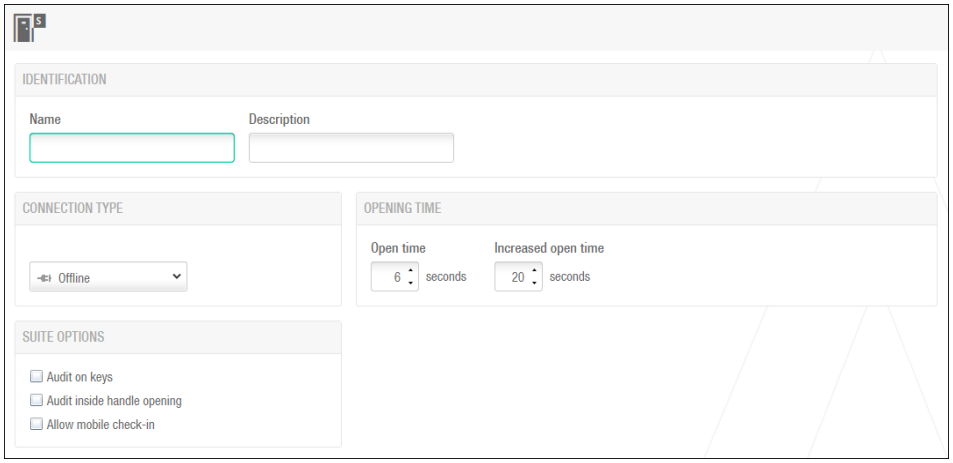
This procedure describes how to create the access control for Suites (wired online, non-wired offline and wireless locks) within the Salto application.

Suites are used for hotel guests only. These access points are then made visible to hotel check in operators within the Salto application.

Note: Salto Suites are represented as Salto Door items in Command Centre.

Procedure

1. Select **Access points > Rooms**.
   The Rooms screen is displayed.
2. Click **Add Suite**.
   The Suite information screen is displayed.



3. Type a name for the Suite in the **Name** field.
   Notes:
   - The Suite naming convention must be the same as that used in the hotel PMS system.
   - Suites are represented as Salto Door items in Command Centre, so it is recommended that you clearly identify this item, (e.g. Suite 1). Characters '@' and '(X)' should not be used in the name field.
   - The Salto Suite name must match the Command Centre name. If the names do not match, card events will not show the source and the next 'Update Access Points' will cause the Command Centre item to be deleted.
4. Type a description for the Suite in the **Description** field.

   Note: If a description is entered, it will not be replicated to Command Centre during an 'Update Access Points'.

5. Select the appropriate configuration options.

   Note: The default opening mode for Rooms and Suites is Standard. However, you can change this to Toggle mode in the General options if required. To do so, select the **Toggle** option from the **Open mode** drop-down list in **System > General options > Hotel**. The selected opening mode applies to all external room doors in the hotel. However, it does not apply to doors in sub-suites.

Field / Checkbox	Description
Connection type	This drop-down provides a list of connection types for the suite. The default option is Offline. When you select any other (wireless) connection types from the **Connection Type** drop-down list, a **Configure** button is displayed on the Suite information screen. Additional panels are also displayed on the Suite information screen, depending on the connection type selected. Connection types are: Offline, Online IP (CU5000), Online IP (CU4200), Online RFnet, Online BLUEnet and Online BAS.
Audit on keys	Allows monitoring of when and where keys are used. You must enable this feature on both the access point and the user's key. When this option is selected, the suite is enabled to write or stamp the audit on the key as long as the key's memory is not full. **Salto Default** = Off (should be changed to ON for non-wired offline locks) **Command Centre Equivalent** = Automatic in Command Centre.
Audit inside handle opening	Allows monitoring of when a guest exits a suite. For RF doors, this data is automatically transferred and displayed in the audit trail.
Allow mobile check-in	Allows mobile user keys to be used to access a suite. Mobile user keys allow users to access a suite by using the JustIN key app on their mobile phone (instead of a separate physical credential). When you select this option, a **Send key to guest's mobile** checkbox and a **Notification message** field are displayed on the Hotel check-in screen for the suite. This option is currently only compatible with smartphones using iOS or Android operating systems.

Field / Checkbox	Description
Open time	This field determines the time passed from the moment access is granted, until the electronic system locks it again. **Salto Default** = 6 **Command Centre Equivalent** = Door unlock time **Command Centre Default** = 5
Increased open time	Defines a longer opening time. This option is designed for disabled or 'hands full' users. The default time value is 20 seconds. The value can be increased or decreased in the range 0 to 255 seconds. You must enable this option in the user's profile. If extended access time is used in Command Centre, it is then used in Salto as the increased open time. **Salto Default** = 20 **Command Centre Equivalent** = Extended access time **Command Centre Default** = 25

6. Click **Save**.

What happens next?

You will now need to associate a Salto zone with the Suite. Salto guest access to the Salto zone will provide access to the Suite.

Salto Zones

Introduction

This procedure describes how to create and configure a Salto zone within the Salto application.

A zone is a specified group of access points that are grouped together to make them easier to manage in the system. For example, a zone could be the doors on the first floor, all the lockers in the gym area, or all the doors in the financial services area.

Note: Salto zones are represented as Salto Access Zone items in Command Centre. Changes made to Salto Zone names and descriptions in Command Centre update automatically in Salto without performing an 'Update Access Points', when Salto is online or comes online after being offline. Likewise, Salto Zones can be deleted from Command Centre and the deletion occurs automatically in Salto when Salto is online.

Procedure

1. Select **Access points > Zones**.
   The Zones screen is displayed.
2. Click **Add Zone**.
   The Zone information screen is displayed.



3. Type in the name of the zone in the **Name** field.
   Notes:
   - Salto zones are represented as Salto Access Zone items in Command Centre, so it is recommended that you clearly identify this item, (e.g. Level 1). Characters '@' and '(X)' should not be used in the name field.
   - The Salto zone name must match the Command Centre name. If the names do not match, card events will not show the source and the next 'Update Access Points' will cause the Command Centre item to be deleted.
4. Type in a description for the zone in the **Description** field, if required.

   Note: If a description is entered, it will not be replicated to Command Centre during an 'Update Access Points'.

5. The **Low zone** checkbox should not be modified unless your locking plan needs more than 96 different zones.
   Zones are classified as 'low' or 'high' according to the way zone information is stored on escutcheons. You can create up to 96 'low' zones, and 928 'high' zones.

   Once this checkbox has been modified and changes saved, it is not possible to modify it again. From the escutcheon point of view, you can make a door belong to a maximum number of 96 'low' zones, but only 20 'high' zones.

What happens next?

You will now need to associate Salto Doors, ESDs, Lockers, Rooms or Suites with the Salto zone. Command Centre Cardholder access to the Salto zone will provide access to the associated items. Salto guest access to the Salto zone will provide access to the associated items.

Salto Outputs

Introduction

This procedure describes how to create Outputs within the Salto application.

In the Salto system, an output is a type of electrical permission or authorization used to activate devices like ESDs or elevators. For example, you can control elevator access to specific floors by creating outputs. If a control unit is connected to a relay extension board, you can use outputs to specify that only a designated user can activate one or multiple relays in an elevator. If you enable Floor 1 and Floor 3 in their access permissions, the user can only access those specific floors and not Floor 2.

Similarly, you can control the energy usage in a room or a floor by creating an output. For example, if you enable an ESD for Room 101, only an authorized key will allow the electrical devices in that room to be switched on.

Procedure

1. Select **Access points > Outputs**.
   The Outputs screen is displayed.
2. Click **Add Output**.
   The Output information screen is displayed.



3. Enter the number of the output in the **Output number** field.
4. Type in the name of the output in the **Name** field.

   Important: The output number matches the number of the relay on the Salto relay extension board.
5. Type in a description for the output in the **Description** field, if required. You may choose to explain the use of the relay in the relay extension board.

What happens next?

You will now need to associate a Salto zone with the Output. Command Centre Cardholder access to the Salto zone will provide access to the Output. Salto guest access to the Salto zone will provide access to the Output.

Salto wired (online) devices

Introduction

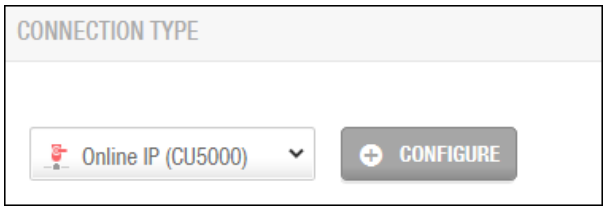
When creating a Salto wired reader with online control unit, you will need to assign an IP address to the control unit and initialise it at the same time.

Before you begin

Before you begin this procedure, ensure you have created the Salto Door within the Salto application.

Procedure

1. On the Door screen, click the **Save** button.
   The **Configure** button becomes enabled.



   Note: The **Update Required** button (located at the top of the screen) can be used to transmit new information to this wired door when changes are made. This button is available once the door has been saved and initialised.

2. Click **Configure**.
   The Peripheral screen displays.



3. Enter the **IP address** you are going to assign to this control unit in your local area network.
   Note: Consult your LAN Administrator if you are not sure which IP address should be given to this device. Ensure the IP address is a valid one that is not already in use by another device.
4. Click **Save**.
5. What type of online control unit are you initialising?

If...	then...
UBOX900003 (update point), UBOX4000 (update point), OR CU50ENSVN (update point with door control)	either: • press the **CLR** button on the control unit circuit for several seconds until the LED starts flashing. • In the Salto application open the 'Monitoring of online locks' screen and click the **Maintenance** tab. • Check the checkbox for the door, then click the **Address** button to send the address to the reader. **Note:** Ensure the LED is flashing on the control unit before addressing the reader. OR initialise the door using the Salto Portable Programming Device (PPD). See ***Initialising a door using the PPD*** (on page 74-64).
CU42E0	Initialise the door using the Salto Portable Programming Device (PPD). See ***Initialising a door using the PPD*** (on page 74-64).

Salto wireless RF devices

Introduction

The Salto network includes items like encoders, gateways, radio frequency (RF) nodes, CU4200 nodes, online doors, and control units. These are added and managed in the Salto application.

Note: Salto ProAccess SPACE supports Salto RF mode 2 only. If using Salto devices that use RF mode 1, please contact your Gallagher representative, as these may need to be replaced.

Procedure

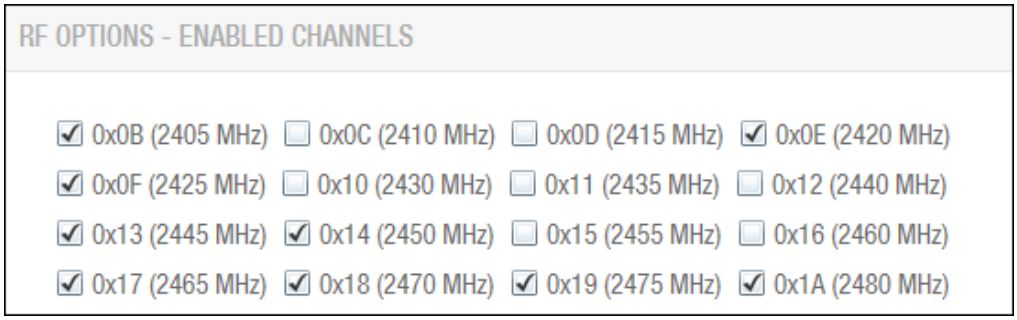
This procedure is split into several smaller procedures to cover the whole process involved in configuring a wireless lock. The procedures, in the order they should be performed are:

- RF channels
- Viewing the Salto network
- Adding an RF gateway
- Adding an RF node

RF channels

You can view the enabled channels for RF signals in the Salto software. To do so, select **System > General options > Devices**. There are 16 channels available and all of these are enabled by default. The frequency range of each channel is also displayed. You can disable a channel if required by clearing the checkbox for the channel and clicking **Save**.

If the site is already utilising wireless RF functionality, (e.g. for wireless internet, RFID applications, etc.) then you will need to carefully select the enabled channels, so that there is no, or minimal crossover of RF signal on site. The scan utility **inSSIDer.exe** which is free to download from the internet, can be used to detect clogged RF channels.



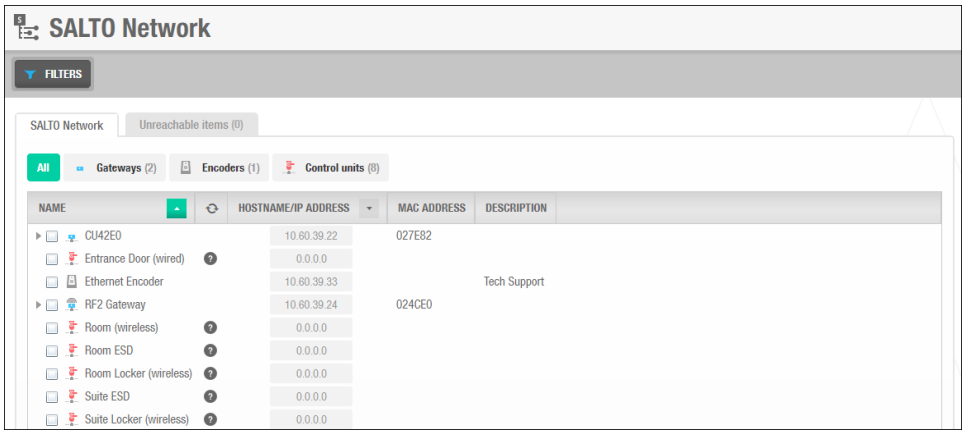
How you know if there is RF crossover?

- It will likely not become apparent until you notice that certain RF escutcheons are either not properly communicating or events are being returned in 'bursts'.
- If there is another RF application utilising the frequencies required by locks or gateways, then the Salto hardware will retain the events/configuration until they are able to utilise the frequencies.

If you do find this type of behaviour on your site, you will need to ascertain what Site Scan Channels are being utilised by non-Salto applications or hardware on site, and de-select those enabled channels accordingly within Salto. This means that the Salto gateways will only use the channels specified, and communication should be constant.

Viewing the Salto network

You can view the list of Salto network items by selecting **System > SALTO Network**.
The Salto Network screen displays a list of all network items that have been added and are currently connected to the system.



The information is displayed in four different filtered views:

View	Description
All	This view shows all of the gateways, encoders, and control units on the system.
Gateways	This view shows RF gateways. When you click the triangular Expand icon on the left-hand side of gateway names, all of the items to which they are connected are displayed. You can view all of the RF nodes and online RF (Salto) access points connected to each RF gateway and all RF gateway nodes.
Encoders	This view shows the encoders on the system
Control units	This view shows online control units (UBOX900003, CU50ENSVN and CU42E0).

Adding an RF gateway

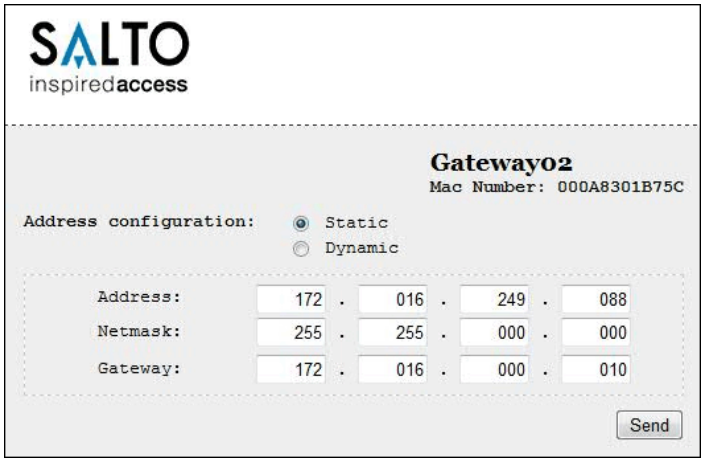
Gateways are hardware devices that provide a link between networks that use different base protocols. RF gateways allow data to be transmitted from the system to the Salto RF locks, and from the RF locks to the system. RF gateways control RF nodes.

You must physically connect RF nodes to an RF gateway using an RS485 cable to establish communication between the RF nodes and the RF gateway. You must also connect RF nodes and RF gateways in the Salto application so the system can show which nodes and gateways are connected.

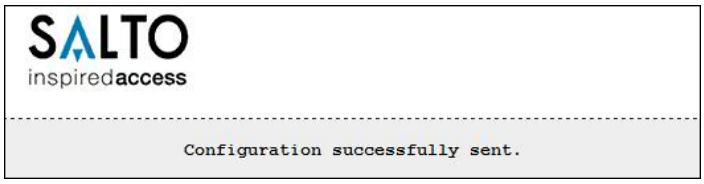
1. Select **System > Salto Network**.
   The Salto Network screen is displayed.
2. Click **Add Network Device**.
   The Add network device dialog box is displayed.
3. Select **RF gateway** from the drop-down list, then click **OK**.
   The RF gateway information screen is displayed.



4. Enter a name for the RF gateway in the **Name** field.
5. Enter a description for the RF gateway in the **Description** field, if required.
6. Type the media access control (MAC) address in the **MAC address** field.
   Note: This is usually displayed on the Ethernet board of the RF gateway.
7. Select either the **Network name (DHCP)** or **IP address** option.
   If you select the **Network name (DHCP)** option, this automatically assigns an IP address to the RF gateway. A Dynamic Host Configuration Protocol (DHCP) server and a DNS are required for this option. If you select the **IP address** option, you must type a static IP address in the field.
8. To address the Gateway RF2, connect the Gateway to the LAN (do not use a crossed cable). Press the **CLR** button on the Gateway RF2 circuit board for several seconds until the LED turns orange.
9. Using a Web Browser, access the IP address **192.168.0.234** and enter the IP address of the Gateway RF2 and select the **Static** Address configuration radio button.
   To ensure you can communicate to the Gateway RF2 set your configuration PC to an IP address of **192.168.0.1**.



10. Ensure the LED is flashing on the Gateway RF2 circuit board, then click the **Send** button. The 'Configuration successfully sent' screen displays. The IP address is assigned and the device has been initialised at the same time.



Note: Gateway RF2s are compatible with PoE routers. For more information consult the Salto Gateways technical documentation.

11. Click **Add/Delete** in the RF Nodes panel.
The Add/Delete dialog box, showing a list of RF nodes is displayed.

    The Add/Delete dialog box only displays RF nodes if you have already added them to the system. You can also connect RF nodes to RF gateways when you add RF nodes to the system.

12. Select the required RF node in the left-hand panel and click the chevron.
The selected RF node is displayed in the right-hand panel.
Note: You can hold down the Ctrl key while clicking the RF nodes to make multiple selections. You cannot add RF nodes that already belong to another gateway.

13. Click **Accept**.
The selected RF node is displayed in the RF Nodes panel.

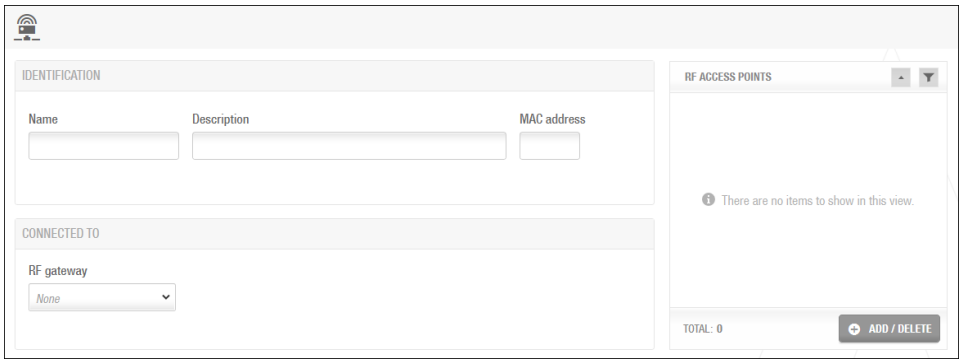
14. Click **Save**.

Adding an RF node

RF nodes are network connection points that are physically connected to an RF gateway using an RS485 cable. This establishes communication between the RF nodes and the RF gateways. In the Salto application you must connect RF nodes to RF gateways, and RF access points to RF nodes. This means that the system can show which items are connected.

Note: You must select **Online RF (SALTO)** in the Connection Type panel on the Door or Room information screen to define a door as an RF access point.

1. Select **System > SALTO Network**.
   The SALTO Network screen is displayed.
2. Click **Add Network Device**.
   The Add network device dialog box is displayed.
3. Select **RF node** from the drop-down list, then click **OK**.
   The RF node information screen is displayed.



4. Type a name for the RF node in the **Name** field.
5. Type a description for the RF node in the **Description** field.
6. Type the MAC address of the antenna in the **MAC address** field.
7. Select the RF gateway to which you want to connect the RF node from the **Connected to** drop-down list. The default option is **None**.
8. Click **Add/Delete** in the RF Access Points panel.
   The Add/Delete dialog box, showing a list of RF access points is displayed.

   The Add/Delete dialog box only displays RF access points if you have already defined doors as RF access points by selecting **Online RF (SALTO)** in the Connection Type panel on the Door or Room information screens. You can also connect online RF (SALTO) doors to RF nodes by using the **Connected to** field on the Online RF information screen.
9. Select the required RF access point in the left-hand panel and click the chevron.
   The selected RF access point is displayed in the right-hand panel.
   Note: You can hold down the Ctrl key while clicking the RF access points to make multiple selections. You cannot add RF access points that already belong to another RF node.
10. Click **Accept**.
    The selected RF access point is displayed in the RF Access Points panel.
11. Click **Save**.
    Note: RF gateways have a mini node connected to them. You must add this node in the Salto application by following the procedure above.

Initialising a door using the PPD

Introduction

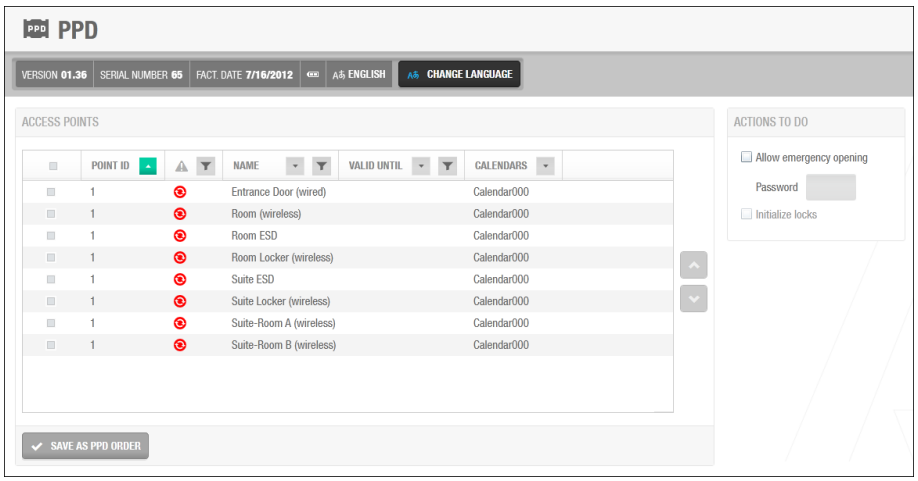
The Portable Programming Device (PPD) allows data to be transferred between the operator's PC and the locks. Data is downloaded from the PC to the PPD, and the PPD is used to perform tasks such as lock initialization and emergency openings.

Before you begin

- It is important that the time is set correctly for the PC on which the Salto software is running, as this controls the time and date settings for locks.
- The locking schedule configured in Salto will be transferred to the door when the door is initialised.
- If you initialize a lock that is already in use, its audit trail is deleted.
- If the Salto Local IO Bridge software has not been installed, the installer will launch when a USB device is connected to Salto ProAccess SPACE.

Procedure

1. Connect the PPD to the Salto server.
2. On the PPD, switch the **Power** button on.
   The screen on the PPD displays the main menu with the options available.
3. In the Salto application, select **System > PPD**.
   The PPD information screen is displayed.

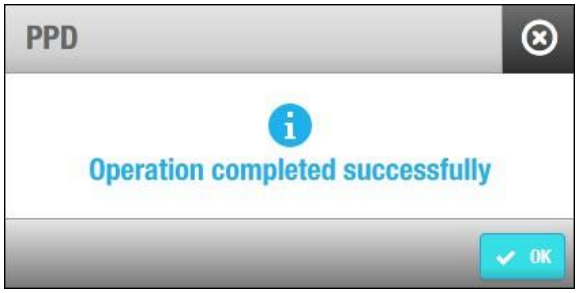


Note: It is not compulsory to initialise all of the doors simultaneously, although it is highly recommended not to leave any pending doors.

4. Select the checkbox of the access point for which you want to initialize the lock.
   You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar.

Note: By selecting **Initialise locks**, this will now be one of the options available on the main menu of the PPD.

5. Select the **Initialise locks** checkbox in the Actions To Do panel.
6. Click the **Download** button.
   The PPD progress screen is displayed.
7. Wait for the download to complete. A pop-up is displayed confirming that the operation was completed successfully.



8. Disconnect the PPD from the PC and take it to the door to initialise it.
9. Connect the 3 pins cable to the PPD. This cable has 3 conductors on one end and an RJ11 phone connector on the opposite end.

   Bluetooth PPD's do not connect by pins, so if you have a Bluetooth PPD hold it near the lock.
10. Turn the PPD on by pressing the red key once.
11. To initialise the door:
    a) Turn the PPD on by pressing the 'red' key once.
    b) From the PPD main menu, select the **Initialize Lock** menu option.
       The Door list displays.
    c) Select the door that you want to initialiase.
       Note: Take extra care that you are selecting the correct door, as the door names have a limited length.
    d) When the name of the door displays on the PPD screen, press the **OK** button on the PPD.
       The message *"Connect to lock"* displays on the PPD.
    e) Press and hold the **CLR** button on the hardware you are initialising.
    f) Insert the 3 pins cable into the lock reader.
       A progress bar displays on the PPD screen, a sharp beep sound is emitted and the LED turns red, indicating that the data transfer is in progress. The message *"Initialized"* displays on the PPD, once the door has been initialised.

       Note: If the communication is interrupted for longer than three seconds, you will need to repeat the communication, (i.e. reconnect the PPD).
12. Once you have initialised the door, reconnect the PPD to the PC using the USB cable and select **System > PPD**. This will update the software data comparing it with actual battery status values, as well as pending updates.

Audit Trail (collecting door opening data using the PPD)

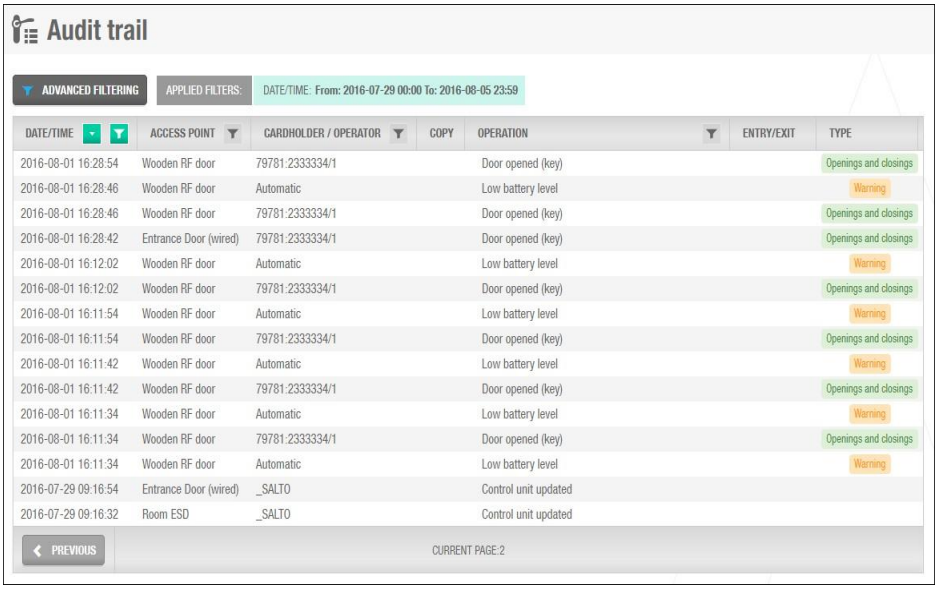
Introduction

It is possible to know who has opened a door and at what time, by performing an audit trail on the door using the Portable Programming Device (PPD). This procedure describes how to audit a door (wireless lock only).

Note: You can filter the audit trail data by event date/time, access point, user/operator, operation, and/or type

Procedure

1. Take the PPD and go to the door to be audited.
2. Turn the PPD on by pressing the 'red' key once.
3. From the PPD main menu, select the **Collect Openings** menu option.
4. Press the 'green' key to validate the choice.
   The message *"Connect to lock"* displays on the PPD.
5. Connect the PPD to the lock using the communication cable.
   Data transfer takes place.
6. Go back to the Salto server and connect the PPD to the USB port.
7. If the message *"Connect to lock"* displays on the PPD, press the 'red' key to go back one menu level.
   Note: If you do not do this step, you will not be able to communicate with the Salto server.
8. In the Salto application select **System > PPD**.
   The PPD information screen is displayed. The Audit Trail information screen is automatically updated with the information from the connected PPD when you display the PPD information screen.
9. Select **Monitoring > Audit Trail**.
   The Audit trail information screen, showing the new audit trail data is displayed.



Note: Any failed opening attempts, (e.g. someone attempts to open a door they do not have access to), display in 'red'.

10. Use the remainder of the buttons as (and if) required.
    Note: Once these events have been uploaded to the Salto server they will be automatically synchronised in Command Centre.

Button	Description
Advanced filtering	By clicking this button you are able to filter events to find specific information.
Purge	It is recommended that you make audit trail purges at least once a month. When the audit trail is not too full, all the communications with the wired units are faster, (i.e. communication with the Control Units, upload and download of PPD data.
Print	This button allows you to have all the information in the audit trail printed on paper.

Enable mobile audit trail for Salto offline doors/locks

Introduction

Support for audit trails when using mobile credentials has been added in version vEL9.00 of command centre. This allows reporting of cardholder door access events via the Command Centre Cloud for Salto offline doors/locks, similar to using cards with an update point.

When the pre-requisites are fulfilled, cardholder mobile credentials will be issued a Salto key with the appropriate settings to enable this feature. Audit trails will be sent from Mobile Connect to Command Centre Cloud and received by the site.

Note: Exisitng sites will need to wait until their cardholder's Salto key expires, which is typically the next day, but may take up to the key revalidation limit that is 7 days by default, and can be configured in the "Normal Card Access" field in the Settings page of the Salto Server's properties.

This feature can be enabled site wide and enabled per-cardholder. The default for new installations and existing sites on upgrade is enabled.

Prerequisites

- Gallagher Command Centre Cloud must be connected.
  Refer to ***Connecting to the Cloud*** (on page 28-7) for further detail.
- Salto offline door must have "Audit on keys" enabled.
  Refer to ***Salto Doors or ESDs*** (on page 74-41) for further detail.
- Salto Mobile Events must be enabled in Command Centre in the Salto Server item (on by default).
- Salto Mobile Events must be enabled per cardholder (on by default).

Limitations

Similar to audit trails in cards reported via update point, cardholder events via Mobile Connect are not guaranteed to be reported. Mobile connect will attempt to retry if the cardholder has no active internet connection at the time of access.

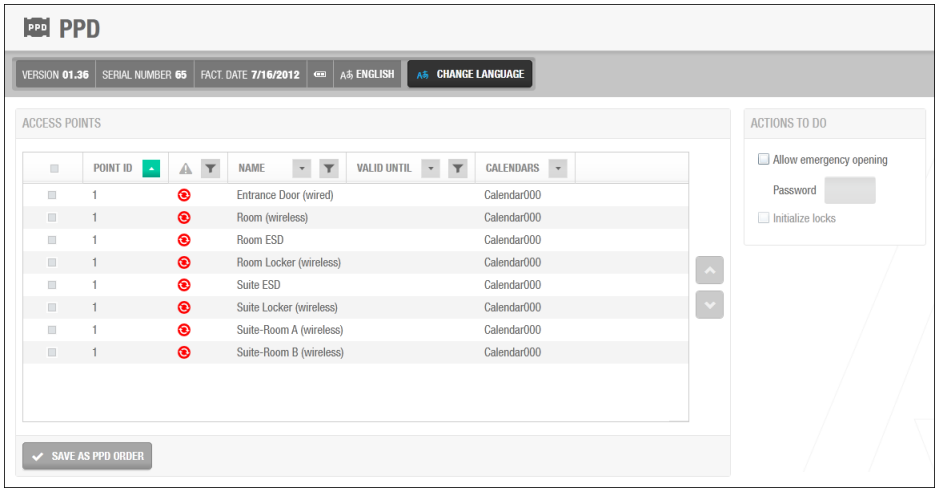
Emergency Opening

Introduction

This procedure describes how to perform an emergency opening. This may be necessary if the battery for a door electronic lock goes flat.

Procedure

1. Connect the PPD to the Salto server.
2. On the PPD, switch the **Power** button on.
   The screen on the PPD displays the main menu with the options available.
3. In the Salto application, select **System > PPD**.
   The PPD information screen is displayed.



4. Select the checkbox of the access point for which you want to perform the emergency opening.
   You can select more than one access point if required. However, you cannot select access points with different calendars; multiple selections must be controlled by the same calendar.
5. Select the **Allow emergency opening** checkbox in the Actions To Do panel.
   The checkbox is greyed out if you have set emergency opening as a default option in the General options. Otherwise, you must select it each time you want to perform an emergency opening.
6. Type a password for the emergency opening in the **Password** field, if required. If you type a password, you must enter this password in the PPD before you can perform the emergency opening. If a password is not entered, the PPD could be misused, if in the possession of an unauthorised person, to open all doors on site.
   Notes:
   - Your PPD firmware must be version 01.29 or higher to use this option.

- The password can only contain digits.
- The **Password** field is greyed out if you have set emergency opening as a default option in the General options and entered a password there already for the option
- If the **Password** field is left blank, no password will be required for emergency openings (not recommended).

7. Click the **Download** button.
   The PPD progress screen is displayed.
8. Wait for the download to complete.
   A pop-up is displayed confirming that the operation was completed successfully.
9. Click the **OK** button.
   You can now use the PPD to perform an emergency opening of the selected access point by selecting **Emergency Opening** in the PPD's menu and connecting the PPD to the lock.
10. Insert the 3 pins cable into the lock reader. You will hear the lock engine sound, and in a few seconds the door is ready to be opened. The message *"Door open, room number"* displays on the PPD.

    Note: If a password has been set, before the PPD will open the door, you will be prompted to enter the password. The PPD will display the message *"Insert password"*. Using the up and down arrows look for the digits of the password. When found click the **OK** key and the digit will be replaced by a star. Look for the next digit of the password using the same process. Once the last digit of the password has been introduced, click the **OK** key and the door will open.

    If the reason you had to use the PPD for an emergency opening is that the door's batteries have gone flat, then it is recommended that you replace lock batteries of the newly opened door immediately. Salto locks are equipped with three alkaline batteries, depending on which lock type you purchase, (i.e. LR03 AAA, 1.5 V model). After battery replacement, you must update the electronic lock with the PPD, as the internal clock stopped and the Time Zones and Calendar settings were lost when the batteries ran out.

Other Salto Configuration

There are a number of other Salto configuration procedures that you may or may not need to perform. They are:

- Defining Calendars
- Defining Access Point Timed Periods
- Configuring Daylight Saving Time (enabled by default)
- Enabling Access Point Automatic Changes
- Defining Access Point Lock Settings
- User Card Cancellation
- Managing the Blacklist
- Automatic Audit Trail Purging
- Automatic System Auditor Purging
- Automatic Database Backups
- Defining Bluetooth settings for Gallagher Mobile Connect App
  For further detail, see ***SALTO Mobile Access Integration*** (on page 31-19).

***** Refer to your *Salto ProAccess SPACE User Manual* for information about the above procedures or any additional configuration that you require.

Forced Door and Door Open Too Long alarms

If you require Command Centre to generate 'Forced Door' and 'Door Open Too Long' alarms from Salto wired readers (Salto update point with relays), configure the following:

1. Set up a dummy door in Command Centre, with Door Lock open and Lock inputs physically connected to the door hardware.
2. The door lock relay for the Salto wired door must be connected to and defined as a push-button door release input on the dummy door.
3. The dummy door must have the door open/door locked inputs brought in via the Gallagher Controller. Therefore, the Salto wired readers need to be close enough to a Gallagher Controller to be able to bring in the door monitoring inputs

Command Centre Site Configuration

You will need to configure user access using Command Centre. There are a number of procedures that need to be performed in Command Centre. They are:

- ***Opening the Salto List Window*** (on page 74-72)
- ***Editing the Salto Server*** (on page 74-73)
- ***Performing Overrides on the Salto Server*** (on page 74-76)
- ***Salto Full Re-sync*** (on page 74-79)
- ***Configuring Access Groups*** (on page 74-80)
- ***Updating Access Points*** (on page 74-82)
- ***Configuring Salto Doors*** (on page 74-84)
- ***Configuring Salto Access Zones*** (on page 74-86)
- ***Configuring Salto options for Cardholders*** (on page 74-88)
- ***Configuring access to Salto Outputs*** (on page 74-89)
- ***Encoding cards*** (on page 74-91)
- ***Adding Salto to the URL Tile*** (on page 74-105)
- ***Door Icons*** (on page 74-106)
- ***Salto Key Assignment*** (on page 74-107)

Opening the Salto List Window

Introduction

The Salto-specific List Window displays the Salto Server and any Salto Doors, ESDs (Energy Saving Devices), Lockers, Rooms, Suites and Access Zones that have been created within the Salto application.

The Salto Server is the single parent item and all Salto Doors, ESDs, Lockers, Rooms, Suites and Zones appear as children of that parent.

Procedure

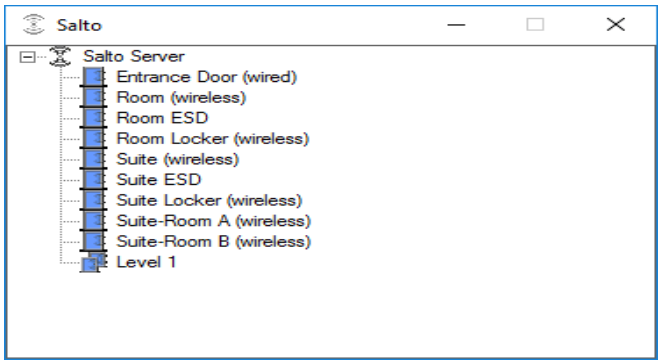
1. Click **Configure** from the menu bar.
2. Click **Salto**.

Result

The Salto List Window displays.

To refresh the Salto List Window, **right click** on the Salto Server and select **Update Access Points**.
The Salto List Window will be updated to display any Salto Doors, ESDs, Lockers, Rooms, Suites and Access Zones.

Immediately upon connecting to Salto server the Salto List Window lists Doors under their assigned Zone if they belong to only one Zone.



The "Salto Server" item is automatically created when the Command Centre Service starts, if it does not already exist, and the license file contains a count of Salto Doors that is greater than zero, (i.e. Salto Doors=nnn in the [Limits] section of the license file). It is initially named "Salto Server", and is placed in the Root Division, though the division can be changed later. There can only be one of this item, and it cannot be deleted.

Note: The "Salto Server" item can be placed in the Status Viewer, used on Site Plans, and in Site Configuration Reports.

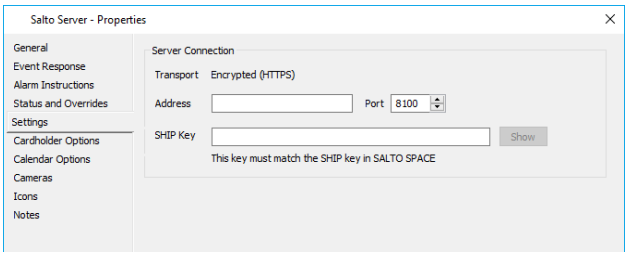
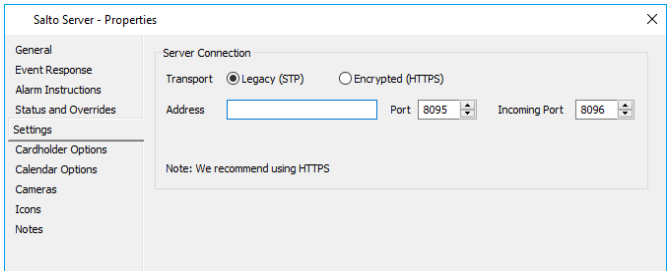
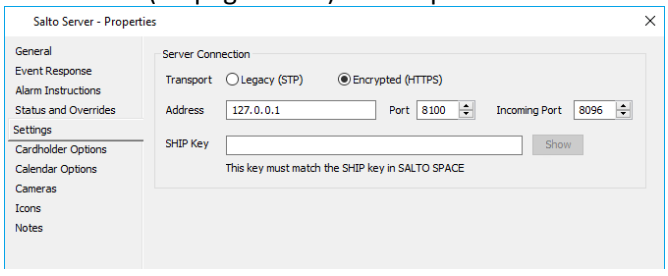
Editing the Salto Server

Introduction

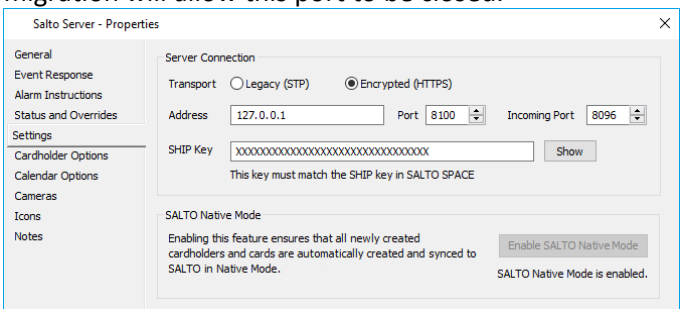
Operators require the "Edit Site" privilege in a division to be able to modify the Salto Server item.

Procedure

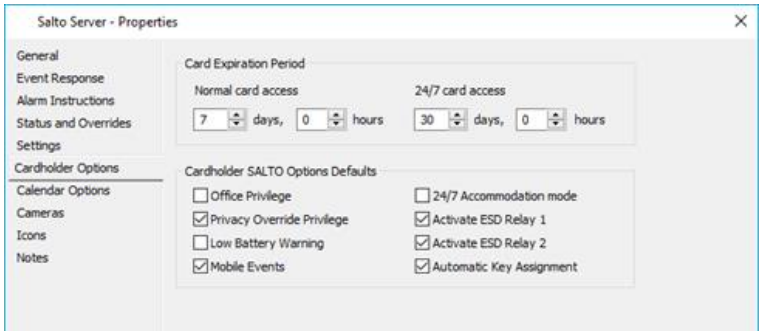
1. Click **Configure** from the menu bar, then **Salto**. The **Salto** List Window opens.
2. **Right click** on the Salto Server and select **Properties**.
3. Click the **Settings** tab.
   How this screen looks depends on whether this is a new or an existing site.

If…	then…
a new site,	**Encrypted (HTTPS)** is the default "Transport" connection. If your site chooses to use Salto Native Mode. Before changing connections to HTTPS, settings from the Salto server side need to be changed. Refer to ***Salto Server Connection*** (on page 74-24) for the procedure. 
an existing site,	there are two "Transport" options to choose from, i.e. **Legacy (STP)** & **Encrypted (HTTPS)**. Select the appropriate "Transport" radio button. • **Legacy (STP) Transport with Legacy Mode:** This option is available for STP (TCP/IP) connection, however it is recommended to use the **Encrypted (HTTPS)** option to secure communication.  • **Encrypted (HTTPS) Transport with Legacy Mode:** If your site chooses to use Salto Native Mode, this option must first be selected. Before changing connections to HTTPS, settings from the Salto server side need to be changed. Refer to ***Salto Server Connection*** (on page 74-24) for the procedure. 

If…	then…
	• **Encrypted (HTTPS) Transport with Native Mode:** After the site enabled Native Mode, the Server Connection page will still display the incoming port so that existing Legacy Mode cards can use the STP connection. Completing Native Mode card migration will allow this port to be closed.



4. The single Salto Server Command Centre item has the following properties which are valid for the Server only:
    1. **Address** of Salto Server (default = empty). This needs to be changed to the Server name or IP Address for the Server running the Salto application, if the Salto Server does not reside on the same PC as the Command Centre Server. It can take up to approximately ten seconds for the Salto server to come online after configuring or re- configuring the Name / IP-Address.
    2. **Port** is the port for outgoing requests to Salto Server (Default to 8100 for Encrypted HTTPS and 8095 for Legacy STP).
    3. **Incoming Port** is the port for incoming STP requests from Salto Server (Default to 8096).
5. Click the **Cardholder Options** tab.



6. Set the **Card Expiration Period** settings as appropriate:
    - **Normal card access** is the period of time a card can be used until such time as an update at a Salto wired lock is required (Default is 7 days).
    - **24/7 card access** is the period of time a card can be used, ignoring all Schedules and Day Categories, (e.g. Public Holidays) until such time as an update at a Salto wired lock is required (Default is 30 days).
7. The single Salto Server Command Centre item also has the following properties to set default values for items which are configured by Cardholder:
    - **Office Privilege** defaults to “Off”.
      The Office Privilege enables a Cardholder to override a Salto lock to "Office" (Command Centre Equivalent = Override to Free) mode, when the lock is scheduled to allow this override (Office mode).

- **Privacy Override Privilege** defaults to “On”.
  The Privacy Override Privilege relates to locks that come fitted with an internal privacy button, disallowing Cardholders from entering while this button is pressed. Those with the Privacy Override Privilege will be able to enter through locks that have this button activated.
- **Low Battery Warning** defaults to “Off”.
  This setting defines whether or not Low Battery events are written to card-holders' cards, as default. Cards must be formatted with 6 or more sectors in order for this event to be passed to the cards.
- **Mobile Events** defaults to “On”.
  When checked, if a cardholder gains access via the Mobile App, even if the Salto door is offline, events will go through to the Cloud and then to Command Centre.
  Note: This feature will have a small delay in activating upon upgrading from a previous Command Centre version. The settings will go out with the next Salto key update, which is typically the next day. Users that are offline will not get the update though, and it may take up to 7 days for all users to get the key update as the expiry for the key is 7 days.
- **24/7 Accommodation mode**
  There are two operating modes available - **"Normal"** and **"24/7 Accommodation"** modes. The system default is Normal mode, (i.e. the 24/7 Accommodation mode checkbox is not checked.
  In both modes there is a default number of days that cards must be able to work at Salto wireless readers before the card must be badged at a Salto wired reader in order to maintain their access rights for Salto doors. This period is measured from the start of the day the card was last updated at a Salto wired reader.
  Default for Normal mode is 7 days between wired updates but can be configured to be less or more than this (valid range is 1 hour to 999 days).
  "24/7 Accommodation" mode ignores all schedules in Command Centre and therefore allows longer periods than 7 days to be specified before cards have to visit a wired reader. Default for this mode is 30 days (same as default expiry in Salto application) but can be configured to be up to 365 days (valid range is 1 hour to 365 days).
- **Activate ESD Relay 1 and 2** default to "On".
  A Salto Door Command Centre item may correspond to a Salto ESD (Energy Saving Device).
- **Automatic Key Assignment**
  When checked, the Automatic Key Assignment feature is enabled from Salto for a cardholder. Refer to ***Salto Key Assignment*** (page 74-109) for further detail.

8. Click the **Calendar Options** tab.
   This tab applies to Salto Native Mode only. Therefore, if your site is using Legacy Mode, refer to ***Changing to HTTPS connection in Command Centre*** (on page 74-26) for the procedure.
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.

Result

The settings of the Salto Server have been modified and will take effect after saving the changes.

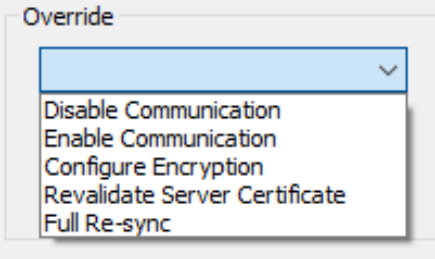
Performing Overrides on the Salto Server

Introduction

This procedure describes how to perform an override on the Salto Server from Command Centre.

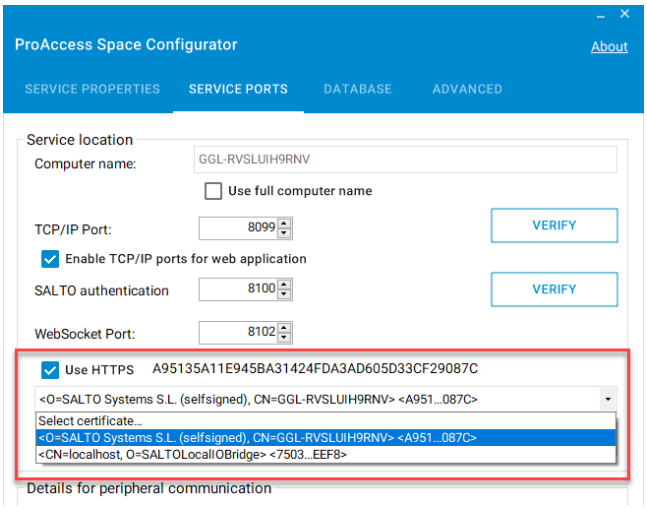
Procedure

1. Click **Configure** from the menu bar, then **Salto**.
   The **Salto** List Window opens.
2. **Right click** on the Salto Server and select **Override…** from the drop-down menu. The **Status and Overrides** tab displays.
3. Click within the **Override** field and select the appropriate option from the drop-down list.



4. Select the required Override option.

Override option	Description
Disable Communication	This disconnects the Salto Server from Command Centre from the Salto Space Server, and remains that way until you "Enable Communication". Cardholders can still badge their card and get access to the Salto door, however, there are no access granted events. All access granted events are displayed after communication is re-enabled.
Enable Communication	The Salto Server from Command Centre re-establishes communication. All the events which are from the period of time the "Disabled Communication" override was in place will display.
Configure Encryption	This allows Salto locks to read MIFARE cards that are encoded by Command Centre with Salto data. This override only needs to be performed once, after upgrading to Salto Space. Refer to ***Performing a Configure Override on the Salto Server*** (below) for full details.

Override option	Description
Revalidate Server Certificate	This override is only applicable to sites using HTTPS connection. When the **Salto ProAccess Space Configurator** certificate changes, the Command Centre Salto Server loses connection to Salto Space. Applying a "Revalidate Server Certificate" override re-establishes the connection. 
Full Re-sync	This override is only applicable to sites using the Salto Native Mode. Refer to ***Salto Full Re-sync*** (on page 74-79) for full details.

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

Result

The Salto Server is overridden.

Note: Another type of override that can be performed on the Salto Server is an "Update Access Points" override. Refer to ***Updating Access Points*** (on page 74-82) for further information.

Performing a Configure Encryption Override on the Salto Server

Introduction

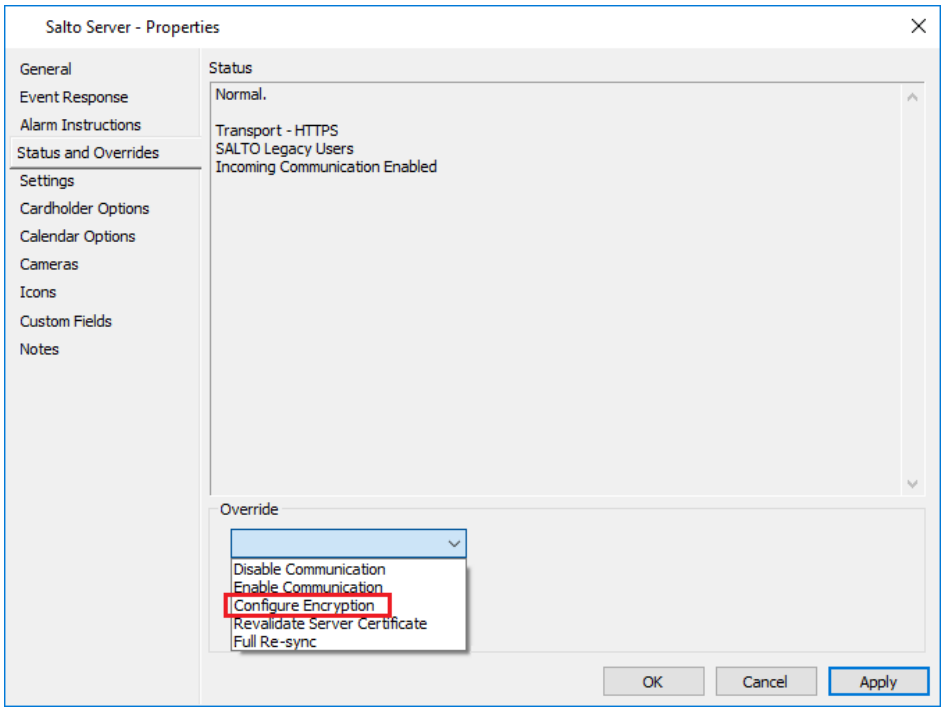
The Configure Encryption override allows Salto locks to read MIFARE cards that are encoded by Command Centre with Salto data. This override only needs to be performed once, after upgrading to Salto Space.

Operators require the "Manage Keys" privilege in a division to perform an encryption override on the Salto Server. Please ensure this override is actioned before configuring or initialising any Salto Readers.

Configure Encryption overrides can only be performed on the PC that has Command Centre Server installed.

Procedure

1. Click **Configure** from the menu bar, then **Salto**.
   The **Salto** List Window opens.
2. **Right click** on the Salto Server and select **Properties**.
   By default the **General** tab displays.
3. Click the **Status and Overrides** tab.



4. Select **Configure Encryption** from the Override drop-down menu.
5. Click the **Override Now** button.
6. 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. Any Salto doors/locks displaying the symbol in Salto SPACE need to be updated, and any locks that will not read cards encoded with Salto information via Gallagher Command Centre, will need to be re-initialised.

Salto Full Re-sync

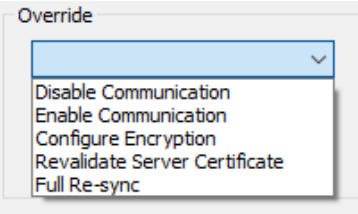
Introduction

This procedure describes how to re-sync the Salto Server in Command Centre, so that all Salto cardholder related items will be mapped to Salto Space.

Note: The "**Full Re-sync**" override is only applicable to sites using the Salto Native Mode.

Procedure

1. Click **Configure** from the menu bar, then **Salto**.
   The **Salto** List Window opens.
2. **Right click** on the Salto Server and select **Override…** from the drop-down menu. The Status and Overrides tab displays.
3. Click within the **Override** field and select "**Full Re-sync**" from the drop-down list.

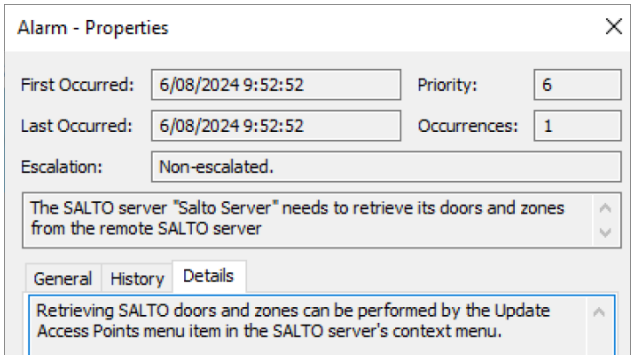


4. Click the **Override Now** button.
   From this screen you can see the status change as a result of the override.
5. Click the **OK** button.

Result

The Salto Server is overridden, and a "GallagherCommandCentre" partition is created in Salto Space which will be used to separate Command Centre created/used items from other items in Salto.

Note: A Full Re-sync may fail if the Salto server needs to retrieve its access points, (i.e. Doors and Access Zones) into Command Centre.
If a resync fails for this reason, the following alarm will be generated and an "Update Access Points" override is required. Refer to ***Updating Access Points*** (on page 74-82) for full details.



Configuring Access Groups

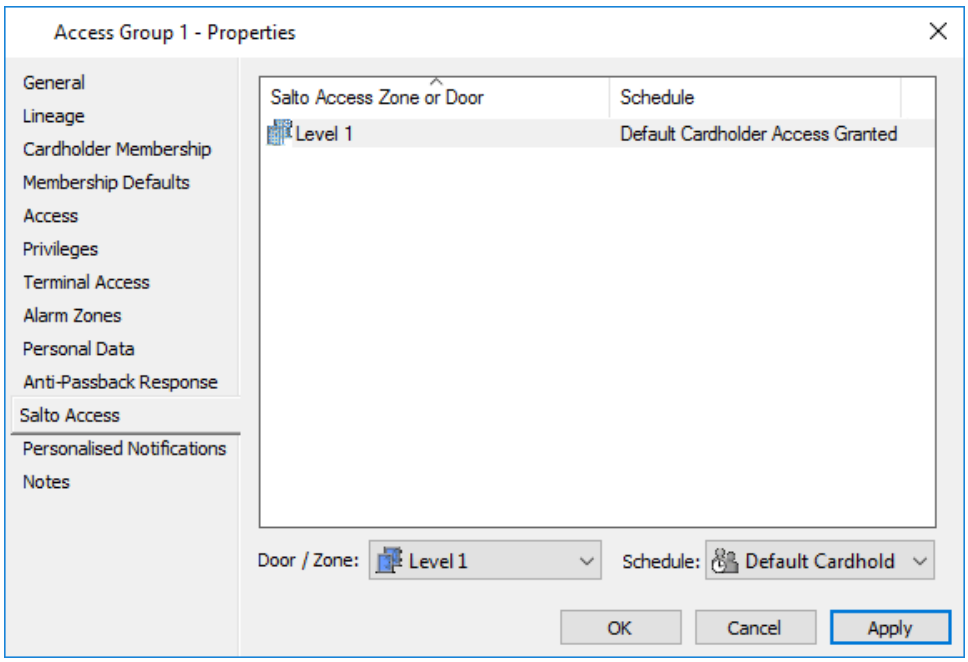
Introduction

A Salto Access Triplet is the relationship between an Access Group, a Salto Access Zone or Salto Door, and a Schedule. These appear as rows on the Salto Access tab of an Access Group.

This procedure describes how to configure an Access Group in Command Centre to accommodate a Salto Access Triplet.

Procedure

1. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).
2. **Right click** and select **New...Access Group**.
3. Configure the new Access Group as required.
   See ***Setting up Access Groups*** (on page 34-4) for further detail.
4. Click the **Salto Access** tab.
   Note: This tab is only available if your site is licensed for one or more Salto Doors.



5. Click **Configure** from the menu bar, then **Salto**.
   The **Salto** List Window opens.
6. Select those Salto Access Zone(s), Salto Door(s), Salto ESD(s), Salto Room(s), Salto Suite(s), or Salto Locker(s) appropriate for this Access Group.
   Drag and drop them into the **Salto Access** tab.

Notes:

- It is recommended that you assign Salto Access Zones to the Access Group, rather than a large number of Doors. This will help minimise the data required on a Cardholder's card.
- The Salto Access Zone may already contain the appropriate Salto devices for this Access Group. If this is the case, you will only need to assign the Salto Access Zone to this Access Group.
- Salto Access Zones cannot be mixed with Command Centre Access Zones for viewing.

7. Close the **Salto** List Window.
8. Click **Configure** from the menu bar, then **Schedules**.
   The **Schedule** List Window opens.
9. Select the Cardholder Access Schedules appropriate for this Access Group. Drag and drop them into the **Salto Access** tab.
10. Close the **Schedule** List Window.
11. 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.

Updating Access Points

Introduction

This procedure allows installers to import Salto access points, (i.e. Doors and Access Zones) into Command Centre, so they can configure access for Cardholders from Command Centre.

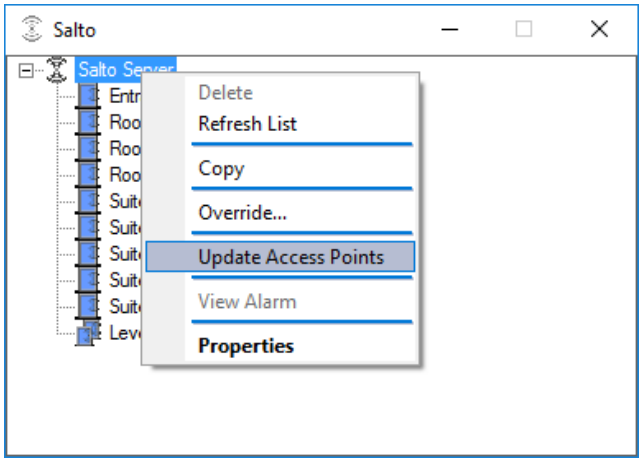
This procedure describes how to update the Salto Server in Command Centre, so that the Salto List Window refreshes with any Salto Doors, ESDs, Lockers, Rooms, Suites and/or Access Zones created, modified or deleted.

To successfully perform an update the operator must have either the “Edit Salto Items” operator privilege, or the “Edit Site” operator privilege in the Salto Server division, as well as the “Edit Site” privilege in every division that contains a Salto Door or Salto Access Zone.

When creating new items, the last division an operator used for creating or saving an item in Command Centre would normally populate the Division field. However, if the operator’s last used division is not available, then by default the system will select the highest division that the operator has access to. If there is more than one division at the same level, then the system will select the division which was created first.

Procedure

1. Open Command Centre.
2. Click **Configure** from the menu bar, then **Salto**.
   The Salto List Window displays.
3. **Right click** on the Salto Server and select **Update Access Points**.



Result

An Update Access Points override is performed and the Salto access points are imported into Command Centre.

Note: Some entities may fail to update for various reasons, (e.g. network downtime, server downtime, timeout).

If an Update Access Points override does fail, the Status and Overrides tab of the Salto Server item will highlight the failed entities.

If an Update Access Points override fails, correct the problem and retry the override. Failure can be caused by any of the following:

- the Salto Server is offline,
- there are more Salto devices than the Command Centre license allows,
- the operator does not have sufficient privilege to modify the Salto device,
- one or more Salto devices are being modified by another operator, or
- an existing Salto device that needs to be deleted is used on a Site Plan or in an Access Group.

Configuring Salto Doors

Introduction

Salto Doors, Salto Lockers, Salto Rooms, and Salto Suites are treated as Salto Door items in Command Centre.

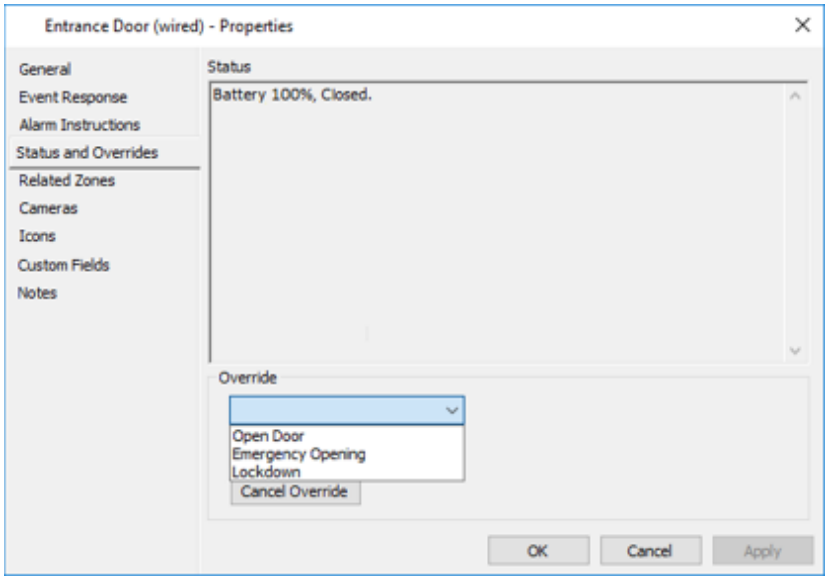
Salto Door properties are editable in Command Centre with the "Edit Salto Items" operator privilege, once the Salto Door, Salto Locker, Salto Room, or Salto Suite has been transferred from the Salto Server, (i.e. Salto Doors are automatically created in Command Centre once an 'Update Access Points' operation on the Salto Server has occurred).

Changes made to Salto Door names and descriptions in Command Centre update automatically in Salto without performing an 'Update Access Points', when Salto is online, or comes online after being offline. Likewise, Salto Doors can be deleted from Command Centre and the deletion occurs automatically in Salto when Salto is online.

Procedure

1. Click **Configure** from the menu bar, then **Salto**.
   The **Salto** List Window opens.
2. **Right click** on the appropriate Salto Door, and select **Properties**.
   By default the **General** tab displays.

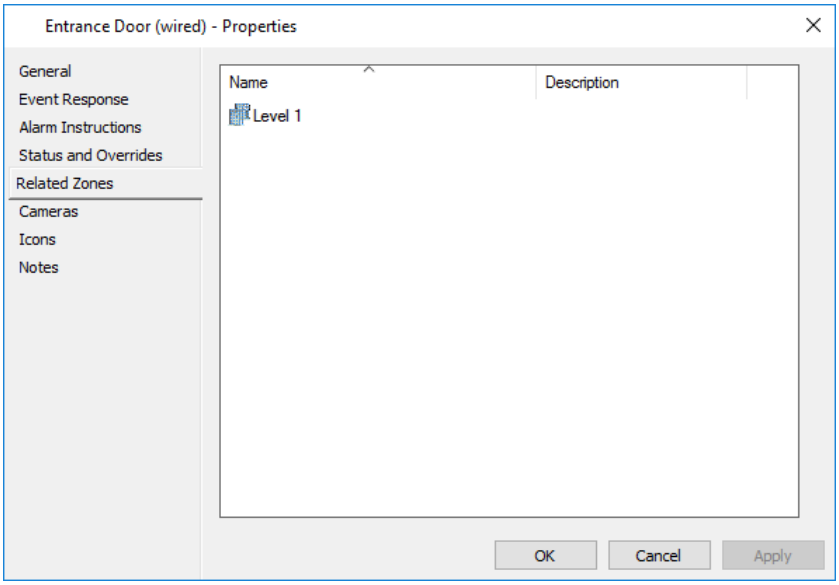
   Notes:
   - If you change the name in Command Centre, you need to right-click on Salto Server and click 'Update Access Points' and the changes will be updated.
   - The **Division** that appears on the **General** tab will be the last division used by the operator that did an 'Update Access Points' of the Salto Server. Check this is the required division.
3. If using the Salto Space integration, click the **Status and Overrides** tab.



Overrides that can be performed using the Salto Space integration are: Open Door, Emergency Opening and Lockdown.

Note: Salto online doors can be added to a Macro which will enable you to Lockdown multiple Salto online doors simultaneously.

4. Click the **Related Zones** tab.



This screen shows the Salto Access Zone(s) that this Salto Door belongs to. Salto Access Zone(s) can be added to this screen using drag-and-drop, or removed by right-clicking on the Zone and selecting **Delete**.

5. 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.

Result

A Salto Door has been configured in Command Centre.

Configuring Salto Access Zones

Introduction

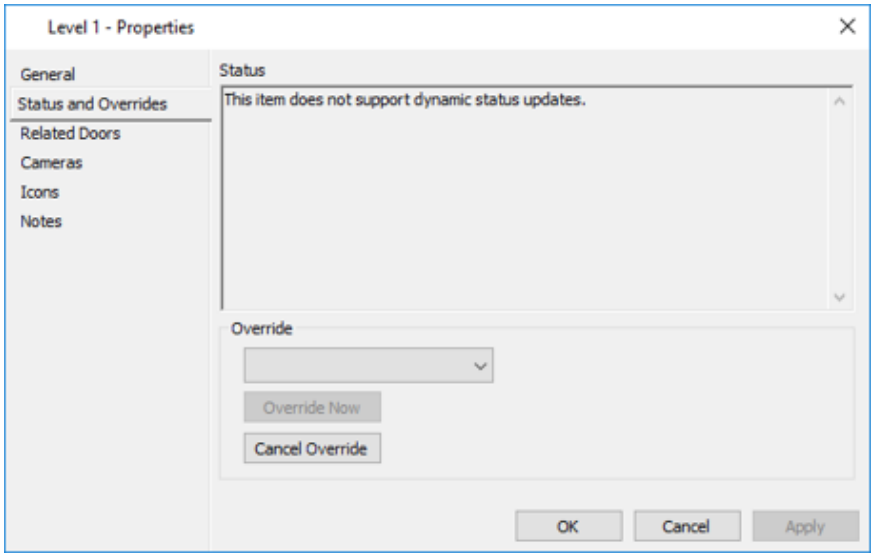
Salto Access Zone properties are editable in Command Centre with the "Edit Salto Items" operator privilege, once the Salto Access Zone has been transferred from the Salto Server, (i.e. Salto Access Zones are automatically created in Command Centre once an 'Update Access Points' of the Salto Server has occurred).

Changes made to Salto Access Zone names and descriptions in Command Centre update automatically in Salto without performing an 'Update Access Points', when Salto is online or comes online after being offline. Likewise, Salto Access Zones can be deleted from Command Centre and the deletion occurs automatically in Salto when Salto is online.

Procedure

1. Click **Configure** from the menu bar, then **Salto**.
   The **Salto** List Window opens.
2. **Right click** on the appropriate Salto Access Zone, and select **Properties**.
   By default the **General** tab displays.

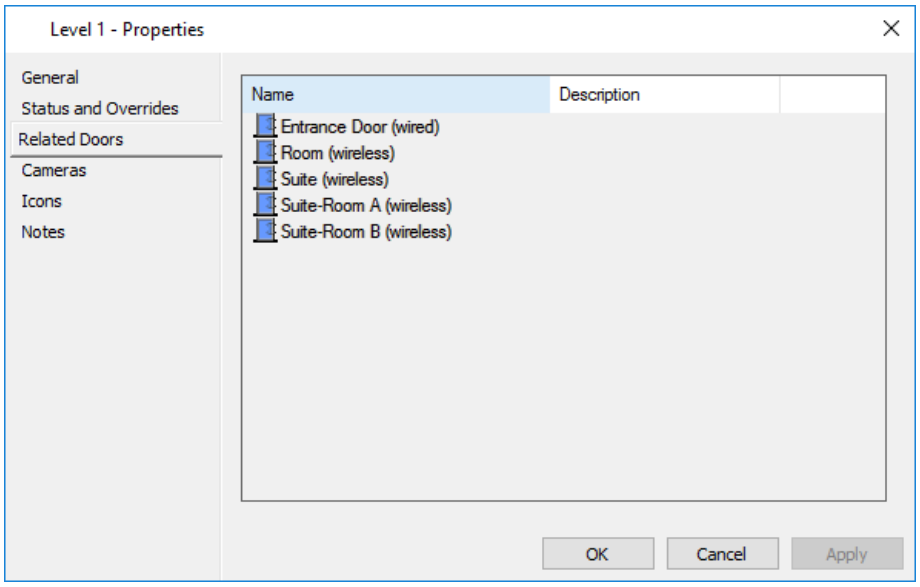
   Notes:
   - If you change the name in Command Centre, you need to right-click on Salto Server and click 'Update Access Points' and the changes will be updated.
   - The **Division** that appears on the **General** tab will be the last division used by the operator that did an 'Update Access Points' of the Salto Server. Check this is the required division.
   - Everything can be changed for the Access Zone, except the information on the **Related Doors** tab.
3. If using the Salto Space integration, click the **Status and Overrides** tab.



Salto Space overrides that can be performed are Emergency Opening and Lockdown.

Note: Salto Access Zones can be added to a Macro which will enable you to Lockdown multiple zones simultaneously.

4. Click the **Related Doors** tab.



This screen shows the Salto Door(s) that belong to this Salto Access Zone.

5. 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.

Result

A Salto Access Zone has been configured in Command Centre.

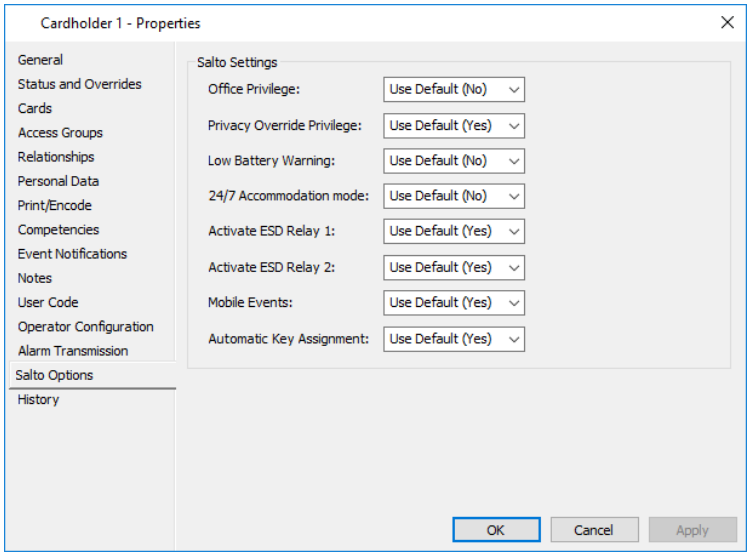
Configuring Salto options for Cardholders

Introduction

Operators require the "Edit Cardholders" operator privileges to be able to perform this procedure.

Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
2. **Right click** on the appropriate Cardholder, and select **Properties**.
   By default the **General** tab displays.
3. Click the **Salto Options** tab.
   Notes:
   - This tab is only available if your site is licensed for one or more Salto Doors.
   - The Automatic Key Assignment option is only visible in Native Mode.



   Each of the fields on this screen default to "Use Default", which means that they use whatever default is configured on the Salto Server Properties, (i.e. when the Salto Server default value is changed, the new value will also be used for the Cardholder from then on). Regardless of whether you choose 'Yes' or 'No', these settings will remain in place even if the server details have been changed.

   Refer to Step 7 of ***Editing the Salto Server*** (on page 74-73) for an explanation of these settings.

   Notes:
   - If the Cardholder properties are open and the Salto Server properties are changed, the Cardholder properties won't update until they are closed and then reopened.
   - If your site is using multi-server, Cardholders will replicate but the Salto options on the **Salto Options** tab will not. They can be adjusted on any server and those options will not be synced.

Configuring access to Salto Outputs

Introduction

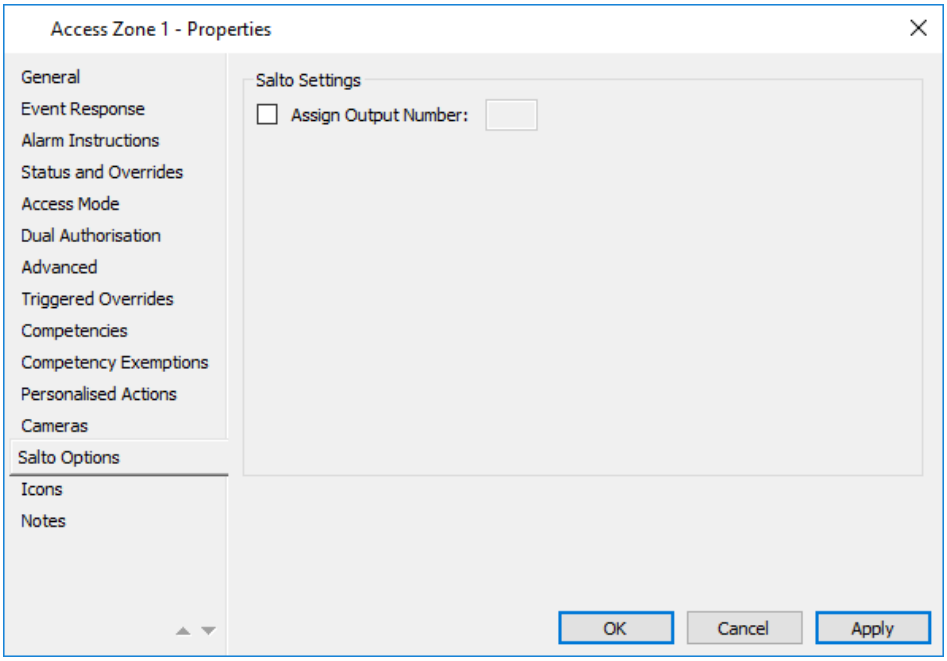
A Salto Output number can be assigned to an Command Centre Access Zone item. When a Cardholder's card is encoded with Salto data by Command Centre, the Salto Output numbers for any Access Zones the Cardholder is required to access are added to the card. When a Cardholder presents their card at a Salto wired reader, (i.e. located within a lift), the Salto Outputs for which the Cardholder has access will be activated, thus enabling the Cardholder to access one or more floors.

Notes:

- This feature has been designed to work with a low-level elevator interface managed by the Salto system.
- This feature supports a Command Centre multi-server environment. However, it is important to note, that the Salto Output number configured for an Command Centre Access Zone item, must correspond to a Salto Output on the *connected* Salto Server.
- Salto Output numbers available are 1-128.
- Multiple Access Zones can share the same Salto Output number.
- The Salto Output number must correspond to a Salto Output in the Salto application, (i.e. a Salto relay on a Salto relay expansion board).
- When using two Salto relay expansion boards, the Output on each relay board will activate at the same time, unless you change the Dip Switch settings on the second board.
- The standard functionality for a Command Centre Access Zone item, (e.g. Lockdown, Cardholder Access Schedule, etc.) does not apply to Salto Outputs. Instead, the Salto Door connected to the control unit, (e.g. CU5000) and relay expansion board can be used to prevent access to the Salto Outputs when in lockdown mode.
- Outputs must be configured in Salto when using Salto encoded guest cards. When using Command Centre encoded cards (encoded with Salto data) the Outputs need only be assigned in Command Centre.

Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. **Right click** on the appropriate Access Zone, and select **Properties**.
   By default the **General** tab displays.
3. Click the **Salto Options** tab.
   Note: This tab is only available if your site is licensed for one or more Salto Doors.



4. Check the **Assign Output Number** checkbox.
   The Output Number field is enabled.
5. Enter the Salto Output number for this Access Zone. Cardholders with access to this Access Zone will have access to the Salto Output.
6. 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.

Result

A Salto Output has been assigned to an Access Zone in Command Centre.

Encoding cards

Introduction

Each Cardholder can be issued with a single MIFARE SmartCard that can be used to grant access through Gallagher doors, Salto doors or doors using Morpho readers. Encoding of all three types together on the same card is only possible on 4k MIFARE Classic cards, 4k MIFARE DESFire EV1 to EV3 cards, or 8k MIFARE DESFire EV1 to EV3 cards. **Notes:**

- MIFARE DESFire EV1 to EV3 cards are encoded using the MIFARE DESFire Object added to the Card Layout.
- If your site is using Gallagher, Salto, and Morpho Biometric Readers, the Salto information will NOT fit onto 1k MIFARE Classic cards along with the currently encoded data.

  There are 15 'usable' sectors (16 in total) on a 1k MIFARE Classic card encoded with Gallagher data.

  Gallagher requires 2 MIFARE sectors.
  1 MIFARE sector is used for the Card Application Director (CAD) and the other for Gallagher data.

  Salto requires at least 5 MIFARE sectors (4-14 are default sectors).

  Morpho fingerprint readers require 10 MIFARE sectors.
  Allow 25 MIFARE sectors when using both fingerprint and finger vein readers.

  This is 17 sectors in total - too many to fit onto a 1k MIFARE Classic card.
- Salto encoding from Command Centre is supported for both 4k and 8k MIFARE DESFire EV1 to EV3 cards (as stated above). Differentiation between the two can be achieved by using two Card Types in Command Centre if needed. For instance, "Gallagher 4k DESFire Card Type" and "Gallagher and Salto 8k DESFire Card Type".
- If a card has been encoded with Gallagher data and either Salto, Morpho or ASCII data; when re-encoding the card, ensure the Gallagher object is present on the Card Layout, unless an object is going to overwrite the sector that the Card Application Directory (CAD) has previously been written to.
- Encoding of the MIFARE SmartCard used for accessing both Command Centre doors and Salto doors is performed via Command Centre.
- A Salto USB or Ethernet encoder must be connected to the Salto Server to enable encoding of Salto data on MIFARE cards from the Command Centre workstation.

Procedure

1. Does your site have Cardholders that will be accessing **only** Salto Doors?

If...	then...
yes	create a new Card Type, (or edit an existing one). Refer to ***Setting up Card Types*** (on page 7-2) for the procedure.
no	go to Step 2.

2. Either create a new card layout, or copy an existing card layout. Refer to ***Designing Card Layouts*** (on page 47-13) for full details on configuring a card layout.
3. Add a Salto MIFARE object to the card layout. Refer to ***Adding Salto MIFARE objects to a card layout*** (on page 74-99) for the procedure.
4. Print and/or encode the card. Refer to ***Printing and/or Encoding a card from a cardholder*** (on page 47-49) for the procedure.
5. Repeat Step 4 for all subsequent Cardholders.

Set up a SALTO reader as a Third-party reader using Wiegand connection

Introduction

Cards encoded in Command Centre that include a Salto Object, will either be encoded as 26 bit, 64 bit or 128 bit. **Notes:**

- You cannot use 26 bit, 64 bit and 128 bit Wiegand format on the same Salto Space Server. If you upgrade to Salto Native mode from an original 26 bit Wiegand format card type configuration, you will need to configure 26 bit Wiegand in Salto Space.
- You cannot return to 26 bit or 64 bit once at 128 bit.
- A card needs to be encoded before the Salto status in Command Centre will show as 128 or 64 bit.
- If you want to use mobile credentials with a Salto third party reader, 128 bit is required.

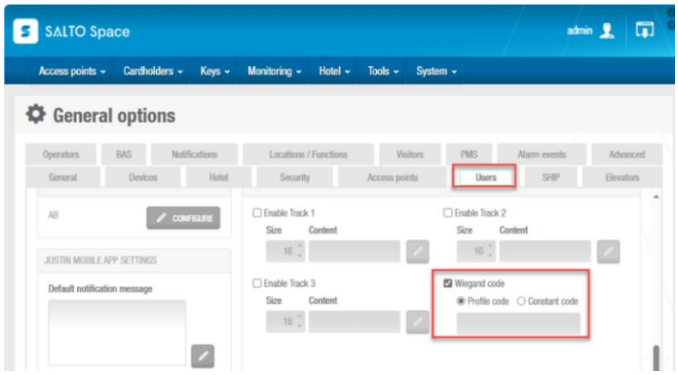
Procedure

This procedure describes how to configure Salto Space Wiegand code so you can use a wired Salto reader as a third-party reader in Command Centre using Wiegand connection in Native Mode. 128 bit is recommended.
This procedure is split into four parts, as follows:

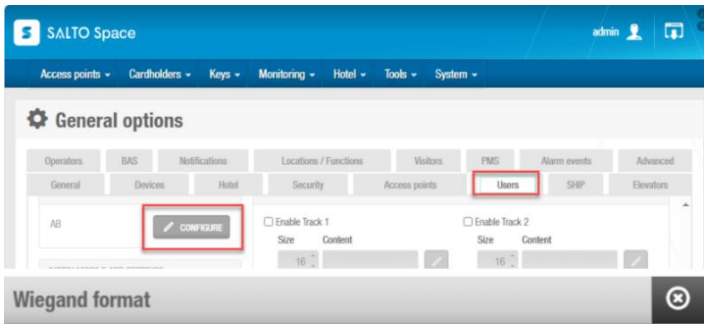
1. Salto Space Procedure
2. Salto Reader Configuration
3. Wiring SALTO reader as Wiegand connection third-party reader
4. Third-party reader configuration in Command Centre

1. Salto Space Procedure

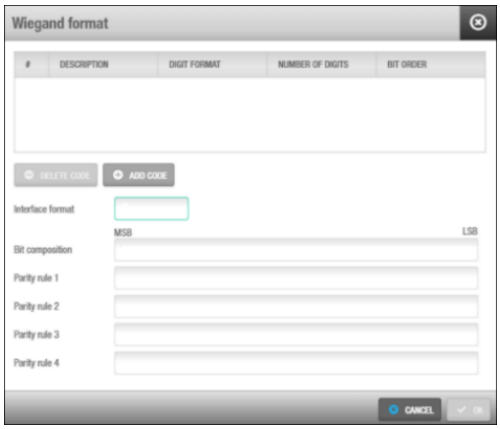
1. Log into Salto Space, select **System** > **General options** > **Users**. The Users tab displays.
2. Tick the **Wiegand code** checkbox, then select the **Profile code** radio button.



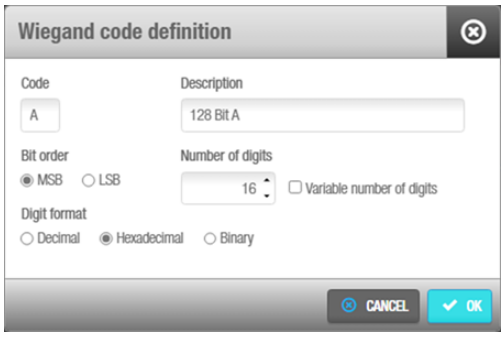
3. Click the **CONFIGURE** button.



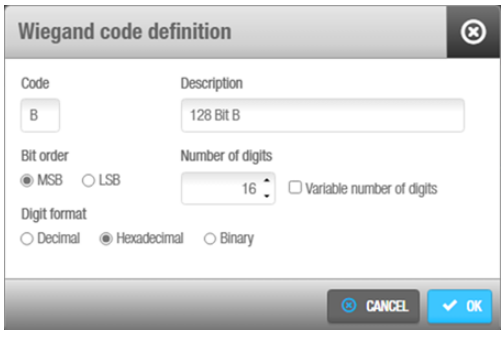
The Wiegand format configuration dialog box displays.



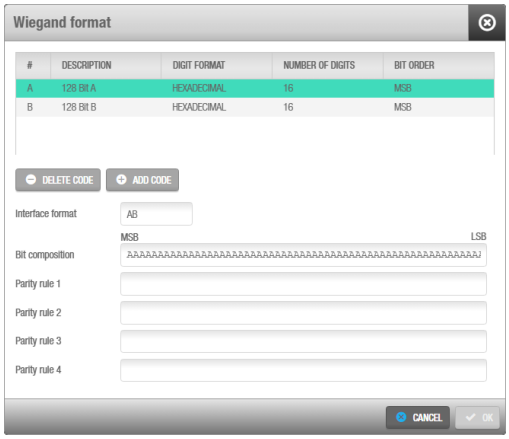
4. Click the **ADD Code** button. The Wiegand code definition dialog box displays. This allows you to specify the different parts that form the Wiegand code and define their characteristics.



5. Once you have configured A code for 128 Bit click **OK**, then click the **ADD CODE** button again and add another code for B code.



6. Click the **OK** button. The Wiegand code definition dialog box closes.
7. Add AB in the **Interface format** field.



8. Add 64 A's followed by 64 B's in the **Bit composition** field.
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAABBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBB

   Note: We currently support Wiegand code for 26 bits (Legacy only), 64 bits and 128 bits. Refer ***to Reason for using 128 bit Wiegand format*** (on page 74-98) for details of the limitations there are with using 26 bit format.

9. Define the parts of the Wiegand code appropriate for the format you're using:

   26 bit format (Legacy mode only):

   The default **Code** option is "A", but you can change this if required.
   Any letter can be entered except "P" as this is used to identify the parity of the codes at the beginning and end of the Wiegand code.

Code:	A	B
Description:	Facility code. Any description can be used.	Card number. Any description can be used.
Bit Order:	MSB	MSB
No. of Digits:	2	4
Digit format:	Hexadecimal	Hexidecimal

   64 bit format:

   - **Code:** A
     The default option is "A", but you can change this if required.
     Any letter can be entered except "P" as this is used to identify the parity of the codes at the beginning and end of the Wiegand code.
   - **Description:** 64Bit. Any description can be used.
   - **Bit order:** MSB
   - **Number of Digits:** 16
   - **Digit format:** Hexadecimal

   128 bit format:

   The default **Code** option is "A", but you can change this if required.
   Any letter can be entered except "P" as this is used to identify the parity of the codes at the beginning and end of the Wiegand code.

Code:	A	B
Description:	128 Bit. Any description can be used.	128 Bit. Any description can be used.
Bit Order:	MSB	MSB
No. of Digits:	16	16
Digit format:	Hexadecimal	Hexidecimal

10. Click the **OK** button to return to the Wiegand format configuration dialog.

11. Define the format of the Wiegand code appropriate for the format you are using:

128 bit format:

- **Interface format:** AB
- **Bit composition:** <64 A's><64 B's>
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAABBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
  BBBBBBB

64 bit format:

- **Interface format:** A
- **Bit composition:** <64 A's>
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAA

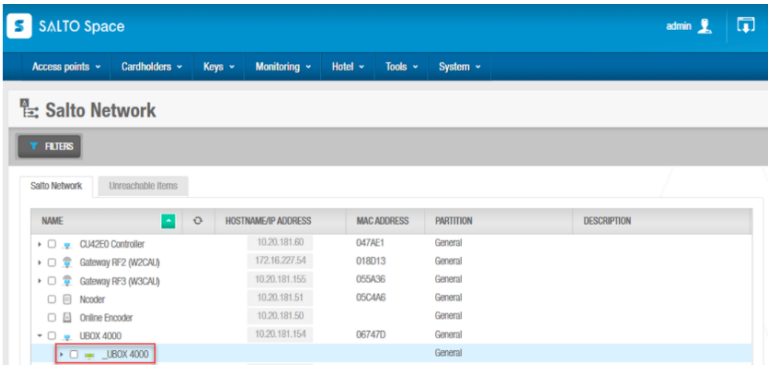
26 bit format (Legacy mode only):

- **Interface format:** AB
- **Bit composition:** <P> <8 A's> <16 B's> <P>
  < PAAAAAAAABBBBBBBBBBBBBBBP >
- **Parity rule 1:** <E> <12 X's> <13 -'s>
  < EXXXXXXXXXXXX---------- >
- **Parity rule 2:** <13 -'s> <12 X's> <O>
  < ----------XXXXXXXXXXXXO >

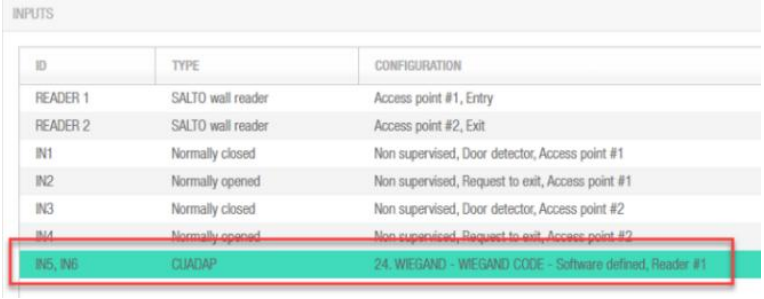
12. Click the **OK** button to complete the custom Wiegand format.
Note: Copy from notepad ++ to help count the letters for Bit composition.

2. SALTO reader configuration

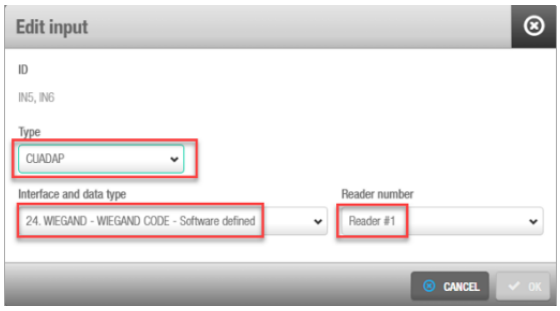
1. From Salto Space, select **System** > **SALTO Network** and expand **CU4xxx Auxiliary** or **UBOX4000 Auxiliary**.
Click on **CU4xxx Controller** or **UBOX4000 Controller**.



2. From the INPUTS panel, double-click on **IN3**, **IN4** or **IN5**, **IN6** from the list.



The Edit input page displays.

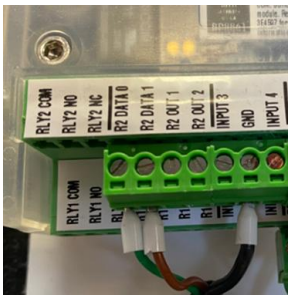


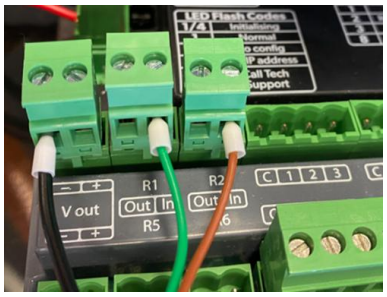
3. Select the following options from the drop-down lists:
   - **Type: CUADAP**
   - **Interface and data type:** 24, WIEGAND - WIEGAND CODE - Software defined
   - **Reader number:** Reader #1 (Reader number can be different as required)
4. Click the **OK** button to apply.

3. Wiring SALTO reader as Wiegand connection third-party reader

From the UBOX4000/CU4xxx Controller:	From the Wiegand HBUS Module:	From an 8R Module connected to the Gallagher Controller:
IN5+	DATA0	R1 In
IN6+	DATA1	R2 In
IN6-	GND	GND

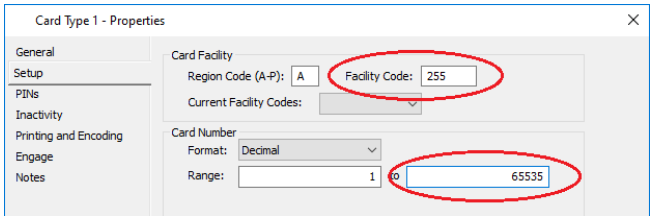






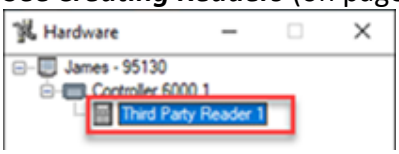
4. Third-party reader configuration in Command Centre

1. Create a card type containing a SALTO object, as follows:
   Note: For Native mode from v9.40 or later, 64 bit and 128 bit Wiegand card formats are set in SALTO Space only, not through the card type in Command Centre.
   a) In Command Centre Configuration Client, add a Salto MIFARE object to the card layout. Refer to ***Adding Salto MIFARE objects to a card layout*** (on page 74-99) for the procedure.
   b) If you are using 26 bit format, when configuring the Card Type the following ranges are supported:
      - Facility Code = 1 – 255
      - Card Number = 1 – 65535

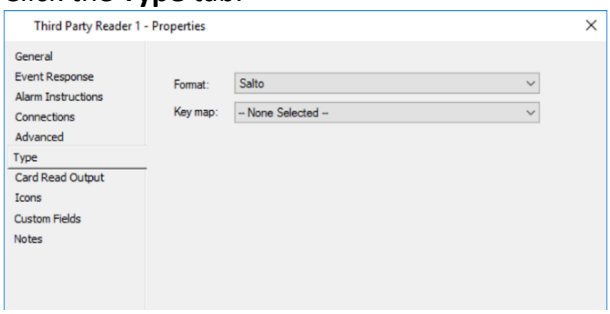


2. Create a Third-party reader and assign it to a Controller, as follows:
   a) In Command Centre Configuration Client, click **Configure** from the menu bar, then **Hardware**. The **Hardware** List Window opens.

b) **Right click** and select **New...Third Party Reader**.
See ***Creating Readers*** (on page 21-57) for the full procedure.

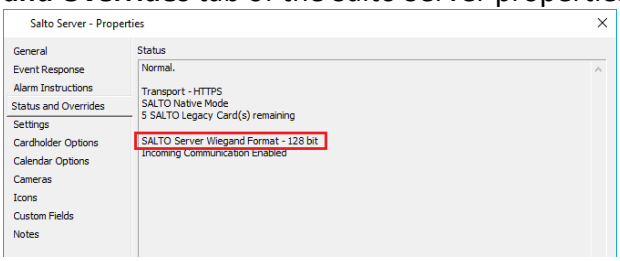


c) Click the **Type** tab.



d) Select the appropriate **Format** from the drop-down list.

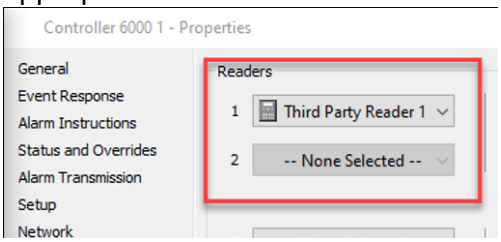
e) Did you select 'Salto' as the Format?
If **yes**, no **Key Map** is necessary. Go to the next tab.
If **no**, go to Step f.
Note: The current Wiegand Format supported will display on **the Status and Overrides** tab of the Salto Server properties.



Notes:

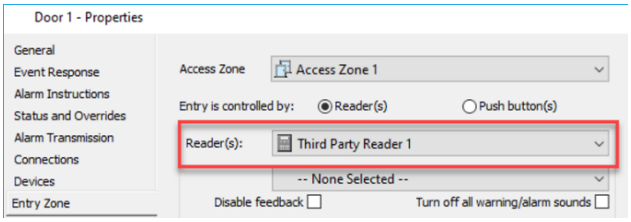
- It is not possible to change back to a smaller Wiegand format once 128 bit is configured.
- New Salto sites are by default given a 128 bit Wiegand format.
- Legacy mode does not support 128 bit, nor does it support mobile connect at a Salto Third Party reader outputting Wiegand data.
- When upgrading from legacy mode, as long as the legacy mode was configured with 26 bits, then it can be supported in native mode. 26 bit format is also required to be configured in Salto Space.

f) Assign the third-party reader to a Controller by:
- opening the property pages for the Controller that the third-party reader is to be assigned to,
- clicking the **Readers** tab, and assigning the third-party reader to the appropriate slot:



g) Click the **OK** button to exit the Controller properties and save your changes.

3. Add the SALTO Third-party reader to a Door, as follows:
   a) From the **Hardware** List Window, select the Door that you want to add the SALTO third-party reader to.
   b) Click the **Entry Zone** tab.
   c) Select the third-party reader from the relevant **Reader(s)** drop-down list.



   d) Click the **OK** button to exit the Door properties and save your changes.
4. Encode a card for a cardholder with SALTO card type assigned.
   Refer to ***Printing and/or Encoding a card from a cardholder*** (on page 47-58) for the procedure.

Reason for using 128 bit Wiegand format

The Salto Integration supports encoding a card's number in 26-bit Wiegand format on one of the Salto sectors of the card. However, there are limitations with the 26-bit format, namely:

- The range of Card Numbers that can be supported is 1 to 65,000.
- The Issue Level is ignored so changing the Issue Level on a card assignment has no impact on the Cardholder's ability to gain access through Salto doors using third party readers.
- Only the first two characters (first byte) of the Card's Facility Code will be encoded on the Wiegand portion of the card which means that where there are two cards with the same Card Number, different Facility Codes but the first two characters of those Facility Codes are the same, Command Centre will be unable to distinguish between them.

Command Centre v9.40 introduces support for 128 bit Wiegand data format, enabling mobile credentials to work seamlessly with wired SALTO readers and Gallagher controllers via the UBOX 4000 hardware. Command Centre now supports access and event tracking for mobile devices alongside traditional cards at SALTO wired readers setup as Gallagher Third party Wiegand readers. Note this functionality is only available in SALTO Native mode.

Configuring Salto wired readers to display green/red LED based on access decision

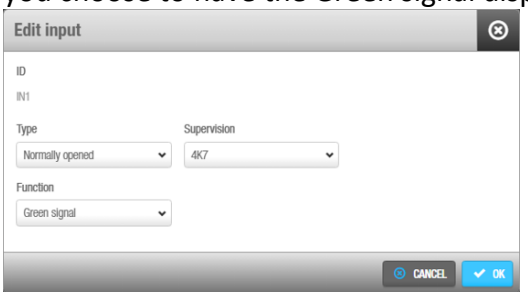
Where a Salto reader is used but the access decision is being made by Command Centre, the latter should control whether the LED on the Salto reader goes green to indicate access is granted or red when access is denied. To achieve that the system must be configured in the following way:

To pulse the green LED on the Salto Control Unit when access is granted:

1. Create an Output to be activated when the door is unlocked.
2. Create a Logic Block with the following:
   - A Rule which triggers when the Unlock Output on the door is ON.
   - Timing so that the 'Logic Block is pulsed when the rules are met'. The Pulse on time should be configured so that it is long enough for the Cardholder to see that access has been granted.
   - Create a reflected Output and assign it to the reflected output page of

the logic block and connect it to the door input on the Salto Control Unit. This Output will be activated when the logic block turns ON.

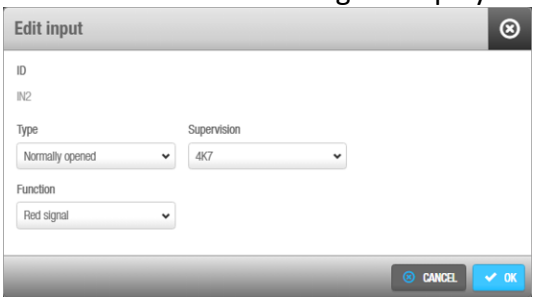
3. Navigate to UBOX 4000 / CU42E0 controller Auxiliary, click on the input you choose to have the Green signal display.



4. Wire up the output controlling the Green signal to the input selected on the Salto controller.
   Note: A Logic Block is required because the time an Output will be pulsed by some door mechanisms supported, (e.g. boom gates), will be insufficient for this purpose.

To pulse the red LED on the Salto Control Unit when access is denied:

1. Create an Action Plan and assign it to the Access denied Event Group of the door.
2. Create an Output to be triggered when the Action Plan is activated. Assign the Output in all Action Plan tabs, (i.e. Armed, Disarmed, User1 and User2), and connect this Output to the Exit Input of the Salto Control Unit.
3. On the **Advanced** tad of the Output, configure the number of seconds the Output is to be pulsed. When the Output is turned ON the Red LED on the Salto Control Unit will display for a number of seconds configured for the Output to pulse.
4. Navigate to UBOX 4000 / CU42E0 Auxiliary and click on the input you choose to have the Red signal display.



5. Wire up the output controlling the Red signal to the input selected on the Salto controller.

Adding Salto MIFARE objects to a card layout

Introduction

Salto MIFARE objects can be added to a Card Type, allowing you to encode Salto data onto MIFARE card technologies as follows:

Salto Objects	Allows you to encode Salto data on...
Salto MIFARE Classic	MIFARE Classic cards.
Salto DESFire	MIFARE DESFire® EV1 to EV3 (AES) cards.

Notes:

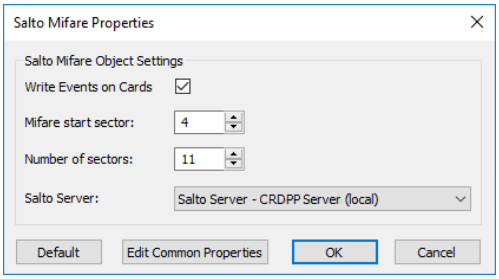
- A site can use all three card technologies, (i.e. MIFARE DESFire EV1 to EV3 and MIFARE Classic) con-currently, when using Salto readers that support these card technologies.
- Salto and Morpho FVP objects on the same card layout is not supported.
- Events from Salto offline readers are stored on the card. The older events are transferred from the card to the Salto server when the card is presented at a Salto wired reader. Using the default configuration (of 11 sectors) approximately 24 events can be stored on a card.
  Note: Of the 11 sectors approximately 5 sectors are dedicated to access, (i.e. they cannot store events).

Procedure

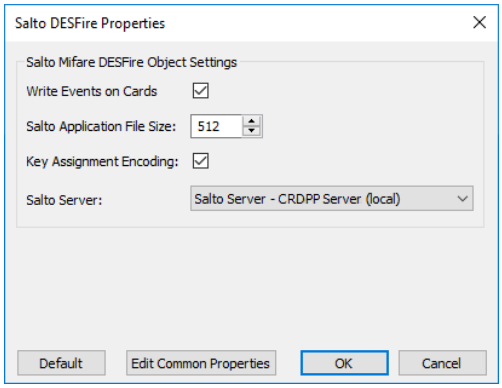
This procedure describes how to add a Salto MIFARE object, (i.e. Salto MIFARE Classic or Salto MIFARE DESFire), to a card layout.

1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. **Right click** on the required card, and select **Edit Card Layout**.
   The **Card Editor** window displays.
3. Select the Salto MIFARE object type you want to add. Either:
   - **New Salto MIFARE Classic Object**
   - **New Salto MIFARE DESFire Object**

   An object box displays with placeholders around it. **Notes:**
   - These options are only available if your license contains one or more Salto doors.
   - The size of the object box can be expanded if necessary. See *Expanding an Object Box* for procedure.
4. **Right click** on the Salto object, then click **Properties** from the drop-down menu. What Salto object type did you select?
   If **Salto MIFARE Classic**, then the Salto MIFARE Properties dialog displays:



   If **Salto MIFARE DESFire**, then the Salto DESFire Properties dialog displays:



5. Configure the Salto MIFARE properties as required:

Salto object type	Option	Description
Both	Write Events on Cards	Indication of whether to write events on the card or not. (Default = Checked). If you change this setting, any cards that have been previously encoded will need to be reencoded. Otherwise a long beep is heard from the wired reader after the card grants access, and if the setting is being turned on, then it will not take effect until reencoding the card. **Note:** Salto offline doors also need to have 'Audit on keys' enabled.
	26-bit	This option is used for encoding the Card Identifier in 26-bit format, and is the default setting.
	64-bit prox	This option is used for encoding the Card Identifier in 64-bit prox format. **Notes:** • When adding the Salto DESFire Object to the Card Layout, ensure 64-bit prox is selected. • If you select this format, you need to configure the Salto card format to support 64-bit integration, otherwise encoding Salto from Command Centre will not work. See ***Configuring Key to support Space CUADAP 64-bit integration*** (on page 68-81) for the procedure.
	Salto Server	If your site supports multiple Salto Servers, specify the Salto Server data to be encoded from the drop-down list.
Salto MIFARE Classic	MIFARE start sector	This field must be between 1 and 11, or 17 and 27.
	Number of sectors	This field must be between 5 and 15, and the "MIFARE start sector" plus the "Number of sectors" must be less than or equal to 16, or less than or equal to 32 if "MIFARE start sector" is greater than 16. **Note:** Approximately 10 events are stored per sector, and approximately 5 sectors are dedicated to access, (i.e. they cannot store events).
Salto MIFARE DESFire	Salto Application File Size	The file size (in bytes) for this Salto application. (Range 320 - 7200 bytes. Default 512 bytes) Reducing the file size will decrease the number of card events (from Salto wireless readers) that can be stored on the card. Increasing the file size will limit the available space for other applications on the card. Supported card sizes are 2K, 4K and 8K. **Note:** The default file size of 512 bytes will store approximately 28 card events on the card.
	Key Assignment Encoding	This card needs to be created on your third party system (non-Salto) with the checkbox ticked. You do not need to have a card type on your Command Centre Salto System with this checked. (Default = Unchecked)

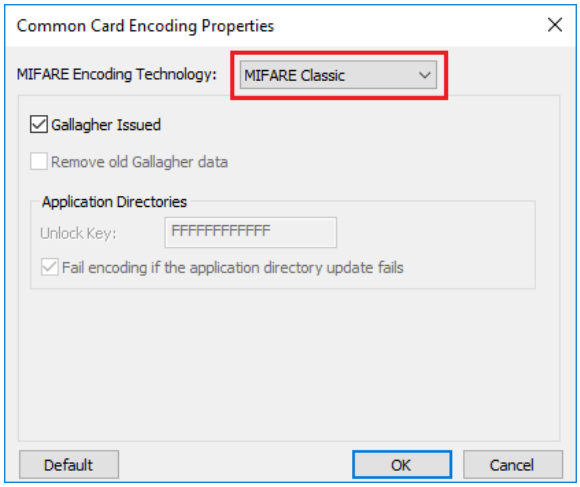
Note: The **Default** button allows you to reset the Salto MIFARE properties back to the default settings.

6. If you want to configure common encoding properties, click the **Edit Common Properties** button.

   The Common Card Encoding Properties dialog box displays.

7. If not already selected, select the appropriate card technology, (i.e. MIFARE Classic or MIFARE DESFire), from the **MIFARE Encoding Technology** drop-down list.

   The fields that populate the dialog box depends on the card technology selected, (e.g. the following screen example demonstrates how it will look when **MIFARE Classic** is selected).



   Regardless of the card technology selected, by default the **Gallagher Issued** checkbox is enabled (ticked), which means that when you configure the MIFARE object on a card layout, all other configuration options are disabled.

8. To alter the MIFARE properties, uncheck the **Gallagher Issued** checkbox. All the fields become enabled.

9. Configure the MIFARE properties as required:

Salto object type	Option	Description
Salto MIFARE Classic	Remove old Gallagher data	This checkbox allows you to either leave the old Gallagher data on the card or remove it. **Notes:** • Removing the old Gallagher data will only succeed if the old card data was encoded with the same MIFARE DESFire key seed and same facility code as this Card Type. • If you write to the same sector as previously, the Gallagher data is removed and re-written if the facility code of the sector is the same facility code as this Card Type.

Salto object type	Option	Description
	Unlock Key (Application Directories)	This field allows you to access Sector 0 in the Application Directory. For example, a third parties MAD write key should be entered in this field if the MAD has been locked by the other party and hence the card manufacturer's key or Gallagher unlock key won't work. The key must consist of 32 hexadecimal digits (0-9 and A-F).
	Fail encoding if the application directory update fails	The MIFARE Application Directory (MAD) is the directory of all the sectors on the card. By default this checkbox is enabled (ticked), which means if the MAD can be unlocked, then it will always be updated with this Information. If you choose to encode cards with the MAD or CAD locked, uncheck this checkbox.
Salto MIFARE DESFire	Use card master key	If the card has been initialised by a third party using a card master key, you will need to enter the third parties master key in this field, in order to encode data onto the card. When checked, the **Type** drop-down box and the **Card Master Key** field are enabled.
	Type	This drop-down box lists the values "AES", "2K3DES" or "3K3DES". This allows selection of the type of encryption used for the Card Master Key.
	Card Master Key	This field must have either 32 hexadecimal characters for AES or 2K3DES encryption types, or 48 hexadecimal characters for 3K3DES encryption type. Hexadecimal character validation occurs when the **OK** button is clicked.
	Default Application Key	The Default Application Key is required when encoding cards that have been personalised by a third party site. This is the key that will allow the Gallagher applications to be created on the card. This field must have 48 hexadecimal characters. If the third party key provided is only 32 characters in length, this field must be padded out to make a 48 hexidecimal character key with the additional characters added to the end of the key. Hexadecimal character validation occurs when the **OK** button is clicked.

Note: The **Default** button allows you to reset the MIFARE Classic properties back to the default settings.

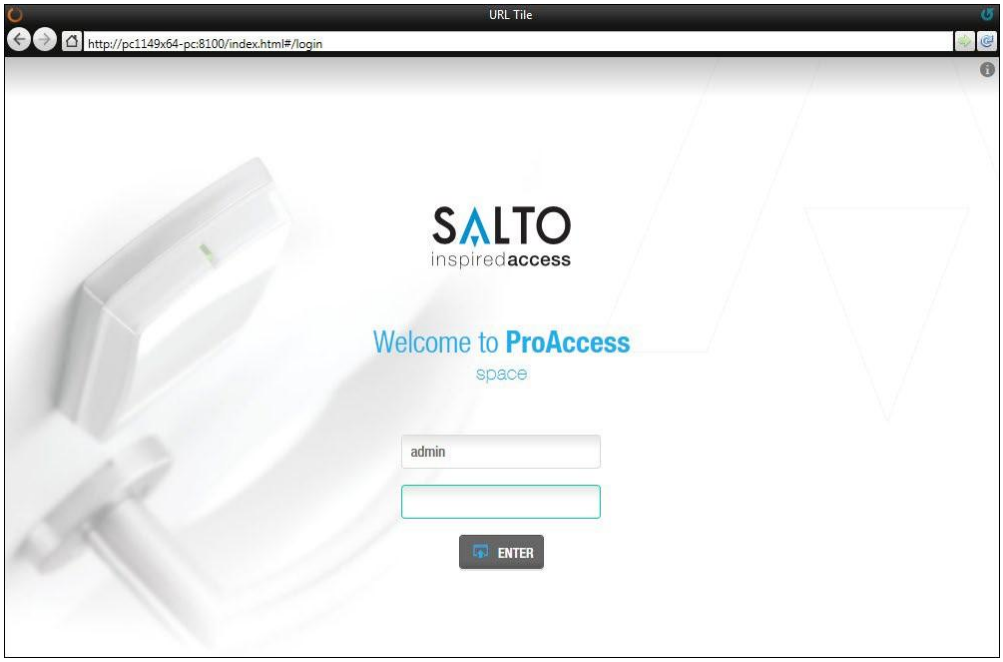
10. Click the **OK** button to save the MIFARE Classic encoding properties.
    The Common Card Encoding Properties dialog box closes.
11. Click the **OK** button to save the Salto MIFARE encoding properties.
    The Salto MIFARE Properties dialog box closes.

Adding Salto Space to the URL Tile

The Salto ProAccess SPACE software can be accessed from within Command Centre using the URL Tile.

Create and configure a URL Tile in Command Centre. Refer to the topic *"Configuring a URL Tile"* in the Command Centre Online Help. Enable Restricted Navigation within the URL Tile configuration.

Copy the Salto ProAccess SPACE URL, (e.g. *http://PC1149WX32:8100/ProAccessSpace/*) located on the **Service ports** tab in the ProAccess Space Configurator and paste into the tile's URL field.



Door Icons

Salto Space Door icons are:

Icon	Description
	The Door is open
	The Door is closed
	The Door is in an unknown state, (e.g. Door is offline)
	The Door is in a lock down state
	The Door is in an emergency opening state

Salto Space Door icon overlays are:

Overlay	Description
	Communication loss
	Forced door
	Low battery (20%)
	Critical battery (10%)
	Door requires PPD update

Salto Key Assignment

Introduction

The Salto Key Assignment feature allows Salto cards to be automatically encoded when presented at a wired Salto update point. This streamlines credential management for sites using Salto Space integration with Gallagher Command Centre.

This option is useful in university installations, for example, where thousands of new users (students) arrive at the start of each academic year. The automatic key assignment functionality means that users do not have to wait in line to have their key encoded. Instead, their key is assigned automatically when it is presented to a Salto update point.

Operators require the "Manage Keys" operator privilege to set up Salto Key Assignment. **Notes:**

- The Automatic Key Assignment options do not appear for Legacy mode.
- Only wired readers can be used, (e.g. UBox400, CU4000s).
- "In-Memory Code" is for Salto DESFire cards only, (i.e. EV1 4K, EV2 4K, EV3 4K and EV3 8K), and "Card Serial Number (CSN)" is for Salto MIFARE Classic cards only.
- MIFARE Classic 1K cards are not supported as they may run out of space with multiple Card Objects. MIFARE Classic 4K cards are recommended instead.
- DESFire settings must be the same on both Command Centre systems, regardless of the fact that the Salto Server will not be online on the “Third Party” system.
- Only new cards are usable for automatic key assignment.

Use Cases

This feature allows for two possible scenarios, as follows:

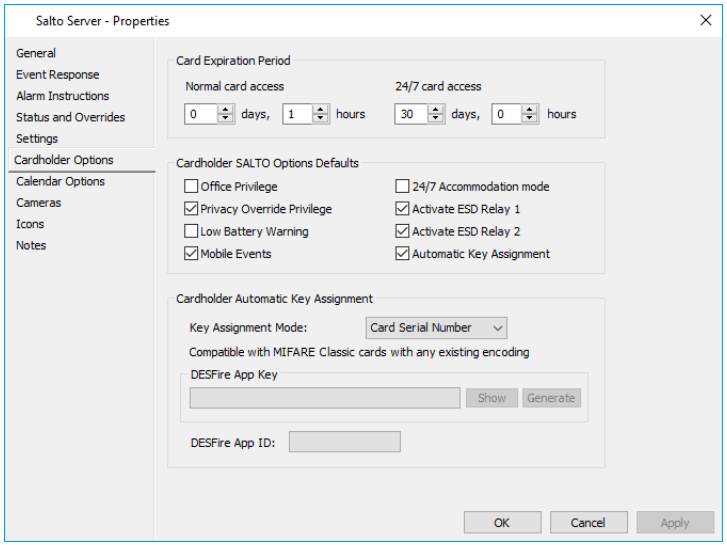
- **Adding Salto to Gallagher Cardholders**
  Sites may want to use the auto encoding feature to help migrate existing Gallagher users to having Salto access. Cardholders that benefit most would be those in remote campuses where there is no easy encoder access.
- **Pre-encoded Salto Cards**
  Sites will order Gallagher pre-encoded cards. Customers with Salto Integration will not be able to use these cards at Salto doors without going through the encoding process. Allowing pre-encoded Gallagher and Salto cards will prevent sites to encode Salto onto their cards.

Configuration - Adding Auto Assignment using Card Serial Number

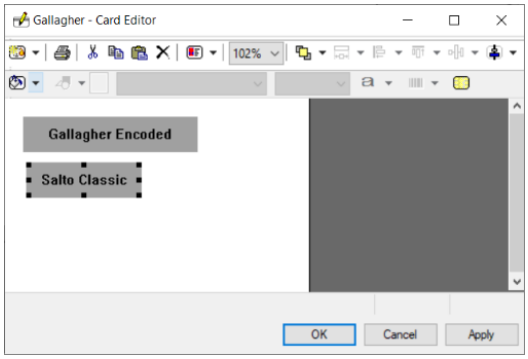
This procedure is split into two parts, (i.e. *Configuration in Command Centre Configuration Client*, and *Configuration in Salto ProAccess SPACE*).
Note: This is only supported with MIFARE Classic cards.

Configuration in Command Centre Configuration Client

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Salto**. The **Salto** List Window opens.
2. **Right click** the Salto Server and select **Properties**.
   By default the **General** tab displays.
3. Click the **Cardholder Options** tab.



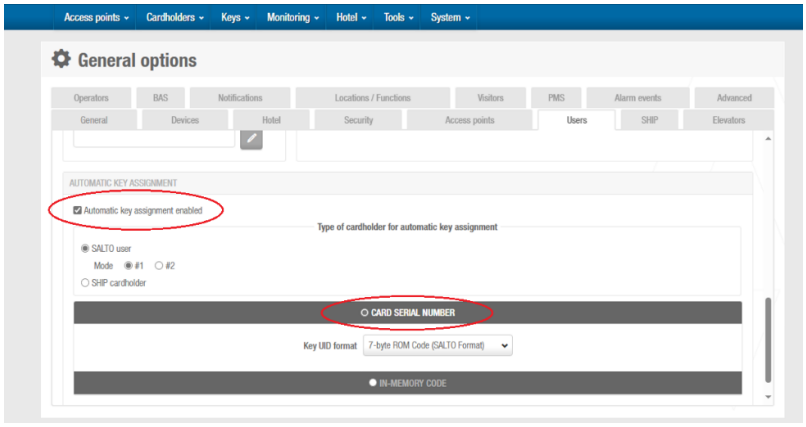
4. Tick the **Automatic Key Assignment** checkbox.
   This will by default enable Automatic Key Assignment for all Salto Cardholders. This can also be enabled per-cardholder via the **Salto Options** page of the Cardholder properties.
5. Select "Card Serial Number" from the **Key Assignment Mode** drop-down.
   Note: The DESFire App Key, buttons and DESFire App ID only become enabled in "In-Memory Code" assignment mode. They otherwise are meaningless outside of this mode.
6. Click **OK** to exit and save your changes.
7. Click **Configure** from the menu bar, then **Card Types**.
   The Card Type List window displays.
8. Select your Gallagher Card Type you wish to add Salto access to, right click and select **Edit Card Layout**.
   The Card Editor window opens. This card type should already have a **Gallagher MIFARE Classic** object on it.
9. Insert a new **Salto MIFARE Classic** object.



10. Click **OK** to exit and save your changes.

Configuration in Salto ProAccess SPACE

1. Open Salto ProAccess SPACE, and select **System** > **General options** > **Users**. The Users tab displays.
2. Tick the **Automatic key assignment enabled** checkbox.
   Note: There are two format options available for the identifier, (i.e. "Card Serial Number" or "In-Memory Code").
3. Click the required **CARD SERIAL NUMBER** radio button. Verify that the Key UID format is **7-byte ROM Code (SALTO Format)**.



4. Click the **SAVE** button.

Note: Make sure the SAM & Issuing options have been configured for Salto MIFARE Classic.

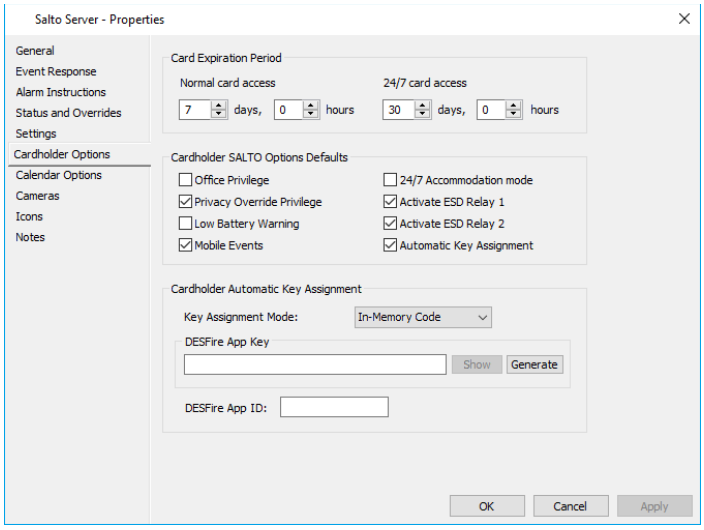
Configuration - In-Memory Code Auto Assignment

This procedure is split into two parts, (i.e. *Configuration in Command Centre Configuration Client*, and *Configuration in Salto ProAccess SPACE*).

Note: This is only supported with DESFire cards.

Configuration in Command Centre Configuration Client

1. In Command Centre Configuration Client, click **Configure** from the menu bar, then **Salto**. The **Salto** List Window opens.
2. **Right click** the Salto Server and select **Properties**. The **General** tab displays.
3. Click the **Cardholder Options** tab.



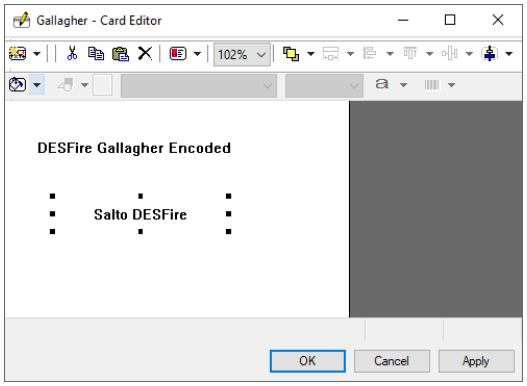
4. Tick the **Automatic Key Assignment** checkbox.
5. The **Cardholder Automatic Key Assignment** section will contain the

default settings for this feature, and controls whether cardholders by default get their key identifier sent to SPACE.

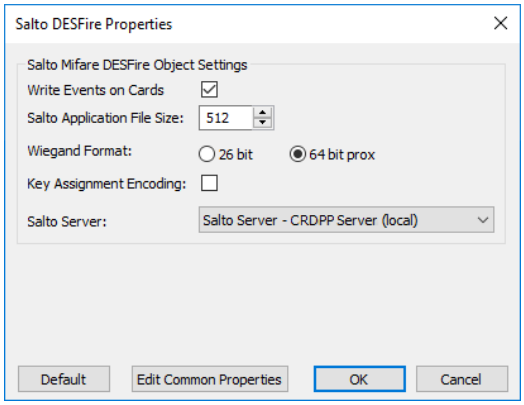
6. Select "In-Memory Code" from the **Key Assignment Mode** drop-down list.
   Note: The DESFire App Key, buttons and DESFire App ID only become enabled in "In-Memory Code" assignment mode. They otherwise are not relevant outside of this mode.
7. Configure as required:

Field	Description
DESFire App Key	Populate this field with a 32 character hexadecimal string. Characters accepted are only A-F and 0-9. Clicking the **Generate** button automatically populates the field with a random hexadecimal string and enables the **Apply** button. If the **Apply** button is clicked now, the 32 characters are converted to 32 X's. **Note:** Clicking the **Show** button will display the key that you have entered. Clicking the **Apply** button changes the text back to X's and the **Show** button is enabled again. An operator event is also logged.
DESFire App ID	Must be a hexidecimal value of exactly 6 characters.

8. Click **OK** to exit and save your changes.
9. Click **Configure** from the menu bar, then **Card Types**.
   The Card Type List window displays.
10. Select your Gallagher Card Type you wish to add Salto access to, right click and select **Edit Card Layout**. The Card Editor window opens.
11. Insert a new **Salto MIFARE DESFire** object.



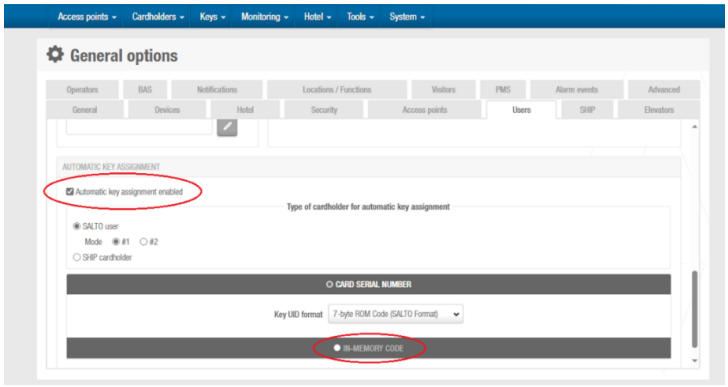
12. **Right click** on the Salto object, then click **Properties** from the drop-down menu. The Salto DESFires Properties dialog box displays:



13. Tick the **Key Assignment Encoding** checkbox.
14. Click **OK** to exit and save your changes.

Configuration in Salto ProAccess SPACE

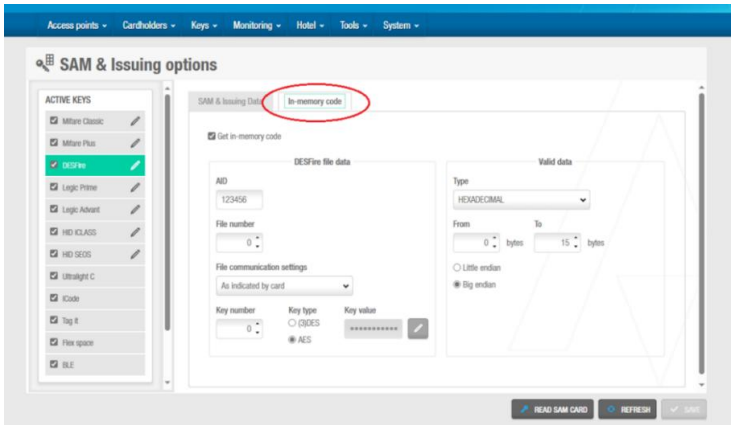
1. Open Salto ProAccess SPACE, and select **System** > **General options** > **Users**. The Users tab displays.
2. Tick the **Automatic key assignment enabled** checkbox.
   Note: There are two format options available for the identifier, (i.e. "Card Serial Number" or "In-Memory Code").
3. Click the required **IN-MEMORY CODE** radio button.



4. Click the **SAVE** button.



5. Select **System** > **SAM & Issuing options**.
6. Tick **DESFire**, and select the **In-memory code** tab.



7. Tick the **Get in-memory code** checkbox.
8. Make the **AID** field the same as the **DESFire App ID** in Command Centre (on the **Cardholder Options** tab of the Salto Server properties).
9. Select the following options from the appropriate drop-downs: '0' for **File number**, 'As indicated by card' for **File communication settings**, and '0' for **Key number**.
10. Click the **AES** radio button for the **Key type**.
11. Make the **Key value** field the same as the **DESFire App Key** in Command Centre (on the **Cardholder Options** tab of the Salto Server properties).
12. In the **Valid data** section, select 'HEXADECIMAL' for the **Type.**
13. In the **From** field, select '0' bytes, and in the **To** field, select '15' bytes.
14. Click the **Big endian** radio button.
15. Click the **SAVE** button.

Note: Make sure the SAM and Issuing options have been configured for Salto DESFire.

SALTO Mobile Access Integration

If your site has SALTO Bluetooth-capable wired or wireless locks, and you have integrated your SALTO server with Command Centre, then you can use the Gallagher Mobile Connect App to open Bluetooth-capable SALTO doors. This requires Gallagher Command Centre version vEL8.10 or newer.

The **Open Salto Door** option will be displayed in the Mobile Connect App when a cardholder is assigned to an Access Zone that has a Salto door assigned to it. The **Open Salto Door** text is always displayed, but will only work with Bluetooth-capable SALTO doors. Cardholders need to be aware of this as it may cause some confusion at Salto doors that are not Bluetooth-capable."

If your site has SALTO Bluetooth-capable wired or wireless online locks, and you have integrated your SALTO server with Command Centre, then you can use the Gallagher Mobile Connect App to open Bluetooth-capable SALTO doors. To request access at the Salto lock, the cardholder needs to press the **Open Salto Door** button, then follow the animation to present their mobile phone to the Salto reader.

For further detail refer to the *Mobile Connect Cloud and App Security TIP.pdf* (located in the `'Mobile Client'` directory of the Command Centre installation files). **Notes:**

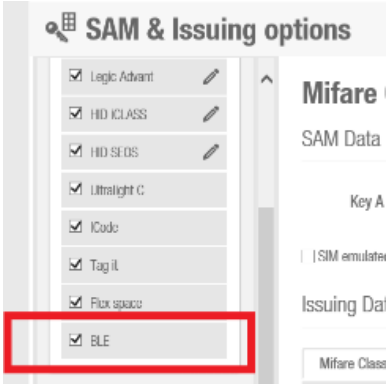
- The Salto Mobile Credential updates every 7 days.
- Only more recent Salto reader models support Mobile Connect when connected as a third-party reader in Command Centre. Any WR 0125 readers will need to be upgraded to later models.

Prerequisites

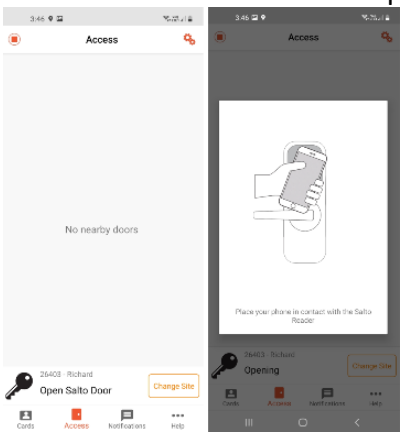
The prerequisites for the Salto BLE credential to be populated to the Gallagher Mobile Connect App are:

- Command Centre mobile connect,
- Command Centre,
- Cloud Server,
- Salto Server,
- Salto BLE licenses,
- Salto Ethernet Encoder (Dongle), and
- SALTO Bluetooth-capable wired or wireless online locks
- Bluetooth settings defined in SALTO, as follows:

  a) Select **System** > **SAM & Issuing options**, and tick **BLE**.



b) From the Gallagher Mobile Connect App, press on **Open Salto Door** and hold near the reader to open the door.



Licensing

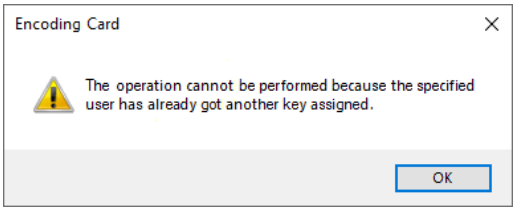
Salto SPACE licensing required:

- C866020 - SALTO BLE SITE LICENSE (SPACE OPT 0028-2 - ANNUAL)
- C866023 - SALTO BLE WIRELESS DOOR LICENSE (SPACE OPT 0033) Converts BLE Offline readers to Online. Requires one per wireless door.

Note: From v9.30, if you are in Salto Native mode you will not require C866020 SALTO BLE SITE LICENSE (only required in Salto Legacy mode).

Troubleshooting - Salto Lock Interface

The following table provides possible solutions to problems you may encounter when using the Salto Lock Interface:

Problem	Solution
On a multi-server site, Cardholders replicate but the Salto options (on the **Salto Options** tab of the Cardholder properties) do not replicate.	They can be adjusted on any server and those options will be synced.
A "Full Re-sync" override has failed and the following alarm has generated: 	The Salto server needs to retrieve its access points, (i.e. Doors and Access Zones) into Command Centre. To do this, an "Update Access Points" override is required. Refer to ***Updating Access Points*** (on page 74-83) for full details.
An attempt to encode another card with the same card number in Native Mode has resulted in the following error message: 	Increase the issue level of this card, or create a new card with a new card number and encode this.

Salto to Command Centre Event Mapping

Introduction

This topic describes the events mapped from Salto ProAccess SPACE 6.10.4.3 to Command Centre.

Note: Anything in [Square Brackets] is a representative token, rather than literal text in the event.

Events

Salto		Command Centre			
Salto ID	**Salto Description**	**Message**	**Event Group**	**Event Type**	**Source**
16	Door opened: inside handle	Button release at [Salto Door].	Non-Card Door Unlock	Button Release Granted	Salto Door
17	Door opened: key	[Cardholder] was granted entry at [Salto Door].	Card Event	Salto Door Access Granted	Salto Door
19	Door opened: multiple guest key	[Cardholder] was granted entry at [Salto Door].	Card Event	Salto Door Access Granted	Salto Door
20	Door opened: unique opening	[Cardholder] was granted entry at [Salto Door].	Card Event	Salto Door Access Granted	Salto Door
21	Door opened: switch	Button release at [Salto Door].	Non-Card Door Unlock	Salto Door Access Granted	Salto Door
22	Door opened: mechanical key	Button release at [Salto Door].	Non-Card Door Unlock	Button Release Granted	Salto Door
24	Door opened: after second double card presented	[Cardholder] was granted entry at [Salto Door].	Card Event	Salto Door Access Granted	Salto Door
25	Door opened: PPD	A PPD was used to perform an emergency opening of the Salto Door [Salto Door].	Non-Card Door Unlock	PPD Emergency Opening	Salto Door
26	Door opened: keyboard	Code only access granted at [Salto Door].	Non-Card Door Unlock	Salto Code only Access Granted	Salto Door
27	Door opened: spare card (hotel)	[Cardholder] was granted entry at [Salto Door].	Card Event	Salto Door Access Granted	Salto Door
28	Door opened: online command	[Salto Door] has opened.	Door Status	Door Opened	Salto Door
33	Door closed: key	[Cardholder] was granted the ability to close [Salto Door].	Card Event	Salto Door Closing Granted	Salto Door
35	Door closed: keyboard	[Cardholder] was granted the ability to close [Salto Door].	Card Event	Salto Door Closing Granted	Salto Door

Salto		Command Centre			
Salto ID	**Salto Description**	**Message**	**Event Group**	**Event Type**	**Source**
37	Key inserted (energy saving device)	[Salto Door] inserted their card into [Cardholder]	Card Event	Card Inserted	Salto Door
38	Key removed (energy saving device)	[Salto Door] removed their card from [Cardholder]	Card Event	Card Removed	Salto Door
40	Start of privacy	Privacy Started for [Salto Door].	Door Status	Start of Privacy	Salto Door
41	End of privacy	End of Privacy for [Salto Door].	Door Status	End of Privacy	Salto Door
49	Start of office mode	[Cardholder] has set [Salto Door] to Office mode	Salto Door Mode Change	Start of Office Mode	Salto Door
50	End of office mode	[Cardholder] has ended Office mode for [Salto Door]	Salto Door Mode Change	End of Office Mode	Salto Door
51	Hotal guest cancelled	Guest key ([Salto Door]) has been cancelled.	Card Event	Guest Key Cancelled	Salto Door
55	New hotel guest key	A new guest key has been issued ([Salto Door]).	Card Event	New Guest Key	Salto Door
56	Start of forced opening (online)	Start of emergency opening for [Salto Door].	Door Status	Start of emergency forced opening	Salto Door
57	End of forced opening (online)	End of emergency opening for [Salto Door].	Door Status	End of emergency opening	Salto Door
58	Start of forced closing (online)	Lockdown initiated for [Salto Door].	Door Status	Start of lockdown	Salto Door
59	End of forced closing (online)	Lockdown ended for [Salto Door].	Door Status	End of lockdown	Salto Door
60	Alarm: intrusion (online)	[Salto Door] has been forced.	Forced Door	Intrusion	Salto Door
61	Alarm: tamper (online)	[Salto Door] has been tampered.	Tamper	Salto Door Tampered	Salto Door
62	Door left opened (DLO)	[Salto Door] open too long.	Door Open Too Long	Door Open Too Long	Salto Door
63	End of DLO (door left opened)	[Salto Door] has been resecured.	Door Status	Door Re-secured	Salto Door
64	End of intrusion	[Salto Door] has been resecured.	Door Status	Door Re-secured	Salto Door
67	End of tamper	[Salto Door] is no longer tampered.	Tamper Return To Normal	Salto Door No Longer Tampered	Salto Door
72	Online peripheral updated	The Salto control unit for [Salto Door] was updated.	Door Status	Salto control unit updated	Salto Door
76	Key updated (online)	A card held by [Cardholder] was updated at [Salto Door].	Card Event	Card Updated	Salto Door

Salto		Command Centre			
Salto ID	**Salto Description**	**Message**	**Event Group**	**Event Type**	**Source**
78	Key deleted (online)	A card held by [Cardholder] was cancelled by the Salto system.	Card Event	Card Cancelled	Salto Server
79	Communication with Salto software lost	[Salto Door] - Command Centre comms interrupted	Command Centre Comms Interrupted	Comms failed to Command Centre	Salto Door
80	Communication with Salto software established	[Salto Door] - Command Centre comms established	Command Centre Comms Established	Controller Command Centre comms established	Salto Door
81	Opening not allowed: key no activated	An unauthorised card ([Cardholder]) was used to attempt access at [Salto Door].	Access Denied	Unauthorised Salto Card	Salto Door
82	Opening not allowed: key expired	An unauthorised card ([Cardholder]) was used to attempt access at [Salto Door].	Access Denied	Unauthorised Salto Card	Salto Door
83	Opening not allowed: key out of date	[Cardholder] was denied access at [Salto Door]. Reason: The access on the card is out of date.	Salto Card Out of date	Card Out of date	Salto Door
84	Opening not allowed: key not allowed in this door	[Cardholder] was denied access at [Salto Door]. Reason: no zone privilege.	Access Denied	No Salto Zone Privilege	Salto Door
85	Opening not allowed: out of time	Access denied at this time for [Cardholder] through [Salto Door].	Access Denied	No Salto access at this time	Salto Door
87	Opening not allowed: key does not override privacy	[Cardholder] was denied access at [Salto Door]. Reason: no privacy override privilege.	Access Denied	No Privacy Override Privilege	Salto Door
88	Opening not allowed: old hotel guest key	An unauthorised card ([Cardholder]) was used to attempt access at [Salto Door].	Access Denied	Unauthorised Salto Card	Salto Door
89	Opening not allowed: hotel guest key cancelled	[Cardholder] was denied access at [Salto Door]. Reason: Card Cancelled or Invalid Issue	Access Denied	Cancelled Salto Card	Salto Door
92	Opening not allowed: no associated authorization	An unauthorised card ([Cardholder]) was used to attempt access at [Salto Door].	Access Denied	Unauthorised Salto Card	Salto Door
95	Opening not allowed: door in emergency state	[Cardholder] was denied access at [Salto Door]. Reason: the door is in an emergency state.	Access Denied	Door in emergency state	Salto Door

Salto		Command Centre			
Salto ID	**Salto Description**	**Message**	**Event Group**	**Event Type**	**Source**
96	Opening not allowed: key cancelled	[Cardholder] was denied access at [Salto Door]. Reason: Card Cancelled or Invalid Issue	Access Denied	Cancelled Salto Card	Salto Door
97	Opening not allowed: unique opening key already used	An unauthorised card ([Cardholder]) was used to attempt access at [Salto Door].	Access Denied	Unauthorised Salto Card	Salto Door
99	Warning: key has not been completely updated (online)	Warning, a card held by [Cardholder] was not fully updated at [Salto Door].	Card Event	Card Not Fully Updated	Salto Door
100	Opening not allowed: run out of battery	[Cardholder] was denied access through [Salto Door]. Reason: The battery was too low to open the door.	Access Denied	Battery Too Low	Salto Door
101	Opening not allowed: unable to audit on the key	[Cardholder] was denied access at [Salto Door]. Reason: There was no buffer space left for the event.	Access Denied	Buffer Full	Salto Door
102	Opening not allowed: Locker occupancy timeout	Locker occupancy timeout for [Salto Door] at [Cardholder]	Card Event	Locker occupancy timeout	Salto Door
104	Blacklisted key deleted.	A card held by [Cardholder] was cancelled by the Salto system.	Card Event	Card Cancelled	Salto Server
113	PPD Connection	A PPD was connected to the Salto Door [Salto Door].	Door Status	PPD Connection	Salto Door
114	Time modified (daylight saving time)	A daylight savings time adjustment occurred for the Salto Door [Salto Door].	Door Status	Daylight savings Time Adjustment	Salto Door
117	RF Lock date and time updated	RF Lock "[Salto Door]" date and time updated	Door Status	RF Lock Date and Time Updated	Salto Door
118	RF Lock updated	RF Lock "[Salto Door]" has been updated.	Door Status	RF Lock Updated	Salto Door

Chapter 75: Nedap Readers

Gallagher Command Centre supports the following Nedap Readers:

Reader	Description
uPASS	*Go:* A long range UHF reader for vehicle identification, read range up to 10 meters (33 ft). *Target:* A long range UHF reader for vehicle identification, read range up to 15 meters (50 ft).
Transit	A long-range vehicle identification reader. Offers identification up to 10 meters (33 ft) with a travelling speed up to 200 km/h (125 mph). The 'Nedap Booster DESFire' feature allows MIFARE DESFire cards to be used with Nedap Booster devices for access with Gallagher Command Centre. See ***Nedap Booster DESFire feature*** (on page 75-5) for full configuration details.
ANPR	The Nedap ANPR License plate reader offers automatic number plate reading. *ANPR Access:* Offers identification from 3 to 6 meters. *ANPR Access HD:* Offers identification from 6 to 10 meters. *ANPR Lumo:* Offers identification from 2 to 10 meters. The 'Nedap ANPR Lumo' feature enhances the experience for sites using Nedap ANPR Lumo cameras (vehicle identification readers). With this feature installed, operators can enter a vehicle's licence plate directly as a text format card number. See ***Nedap ANPR Lumo feature*** (on page 75-11) for full configuration details.

Note: The ANPR Lumo and DESFire Booster customisations are still available. Contact Tech Support if required.

This topic is separated into individual procedures that make up the process for configuring Nedap Readers so they work with Gallagher Command Centre.

Note: There are installation guides available in the `'Utilities\Nedap'` folder of the Command Centre installation files if required.

- ***Nedap uPASS Readers*** (on page 75-2)
- ***Nedap Transit Readers*** (on page 75-5)
- ***Nedap ANPR Lumo Readers*** (on page 75-11)

Nedap uPASS Readers

Connecting the reader

A Nedap Reader is connected to a Gallagher Controller as a Wiegand Reader. For Wiegand Reader connection details, refer to the Gallagher Controller installation note.

Note: Instructions for connecting uPASS Go and uPASS Target readers to an HBUS 4 In 2 Out Door Module - Wiegand are as follows:

For a uPASS…	Connector 2 Wiegand…	to the HBUS 4 In 2 Out Door Module - Wiegand…
Go reader	OUT2	R1/R2 DATA 0
	OUT3	R1/R2 DATA 1
	GND	GND
Target reader	Pin 2 Data 0	R1/R2 DATA 0
	Pin 4 Data 1	R1/R2 DATA 1
	GND	GND

Creating a new third-party reader

Create a new third-party reader for each Nedap Reader.

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
2. **Right click** and select **New...Third Party Reader**.
   By default the **General** tab displays.
3. Enter a Name and Description, and select the division for this third party reader.
4. Configure the remaining tabs as required, and click the **OK** button.

Creating a new Card Type

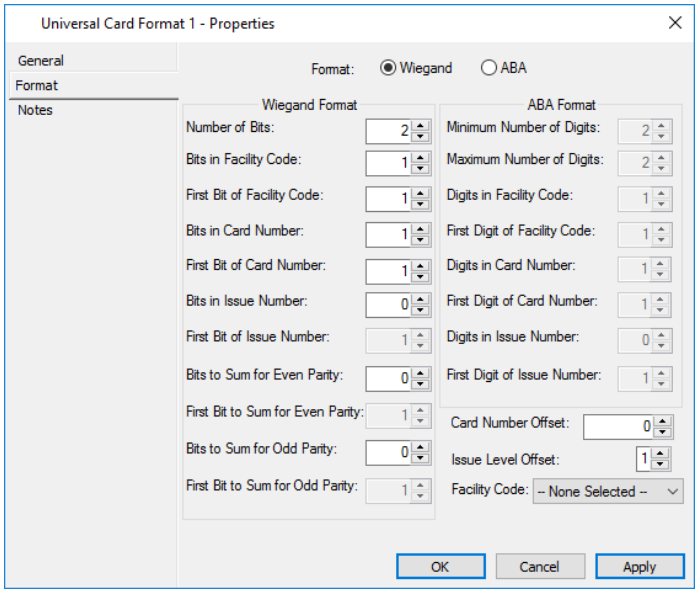
1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. **Right click** and select **New...Card Type**.
   By default the **General** tab displays.
3. Enter a Name and Description, and select the division for this Card Type.
4. Configure the remaining tabs as required, and click the **OK** button.

Creating a new Universal Card Format

Create a new Universal Card Format for each tag format you will be using.

1. Click **Configure** from the menu bar, then **Universal Card Format**.
   The **Universal Card Format** List Window opens.
2. **Right click** and select **New...Universal Card Format**.
3. Enter a Name and Description, and select the division for this Universal Card Format.

4. Click the **Format** tab.
5. Select the **Wiegand** radio button.



6. Change the following fields to the figures indicated, for the type of reader you are using:

Field	uPASS Reader and 26 bit tags	uPASS Reader and 38 bit tags
Number of Bits:	26	38
Bits in Facility Code:	8	12
First Bit of Facility Code:	2	2
Bits in Card Number:	16	24
First Bit of Card Number:	10	14
Facility Code:	A00010	A00010

7. Click the **OK** button.

Assigning the new items to the Controller

1. From the **Hardware** List Window, open the property pages for the Controller that the third-party reader will be assigned to.
2. Click the **Readers** tab.
3. Assign the third-party reader to the appropriate slot, depending on how you wired it to the Controller, or HBUS Wiegand Reader port.
4. Click **OK**.
5. Click the **Card Formats** tab.
6. On the **Universal Card Format** List Window, highlight the new Universal Card Format (created in the previous procedure), and drag and drop it into the **Card Formats** tab of the Controller.

Note: If using a uPASS Reader and both 26 and 38-bit tags, drag and drop both Universal Card Formats (previously created) into the **Card Formats** tab of the Controller.

7. Click the **OK** button.

Creating cards for cardholders and/or vehicles

Create cards for each of the cardholders and/or vehicles as required.
See ***Adding a Card to a Cardholder*** (on page 32-9) for the complete procedure.

Note: When using uPASS Readers, ensure that the Card Type selected uses the Facility Code A00010 as entered into the new Universal Card Format you created earlier.

Nedap Booster DESFire feature

The 'Nedap Booster DESFire' feature allows MIFARE DESFire cards to be used with Nedap Booster devices for access with Gallagher Command Centre.

This section is separated into individual procedures that make up the process for configuring Nedap Booster devices for access with Gallagher Command Centre.

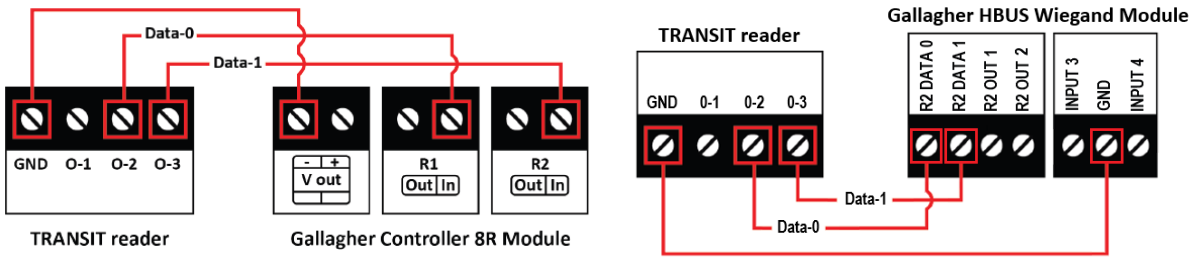
- Nedap TRANSIT reader installation
- Command Centre Nedap Booster configuration
- DESFire Card Type configuration
- Nedap Booster configuration

Nedap TRANSIT reader installation

To install a **Nedap TRANSIT** reader so it is ready to communicate with the Gallagher Controller, connect it to the Controller's 8R Module, or HBUS Wiegand Module as follows:

Wire the TRANSIT Reader…	to the Controller 8R Module…	To the HBUS Wiegand Module:
GND	V out -	GND
Data-0 (0 - 2)	R1-in, R3-in, R5-in or R7-in	R1/R2 Data 0
Data-1 (0 - 3)	R2-in, R4-in, R6-in or R8-in	R1/R2 Data 1

The following diagrams demonstrates wiring the Nedap TRANSIT reader to the R1-in and R2-in ports of a Gallagher Controller 8R Module, or HBUS Wiegand Module:



Command Centre Nedap Booster configuration

This section details the standard Command Centre configuration required to use Nedap Booster devices and TRANSIT readers with Command Centre.

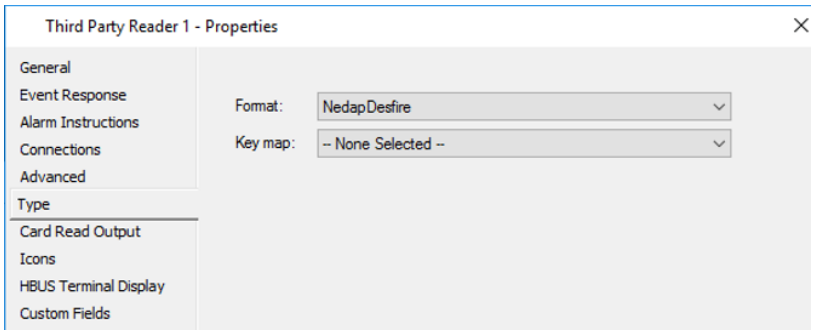
1. Configure Nedap Transit readers as third party readers

Nedap TRANSIT readers are configured in Configuration Client as third party readers and assigned to the appropriate Controller and Door.

a) Create a third party reader.
Note: The ***Creating Readers*** topic (on page 21-57) provides detailed instructions for creating a third party reader.

On the **Type** tab of the Reader properties, add a card format to the third

party reader from the **Format** drop-down list (NedapDesfire).



Note: This option is only needed for MIFARE DESFire cards. Classic cards can work with any format.

b) Open the properties of the Controller that has the Nedap TRANSIT reader connected to it, and click the **Readers** tab.

c) Assign the third party reader to the appropriate slot, depending on how you wired it to the Controller, or HBUS Wiegand Reader port.

d) Click **OK**.

e) Assign the third party readers to the appropriate Door items' **Entry Zone** tabs. Refer to ***Creating Doors*** (on page 22-2) for further detail.

2. Configure vehicles as Cardholders

Vehicles can be configured as Cardholders in Command Centre to allow the vehicle to be assigned a "card" so it can be granted access. The vehicle's "card" is really a Nedap Booster. When the vehicle approaches a Nedap TRANSIT reader, it presents its Nedap Booster to the reader, and the vehicle is either granted or denied access.

a) Create a new Cardholder to represent the vehicle.
Refer to ***Adding a new Cardholder*** (on page 32-2) for the procedure.

b) Assign the vehicle Cardholder to the appropriate Access Group containing vehicle Cardholders.
If you have not created one yet, refer to ***Setting up Access Groups*** (on page 34-4) for the procedure.

c) Assign the vehicle Cardholder a card to represent the vehicle's Nedap Booster. Refer to ***Adding a Card to a Cardholder*** (on page 32-9) for the procedure.
Notes:

- The **Number** field (on the **Cards** tab of the Cardholder properties) must be the Nedap Booster's ID number. The ID number is printed on the back of the Nedap Booster device.
- You can configure the booster to only transmit the Driver ID using the Smartcard Booster Config application.

3. Configure Dual Authorisation

An Access Zone that vehicles enter can be configured with Dual Authorisation. This means access is only granted if the vehicle provides **two** means of

authorisation: a credential (Nedap Booster) held by a Cardholder (vehicle) from the vehicle Access Group and a credential (card) held by a Cardholder (person) from the driver Access Group.

Perform the following procedure to configure an Access Zone so it requires a valid vehicle *and* driver to grant access (Dual Authorisation):

a) Click **Configure** from the menu bar, then **Access Zones**.
The Access Zone List Window opens.

b) Right click on the Access Zone that will require a valid vehicle and driver for access to be granted, and select **Properties**.
Note: If you haven't yet created the Access Zone, create one using ***Adding a new Access Zone*** (on page 10-3) for the procedure.

c) Click the Dual Authorisation tab.

d) From the **First Card** drop-down list, select the Access Group (that contains the vehicle Cardholders) that you wish to access this zone.

e) From the **Second Card** drop-down list, select the Access Group that contains the drivers you want to access this zone.

f) Ensure the Access Zone's Access Mode is set to 'Dual Auth - No PIN' during the times Dual Authorisation is required. Do this by either:
- configuring and applying a 'Schedule' on the **Access Mode** tab of the Access Zone, OR
- overriding the zone to 'Dual Auth - No PIN' on the **Status and Overrides** tab of the Access Zone.

g) Click **OK** to close and save your changes.

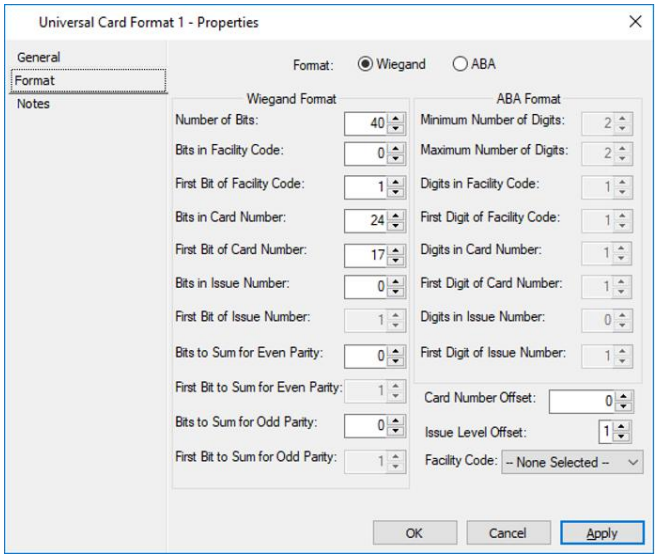
4. Configure the Universal Card Format

Note: The ***Adding a new Universal Card Format*** topic (on page 26-2) provides detailed instructions for configuring a Universal Card Format (UCF).

Perform the following procedure to configure an Access Zone so it requires a valid vehicle *and* driver to grant access (Dual Authorisation):

a) On the **Format** tab of the UCF, select the **Wiegand** radio button and ensure the following fields are populated as follows:

Field	Value
Number of Bits:	40
Bits in Facility Code:	0
First Bit of Facility Code:	N/A
Bits in Card Number:	24
First Bit of Card Number:	17
Facility Code:	Select the facility code on the Card Type that will be used when you create cards for cardholders/vehicles later.



b) Open the properties of each Controller connected to a Nedap TRANSIT reader, and click the **Card Formats** tab.

c) Assign the UCF you have just created by dragging it (or using copy and paste) into the grid on the **Card Formats** tab.

5. Creating cards for cardholders and/or vehicles

Create cards for each of the cardholders and/or vehicles as required.
See ***Adding a Card to a Cardholder*** (on page 32-9) for the complete procedure.
Note: When using Transit Readers, ensure that the Card Type selected uses the same Facility Code as the new Universal Card Format you created earlier.

DESFire Card Type configuration

MIFARE DESFire cards that are to be used with Nedap Booster devices must be created as a certain card type.

1. Create a new card type.
   Note: The ***Setting up Card Types*** topic (on page 7-2) provides detailed instructions for creating a new card type.
2. Edit the card layout by **right-clicking** on the new Card Type you just created, and select **Edit Card Layout**.
   The **Card Editor** window displays.
3. Select **New Non-diversified MIFARE DESFire Object**.
   Note: This particular object MUST be selected for use with Nedap Boosters.
   Refer to ***Adding a Non-diversified MIFARE DESFire object*** (on page 47-46) for the full procedure.

Nedap Booster configuration

Introduction

To enable your Nedap Boosters to read MIFARE DESFire cards, you must have them read a configuration card. This card is encoded with configuration

instructions for a Nedap Booster. When a Nedap Booster reads this card, it reads and applies the configuration to enable it to read DESFire cards.

Prerequisites

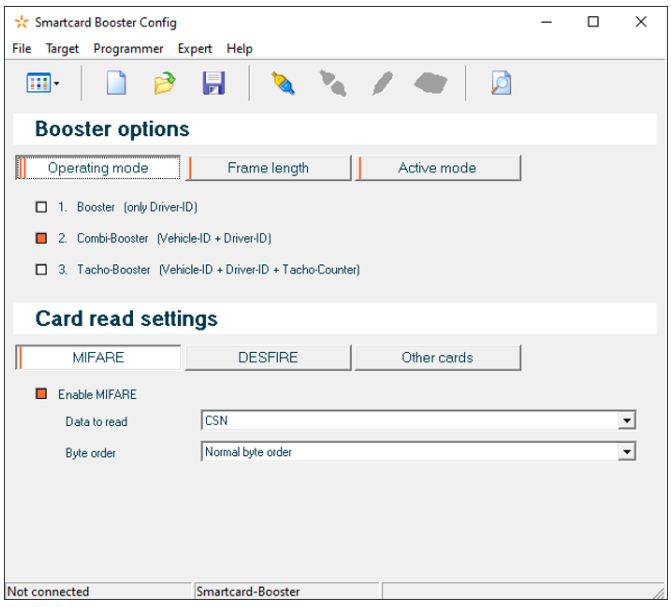
For this procedure you will need:

- the Smartcard Booster Config installer file **'CfgSmartcard-install.msi'** located in the `'Utilities\Nedap\Transit Reader'` folder of the Command Centre installation files.
- the configuration template file provided
  Note: You must restrict access to the **'Classic_DESFire.sbcf'** file. This file contains sensitive configuration data, so must be stored securely.
- access to the Card Type layout properties (in Configuration Client)
- a blank MIFARE Classic card (for configuration)
- a USB MIFARE card encoder (ensure the relevant driver is installed)
- the Nedap Boosters you wish to configure

Procedure

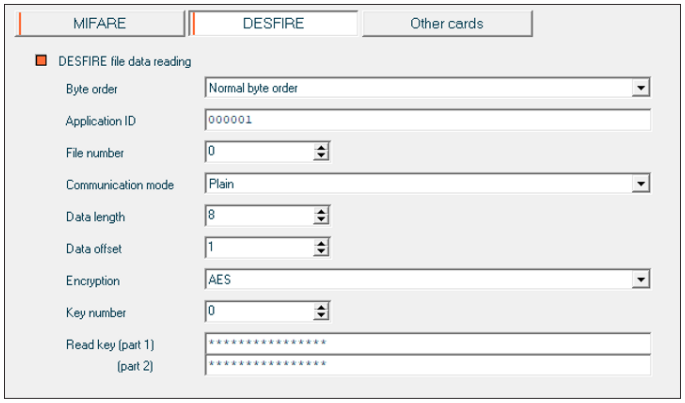
To configure the Nedap Booster configuration card, perform the following procedure:

4. Install the utility by running the installation file **'CfgSmartcard-install.msi'**. Follow the installation steps to install the Smartcard Booster Config utility.
5. If 'Launch Smartcard Booster Config' is selected when you finish installation, the utility opens. Otherwise, open 'Smartcard Booster Config' from the **Start** menu.

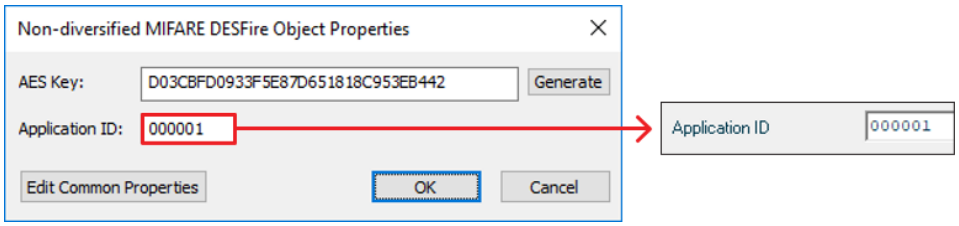


6. Ensure your USB MIFARE card encoder is connected to your PC.
7. Click the  button and select your USB MIFARE card encoder, then click **OK**.
8. From the menu bar, select **File** > **Open...**
   The Open window displays.

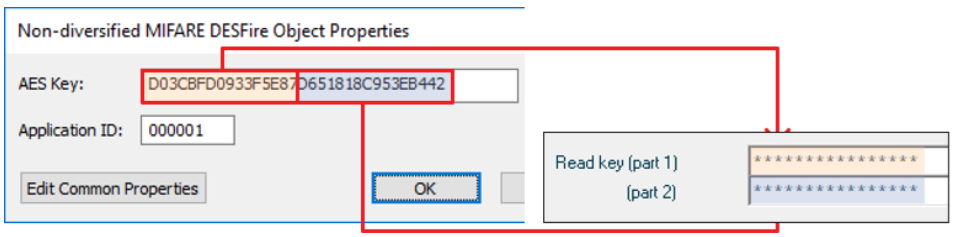
9. Browse to and select the **'Classic_DESFire.sbcf'** file and click **Open**. The utility loads the configuration.
10. Under 'Card read settings', click the **DESFIRE** tab.



11. In the **Application ID** field, enter the Application ID from the DESFire object in your DESFire Card Type's card layout.



12. The **Read key** is split into two parts. Part 1 is the first half (first 16 characters) of the AES Key from the DESFire object in your DESFire Card Type's card layout. Part 2 is the other half.



13. Place your blank MIFARE Classic card on the USB MIFARE card encoder.
14. Click the  button to write the configuration to the card, and click **Yes** in the pop-up window.
15. For each Nedap Booster you wish to enable DESFire compatibility for, place the configuration card inside the Nedap Booster as you would with a regular card.
16. Press the button on the Nedap Booster device to load configuration from the card to the Nedap Booster device.
17. To verify that you have enabled MIFARE DESFire on the Nedap Booster:
    a) Assign a DESFire card of the required Card Type to a Cardholder.
    b) Encode a DESFire card with this card.
    c) Check that the card can be used with the Nedap Booster to grant access to an Access Zone at a TRANSIT reader.

Nedap ANPR Lumo feature

The 'Nedap ANPR Lumo' feature enhances the experience for sites using Nedap ANPR Lumo cameras (vehicle identification readers). With this feature installed, operators can enter a vehicle's licence plate directly as a text format card number.

This section is separated into individual procedures that make up the process for configuring Nedap ANPR Lumo devices for access with Gallagher Command Centre.

- First time configuration
- Modifying existing configuration

First time configuration

If you do not have any licence plate cards configured already, perform the following procedure to set up your Nedap ANPR Lumo cameras and create licence plate cards:

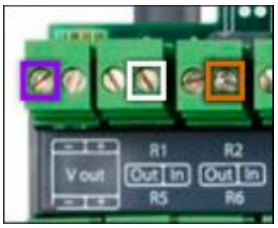
Nedap ANPR Lumo reader installation

To install a **Nedap ANPR Lumo** reader so it is ready to communicate with the Gallagher Controller, connect it to the Controller's 8R Module, or HBUS Wiegand Module as follows:

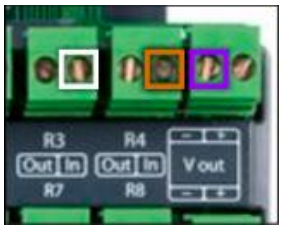
Wire the Nedap ANPR Lumo…	to the Controller 8R/4R Module…	To the HUS Wiegand Module…
White wire (Wiegand Data - 0)	R1-in or R3-in	R1/R2 Data 0
Brown wire (Wiegand Data - 1)	R2-in or R4-in	R1/R2 Data 1
Purple wire (Wiegand GND)	V out -	GND

For example:

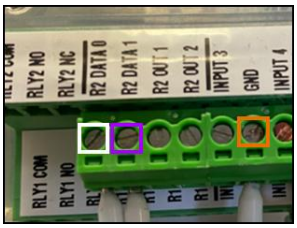
Controller 8R/4R Module



Or,



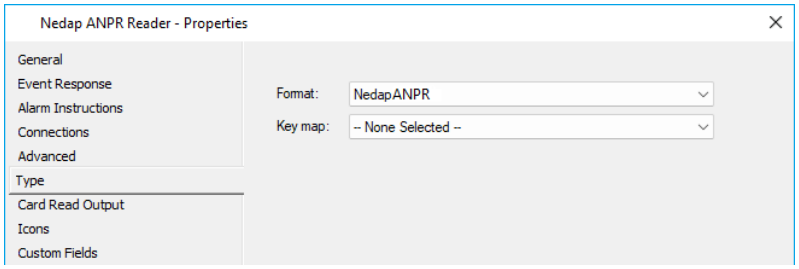
HUS Wiegand Module



Configuration in Command Centre

1. In Gallagher Configuration Client, configure a Third Party Reader for each Nedap ANPR Lumo camera.
   Note: The ***Creating Readers*** topic (on page 21-57) provides detailed instructions for creating a third party reader.

   On the **Type** tab of the Reader properties, add a card format to the third party reader from the **Format** drop-down list (NedapANPR).



2. Open the properties of each Controller that has a Nedap ANPR Lumo camera connected to it, and click the **Readers** tab.
3. Assign the third party reader to the appropriate slot, depending on how you wired it to the Controller, or HBUS Wiegand Reader port.
4. Click **OK**.
5. Assign the Third Party Readers to the appropriate Door items' **Entry Zone** tabs. Refer to ***Creating Doors*** (on page 22-2) for further detail.
6. Click **Configure** from the menu bar, then **Card Types**.
   The Card Type List Window opens.
7. From the Card Type list window, select **New…Card Type**.
8. Enter a **Name**, (e.g. 'Nedap ANPR licence plate') and **Description**, then click the **Setup** tab.
9. Configure the Card Type with the following settings:
   - **Region Code:** A
   - **Facility Code:** 00006
   - **Format:** Text
10. Configure the remaining settings as required.
    Refer to ***Setting up Card Types*** (on page 7-2) for full instructions.
11. Open the properties of each Cardholder that requires a licence plate card for gaining access with a vehicle.
12. Click the **Cards** tab, and assign a new card. Select the licence plate Card Type you have created (in Steps 12-15) and enter the required licence plate number as the card Number. Card numbers are case-sensitive; enter the licence plate in all capital letters.
13. Click **Configure** from the menu bar, then **Universal Card Format**.
    The Universal Card Format List Window opens.
14. Create a new Universal Card Format for each tag format you will be using. Refer to ***Adding a new Universal Card Format*** (on page 26-2) for detailed instructions for configuring a Universal Card Format (UCF).
15. On the **Format** tab of the UCF, select the **Wiegand** radio button and ensure the following fields are populated as follows:

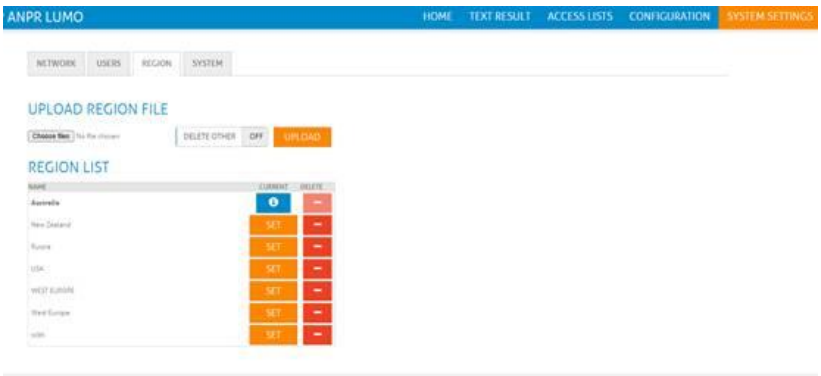
Field	Value
Number of Bits:	64
Bits in Facility Code:	4
First Bit of Facility Code:	1
Bits in Card Number:	60

Field	Value
First Bit of Card Number:	5
Facility Code:	A00006

16. Create cards for each of the cardholders and/or vehicles as required. See ***Adding a Card to a Cardholder*** (on page 32-9) for the complete procedure. **Note:** When using ANPR Readers, ensure that the Card Type selected uses the Facility Code A00006 as entered into the new Universal Card Format you created earlier.

Nedap ANPR Lumo camera configuration in a web browser

1. Access your Nedap ANPR Lumo camera so you can configure it in your web browser as follows:
   d) Enter the camera's IP address into your web browser (Internet Explorer is not supported). The default IP address is 192.168.3.15
   e) Enter the Username 'admin' and Password 'secret' to log in.
   f) If your camera's IP address is still the default, you should change it if you have more than one Nedap ANPR Lumo camera.
2. Enable the 'Wiegand64' READ action on the camera, so the camera communicates to the Gallagher Controller, as follows:
   a) In the camera's settings in your web browser, go to **CONFIGURATION** and click the **ACTIONS** tab.
   b) Expand the READ actions and click **ADD**.
   c) In the ADD/EDIT ACTION window, select **WIEGAND64**.
   d) Ensure it is set to enabled, then click **SAVE**.
3. Set the appropriate classifier for your country/region so the camera reads licence plates correctly, as follows:
   a) In the camera's settings in your web browser, go to **SYSTEM SETTINGS** and click the **REGION** tab.
   b) 'SET' the appropriate classifier for your country/region from the **REGION LIST**.



4. Save your Nedap ANPR Lumo camera's configuration as follows:
   a) In the camera's settings in your web browser, go to **SYSTEM SETTINGS** and click the **SYSTEM** tab.
   b) Select **SETUP SERIAL** under 'System Management'.
   The SETUP SERIAL dialog displays.



c) Ensure **BASIC** is selected (older ANPRs do not have the SETUP serial).

d) Click the **APPLY** button. The SETUP SERIAL dialog closes.

e) Click the **SAVE CONFIGURATION** button.

Modifying existing configuration

If you already have licence plate cards configured with decimal-converted card numbers (old method), perform the following procedure to re-configure them for the Nedap ANPR Lumo feature:

1. In Gallagher Configuration Client, open the properties of all Controllers that have Nedap ANPR cameras connected to them.
2. Click the **Card Formats** tab.
3. Remove the Universal Card Format that has been configured to convert licence plate data to decimal. This Universal Card Format should be configured with Facility Code A00006.
4. Open the properties of all Cardholders that have been assigned cards with decimal-converted licence plate card numbers.
5. Click the **Cards** tab.
6. Remove all cards that have a card number that is a licence plate converted to decimal.
7. Open the Card Type window and delete the Card Type that those decimal-converted licence plate cards were using. This Card Type should have a Facility Code of A00006.
8. **Right-click** in the Card Type window and select **New…Card Type**.
9. Enter a **Name**, (e.g. 'Nedap ANPR licence plate') and **Description**, then click the **Setup** tab.
10. Configure the Card Type with the following settings:
    - **Region Code:** A
    - **Facility Code:** 00006
    - **Format:** Text
11. Configure the remaining settings as required.
    Refer to ***Setting up Card Types*** (on page 7-2) for full instructions.
12. For each Cardholder from whom you removed a card (in Step 6), assign them a new card of the new Card Type you have created (in Steps 8-11). For the card number, enter the licence plate number as text (not converted to decimal). Card numbers are case-sensitive; enter the licence plate in all capital letters.

Chapter 76: Aperio Integration

Introduction

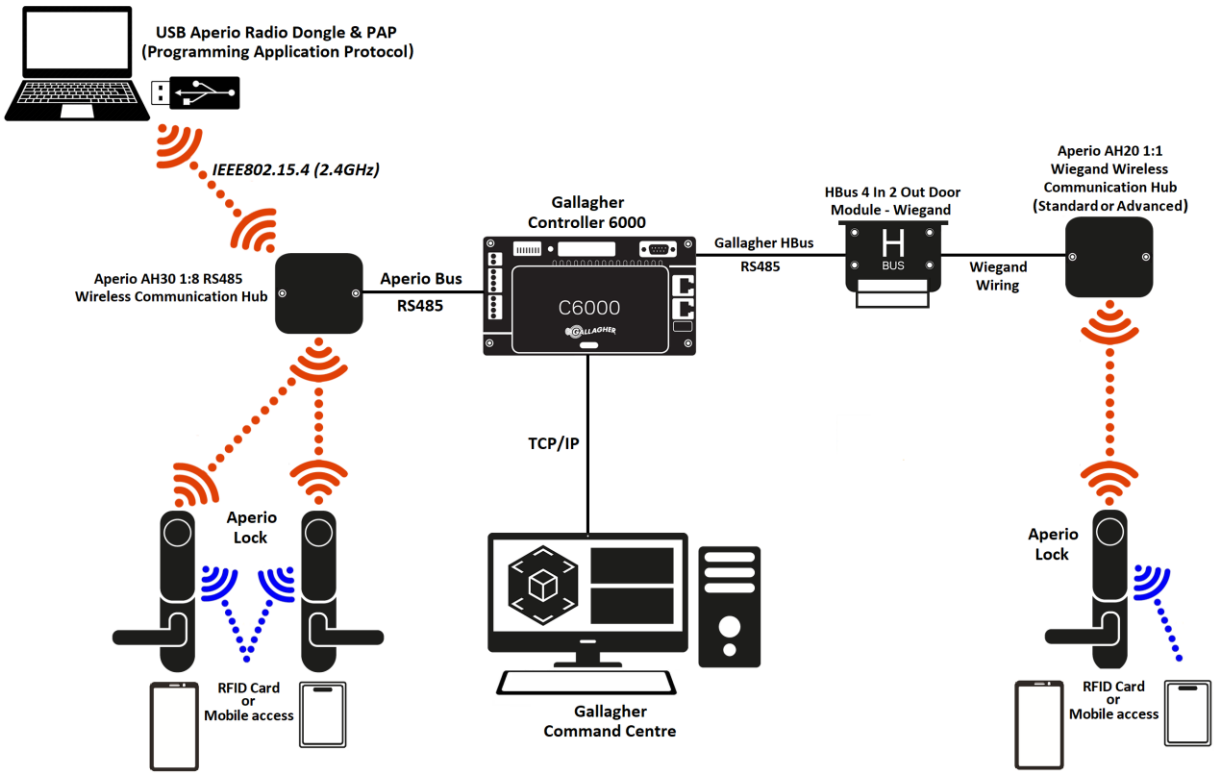
The Aperio Integration is a licensed feature of Gallagher Command Centre. This feature provides a solution for MIFARE SmartCard access through an Aperio unwired lock, (e-cylinder or escutcheon).

- MIFARE CSN
- MIFARE Classic
- DESFire EV1 to EV3
- Mobile Credential

Note: Although Command Centre supports all of these card types, compatibility depends on the type of Aperio lock you are using. To configure mobile credentials you will need to use the latest PAP software and firmware located in the `'Utilities\Aperio'` directory of the Command Centre installation files. Refer to your Aperio Lock documentation for information on what cards are compatible with your lock.

The Aperio System

An Aperio wireless lock contains a MIFARE SmartCard reader, and works with MIFARE or DESFire cards and mobile. The reader reads the information from a cardholder's SmartCard or Mobile Phone when they attempt to gain access at the door. This information is sent wirelessly from the lock to a communication hub, which is connected directly to a Gallagher Controller. Gallagher Command Centre then makes the access decision. The decision is sent via the communication hub to the lock and access is granted or denied.



Aperio Doors function similarly to other Command Centre doors. Some of their features include being able to:

- Apply Access Zone overrides in real time (refer to the ***Performing Overrides*** on page 45-7 for more details)
- Apply Lock / Unlock / Lockdown changes in real time (refer to the ***Performing a Lockdown Override*** on page 10-12 for more details)
  Note: The above functionalities are applied to Version 3 (V3) locks in real time, but Version 2 (V2) locks still require a card to be badged in order for the change to take effect.
- Support all Access Zone modes (including PIN and Card access, dual-auth, and Code or Card mode) (see ***Access Zones*** on page 10-1 for further detail)

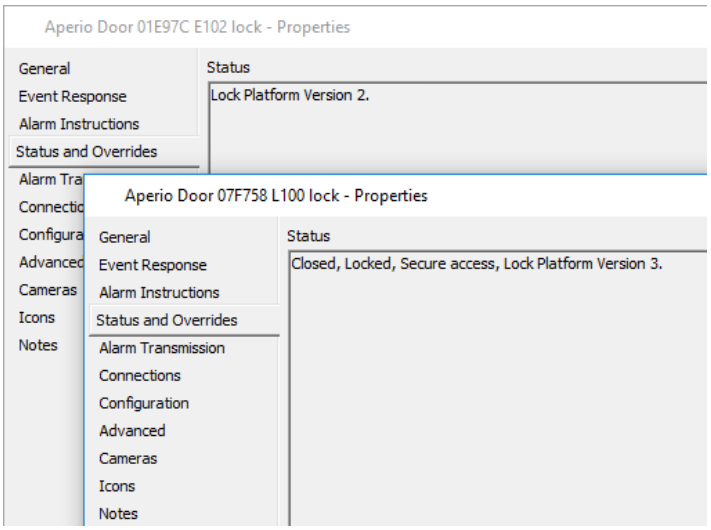
Aperio doors also have unique functionality, for example:

- Single Card/Double Card Access Zone Override (see ***Performing Overrides on an Aperio Door*** on page 76-39)
- Privacy Mode (see Configuring Access Group Privileges for Aperio on page 76-38)
- Security Mode (see ***Configuring the Security Mode*** on page 76-57)
- Override Credentials for Offline Access (see ***Configuring Override Credentials for Offline Access*** on page 76-70)
- Enable Smart Credentials (see ***Enabling the Smart Credential cache (Dynamic cache)*** on page 76-64)

To see what version of lock you have, open the door's Properties window in Configuration Client and click on the **Status and Overrides** tab. The lock version number will be listed in the **Status** field.

Notes:

- Controllers update the clock in Aperio devices every 24 hours.
- Version 2 locks will only display version information; version 3 locks will also display the lock's status.



- Status displayed in Version 3 locks would vary as per the sensors present in the lock. The following table lists the sensors supported by different locks.

	Aperio Models										
Sensors	**C100**	**H100**	**P100**	**KS100**	**K100**	**G100**	**R100**	**E100**	**IN100**	**AU100**	**L100**
DPS (Door Position Sensor)	×	×	×	✓	✓	✓	×	×	✓	✓	✓
RX (Request-to-exit)	×	×	×	×	×	✓	×	✓	✓	✓	✓
DX (Deadbolt)	×	×	×	×	×	×	×	×	×	×	✓
CX (Key override)	×	×	×	×	×	×	×	×	×	×	✓
Tamper	×	×	×	✓	×	×	×	×	×	×	✓

- Aperio locks/readers that do not have any sensors, (i.e. C100, H100 and P100) will not show anything in the status except the platform version. Aperio locks/readers with DPS will show the open/closed lock state along with the Access Zone state.
- Although the KS103 locks do not have CX sensors, when a key is used to unlock the door, a "door forced" alarm is generated.

Select the item below that you require further detail on:

- ***Aperio Communication Hubs*** (on page 76-4)
- ***Connecting the communication hubs to a Gallagher Controller*** (on page 76-7)
- ***Aperio Site Configuration*** (on page 76-10)
- ***Gallagher Command Centre Site Configuration*** (on page 76-29)
- ***Configuring the Aperio Locks/Readers*** (on page 76-42)
- ***Troubleshooting - Aperio Integration*** (on page 76-78)

Aperio Communication Hubs

Introduction

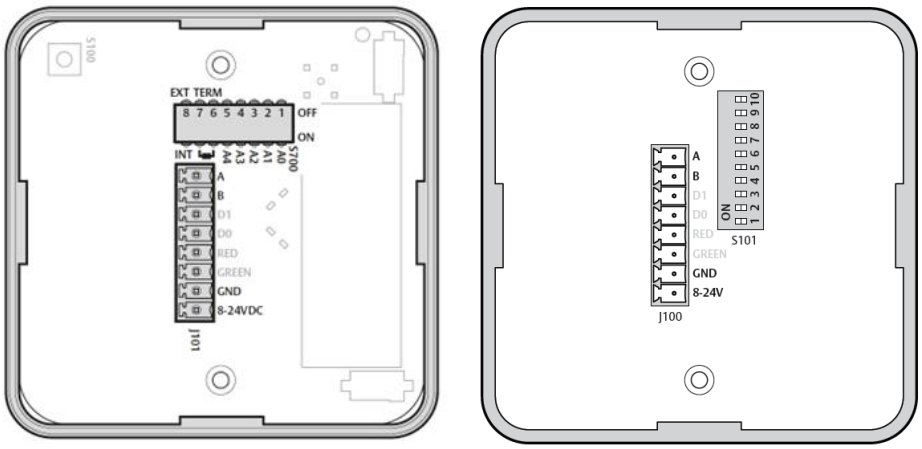
Aperio Hubs supported by Command Centre are:

- Aperio AH30 Standard 1:8 RS485 Hubs
- Aperio AH20 1:1 Wiegand Hubs:
  - Aperio AH20 Standard Wiegand Hubs
  - Aperio AH20 Advanced Wiegand Hubs
- The latest Gen5 Hubs have a tamper switch and 8 DIP switches, as opposed to the original Hubs with 10 DIP switches.

Aperio AH30 Standard 1:8 RS485 Hubs

Aperio AH30 standard hubs connect into the RS485 bus on a Gallagher Controller. Each AH30 Gen5 hub can support 16 locks, and AH30 standard hubs can be paired with up to 8 Aperio locks. The hubs can also be daisy-chained together to have multiple hubs on a single RS485 bus.

AH30 Gen5 connectors *AH30 Standard connectors*



Hub Connector	Description
A	RS485 Data A.
B	RS485 Data B.
GND	GND = Signal ground. Should be connected to EAC system GND and power supply GND.
8-24 VDC	Power supply input, 8-24 VDC, 1.1 W.

For DIP switch settings refer to ***Connecting the communication hubs to a Gallagher Controller*** (on page 76-7).

Aperio AH20 1:1 Wiegand Hubs

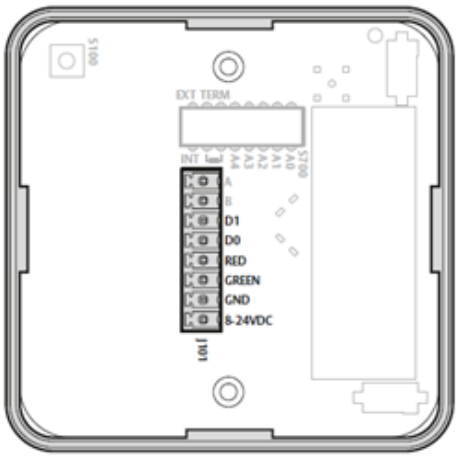
As an entry level installation, an Aperio Wireless Lock may be connected to a Gallagher Controller through either an "Aperio AH20 Advance Wiegand" Hub or an "Aperio AH20 Standard" Hub. Each Aperio Wiegand Hub can only support one Aperio wireless lock or reader.

AH20 Standard Wiegand Hubs

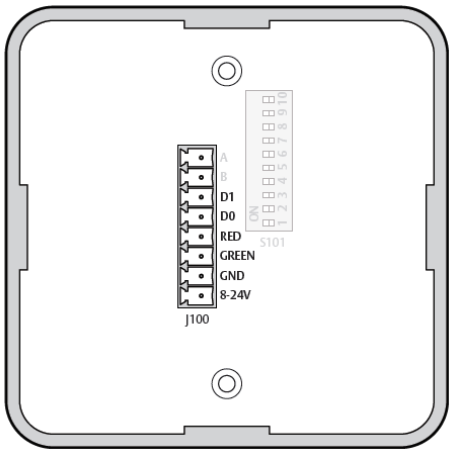
When installed in this configuration, the Aperio wireless lock will only be able to offer basic functionality at the same level as other standard Wiegand third party readers. Gallagher Command Centre will not be able to distinguish an Aperio Wiegand Hub/Lock configuration from other standard wired Wiegand readers.

Note: AH20 Standard Wiegand Hubs do not support battery monitoring, DPS (Door Position Sensor), RX (Request-to-exit), or tamper.

AH20 Gen5 Wiegand connectors



AH20 Standard Wiegand connectors



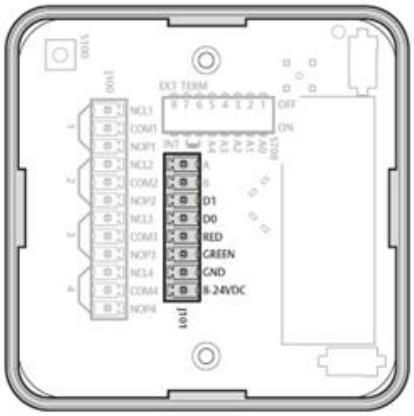
The AH20 communication hub has four Wiegand signals plus ground. The following table describes the purpose and connection of these signals:

Hub Connector	Description	Connected to
DATA 0	Wiegand Data 0 signal	Output from AH20 hub that connects to Gallagher Wiegand device DATA0.
DATA 1	Wiegand Data 1 signal	Output from AH20 hub that connects to Gallagher device DATA1.
GREEN	Wiegand Green LED signal	Input to AH20 hub, that connects to Gallagher device Out 1, used for access decision from the Gallagher Controller.
RED	Wiegand Red LED signal	Input to AH20 hub, that connects to Gallagher device Out 2, used for access decision from the Gallagher Controller. (Alternatively, leave unconnected if signal is selected not to be used by DIP switch 1.)
GND	Ground	Signal ground needs to be common with the Gallagher device and the power supply GND.
8-24 VDC	Positive voltage	Power supply positive. Power supply input, 8-24 V DC. The power supply shall be a Limited Power Source (LPS) according to EN 60950-1. The power supply shall be 3A over current protected. Wire requirements 16-22 AWG.

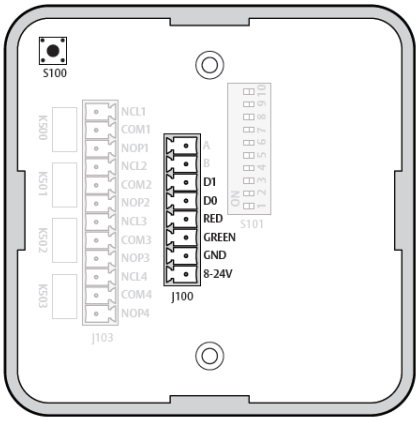
AH20 Advanced Wiegand Hubs

The "AH20 Advanced Wiegand" Hub provides for additional relays at the Wiegand connection point to facilitate outputs from the Aperio wireless lock. Such outputs could be used to monitor the door position sensor, key override, request to exit, or any other sensor that may be present on an Aperio lock.

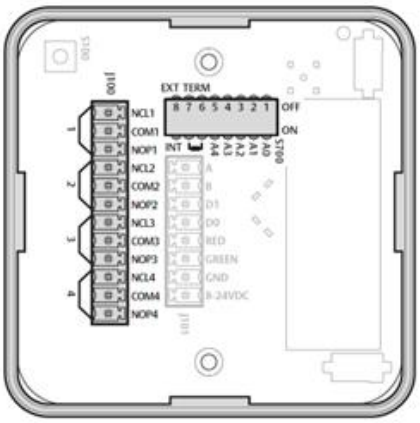
AH20 Gen5 Advanced Wiegand connectors



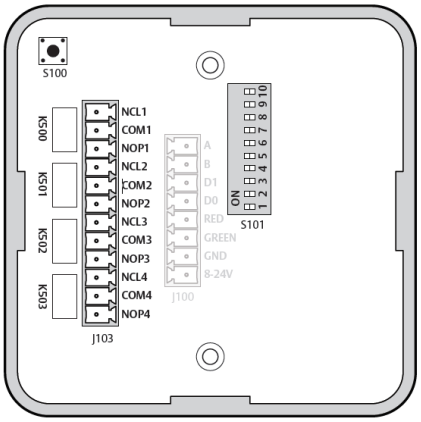
AH20 Standard Wiegand connectors



AH20 Gen5 Advanced Wiegand connectors



AH20 Standard Wiegand connectors



Relays	Description
Relay 1/K500	DPS (Door Position)
Relay 2/K501	RX (Request to exit)
Relay 3/K502	Battery Alarm Output
Relay 4/K503	Tamper Alarm Output /Lock Jammed

Relay Contacts	Description
NCL	Normally Closed
COM	Common
NOP	Normally Open

Note: The latest Gen5 Hubs have a tamper switch and 8 DIP switches, as opposed to the original Hubs with 10 DIP switches.

For further details of connections on the AH20 Hubs, refer to ***Aperio Hub AH20-AH30 Installation Instructions.pdf***

Connecting the communication hubs to a Gallagher Controller

The RS-485 bus

The RS-485 bus is made up of a pair of twisted-pair cable with characteristic impedance between 90 Ohm & 120 Ohm. The maximum bus length is 1000m. If there is more than one communication hub to connect they should be connected in a daisy chain (not a star) on the Aperio RS-485 bus so that all RS485 A connectors are connected together and all RS485 B connectors are connected together. Both ends of the Aperio RS-485 bus must be terminated.

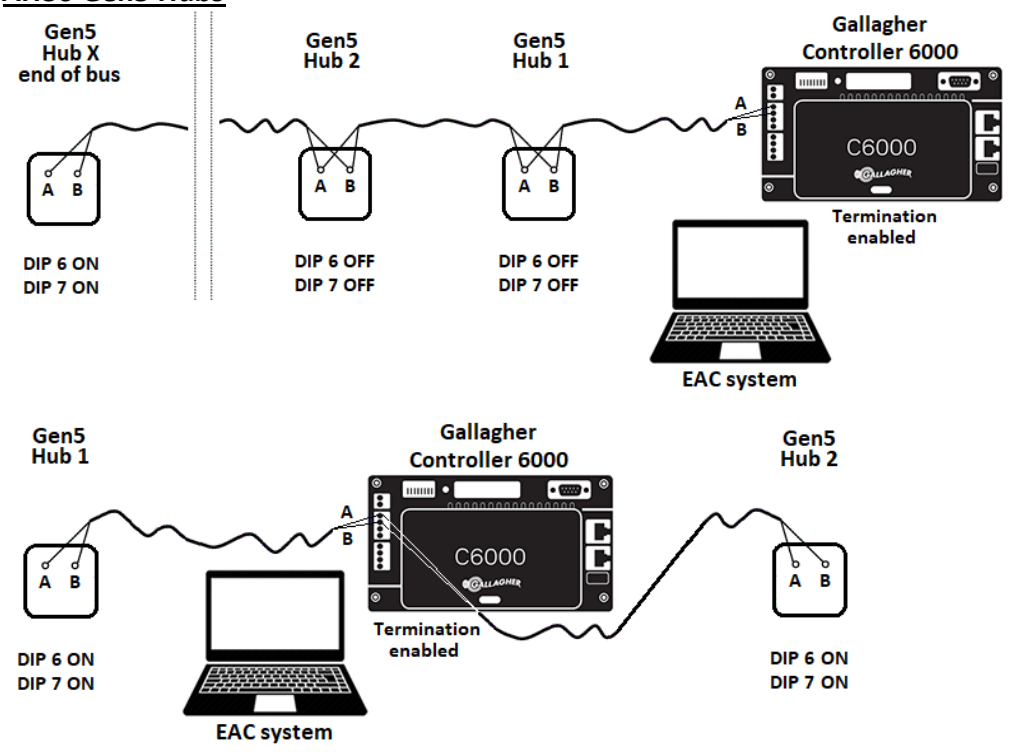
AH30 Hubs

Aperio AH30 Hubs connect directly into the RS-485 bus. The RS485 bus needs to be configured for Aperio from the Controller's **Setup** tab in Command Centre. Note that other devices such as HBUS units will not be able to be used on this Aperio RS485 bus line. Aperio AH30 Hubs do not connect into I/O Expansion Boards.

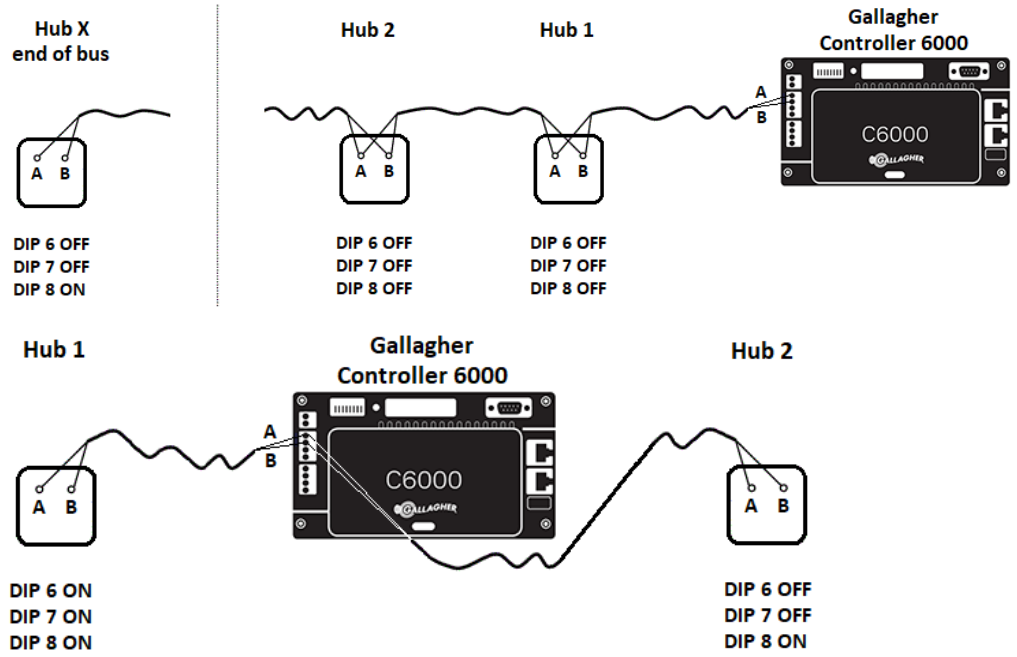
DIP switch settings for AH30 Hubs

The communication hub DIP switches 1-4 can be used to address the communication hub, or by using the Aperio Programming Application Protocol (PAP). It is advised to use the Aperio PAP to address the communication hubs rather than the dip switches, as this is a more secure method. A communication hub at the end of the bus must have switch 8 of the DIP switch in position ON. All other communication hubs must have switch 8 of the DIP switch in position OFF. Pull up and pull down-resistors should be enabled once per bus. However, Gallagher Controllers already have hard wired pull up and pull down resistors fitted. This means all of the communication hubs should have switches 6 and 7 set to the OFF position.

AH30 Gen5 Hubs



AH30 Standard Hubs



The purpose of each DIP switch is summarized in the table below:
Note: Settings indicated in **Bold** text are the Gallagher settings.

AH30 Gen5 Hubs

DIP Switch	Label	Description
1-5	A0-A4	RS-485 addressing BIT 0-BIT 4. ON = Address bit set. **OFF** = Address bit NOT set.
6 - 7	Term	Controls use of termination resistor between RS485 A & RS485 B. For termination to be enabled, both switches must be set to ON. ON = 120 Ohm termination resistor connected/enabled. **OFF** = 120 Ohm termination resistor disconnected/ disabled.
8	Int/Ext	Controls use of external/internal antenna if required. **ON** = Selects use of Internal antenna OFF = Selects use of External antenna

AH30 Standard Hubs

DIP Switch	Label	Description
1-5	A0-A4	RS-485 addressing BIT 0-BIT 4. ON = Address bit set. **OFF** = Address bit NOT set.
6	Down	RS485 pull down resistor (620 Ohm); set at the Controller. ON = 620 Ohm pull down connected. **OFF** = 620 Ohm pull down disconnected.
7	Up	RS485 pull down resistor (620 Ohm); set at the Controller. ON = 620 Ohm pull down connected. **OFF** = 620 Ohm pull down disconnected.
8	Term	Controls use of termination resistor between RS485 A & RS485 B. ON = 100 Ohm termination resistor connected. **OFF** = 100 Ohm termination resistor disconnected.

DIP Switch	Label	Description
9		Not used.
10	Int/Ext	Controls use of external/internal antenna. **ON** = Internal antenna. OFF = External antenna.



Example 1: Hub with DIP switches OF for not an end-of-line hub with External antenna.



Example 2: Hub with DIP switches 6, 7 and 8 ON for an end-of-line hub with Internal antenna.

AH20 Hubs

The communications protocol used on a Wiegand interface is known as the Wiegand protocol. The Aperio AH20 1:1 Wiegand Hubs connect into the following Gallagher Devices:

Part No.	Description	Wiegand Devices
C300665	HBUS Wiegand Door Module	2 x AH20 Wiegand Hubs
C300181	8R Module	4 x AH20 Wiegand Hubs
C300141	4R Module	2 x AH20 Wiegand Hubs

When using HBUS Wiegand door or 8R/4R module, the GREEN hub connector should be connected to OUT2.
Gallagher recommends that the Wiegand wiring between the Gallagher Controller and the Aperio AH20 Hub is installed to national wiring regulations.

DIP switch settings for AH20 Hubs

The purpose of each DIP switch is summarized in the table below:
Note: Settings indicated in **Bold** text are the Gallagher settings.

AH20 Gen5 Wiegand Hubs

DIP Switch	Label	Description
1	A0	Controls use of Red LED signal for access decision. ON = Red LED is used. **OFF** = Red LED is ignored.
2	A1	Set to **OFF** by default. Reserved for future use.
3	A2	Controls addition of parity bits if required. ON = Addition of parity bits is enabled. **OFF** = Addition of parity bits is disabled. Credentials are transmitted as received.

DIP Switch	Label	Description
4	A3	Controls byte order of transmitted credentials. ON = The byte order is reversed on the Wiegand interface compared to what is received from the Aperio lock. **OFF** = The byte order is left as is.
5	A4	Used in "Pairing Mode". ON = Starts in pairing mode. **OFF** = Normal use. **Note:** If the DIP switch is moved from ON to OFF within 10 seconds from boot up and the Hub LED is lit, all paired devices wi be unpaired.
6-7		Not applicable (only used for AH30).
8	Int/Ext	Controls use of external/internal antenna. **ON** = Internal antenna. OFF = External antenna.

AH20 Wiegand Hubs

DIP Switch	Label	Description
1	A0	Controls use of Red LED signal for access decision. ON = Red LED is used. **OFF** = Red LED is ignored.
2	A1	Set to **OFF** by default. Reserved for future use.
3	A2	Controls addition of parity bits if required. ON = Addition of parity bits is enabled. **OFF** = Addition of parity bits is disabled. Credentials are transmitted as received.
4	A3	Controls byte order of transmitted credentials. ON = The byte order is reversed on the Wiegand interface compared to what is received from the Aperio lock. **OFF** = The byte order is left as is.
5	A4	Used in "Pairing Mode". ON = Starts in pairing mode. **OFF** = Normal use.
6-8	Down	Not applicable (only used for AH30).
9		Not used.
10	Int/Ext	Controls use of external/internal antenna. **ON** = Internal antenna. OFF = External antenna.

Aperio Site Configuration

This section contains information on the following configuration instructions required:

- ***Installing the Aperio PAP software*** (on page 76-11)
- ***Creating a new installation*** (on page 76-12)
- ***Scanning for Communication hubs*** (on page 76-15)
- ***Configuring the Hub addressing mode*** (on page 76-17)
- ***Pairing the Aperio locks*** (on page 76-19)
- ***Configuring the Radio Channels*** (on page 76-21)
- ***Upgrading Aperio hubs/locks firmware*** (on page 76-25)

Installing the Aperio PAP software

Introduction

The Aperio programming application is used for the configuration of a door installation. It is normally installed on a laptop and is used with an Aperio USB radio dongle connected to one of the USB ports. The Aperio Programming Application Protocol (PAP) uses the USB radio dongle to connect to a communication hub and an online lock (via the communication hub) or directly to an offline lock. Version 3 locks can also be connected to PAP software using a USB micro connection.
The file for installing PAP s/w, "setup-progapp-30.0.23-62f3555" file is available in the **`'Utilities\Aperio'`** directory of the Command Centre installation files.
Follow the procedure below to install the PAP software. Refer to *'Aperio programming application Manual'* for further details. This manual can be found in the **`'Utilities\Aperio'`** directory of the Command Centre installation files.

Computer Specifications

The Aperio programming application should be installed on a computer with the following specifications:

- Laptop
- 32/64-bit version of Windows 8, Windows 8.1 or Windows 10
- USB 2.0.

Procedure

Complete the following procedure to install Aperio PAP and the drivers for the USB radio dongle and the Version 3 USB cable:

1. Run the **setup-progapp-30.0.23-62f3555** file (located in the '**`Utilities\Aperio'`** directory of the Command Centre installation files).
2. Select your language when prompted, then click **OK**.
   The Aperio Programming Application Setup Wizard opens.
3. Follow the wizard's instructions and click **Finish** when done.
   An icon should get created on the desktop.



The latest PAP software tested by Gallagher is 30.0.23

Creating a new installation

Introduction

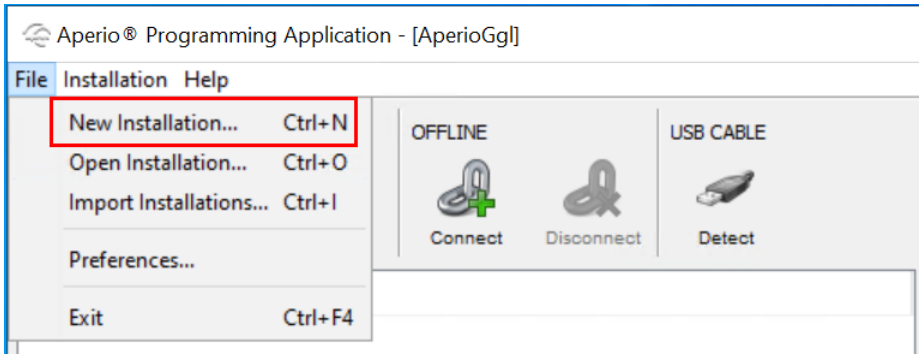
An installation is a password protected set of settings you need when you want to communicate with a hub and/or a lock. An installation is linked to an encryption file that is needed in order for the communication to work. The encryption key would be provided to you by Gallagher Sales Order Management (SOM).

This encryption key should be handled with the same care as the Master Key in a traditional Master Key System. A person with access to the encryption key can gain unauthorized access to any Aperio door in the system. Once loaded into the PAP, it will be stored encrypted in a local database. It is recommended that a copy of the encryption key should be stored safely.

Procedure

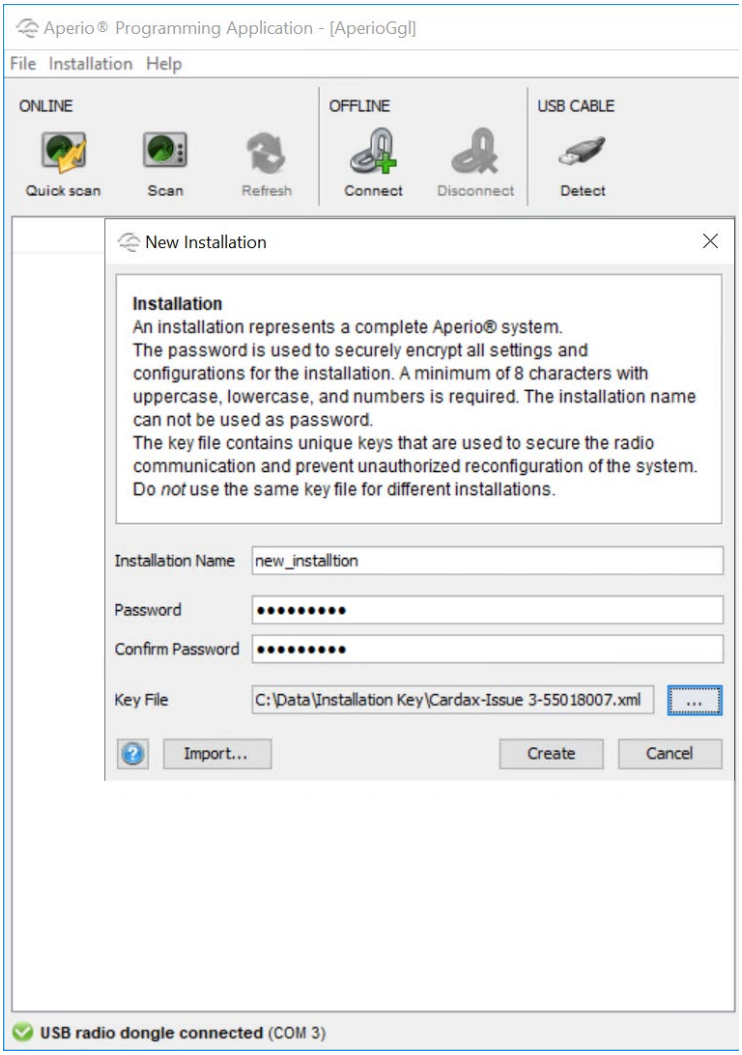
Complete the following procedure to create a new installation:

1. Ensure that the Aperio Tritech USB dongle is plugged in and start the Aperio Programming Application.
2. Select **File** > **New Installation…** in the Aperio Programming Application menu.

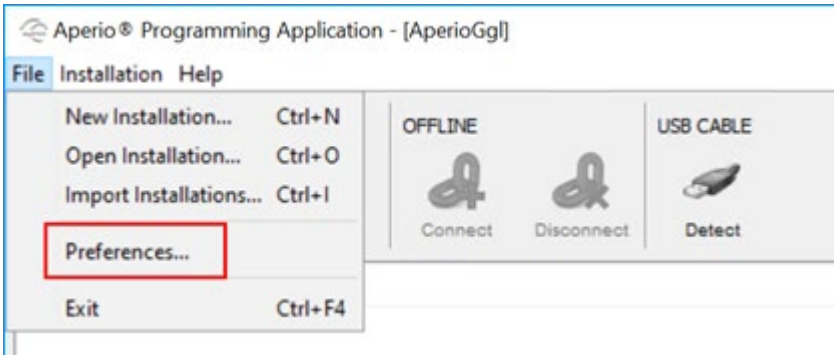


The New Installation window displays.

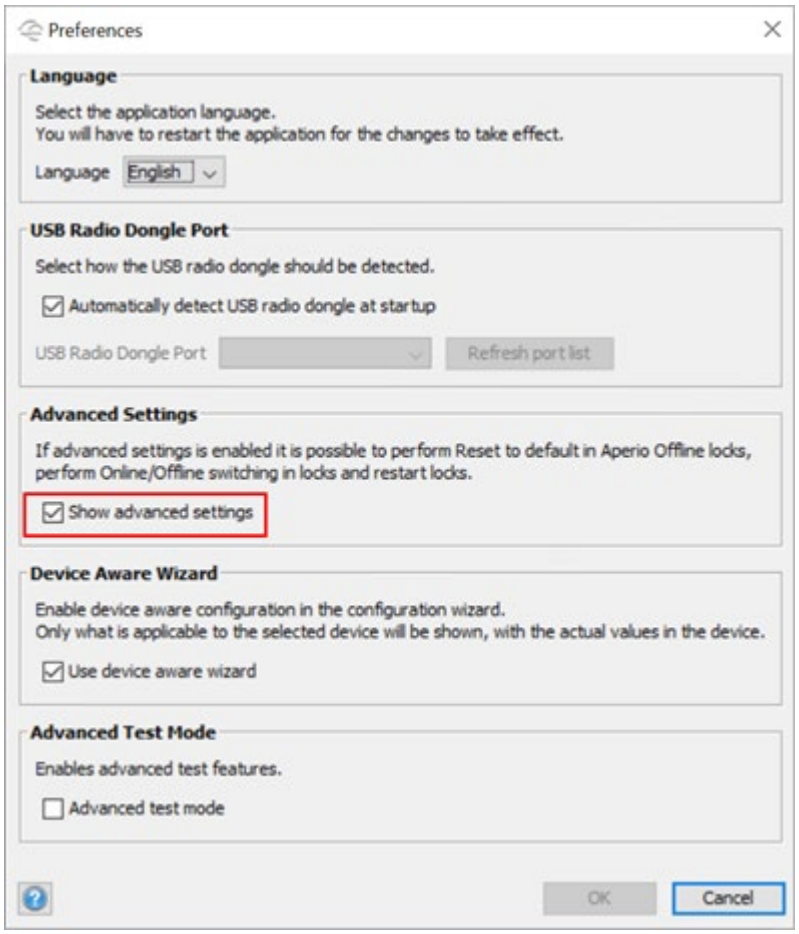
3. Type a name into the Installation **Name** field.
4. Type a new password into the **Password** field, then retype it into the **Confirm Password** field.
5. Click the browse button next to the **Key File** field, navigate to the customer key .xml file, and open it.
   Note: This is an 8-digit file name and was supplied by Sales Order Management (SOM).



6. Click **Create**.
   Note: If you are new to using Aperio, you need to request a key from Gallagher Sales Order Management (SOM).
7. Select File > Preferences…



   The Preferences dialog displays.
8. Advanced settings need to be enabled to perform advanced hub and lock configurations, (e.g. changing the radio channel, advanced lock settings). Tick the **Show advanced settings** checkbox to enable advanced settings.



9. Click **OK**.
   The Preferences dialog closes.

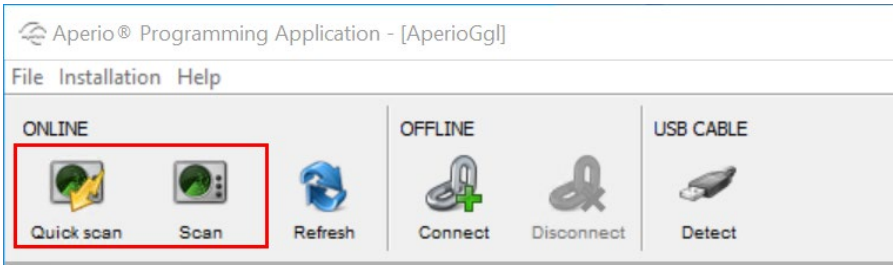
Scanning for Communication hubs

Introduction

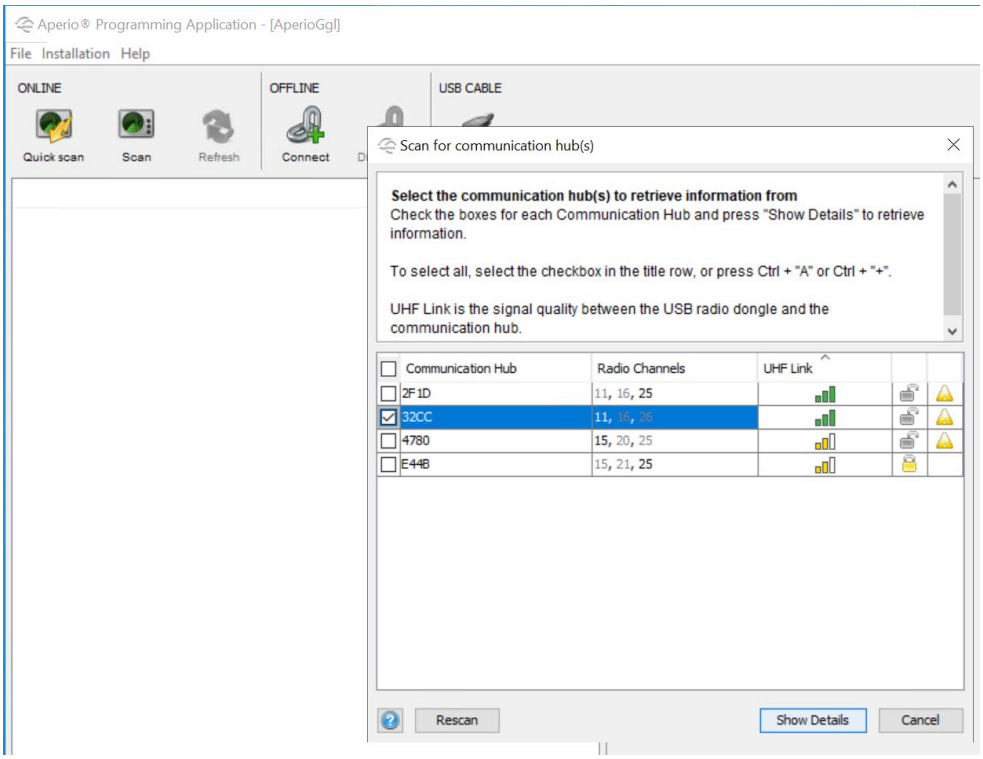
Once the PAP software is installed and the installation is created, we can connect to the communication hubs. Ensure that the hubs to be configured are powered on and follow the below mentioned procedure.

Procedure

1. Select either **Scan** or **Quick scan** to find communication hubs.
   All communication hubs within reach of the USB Radio dongle of your computer are displayed in the scan result table.

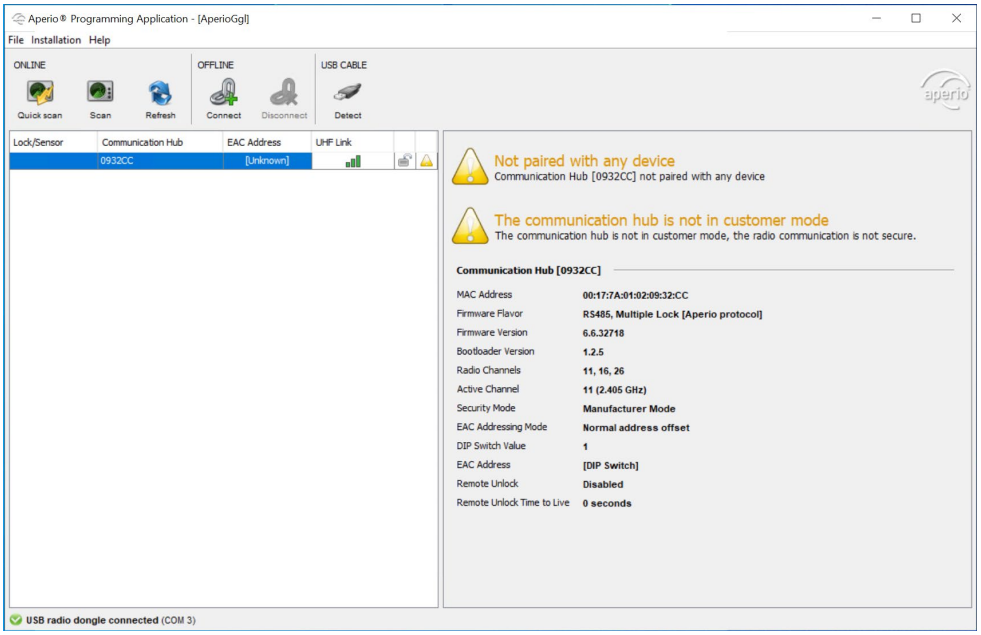


2. Locate a communication hub by the last four characters of the communication hub MAC address, (e.g. 32CC) in the scan result table. The same characters should be on a label on the cover of the communication hub.
   Click **Rescan** if the communication hubs that you want to configure are not shown in the list.



3. Select the communication hub(s) that you want to include in your installation. Click **Show Details** to view detailed information in the installation view.

   Any locks already paired with the hub will be displayed. If there are no locks paired, it will just show the communication hub as shown in the screenshot below.



Configuring the Hub addressing mode

Default PAP EAC Addressing mode (RS485 hub only)

The default addressing mode for AH30 hubs is **Normal address offset**, which means that the communication hub assigns the EAC address to the paired locks according to the following formula:

Lock address = Hub address + (n*16) where n = 0,1,2… for 1st, 2nd, 3rd lock paired with the hub respectively

The following example shows the addresses assigned to the locks on a communication hub with address 1:

- **Normal EAC address offset:** 1, 17, 33, 49 and so on

  1st lock = 1 + (0 * 16) = 1

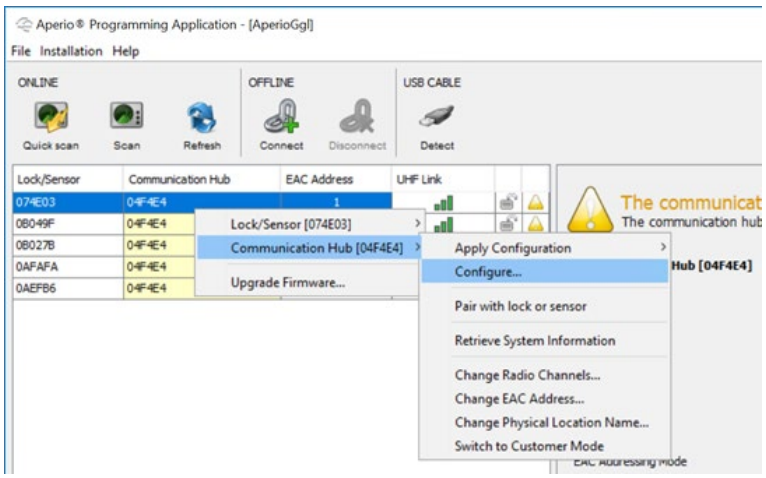
  2nd lock = 1 + (1 * 16) = 17

  3rd lock = 1 + (2 * 16) = 33

Procedure

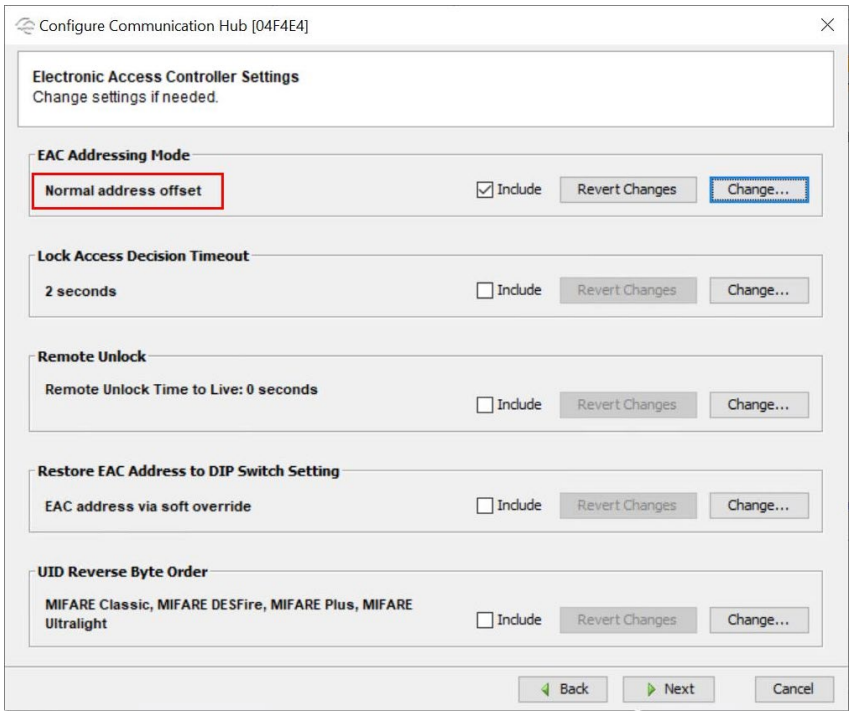
Follow these steps to check you have the default addressing mode set:

1. In the Aperio Programming Application, **right-click** on the hub and select **Communication Hub** > **Configure**.

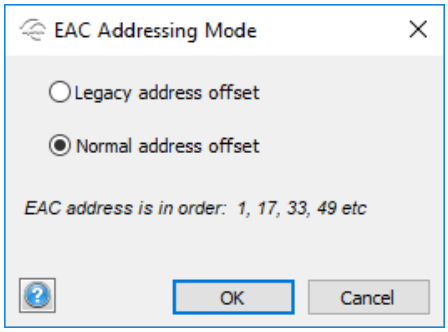


   The Configure Communication Hub wizard displays.

2. Keep clicking **Next** until you reach the **Electronic Access Controller Settings** screen of the wizard.



3. The EAC Addressing Mode should show "Normal address offset" (as shown in the screen above). If it shows "Legacy address offset", click **Change…** and select **Normal address offset** instead.



Pairing the Aperio locks

Introduction

The number of locks/readers that the communication hubs can be paired with depends on the type of the communication hub, as follows:

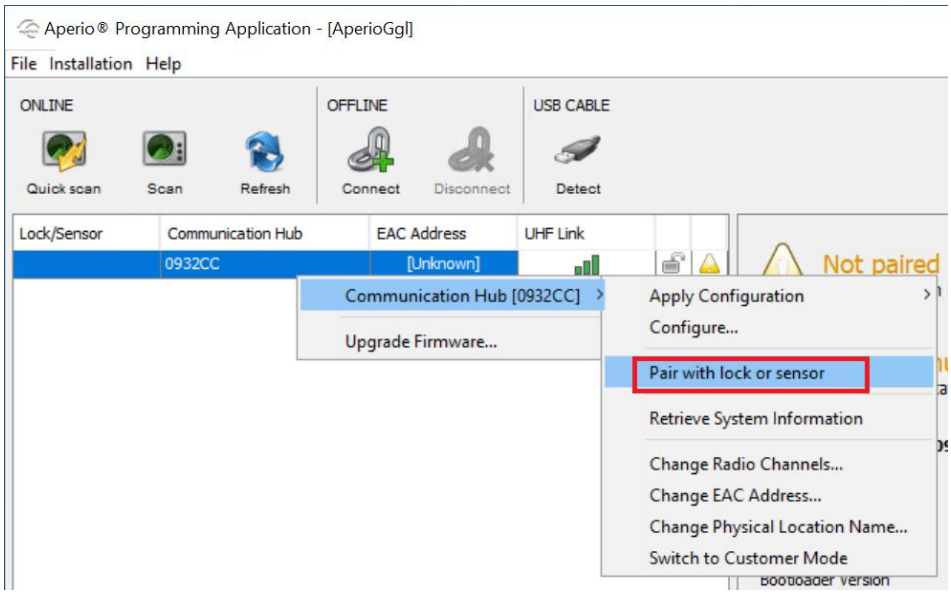
Type	Version of hub	can be paired with…
RS485	AH30	a combination of up to 8 locks.
Wiegand	AH20	one lock/reader.

Note: Aperio R100 locks are only supported with AH20 hubs.

IMPORTANT: No more than 32 Aperio Doors can be assigned to a Controller 7000, 20 per Controller 6000, or 16 per Controller 7000 Single Door. With no more than 16 Aperio Doors on a single Bus.

Procedure

1. Position the hub LED to face the lock/reader.
2. Right-click and select Communication Hub > Pair with lock or sensor.

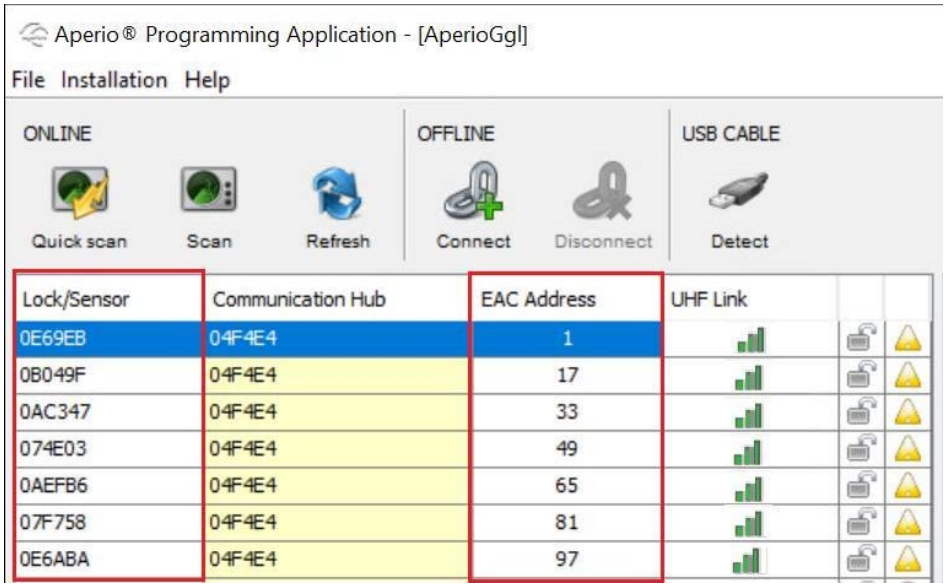


The pairing process starts.

3. Wake up the lock by pressing any button or presenting any card credential that can be read by the lock or engaging the magnet for the door position sensor.
   The communication hub pairs with the lock and indicates with alternating yellow and green flash.
4. When the lock has flashed green, click **Done** to see the pairing result.

Note: The communication hub LED is constant yellow and indicates successful pairing with a green flash.

5. Repeat the pairing for all communication hubs and locks/readers within reach of the USB Radio Dongle.
6. Once the locks are paired with the hub, they will show in the PAP software with their respective MAC addresses and the assigned EAC address.



Note: Pairing might fail because of different reasons, most common being the hub and the lock having different radio channels configured. Refer to ***Configuring the Radio Channels*** (next) for details on how to check and configure the channels. Refer to ***Troubleshooting*** (on page 76-77) for any other reasons.

Configuring the Radio Channels

Introduction

Aperio Hubs and Locks/Readers communicate with each other using a pre-configured frequency from within the 2.4GHz band. Each Aperio device is factory set to 3 default radio channels based on the region of manufacture.

Aperio Hub and lock devices manufactured from USA are set to 11, 16 and 25.

Aperio Hub and lock devices manufactured from Europe/Asia/Australia are set to 11, 16 and 26.

The wireless signal will communicate using one of the chosen channels at any one time. If the active communication channel encounter external wireless interference during operation, then the Aperio Lock/Reader and Hub pair will change to the next available pre-configured radio channel frequency.

If all configured channels encounter interference, then the lock and hub pair will continue to search and change channels until a channel becomes available, or the batteries of the lock/reader become depleted.

Changing the Aperio radio channels will be necessary if you experience interference between communication hubs in close proximity of each other or from external devices, (i.e. Data Access Points), using the open 2.4GHz radio channel frequency band.

It is highly recommended that the chosen Aperio frequencies are managed to ensure they differ from the frequencies adopted by other wireless devices.



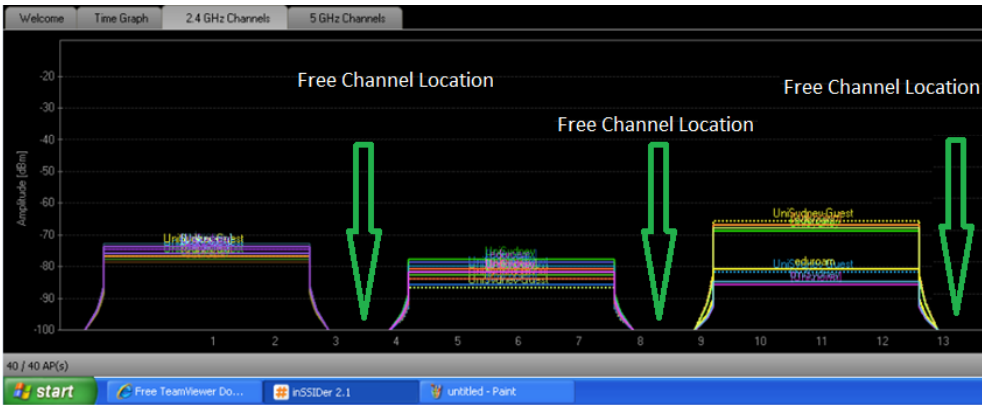
Recommendation

1. Before configuring the Aperio radio channels on a site, it is highly recommended to perform a site survey to analyse the 2.4 GHz radio channel frequency band from external activity. This will identify the free channels that can then be applied to Aperio devices.
2. Any wireless transmitting devices subsequently introduced into the environment should then be included with future site surveys.

Steps:

a) Check 2.4 GHz band for possible conflicting Wi-Fi activity using the **inSSIDer.exe** application (downloadable freeware https://inssider.informer.com)

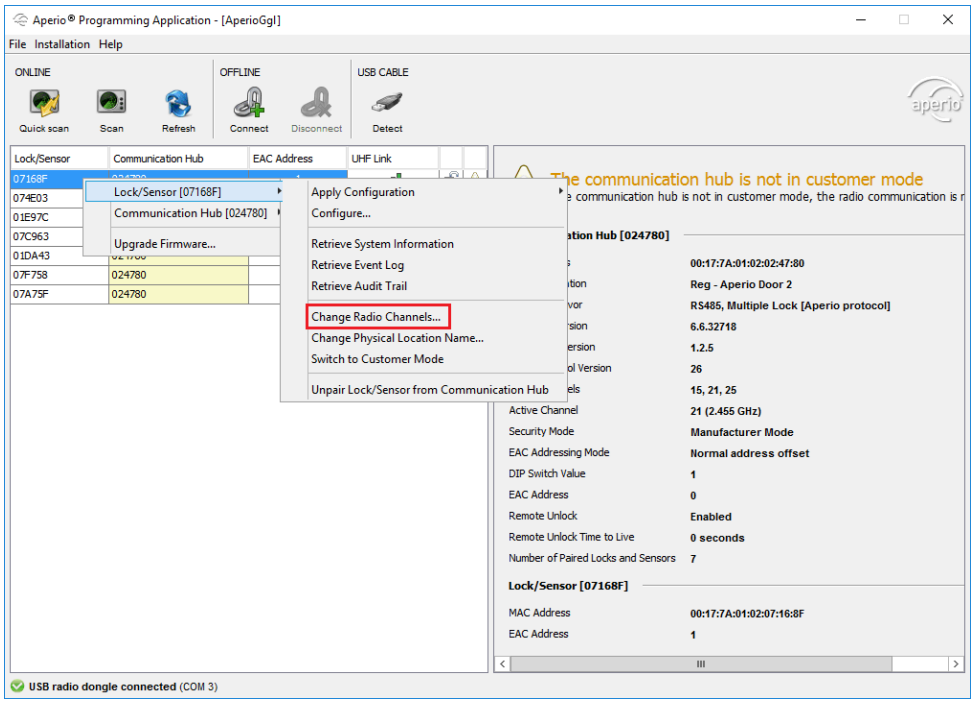
b) Detect the channels with low/least activity.
The following example detects 32 separate wireless Access Points using their factory default radio channel frequency:



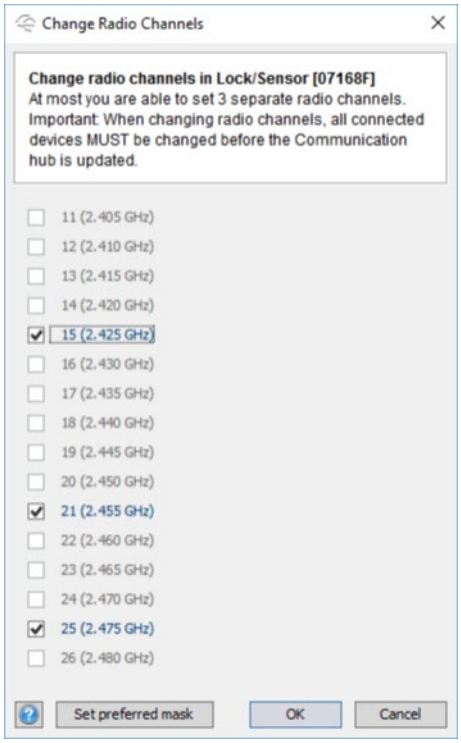
Procedure

Note: When using the Aperio Dongle to manage lock and hub radio channel frequencies, always change the radio channel frequency in the locks/Readers before changing in the communication hub. (If the lock and Hub frequencies become miss aligned to a point where the lock is no longer communicating with the hub, then it is possible to connect a micro USB cable to the Aperio lock/reader (V3 only) to re-configure the Lock/Reader radio channel frequency from the PAP SW).

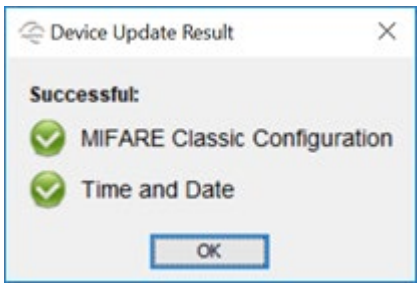
1. Hover over Lock/Sensor and click Change Radio Channels…



The Change Radio Channels dialog displays.



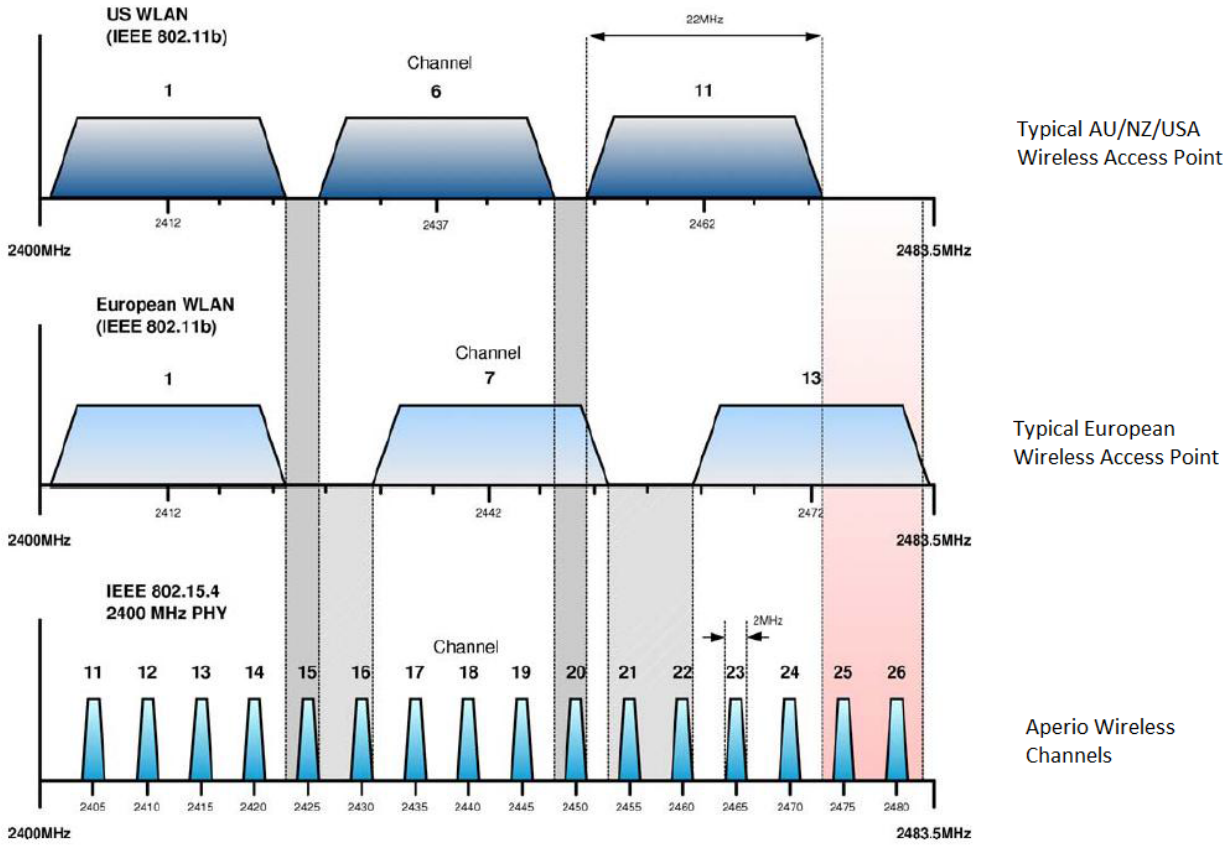
2. Select the radio channel(s) and click **OK**.
   Notes:
   - Deselect one or several of the used channels to make a new selection of channels.
   - Refer to the diagram shown at the end of Step 5 to determine the appropriate frequency channel to assign to each Lock/Hub.
3. Click **OK** on the pop-up confirmation message that displays.



4. Repeat this procedure for all locks/readers connected to the current communication hub.
   Note: All locks/readers should use the same three channels in order to create a more stable radio connection. Communication problems occur more likely between closely installed communication hubs than between closely installed locks /sensors paired with one hub.

   During the configuration process, when the channels do not match between the hub and the lock, it will show a channel conflict in the PAP software. This will go away once the same channels have been set on the hub.

5. Finally, change the radio channel for the communication hub, as follows:
   a) **Right-click** and select **Communication Hub** > **Change Radio Channels**.
   b) Unselect any of the three currently used channels to be able to select the same radio channels as for the lock/reader.
   c) Click **OK**.



Upgrading Aperio hubs/locks firmware

Introduction

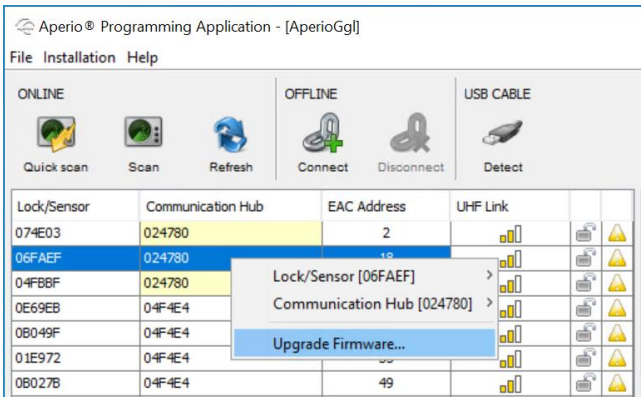
You will need to update the Aperio hubs and locks to the latest released firmware version. The firmware files are located in the **'Utilities\Aperio \Aperio HW firmware'** directory of the Command Centre installation files.
Note: Always upgrade the hub before upgrading the locks as a newer hub firmware always supports the older lock versions but not vice versa.
The latest firmware versions files tested by GGL are:

- For AH20/AH30 hubs: 3.9.0.3457
- For AH20/AH30 Gen5 hubs: 1.4.6
- For Aperio locks: 3.20.0_3.20.41

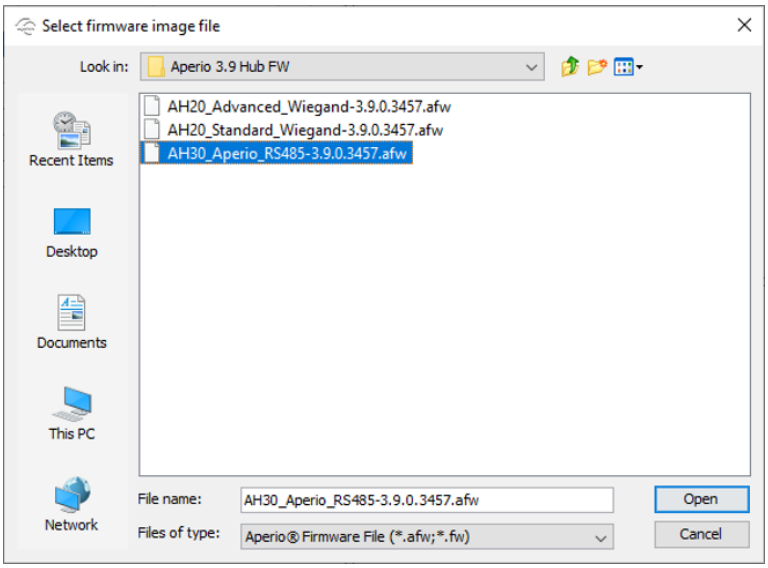
Procedure

Upgrade the hub

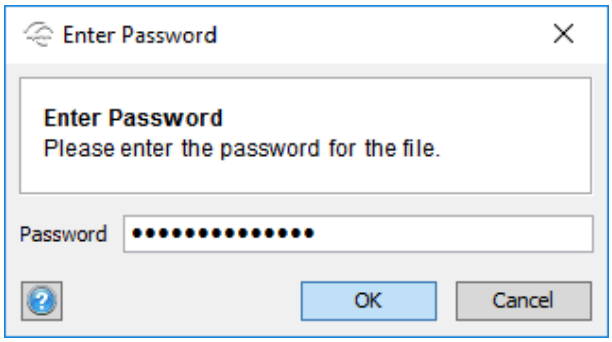
1. **Right-click** on the hub to be upgraded, and select **Upgrade Firmware...**



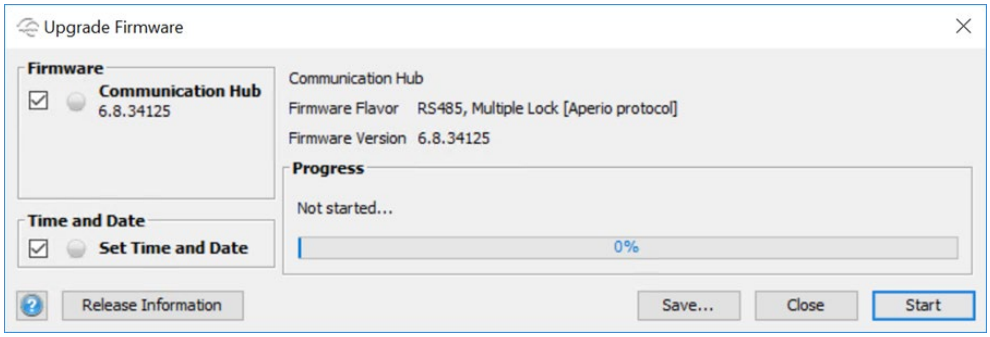
A Select firmware image file dialog displays.



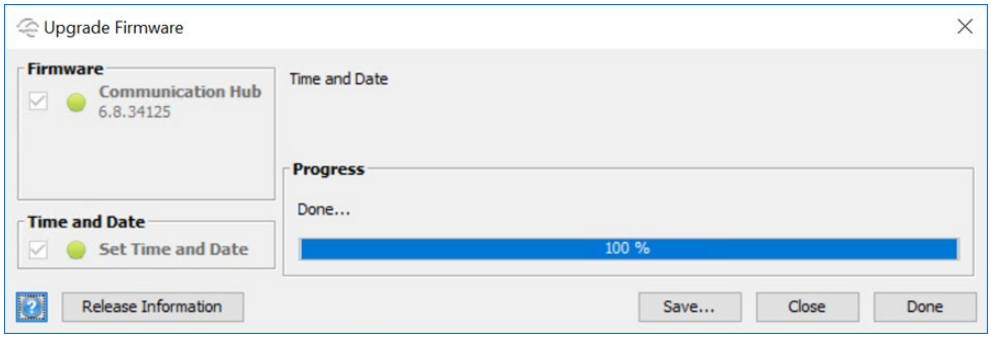
2. Select the appropriate firmware file, (i.e. AH30/ AH20 Std/ AH20 Adv.) and click **Open**.
   Important: You should never select an older firmware version than the one currently installed, as it can cause the hardware to malfunction.
3. Enter the firmware password.
   Note: The password to be used is located in the same directory as the firmware files in Command Centre installation folder.



4. The Firmware upgrade window displays a list of units to be upgraded. Proceed with the default selection and click **Start** to initiate the upgrade and follow on-screen instructions.

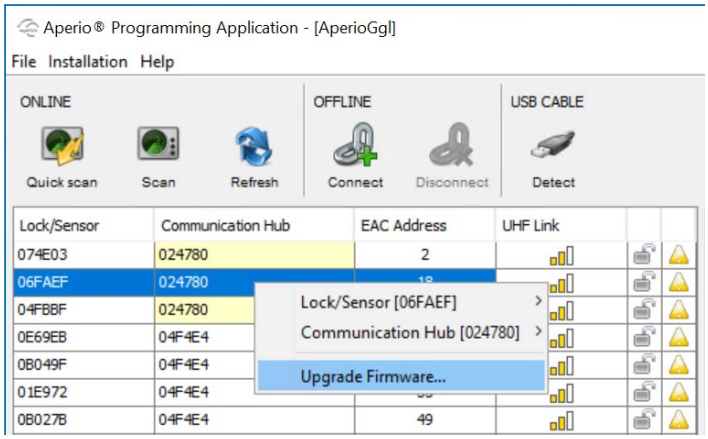


5. Click **Done** when finished.
   Note: Ensure that the hardware is not powered off during the upgrade.

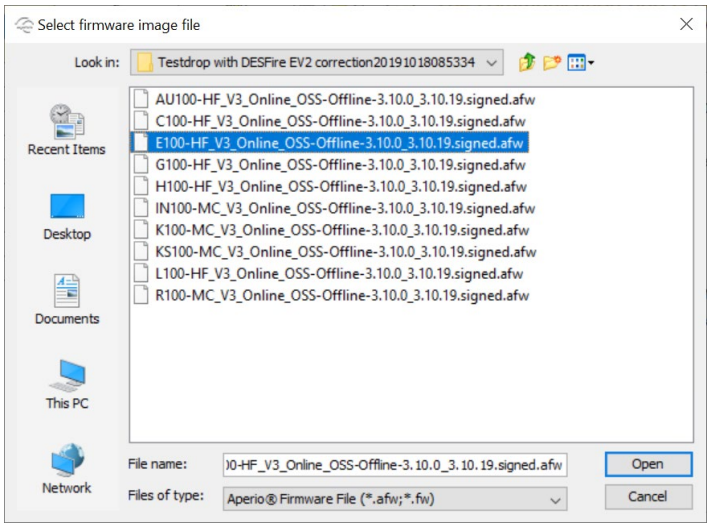


Upgrade the lock/reader

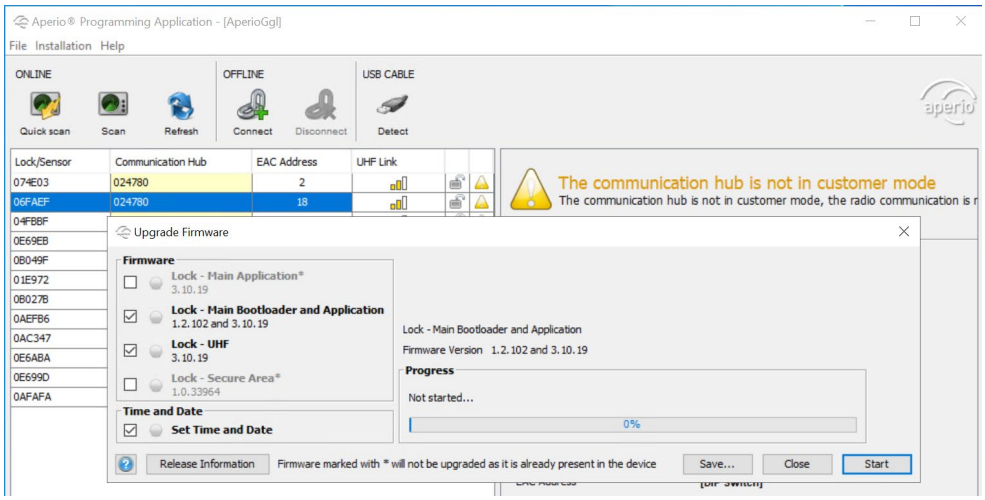
1. **Right-click** on the lock/reader to be upgraded and select **Upgrade Firmware...**



The Select firmware image file dialog displays.



2. Select the appropriate firmware file (as per the model of your lock) and click **Open**.
3. Enter the firmware password.
4. The Firmware upgrade window displays a list of units to be upgraded. Proceed with the default selection and click **Start** to initiate the upgrade and follow on-screen instructions.



5. The upgrade proceeds through all selected firmware in the list.
   Keep clicking **Next** to proceed through the list. The hardware resets in between.
   Note: Ensure that the hardware is not powered off during the upgrade.



Important: The upgrade can fail in-between due to radio disturbances. A workaround is to move closer to the hub/lock and try upgrading again. If upgrade fails repeatedly, try selecting all the checkboxes shown above to do a full upgrade.

Use USB cable for direct connection between PAP software and V3 Aperio locks/readers. The V3 locks can also be connected through USB for upgrade.

Gallagher Command Centre Site Configuration

This section contains information on the following configuration instructions required:

- ***Creating an Aperio Door*** (on page 76-30)
- ***Assigning an Aperio Door to a Gallagher Controller*** (on page 76-35)
- ***Configuring Access Group Privileges for Aperio*** (on page 76-38)
- ***Performing Overrrides on an Aperio Door*** (on page 76-39)

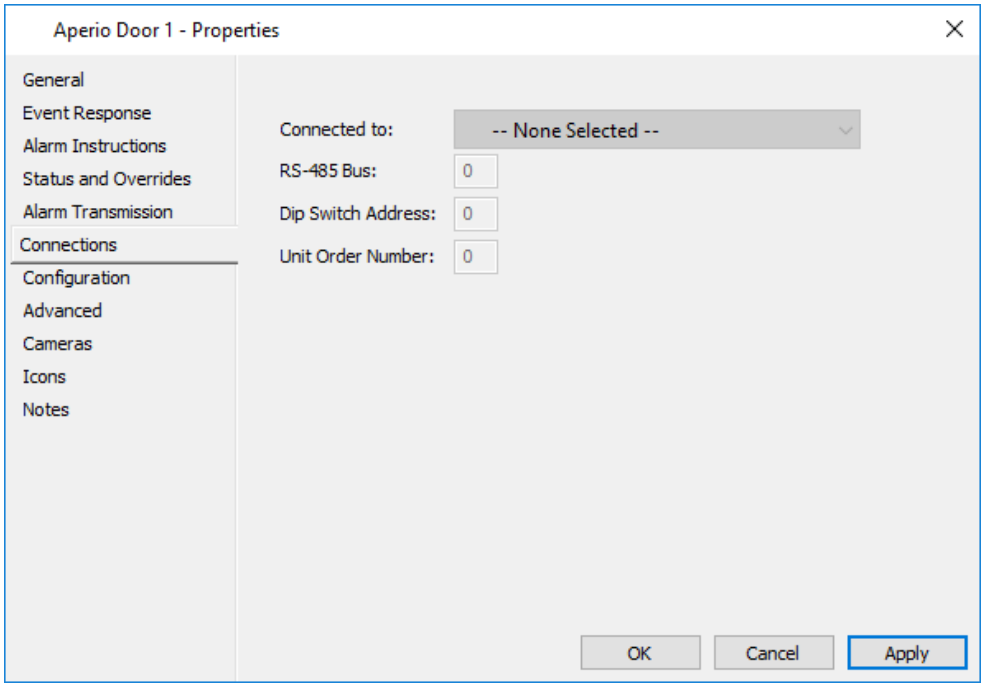
Creating an Aperio Door

Introduction

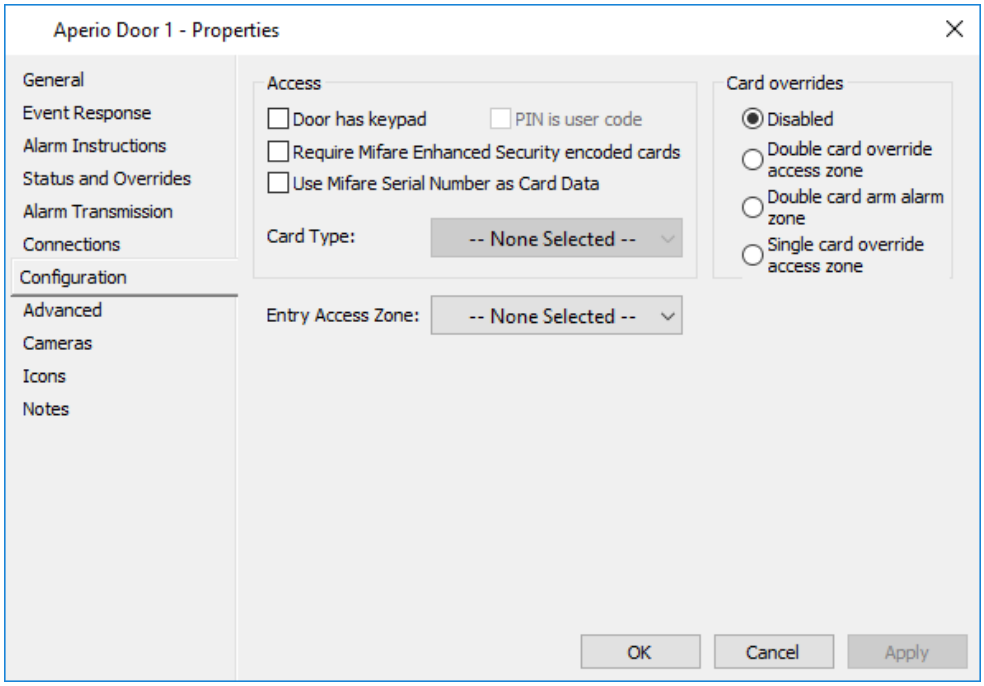
This procedure describes how to create an Aperio Door in Gallagher Command Centre.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Aperio Bus Devices**>**Aperio Door.**
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab, select an Alarm Zone and configure as required. For further detail see ***Event Response tab*** (on page 3-20).
5. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
6. Click the **Connections** tab.



   These fields are "read-only" and will be populated once you assign this door to a device, which is explained later in this procedure.
7. Click the **Configuration** tab.



8. The following checkboxes are available:

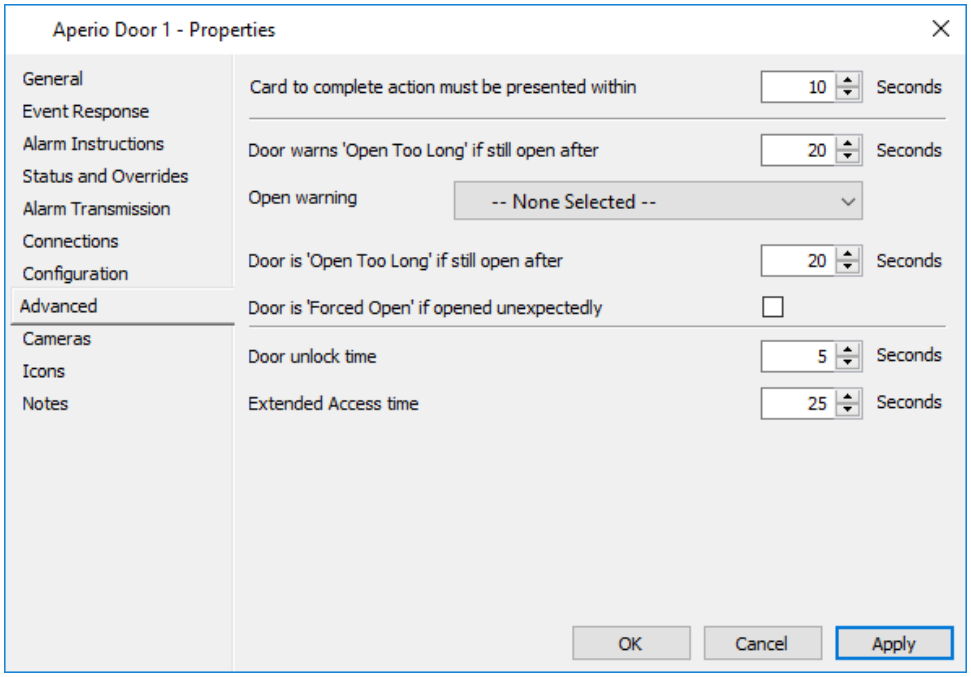
Option	Function
Door has keypad	It is recommended that this checkbox is ticked whenever the associated door has a keypad. If the door has a keypad and this is not ticked, then Command Centre may deny access without waiting for a PIN to be entered, when the Access Zone is in PIN mode. When this checkbox is ticked, it enables the **PIN is user code** option.
PIN is user code	The user is allowed through the door using the User Code number assigned to their cardholder record.
Require MIFARE Enhanced Security encoded cards	When ticked, the reader is instructed to only accept MIFARE Classic cards that have the enhanced security data when deciding whether to grant a cardholder access. The MIFARE Enhanced security key is configured on the **Card Security** tab of the Server Properties. **IMPORTANT:** Leave this checkbox unchecked in the following situations: • When not using the MIFARE Enhanced Security feature or when not using it for part of a site. • When some cardholders requiring access using this reader have not yet had their cards re-encoded. It is important to remember to

Option	Function
	enable the setting once all cards have been re-encoded. Disabling this setting will also allow cards encoded at sites using the MIFARE Enhanced Security feature to be used at sites who are not using this feature. Cards not encoded using the MIFARE Enhanced Security feature will be denied access with an event saying *"Denied - MIFARE High Security Card Required at [Door]"*. To enable the card to gain access at the door, uncheck the checkbox for the Door Reader.
Use MIFARE Serial Number as Card Data	When ticked, the reader is instructed to read the MIFARE Classic Card Serial Number (CSN). The CSN is used to identify a Cardholder in Command Centre.

Notes:

- The **Require MIFARE Enhanced Security encoded cards** and **Use MIFARE Serial Number as Card Data** options cannot be used at the same time, therefore when one of these checkboxes is ticked, the other checkbox is disabled. However, **PIN is user code** can be used in conjunction with either option.
- An Aperio lock is configured using the Aperio PAP to read either a MIFARE Classic sector 1 to 15, or to just read the MIFARE Classic Serial Number (CSN). The second checkbox should only be ticked if the Aperio lock has been configured to read the Card Serial Number (CSN). When using a MIFARE sector it is important that all cards for your site have their Gallagher data encoded onto the same sector.

9. When using the CSN, you will need to specify a Card Type to be used with this door.
   Click the **Card Type** drop-down list and select the correct Card Type.
10. Click the **Entry Access Zone** drop-down list and select the zone you enter into.
11. If you want to configure **Double card overrides** for this Aperio Door, refer to Configuring Local Overrides at Card Readers for the procedure.
12. Click the **Advanced** tab.



13. Configure the Aperio Door timeouts as required.

Option	This setting determines...
Card to complete action must be presented within	either: • the maximum time between card swipes for Dual Authorisation, **OR** • the time between pressing a function key on a keypad reader and badging the card for an Access Zone or Alarm Zone override. (Default = 10 seconds. Valid range = 1-99 seconds)
Door warns 'Open Too Long' if still open after	when the open warning output turns on and when the status of the door changes to show that it has been open too long. (Default = 20 seconds. Valid range = 0-9999 seconds) **Note:** This cannot be set as greater than the alarm time, (i.e. the **Door is 'Open Too Long' time**). If it is, and you attempt to save the door, the following error message displays: *"The 'Open Too Long' warning time must be less than or equal to the 'Open Too Long' alarm time."*

Option	This setting determines...
Open warning	the Output to activate when the door has been open too long.
Door is 'Open Too Long' if still open after	when a 'Door Open Too Long' alarm is generated. (Default = 20 seconds. Valid range = 5-9999 seconds)
Door is 'Forced Open' if opene unexpectedly	whether or not a Forced Door alarm will be generated if the open sensor (if the lock has it) detects the door is opened.
Door unlock time	the maximum time the Unlock relay is energised. (Default = 5 seconds. Valid range = 1-86400 seconds (24 hours))
Extended Access time	the period of time the door will remain unlocked for in addition to the **Door unlock time**, for cardholders who require it (e.g. disabled people, couriers, delivery vehicles). **Note:** For further detail about extended access time, and how to identify cardholders that require special access, see ***Configuring extended access time for a Door*** (on page 22-10). (Default = 25 seconds. Valid range = 0-86400 seconds (24 hours))

14. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Aperio Door.
    For further details see ***Cameras tab*** (on page 3-24).
15. Click the **Icons** tab if you want to change the Icon Set for this Aperio Door.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-71).
16. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Aperio Door.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
17. Click the **Notes** tab if you want to add a note(s) about this Aperio Door.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
18. 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 an Aperio Door to a Gallagher Controller

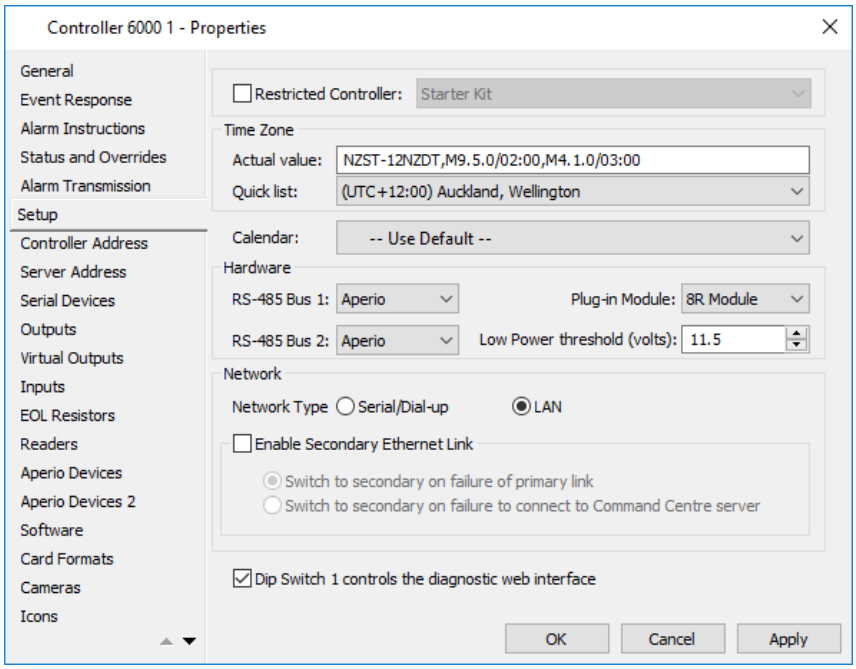
Introduction

This procedure describes how to assign an Aperio Door to a Gallagher Controller.

Procedure

1. From the **Hardware** List Window, highlight the Gallagher Controller you want to assign the new Aperio Door to.
2. **Right click** and select **Properties**.
   By default the **General** tab displays.
3. Click the **Setup** tab.
4. In the **Hardware** section of this screen, select the 'Aperio' option from the **RS-485 Bus 1** and/or **RS-485 Bus 2** drop-down lists.
   The **Aperio Devices** tab appears, allowing you to add up to 16 Aperio Doors to the Bus port of this Gallagher Controller.

   Note: For Controller 7000 Single Doors, there is only 1 **RS-485 Bus** field. The following screen shot is an example for a Controller 6000.

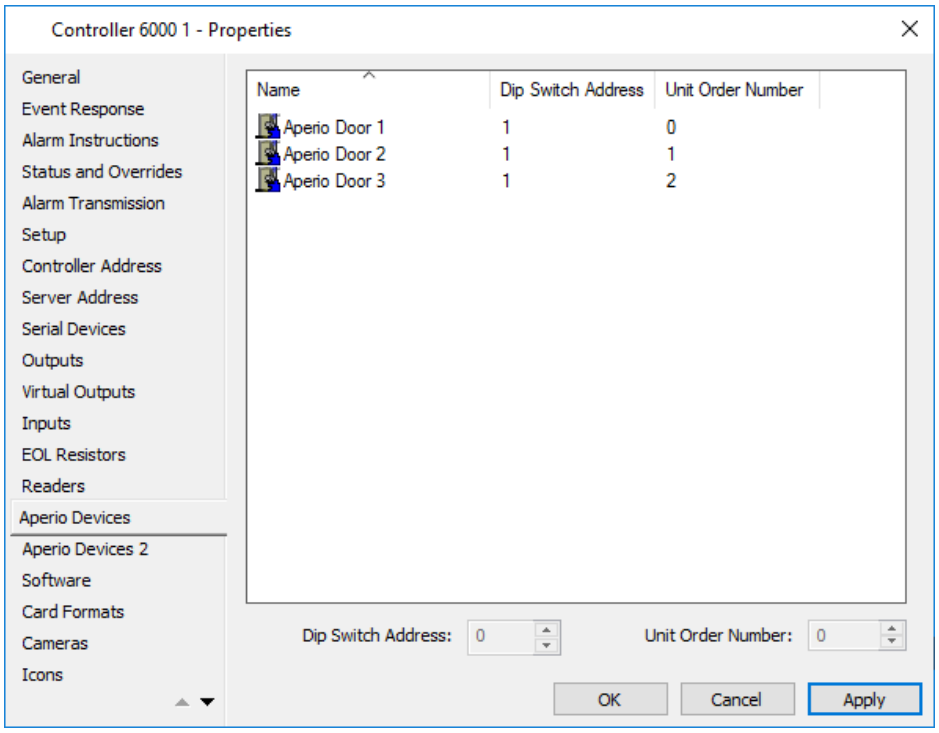


Notes:

- No more than 32 Aperio Doors can be assigned to a Controller 7000, 20 per Controller 6000, or 16 per Controller 7000 Single Door. With no more than 16 Aperio Doors on a single Bus.
- If the controller has two RS-485 buses, one can be used for Aperio while the other can be used for another device. For further detail refer to ***Linking Devices to Controllers*** (on page 21-31).

- An Aperio RS485 bus can only be used exclusively for Aperio AH30 hubs.

5. Click the **Aperio Devices** tab.



6. From the **Hardware** List Window, select the Aperio Doors attached to this Bus. Drag and drop each Aperio door into the grid on the **Aperio Devices** tab.
   Note: The same Aperio Door cannot be assigned to multiple Buses.
7. Enter the **Dip Switch Address** (Hub address) of the Aperio lock, by selecting the appropriate door from the grid and entering the address into the Dip Switch Address field below. (Range = 1-15)
   Note: The DIP switch added for the door should be the same as the EAC address of the hub in the PAP software.
8. Enter the **Unit Order Number** (Door order number on Hub) of the Aperio lock, by selecting the appropriate door from the grid and entering the unit order number into the Unit Order Number field below. (Range = 0-7)
   Note: The unit order number pairs multiple locks with one hub. The first pairing is unit order number 0. If the locks paired with Aperio hubs have EAC addresses 1, 17, 33…, set the unit order number to be 0, 1, 2… respectively.
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.

Result

An Aperio Door has been created, with an Entry Access Zone assigned to it, and it has been assigned to a Gallagher Controller. As a result, the following occurs:

- the Aperio Door will display within the **Hardware** List Window.
- on the **Connections** tab of the Aperio Door, the Gallagher Controller name will appear in the **Connected to** field.

Note: The appearance of Aperio locks in the **Hardware** List Window follows this order: Aperio Hub DIP Switch Address/Aperio Lock Unit Order Number.

Important: Special care will need to be taken to ensure that Aperio locks have the correct Unit Order Number after pairing the hub and lock.

Configuring Access Group Privileges for Aperio

Introduction

This procedure describes how to configure Access Group Privileges for Aperio.

Procedure

1. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).
2. **Double click** the Access Group you want to assign privileges to.
   By default the **General** tab displays.
3. Click the **Privileges** tab.
4. Tick the checkboxes as required for this Access Group.
   Access Privileges that are specifically available for Aperio Doors are listed below; other (generic) options are explained in Setting up Access Groups.

Access Privilege	Allows Cardholders in this Access Group to...
Aperio Privacy Override	unlock doors even when in Privacy Mode. Default = unticked. **Notes:** • Privacy Mode is activated by a button on certain Aperio locks. This feature needs to be enabled in Aperio Programming Application Protocol (PAP) in order to take effect. • An Aperio door that is closed, locked, and in Privacy Mode displays a red and yellow padlock icon in the Hardware window of Configuration Client. For details on configuring Privacy mode, refer to ***Enabling the Privacy Mode*** (on page 76-61).
Aperio Offline Access	unlock doors even when the door is offline (only supported by V3 type locks; V2 type locks do not support this functionality). **Important:** This privilege should be enabled for an admin Access Group whose members would then be granted access through Aperio doors, even when the controller or hub is offline. **Note:** This feature requires configuration in PAP to configure override credentials for locks. For details refer to ***Configuring Override Credentials for Offline Access*** (on page 76-70).

Performing Overrides on an Aperio Door

Introduction

These procedures describe how to temporarily override the status of an Aperio Door.

Note: When using double-card overrides or dual authorisation at an Aperio lock, the cardholder must wait until the Aperio LED has ceased flashing before the second card can be presented at the lock.

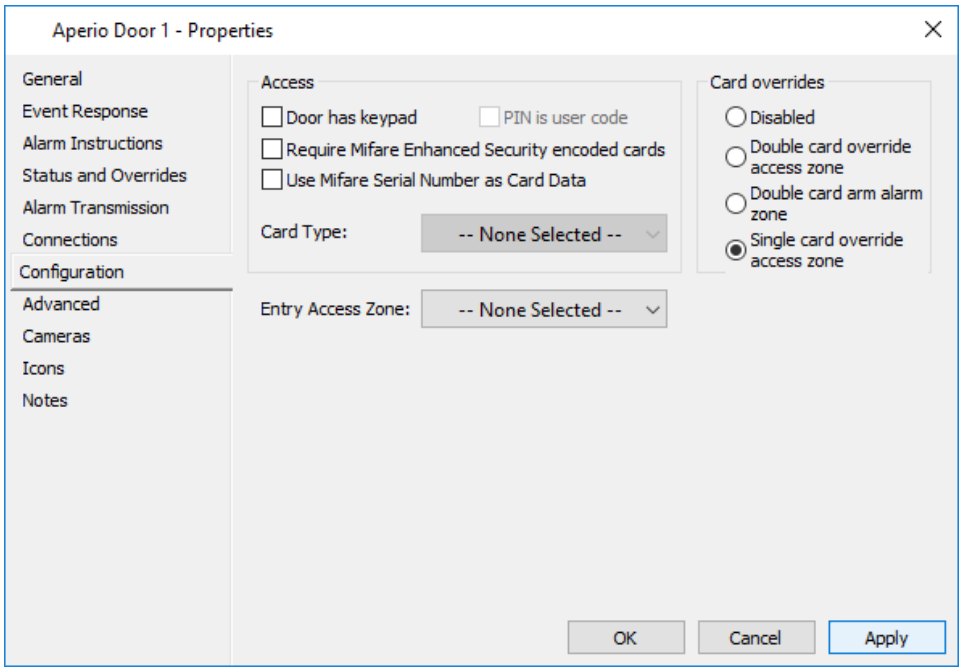
Procedures

To enable a single/double card override for access zone

This override allows cardholders to set the door into a pre-configured 'Mode 2' when they badge their card, and reset it into its scheduled state when they badge it again. For example, if the scheduled state is 'Secure - No PIN' and Mode 2 is 'Free - No PIN', the first card badge will set the door into free access mode until the card is badged again, which will reset it to secure mode.

Only cardholders with the 'Lock and unlock Access Zone' privilege are able to do this.

1. Set Access Zone schedule and Mode 2.
   Refer to ***Configuring Local Overrides at Card Readers*** (on page 45-14) for instructions.
2. Assign appropriate Access Groups the 'Lock and unlock Access Zone' privilege.
   Refer ***Setting up Access Groups*** (on page 34-4) for instructions.
3. From the **Hardware** List Window, right-click the Aperio Door you want to perform an override on and select **Properties**.
   By default, the **General** tab displays.
4. Click the **Configuration** tab.
5. Click the appropriate override radio button, as follows:
   - **Single card override access zone** radio button to allow the override to occur when a card is badged once; or
   - **Double card override access zone** radio button to allow the override to occur when a card is badged twice.



6. Click **OK**.
   The override feature is enabled.

To perform a double card override for alarm zone

This override allows cardholders to arm the alarm zone configured on the selected Aperio door when they badge their card twice. Only the cardholders with the *"Change to Armed state"* and *"Change to Disarmed state"* alarm zone privileges can do this.

1. Assign the appropriate Access Groups the *"Change to Armed state"* and *"Change to Disarmed state"* privileges.
2. From the **Hardware** List Window, right-click the Aperio Door you want to perform an override on and select **Properties**.
   By default, the **General** tab displays.
3. Click the **Configuration** tab.
4. Select the "Double card arm alarm zone" radio button to allow the alarm zone to set armed when a card is badged twice.
5. Click the **OK** button.
   The arm alarm zone feature is enabled.

To perform a one-off override

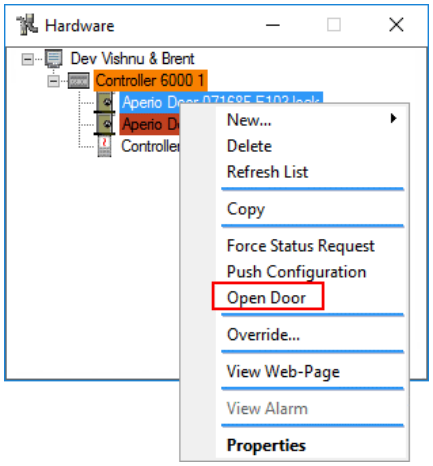
1. From the **Hardware** List Window, right-click the Aperio Door you want to perform an override on and select **Properties**.
   By default, the **General** tab displays.
2. Click the **Status and Overrides** tab.
   Five options are available in the Override drop-down menu:

Menu Option	Function	Privilege Required
Reset Hub	Performs a software reset on the Aperio Hub that the Door is connected to.	Override
Shunt	Stops communication to the device (door).	Maintenance Override
Unshunt	Restarts communication to the device (door).	Maintenance Override
Open Door *	Unlocks the selected Door regardless of what status the current Access Zone is in (only supported by V3 type locks; V2 type locks do not support this functionality).	Override - Open Door
Clear dynamic cache	Erase any credentials stored in the lock's memory if dynamic cache is enabled (only supported by V3 type locks). The lock will then NOT grant access to any cardholders using cached credentials when offline. For further detail see ***Enabling the Smart Credential cache (Dynamic cache)*** (on page 76-64).	Override

3. Click the **Override Now** button.
   From this screen you can see the status change as a result of the override.
4. Click the **OK** button.
   For further information, see ***Status and Overrides*** (on page 45-1).

Notes:

- You can also right-click the door from the **Hardware** List window and click **Open Door** to override the lock and open the door.



- Overrides can stay in effect until either the next automatic change (as programmed on the time schedule), or for a specified length of time entered by the operator. Overrides that have been implemented for a specified time will persist if the Server resets, or a configuration in the system occurs.

Configuring the Aperio Locks/Readers

Refer to the relevant topic for the instructions on how to configure Aperio Locks/Readers:

- ***Configuring locks to read different card technologies at Aperio doors*** (on page 76-43)
- ***Configuring Status Report and Polling Intervals*** (on page 76-54)
- ***Configuring the Security Mode (Encryption between hub and lock*** (on page 76-57)
- ***Enabling the Privacy Mode (if required)*** (on page 76-61)
- ***Enabling the Smart Credential cache (Dynamic cache)*** (on page 76-64)
- ***Configuration for Mobile Connect*** (on page 76-67)
- ***Configuring Override Credentials for Offline Access for System Administrators*** (on page 76-71)
- ***Configuring R100 Readers*** (on page 76-74)

For more configuration options, refer to the "Aperio Online Quick Installation Guide".

Configuring locks to read different card technologies at Aperio doors

Command Centre supports reading the following cards on Aperio locks/ sensors:

- MIFARE DESFire cards
- HID IClass 26/8 cards (high frequency)
- HID 125khz 26/8 cards (low frequency)
- MIFARE Classic cards
- MIFARE CSN

However, these card types need to be configured using the PAP software to match the card layout properties/settings in Command Centre.

Refer to the relevant topic for the instructions on how to configure the type of cards your site is using:

- ***Configuring MIFARE DESFire cards for use at Aperio Doors*** (on page 76-43)
- ***Configuring HID 26/8 cards for use at Aperio Doors*** (on page 76-46)
- ***Configuring MIFARE Classic cards for use at Aperio Doors*** (on page 76-48)
- ***Locks failing to update*** (on page 76-53)

Configuring MIFARE DESFire cards for use at Aperio Doors

Introduction

MIFARE® DESFire® cards can interact with doors fitted with Aperio locks within a Command Centre environment.

Prerequisites

The latest version of the Aperio Programming Application Protocol (PAP) must be installed from the **`'Utilities\Aperio'`** directory of the Command Centre installation files.

Procedure

Configuring a card type with a non-diversified MIFARE DESFire object

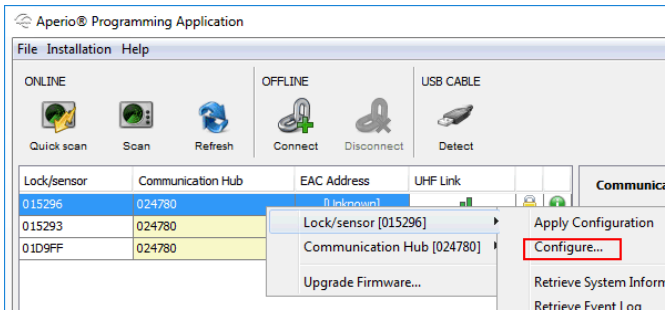
Non-diversified MIFARE DESFire objects can only be added to card types with a facility code that matches the one in your license. More than one non-diversified MIFARE DESFire object can be added to a card layout.

1. Configure a card layout with a non-diversified MIFARE DESFire object in Configuration Client.
   See ***Adding a Non-diversified MIFARE DESFire object*** (on page 47-44) for the procedure.

Applying the MIFARE DESFire configuration to an Aperio Door/Lock

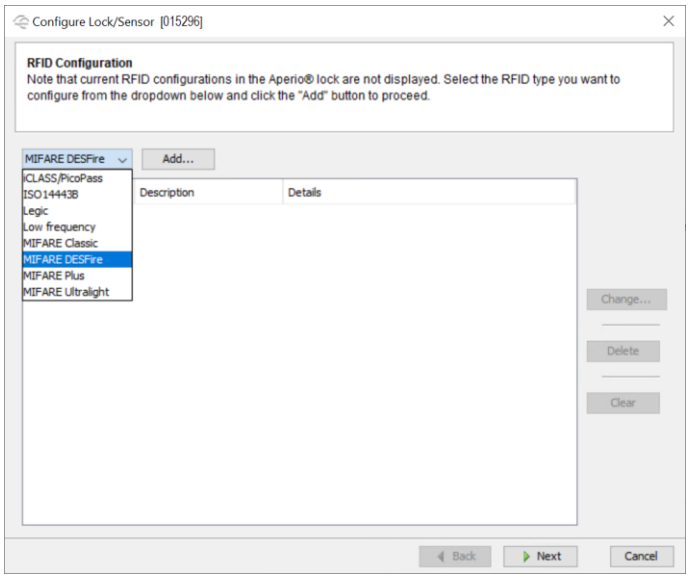
Once you have imported a configuration, you will need to apply the MIFARE DESFire configuration to a lock in Aperio PAP.

2. **Right click** on the lock and select **Lock/sensor** > **Configure…**



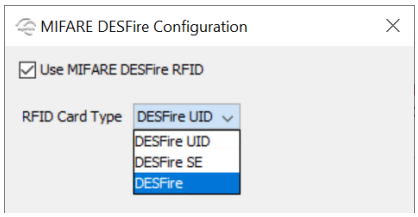
The Configure Lock/sensor screen opens.

3. Select **MIFARE DESFire** from the drop-down list and click **Add**…



The MIFARE DESFire Configuration dialog displays.

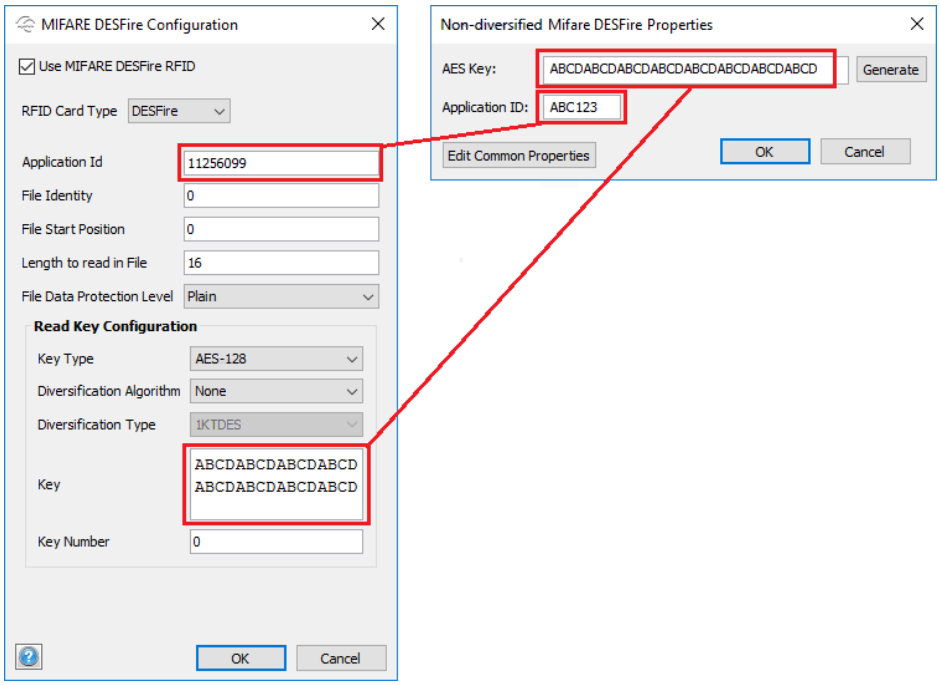
4. Change the **RFID Card Type** from 'DESFire UID' to 'DESFire'.



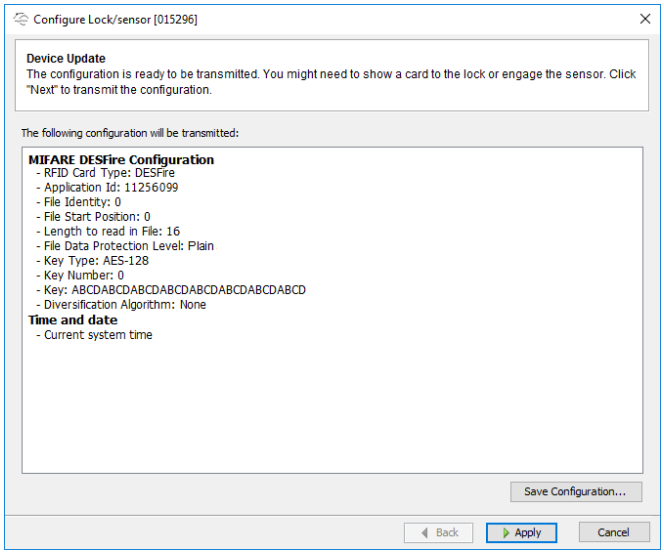
5. Convert the **Application Id** of the non-diversified MIFARE DESFire object (on the card layout) from hexadecimal to decimal digits.
   Note: A programmer mode calculator can be used for this.
6. Enter the decimal number in the **Application Id** field.
   For example: ABC123 (Hex) = 11256099 (Decimal).
7. Configure the other fields as follows:

Field	Enter...
File Identity	0
File Start Position	0
Length to read in File	16 (the length of the non-diversified MIFARE DESFire object properties)
File Data Protection Level	Plain
Key Type	AES-128

Field	Enter...
Key	the **AES Key** from the non-diversified MIFARE DESFire object properties, (i.e. 32 hexadecimal characters)
Key Number	0



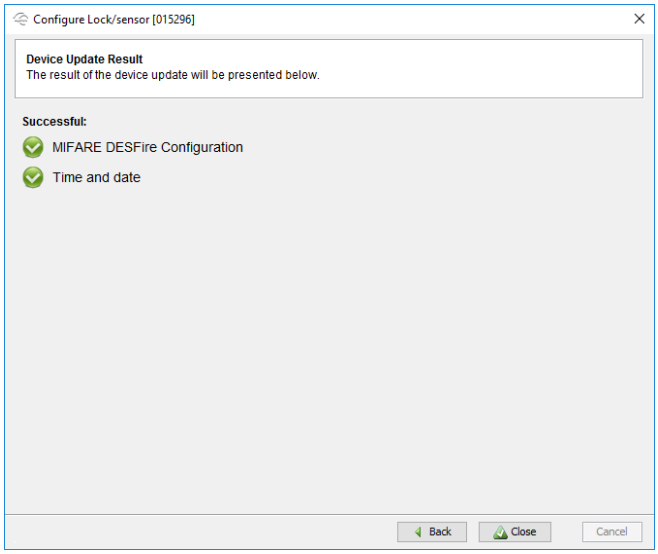
8. Click the **OK** button.
   The MIFARE DESFire Configuration dialog closes and you are returned to the Configure Lock/Sensor screen.
9. Click the **Next** button on each screen until you get to the 'Device Update' screen, where you are prompted to badge a card at the sensor to upload the configuration at each door.



Note: We recommend that you save the configuration at this point in order to more easily apply the configuration to other locks.

10. Click **Apply** and badge the type of card the lock was previously configured to, in order to upload the new configuration to the lock.

11. If the lock is updated successfully, the following screen displays:



See ***Locks failing to update*** (on page 75-53) for details of what happens if the lock configuration fails.

Configuring HID 26/8 cards for use at Aperio doors

Introduction

There are two types of HID 26/8 cards that can be used at Aperio doors:
- HID IClass 26/8 (high frequency) cards, and
- HID 125khz 26/8 (low frequency) cards.

While both types can interact with doors fitted with Aperio locks within a Command Centre environment, the HID IClass 26/8 (high frequency) cards need no additional settings in PAP are required to set this up. Unlike the HID 125khz 26/8 (low frequency) cards which do require additional set up in PAP.
Therefore, this procedure only relates to configuring HID 125khz 26/8 (low frequency) cards.

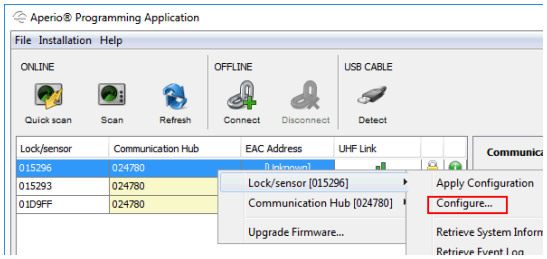
Prerequisites

The latest version of the Aperio Programming Application Protocol (PAP) must be installed from the `'Utilities\Aperio'` directory of the Command Centre installation files.

Procedure

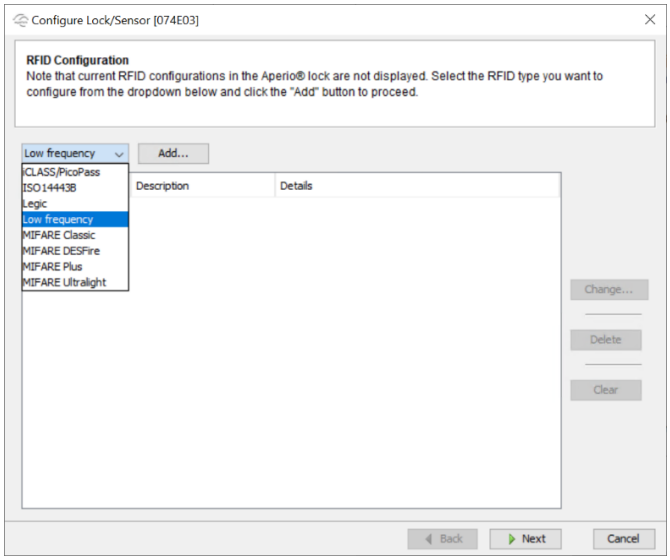
You need to apply the HID 125khz 26/8 configuration to a lock in Aperio PAP.

1. **Right click** the lock and select **Lock/sensor** > **Configure...**

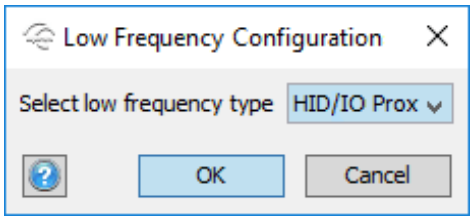


The Configure Lock/sensor screen opens.

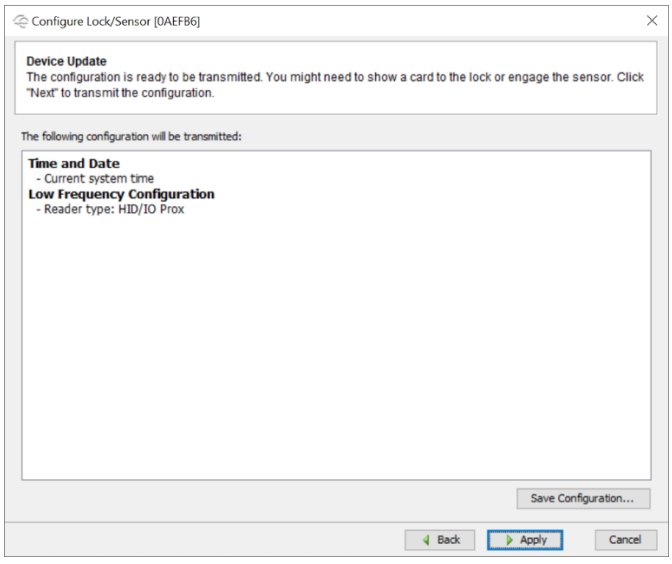
2. Select **Low frequency** from the drop-down list and click **Add...**



The Low Frequency Configuration dialog displays.



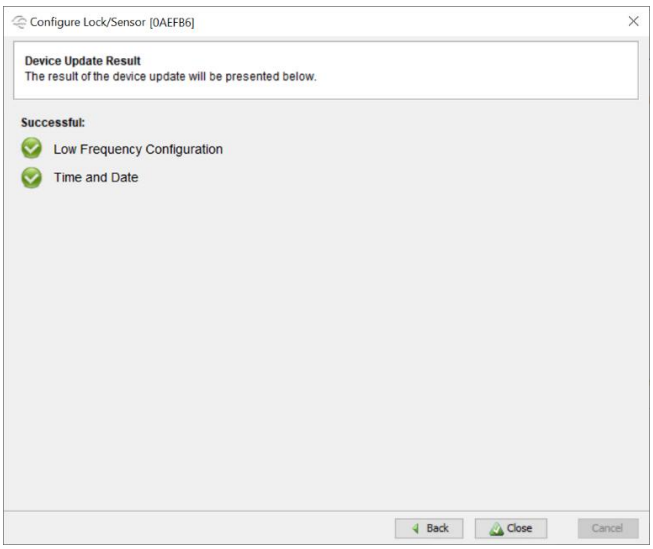
3. Select 'HID Prox' from the drop-down list, then click **OK**.
   The Low Frequency Configuration dialog closes and you are returned to the Configure Lock/Sensor screen.
4. Click the **Next** button on each screen until you reach the 'Device Update' screen.



Note: We recommend that you save the configuration at this point in order to more easily apply the configuration to other locks.

5. Click **Apply** and badge an HID 125khz 26/8 card at the Aperio lock to upload the new configuration to the lock.

   If the lock is updated successfully, the following screen displays:



   See ***Locks failing to update*** (on page 75-60) for details of what happens if the lock configuration fails.

Configuring MIFARE Classic cards for use at Aperio Doors

Introduction

MIFARE Classic cards can interact with doors fitted with Aperio locks within a Command Centre environment. this, you will need to import one of the following configuration files provided by Gallagher. These files enable a lock to read data from either a MIFARE Classic sector 1 to 15, or to just read the MIFARE Classic CSN.

Once imported, the configuration needs to be applied to a lock. Then, the lock will only read the sector specified by the configuration, hence all cards for your site will need to have their Gallagher data encoded onto the same sector.

Configuration files

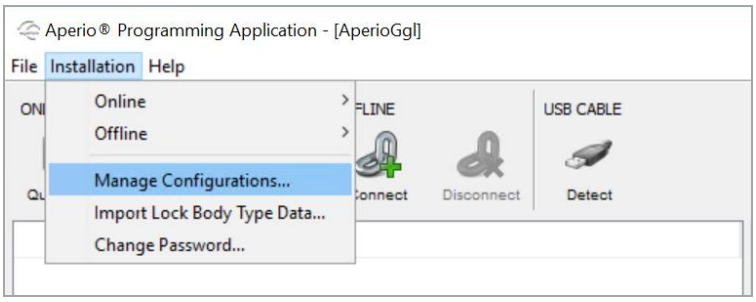
Gallagher - MIFARE Sector 1.xml	Gallagher - MIFARE Sector 9.xml
Gallagher - MIFARE Sector 2.xml	Gallagher - MIFARE Sector 10.xml
Gallagher - MIFARE Sector 3.xml	Gallagher - MIFARE Sector 11.xml
Gallagher - MIFARE Sector 4.xml	Gallagher - MIFARE Sector 12.xml
Gallagher - MIFARE Sector 5.xml	Gallagher - MIFARE Sector 13.xml
Gallagher - MIFARE Sector 6.xml	Gallagher - MIFARE Sector 14.xml
Gallagher - MIFARE Sector 7.xml	Gallagher - MIFARE Sector 15.xml
Gallagher - MIFARE Sector 8.xml	Gallagher - MIFARE CSN.xml

Note: The configuration files are present in the '**`Utilities\Aperio\MIFARE Classic Config Files`**' folder. The folder contains configuration files to be used for both AH30 and AH20 hubs.

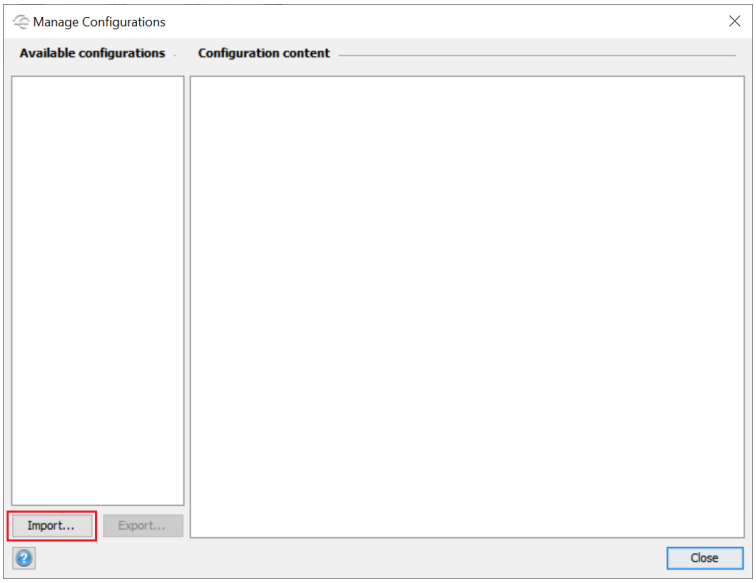
Procedure

Import the configuration file

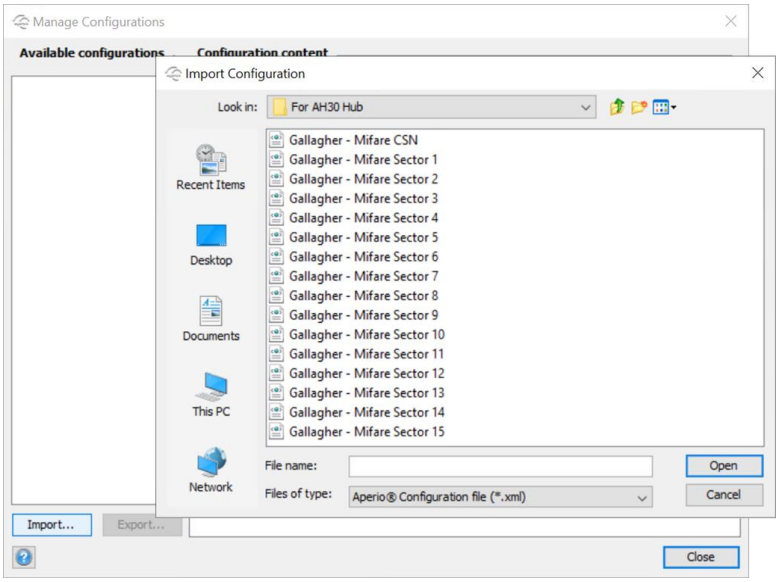
1. In the Aperio PAP menu, select **Installation** > **Manage Configurations**...



2. Click the **Import...** button.



3. Path your way to the '**`Utilities\Aperio\MIFARE Classic Config Files`**' folder.
4. Select the configuration you wish to import from either the '**`For AH20 Hub`**' or '**`For AH30 Hub`**' folder, and click **Open**.

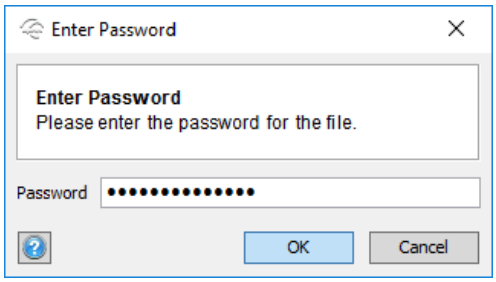


Notes:

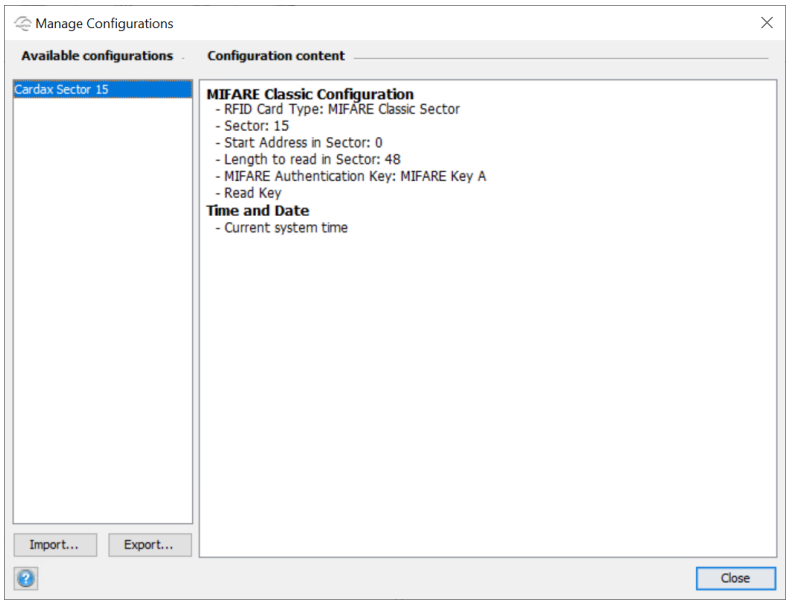
a) For MIFARE Classic cards with data encoded on one of the 15 sectors, select the appropriate file, (e.g. 'Gallagher - MIFARE Sector 15.xml' for cards with data on sector 15).

b) For MIFARE Classic cards using just the card serial number (CSN), select the file 'Gallagher - MIFARE CSN.xml' here. Locks paired with AH20 hub cannot be configured to use CSN. It is only supported for AH30 hubs.

5. Enter the password "**`Gallagherconfig1`**" and click the **OK** button.



6. The configuration is now added to your local configuration storage and is shown in the **Available configurations** list.
Selecting the imported configuration would show the details in the **Configuration content**.

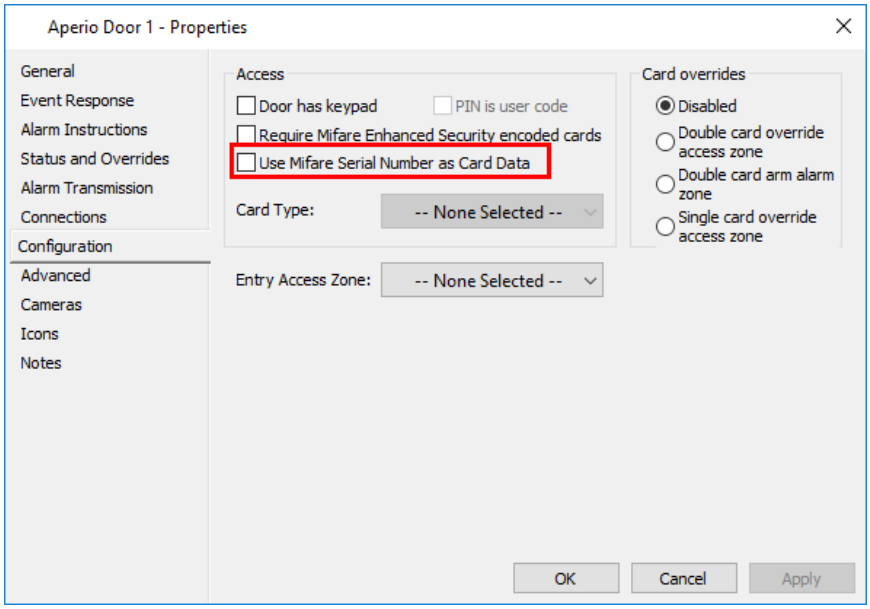


7. The configuration file imported now needs to be applied on the lock.

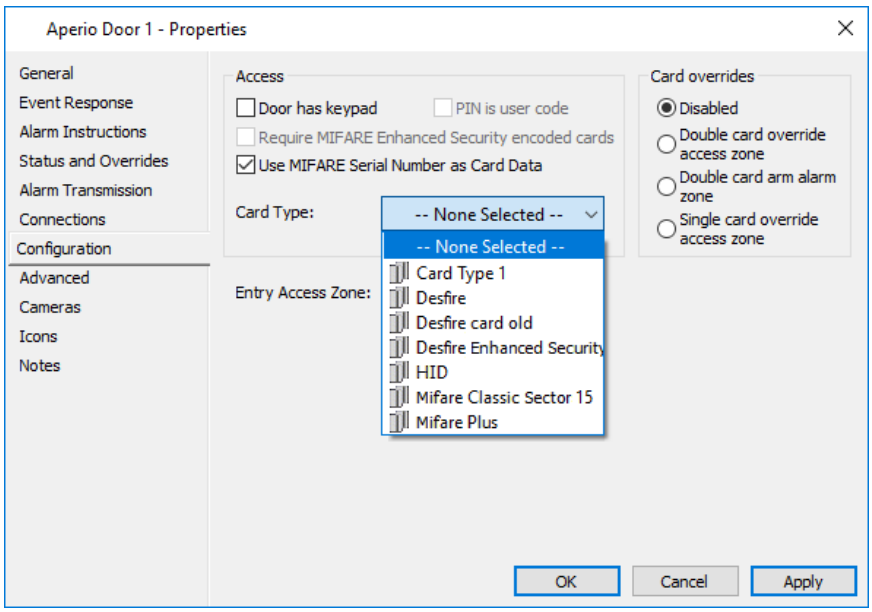
For MIFARE Classic CSN

When using Mifare Classic CSN, you need to do an additional setting in the Aperio door added in command Centre.

1. **Right-click** on the door in Hardware MLW and select **Properties**.
2. Click the **Configuration** tab.
3. Select the checkbox Use Mifare Serial Number as Card Data.



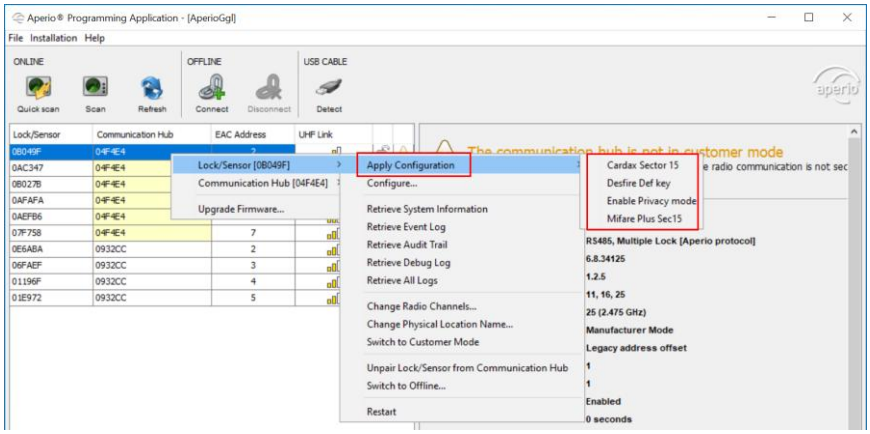
4. Select the card type from the drop-down list and click **Apply**.



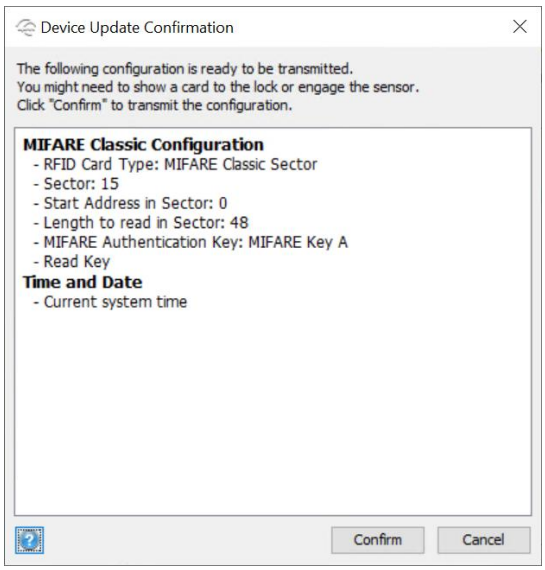
Applying the configuration on the lock

Imported or saved configurations can be applied to a lock from the PAP software, as follows:

1. **Right-click** on the lock to be updated and select **Lock/Sensor** > **Apply Configuration**.
   A list of all the imported or saved configuration files will display.



2. Select the configuration to be applied on the Aperio lock.
   A Device confirmation window displays showing the configuration in the selected file.

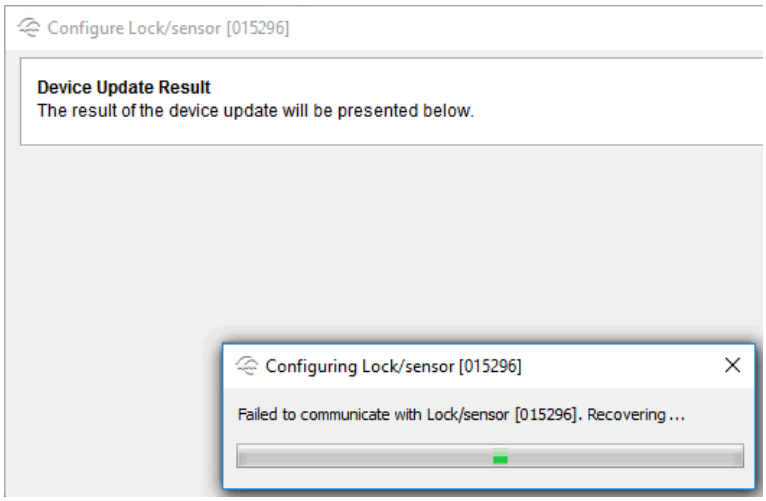


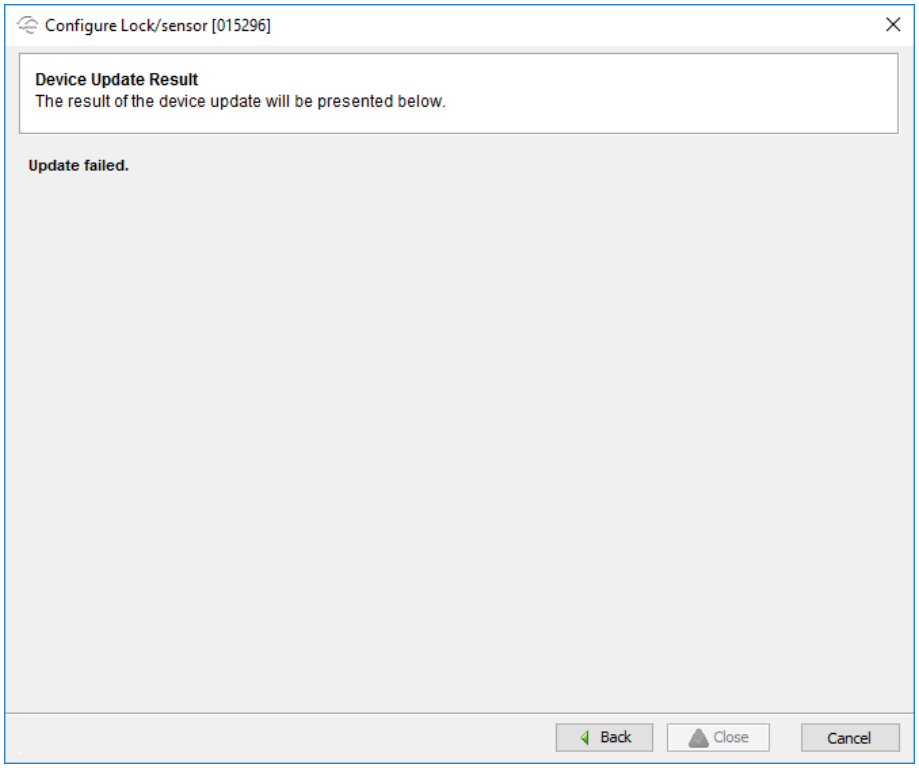
Note: Check the contents displayed to ensure that you have selected the right configuration file.

3. Click **Confirm** to apply the configuration in the selected lock.

Locks failing to update

If configuration of a lock fails, the following screens display:





Reasons why configuration can fail are:

- if configuration is not supported on the lock type, or
- if there are radio channel disturbances. In this case, configuration update should be attempted again.

Configuring Status Report and Polling Intervals

Status Report Interval - Full Polling

The status report interval is used by the communication hub to detect if the lock has gone offline. Any changes to this interval must be done on both the lock and communication hubs.

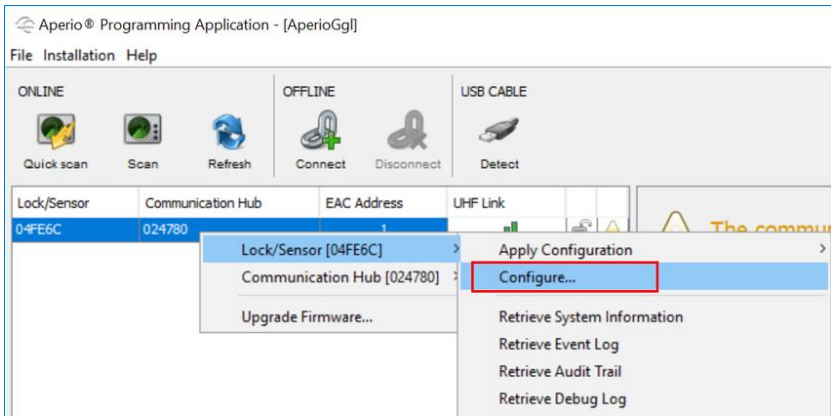
- If one lock is paired with the communication hub this is done automatically.
- If more than one lock is paired with the communication hub (AH30), the status report interval must be set through the communication hub right-click menu with a value, equal or higher than the longest status report interval for the locks paired.

Polling Interval (V3 locks only) - Mini Polling

Mini Polling interval decides how often the lock wakes up and connects to the communication hub to check for information from the controller. Unlike a status report, where the lock status information is also sent to the controller. Mini Polling also allows the Aperio programming application to connect to the lock without the need of activating the radio with a credential (if set to less than 15 seconds). The default polling interval in the lock is 10 seconds.

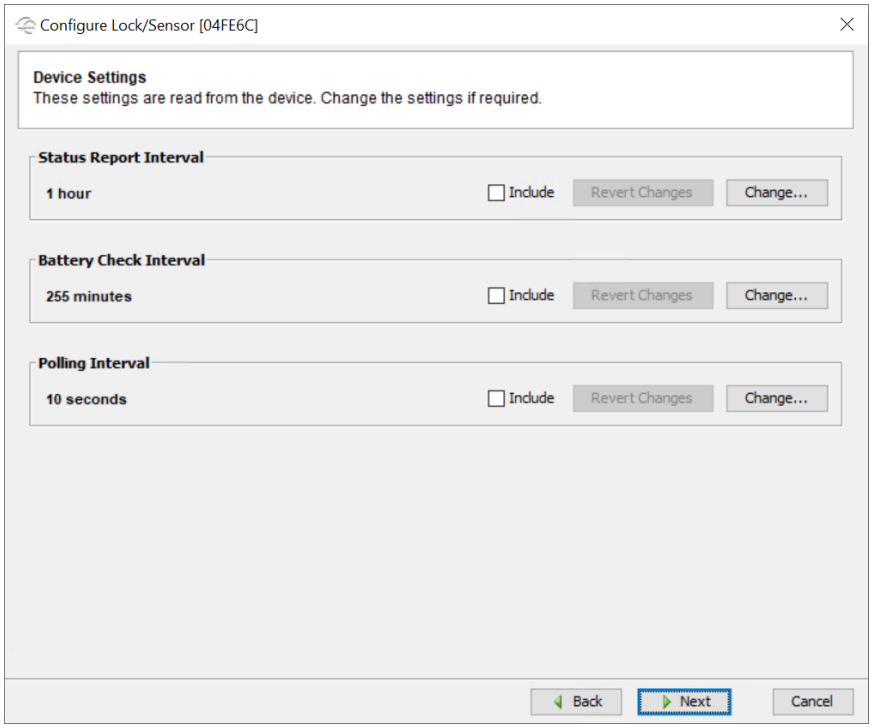
Procedure

1. In the Aperio Programming Application, **right-click** on the lock/reader and select **Lock/Sensor** > **Configure…**

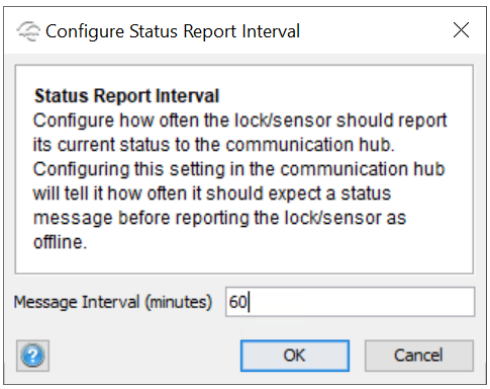


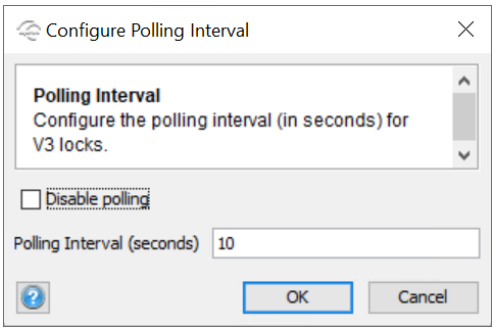
The Configure Lock/Sensor wizard displays.

2. Click **Next** until you reach the **Device Settings** screen of the wizard.



3. Configure as required.

To configure...	then...
Status Report Interval,	a) Click **Change...** in the **Status Report Interval** section of the screen. The Configure Status Report Interval dialog displays.  b) Enter the required status report interval. (Default value of = 60 minutes) **Note:** Lowering the status interval time has an adverse effect on the battery life of the product. c) Click **OK**. The Configure Status Report Interval dialog closes.

To configure…	then...
Polling Interval,	a) Click **Change…** in the **Polling Interval** section of the screen. The Configure Polling Interval dialog displays.  b) Ensure that the **Disable polling** checkbox is unticked and leave the polling time configured at its default value of 10 seconds. c) Click **OK**. The Configure Polling Interval dialog closes.

Configuring the Security Mode (Encryption between hub and lock)

Introduction

Aperio locks support two security modes - Manufacturer mode and Customer mode.
In customer mode, the lock uses secure radio communication with the customer encryption key. Whereas in manufacture mode, the lock uses insecure radio communication with the default encryption key. The default mode is Manufacture mode. Both the hub and the locks/readers must have same security mode configured for successful communication. The hub will not be able to communicate with the lock/reader if the security mode is different.
It is always **recommended to switch to customer mode** but only after the Aperio locks have been paired and configured.
Gallagher recommends the following sequence for switching the locks to customer mode:

1. Pair the locks/readers with communication hub.
2. Configure the communication hubs.
3. Configure the locks/readers.
4. Add the Aperio locks/readers in Command Centre and bring them online.
5. Switch to customer mode on the locks/readers.
6. Switch to customer mode on the hub.

If is not recommended to change the configuration on locks or hubs in customer mode. Always switch back to manufacture mode (locks first and then the hub) before making any configuration changes.
Important:

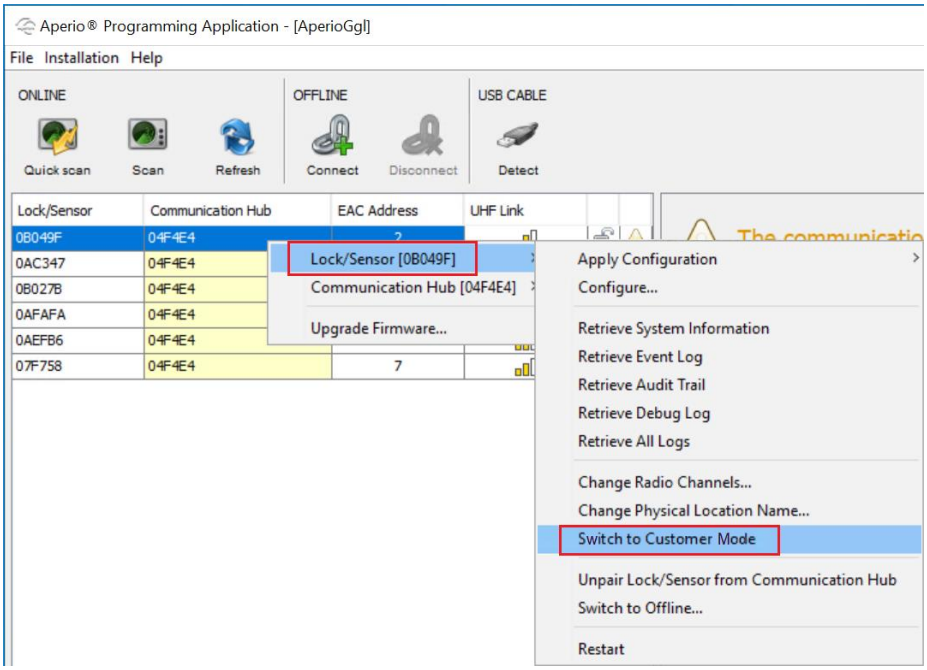
- Never unpair the locks when in customer mode. Always switch to manufacture mode first. If a lock is unpaired in customer mode, it might not be able to use the pair the lock with any other hub unless it's a version 3 lock with USB connection.
  V3 locks with USB can be connected to PAP and configured.
- It is very important to take care of the sequence when changing the security mode. All the locks paired with the hub must be switched to customer mode before switching to customer mode on the hub. Similarly, all the locks paired with the hub must be switched to manufacture mode before changing the mode to manufacture mode on the hub.
- The encryption key used when in customer mode is the same key used when creating an installation in PAP s/w. It is important to keep the key safe and never lose it.

Procedure to switch to customer mode

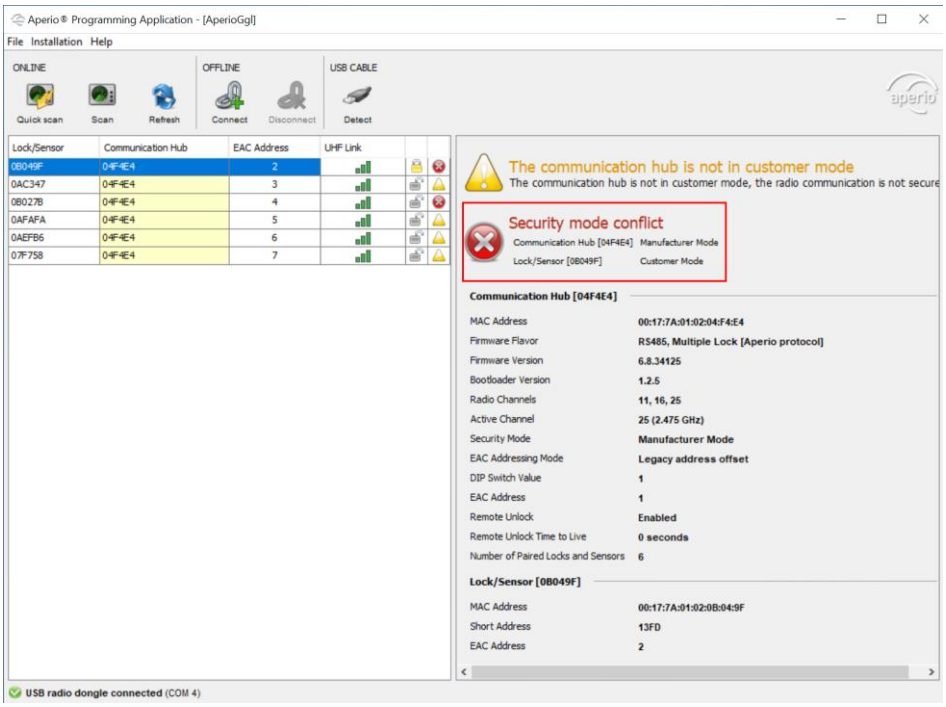
Change security mode on the lock first

1. In the Aperio Programming Application, **right-click** on the lock to be

configured and select **Lock/Sensor** > **Switch to Customer Mode**.

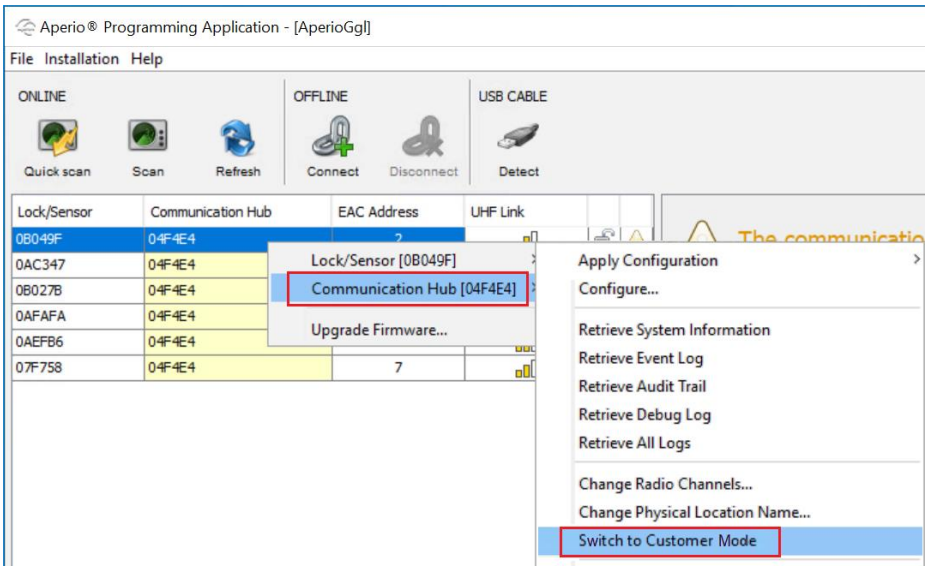


2. Follow the on-screen instructions to show card or engage sensor when required.
3. Once the security mode is changed on the lock, it will show conflict as the hub is still in manufacturer mode.

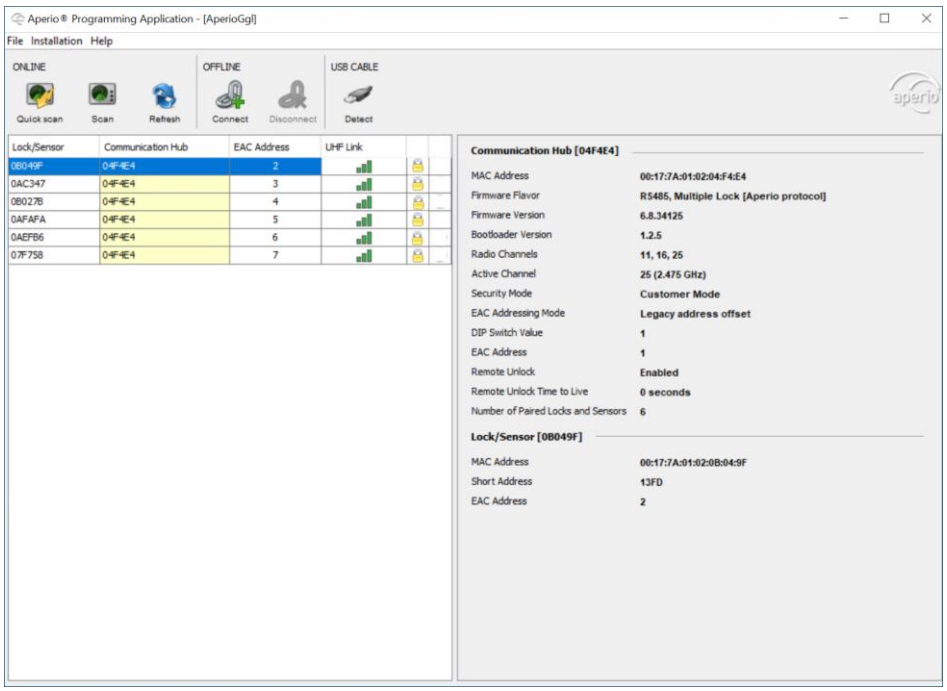


4. Change the security mode to customer mode on all the locks paired with the hub before proceeding further.
5. Change security mode on the hub.

6. Right-click on the hub and select Switch to Customer Mode.



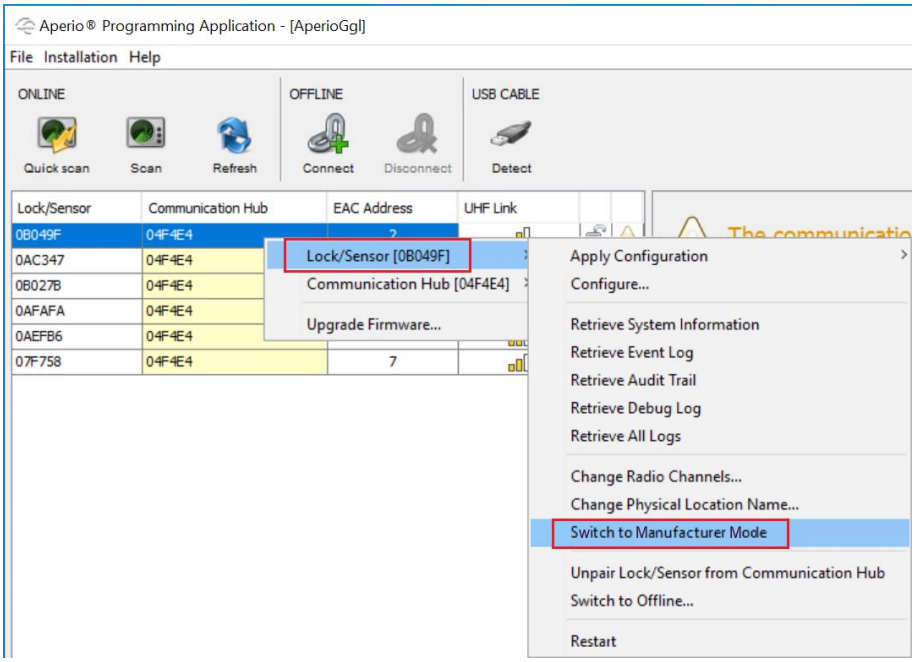
7. Once the mode is changed on both the hub and the locks/readers, the security conflict will be resolved.



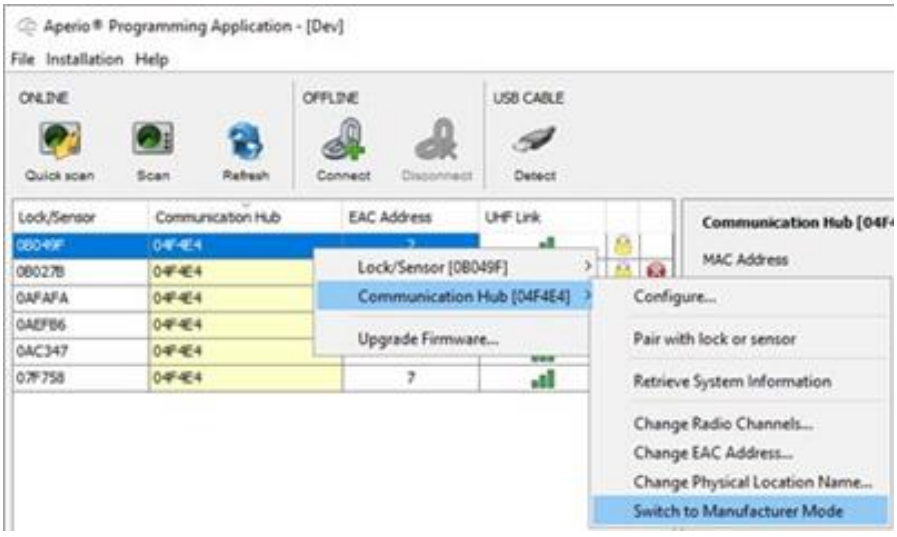
Procedure to switch to manufacturer mode

Change security mode on the lock first

1. In the Aperio Programming Application, **right-click** on the lock to be configured and select **Lock/Sensor** > **Switch to Manufacturer Mode**.



2. Follow the on-screen instructions to show card or engage sensor when required.
3. Change the security mode to manufacturer mode on all the locks paired with the hub before proceeding further.
4. Change security mode on the hub.
5. Right-click on the hub and select Switch to Manufacturer Mode.



Note: Security mode can also be changed from the **Security Mode Setting** screen of the Configure Lock/Sensor wizard.

Enabling the Privacy Mode (if required)

Introduction

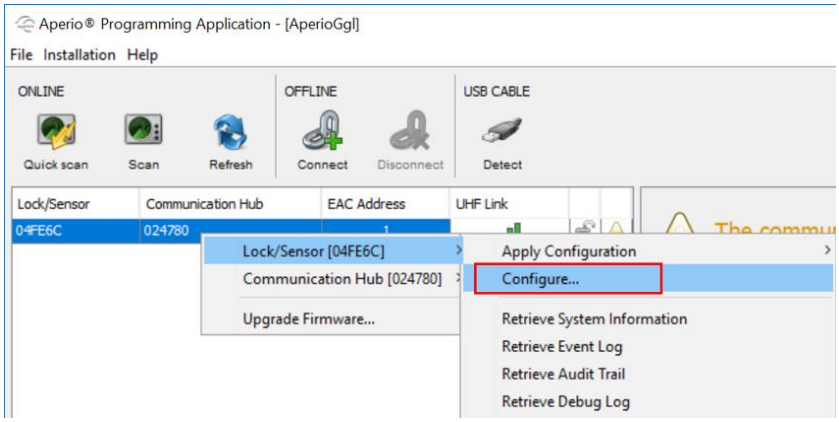
Aperio V3 locks have two modes of locking the doors again after the door opened, as follows:

- **Escape and Return mode**
  This mode allows the door to remain unlocked for a certain period of time after the door has been opened from inside. Escape and Return is enabled by default on Aperio locks.
- **Privacy mode**
  This mode provides a way for the occupant of a room to lock the door from inside and change the access rights to the room. Privacy mode function can only be enabled on locks having a privacy mode button or monitored deadbolt like L100 and E100.

Note: Escape and Return and Privacy mode cannot be enabled at the same time. Enabling one automatically disables the other.

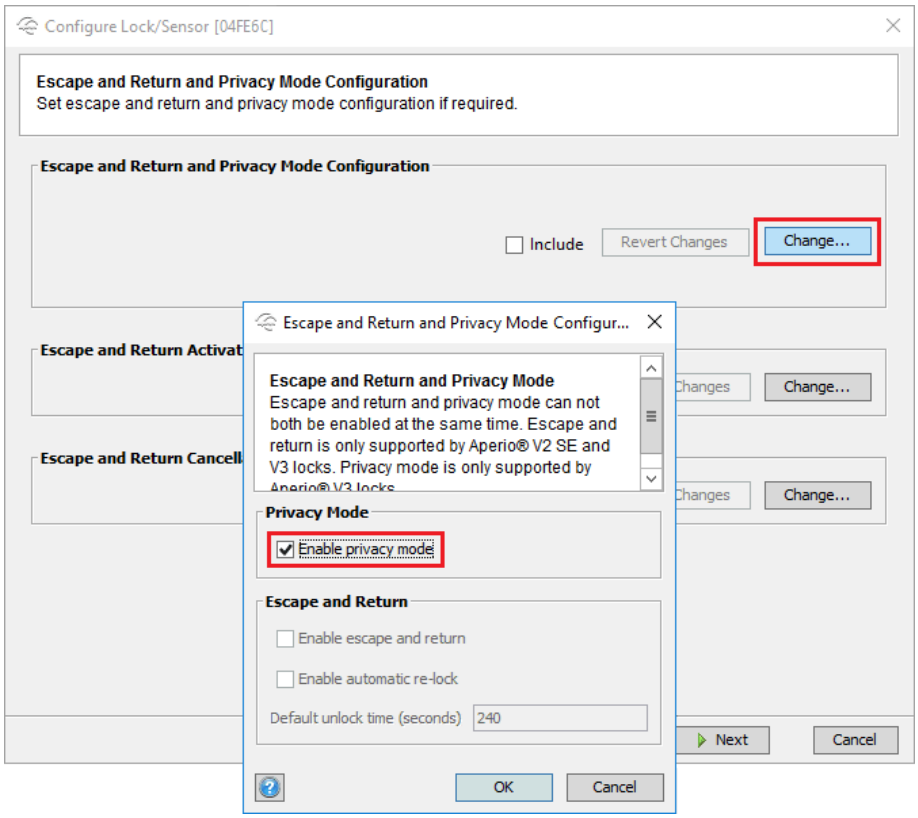
Procedure

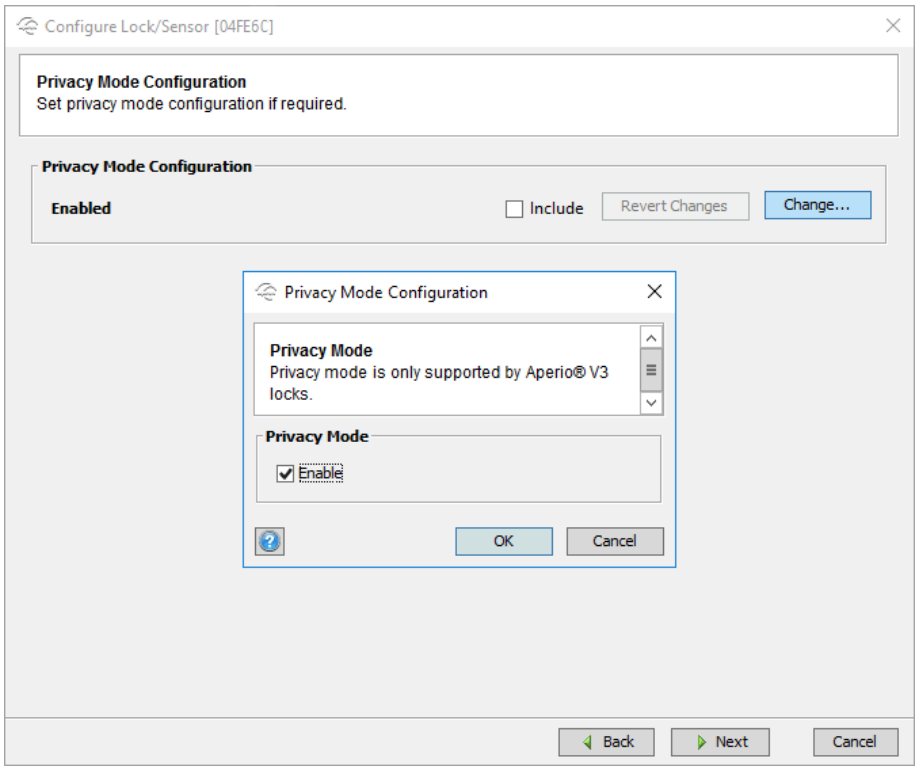
1. In the Aperio Programming Application, **right-click** on the lock/reader and select **Lock/Sensor** > **Configure…**



   The Configure Lock/Sensor wizard displays.

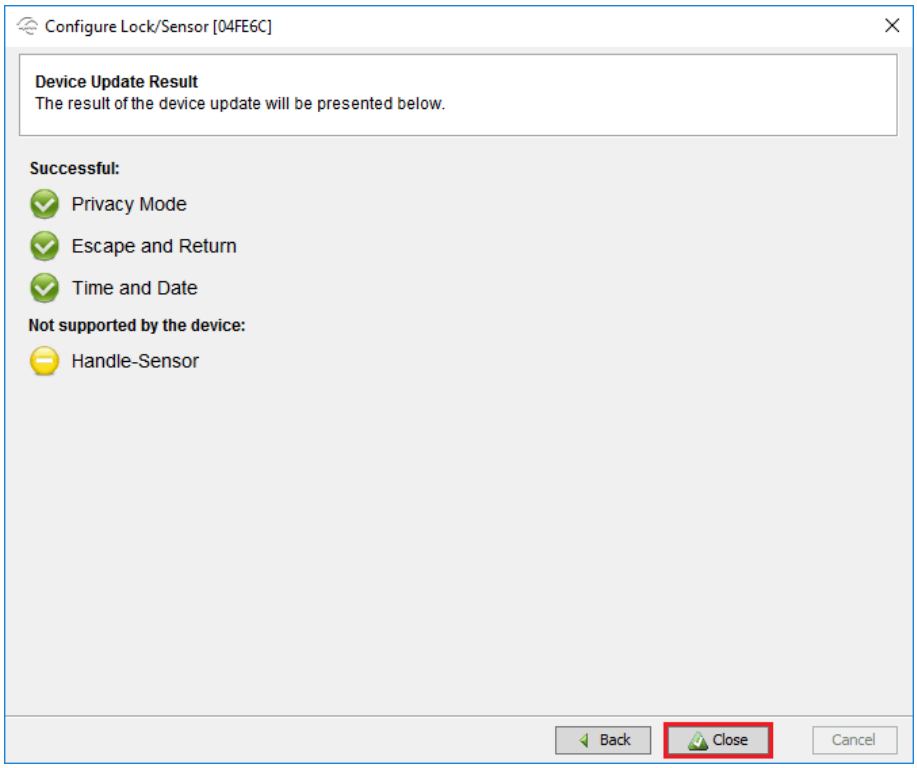
2. Click **Next** until you reach either:
   - the Escape and Return and Privacy mode Configuration screen, OR
   - the Privacy Mode Configuration screen of the wizard.
     Note: The Privacy Mode Configuration screen will only show for locks supporting privacy mode function.
3. Click Change…





4. Click **Change...**
   One of the Configuration dialogs shown above will display.
5. Tick the Privacy Mode checkbox, (i.e. either **Enable privacy mode** or **Enable**) as appropriate, and click **OK**.
   The Configuration dialog closes.

6. Keep clicking **Next** until you reach the Device Update Result screen.



7. Click **Close**.

Enabling the Smart Credential cache (Dynamic cache)

Introduction

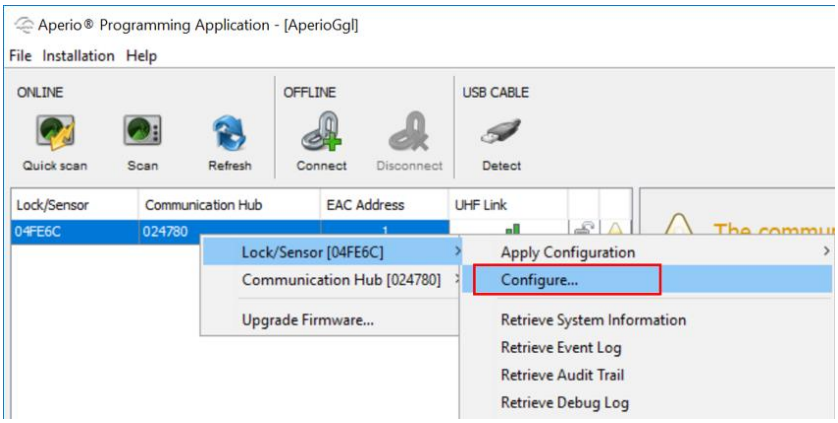
Smart Credential cache (Dynamic cache) saves access granted credentials locally in the lock memory. These cardholders would then be granted access for a predefined period of time even when the lock is offline. The two parameters that can be set when enabling dynamic cache are:

- **Number of credentials:** Sets the maximum number of credentials that can be saved in the cache. The default value is 100. Maximum value that can be set is 1000 in PAP (from version 3.4 or later of PAP).
- **Valid for:** Sets for how long the credentials stored in the cache would be valid from the time when access is granted. Default is 24 hours 0 minutes. Maximum value that can be set is 720 hours (30 days) and minimum value is 1 minute.

Note: Dynamic cache is supported by V3 locks only.

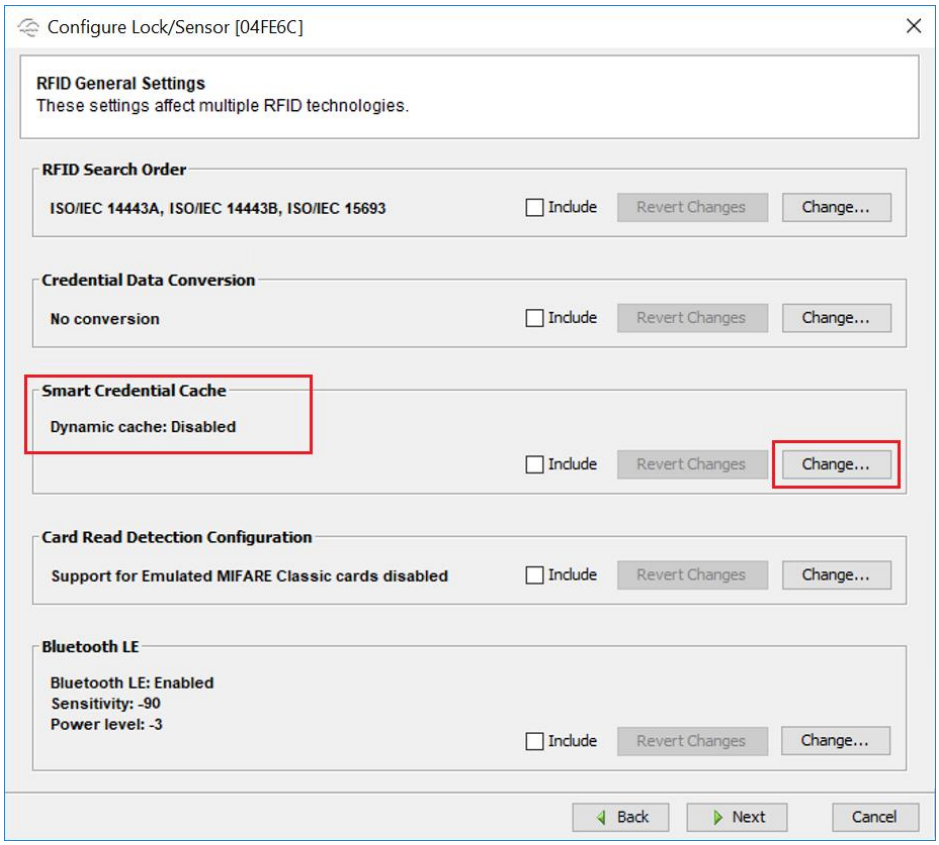
Procedure

1. In the Aperio Programming Application, **right-click** on the lock/reader and select **Lock/Sensor** > **Configure…**

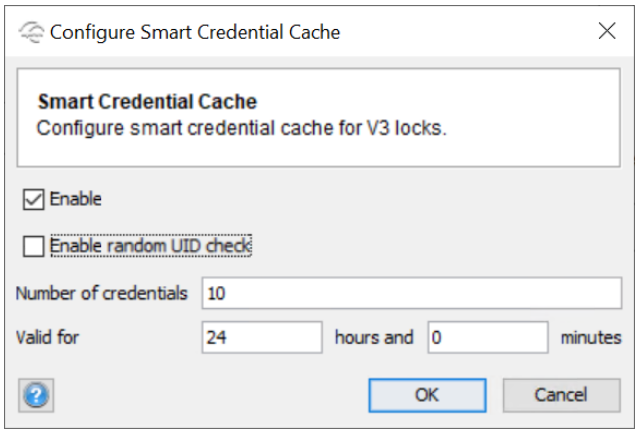


   The Configure Lock/Sensor wizard displays.

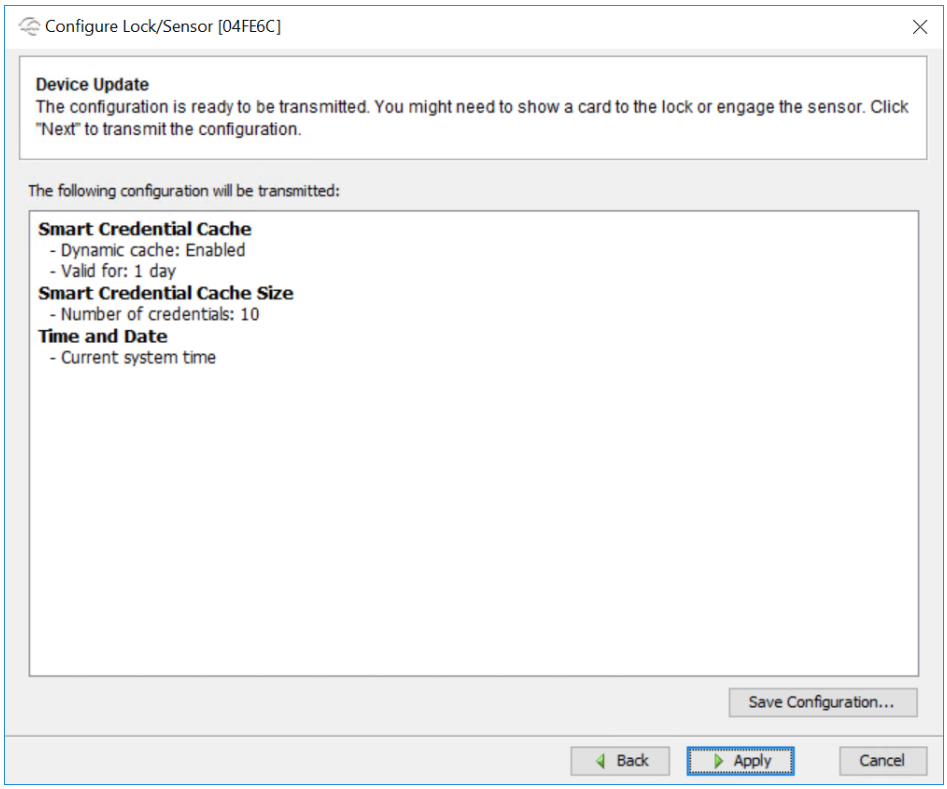
2. Click **Next** until you reach the **RFID General Settings** screen of the wizard.



3. In the **Smart Credential Cache** section of the screen, click **Change…**
   The Configure Smart Credential Cache dialog displays.



4. Enable Dynamic cache by ticking the **Enable** checkbox.
   Enable Random UID check should be disabled.
5. Set the **Number of credentials** to be saved in the lock and the length of time they will be **Valid for**.
6. Click **OK**.
   The Configure Smart Credential Cache dialog closes and the Device Update screen of the wizard displays.



7. Click **Apply** to save the configuration.

Configuration for Mobile Connect

Introduction

This procedure describes how to configure mobile credentials to gain access at Aperio locks.

Note: To improve the user experience, it is strongly recommended that the Aperio reader buzzer be enabled. Doing so, will provide audible feedback to the phone user. All Aperio E100 readers support buzzer configuration.

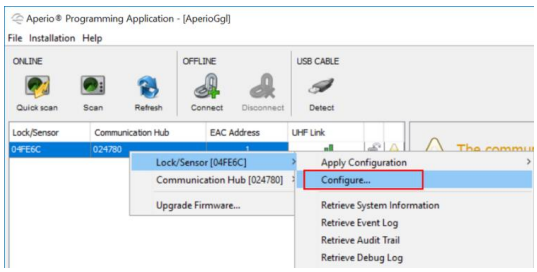
Prerequisites

The Aperio Mobile Site Key, ID and Service Code must be configured on the **Mobile Access Settings** tab of the Server Properites in Command Centre Configuration Client prior to performing this procedure. See ***Mobile Access Settings*** (on page 6-73) for further detail.

Note: You will need to use the latest versions of software and firmware for this to work see below:
- Aperio Programming Application 30.0.23 or later
- wireless lock firmware 3.20.0 or later, using a Bluetooth capable lock
- Mobile Connect App: iOS 16.03.049, Android 16.03.038 or later

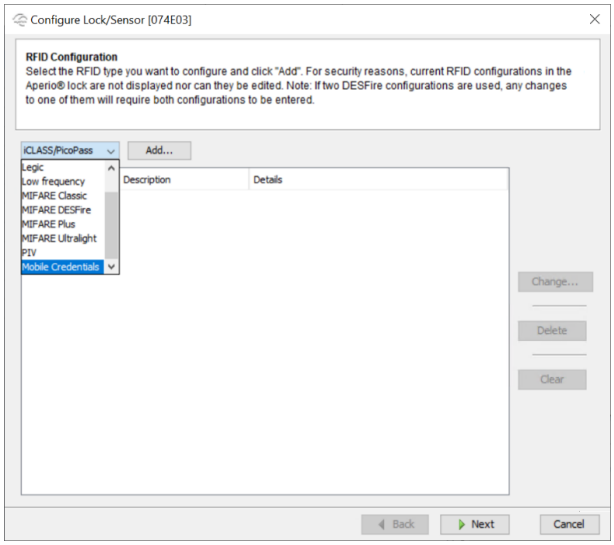
Procedure

1. In the Aperio Programming Application, **right-click** on lock/reader and select **Lock/Sensor** > **Configure**.

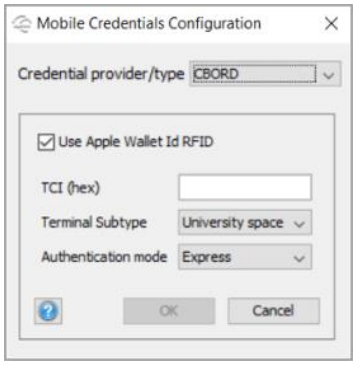


The Configure Lock/Sensor wizard displays.

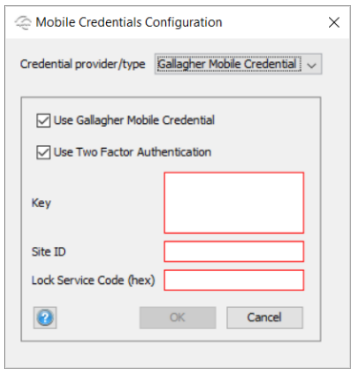
2. Select **Mobile Credentials** from the drop-down list and click **Add...**



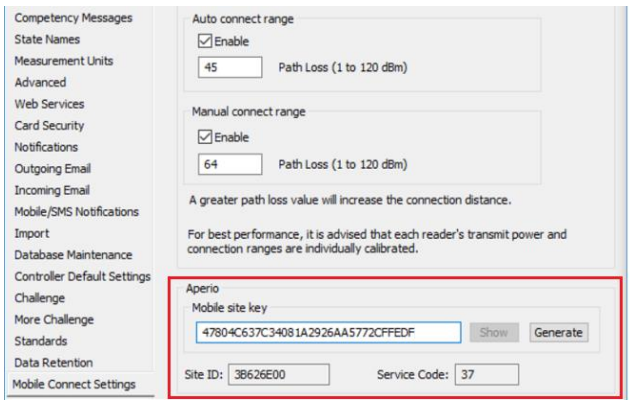
The Mobile Credential Configuration dialog displays.

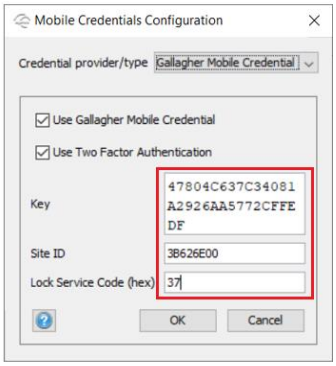


3. From the **Credential provider/type** drop-down list, select "Gallagher Mobile Credential".



4. Only leave the **Use Two Factor Authentication** checkbox ticked if your site requires users to authenticate via mobile screen lock before requesting access at the door.
5. Copy the **Key**, **Site ID** and **Service Code** from the **Mobile Access Settings** tab of the Server Properites in Command Centre Configuration Client.
   See ***Mobile Access Settings*** (on page 6-73) for further detail.



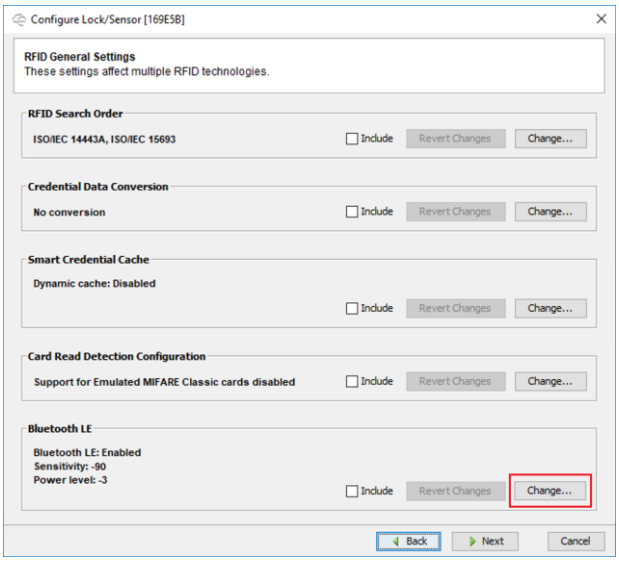


6. Click **Next** until you reach the screen where you can **Apply** the changes.

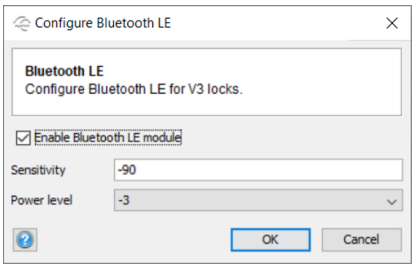
Changing the auto-connect range for an Aperio Door

The auto-connect range, (i.e. the read distance between the phone and the lock), is set in the Aperio Programming Application, as follows:
Note: There is no manual connect.

1. In the Configure Lock/Sensor wizard, click **Next** until you reach the "RFID General Settings" screen of the wizard.



2. Click the **Change...** button in the Bluetooth LE section.
   The Configure Bluetooth LE dialog displays.



3. Adjust the figure in the **Sensitivity** field as appropriate.
   Note: The installer needs to calibrate the locks to the appropriate sensitivity, (i.e. the read distance between the phone and the lock). Unlike Gallagher who use the Path Loss for calibration, Aperio use RSSI.

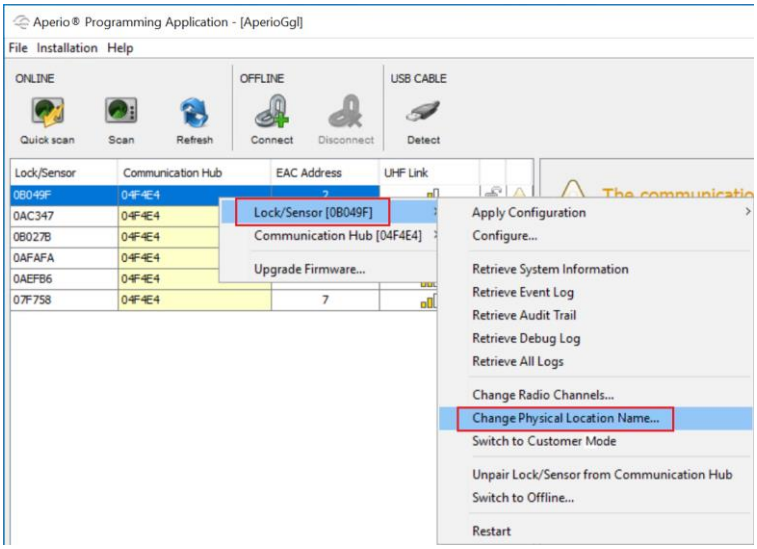


4. Click **OK**. The Configure Bluetooth LE dialog closes.
5. Click **Next** until you reach the screen where you can **Apply** the changes.

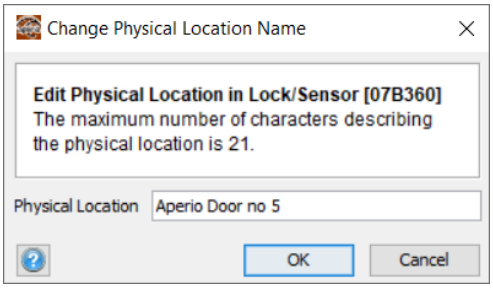
Changing the physical location

This function applies to both communication hubs and locks/sensors. In the example below the physical location name is changed for a lock sensor.

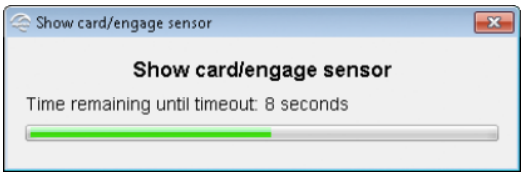
1. Hover over Lock/Sensor and click **Change Physical Location Name…**



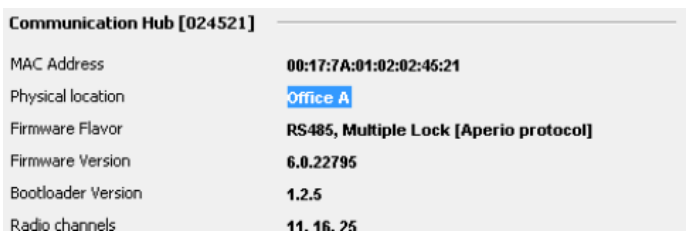
The Change Physical Location Name dialog displays.



2. Enter a description in the **Physical Location** field that clearly identifies the lock position and click **OK**.
   Note: The **Physical Location** field allows 21 characters to be entered but only 19 characters are passed to Mobile Connect.
3. Hold the credential at the lock, or engage the magnet for the sensor.
   For a communication hub the information is updated immediately.
   Note: This step is not necessary for V3 locks that are connected with a USB cable, or online locks that have the polling interval set to less than 15 seconds.



After a successful reading a progress bar shows the download.
After the update completes, the new location name is shown in the Lock/sensor section on the lower right side of the installation view.



Configuring Override Credentials for Offline Access for System Administrators

Introduction

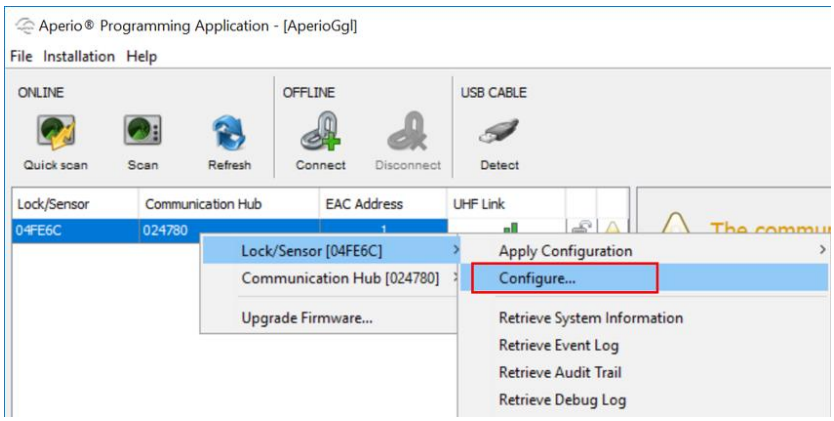
The override credentials are used to gain access to an area when the controller is offline or when the lock has lost connection with the communication hub. Only the credentials from the override list will be granted access when the system is offline. You may add 10 override credentials to a lock.

Important:

- Use of override credentials when using a Wiegand hub requires that DIP switch 1 is set to position ON.
- When adding an override credentials in the lock all existing override credentials are removed from the lock. It can therefore be convenient to include this when saving a configuration.
- You do not have to enter the override credential data manually for every lock to be configured. This can be saved using the Save configuration function as the last step of the configuration wizard.

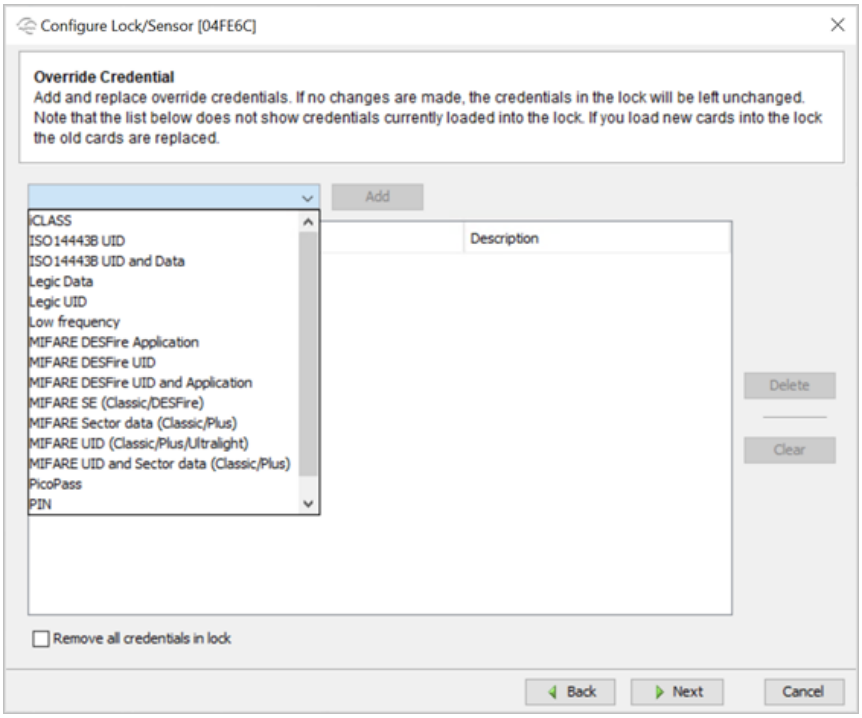
Procedure

1. In the Aperio Programming Application, **right-click** on the lock/reader and select **Lock/Sensor** > **Configure…**



The Configure Lock/Sensor wizard displays.

2. Click **Next** until you reach the **Override Credential** screen of the wizard.

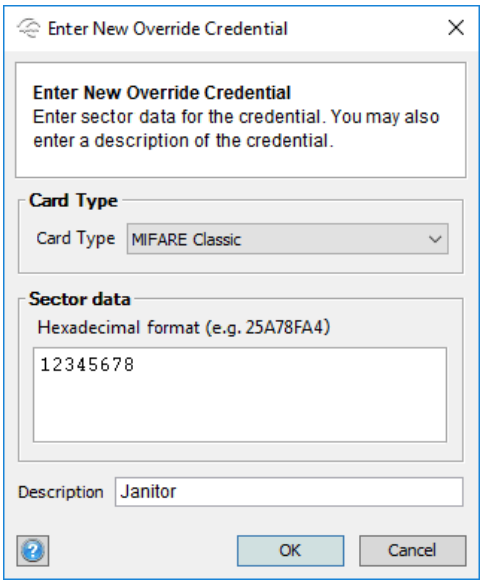


Note: If you check the **Remove all credentials in lock** checkbox, all existing override credentials in the lock will be deleted during the configuration process.

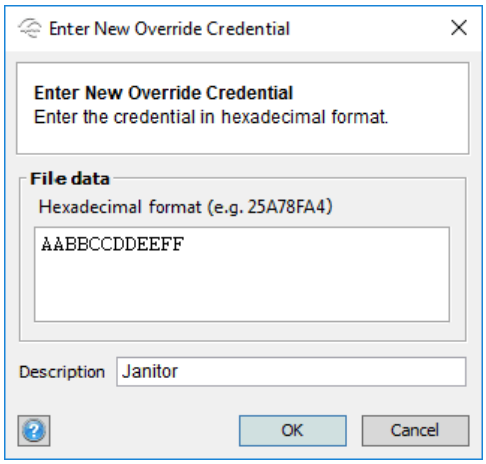
3. Add an override credential by selecting the appropriate card type from the drop-down list and clicking **Add**.
   An Enter New Override Credential dialog displays.

   Note: The information that appears on the Enter New Override Credential dialog will differ depending on the card type you selected.

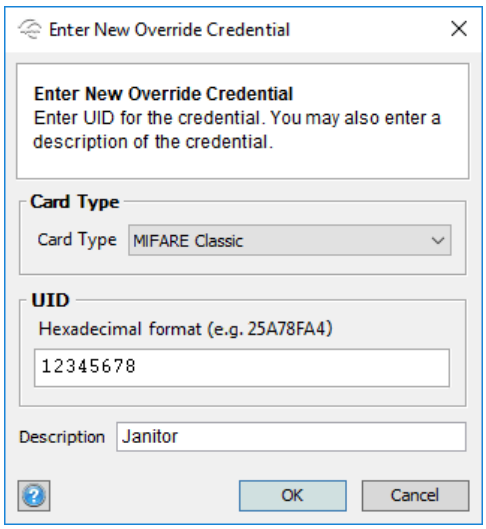
4. Enter the override credentials for the selected card technology.
   A few examples for different card types are given next:



Mifare Sector data (Classic/Plus)
Card Type: MIFARE Classic or MIFARE Plus.
Sector data: Sector data stored on the card.
Description: For example, the credential owner.

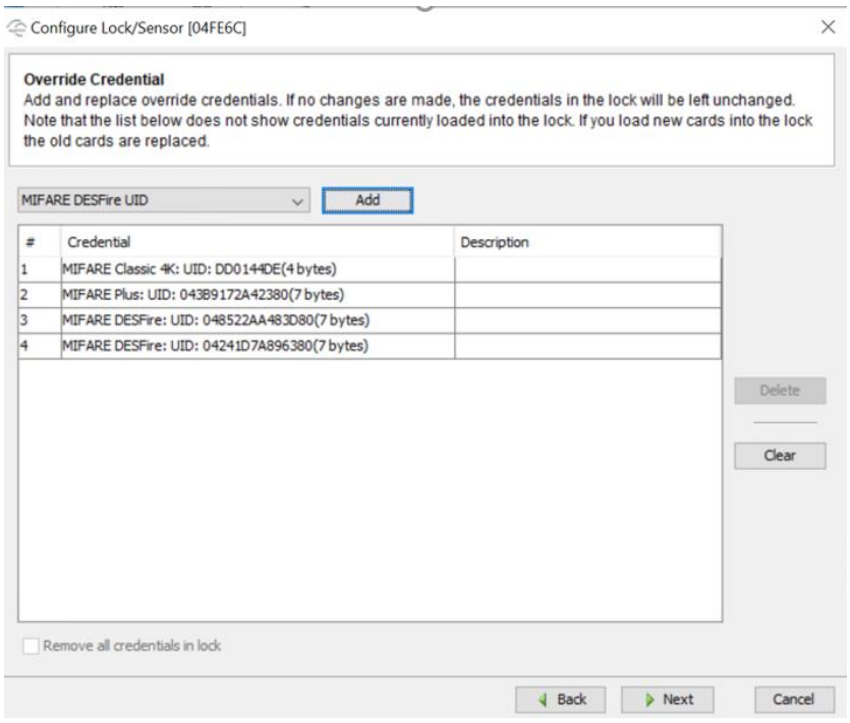


Mifare DESfire Application
File data: File data stored on the card.
Description: For example, the credential owner.



Mifare UID
Card Type: MIFARE Classic or MIFARE Plus.
UID: Card number.
Description: For example, the credential owner.

5. Once all the override credentials have been added, keep clicking **Next** to apply the configuration.



Configuring R100 Readers

Introduction

R100 readers can only be connected to Aperio AH20 Wiegand hub. They are not supported on RS485 bus. They should be configured as any standard third party reader in Command Centre.

Important:

- R100 readers do **NOT** support double card overrides.
- In order to get card events back in Command Centre from when the reader is in free mode, enable 'Remote Unlock' functionality on the hub in PAP.

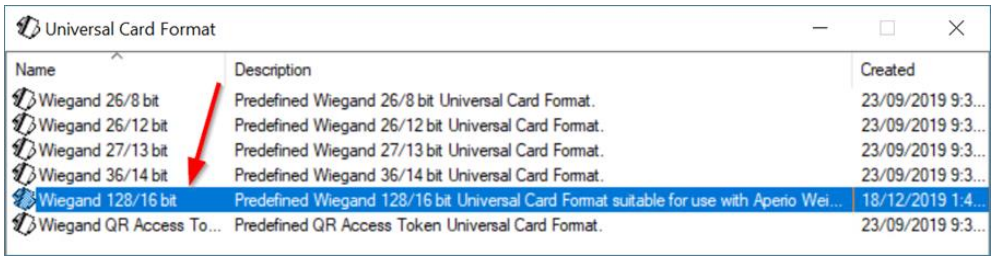
Detailed instructions are given in the procedure below.

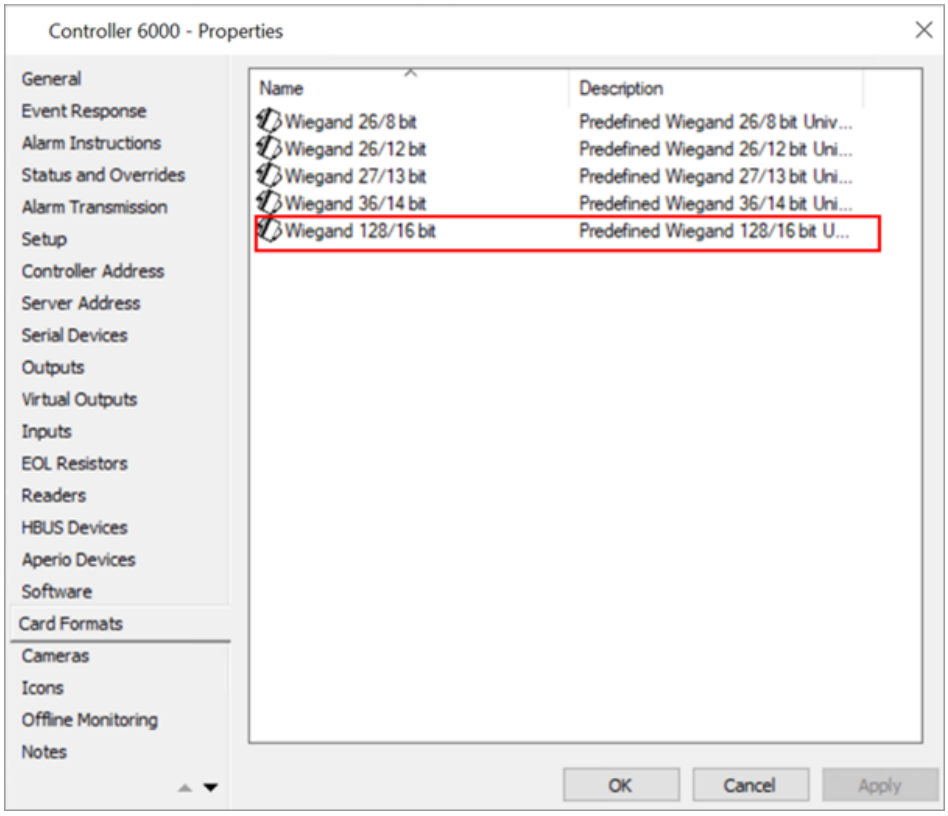
Pre-requisite

Before performing this procedure, the R100 reader must be paired with AH20 hub and connected to the controller.

Procedure

1. Create a Third-Party reader in Command Centre.
   For further detail see ***Creating Readers*** (on page 21-40).
2. Create a door with the reader created in the above step configured at the entry zone.
   For further detail see ***Creating Doors*** (on page 22-2).
3. Click **Configure** from the menu bar, then **Universal Card Format**.
4. Go to the Controller properties and click the **Card Format** tab.
5. Drag the Universal Card Format “Wiegand 128/16 bit” onto the card format tab of the Controller.





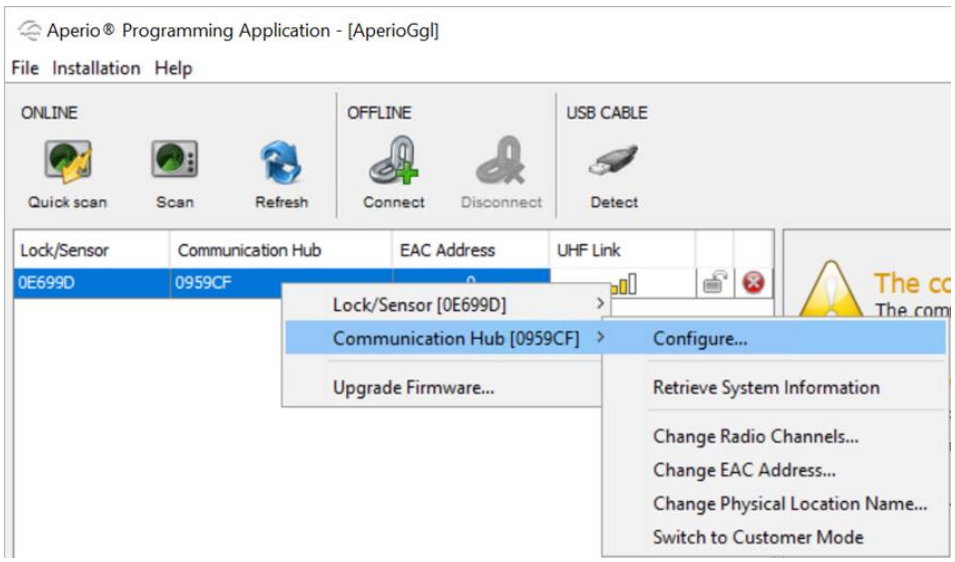
Note: This format would enable the Wiegand reader to read Gallagher encoded cards.

6. Click **Apply**.

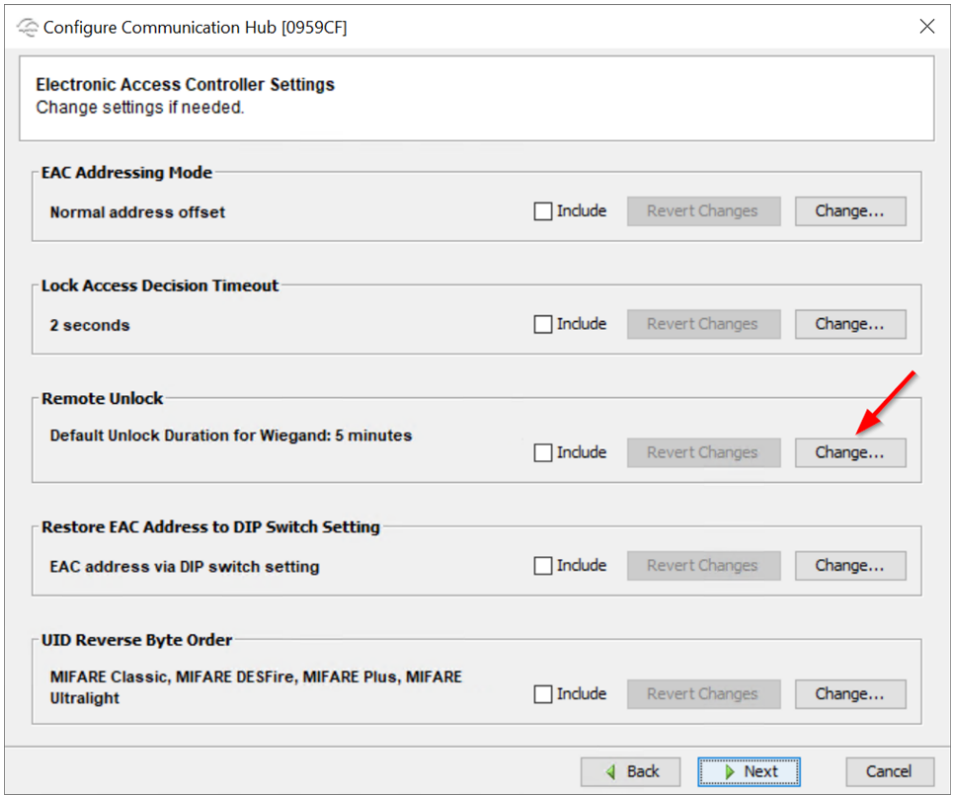
Enable 'Remote Unlock' on the hub

Required to get card events back in Command Centre when the lock is in ***Free*** mode.

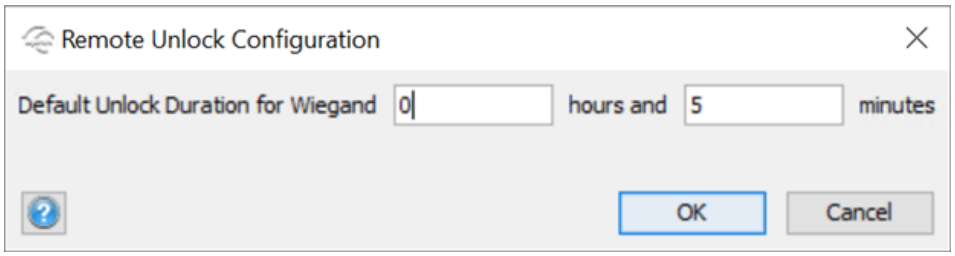
1. Go to Aperio PAP.
2. Right-click the hub and select Communication Hub > Configure...



3. Click Next to go to Electronic Access Controller Settings screen of the wizard.
4. Click Remote Unlock > Change.



5. Set the Remote unlock duration.

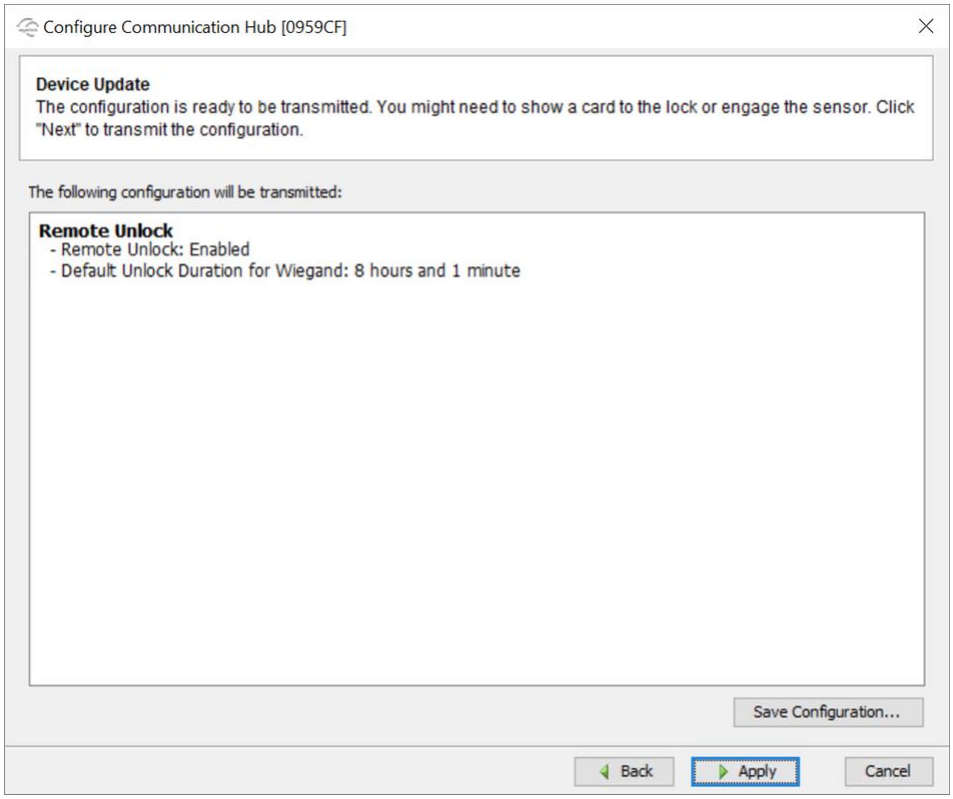


Important: The duration set for Remote unlock must be greater than the scheduled time configured for the lock to be in *Free* mode.

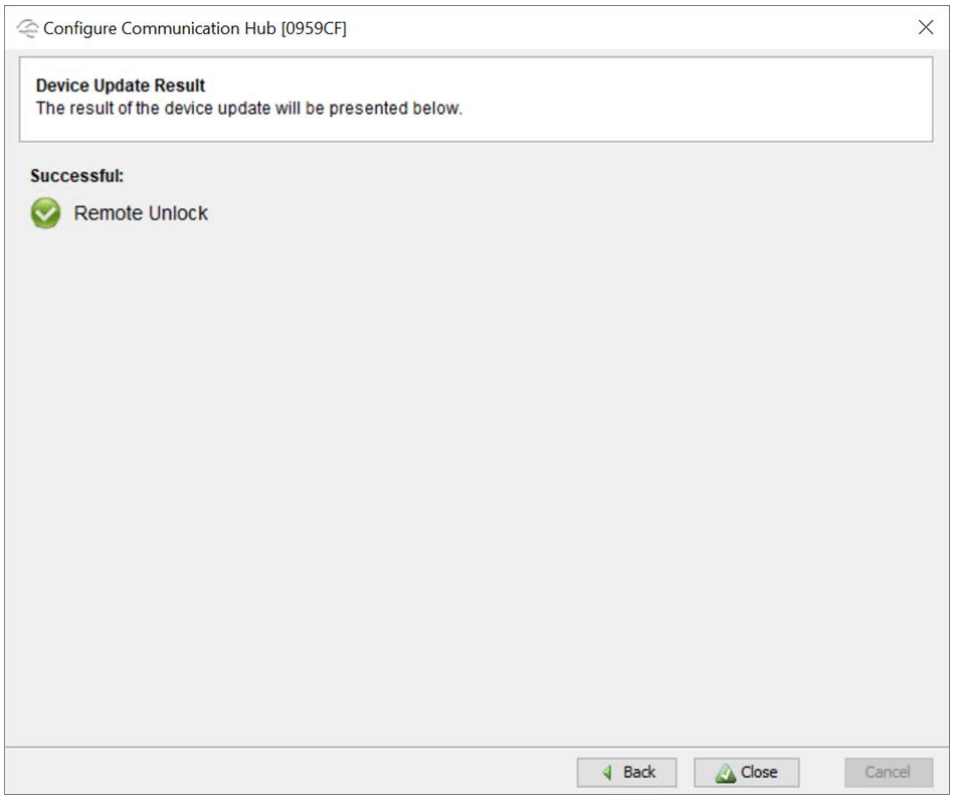
For example: If the Command Centre schedule configured on the lock sets the door in free mode for 8 hours, then the 'Unlock Duration for Wiegand' must be set to greater than 8 hours.

This configuration is however ignored in *Secure* mode.

6. Keep clicking **Next** until you reach the Device Update Result screen.



7. Click **Apply**.



8. Click **Close**.

Troubleshooting - Aperio Integration

The following table describes some of the known issues that can occur, and possible causes:

Problem	Possible Causes
Bad Packet Alarm	• The configuration of the Aperio Door in Gallagher doesn't match the configuration of the Aperio reader in the Aperio Programming Application Protocol (PAP). For example, it could be that the Aperio reader has been configured to send only the MIFARE CSN, but the Gallagher Controller is expecting Gallagher sector data, or it could be that the cylinder has been configured to send only, Gallagher sector data, but the Gallagher Controller is expecting the MIFARE CSN. • The cylinder could be configured to send any portion of bytes from any sector on the card. For example, a site using their own MIFARE keys could configure the cylinder manually and might accidentally select the wrong number of bytes, or the wrong offset in the Aperio PAP. The Gallagher Controller will then receive the wrong number of bytes.
Lock giving unusual set of flashes after presenting a card	There are multiple possible causes. Please consult the *Aperio Installation Manual* section 5.5 to ascertain which state or issue that the lock flash sequence refers to.
Mobile Connect does not see the Aperio Reader in the Access Door list	Check that the Mobile Connect app is current,with at least 16.03.049 for iOS and 16.03.038 for Android. If the Mobile Connect app was upgraded after the Command Centre server, the Cardholders Mobile Credentials state will need to be set to Disabled (manually) and enabled again to resend the Aperio key. This process can be completed with a Bulk Change for multiple cardholders.

Chapter 77: Schlage Lock Interface

Introduction

The Schlage Lock Interface is a licensed feature of Gallagher Command Centre. This feature supports Schlage wired (AD30X) and wireless (AD40X) locks with Gallagher Controller 6000s.

Important: This integration is not intended for use in cases where encryption is required.

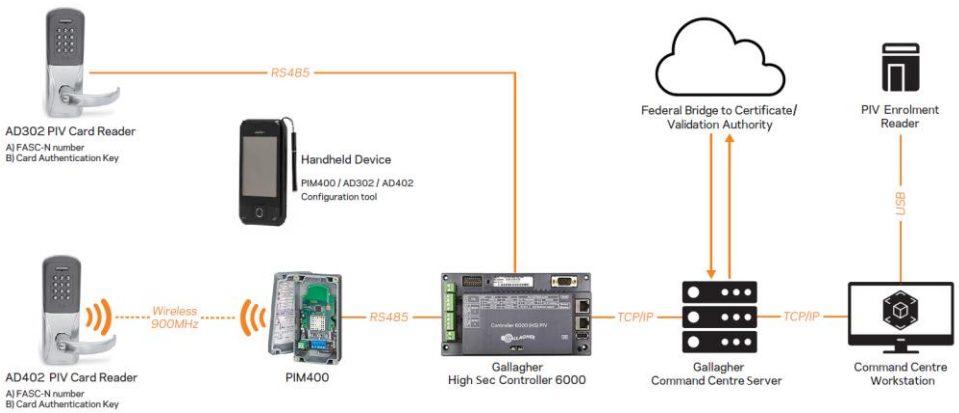
The Schlage Lock Interface allows one Gallagher Controller 6000 or 7000 to manage up to 8 Panel Interface Modules (PIM's), and either 16 Schlage AD40X locks or 8 Schlage AD30X locks, or a combination of both totaling 16. The hardware will consume allocations as below:

- PIM400 will consume one PIM allocation
- AD40X will consume one lock allocation
- AD30X will consume one PIM allocation and one lock allocation

A single PIM400 can have up to 16 Schlage AD40X devices connected to it. If more than one PIM400 is connected to the controller, it is important to note that the total number of locks the controller can manage is still 16, it does not increase. In Command Centre, a Schlage PIM400 is attached to one of the two RS-485 buses on the Controller 6000 or 7000, and a Schlage AD40X lock is assigned to a Schlage PIM400. The Schlage AD30X is attached directly to one of the two RS-485 buses on the Controller 6000 or 7000. Physically, a Schlage PIM400 is wired to one of the two RS-485 ports on a Controller 6000. If more than two PM400s need to be connected, they can be wired together into the RS-485 bus, or an extension board can be used. A Schlage AD40X lock talks to a Schlage PIM400 via 900 MHz wireless communication. The Schlage AD30X lock is wired directly into one of the two RS-485 buses, and they can also be wired together, or an extension board used, if more than two AD30X devices need to be connected to a single controller. If the site wishes to use both Gallagher and the Schlage AD series of locks, an HBUS can be connected to a free RS-485 bus.

Note: If the site is using the PIV functionality available in the AD302 and AD402 locks, a Gallagher High Sec Controller 6000 or 7000 is required.

Schlage High Security (PIV Card) System Diagram

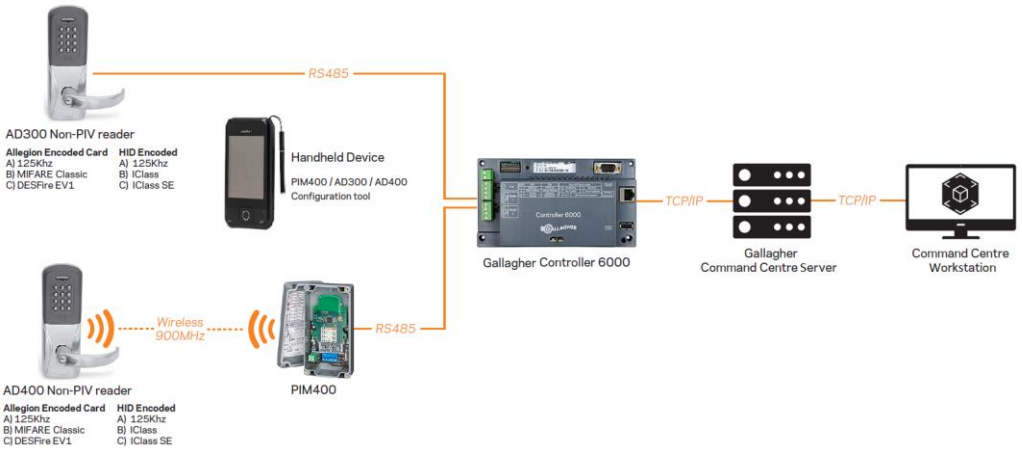


Schlage AD302 and AD402 lock hardware is supplied with the Schlage FMK reader. In addition to supporting PIV cards (for FIPS 202-2 compliance), this reader is also able to support Schlage encoded MIFARE Classic and DESFire credentials.

The AD302 and AD402 locks will require the Gallagher High Sec Controller 6000 device in order to manage the challenge response for PIV credential certificates. The Keypad PIN functionality for this reader would be configured from within Command Centre. For entering PINS the * button on the door lock keypad will clear any numbers entered, and the # button is the **Enter** button. Enrolment of PIV credentials will be performed through the PIV enrolment reader.

Note: Refer to *Chapter 56: PIV Card Support* for further details on how PIV cards work in Command Centre.

Schlage Standard (non-PIV) System Diagram



Schlage AD300 and AD400 hardware is able to support various card technologies supplied by Allegion and HID. This integration has been tested with Low Frequency (125KHz), and High Frequency readers. Schlage and HID credential types 125KHz, MIFARE Classic, DESFire EV1, IClass and IClass SE has been tested with Command Centre. Support of these Credential formats are managed through the configuration of the Universal Card Format section.

Note: The USB enrolment reader used for PIV card enrolment is not required.

Command Centre Door Licensing

Each Schlage AD30X and AD40X lock will require a Command Centre Schlage Door License (2A08900 - Schlage license without hardware (per door)).

The license file must contain the following option:

```
[Limits]
Schlage Doors=x
```

A Command Centre PIV license is required to enable PIV cards to be enrolled.

Schlage Hardware Device Limits

- One Schlage RS485/900MHz PIM400 supports up to 16 Schlage AD40X 900MHZ Doors
- One RS485 port on Controller 6000 or 7000 supports up to 8 Schlage RS485/ 900MHz PIM400's
- One RS485 port on Controller 6000 or 7000 supports up to 16 Schlage AD40X Doors or 8 Schlage AD30X Doors

- One Controller 6000 or 7000 supports up to 8 Schlage RS485/900MHz PIM400's
- One High Sec Controller 6000 or 7000 can support up to 16 Schlage AD40X Doors or 8 Schlage AD30X Doors
- One Controller 6000 or 7000 supports up to 16 Schlage AD400 Doors or 8 Schlage AD300 Doors

Schlage Configuration Settings

- To receive battery status messages from the Wireless AD-40X devices at a frequency of less than 10 minutes, the heartbeat must be manually configured via the Schlage hand-held device.
  Note: Changing the Schlage Door's heartbeat time can cause issues. Therefore, we recommend not changing it where possible.
- For AD40X devices, PIM400 wakeup, Permitted Card Technology and PIV Authentication Mode changes may require up to 2 door heartbeat cycles to take effect. The recommended default door heartbeat period is 10 minutes.
- Access Zones can be in Secure, Secure + PIN and Free access mode.
- Configuration changes and Access Zone access mode changes should not be made at the same time.
- Custom site keys are not available with the GGL/Schlage integration



- RS-485 communications between the controller and Schlage AD30X locks or PIM 400's (Panel Interface Modules) are **not encrypted and should be physically secured against tampering**.

Tips

- If you change the RS-485 address of the PIM it will be dynamically updated on the controller. The RS-485 address of the PIM specified in Command Centre needs to match the one configured in the Schlage HHD.
- All values for RS485 Address and AD-Series Doors must be between 0-254.
- Address values cannot be duplicated on a common RS485 Bus.
- High door value must be >= Low door value.
- High door value cannot be any more than 16 higher than the Low door value.
- If you attempt to give two PIMs on the same bus the same address you will get the following error: *RS-485 Addresses on the same bus must be unique*.
- Wakeup is enabled by default to 10 seconds (from v8.40). This is required to support remote lock overrides from the Command Centre server.

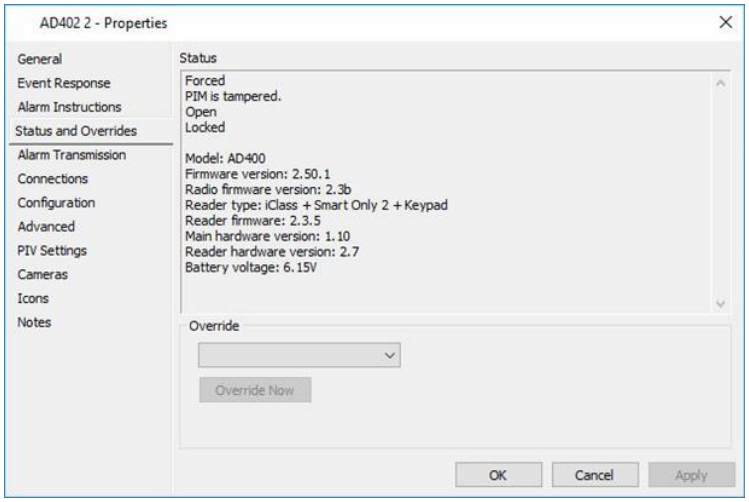
Battery Management

Command Centre is able to monitor the voltage level status of each AD series lock, and display the current voltage level in the Status and Overrides property page of the Schlage Door, as shown in the screen shot below. Low and Critical battery alarms are available help to manage lock failure due to battery depletion.

AD30X locks: AD30X locks must never be powered with batteries. The AD30X requires 12 or 24 VDC 250 ma AUX power. The AD300 must be powered from an external AUX supply to provide sufficient power for the RS-485 communication, the AD30X will not function on batteries.

AD40X locks: AD40X locks can be powered by 4 or 8 batteries. Reader types determine voltage levels needed for operation. Locks with smart card readers,

SM & MT, require higher voltage levels. Locks with Prox and Mag card readers can operate to lower voltages. A low or critical battery alarm is raised when the battery pack of the lock depletes to a certain threshold. The table below shows the battery voltage levels corresponding to the low and critical alarms.



	4 Battery Holder	8 Battery Holder
New batteries	6.2 VDC	12.4 VDC
Low battery alarm	4.7 VDC (for SM & MT readers) 3.7 VDC (for Magnetic swipe and 125KHz readers)	7.2 VDC
Critical battery alarm	4.6 VDC (for SM & MT readers) 3.4 VDC (for Magnetic swipe and 125KHz readers)	6.9 VDC

USB communication with the HHD will stop working at 4 VDC. Gallagher recommends checking the voltage of all locks at the time when a low battery alarm occurs so other locks close to low level can undergo battery replacement at the same time. At critical level, AD40X locks will fail to operate, go to Fail mode of "As-is; Safe; Secure", and lose any data stored within the lock.

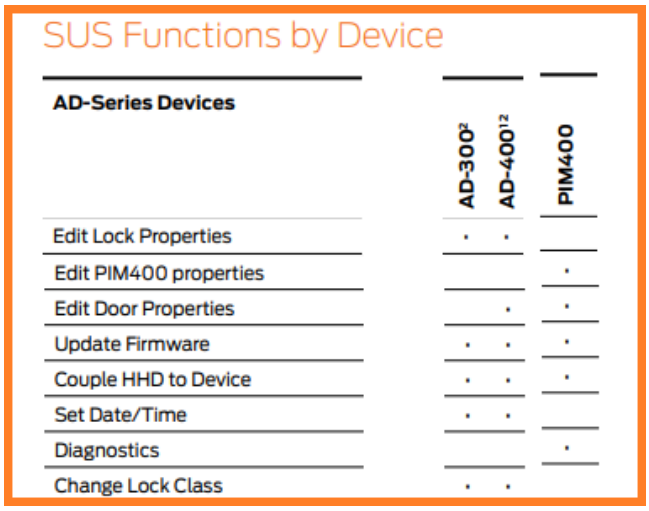
Emergency Opening

A mechanical key override is provided with All Schlage AD series locks. This can be used to mechanically open the door for emergency recovery or manual entry.
Note: The mechanical key override event may not be raised by the lock if the battery depletes to critical level.
This chapter covers the following topics:

- ***Schlage Device Setup and Configuration*** (on page 77-5)
- ***Configuring a Gallagher Controller for Schlage RS485 Devices*** (on page 77-11)
- ***Creating a Schlage PIM (Panel Interface Module)*** (on page 77-12)
- ***Creating a Schlage Door*** (on page 77-15)
- ***Assigning Devices*** (on page 77-20)
- ***Performing Overrides on a Schlage Door*** (on page 76-22)
- ***Configuring a Universal Card Format to support different Schlage Credential Formats*** (on page 77-23)
- ***Configuring PIN Only function on a Schlage AD Series Reader*** (on page 77-26)

Schlage Device Setup and Configuration

Setup and configuration of the Schlage PIM400 wireless gateway and AD30X/ AD40X locks can be performed using the Schlage Utility Software (SUS) application and portable Schlage Handheld Device (HHD).



SUS Functions by Device

AD-Series Devices	AD-300[2]	AD-400[1,2]	PIM400
Edit Lock Properties	•	•	
Edit PIM400 properties			•
Edit Door Properties		•	•
Update Firmware	•	•	•
Couple HHD to Device	•	•	•
Set Date/Time	•	•	
Diagnostics			•
Change Lock Class	•	•	

[1] The AD40X wireless lock properties may also be viewed or edited through the PIM400.

[2] These devices will become AD302 and AD402 when a FMK reader is attached to work with the FIPS201-2 standard.

For complete detailed instructions, refer to the document **Schlage Utility Software User Guide 104390.pdf** located in the `'Utilities\Schlage\Documentation'` directory of the Command Centre installation media.

The latest version of the document can be sourced from the Schlage website: Schlage Utility Software User Guide

Schlage Windows based Handheld Device (HHD) Setup Configuration

To begin using the Schlage Utility Software (SUS), perform the following steps:

1. Download and install Synchronisation Software (page 9)
2. Connect the HHD to your PC (page 13)
3. Configure the Synchronisation Software (page 10)
4. Update SUS (page 13)
5. Start SUS (page 15)
6. Connect the Handheld Device to a Lock or Non-Lock Device (page 20)

You can login to the Schlage Utility Software (SUS) as either a Manager or an Operator. The Manager role has access to all commands. The Operator role has access only to limited commands.

	Manager	Operator
Lock Properties	•	•
Program Lock	•	•
Firmware Update	•	
Change Lock Class	•	
Couple HHD to Device	•	
Set Date/Time	•	
Diagnostic Data Log	•	•
Door Properties	•	•
PIM properties	•	•
Diagnostics	•	
SUS Password	•	•
Coupling Password	•	
Language	•	•
Auto/Manual Update	•	•
List All/Pending Doors	•	•
USB/Serial Connection	•	•

The default SUS password for both the Manager and Operator is 123456. If the password is lost, you must reinstall SUS.

The process of connecting the HHD to a Schlage device is called Coupling. Coupling to each Schlage Hardware device is required to configure and pair Schlage devices to one another. Coupling can only be performed by Managers. The default coupling password is 123456.

Important: It is important to record and store the coupling password in a safe place for future use.

Connecting Handheld Device to AD Series Lock

The HHD will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. If a device is not in Coupling mode, SUS will display a device specific message with instructions for placing the device into Coupling mode.

AD30X and AD40X coupling to device and upgrading firmware:

1. Connect the HHD to the lock using the HH-USB cable.
2. Open the Schlage Utility Software.



3. Log in as Manager using password.



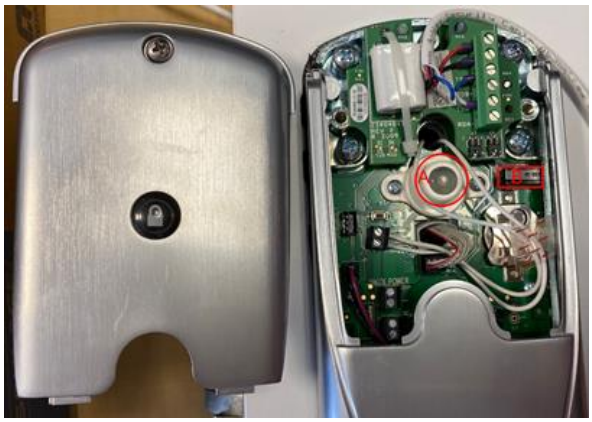
4. Click the bottom right button to change the connection type to USB.



5. Press the **Schlage** button on the lock twice. The lock displays on the screen.



6. On the HHD, select **Device Options**.
7. Remove the top cover of the lock (not the reader).



8. While pressing and holding the **Privacy** button (A), press and release the **Tamper** switch (B) three times.
9. Release the **Privacy** button. The LED of the **Privacy** button will illuminate.
10. On the HHD, select **Couple HHD to Device**.



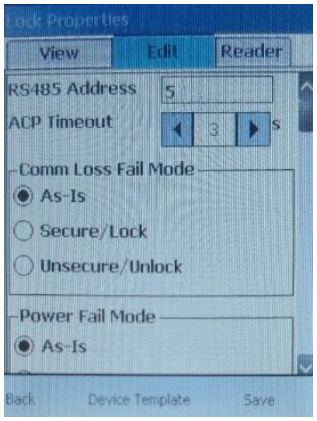
11. When Coupling is successful, a message will be displayed on the screen.

It is important to update the lock firmware to the latest version available. The AD series lock firmware Gallagher has tested is 2.50.1 for AD300/AD400 and 2.2.1 for AD302/AD402. A copy of this firmware is located at `'Utilities\Schlage\AD Firmware\AD.A.130'`.

To upgrade the firmware of the AD30X and AD40X locks, please refer to the procedure in the "Device Firmware Update" section of the *Schlage Utility Software User Guide.*

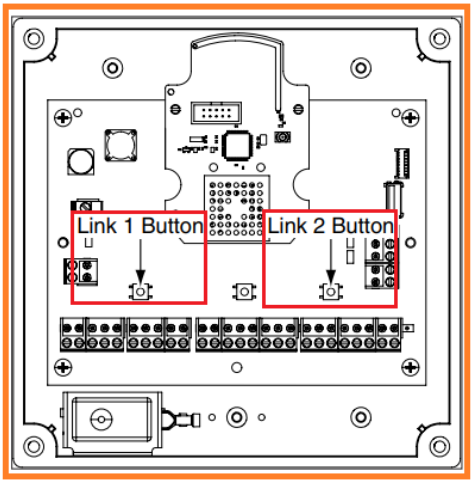
AD30X configuring RS485 address:

After connecting the HHD to device as above steps 1-5 on the HHD, select **Lock Properties** > **Edit** tab and set **RS485 Address** field to a value in the range of 0 - 254 (except 170). Different addresses should be used for devices connected to the same RS485 port on the controller.



Connecting Handheld Device to PIM400

1. Remove the PIM400 cover.
2. The HHD must be in USB mode.
3. Connect the HHD to the PIM400 using the HH-USB cable.
   The PIM400 will be displayed on the HHD screen.
4. On the HHD, select **Device Options**.
5. On the PIM400, press and hold the **LINK 1** button. Then press the **LINK 2** button three times.



6. On the HHD, select **Couple HHD to Device**.
7. When Coupling is successful, a message will be displayed on the HHD screen.
8. Click Device Options/PIM Properties/Edit tab.
9. On the PIM Properties Edit page configure:
   a) ***RS485 Address***
   Note: This can be a value in the range from 0 - 254, except 170.
   b) Low Door, and
   c) ***High Door*** then click **Save**.
   Note: Settings being set should be the same settings to set when configuring Schlage PIM and Door.



In the example shown, the PIM400 is set to RS485 address 1 with 2 doors attached at address locations 0 and 1.

Coupling an AD40X with a PIM400

1. Click on the **Link** tab, and set the door number and click **Link**.



2. Open Schlage AD40X back door handle and press "**#**" once then "**SCHLAGE**" button twice. Keep the Schlage back door handle open until the "SCHLAGE" LED blink in **GREEN**.
3. Wait for 6 **BEEP** response on the Schlage door sensor or the SUS link page finished the linking. The door is linked to the PIM now.

Finishing configuration

After configuration of the PIM and lock is finished, go back to the SUS Main screen, navigate to **SUS options** > **Connection Type** and change the connection type back to serial.

It is important to update the PIM400 firmware to the latest version available. The PIM400 firmware Gallagher has tested is 2.30.1. A copy of this firmware is located at `'Utilities\Schlage\AD Firmware\AD.A.130'`.

To upgrade the firmware of the PIM400, please refer to the procedure in the "Device Firmware Update" section of the *Schlage Utility Software User Guide.*

It is now possible to configure the Schlage PIM400 and Schlage AD series Hardware from within Command Centre.

From in Command Centre, set the values for **RS485 Address**, **Low Door** and **High Door** to align with the Schlage PIM400 configuration.

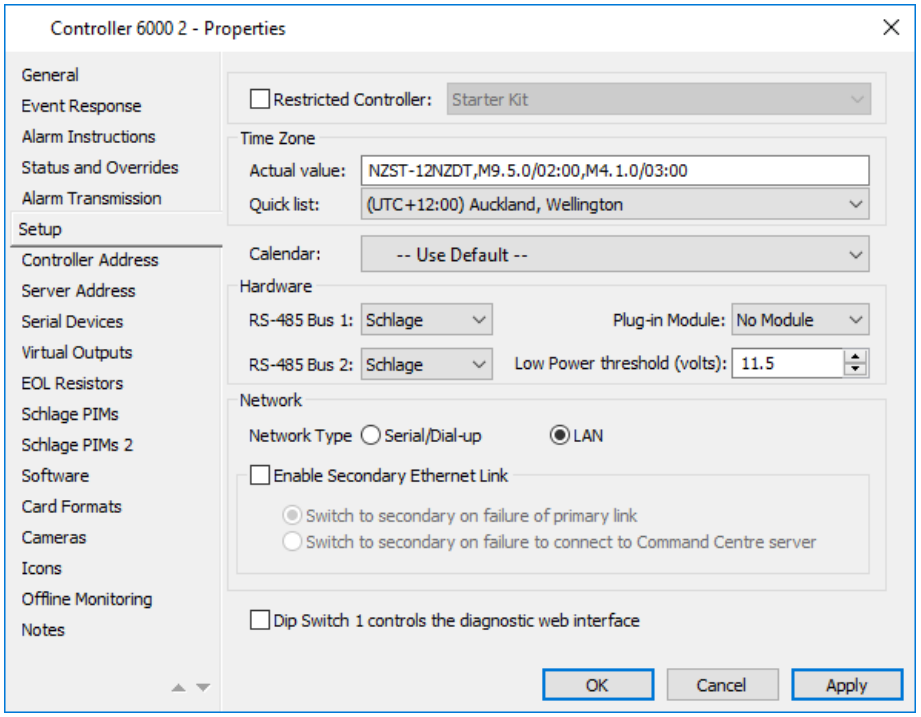
Configuring a Gallagher Controller for Schlage RS485 Devices

Introduction

This procedure describes how to configure a Gallagher Controller for Schlage devices.
Note: AD30X locks and PIMs (AD40X) can be used on the same bus.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Controller you want to assign the new Schlage devices to.
3. **Right click** and select **Properties.**
   By default the **General** tab displays.
4. Click the **Setup** tab.



In the Hardware section of this screen, select the 'Schlage' option from the appropriate drop-down list, (i.e. **RS-485 Bus 1** or **RS-485 Bus 2**).
Depending on which RS-485 Bus option you selected 'Schlage' for, a **Schlage PIMs 1** or **Schlage PIMs 2** tab appears, allowing you to add up to 16 Schlage Doors to the Bus port on this Controller.

5. 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.

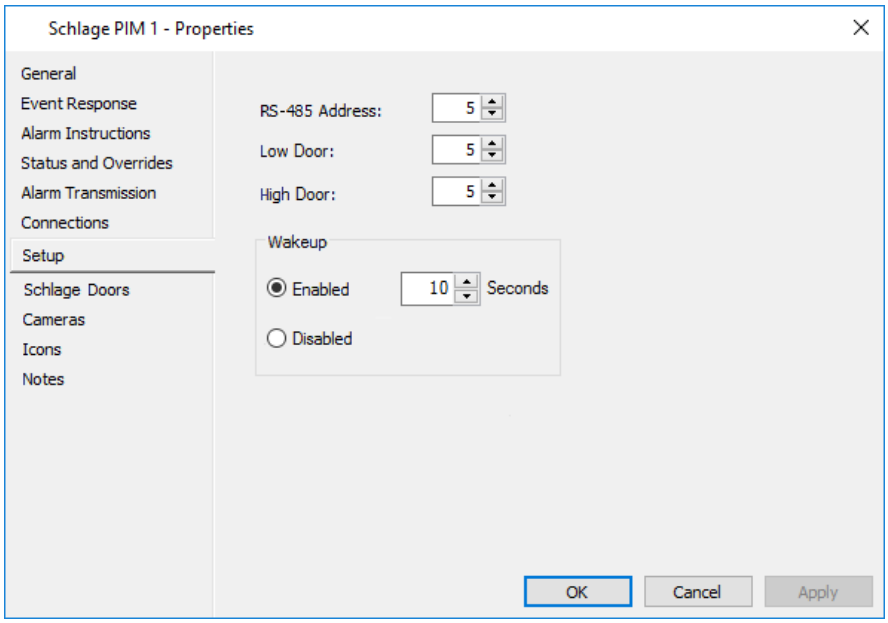
Creating a Schlage PIM (Panel Interface Module)

Introduction

This procedure describes how to create a Schlage PIM (Panel Interface Module) in Gallagher Command Centre.

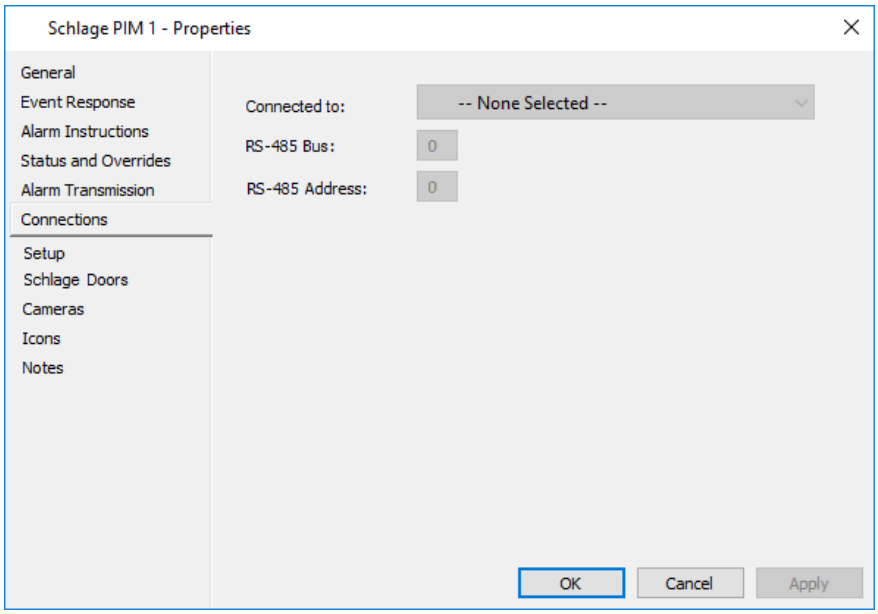
Note: AD30X locks should be assigned to a PIM in Command Centre although an AD30X lock is not physically connected/wired to a PIM400 (one AD30X lock per PIM), and the RS-485 Address, Low Door and High Door fields on the Setup Page of the PIM properties should always use the same value as the RS485 Address configured on SUS > Lock Properties > Edit screen in the HHD.

For example, when the RS485 Address of a AD30X lock is set to 5 in the HHD, the Setup page of the Schlage PIM to which the lock, (i.e. the corresponding Schlage Door) is assigned would look like something below.



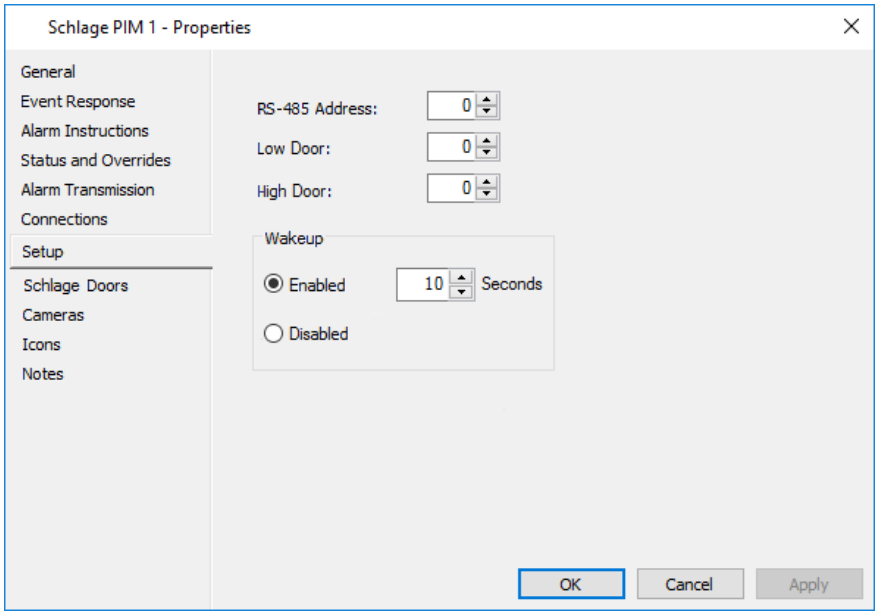
Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Schlage Devices**>**Schlage PIM.**
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
5. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
6. Click the **Connections** tab.



The three fields, (i.e. **Connected to**, **RS-485 Bus** and **RS-485 Address**) will be populated once you assign this Schlage PIM to a Controller 6000 or 7000, which is explained later in ***Assigning Devices*** (on page 77-20).

7. Click the **Setup** tab.



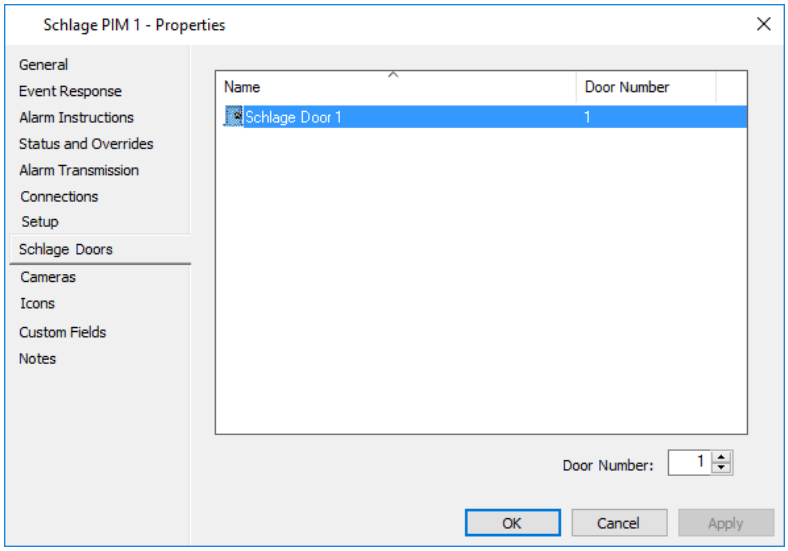
8. Configure these fields as appropriate.

Field	Description
RS-485 Address	Each Schlage PIM must have it's own RS-485 address.
Low Door	This is the lowest RS-485 address.
High Door	This is the highest RS-485 address. It must be higher than the **Low Door** value, but no more than 16 higher than the **Low Door** value.

Field	Description
Wakeup	If you want to use the Free/Secure mode leave the **Enabled** option selected and apply the appropriate number of seconds (Range = 1 - 10). **Note:** Applying 0 seconds will automatically select the **Disabled** radio button and the Seconds box will become disabled.

Note: Where there are two (or more) PIMs configured on one BUS, the Low Door - High Door ranges on those PIMs cannot overlap, (i.e. those doors cannot share RS-485 addresses). For the first PIM (say for 16 doors), set the range as 1-16, for the second PIM use 17-32. This restriction does not apply where PIMs are not sharing a BUS.

9. Click the **Schlage Doors** tab.



This screen allows Schlage Doors to be associated with the Schlage PIM. See ***Assigning Devices*** (on page 77-20) for the procedure.

10. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Schlage PIM.
    For further details see ***Cameras tab*** (on page 3-24).
11. Click the **Icons** tab if you want to change the Icon Set for this Schlage PIM. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
12. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Schlage PIM.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
13. Click the **Notes** tab if you want to add a note(s) about this Schlage PIM. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
14. 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.

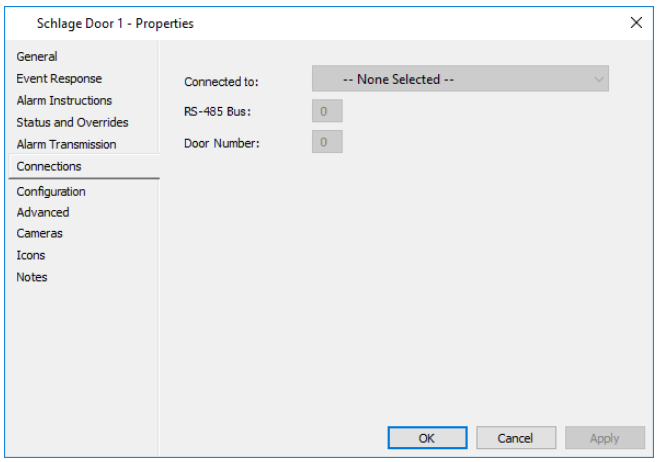
Creating a Schlage Door in Command Centre

Introduction

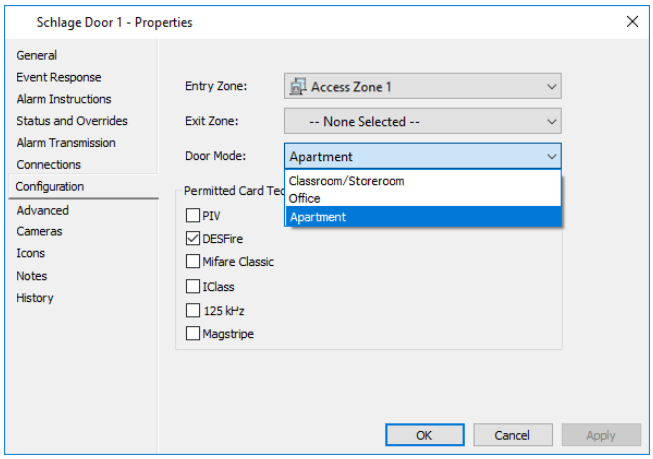
This procedure describes how to create a Schlage Door in Gallagher Command Centre.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Schlage Devices** > **Schlage Door.**
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
5. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
6. Click the **Connections** tab.



   The three fields, (i.e. **Connected to**, **RS-485 Bus** and **Device Number**) will be populated once you assign this door to a Schlage PIM, which is explained later in ***Assigning Devices*** (on page 77-20).
7. Click the **Configuration** tab.

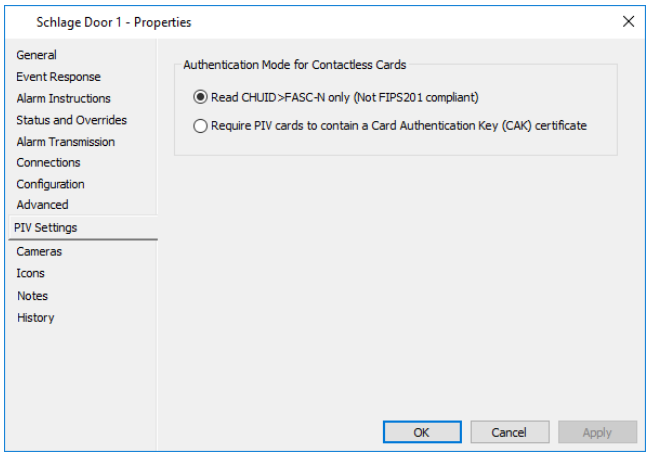


8. Select the appropriate entry and exit zones for this door from the **Entry Zone** and **Exit Zone** drop-down lists.
   Note: Exit Zones always show the puzzle icon if they are only assigned to Schlage Doors.
9. Click the **Door Mode** field and select the appropriate mode from the drop-down, (i.e. "Classroom/Storeroom", "Office" or "Apartment").
   Important: These door modes are supported on AD devices from v8.80. To make sure this feature works correctly:
   1. Update Command Centre to vEL8.80 or later.
   2. Update the Controller software to the latest version.
   3. Once all updates are complete, right-click on the AD Lock and click **Push Configuration**.
   4. Right-click on the Alarm Zone and click **Push Configuration**.

Door Mode	Explanation
Classroom/ Storeroom	The door access is totally controlled by the Entry Access Zone. It works the same way as normal Gallagher doors. Pressing the IPB (Inside Push Button) indicates the door secure/free mode as follows: - Red LED flash = door locked (secure) - Green LED flash = door unlocked (free) "Classroom/Storeroom" door mode is the default setting after door set up.
Office	Without the IPB (Inside Push Button) function, "Office" mode functions the same way as "Classroom/Storeroom" mode. Pressing the IPB button changes the lock status to the opposite state of the access zone schedule. Pressing the IPB button again brings the AD lock back to access zone schedule status. Once the door goes back to access zone schedule status, the next IPB change will be counted as the 'First' IPB state change. During the IPB state time, if access zone schedule changes or /override/lockdown applied, will change the AD lock status. The IPB button LED should show lock/unlock state of the door for each IPB pressing: - 1 green flash = in IPB state and door unlocked - 1 red flash = in IPB state and door locked - 2 green flashes = back to access zone and door unlocked - 2 red flashes = back to access zone and door locked
Apartment	The door does not follow an Access Zone Schedule. Its lock/ unlock behaviour is controlled by the end user, i.e. pressing the IPB (Inside Push Button) or badging a valid card toggles the door access between lock and unlock. Pushing inside handle to request to exit puts the door to unlock. "Apartment" door mode supports the Access Zone lockdown feature. **Note:** The door will not return to lockdown state automatically when the door is unlocked via the inside handle/IPB button, you

Door Mode	Explanation
	will need to press the IPB button to re-secure the door. There are other Access Zone features that are not supported in this mode, (e.g. Access Zone Schedule, Access Zone normal overrides, double card overrides, PIN, Dual Authorisation are not supported). The Apartment mode LED patterns are: **Inside IPB LED:** Any door inside behaviours (press IPB button or press inside handle to exit) will cause the IPB LED flash, showing the result secure state: - 1 green flash = door unlocked (free) - 1 red flash = door locked (secure) **Outside Schlage LED:** Badge card outside of the door will cause the Schlage LED flashing, showing result secure state and card valid or not: - 1 red flash = badge valid card, and the door is changed to locked (secure) when door in closed. - 2 green flashes = badge valid card, and the door is unlocked (free) or locked but door is open. - 2 red flashes = badge invalid card

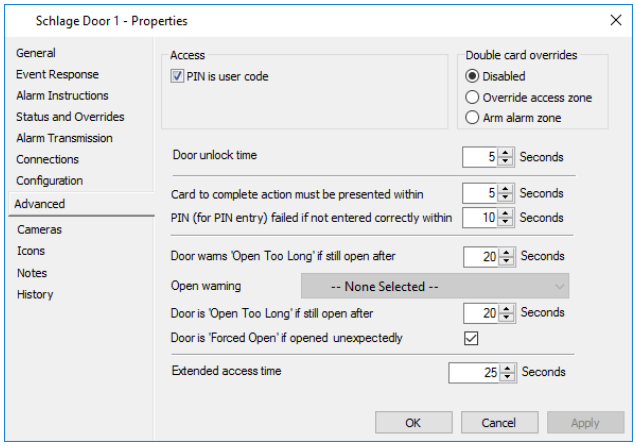
10. Select the appropriate checkboxes in the Permitted Card Technology section to indicate what types of cards will be accepted at the door. **Notes:**
    - Selecting **MIFARE Classic**, **125 kHz** or **Magstripe** technologies result in the following warning message: *"Some of the card technology options selected have known security vulnerabilities."*
    - For AD-400 and AD-402 devices, card technology and PIV authentication mode changes may need 1-2 door heartbeat time to take effect.
11. Did you select the **PIV** checkbox?
    If **no**, go to the **Advanced** tab.
    If **yes**, then an additional **PIV Settings** tab will display.
    Note: Only AD302 and AD402 locks can be configured to use PIV cards, and PIV support requires a Gallagher PIV Controller 6000 or 7000.



12. Select the appropriate Authentication Mode by clicking the relevant radio button. **Notes:**
    - Only one authentication mode can be selected.

- PIV Authentication mode is only valid when using PIV Contactless cards.
- For AD-400 and AD-402 devices, card technology and PIV authentication mode changes may need 1-2 door heartbeat time to take effect.

13. Click the **Advanced** tab.



The settings on this screen enable alarms to trigger.

14. Check the **PIN is user code** checkbox if required.
With **PIN is user code** checked, the user code will be required in place of a PIN for any transactions at the reader which would normally require a PIN. This includes door access and overrides.
Note: The following settings do not work in **PIN is user code** mode:
    - *Double-card overrides*. Therefore, if you do select **PIN is user code** mode, leave the Double card overrides as **Disabled**.
    - *"Apartment" Door Mode*. If "Apartment" has been selected (on the **Configuration** tab) and you select **PIN is user code**, the following warning message will display:
    "Schlage doors in the apartment mode do not support User code or PIN."
15. If you want the double-card override feature to be available, 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.
Notes:
    - Access Group Privileges are required for the overrides to work.
    - If "Apartment" door mode has been selected (on the **Configuration** tab), and you select either of the **Double card overrides**, the following warning message will display: *"Schlage doors in the apartment mode do not support double card overrides."*
16. Configure the Schlage Door timeouts as required.

Option	This setting determines...
Door unlock time	the maximum time the Unlock relay is energised. (Default = 5 seconds. Valid range is 1 - 255 seconds)
Card to complete action must be presented within	the maximum time between two card badges. (Default = 5 seconds. Valid range is 1 - 99 seconds)

Option	This setting determines...
PIN (for PIN entry) failed if not entered correctly within	either: - the maximum time between badging a card and starting to enter a PIN at the reader for access through a door in PINs mode, **OR** - overriding an Access Zone or Alarm Zone in PINs mode. (Default = 10 seconds. Valid range is 1 - 99 seconds)
Door warns 'Open Too Long' if still open after	when the open warning output turns on and when the status of the door changes to show that it has been open too long. (Default = 20 seconds. Valid range is 0 - 9999 seconds) **Note:** This cannot be set as greater than the alarm time, (i.e. the **Door is 'Open Too Long' time**). If it is, and you attempt to save the door, the following error message displays: *"The 'Open Too Long' warning time must be less than or equal to the 'Open Too Long' alarm time."*
Open warning	the Output to activate when the door has been open too long.
Door is 'Open Too Long' if still open after	when a 'Door Open Too Long' alarm is generated. (Default = 20 seconds. Valid range is 5 - 9999 seconds)
Door is 'Forced Open' if opened unexpectedly	whether an alarm will be generated. When checked, a 'Forced Door' alarm will be generated if the open sensor detects the door is opened. **Note:** Unchecking this will result in no 'Forced Door' alarms being generated, therefore it is recommended you leave it checked.
Extended access time	the maximum time the door is to unlock for. (Default = 25 seconds. Valid range is 0 - 255 seconds) **Note:** The **Extended access time** affects the times used for all of the following: - Door unlock time - Door Open Too Long Warning - Door Open Too Long Alarm

17. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Schlage Door. For further details see ***Cameras tab*** (on page 3-24).
18. Click the **Icons** tab if you want to change the Icon Set for this Schlage Door. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
19. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Schlage Door. For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
20. Click the **Notes** tab if you want to add a note(s) about this Schlage Door. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
21. 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 Devices

Introduction

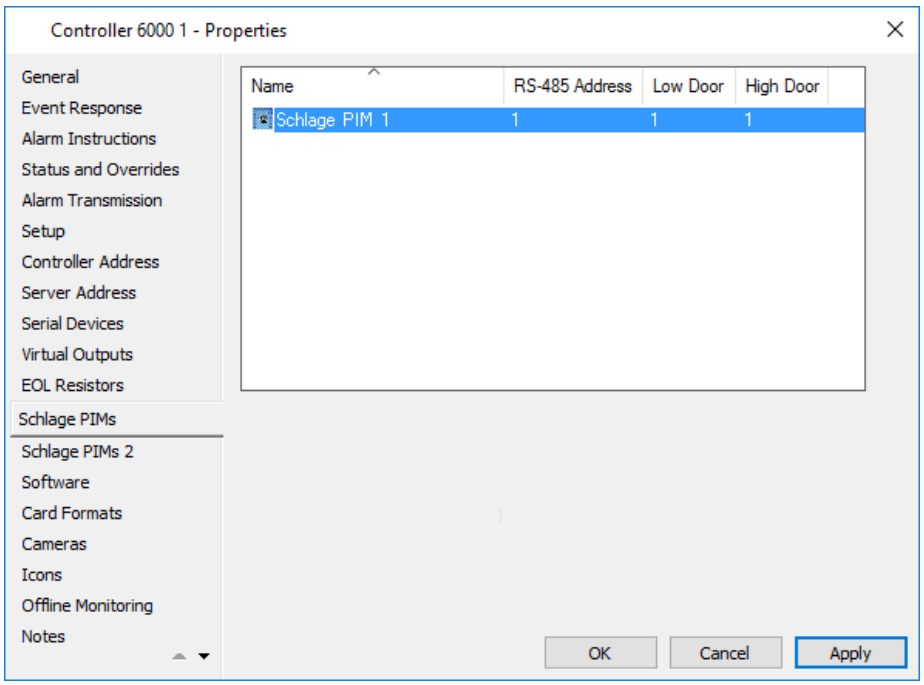
This procedure is split into two parts to describe how to assign Schlage devices, as follows:

- Assigning Schlage PIM's (Panel Interface Modules) to a Gallagher Controller
- Assigning Schlage Doors to Schlage PIM's

Procedure

Assigning Schlage PIMs to a Gallagher Controller

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Controller you want to assign the Schlage PIM to.
   Note: The Gallagher Controller should already be configured for Schlage devices. See ***Configuring a Gallagher Controller for Schlage RS485 Devices*** (on page 77-10) for the procedure.
3. **Right click** and select **Properties.**
   By default the **General** tab displays.
4. Click the **Schlage PIMs** tab.



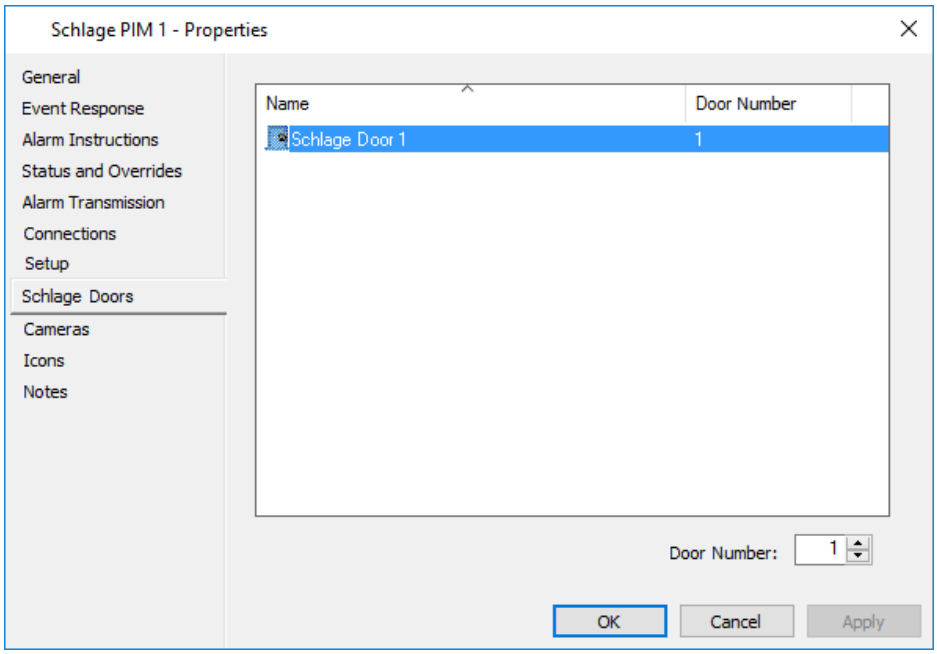
5. From the **Hardware** List Window, select the Schlage PIMs attached to this Bus. Drag and drop each Schlage PIM into the grid on the **Schlage PIMs** tab.

   Each of the columns, (i.e. **RS-485 Address**, **Low Door** and **High Door**) are populated according to configuration on the **Setup** tab of the Schlage PIM.

6. 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 Schlage Doors to Schlage PIM's

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Schlage PIM you want to assign a Schlage Door(s) to.
3. **Right click** and select **Properties.**
   By default the **General** tab displays.
4. Click the **Schlage Doors** tab.



This screen allows Schlage Doors to be associated with the Schlage PIM.
For AD30X, the door number needs to be the same as the RS485 address of the lock. You can only add one AD30X lock per PIM (no physical PIM required).
For AD40X, the door number needs to be the same as the number configured in ***Coupling an AD40X with a PIM400*** (on page 77-9).

5. Open the **Hardware** List Window, and drag and drop the Schlage Door(s) required onto this screen, and click **Apply**.
6. Enter the **Door Number** for each Door, by selecting the appropriate Door from the grid and entering the address into the **Door Number** field.
   (Range = 1 - 16 depending on the Low and High Door range)
7. 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.

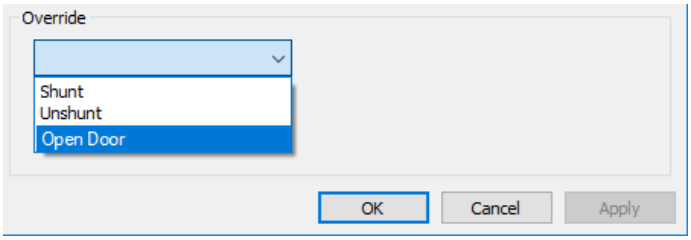
Performing Overrides on a Schlage Door

Introduction

This procedure describes how to temporarily override the status of a Schlage Door.

Procedure

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



3. Select the type of override you want to perform from the **Override** drop-down list.

Option	Function
Shunt	Stops communication to the device (door).
Unshunt	Restarts communication to the device (door).
Open Door	Unlocks the door momentarily allowing a person to pass through.

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

Configuring a Universal Card Format to support different Schlage Credential Formats

Introduction

Schlage credentials can be in different Wiegand formats, (i.e. 26A, 32X, 35X, 35C, 36X, 37H, 37X, 40X and 48X), of which some may not be supported by default, (e.g. the standard 26A format works, however 37H format does not unless a Universal Card Format is configured in Command Centre). A Schlage Credential Formats document can be obtained from Allegion on request, and you should contact Allegion if you intend using any credentials other than the standard 26A format.

The default Schlage 26A format contains a total of 26 bits. The 8-bit facility code of this format will be randomly generated with the badge ID.

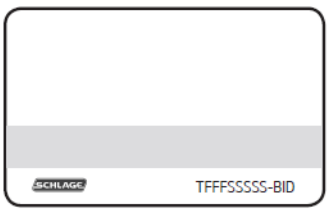
Bit formats	Facility Code Range	Number Range	Prox	Smart
26A (125 kHz Standard)	0-255	0-65,535	Y	Y
32X	N/A	0-1,073,741,823	Y	Y
34N	0-255	0-65,535	Y	Y
34S	0-4,095	0-1,048,575	Y	Y
35C *	0-4,095	0-1,048,575	Y	Y
36X	0-4,095	0-2,097,151	Y	Y
37H	Not Applicable	0-34,359,738,367	Y	Y
37X	0-65,535	0-524,288	Y	Y
40X * (13.56 MHz Standard)	0-1,023	0-268,435,455	N	Y
48X	0 – 1,048,575	0-1,048,575	N	Y

Additional credential detail can be found in the ***Schlage Credential Formats-200624*** documentation located in the `'Utilities\Schlage\Documentation'` directory.

Schlage MIFARE Classic 26A standard card data will be encoded on sector 1, while Schlage Mifare DESFire EV1 to EV3 card data will be encoded using AppID F532F0. Other Command Centre encoded card data, (i.e. Morpho) should be co-located around the fixed Schlage data.

Schlage Card Identification

The Schlage encoded card format and badge ID can be identified by applying the following key to the text printed on the credential (ISO card shown).



KEY	
T	Technology
P	Proximity
S	Smart
C	Combo/Multi
FFF	Format Number (Fixed)
SSSSS	Order Number (Fixed)
BID	Badge ID Number
PN	Existing Printed PN from Supplier

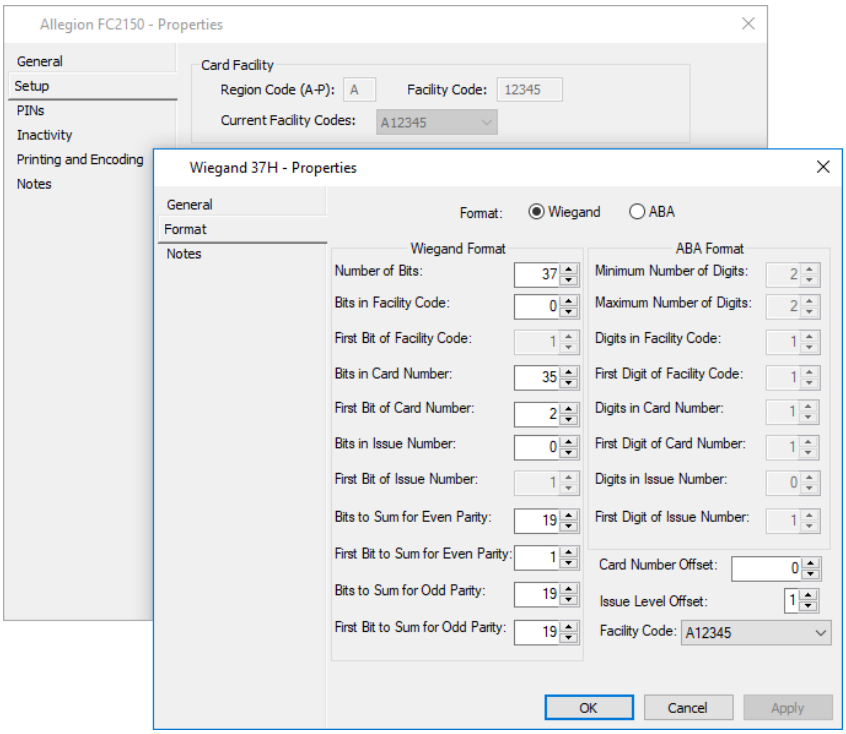
Should the site inherent Schlage encoded cards that fall outside of the standard 26A format, then Command Centre will look for the card format configuration

found within the Universal Card Format (UCF) configurator. A UCF format will need to be created to suit.

This procedure describes how to configure a new Card Type and a Universal Card Format to support the 37H format.

Procedure

1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. **Right click** and select **New...Card Type.**
   By default the **General** tab displays.
3. Enter a Name and Description, and select the division for this Card Type.
4. Configure the remaining tabs as required, and click the **OK** button.
5. **Configure** from the menu bar, then **Universal Card Format**.
   The **Universal Card Format** List Window opens.
6. **Right click** and select **New...Universal Card Format**.
7. Enter a Name and Description, and select the division for this Universal Card Format.
8. Click the **Format** tab.
9. Select the **Wiegand** radio button to indicate the required format.



10. Change the parameters to describe the data on the cards to be supported as follows:
    Number of Bits = 37
    Bits in Facility Code = 0
    Bits in Card Number = 35
    First Bit of Card Number = 2
    Bits to Sum for Even Party = 19

Bits to Sum for Odd Party = 19
First Bit to Sum for Odd Parity = 19

11. Select the **Facility Code** on the Card Type you created that will be used when you create Schlage credentials later.
12. Click the **OK** button.
13. Assign the new Universal Card Format to the Controller's **Card Formats** property page.

For further information about Universal Card Formats, refer to ***Chapter 26: Universal Card Format***.

How to read Schlage card details and create a cardholder

1. Connect the MT20 Allegion card reader to the PC, and open a notepad++ or similar application.

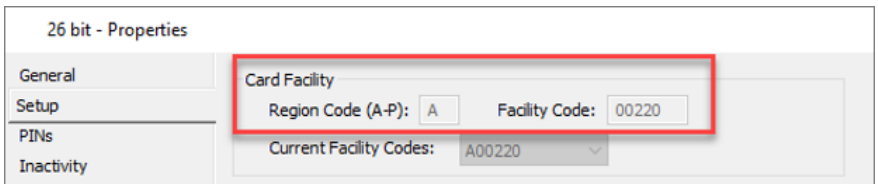


2. Badge a Schlage card.
3. Check the information on the card, it basically contains the following details:

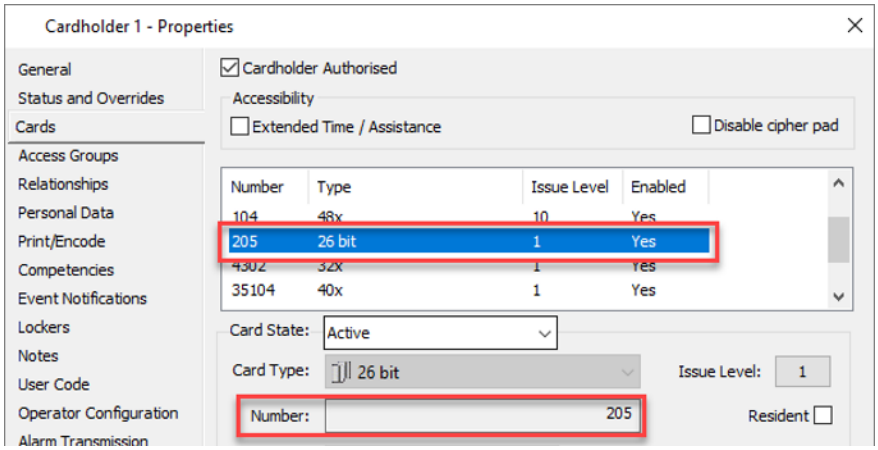
   For example: UCF 26-Bit Standard(26A) format, once the card is badged, the card information displays as follows:
   EE006680;26A;220;205;

	Engage Card format	**Facility Code**	**Card number**
EE006680	26A	220	205

4. Create a card type by using the above information.



5. Create a cardholder with this correct card type and card number.



6. Badge the card at an Allegion door and check the correct cardholder has gained access to door lock.

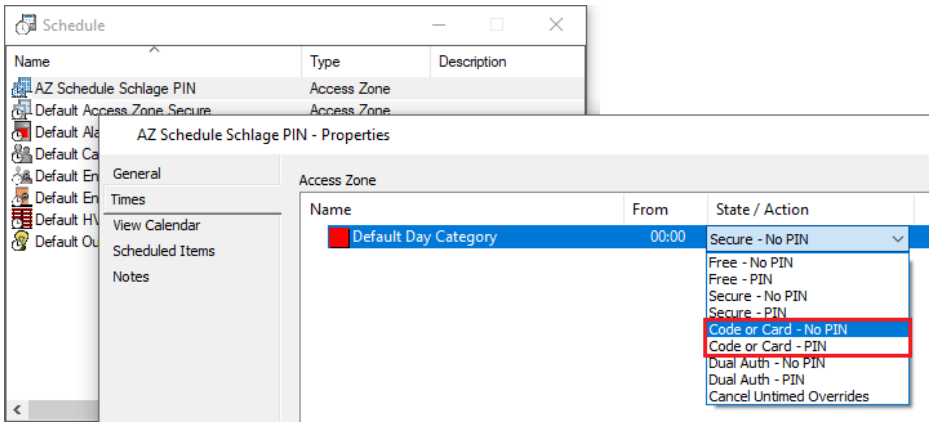
Configuring PIN Only function on a Schlage AD Series Reader

Introduction

This procedure describes how to configure the "PIN only" function on a Schlage AD Series Reader.

Procedure

1. Click **Configure** from the menu bar, then **Schedules**.
   The **Schedule** List Window opens.
2. Highlight the Access Zone Schedule to be assigned.
3. Click the **Times** tab.



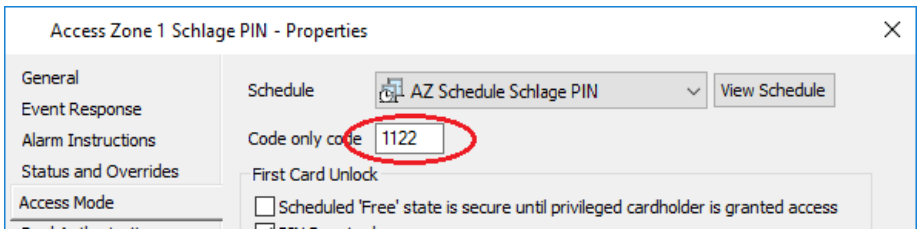
4. Click on the **State/Action**, and select either the "Code or Card - No PIN" or "Code or Card - PIN" option from the drop-down list.
5. Click the **OK** button.
6. To complete configuration, use one of the methods below as appropriate for your site:

Method	Description
By Access Zone	This method configures one code that can be shared by anyone who wants to gain access to the system. The disadvantage of this is that there is no way to track who used the code.
By Cardholder	This method uses unique codes assigned to Cardholders, so the system can identify who gained access.

By Access Zone

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens.
2. Highlight the Access Zone to be configured.
3. **Right click** and select **Properties**.
4. Click the **Access Mode** tab.
5. From the **Schedule** drop-down list, select the appropriate Schedule.

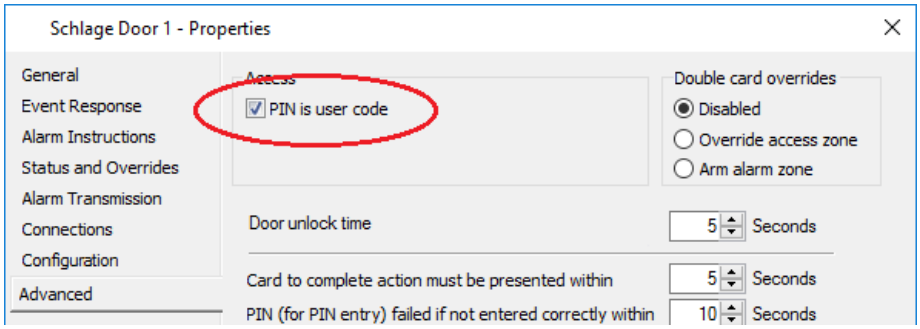
6. Enter a user code in the **Code only code** field.
   The example below shows 1122 has been entered as the code.



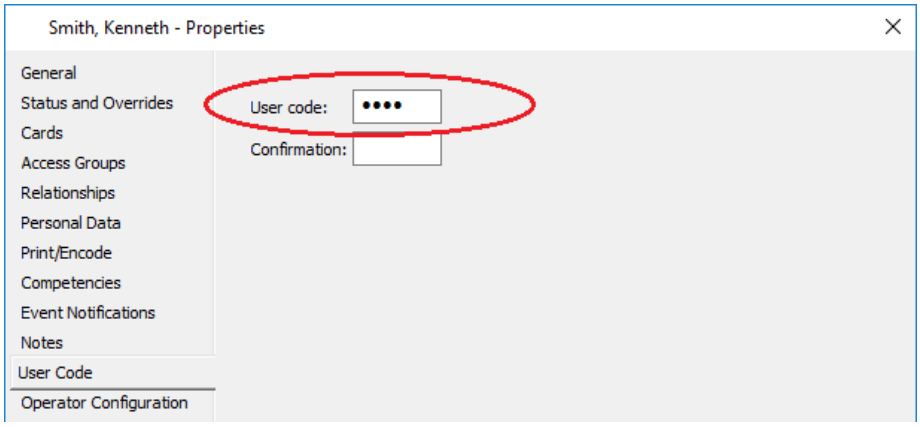
7. Click the **OK** button.

By Cardholder

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
2. Highlight the Schlage Door you want to configure the "PIN only" function for.
3. **Right click** and select **Properties**.
4. Click the **Advanced** tab.



5. Check the **PIN is user code** checkbox, and click the **OK** button.
6. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
7. Highlight a Cardholder that requires access via the Schlage Reader.
8. **Right click** and select **Properties**.
9. Click the **User Code** tab.



10. Enter a 4-6 digit user code in the **User code** field.
11. Confirm the user code by re-typing it in the **Confirmation** field.
12. Click the **OK** button.
13. Repeat Steps 7 - 12 for each Cardholder that requires access at the Reader.

Chapter 78: Allegion Engage Interface

Introduction

The Allegion Engage Interface is a licensed feature of Gallagher Command Centre. This feature supports the following Schlage wireless locks offered by Allegion:

- LE and LE-B locks
- NDE and NDE-B locks
- Control locks

Notes:

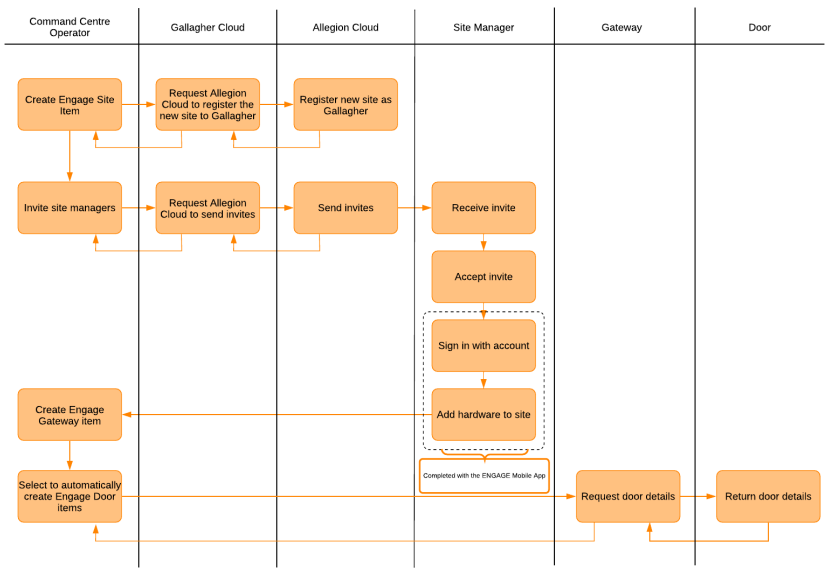
- Engage readers do NOT support Gallagher Mobile Credentials.
- While Engage Gateways, Doors and Card Types are all created in the Command Centre Configuration Client, Engage Scheduling is configured in Command Centre Client. See *"Allegion Engage Interface"* in the Command Centre Client Help file for further detail.
- A maximum of 8 Engage Gateways are supported per controller.
- A maximum of 80 locks are supported by a Controller.
- A maximum of 10 locks are supported by an Engage Gateway.
- The Engage Gateway cannot be pinged as it will not handshake.

Gallagher encoded cards are not supported with this integration, you will need to use a Schlage encoded card. You can add a Gallagher DESFire object to the Schlage DESFire card to use these cards for both ENGAGE door locks and Gallagher readers. For further information see **Encoding Gallagher Credentials to an Engage Card** (on page 78-30).

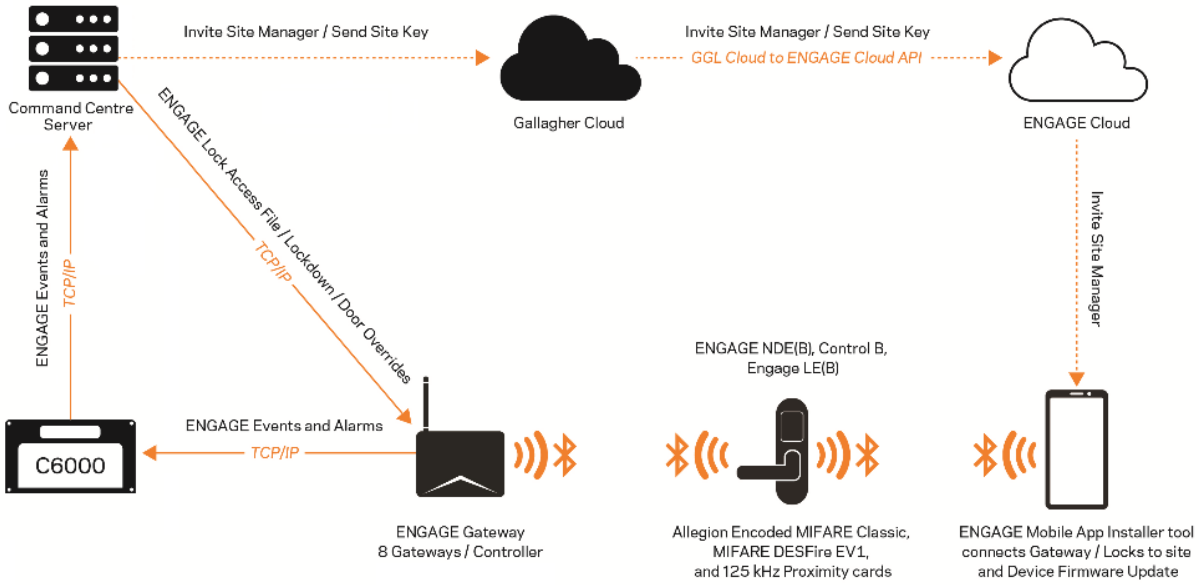
For further information about door/lock functionality, see ***Engage Doors/ Locks*** (on page 78-14).

Process Overview to setup an Allegion Engage site

This topic is separated into several individual procedures that make up the process for setting up an Allegion Engage site. The procedures are performed in either Command Centre Configuration Client or the Allegion Engage™ Mobile App.



Engage Site architecture diagram



Licensing

Allegion Engage is a licensable feature which requires one of the following license files with a unique license serial number for the Cloud:

2A08903 Engage License with hardware (per Door)
2A08904 Engage License without hardware (per Door)

The License file must contain the following option:

`[Limits]`
`ENGAGE Doors=x` (where `x` is the number of Engage Doors required)

Operator Privileges

The minimal operator privileges required for Allegion ENGAGE are:

- "Launch Configuration Client"
- "Edit Site"
- "Configure Site" (for editing the Card Type)
- "Override"

Select the item below that you require further detail on:

- ***Creating an Engage Site in Gallagher Configuration Client*** (on page 78-3)
- ***Allegion Engage configuration*** (on page 78-8)
- ***Command Centre configuration*** (on page 78-19)

Creating an Engage Site in Gallagher Configuration Client

Introduction

This procedure details how to create an Engage Site and add site managers to the site.

Notes:

- Engage Site Managers can delegate access using the Allegion Engage™ Mobile App to Allegion Engage™ Mobile App Operators. Operators can run diagnostics, perform firmware updates, and link and unlink devices to Gateways.
- An Engage Site cannot be deleted while there are Gateways or Site Managers still attached to the site.

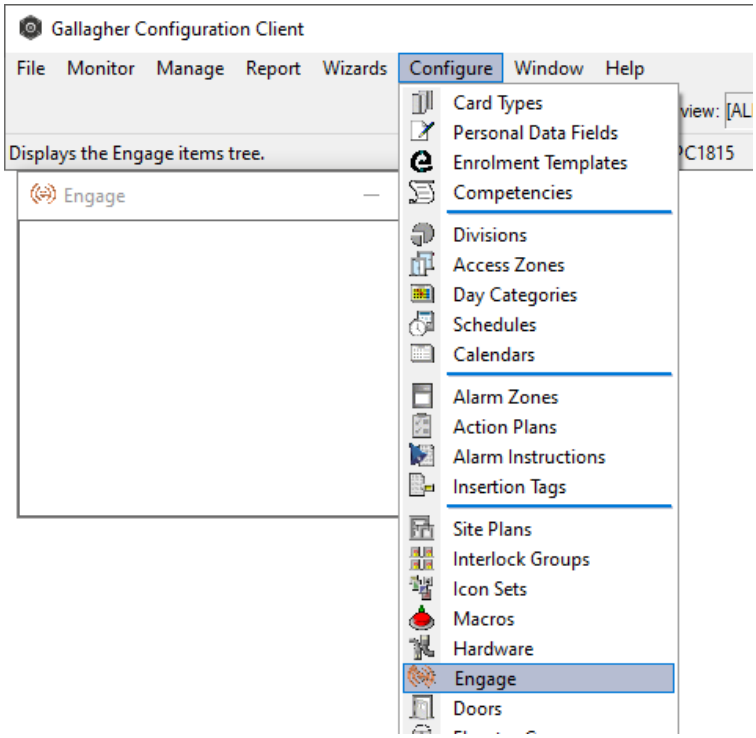
Prerequisites

Prior to creating an Engage Site, a Command Centre Cloud item needs to be created first. See ***Connecting to the Cloud*** (on page 31-3) for the procedure.

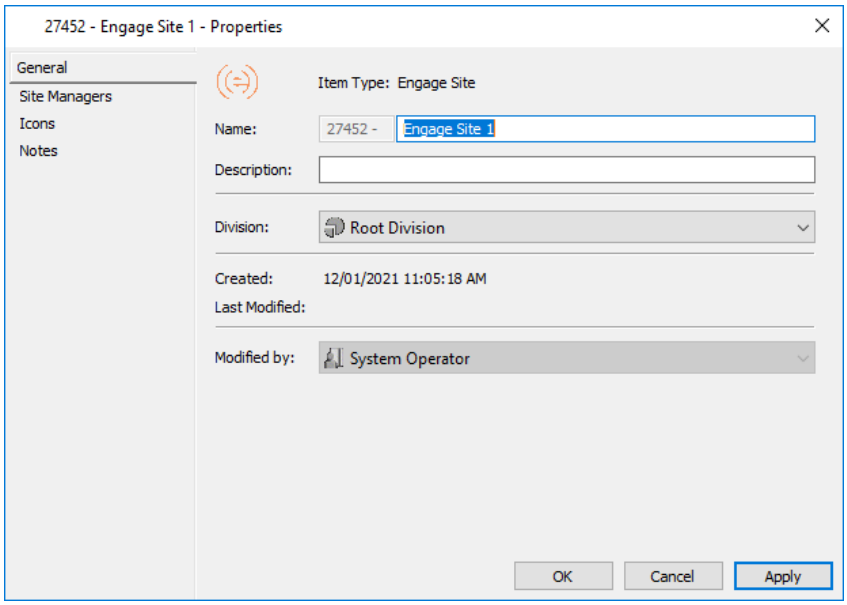
Configuration

To configure an Engage Site, perform the following procedure in Gallagher Configuration Client:

1. Click **Configure** from the menu bar, then **Engage**.
   The Engage List Window opens.

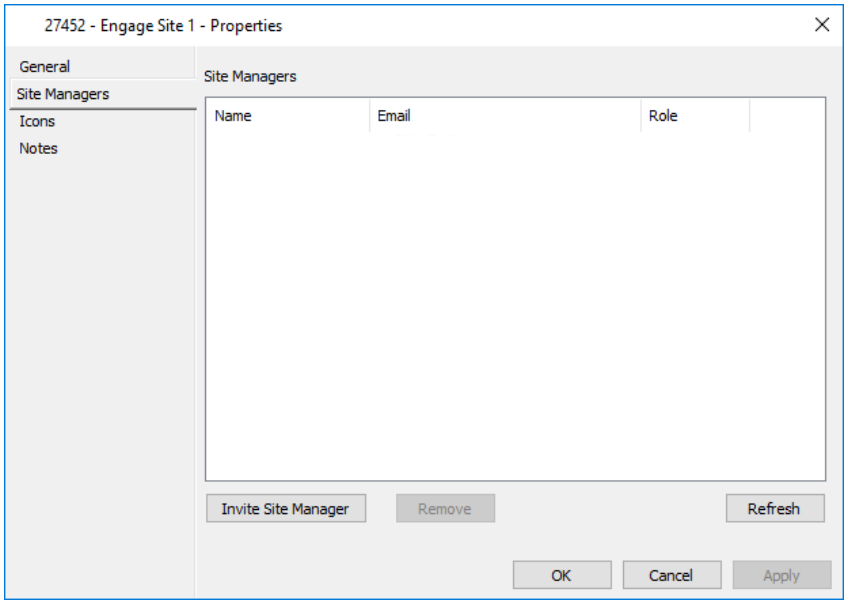


2. **Right click** and select **New...Engage Site**.
   By default the **General** tab displays.

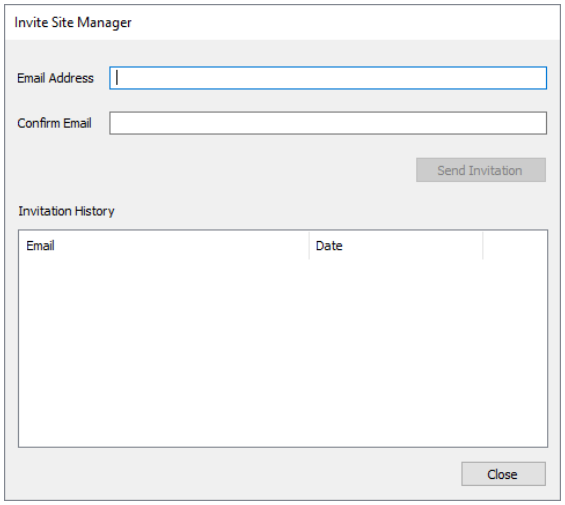


Note: The Engage Site Name is prefixed with the unique server serial number (from the license file).

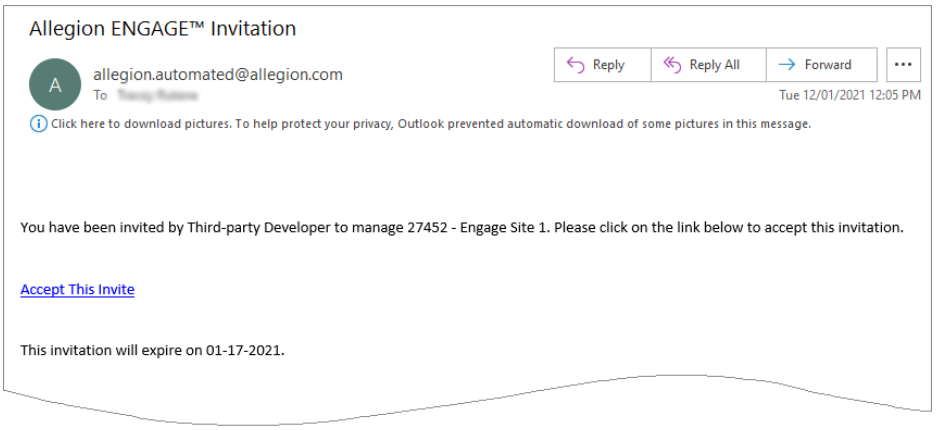
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Apply** button.
   Notes:
   - If you did not create a Command Centre Cloud item prior to starting this procedure, the following error message will display:
     "The operation failed. Please ensure Command Centre is configured to communicate to the cloud."
   - If you miss this step the "Send Invitation" option will fail with an error message.
5. Click the **Site Managers** tab.
   This tab allows you to invite Site Managers.



6. Click the **Invite Site Manager** button.
   The "Invite Site Manager" dialog displays.



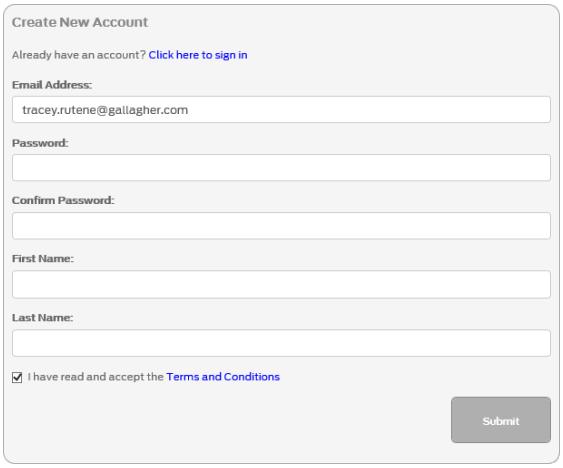
7. Type in the **Email Address** of the person you require as a Site Manager.
8. Confirm the email address by re-typing it in the **Confirm Email** field.
9. Click the **Send Invitation** button.
   An email is sent to the email address and the date and time the email was sent displays in the **Invitation History** grid.
10. Click the **Close** button.
    The "Invite Site Manager" dialog closes.
    The details of the email recipient will not display in the **Site Managers** grid until they have accepted the invitation.
11. The email recipient accepts the invitation as follows:
    a) Click the **Accept This Invite** link in the email.
    The Engage Terms & Conditions page displays.



Note: If the Engage invite is not accepted it will be withdrawn after five days and is unable to be resent to the same email address.

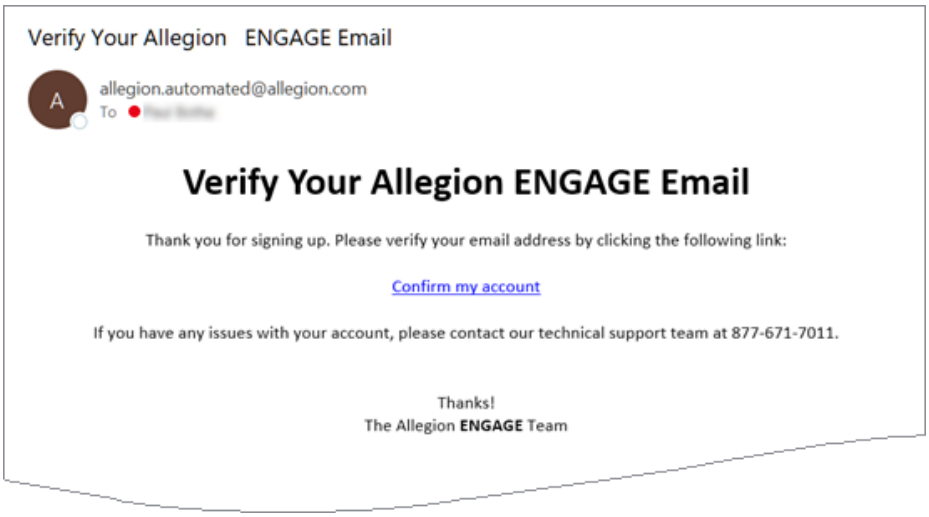
    b) Scroll down and read through the Terms & Conditions.

c) At the end of the Terms & Conditions page click the **I ACCEPT** button.
The "Create New Account" dialog displays.

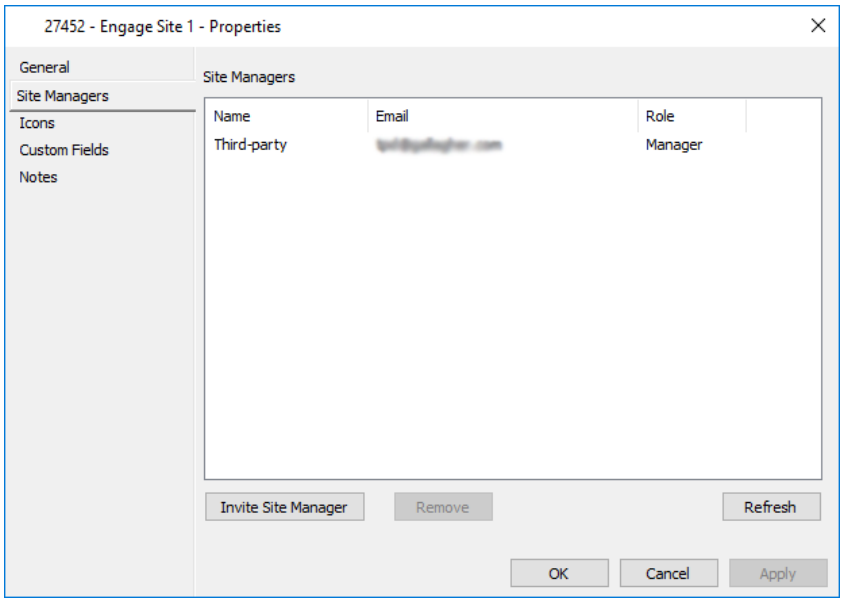


Note: If the email recipient already has an account, they should click **Click here to sign in** instead with their account.

d) Enter your details and click the **Submit** button.
Another email is sent, and you need to click **Confirm my account**.



12. Once the invitation has been accepted, click the **Refresh** button on the **Site Managers** tab.
The name and email address of the person who accepted the invitation will also populate the **Site Managers** grid.



Notes:

- The Username is taken from the User Profile on the Allegion Engage webpage. Changing it there automatically changes it on this tab also.
- Any Allegion Engage™ Mobile App Operators will also show in the **Site Managers** grid. Their role will be Operator.
- If you wish to remove a Site Manager, simply highlight the Site Manager in the **Site Managers** grid and select the **Remove** button.

13. Click the **Icons** tab if you want to change the Icon Set for this Engage Site.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
14. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Engage Site.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
15. Click the **Notes** tab if you want to add a note(s) about this Engage Site.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
16. 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.

Allegion Engage configuration

There are a number of procedures that need to be performed in the Allegion Engage™ Mobile App. They are:

- ***Installing the Allegion Engage™ Mobile App*** (on page 78-9)
- ***Commissioning Engage Gateways from the Allegion Engage™ Mobile App*** (on page 78-10)
- ***Commissioning Engage Doors from the Engage™ Mobile App*** (on page 78-12)

Installing the Allegion Engage™ Mobile App

Introduction

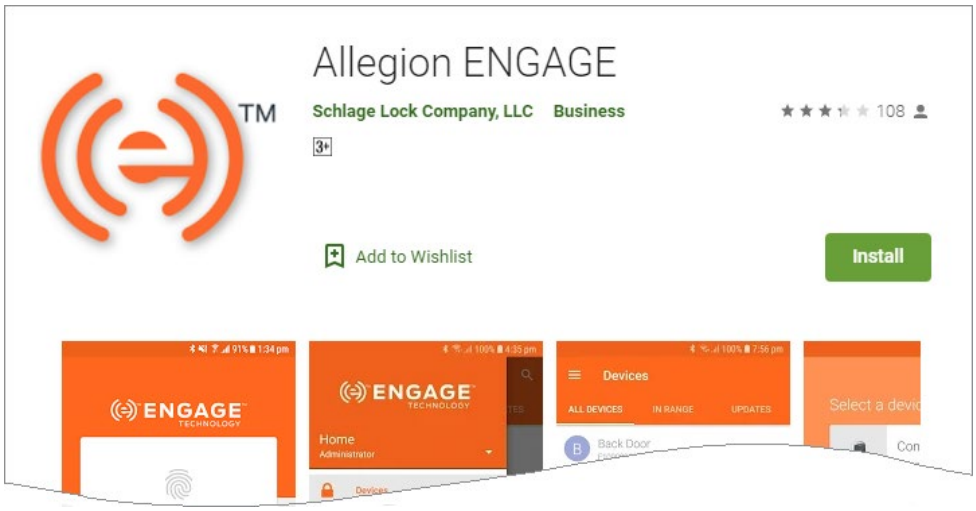
This procedure describes how to install the Allegion Engage™ Mobile App on your device.

Prerequisites

The installer should have already created an Allegion Engage™ account by accepting an email invitation as described in ***Creating an Engage Site in Gallagher Configuration Client*** (on page 78-3).

Configuration

1. Go to:
   https://play.google.com/store/apps/details?id=com.allegion.stingray or
   http://apps.apple.com/us/app/allegion-engage/id920140172
   The Allegion ENGAGE Technology Sign In screen displays.



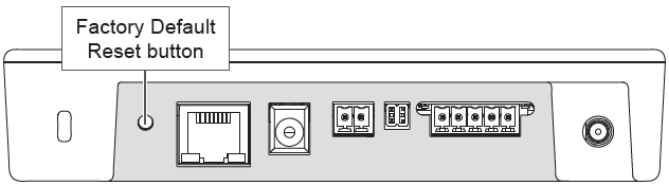
2. Click the **Install** button.
   The Allegion Engage™ Mobile App installs on your device.

Commissioning Engage Gateways from the Allegion Engage™ Mobile App

Introduction

This procedure details how to commission an Engage Gateway using the Allegion Engage™ Mobile App.

Note: All Gateways need to be factory reset before they can be used on a site, including moving to a new site. Press and hold the **Factory Default Reset** button until the Gateway Status LED flashes green two times and remains solid. After the indicator flashes twice, release the **Factory Default Reset** button.

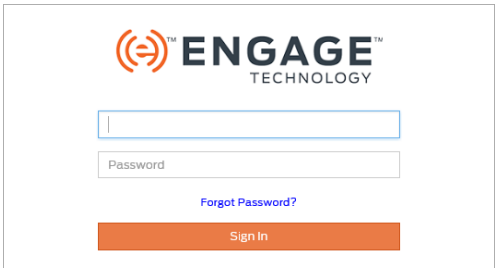


Top View

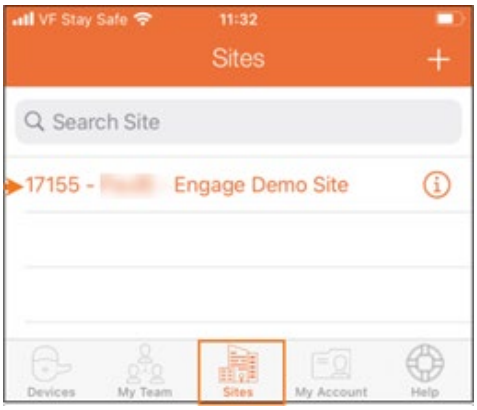
Configuration

To commission an Engage Gateway, perform the following procedure in the Allegion Engage™ Mobile App:

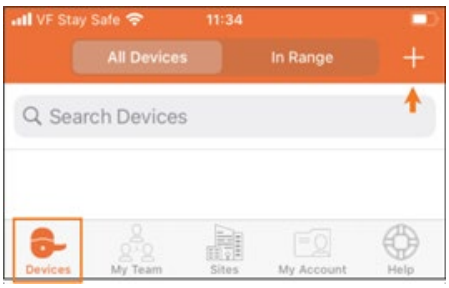
1. Log into the Allegion Engage™ Mobile App on your device.



2. Select the right Site for commissioning/installing devices.



3. Click the + button on the Devices screen.
   The Select a device type menu displays.



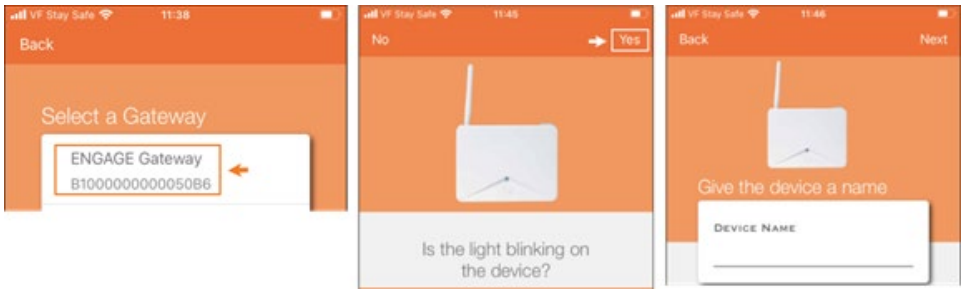
4. Select **Gateway**.



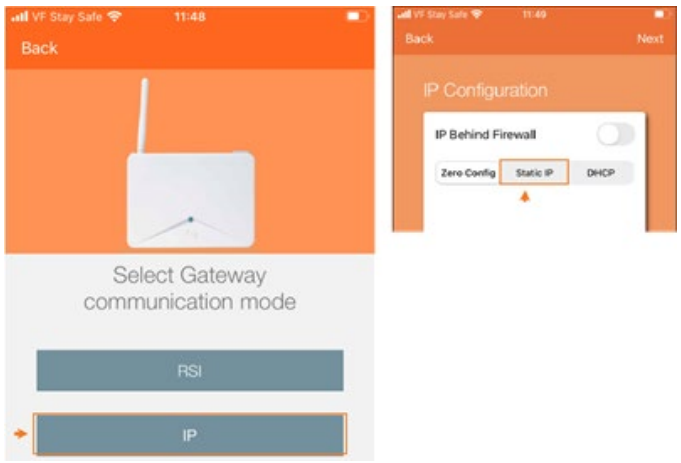
The App searches for Gateways and any that are online appear for selection.

Note: The serial number shows on the back of the device and should match what the App has found.

5. Select the Gateway and follows instructions.
   - Select **YES** when the Gateways LED starts blinking.
   - Give the Gateway a name, then select **Next**.



6. Select the IP and then select the IP Settings: Static IP.



7. Enter an IP address, default gateway, netmask, etc.
8. Click **Next**, then click **Finish**.

Commissioning Engage Doors from the Allegion Engage™ Mobile App

Introduction

This procedure details how to commission Engage Doors using the Allegion Engage™ Mobile App.

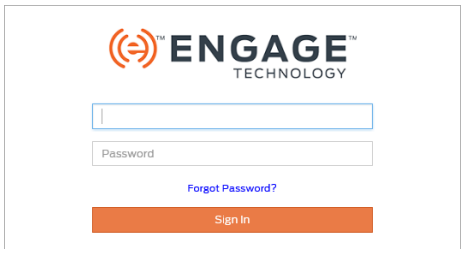
Note: All locks need to be factory reset before they can be used on a site, including moving to a new site. See ***Performing Factory Resets on Locks*** (on page 78-18).

For further information about door/lock functionality, see ***Engage Doors/ Locks*** (on page 78-14). For information on the door modes that can be set in the Allegion Engage™ Mobile App, see ***Door Modes*** (on page 78-16).

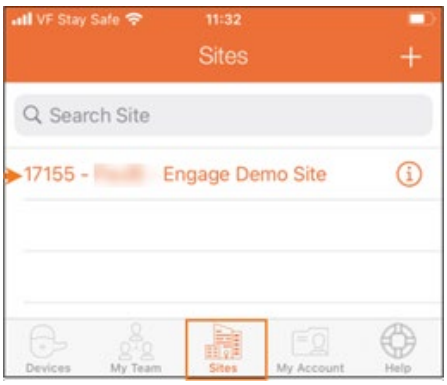
Configuration

To commission an Engage Door, perform the following procedure in the Allegion Engage™ Mobile App:

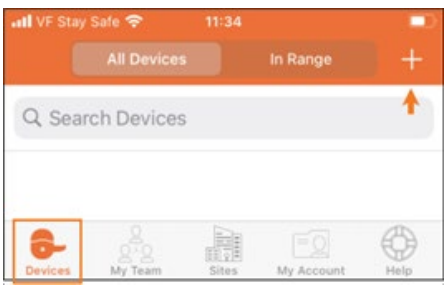
1. Log into the Allegion Engage™ Mobile App on your device.



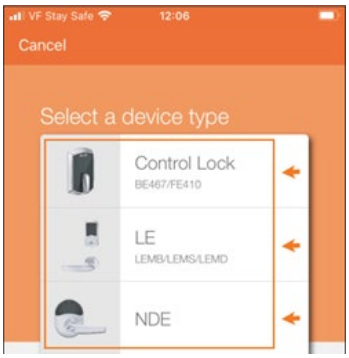
2. Select the right Site for commissioning/installing devices.



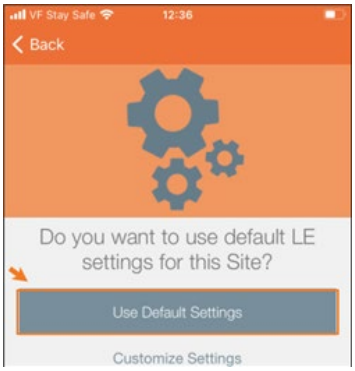
3. Click the + button on the Devices screen.
   The Select a device type menu displays.



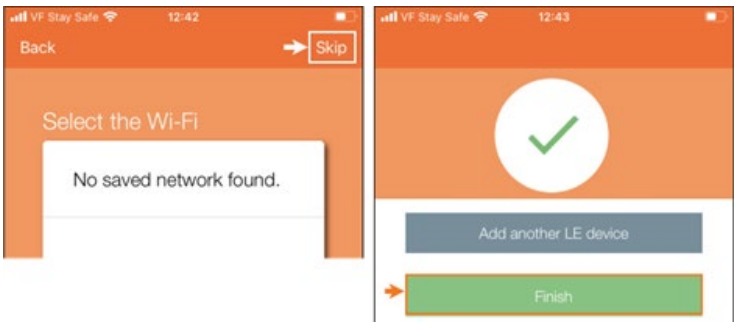
4. Select the type of lock.



5. Use **Default Settings**.



6. Enable **Select the lock function** on the Door.
   Notes:
   - Privacy needs to be set here before linking it to a Gateway, and is required to be able to do privacy overrides later.
   - If a door mode needs to be changed, delete it first in the Engage™ Mobile App, and then set it up again in the App with the new mode.
7. Run through the steps to bring it online.
8. Skip the Wifi options and click **Finish**.



9. The Door now appears in the Devices list.
10. Link the Door to the Gateway as follows:
    a) Select the **Gateway**.
    b) Select the Linked Devices.
    c) Click the + button to add a Door.
    The Device scans for any Doors it can find.
    d) Select the Door.
    The Door links to the Gateway.

Engage Doors/Locks

If a new lock is introduced with a higher version of firmware, it is recommended to downgrade the lock to the same version as the existing gateway/locks, using the mobile app, before bringing the lock online.
Note: Engage Doors will not be included in Access Reports.

Setting the time on the doors

As the Engage series make the decision to grant or deny access, they will be kept up to date with the time based on the time zone selected on the controller. If no time zone is selected, the doors will be updated with the server time. This solution does not support countries that have fixed daylight savings dates. In addition to this, countries that change daylight savings time between the hours of 4pm and 11pm, will have the time change take effect at 3pm. This can cause the access decisions made by the door to be out of sync with what is configured in Command Centre for a short period of time.
Note: The time on the door can creep. The door can be 2.5 minutes out from the gateway time, and the gateway will not force it to update. The gateway will check for the device time every 8 hours, and if it is more than 2.5 minutes out, it will push the gateway time down to the device. The controller time is also pushed to the gateway every day at 1am, and this is propagated to the doors. This creep shouldn't be noticeable, but it can affect the time a cardholder will gain access.

Door file

If there are changes to access schedules, access zones, or changes affecting all users, a full door file is required to be sent. Depending on the number of users on the doors, the changes can take up to 30.5 minutes to apply. While the change is in progress, the previous access configuration will still be in effect at the door. Here are some guidelines as to how long a full door file will take to apply:

- 200 Users, sync time is 94 sec (1.5 min)
- 300 Users, sync time is 118 sec (2.0 min)
- 2500 Users, sync time is 925 sec (15.5 min)
- 5000 Users, sync time is 1835 sec (30.5 min)

The following changes will trigger a full door file. Operators need to be aware of the implications of door access, (i.e. the old file will be in effect until the new one finishes downloading), which is dependent on the number of users on the door.

- Changing card type properties: Engage Card Type, UCF
- Hierarchy: Parenting or un-parenting an Access Group
- Access Group Field privilege: Entry allowed during lockdown
- Deleting Access Group
- Add/Modify/Remove Access Triplets (Engage Door, Engage Door Schedule, Engage Cardholder Access Schedule)

Overrides

"Lockdown" and "Emergency Open"
When a "Lockdown" or "Emergency Open" override is cancelled, all doors will be placed in the state that the Schedule would have them in. This means if a door

had been in 'privacy mode' prior to the override, after the override is lifted the door will no longer be in 'privacy mode'. Overrides also cancel privacy on doors.

"Door Open"

A "Door Open" override opens the door momentarily, and then it returns to the state it was in before it was unlocked.

Notes:

- Cardholders granted entry during "Lockdown" privilege will still adhere to the Engage Cardholder Access Schedule. This means if the door goes into lockdown and the schedule says to deny entry, they cannot get in. This differs from Gallagher behaviour.
- No overrides from the Access Zone will work for the Engage Doors.

Control Lock

- The Control lock does not have a door sensor, so cannot be shown as open or closed. We can show if the state is in "lockdown" or "emergency open" mode, otherwise it will be shown as unknown.
- The Control lock cannot be put into a free state, including using the Engage Door Schedules, and overriding on the Engage Door.

Low Battery

Installers will have between 3 and 4 weeks to replace a battery in a lock once a low battery alarm is raised. By the time the battery gets to the critical level, it will become inoperable.

Card Activation and Expiry time for locks

For LE, LE-B, NDE and NDE-B locks, card activation and expiry time can only be set to the nearest hour. If a customer inputs minutes/seconds these will be ignored. This is a constraint of the device.

For example: If a card has an activation time of 1430, it will become active at 1400. If a card has an expiration time of 1430, it will expire at 1400.

Multi-Server

Things that can be done in Multi-Server:

- Remote Engage Doors can be viewed from an Access Group
- Remote Access Groups can be viewed from the Engage Door Viewer and the Access Group
- Remote Access Groups can be added to a local Engage Door in the Door Viewer
- Local cardholders can gain access at remote Engage Doors

Things that **cannot** be done in Multi-Server:

- Remote Engage Doors cannot be viewed in the Engage Door Viewer
- Remote Engage Doors cannot be added to a local Access Group
- Overrides cannot be performed on Remote Engage Doors
- Remote Schedules cannot be viewed

Door Modes

Door modes that can be set in the Allegion Engage™ Mobile App are:

Apartment

The Apartment Mode applies to the following Locks: LE, LE-B, NDE-B

Notes:

- NDE cannot be set to Apartment mode.
- Open Door does not work for doors in Apartment Mode.

In this mode, the Privacy button is not actually a privacy button. It acts as a toggle to lock and unlock the door. It goes from secure to free and back. It will also toggle between lockdown and emergency open when overridden by an operator.

Feature	Supported
Privacy	N
Toggle free/secure	Y
Lockdown	Y
Toggle enabled during lockdown *	Y
Toggle during emergency open *	Y
Open Override	N
Emergency Open	Y
Follows schedules	N
Free access	N

* Switches between "Emergency Open" and "Lockdown"

Office

The Office Mode applies to the following Locks: LE, LE-B, NDE-B

Note: NDE cannot be set to Office mode.

In this mode, the Privacy button acts as a toggle to lock and unlock the door. It goes from secure to free and back. If lockdown is on, then it does not work.

Feature	Supported
Privacy	N
Toggle free/secure	Y
Lockdown	Y
Toggle enabled during lockdown	N
Toggle during emergency open	N
Open Override	Y
Emergency Open	Y
Follows schedules	Y
Free access	Y

Privacy

The Privacy Mode applies to the following Locks: LE, LE-B, NDE-B

Note: NDE cannot be set to Privacy mode.

This is the only mode that uses the actual privacy feature.

Feature	Supported
Privacy *	Y
Toggle free/secure	N
Lockdown	Y
Open Override **	Y
Emergency Open	Y
Follow schedules	Y
Free access	Y

* Only the Privacy Mode is on. Changing a Schedule will not affect privacy.

** Will work even if the door is set to privacy.

Storeroom

The Storeroom Mode applies to the following Locks: LE, LE-B, NDE-B
Note: This is the only mode that the NDE can be.

Privacy button does not do anything in this mode.

Feature	Supported
Privacy *	N
Toggle free/secure *	N
Lockdown	Y
Open Override	Y
Emergency Open	Y
Follow schedules	Y
Free access	Y

* No button for NDE.

Control B Lock

The Control B Lock does not use any of the modes. It cannot be changed in the Allegion Engage™ Mobile App.
Note: You cannot choose card technologies. It accepts all the types, although it does not work with 125KHz cards.

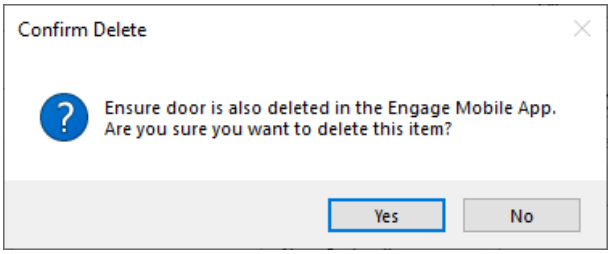
Feature	Supported	Note
Privacy	N	No privacy button
Toggle free/secure	N	No toggle button
Lockdown	Y	No denied entry event will be raised
Open Override	Y	
Emergency Open	Y	Override option is not available
Follow schedules	Y	
Free access	Y	

How to change the door mode

If you want to change door mode, you will need to do the following:

1. Delete the lock from Command Centre Configuration Client. Delete the door lock from Allegion Engage™ Mobile App, and factory reset the lock.
   Note: If you want to change the name of the door lock the same process will need to be followed.

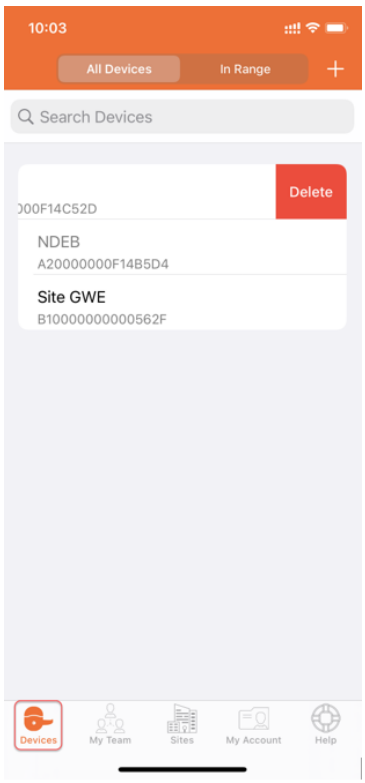
2. To delete the door lock from Command Centre Configuration Client, **right-click** on the lock and click **Delete**. The following message will display:



3. Delete the door lock from Site GWE using Allegion Engage™ Mobile App.
   Click **Sites**, choose the correct site and GWE, then click **Linked Devices**. Hold down finger on the lock you want to delete and swipe left. (See screenshot on the left.)



4. Delete the door lock from Devices using Allegion Engage™ Mobile App. Hold down finger on the lock you want to delete and swipe left. (See screenshot below.)



5. Factory rest the door lock. Refer to ***Performing Factory Resets on Locks*** (next) for the procedure.
6. Once this process has been completed add the new door lock by following the ***Commissioning Engage Doors from the Allegion Engage™ Mobile App*** (on page 78-12) procedure.

Performing Factory Resets on Locks

A Factory Default Reset (FDR) returns the lock to the original settings as shipped from the factory. This removes configurations, databases, and requires the lock to be re-captured.

Note: The FDR process does not remove the lock from your Engage account.

Follow the appropriate procedure below for the type of lock you want to perform a factory default reset on.

NDE and LE locks

1. Open the battery cover.
2. Press the button under the pin hole about the batteries.
3. Press and hold the FDR button for five seconds.
   The NDE will blink green two times and beep two times.
4. Turn the inside lever three times within 20 seconds.
   The LED will blink red and the lock will beep with each turn.
   The factory default reset is complete when you hear one long beep.
5. Install the cover and connect to the lock.

Control Locks

1. Disconnect the batteries for at least ten seconds.
2. Reconnect the batteries.
3. Wait for the lock to beep and flash three times.
4. Within ten seconds, rotate the interior tail piece back and forth two times.
   The lock will flash one long green flash and beep one long beep to indicate the process was successful.

Command Centre configuration

There are a number of procedures that need to be performed in Gallagher Configuration Client. They are:

- ***Gallagher Command Centre Engage Gateway configuration*** (on page 78-20)
- ***Gallagher Command Centre Engage Door configuration*** (on page 78-24)
- ***Creating an Engage Card Type in Gallagher Command Centre*** (on page 78-28)
- ***Encoding Gallagher Credentials to an Engage Card*** (on page 78-30)
- ***Upgrading Engage Firmware*** (on page 78-33)

While Engage Gateways, Doors and Card Type are all created in Configuration Client, Engage scheduling is done in the Command Centre Client. Therefore, see *"Engage Doors"* in the Command Centre Client Help file for further detail.

Gallagher Command Centre Engage Gateway configuration

Introduction

An Engage Gateway provides Command Centre with a certificate which is used to encrypt the communications that are sent to the Gateway. It is also used to decrypt what has been sent from the Gateway to Command Centre.

This procedure details how to create an Engage Gateway.

Prerequisites

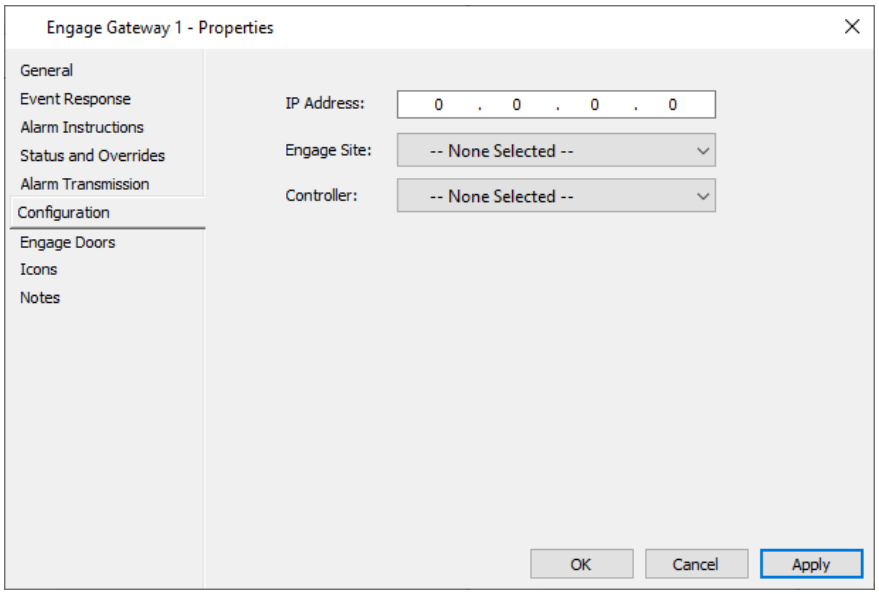
Before proceeding with this procedure, ensure:

- An Engage Gateway has been created in the Allegion Engage™ Mobile App. See ***Commissioning Engage Gateways from the Allegion Engage™ Mobile App*** (on page 78-10) for the procedure.
- Locks have been created in the Allegion Engage™ Mobile App. See ***Commissioning Engage Doors from the Allegion Engage™ Mobile App*** (on page 78-12) for the procedure.
- Your license file allows for the number of doors you are adding.

Configuration

To configure an Engage Gateway, perform the following procedure in Gallagher Configuration Client:

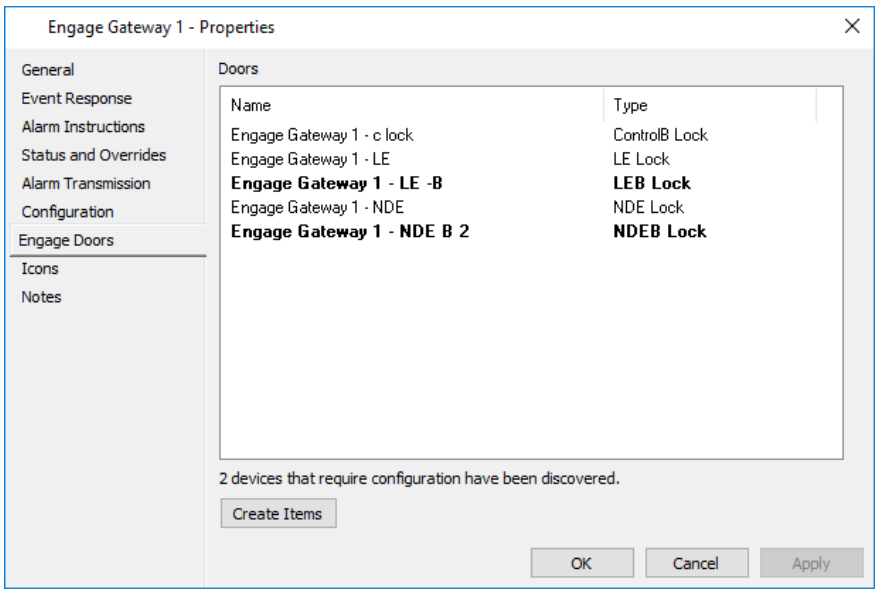
1. Click **Configure** from the menu bar, then **Engage**.
   The Engage List Window opens.
2. **Right click** and select **New...Engage Gateway**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab, and assign a primary Alarm Zone for all events.
   For further detail see ***Event Response tab*** (on page 3-20).
5. Click the **Configuration** tab.



6. Input the **IP Address**, and select the **Engage Site** and **Controller** from the drop-down list.
   Notes:

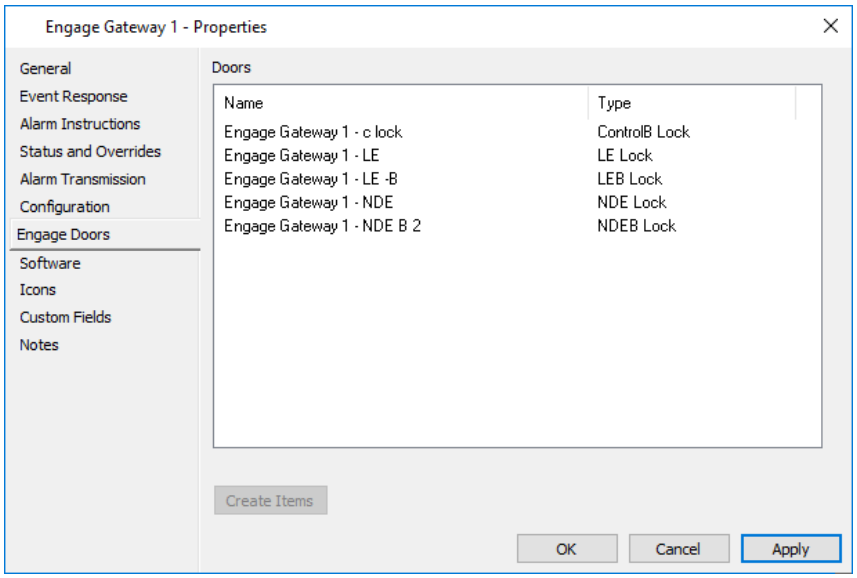
   - The IP Address should be the same IP Address you gave the Gateway when you created it using the App. You can find this on the App by bringing up the Gateway and clicking on **Host Properties**.
   - It is recommended that no more than eight Engage Gateways are connected a single Gallagher Controller.

7. Click the **Engage Doors** tab.



   Doors you have created in the Allegion Engage™ Mobile App appear in bold.

8. Click on the **Create Items** button.
   All Doors that were bold no longer appear in bold, indicating they have been created in Command Centre.



Note: The names of the Doors will be the names given in the Allegion Engage™ Mobile App.

9. Click the **Icons** tab if you want to change the Icon Set for this Engage Gateway. For further details see ***Icons*** (on page 6-80).
10. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Engage Gateway.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
11. Click the **Notes** tab if you want to add a note(s) about this Engage Gateway. For further details see ***Notes*** (on page 6-85).
12. Click **Apply** to save the Gateway.
    Note: If you click **Apply** without first creating the Gateway in the Allegion ENGAGE™ Mobile App, the following error message will display:
    "Unable to connect to the Engage Gateway at the specified IP address."

Failure to create doors

If there are insufficient licenses to create the doors in Command Centre, or if a door is given the same name as an existing Engage Door in the Command Centre server, the doors will fail to create. If the issue is due to licensing, the doors will be created up until the license limit is reached. If the installer wants to choose which doors they want created, they will need to use the Allegion Engage™ Mobile App to remove the doors they do not want to be created. They can also use the app to change the name of a door. They can then go back to the Gateway item and 'Create Doors' to update what has been created in Command Centre.

Editing and Deleting Gateways

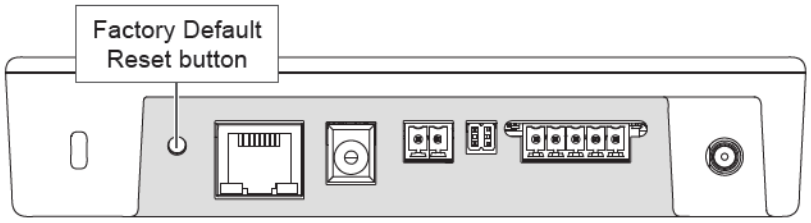
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Engage Gateways.

Notes:

- You cannot delete a Gateway that has Doors assigned to it.

- If for some reason you delete the Gateway from Command Centre it will need to be removed from the site using the Allegion Engage™ Mobile App, as well as it being factory reset before it can be used again.

  Press and hold the **Factory Default Reset** button until the Gateway Status LED flashes green two times and remains solid. After the indicator flashes twice, release the **Factory Default Reset** button.



Top View

For more information refer to the *ENGAGE™ Gateway Installation Instructions and User Guide*.

Gallagher Command Centre Engage Door configuration

Introduction

Access information is stored within the Engage Door itself. Credentials used to access the door are sent at card level, as opposed to the cardholder, and there is a limit of 5000 users allowed per door NDE and LE, and 500 per Control Lock.

This procedure details how to configure an Engage Door in Command Centre, once it has been created using the Allegion Engage™ Mobile App.

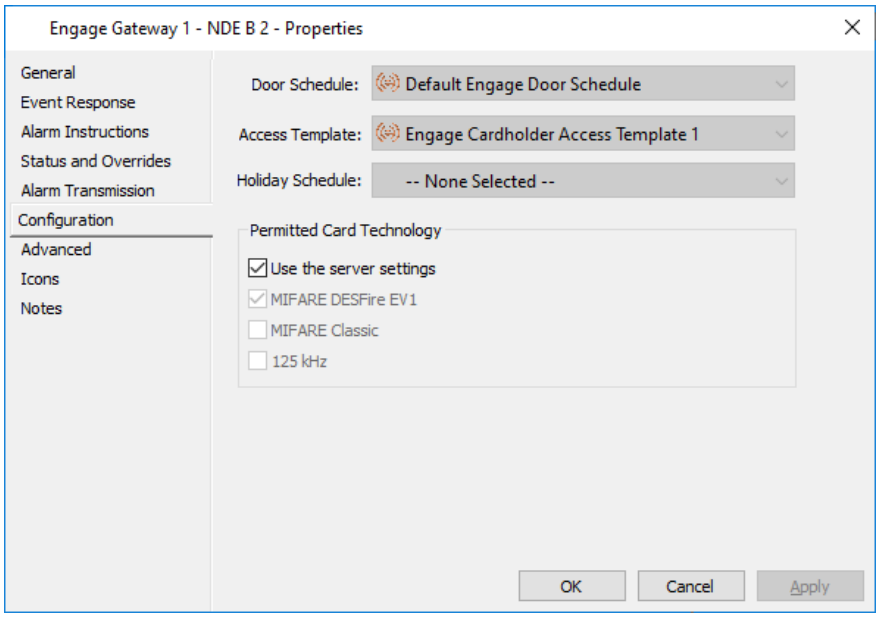
Prerequisites

Doors must be created in the Allegion Engage™ Mobile App first (see ***Commissioning Engage Doors from the Allegion Engage™ Mobile App*** on page 78-12 for further detail), and then generated in Command Centre from the Engage Doors tab of the Engage Gateway (see ***Gallagher Command Centre Engage Gateway configuration*** on page 78-20 for further detail).

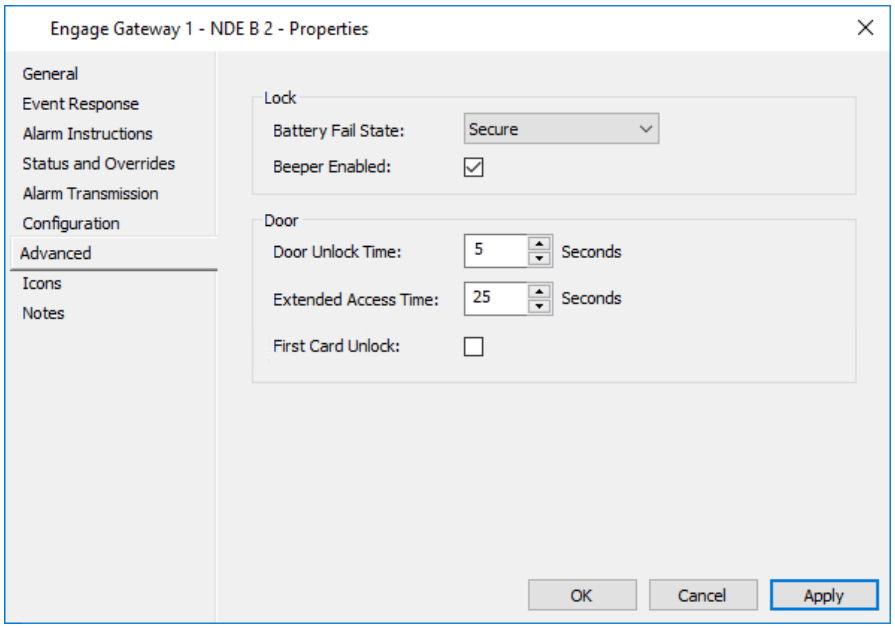
Configuration

To configure an Engage Door, perform the following procedure in Gallagher Configuration Client:

1. Click **Configure** from the menu bar, then **Engage**.
   The Engage List Window opens.
2. **Right click** on the Door to be configured, and select **Properties**.
   By default the **General** tab displays.
   Note: Engage Door names cannot be changed from Command Centre. They need to be changed in the Allegion Engage™ Mobile App, and then sent down to Command Centre.
3. Click the **Event Response** tab, and assign a primary Alarm Zone for all events.
   For further detail see ***Event Response tab*** (on page 3-20).
4. Click the **Configuration** tab.



5. The **Door Schedule**, **Access Template** and **Holiday Schedule** are assigned to the Door in Command Centre Client and cannot be altered here, (i.e. these fields are all 'read-only'). Refer to *"Allegion Engage Interface"* in the Command Centre Client Help file for further detail.
6. 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 door, uncheck the **Use the server settings** checkbox and select the appropriate checkboxes.
   Notes:
   - Selecting **MIFARE Classic** or **125 kHz** technologies results in the following warning message:
     "Some of the card technology options selected have known security vulnerabilities."
   - The "Permitted Card Technology" section does not appear for Control locks.
7. Click the **Advanced** tab.



8. Configure the lock settings as required.

Option	Description
Battery Fail State	Select the required Door state from the drop-down list for when the battery runs out of charge: • As is: Door will remain in the state configured before battery is discharged. • Free: Door will remain UNLOCKED when the battery is discharged. • Secure: Door will remain LOCKED when the battery is discharged. (Default = Secure)
Beeper Enabled	This is enabled by default meaning that the beepers of the door will be turned on. Unchecking this will turn the door's beepers off.

9. Configure the Engage Door timeouts as required.

Option	Description
Door Unlock Time	This determines the maximum time the Unlock relay is energised. (Valid range is 1 - 86400 seconds. Default = 5 seconds)

Option	Description
Extended Access Times	This setting determines an alternate unlock time, allowing the door to remain unlocked for longer than normal for those cardholders who require it, (e.g. disabled people, couriers, etc.). (Valid range is 0 - 86400 seconds. Default = 25 seconds) Refer to ***Configuring alternate unlock time for a Door*** (on page 22-13) for further details.
First Card Unlock	Normally if a schedule grants free access, even if no one has arrived, the door still goes to "Free-PIN". Enabling this setting stops the door from going to free until the first cardholder arrives and badges their card.

12. Click the **Icons** tab if you want to change the Icon Set for this Engage Door.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
13. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Engage Door.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
14. Click the **Notes** tab if you want to add a note(s) about this Engage Door.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
15. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save tour changes and stay in this window.

Editing and Deleting Doors

Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Engage Doors.

Note: If a door is deleted from Command Centre, it must also be removed from the site using the Allegion Engage™ Mobile App and factory reset before it can be re-used. Failure to factory reset the device can result in cardholders continuing to gain access to the door.

Creating an Engage Card Type in Gallagher Command Centre

Introduction

The following card types are supported:

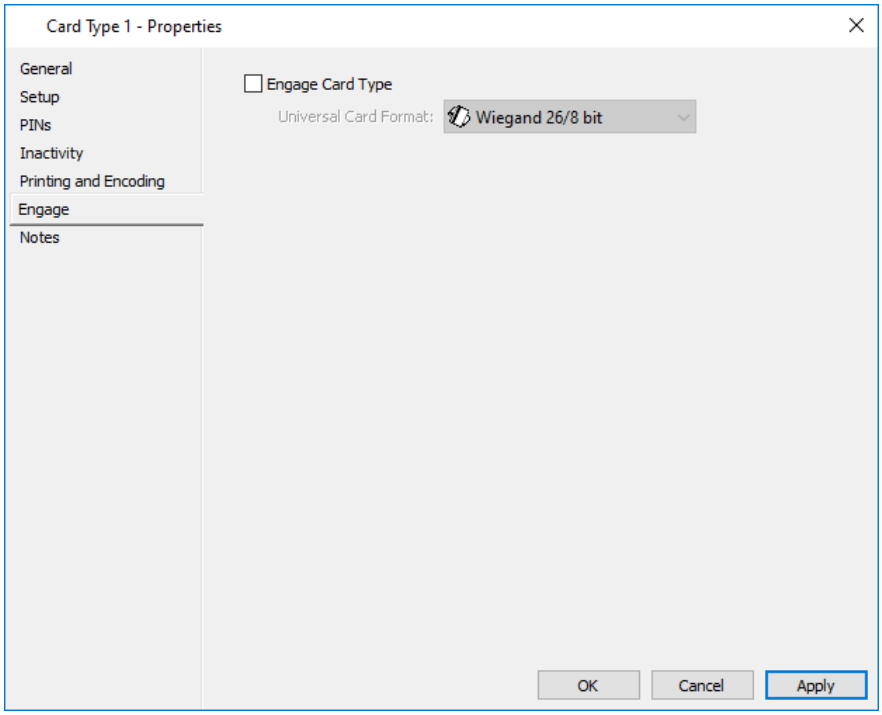
- Prox Smart Card (125khz, i.e. low frequency)
- MIFARE Classic
- MIFARE DESFire

This procedure details how to create an Engage Card Type.

Configuration

To configure an Engage Card Type, perform the following procedure in Gallagher Configuration Client:

1. Click **Configure** from the menu bar, then **Card Types**.
   The Card Type List Window opens.
2. **Right click** and select **New...Card Type**.
   By default the **General** tab displays.
3. Configure the new Card Type as required.
   See ***Setting up Card Types*** (on page 7-2) for further detail.
4. Click the **Engage** tab.
   Note: This tab will only display for sites licensed for the Allegion Engage feature.



5. Tick the **Engage Card Type** checkbox.
   The Universal Card Format field is enabled.
6. Select the appropriate Universal Card Format from the drop-down list. (Default = Wiegand 26/8 bit)
   Refer to ***Configuring a Universal Card Format to support different Schlage Credential Formats*** (on page 78-23) for more information, and the *"How to read Schlage card details and create a cardholder"* section in that topic for how to determine Schlage card details
7. Click the **OK** button.

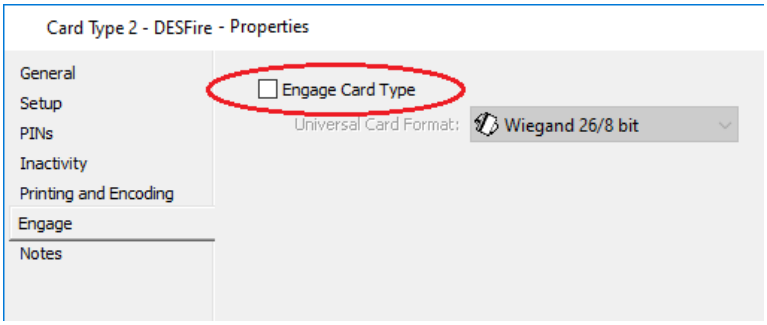
Encoding Gallagher Credentials to an Engage Card

Introduction

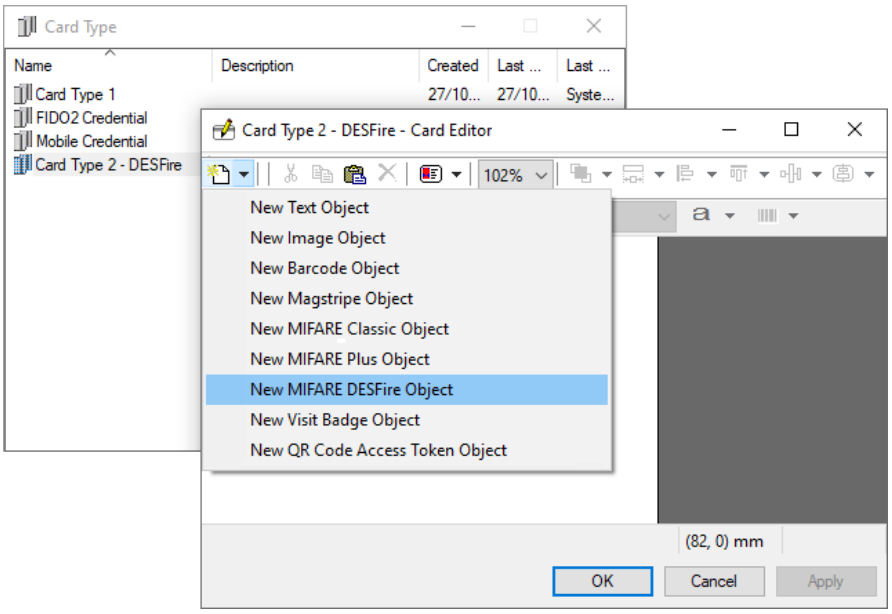
Engage cards can be used for Gallagher readers. This involves setting up two card types, (i.e. an *Engage* Card Type and a *DESFire* Card Type) for a single card to allow the cardholder to access both Engage and Gallagher readers.

Procedure

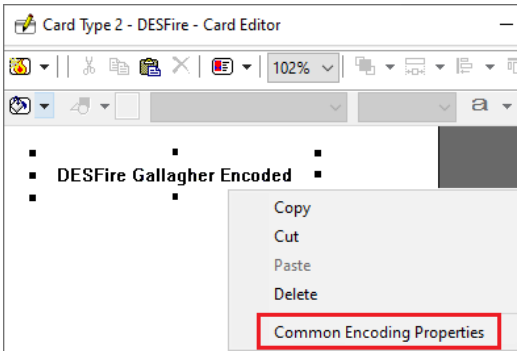
1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. Configure an Engage Card Type.
   See ***Creating an Engage Card Type in Gallagher Command Centre*** (on page 78-28) for the procedure.
3. Create a DESFire Card Type with the correct Facility code on the **Setup** tab, and make sure "Engage Card Type" is unchecked on the **Engage** tab.



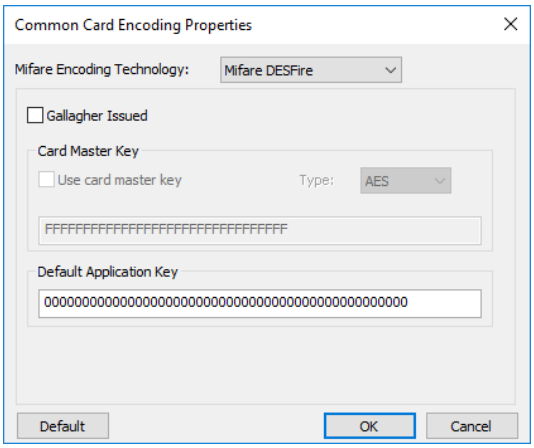
4. Once created, right click on the DESFire Card Type from the **Card Type** List Window, and select **Edit Card Layout**.
   The Card Editor window displays.
5. Select **New MIFARE DESFire Object**
   An object box displays with placeholders around it.



6. Right click on the MIFARE DESFire object, then click **Common Encoding Properties** from the drop-down menu.

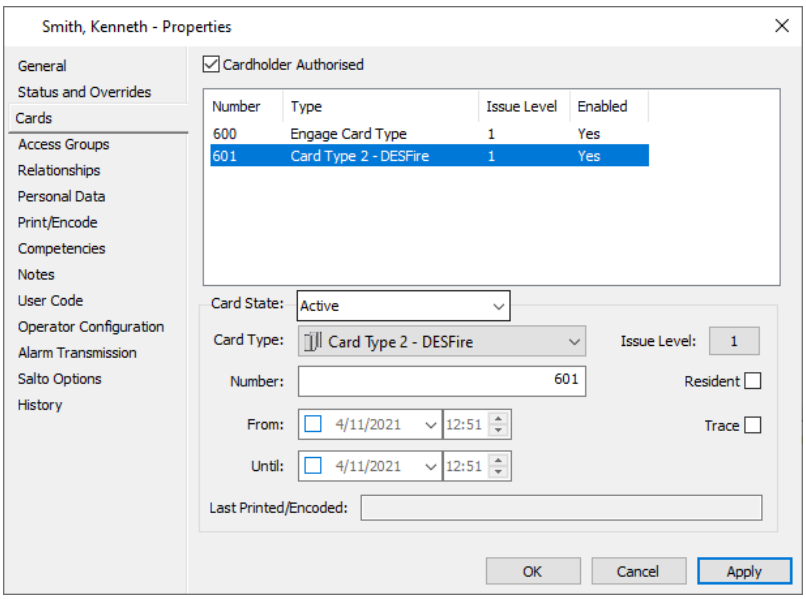


7. Uncheck the **Gallagher Issued** checkbox, and replace all Fs in the **Default Application Key** field to 0s.



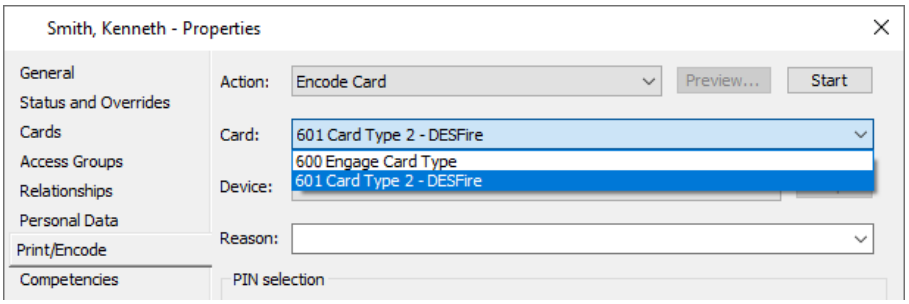
Note: If this step is missed, when encoding the DESFire card, the following warning message will display: *"Authentication failed with supplied key(s)."*

8. Select a Cardholder which already has the Engage Card Type that was created at Step 2.
9. On the Cardholder's **Cards** tab, insert the DESFire Card Type that was created at Step 3.

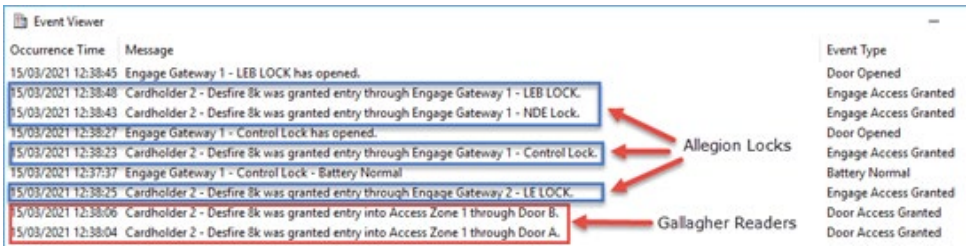


See ***Adding a Card to a Cardholder*** (on page 32-9) for the full procedure if required.

10. Connect the card encoder to the PC and place a DESFire card on the encoder.
11. Click the Cardholder's **Print/Encode** tab.
12. Select "Encode Card" from the **Action** drop-down list.
13. Select the correct card type from the **Card** drop-down list and click the **Start** button to start encoding.



After card encoding completes the card will allow access at Allegion locks and Gallagher door readers.



Upgrading Engage Firmware

Introduction

Upgrading Engage firmware can be done via Command Centre for Gateway versions 1.52.16 and above. For customers using an older version they will need to manually upgrade their devices to 1.52.16 or later in order to take advantage of upgrading firmware via Command Centre.

This procedure for upgrading firmware is split into two parts, as follows:

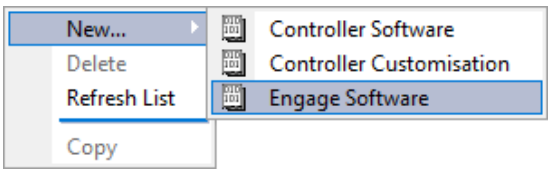
- Creating an Engage Software item
- Assigning Engage Software to the Gateway and devices

Procedure

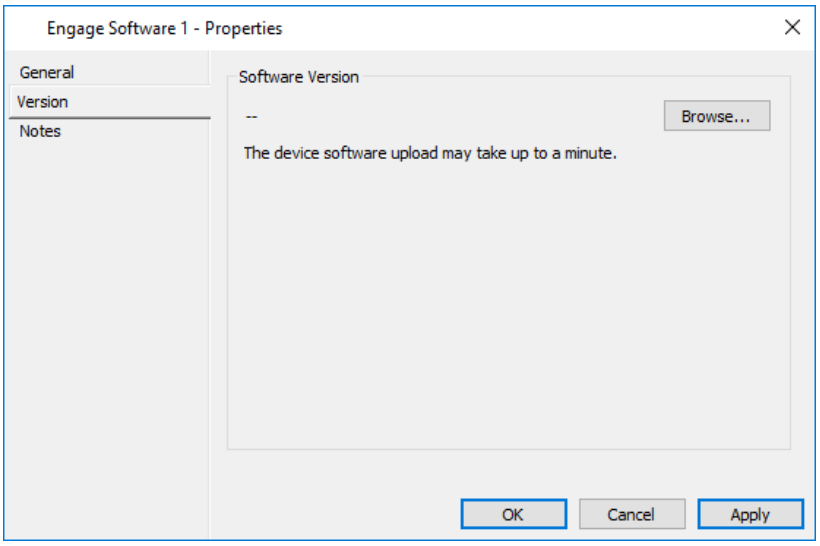
To upgrade Engage firmware, perform the following procedures in Gallagher Configuration Client:

Creating an Engage Software item

1. Click **Configure** from the menu bar, then **Device Software**.
   The **Device Software** List Window opens (in grid view).
2. **Right click** and select **New...Engage Software**.
   By default the **General** tab displays.

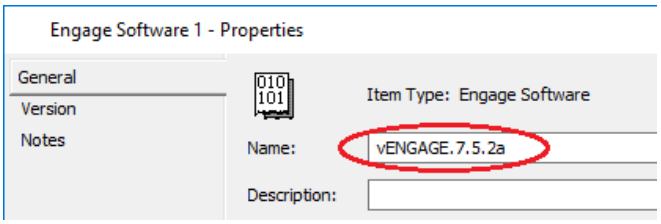


3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Version** tab.

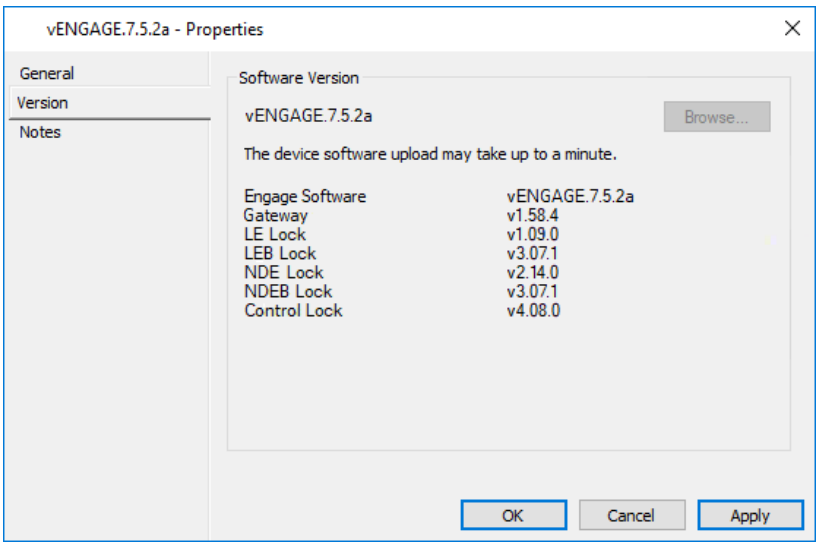


5. Click the **Browse…** button and locate the Engage Firmware package (***.gglsec**) on your computer.
6. Highlight the file once located and click the **Open** button.
   The version of software displays in the **Software Version** field.

   The name of any software selected will automatically populate the **Name** field on the **General** tab.



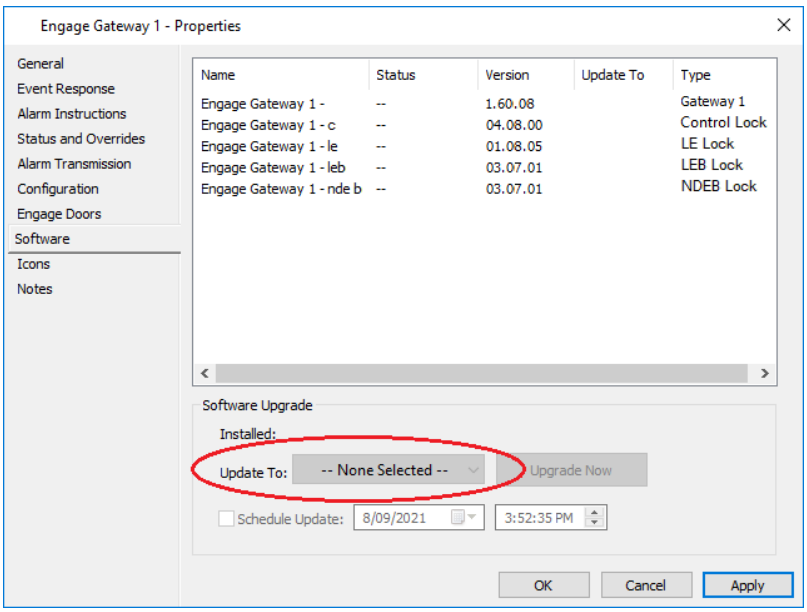
   When an Engage Firmware package is selected, once the software has downloaded, the individual firmware versions for the different device models that are included in the ENGAGE file package display on the **Version** tab.



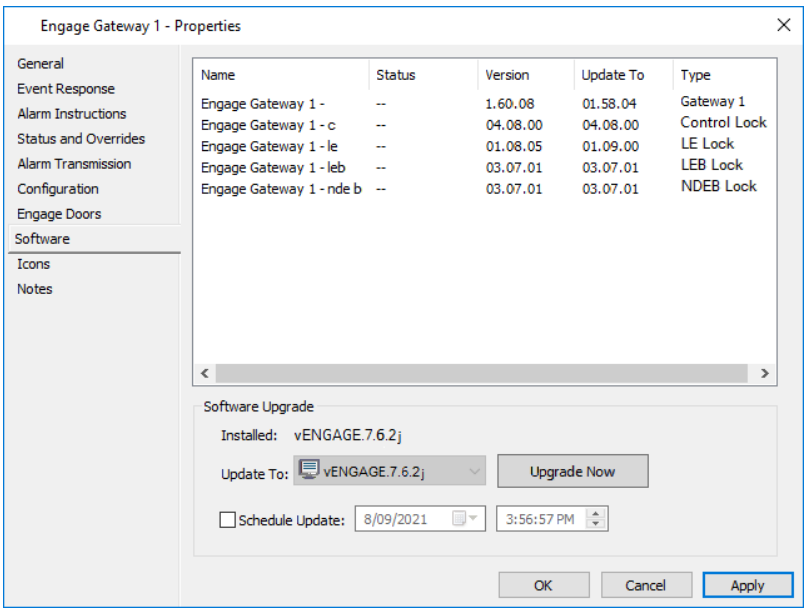
7. Click the **Notes** tab if you want to add a note(s) about this Engage Software item.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
8. Click **OK** to save the Engage Software item.

Assigning Engage Software to the Gateway and devices

9. Click **Configure** from the menu bar, then **Engage**.
   The **Engage** List Window opens.
10. **Right click** on the Engage Gateway to have firmware applied to it, and select **Properties**. By default the **General** tab displays.
11. Click the **Software** tab.



12. Select the required firmware version from the **Update To** drop-down list. The **Upgrade Now** button and **Schedule Update** checkbox both become enabled, and the "Update To" column is populated.

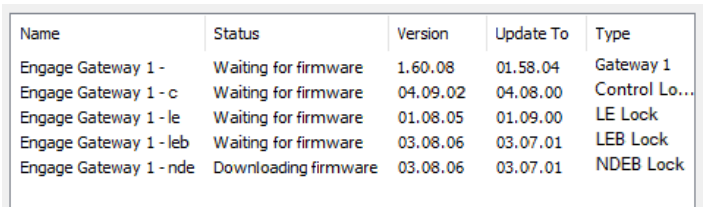


This gives you the option to either update the firmware now or schedule it for another time.

Note: During a firmware update, the Gateway pushes the firmware one by one to each device and no door files can be sent while this is occurring. Updates can take up to 40 minutes per device.

13. Do you want to update the firmware now or schedule it for another time?

If update…	then…
later,	a) Tick the **Schedule Update** checkbox. The Date and Time fields become enabled. b) Enter the date and time you want the upgrade to occur, and click **Apply**.

If update…	then…
	An event is generated indicating the date and time the update is scheduled for, and the following message displays: *"Software update cannot be cancelled once started. Do you wish to continue?"* c) Click **OK** to close the message dialog.
now,	a) Click the **Upgrade Now** button. The following message displays: *"Software update cannot be cancelled once started. Do you wish to continue?"* b) Click **OK** to close the message dialog.  The status (in the "Status" column) for each device changes as the firmware upgrade progresses through the queue. Once complete, the versions in the "Version" column will match those in the "Update To" version on the **Software** tab of the Gateway. **Notes:** • Similar statuses will appear on the **Status and Overrides** tab of the Gateway/devices also. • If a door already has the latest firmware configured, it will show *"Update successful"* afterwards, even though it was never actually updated. • If the currently selected version does not allow downgrading, this will be displayed as a prompt. Once the selected version is installed, it will be persisted as a message on the **Software** tab of the Gateway. Command Centre will still allow firmware to be downgraded, even if the firmware version does not allow this, however the downgrade will eventually fail.

14. Click **OK** to exit the Gateway properties and save your changes.

Result

A new Engage Software item has been created, and a new version of the Engage Firmware has been added to Engage Gateway and devices.

Chapter 79: Open Supervised Device Protocol (OSDP) Integration

Introduction

Open Supervised Device Protocol (OSDP) replaces the Wiegand legacy protocol, and allows security devices such as card readers, controllers and I/O boards to talk to each other through a bi-directional RS485 channel.

Controller 6000: Supports up to 16 OSDP-compliant readers, split across runs - maximum 16 readers per run.

Controller 7000: Supports up to 32 OSDP-compliant readers, split across runs - maximum 16 readers per run.

Functionality

The Gallagher OSDP Integration allows security devices to communicate using the OSDP standard.

Gallagher's OSDP Integration allows messages to be displayed on OSDP readers with 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 card is badged. If two readers are assigned tothe same Exit Zone or Entry Zone of a Door - one OSDP and one non-OSDP - a Cardholder badging at the non-OSDP reader will result in the more descriptive access message being displayed on the OSDP reader (as well as the regular message on the non-OSDP reader).

A number of various default messages will display. See ***List of displayed messages*** (on page 79-2) 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.

Configuration

Select the item below that you require further detail on:

- ***List of displayed messages*** (on page 79-2)
- ***Configuring an OSDP Reader*** (on page 79-3)

  Note: Sites licensed for Personal Identity Verification (PIV) will also have the ability to configure OSDP Veridt Stealth PIV Readers. See ***Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Readers*** (on page 57-21) for further detail.
- ***Assigning an OSDP Compliant Reader to a Gallagher Controller*** (on page 79-7)
- ***Moving OSDP Readers between Controllers*** (on page 79-9)

List of displayed messages

Default status messages (when the reader is idle)

Status or active state	Message displayed on reader screen
Zone is in a locked down state	*Lockdown <date and time inserted>*
Zone is in a Secure access mode (including Code Only)	*Secure <date and time inserted>*
Zone is in Free access mode	*Free <date and time inserted>*
Zone is in a Dual Authorisation access mode	*Dual-authority*
Door Open Too Long	*Door open too long*
Forced Door	*Door forced*

Default access request messages (when a card is badged)

Access event	Message displayed on reader screen
Accept First Card	*Waiting for 2nd authority*
Attempt to access zone during Lockdown	*Zone locked down*
Bad Second Card	*Bad Second Card*
Card used as an invalid issue number	*Invalid Issue*
Cardholder does not have one or more required active competencies to enter access zone	*Competency Required*
Door Access Granted	*Access granted*
Exit Denied when tailgating	*Exit denied*
Foreign Card	*Foreign card*
Incorrect usercode entered	*Wrong usercode entered*
Interlock Rules Prevented Entry	*Interlock rules prevented entry*
No Access At This Time	*No access at <time inserted>*
No Zone Privilege	*No zone access*
PIN or Usercode entered too late	*PIN too late*
Reader is awaiting PIN entry	*Enter PIN:*
Repeated First Card	*Repeated first card*
Second card presented too late when in Dual Auth mode	*Dual Auth Timeout*
The first access attempt is invalid when in Dual Auth mode	*Bad dual authorisation*
Unauthorised Card	*Unauthorised card*
Usercode expected as PIN but it is not set	*No usercode set*
Wrong Facility Code	*Unknown facility code*
Wrong PIN Entered	*Wrong PIN entered*

Configuring an OSDP Reader

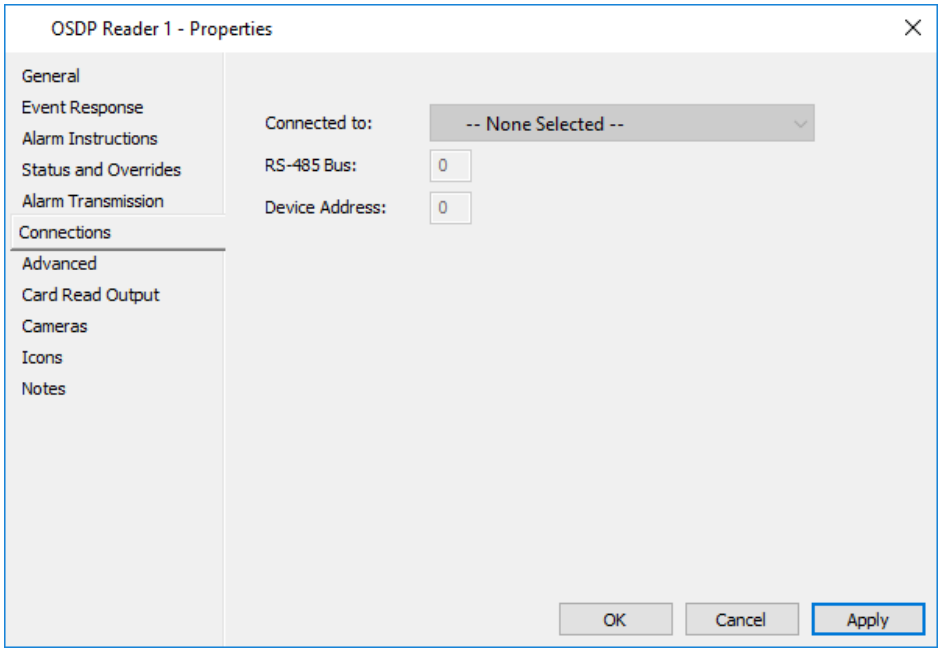
Introduction

This procedure describes how to configure an Open Supervised Device Protocol (OSDP) Reader in Gallagher Command Centre.

Procedure

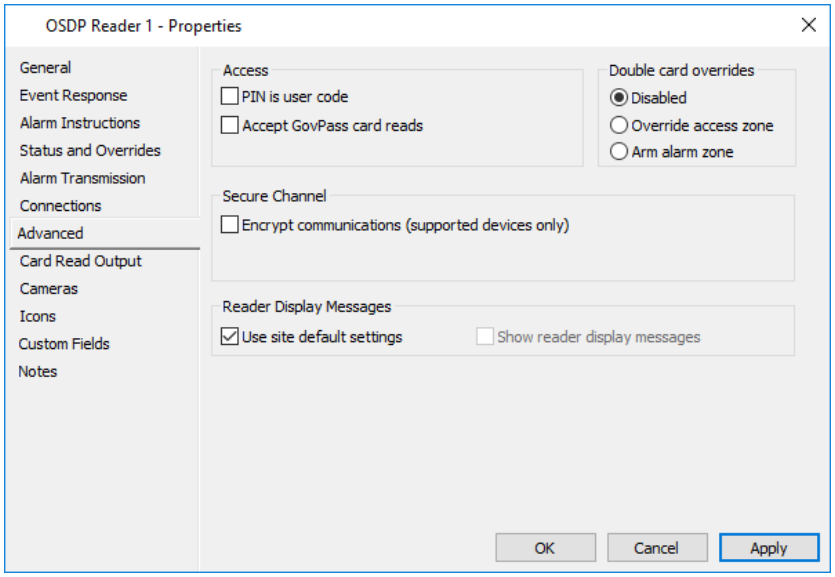
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...OSDP Devices**>**OSDP Reader.**
   By default the **General** tab displays.

   Note: Sites licensed for Personal Identity Verification (PIV) will also have an option for configuring OSDP Veridt Stealth PIV Readers.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
5. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
6. Click the **Connections** tab.



The three fields, (i.e. **Connected to**, **RS-485 Bus** and **Device Number**) will be populated once you assign this reader to a Controller 6000. See ***Assigning an OSDP Compliant Reader to a Gallagher Controller*** (on page 78-7) for further detail.

7. Click the **Advanced** tab.



8. Check the **PIN is user code** checkbox if required.

   With **PIN is user code** checked, the user code will be required in place of a PIN for any transactions at the reader which would normally require a PIN. This includes door access and overrides.

9. Depending on your sites license file, an additional field may display.

If the…	then your site is licensed for…
Accept GovPass card reads checkbox displays,	GovPass, (i.e. the license file contains `UKGovPASS=1`). Check this checkbox if you want this reader to be able to accept a GovPass credential card read.
Accept CipherToken card reads checkbox displays,	CipherToken, (i.e. the license contains `CipherToken=1`). Check this checkbox if you want this reader to be able to accept a CipherToken credential card read.

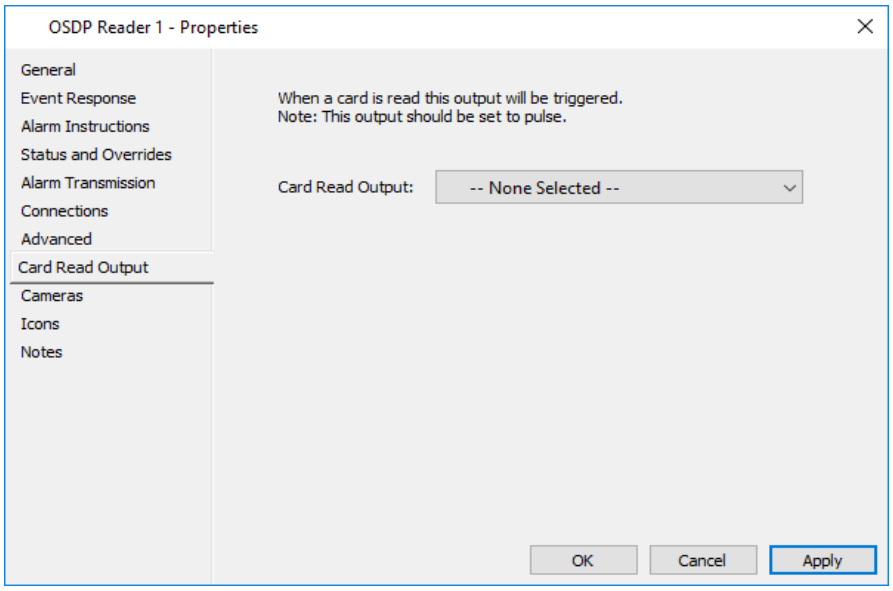
10. If you want the double-card override feature to be available, click either the **Override access zone** or the **Arm alarm zone** radio button, depending on whether you want the double-card override to override the state of the Access Zone or arm the Alarm Zone associated with the Access Zone.
11. The **Secure Channel** setting allows you to turn encrypted communications on and off, (e.g. you may want to turn it off if it affects performance or the device does not support encryption).
    Does the device support encrypted communications?

If…	then…
yes,	check the **Encrypt communications (supported devices only)** checkbox to turn encryption on. If this is not done an alarm will be generated.
no,	Leave the **Encrypt communications (supported devices only)** checkbox unchecked. If it is checked, an event will be generated and it will remain offline until encryption is turned off, (i.e. the **Encrypt Communications** checkbox is unchecked). The device's status will indicate that it is offline and encryption is not supported, (i.e. *"Device not responding. Encryption not supported."*)

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

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 **Show reader display messages** checkbox.

13. Click the **Card Read Output** tab.



14. From the **Card Read Output** drop-down list (which includes virtual outputs), select the output to switch on when a card is badged at the reader. **Notes:**
    - Badging a card at this reader will switch on the associated relay. The relay will then be immediately switched off unless the relay output is configured to pulse, in which case the relay will stay on for the pulse time and then be switched off. The card format does not have to be correct, nor does the card have to be assigned to a cardholder to trigger the relay.
    - It is recommended that the output be configured to pulse (via the **Advanced** tab of the Output's properties). If the Output is not configured as a pulse output then the relay will pulse for 1 second. The Output can be assigned to more than one reader at a time, each reader will cause the relay to pulse.
15. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this OSDP Reader. For further details see ***Cameras tab*** (on page 3-24).
16. Click the **Icons** tab if you want to change the Icon Set for this OSDP Reader.

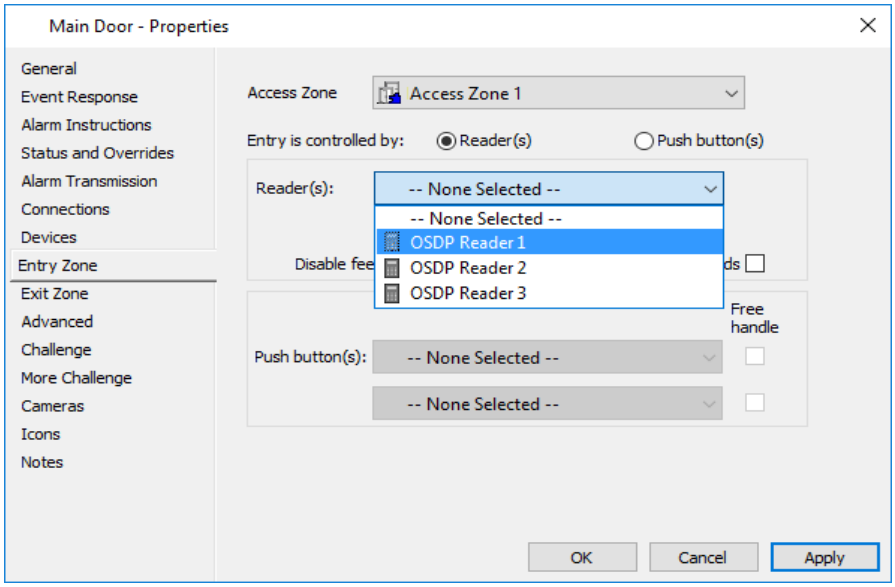
For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).

17. Click the **Custom Fields** tab if you want to add and assign a custom field value to this OSDP Reader.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
18. Click the **Notes** tab if you want to add a note(s) about this OSDP Reader. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
19. 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 Reader

Once the configuration work is complete, you need to assign the Reader to a Gallagher Controller 6000 and a Door.

20. Assign this reader to a Controller. See ***Assigning an OSDP Compliant Reader to a Gallagher Controller*** (on page 79-7) for further detail.
21. From the Door List Window, highlight the door you want to assign this reader to.
22. **Right click** and select **Properties**.
23. Click the **Entry Zone** or **Exit Zone** tab as appropriate.
24. Assign the reader to the appropriate Reader Address by selecting it from the relevant **Reader(s)** drop-down list.



25. 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.

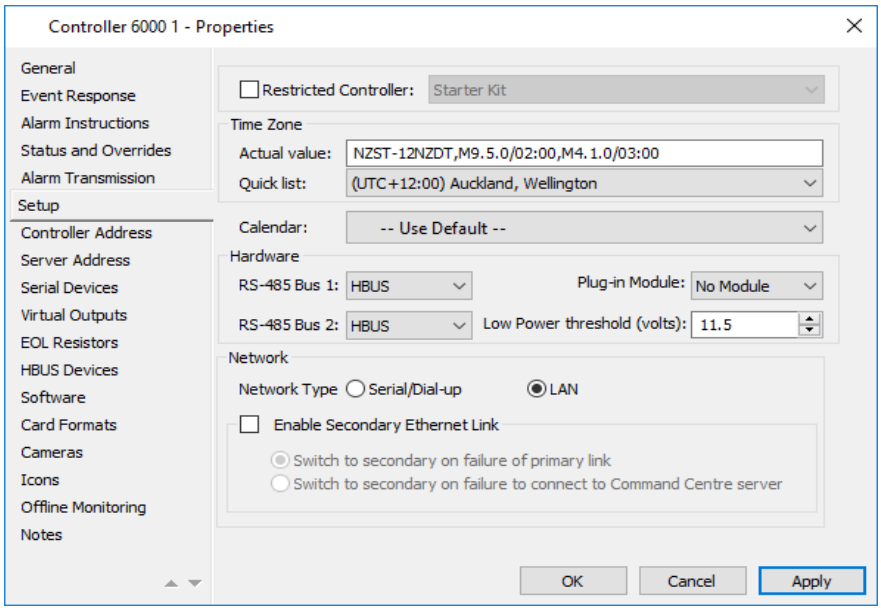
Assigning an OSDP Compliant Reader to a Gallagher Controller

Introduction

This procedure describes how to assign an Open Supervised Device Protocol (OSDP) compliant reader, (i.e. either an **OSDP Reader** or **Morpho Biometric Reader** type in Command Centre) to a Gallagher Controller.
Important: It is recommended you set up the initial connection between a Controller and reader in a secure environment, i.e. connection is made secure via physical security, such as controller/reader are connected via simple short cable. The secure connection is asserted to both the controller and reader by setting the devices into installation mode. For the reader this means using the manufacturer's defined method, and for the controller it occurs automatically when the reader is configured for the first time on that controller, or when a **Re-initialise encryption** override is performed.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Controller you want to assign the new OSDP or Morpho Biometric Reader to.
3. **Right click** and select **Properties.**
   By default the **General** tab displays.
4. Click the **Setup** tab.

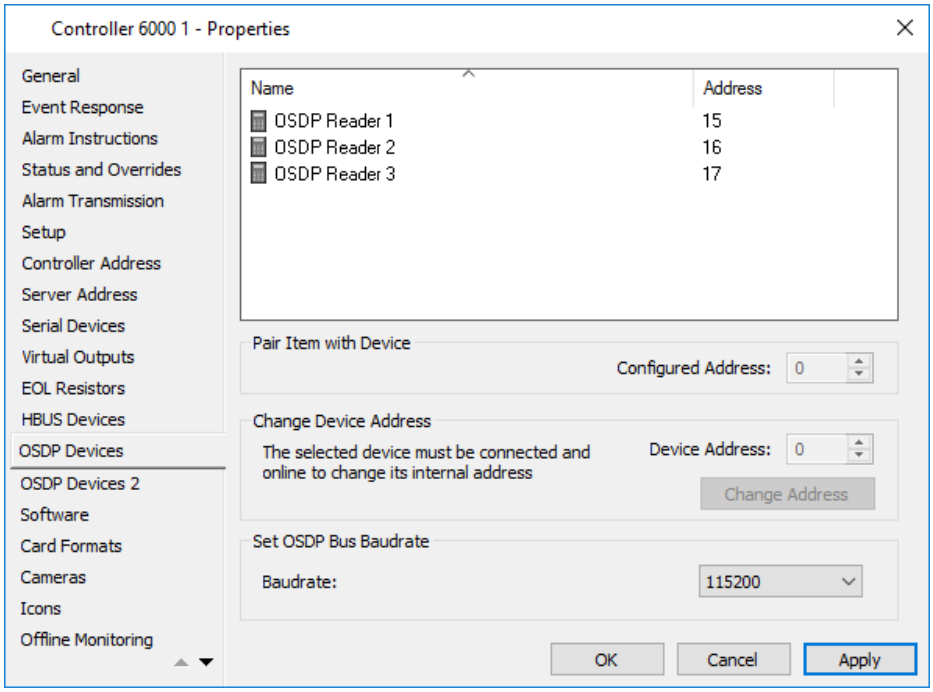


5. In the Hardware section of this screen, select the 'OSDP' option from the **RS-485 Bus 1** and/or **RS-485 Bus 2** drop-down lists as appropriate.
   Depending on which RS-485 Bus option(s) you selected 'OSDP' for, an **OSDP Devices** and/or **OSDP Devices 2** tab appears, allowing you to add up to 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, split across runs - maximum 16 readers per run.
- **Controller 7000:** Supports up to 32 OSDP and/or Morpho Biometric readers, split across runs - maximum 16 readers per run.

6. Click the **OSDP Devices** tab.



7. From the **Hardware** List Window, select the OSDP Readers and/or Morpho Biometric Readers attached to this Bus. Drag and drop each Reader into the grid on the **OSDP Devices** tab.
8. Pair the item with the device by selecting the appropriate reader from the grid and entering the address into the **Configured Address** field below. (Address Range = 0 - 126)
9. If you want to change the device address, select the appropriate reader from the grid and enter an address into the **Device Address** field below. Click the **Change Address** button to push the configuration. (Address Range = 0 - 126)
   Note: The Change Device Address controls will be disabled if the selected device's status is offline, unknown or unconfigured.
10. 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.

Result

An OSDP Reader or a Morpho Biometric Reader has been created and it has been assigned to a Gallagher Controller. As a result, the following occurs:

- the Reader will display within the Hardware List Window.
- on the **Connections** tab of the Reader, the Gallagher Controller name will appear in the **Connected to** field.

Moving OSDP Readers between Controllers

To move an ODSP Compliant Reader from one Controller to another (within the same site) simply move that Reader FT Item from one Controller to another and swap the physical connections.

Should you need to move an OSDP Compliant Reader between sites, the reader will need to be placed into installation mode (as specified by the manufacturer), as it will have a secure key loaded. When the reader is configured on its new controller, it will get an "Encryption Keys tampered" status/event because communications are attempted to be initialised with the secure key, however it will not relate to the new FT Items Master Key.

A **Re-initialise encryption** override will need to be performed which will effectively put the controller into Installation mode, so a new key can be negotiated. The same procedure is used for replacing a reader, as it would result in the same issue, (i.e. either the reader had a secure key or it did not, but it was an incorrect one).

Chapter 80: QR Code Readers

Introduction

QR Code Readers can be connected to Gallagher Command Centre and configured as third party readers, for the purpose of providing access control for areas with lower security requirements, or where the access may be temporary, (e.g. access to cafeterias, meeting rooms, lockers, etc.).

This topic is separated into individual procedures to cover the whole process involved in configuring QR Code Readers to work with Gallagher Command Centre. The procedures, in the order they should be performed, are:

- Connecting and configuring a QR Code Reader
- Creating a new third party reader
- Assigning the reader to the Controller
- Configuring the Card Type

Procedure

Connecting and configuring a QR Code Reader

1. Physically connect the QR Code Reader to a Gallagher Controller as a Wiegand Reader.
   For Wiegand Reader connection details, refer to the Gallagher Controller installation note.

Red – Power	Green – Data 0	Orange – LED 0
Blue – Ground	White – Data 1	Yellow – LED 1

2. Print off the six configuration barcodes on page 79-5, and badge them at the reader.
   Note: If you have a number of QR Code Readers, you may find it easier to badge the barcodes before installing the readers.

Creating a new third party reader

Create a new third party reader for the QR Code Reader in the Configuration Client, as follows:

3. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
4. **Right click** and select **New...Third Party Reader**.
   By default the **General** tab displays.
5. Enter a Name and Description, and select the division for this QR Code Reader.

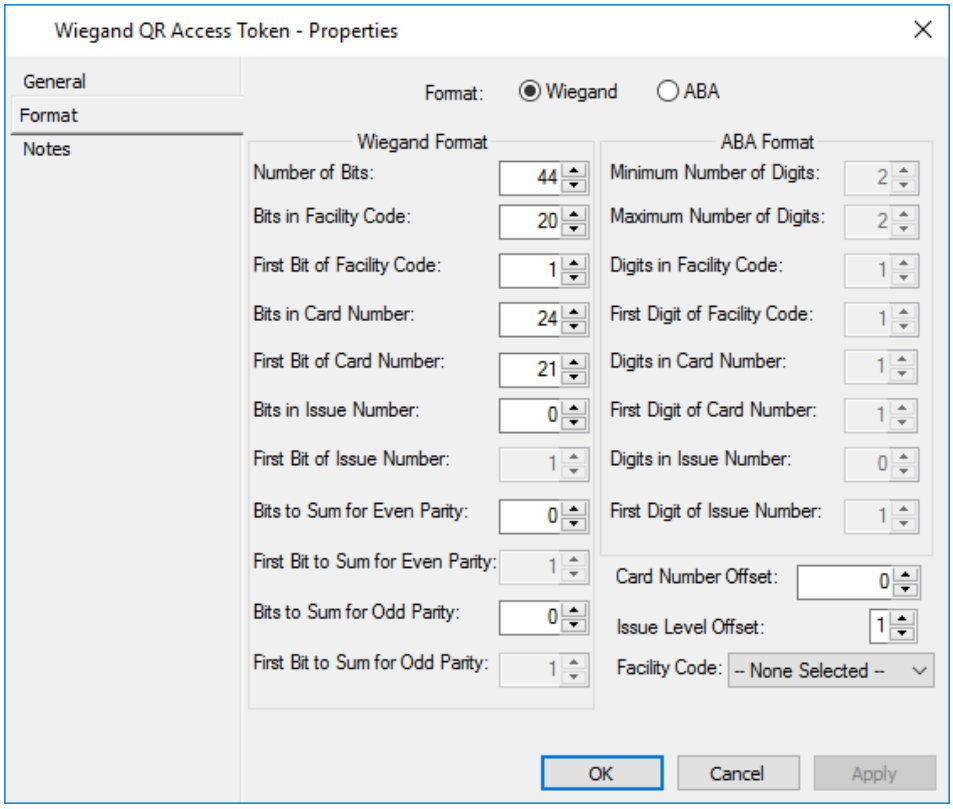
6. Configure the remaining tabs as required, and click the **OK** button.

Assigning the reader to the Controller

Assign the newly created third party reader to a Controller in the Configuration Client, as follows:

7. From the **Hardware** List Window, open the property pages for the Controller that the third party reader will be assigned to.
8. Click the **Readers** tab.
9. Assign the newly created QR Code Reader (third party reader) to the appropriate slot.
   Note: Only slots 1, 3, 5 or 7 can be used.
10. Click the **Card Formats** tab.
11. On the **Universal Card Format** List Window, highlight the 'Wiegand QR Access Token' Universal Card Format, and drag and drop it into the grid on the **Card Formats** tab of the Controller.

    Note: If the 'Wiegand QR Access Token' Universal Card Format is deleted in error, the QR reading process will not work. The UCF would need to be re-created as shown below:



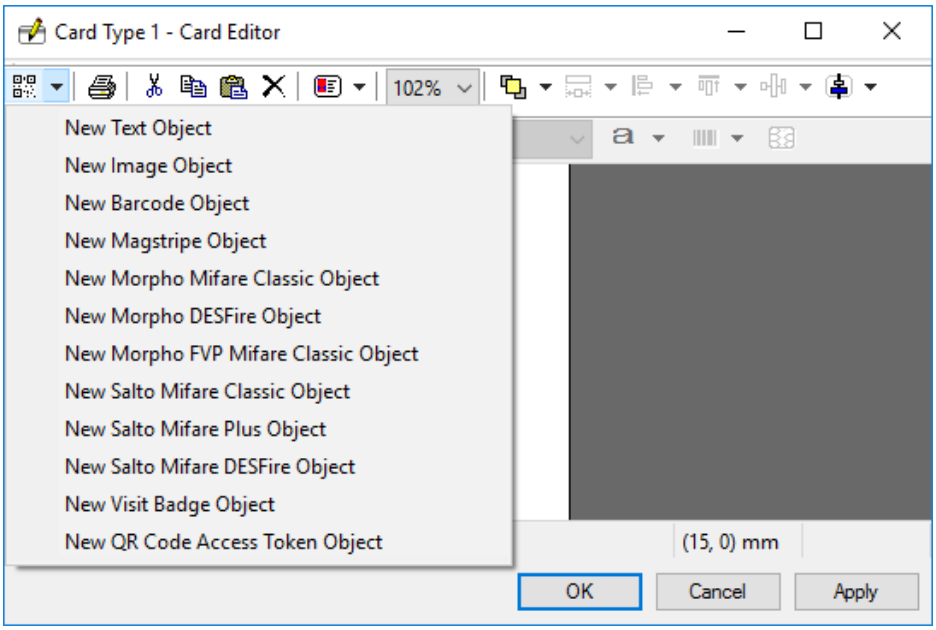
12. Click the **OK** button.
    The QR Code Reader is now set up to read QR Codes created by the Gallagher system and the Controller can make access decisions relative to the cardholders access.

Configuring the Card Type

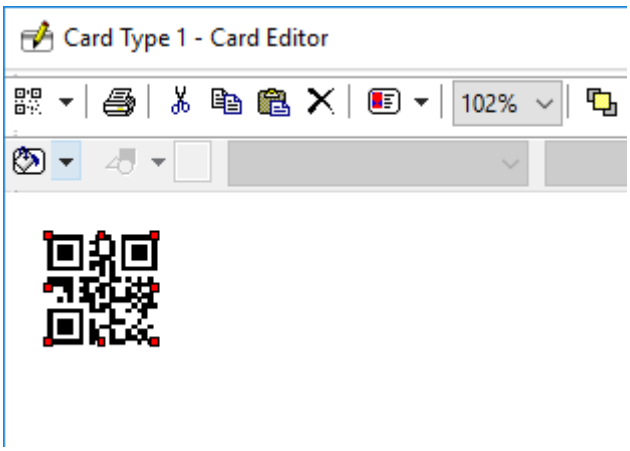
The QR code is data derived from the cardholders "Card number and Facility code". This needs to be set up as an object in the Card type configuration, in the Configuration Client, as follows:

13. Click **Configure** from the menu bar, then **Card Types**.
    The **Card Type** List Window opens.
14. **Right click** on the Card Type you want to add the QR Code to, and select **Edit Card Layout**.
    The Card Editor window displays.

    Note: QR Codes can only be applied to a Card Type configured with Decimal card numbers, (i.e. "Decimal" is selected for the **Format** on the Card Type's **Setup** tab).
15. Select **New QR Code Access Token Object** from the drop-down list of object types.



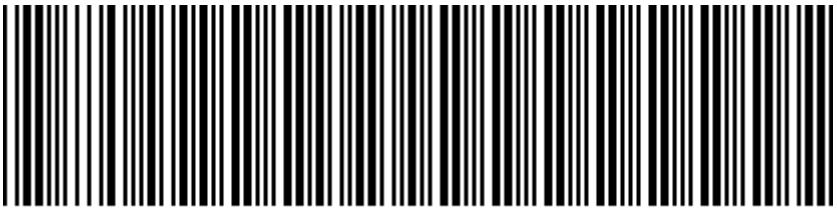
A QR barcode image displays with placeholders around it.

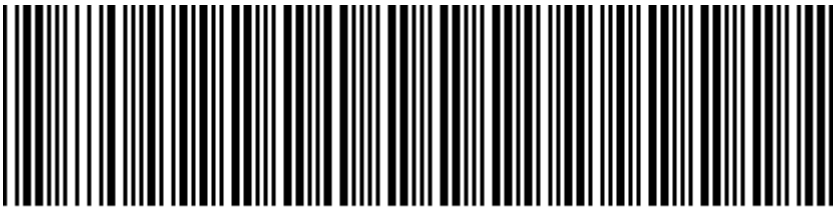


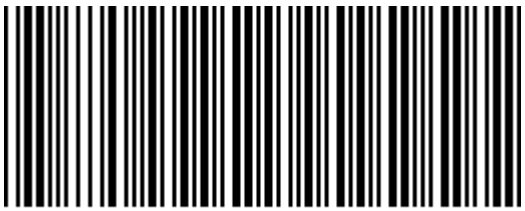
16. Resize and reposition the barcode as required. See ***Expanding an Object Box*** and/or ***Moving Objects*** (both on page 48-18) for the procedure.
17. Make further modifications to the card, (e.g. add a background or another object), if necessary. See ***Designing Card Layouts*** (on page 48-13) for further details.
18. Click the **OK** button.
    The Card Editor window close.

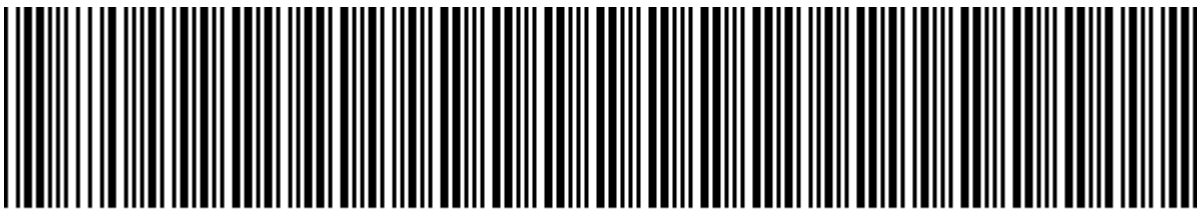
Now when this card type is assigned to a Cardholder and Printed/Copied, this QR code will act as an access code for the configured QR readers for as long as the Cardholders access is configured, (e.g. active card, access group membership, etc.).

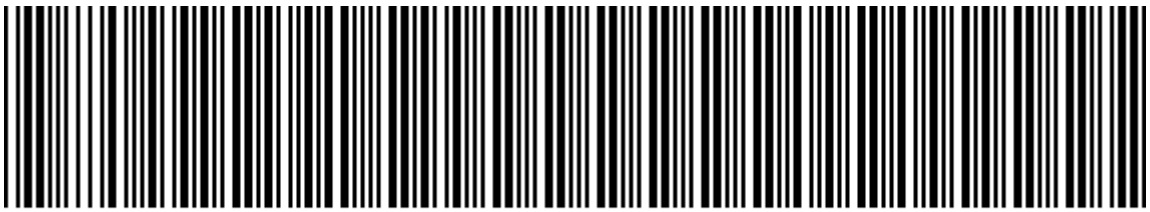
Note: This is a low security option. There is nothing to prevent this code being copied and distributed multiple times.
If the desire is to provide temporary access, then limiting the time is dependant on Card Expiry and or Access Group expiry against specific Cardholders.


%UX00110000000


%UX00600011000


%UX01400


%UX015100000001080009


%UX01608000000202400


%UX0170000000001200

Chapter 81: ThyssenKrupp Insight Elevator Systems

Introduction

ThyssenKrupp Insight Elevator Systems are configured using Command Centre Configuration Client.

Prerequisites

Prior to configuring a ThyssenKrupp Insight Elevator System, the Gallagher Elevator Service must be installed and configured using the Gallagher Elevator Service Configuration Utility.

For further detail refer to the document "Release Note Elevator Service.pdf" located in the `'Utilities'` directory of the Command Centre installation media.

Using the Embedded ThyssenKrupp Card Readers with Elevators and Kiosks

Command Centre supports the use of readers embedded in the Kiosks and Elevators panels. No configuration is required for the Kiosks or Elevators but the appropriate Universal Card Format must be configured on each controller that has a Kiosk or Elevator assigned to it.
The readers are treated as if they are a Third Party Wiegand reader, so the chosen UCF should match the data encoded on the card.

Licensing

ThyssenKrupp Insight Elevator Systems functionality is a licensable feature. The license file must contain the following option:

```
[Features]
ThyssenKrupp EthernetHLI=1
```

The number of Kiosks is also licensed:

```
[Features]
ThyssenKrupp Kiosks=n
```

`[n]` indicates the number of Kiosks that can be created

This chapter covers the following topics:

- ***Configuring a ThyssenKrupp Insight Elevator System*** (on page 81-2)
- ***Configuring a ThyssenKrupp Elevator Group*** (on page 81-5)
- ***Configuring a ThyssenKrupp Elevator*** (on page 81-10)
- ***Creating an Elevator Kiosk Control Schedule*** (on page 81-12)
- ***Configuring a ThyssenKrupp Kiosk*** (on page 81-14)

Configuring a ThyssenKrupp Insight Elevator System

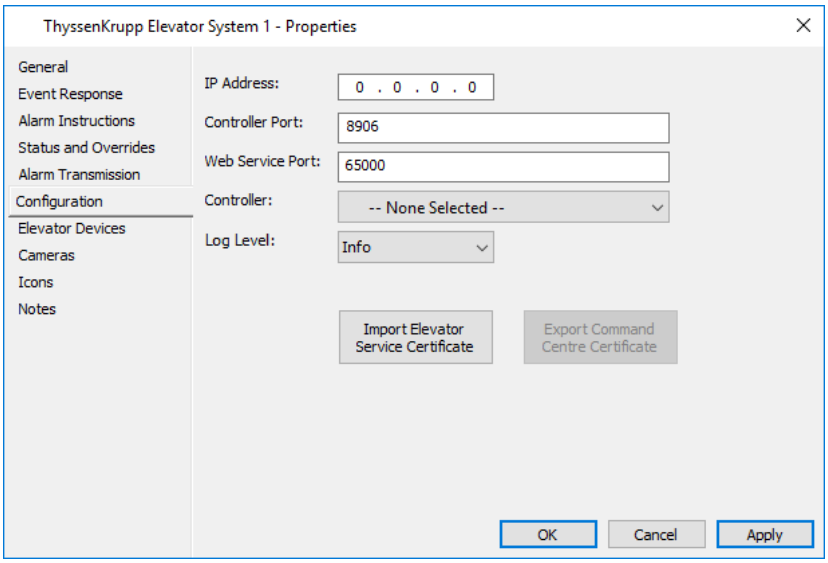
Introduction

This procedure enables an operator with either the "Advanced User" or "Edit Site" privilege to configure a ThyssenKrupp Insight Elevator System.

Configuration

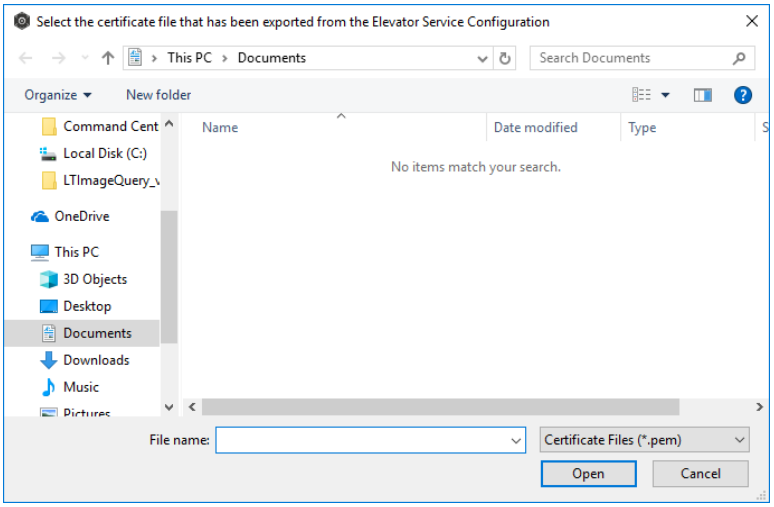
To configure a ThyssenKrupp Insight Elevator System, perform the following procedure in Gallagher Configuration Client:

1. Click Configure from the menu bar, then **Elevator Systems**.
   The **Elevator Systems** List Window opens.
2. Right click and select **New...ThyssenKrupp Elevator System.**
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Configuration** tab.

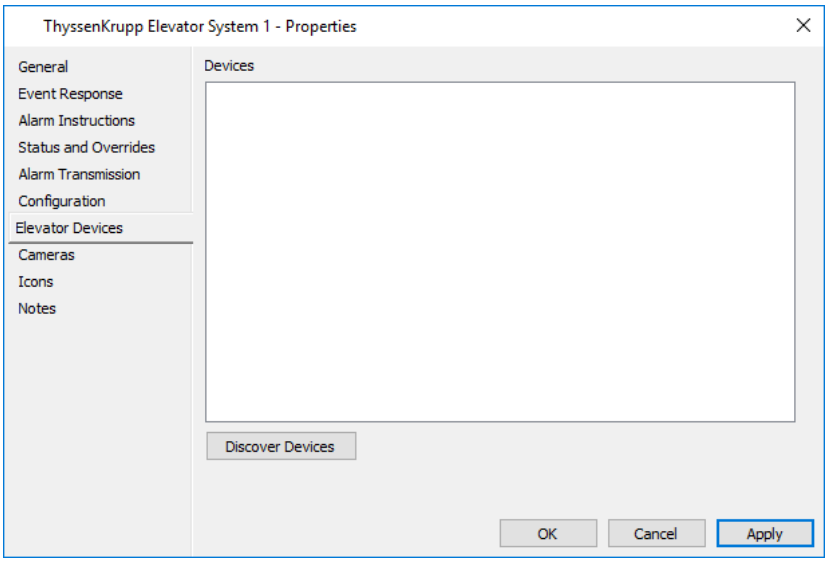


5. Input the **IP Address**, Controller Port and **Web Service Port** of the PC hosting the Elevator Service.
6. Select a **Controller** from the drop-down list and Save the changes so that one TKSystemPart will be created on the specified Controller.
7. The **Log Level** will be set to 'Info' by default. This setting controls the volume of information logged by the Elevator Service and should only be changed when diagnosing problems in cooperation with Gallagher Technical Support.
8. Click the **Import Elevator Service Certificate** button to import the certificate.

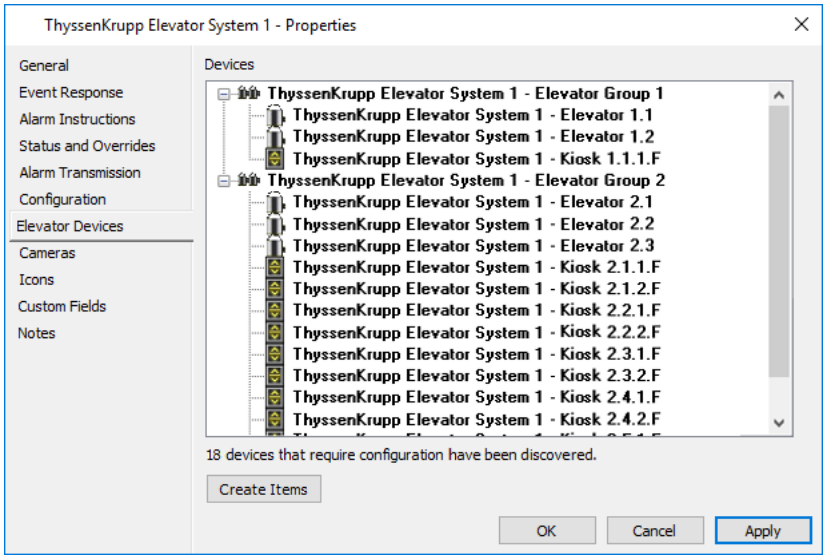
9. From the displayed pop-up window, path your way to the certificate file (***.pem**) that was generated and exported from the Elevator Service Configuration Utility.



10. Click the **Open** button.
11. Export the certificate which will be imported by the Elevator Service Configuration Utility later.
12. Report ThyssenKrupp Insight Elevator system online and offline events.
13. Update ThyssenKrupp Insight Elevator system status.
    By default, when it becomes offline, an alarm should be raised. When it is back to normal, the active status should change back to normal.
14. Click the **Elevator Devices** tab.



15. Click the **Discover Devices** button.
    All enabled devices advertised to the Elevator Service will be displayed. Devices that have not yet been configured in the Command Centre System will be displayed in bold text. Those that have been configured will be displayed with their configured name in normal text.



Clicking the **Create Items** button will create the Elevator Group, Elevator and Kiosk items, populating the Elevator Systems List Window.
These items will be assigned the ThyssenKrupp System's division and Alarm Zone and can be configured later.

16. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Elevator System.
    For further details see ***Cameras tab*** (on page 3-24).
17. Click the **Icons** tab if you want to change the Icon Set for this Elevator System.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
18. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Elevator System.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
19. Click the **Notes** tab if you want to add a note(s) about this Elevator System.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
20. 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.

Result

A ThyssenKrupp Insight Elevator System is configured.

Configuring a ThyssenKrupp Elevator Group

Introduction

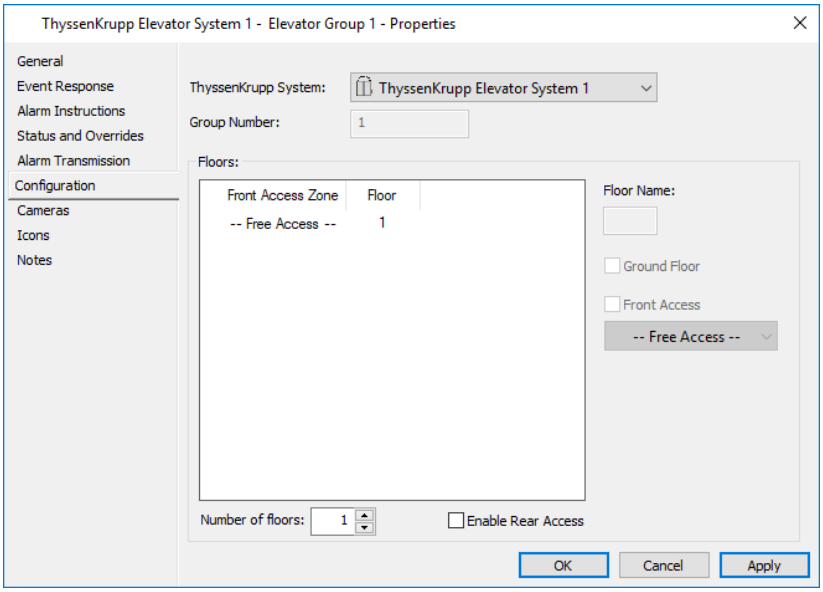
In a ThyssenKrupp Insight Elevator System, an Elevator Group is a collection of elevators and kiosks which service the same set of floors. They consist of 1-15 elevator controllers which are each allocated a unique elevator car number in the range 1-15.

This procedure enables an operator with either the "Advanced User" or "Edit Site" privilege to configure a ThyssenKrupp Elevator Group.

Configuration

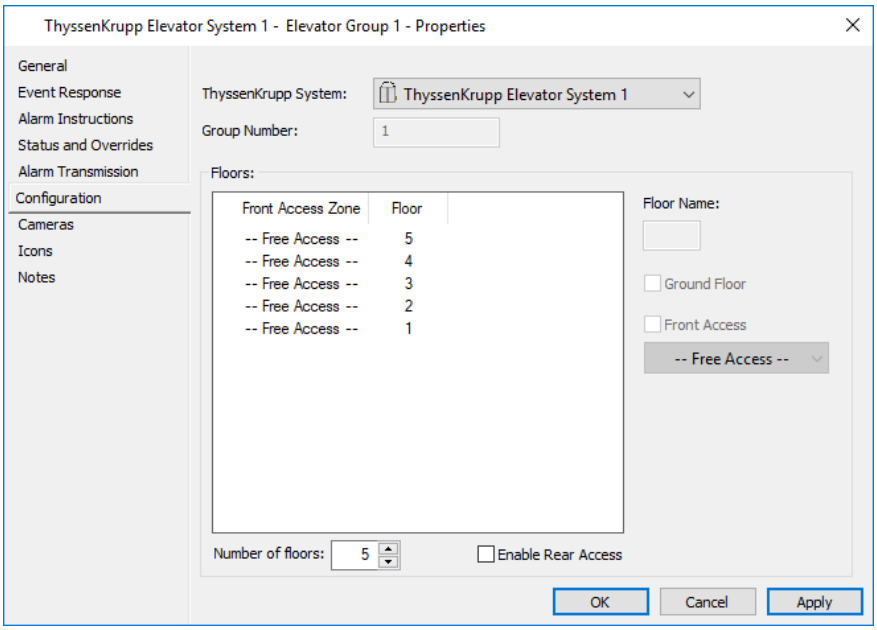
To configure a ThyssenKrupp Elevator Group, perform the following procedure in Gallagher Configuration Client:

1. Click Configure from the menu bar, then **Elevator Systems**.
   The **Elevator Systems** List Window opens.
2. ThyssenKrupp Elevator Group items are created using the Discovery feature described in the *Configuring a ThyssenKrupp Insight Elevator System* procedure.
   Locate the Elevator Group item in the List Window as a child of the ThyssenKrupp System item and open the property sheet as usual. The ThyssenKrupp System's child items may need to be expanded by clicking the **+** button beside its name. The **General** tab will display by default.
   Note: ThyssenKrupp Elevator Group items are created by using the Elevator Devices tab as described in ***Configuring a ThyssenKrupp Insight Elevator System*** (on page 81-2).
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Configuration** tab.

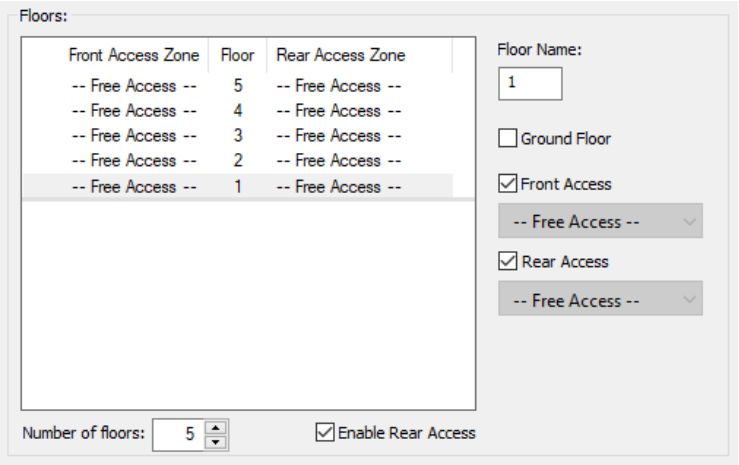


The ThyssenKrupp System or Group number are set when the group is created and cannot be changed.

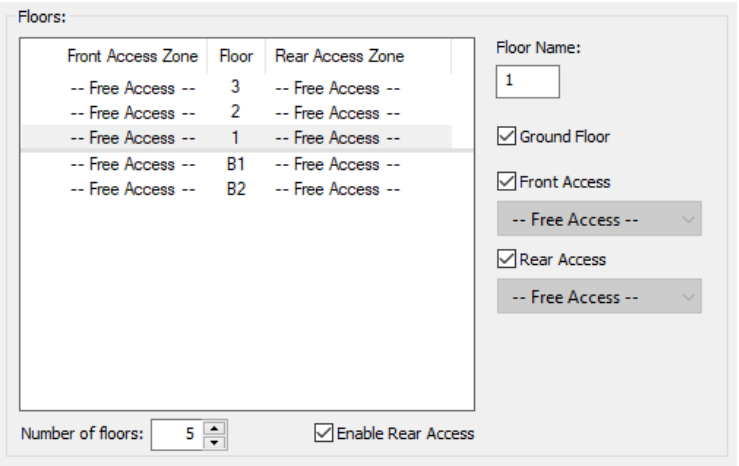
5. Enter or select the **Number of floors** in the building accessed by the elevator group, (range 1-128).
   This automatically populates the grid with the required number of Floors listed, bottom to top, as they would be in an elevator. By default, floors are set to **-- Free Access --** allowing any passenger to go to that floor.



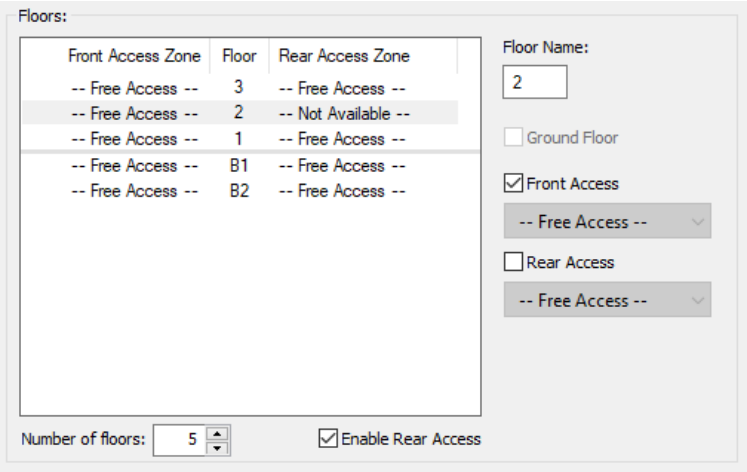
6. If the elevators in this Elevator Group open front and back (opposite sides), check the **Enable Rear Access** checkbox. Rear access properties are then available for configuration.



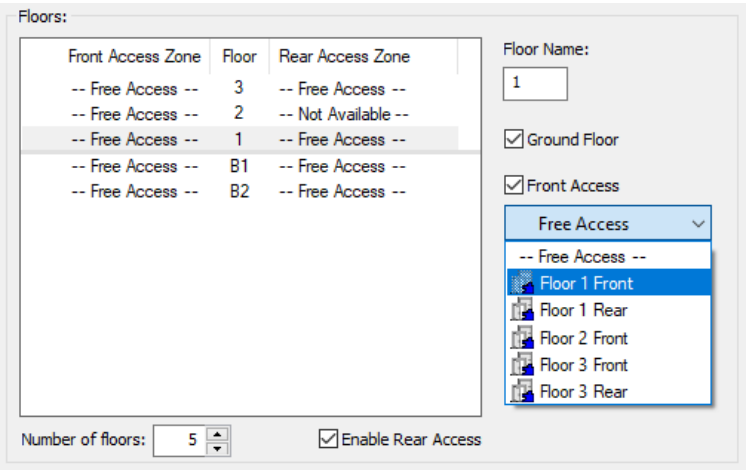
If required, select the floor in the grid that is on ground level and check the **Ground Floor** checkbox.
A line appears underneath that floor indicating that it is the ground floor and floors below this will be re-labelled to indicate that they are basement floors.



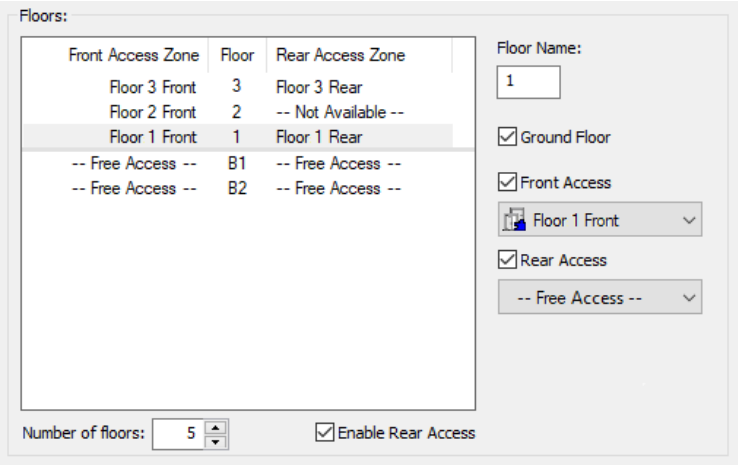
7. Change the **Floor Name** to a four-character label if required.
   Note: The system does not allow duplicates.
8. If the elevator group does not service a building floor, untick the **Front Access** or **Rear Access** checkbox.
   The access will change to **-- Not Available --**.



9. If a floor is access controlled, check the **Front Access** checkbox, (and **Rear Access** checkbox if applicable), and select the Access Zone that represents the area outside the elevator on this particular floor from the drop-down list.
   Note: Access Zones can also be dragged from the Access Zones List Window or the Find Tool and dropped directly on the cell in the **Floors** grid.



10. Keep selecting rows (or floors) and repeating Step 10 until an Access Zone has been selected for each Floor to which access is controlled by Command Centre.
    Note: If you do not select an Access Zone for a Floor, this means the associated floor is in Free Access mode.



In this example, **Floor 1 Front** is the area outside the front access on Floor 1 (the 3rd building floor), and **Floor 3 Rear** is outside the rear access on Floor 3 (the 5th building floor).

11. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Elevator Group.
    For further details see ***Cameras tab*** (on page 3-24).
12. Click the **Icons** tab if you want to change the Icon Set for this Elevator Group.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
13. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Elevator Group.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
14. Click the **Notes** tab if you want to add a note(s) about this Elevator System.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
15. Click OK to exit and save your changes.
    Click Ca**ncel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

A ThyssenKrupp Elevator Group is configured.

Configuring a ThyssenKrupp Elevator

Introduction

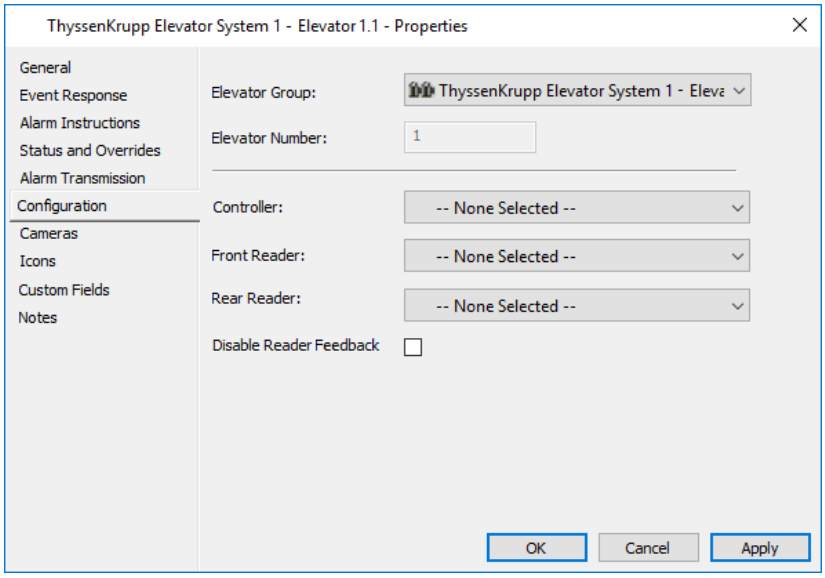
The ThyssenKrupp Elevator Item represents an Elevator that may contain up to two floor selection panels (Front and Rear), with or without associated readers.

This procedure enables an operator with either the "Advanced User" or "Edit Site" privilege to configure a ThyssenKrupp Elevator.

Configuration

To configure a ThyssenKrupp Elevator, perform the following procedure in Gallagher Configuration Client:

1. Click Configure from the menu bar, then **Elevator Systems**.
   The **Elevator Systems** List Window opens.
2. ThyssenKrupp Elevator items are created using the Discovery feature described in the *Configuring a ThyssenKrupp Insight Elevator System* procedure. Locate the Elevator item in the Elevator Systems List Window as a child of the ThyssenKrupp Elevator Group item and open the property sheet as usual. The ThyssenKrupp System or Elevator Group child items may need to be expanded by clicking the **+** button beside its name. The **General** tab will display by default.
3. **Note:** ThyssenKrupp Elevator items are created by using the Elevator Devices tab as described in ***Configuring a ThyssenKrupp Insight Elevator System*** (on page 81-2).
4. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
5. Click the **Configuration** tab.



The ThyssenKrupp Elevator Group and Elevator number are set when the elevator is created and cannot be changed.

6. Select the **Controller** that will be making access decisions for this elevator from the drop-down list.
7. If this elevator has reader(s) installed in it, select them from the **Front Reader** and **Rear Reader** drop-down lists.
   Note: The **Rear Reader** field will be disabled if the elevators in this Elevator Group do not open front and back (opposite sides).
8. Check the **Disable Reader Feedback** checkbox if this is desired.
9. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this elevator.
   For further details see ***Cameras tab*** (on page 3-24).
10. Click the **Icons** tab if you want to change the Icon Set for this elevator.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
11. Click the **Custom Fields** tab if you want to add and assign a custom field value to this elevator.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
12. Click the **Notes** tab if you want to add a note(s) about this elevator.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
13. 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.

Result

A ThyssenKrupp Elevator is configured.

Creating an Elevator Kiosk Control Schedule

Introduction

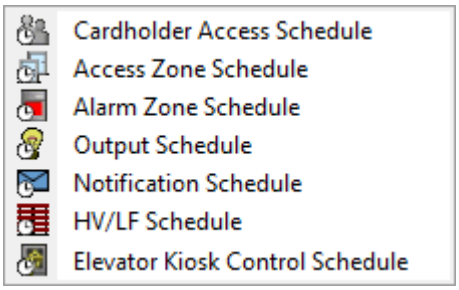
Elevator Kiosk Control Schedules control whether the source control is active or inactive, allowing the source control to be time dependant.

If you intend assigning Elevator Kiosk Control Schedules to floors of a ThyssenKrupp Kiosk, the Elevator Kiosk Control Schedules need to be configured before configuring the **Source Control** tab of the ThyssenKrupp Kiosk.

Configuration

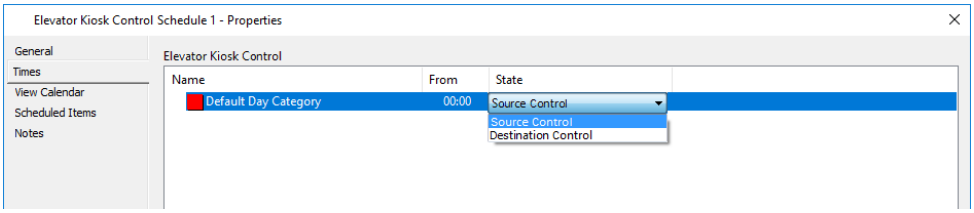
To configure an Elevator Kiosk Control Schedule, perform the following procedure in Gallagher Configuration Client:

1. Click **Configure** from the menu bar, then **Schedules**.
   The **Schedule** List Window opens.
2. **Right click** and select **New...Elevator Kiosk Control Schedule**.



Note: The Elevator Kiosk Control Schedule type only appears if your site is licensed for ThyssenKrupp Elevator Systems.

3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Times** tab.



This tab provides a grid where 'From' times and states can be entered/edited for each Day Category. There are only two states available, (i.e. 'Source Control' and 'Destination Control').

5. Add and remove any other Day Categories required for this Schedule. See ***Adding Day Categories to Schedules*** (on page 12-6) and ***Removing Day Categories from Schedules*** (on page 12-7) for procedures.
6. Add, remove or change the times and states of each Day Category as required. See ***Changing times and states within Schedules*** (on page 12-8) for procedure.
7. 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.

Result

An Elevator Kiosk Control Schedule is created.

Configuring a ThyssenKrupp Kiosk

Introduction

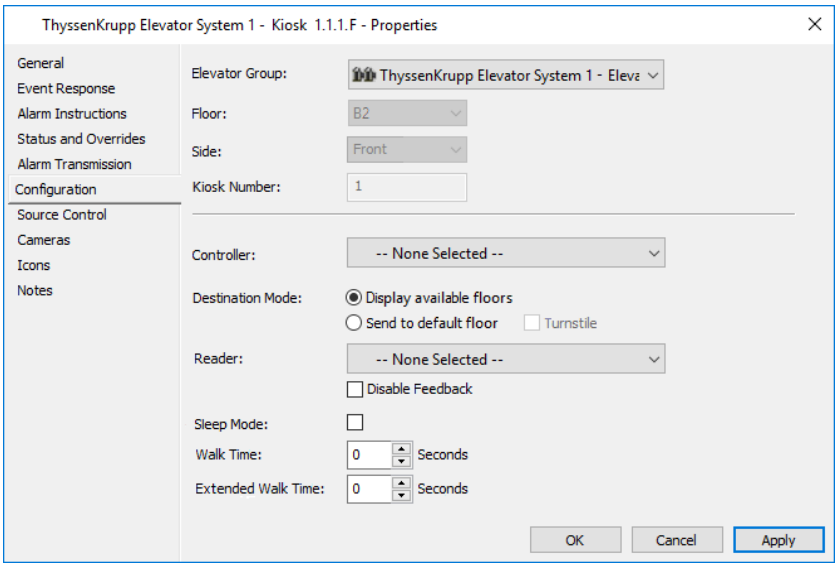
Kiosks tend to be situated in lobbies / waiting areas on different floors outside of an elevator. The ThyssenKrupp Kiosk Item represents a kiosk, with or without associated readers.

This procedure enables an operator with either the "Advanced User" or "Edit Site" privilege to configure a ThyssenKrupp Kiosk.

Configuration

To configure a ThyssenKrupp Kiosk, perform the following procedure in Gallagher Configuration Client:

1. Click Configure from the menu bar, then **Elevator Systems**.
   The **Elevator Systems** List Window opens.
2. ThyssenKrupp Kiosk items are created using the Discovery feature described in the *Configuring a ThyssenKrupp Insight Elevator System* procedure. Locate the Kiosk item in the Elevator Systems List Window as a child of the ThyssenKrupp Elevator Group item and open the property sheet as usual. The ThyssenKrupp System or Elevator Group child items may need to be expanded by clicking the **+** button beside its name. The **General** tab will display by default.
   Note: ThyssenKrupp Kiosk items are created by using the Elevator Devices tab as described in ***Configuring a ThyssenKrupp Insight Elevator System*** (on page 81-2).
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Configuration** tab.

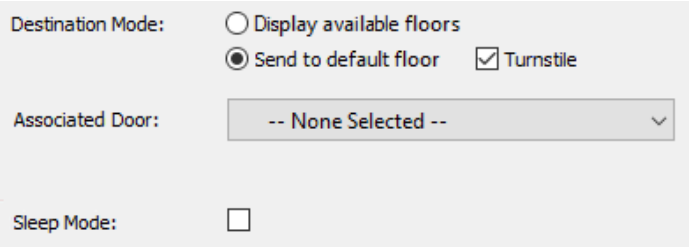


The ThyssenKrupp Elevator Group, Floor, Kiosk Number and Side are set when the kiosk is created and cannot be changed.

5. Select the Controller that will be making access decisions for this kiosk from the drop-down list.
6. The behaviour of the kiosk on how it directs a cardholder to a floor can be changed via the **Destination Mode** radio button you select.
   Click the appropriate radio button:

If you select…	then…
Display available floors,	it disregards any designated default floor for a cardholder by displaying all available floors.
Send to default floor,	the **Turnstile** checkbox becomes enabled. Is the site using turnstiles in conjunction with the Kiosk? If **no**, go to Step 7. If **yes**, go to Step 9.

7. Select the **Reader** associated with the kiosk from the drop-down list.
   As soon as the cardholder badges, they will be directed to a particular elevator which will take them to the default floor without any further interaction.
   Note: If you want to to use an integrated DED reader with the kiosk, configure as follows:
   a) Leave the **Reader** as "-- None selected --".
   b) Add the appropriate UCF to the Controller **Card Formats** tab.
      Note: Ususally the 'Weigand 26/8 bit' UCF will work.
8. Check the **Disable Feedback** checkbox to prevent commands (display prompts, icons, LEDs, and playing tunes) from being sent to the reader(s). These commands would normally be associated with access attempts when a cardholder presents their card.
   Go to Step 11.
9. Check the **Turnstile** checkbox.
   The **Reader** field below it changes to **Associated Door**, and the **Disable Feedback** checkbox disappears.



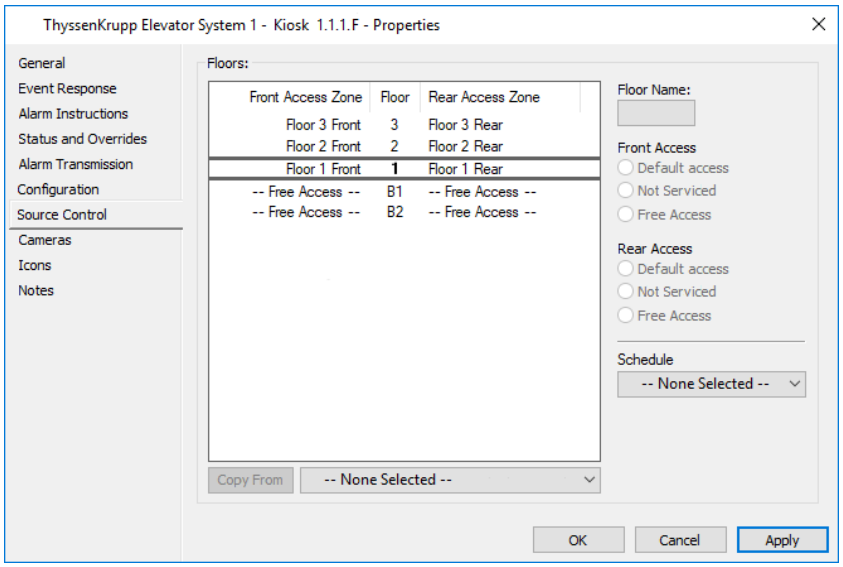
10. Select the door associated with the kiosk from the **Associated Door** drop-down list. This allows a door to be associated with the kiosk to perform the access granted behaviour required for setting up a Turnstile.
11. Check the **Sleep Mode** to enable the sleep mode on the Kiosk.
    Sleep mode requires that a passenger badges their card to 'wake up' the kiosk before they select a floor.
12. Configure the Walk Time and Extended Walk Time settings as appropriate. (Range = 0 - 255 seconds)

Setting	Function
Walk Time	The estimated time it takes to walk from the kiosk to the elevator.
Extended Walk Time	The estimated additional time it takes an ADA passenger to walk from the kiosk to the elevator.

Notes:

- While the allowable range for both **Walk Time** and **Extended Walk Time** is 0 - 255 seconds, the maximum **combined value** of both fields can be no more than 255 seconds.
- These times are only taken into consideration when the Register Call messaging is used for the Default Floor Feature.

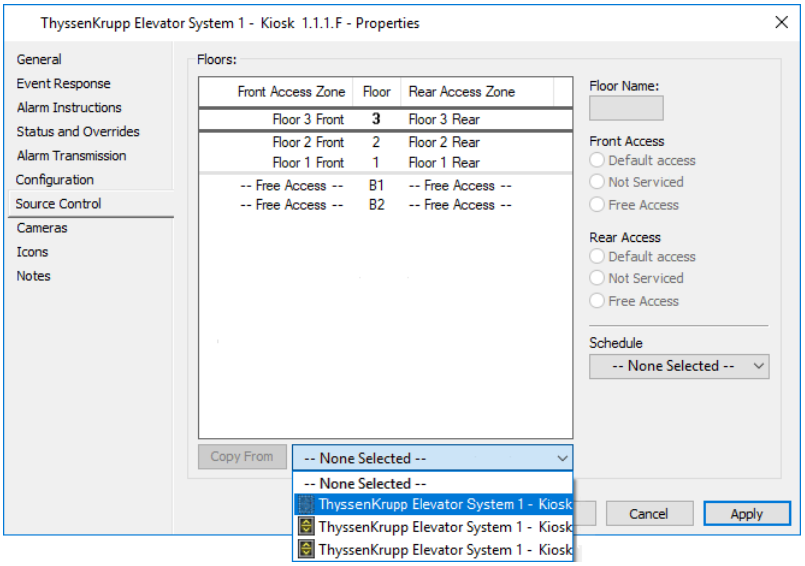
13. Click the **Source Control** tab.



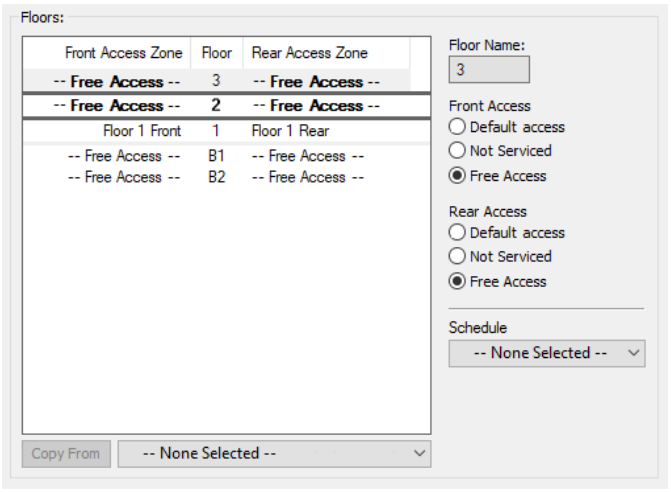
This tab allows a site to set different access options for the kiosk in different parts of the building.

The **Floors** grid is initially populated with the floor map from the Elevator Group the kiosk is a member of, and the two borders indicate which floor the kiosk is on, (e.g. Floor 1 in the screen shot above).

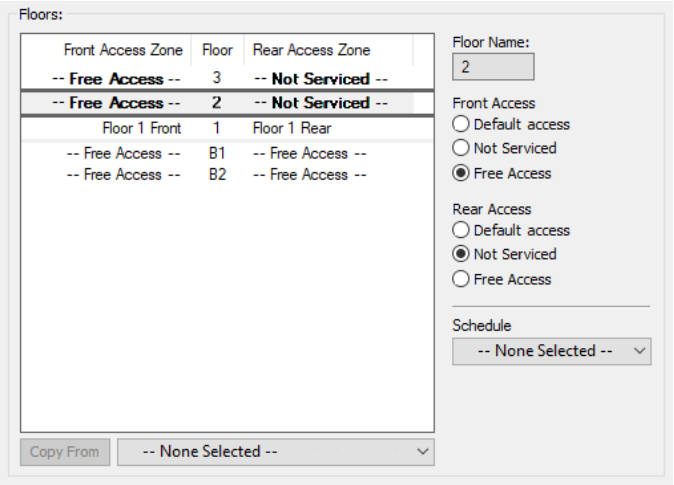
14. If you want to update the kiosk with the same Source Control settings as another kiosk, click the **Copy From** button, and select the appropriate kiosk from the drop-down list next to the button.
    Note: The drop-down list will be restricted to kiosks with Source Control within the Elevator Group.



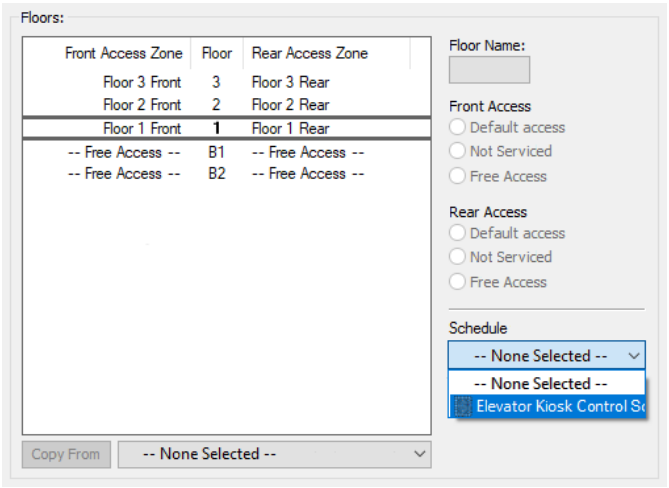
15. To enable free access between floors, (e.g. Floors 2 and 3 in the screen shot below), select each floor requiring free access in turn, and click the **Free Access** radio buttons for Front and Rear Access.
    Note: The changes show in **bold** before saving.



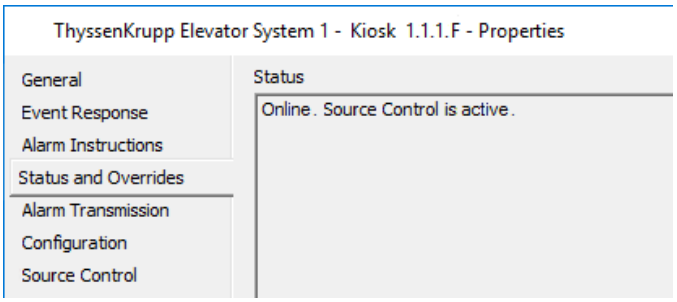
To enable free access only to the front and NOT the rear between floors 2 and 3, click the **Free Access** radio button for Front Access and the **Not Serviced** radio button for Rear Access.



16. If you want to assign an Elevator Kiosk Control Schedule to a floor, select the appropriate one from the **Schedule** drop-down list.
Note: If you intend assigning Elevator Kiosk Control Schedules to the kiosk, the schedules need to be created first. See ***Creating an Elevator Kiosk Control Schedule*** (on page 81-12) for the procedure.



The state configured in the schedule you select, (i.e. either 'source control' or 'destination control' state) will now be active on the kiosk.
Note: The **Status and Overrides** tab of the kiosk will show whether source control or destination control is active at the moment.



17. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this kiosk.
For further details see ***Cameras tab*** (on page 3-24).

18. Click the **Icons** tab if you want to change the Icon Set for this kiosk.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
19. Click the **Custom Fields** tab if you want to add and assign a custom field value to this kiosk.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
20. Click the **Notes** tab if you want to add a note(s) about this kiosk.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
21. 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.

Result

A ThyssenKrupp Kiosk is configured.

Chapter 82: HALO Smart Sensor Integration

Introduction

The Gallagher HALO Smart Sensor Integration provides an integration between HALO Smart Sensor devices and Gallagher Command Centre. Command Centre operators can monitor HALO Smart Sensors from within Command Centre Client. When a HALO Smart Sensor sends an alert, an alarm is raised in Command Centre, with details of what the HALO device has detected.

Site Plans

You can add HALO Devices to Site Plans in Command Centre Client only. When a HALO Device is in an alarm state, it flashes on the Site Plan with a colour to represent the alarm priority. The alarm can be viewed and processed from the Site Plan.

Reports

You can configure Activity Reports to report on alarms raised by HALO Devices. You can filter the report by the type of HALO Alarm, (e.g. 'HALO gunshot alert' events).

Events

The Gallagher HALO Smart Sensor Integration makes use of the 'Integrated Device Events' Event Group and its 'HALO' Event Types. The HALO Event Types correspond to the various HALO Smart Sensor alerts (e.g. aggression, air quality) and all have various default Action Plans (alarm priorities) which can be changed. All HALO Device alarms are raised as active alarms. If your site needs to change how HALO events are raised in Command Centre (e.g. change the event message, raise them as inactive), this can be achieved with the help of the Gallagher Support Team.

HALO configuration: To enable HALO alarm functionality in Command Centre, HALO Smart Sensors must be configured to set and reset each event message within their 'Actions' configuration. Refer to the HALO Administrator Manual for instructions.

Alerts while device offline: If a HALO Device is offline in Command Centre, any alerts the device raises while it is offline are *not* raised as events in Command Centre when the device comes back online.

More information

For further detail, refer to the document **"Release Note HALO Smart Sensor Integration (vx.xx).pdf"** located in the `'Utilities\System Interfaces'` directory of the Command Centre installation media.

Appendices

This part of the User Guide includes the following Appendices:

- **Appendix A: Country Codes**
- **Appendix B: XYZ Event Mappings**
- **Appendix C: CCC Identifiers**

Appendix A: Country Codes

The Country Code needs to be set for an Alarm Dialler.
The following is a list of all the Country Codes supplied. You will note that most countries are Country Code 52.

Code	Country
01	Australia
09	New Zealand
16	Japan
48	Hong Kong
	Hungary
	India
	Indonesia
	Israel
	Korea-Democratic People's Republic of
	Malaysia
	Philippines
	Poland
	Singapore
	Slovenia
	Vietnam
52	Afghanistan
	Albania
	Algeria
	American Samoa
	Andorra
	Angola
	Anguilla Antarctica
	Antigua & Barbuda
	Argentina
	Armenia
	Aruba
	Austria
	Azerbaijan
	Bahamas
	Bahrain
	Bangladesh
	Barbados
	Belarus
	Belgium
	Belize
	Benin
	Bermuda
	Bhutan

Code	Country
52	Bolivia
	Bosnia & Herzegowina
	Botswana
	Bouvet Island
	Brazil
	British Indian Ocean Territory
	Brunei Darussalam
	Bulgaria
	Burkina Faso
	Burundi
	Cambodia
	Cameroon
	Canada
	Cape Verde
	Cayman Islands
	Central African Republic
	Chad
	Chile
	China
	Christmas Island
	Cocos (Keeling) Islands
	Colombia
	Comoros
	Congo
	Cook Islands
	Costa Rica
	Cote D'Ivoire
	Croatia
	Cuba
	Cyprus
	Czech Republic
	Denmark
	Djibouti
	Dominica
	Dominican Republic
	East Timor
	Ecuador
	Egypt
	El Salvador
	Equatorial Guinea
	Eritrea
	Estonia
	Ethiopia
	Falkland Islands (Malvinas)
	Faroe Islands
	Fiji

Code	Country
52	Finland
	France
	France-Metropolitan
	French Guiana
	French Polynesia
	French Southern Territories
	Gabon
	Gambia
	Georgia
	Germany
	Ghana
	Gibraltar
	Greece
	Greenland
	Grenada
	Guadeloupe
	Guam
	Guatemala
	Guinea
	Guinea-Bissau
	Guyana
	Haiti
	Heard and Mc Donald Islands
	Honduras
	Iceland
	Iran
	Iraq
	Ireland
	Italy
	Jamaica
	Jordan
	Kazakhstan
	Kenya
	Kiribati
	Korea-Republic of
	Kuwait
	Kyrgyzstan
	Lao People's Democratic Republic
	Latvia
	Lebanon
	Lesotho
	Liberia
	Libyan Arab Jamahiriya
	Liechtenstein
	Lithuania

Code	Country
52	Luxembourg
	Macau
	Macedonian-Former Yugoslav Republic of
	Madagascar
	Malawi
	Maldives
	Mali
	Malta
	Marshall Islands
	Martinique
	Mauritania
	Mauritius
	Mayotte
	Mexico
	Micronesia (Federated States of)
	Moldavia -Republic of
	Monaco
	Mongolia
	Montserrat
	Morocco
	Mozambique
	Myanmar
	Namibia
	Nauru
	Nepal
	Netherlands
	Netherlands Antilles
	New Caledonia
	Nicaragua
	Niger
	Nigeria
	Niue
	Norfolk Island
	Northern Mariana Islands
	Norway
	Oman
	Pakistan
	Palau
	Panama
	Papua New Guinea
	Paraguay
	Peru
	Pitcairn
	Portugal
	Puerto Rico
	Qatar

Code	Country
52	Reunion
	Romania
	Russian Federation
	Rwanda
	St. Helena
	Saint Kitts and Nevis
	Saint Lucia
	St. Pierre and Miquelon
	Saint Vincent and the Grenadines
	Samoa
	San Marino
	Sao Tome and Principe
	Saudi Arabia
	Senegal
	Seychelles
	Sierra Leone
	Slovakia
	Solomon Islands
	Somalia
	South Georgia and the South Sandwich Islands
	Spain
	Sri Lanka
	Sudan
	Suriname
	Svalbard and Jan Mayen Islands
	Swaziland
	Sweden
	Switzerland
	Syrian Arab Republic
	Taiwan-Province of China
	Tajikistan
	Tanzania-United Republic of
	Thailand
	Togo
	Tokelau
	Tonga
	Trinidad and Tobago
	Tunisia
	Turkey
	Turkmenistan
	Turks and Caicos Islands
	Tuvalu
	Uganda
	Ukraine
	United Arab Emirates

Code	Country
52	United Kingdom United States United States Minor Outlying Islands Uruguay Uzbekistan Vanuatu Vatican City State (Holy See) Venezuela Virgin Islands (British) Virgin Islands (U.S.) Wallis and Futuna Islands Western Sahara Yemen Yugoslavia Zaire Zambia Zimbabwe
53	South Africa

Appendix B: XYZ Event Mappings

Introduction

This topic provides a list of all the Event Groups and Event Types in the Gallagher Command Centre system. For Contact ID, the **XYZ** Event Codes have been mapped to an existing Event Group. In the table below, the **XYZ** Event Codes are displayed in **"bold"** print under the relevant Event Group.
See also ***CCC Identifiers*** (on page Appx C-1) for a list of what CCC will be sent when a particular **XYZ** event occurs.

Event Group	Event Type
Access Denied **421 - Access denied**	Access Challenged Access change denied Access Zone locked down Alarm change denied Bad 2nd authorization Bad Level Bad Second Card Battery Too Low Biometric - No Record Found Biometric - Operation Timeout Biometric - Unknown Error Buffer Full Card Blocked Code Only Access Not Available while Alarms set Door in emergency state Exit Denied Invalid Card Issue Invalid Salto Card Issue More than One Visitor No 2nd authorization No access at this time No Escort No Privacy Override Privilege No Salto access at this time No Salto Zone Privilege No user code No Zone Privilege Not an escort Passback Attempted PIN Too Late Repeated First Card Terminal: Bad facility code Terminal: Invalid issue Terminal: No access Terminal: PIN too late Terminal: Unauthorized card

Event Group	Event Type
Access Denied **421 - Access denied** (cont'd…)	Unauthorised Card Unauthorised Salto Card Unknown Biometric Wrong Facility Code Zone Set - No Access
Alarm Transmission Failure **393 - Maintenance Alert**	Dial cycle completed without success Periodic dialtone check failed
Alarm Transmission Warning **393 - Maintenance Alert**	Backup dialler failed Dialler forwarding Dialler gave up Dialler link broken Dialler no backup Dialler no dial tone Dialler no handshake Dialler no modem Dialler retry wait Dialler transmit error
Alarm Zone Change Problem **454 - Failed to close**	Arm failed Code Only Set Already Code Only Set Failed Code Only Set Failed - Not User Mode Code Only Set Failed - Offline Input Set Fail Set Failed - No Access Set Failed – Offline Terminal: Arm failed Terminal: Force arm Terminal: Isolate arm Zone Set Already Zone Set Failed Zone Set Not User Mode
Card Error **421 - Access denied**	Foreign Card Illicit Card Non High-Security Card Terminal: Foreign card Terminal: Illicit card
Card Event **422 - Access report by User**	Accept First Card Cancel Override Card Cancelled Card Exit Granted Card Not Fully Updated Card Updated Code only No Entry Door Access Granted Door Free Access

Event Group	Event Type
Card Event **422 - Access report by User** (cont'd…)	Door Secure Access Elevator Access Granted Interlock Rules Prevented Code only Entry Interlock Rules Prevented Entry Level Access Granted Level Not Selected No Entry Taken Override Mode 1 Override Mode 2 Salto Door Access Granted Salto Door Closing Granted Terminal: Active Alarm Acknowledgement Terminal: Alarm Acknowledgement Terminal: Auto-Logout Terminal: Cancel override Fence Zone Terminal: Logon Terminal: Logout Terminal: Override Off Fence Zone Terminal: Override On Fence Zone Terminal: Shunt Terminal: Shunt Fence Zone Terminal: Unshunt Terminal: Unshunt Fence Zone
Card Trace **422 - Access report by User**	Auto-Forgive on Exit From Site Card Trace Exit Allowed Passback Allowed Terminal: Card trace
Closed/On **130 - Burglary**	Input Closed Logic Block On Output On
Command Centre Comms Interrupted **330 - System Peripheral trouble**	Biometric Reader Comms Failed Comms failed to Command Centre Communications Server Offline Controller Not Connected to Server Yet Controller Offline Event Server Offline External System Offline Intercom System endpoint offline Remote Server Offline Salto Server Offline Service Offline
Copper Sync Detected **131 - Perimeter**	Copper Sync Detected

Event Group	Event Type
Copper Sync Lost **131 - Perimeter**	Copper Sync Lost
Door Not Locked **426 - Access Door propped open**	Door Not Locked
Door Open Too Long **426 - Access Door propped open**	Door Open Too Long
Door Status **422 - Access report by User**	Daylight savings Time Adjustment Door Opened Door Re-secured End of forced closing PPD connection Salto control unit updated Start of forced closing
Duress **121 - Duress**	Cardholder Duress Code only DURESS DURESS, Entry Denied DURESS, Entry OK Terminal: DURESS
Earth Warning **131 - Perimeter**	Earth warning
External Event Group 0 - 29 **140 - General Alarm**	External Event 0 - 29
External System **140 - General Alarm**	External System Online Intercom System call connected at Command Centre Intercom System call disconnected at Command Centre Intercom System call received at Command Centre Intercom System endpoint isolated Intercom System endpoint normal mode of operation Intercom System endpoint online Intercom System endpoint remoted SchindlerID Third-Party Database Online Interface Online
Fence Alarm **131 - Perimeter**	Fence alert
Fence Low Feel Alarm **131 - Perimeter**	Fence Low Feel Alert
Fence Low Feel Warning **131 - Perimeter**	Fence Low Feel Warning

Event Group	Event Type
Fence Override High Voltage **393 - Maintenance Alert**	Overridden High Voltage
Fence Override Low Feel **393 - Maintenance Alert**	Overridden Low Feel
Fence Override Off **393 - Maintenance Alert**	Overridden off
Fence Override On **393 - Maintenance Alert**	Overridden on
Fence Shunted **570 - Zone/Sensor bypass**	Fence shunted
Fence Warning **131 - Perimeter**	Fence warning
Fence Zone High Voltage **140 - General Alarm**	Fence High Voltage
Fence Zone HVplus **140 - General Alarm**	Fence HVplus
Fence Zone Lockout **140 - General Alarm**	Fence zone Lockout
Fence Zone Low Feel **140 - General Alarm**	Fence Low Feel
Fence Zone Off **140 - General Alarm**	Fence off
Fence Zone On **140 - General Alarm**	Fence on
Forced Door **423 - Forced Access**	Forced Door Interlock Breach Intrusion
HV Sync Pulse Absent **140 - General Alarm**	HV Sync Pulse Absent
HVplus Escalation **140 - General Alarm**	Fence Controller escalated to HVplus
Input Not Triggered **380 - Sensor trouble**	Input not Triggered
Intercom Call **140 - General Alarm**	Intercom Call Button Pressed

Event Group	Event Type
Inter-Controller Offline Monitoring **140 - General Alarm**	Monitored Controller Offline
Invalid Logon **461 - Wrong Code Entry**	Operator Logon Failed Terminal: Invalid user code Wrong Code only Code
Maintenance Failure **393 - Maintenance Alert**	A configuration object could not be sent to the Controller because it was too big. An Access Group has too many zones. Archive Failed Biometric Reader MIFARE Key Update Failed Central Database Backup Failed Controller bad diary action Controller bad diary data Controller bad event log Controller bus message revision Controller Database - cannot open Controller Database - cannot read Controller Database - cannot write Controller Database - full Controller dynamic RAM checksum test failed Controller dynamic RAM test failed Controller flash memory failure Controller Incorrectly Configured Controller invalid object Controller message failed Controller Network - bad authentication Controller Network - bad protocol version Controller Network - bad session message Controller Network - GetHostByName failed Controller Network - TCP failure Controller Network - unrecognised application message. Controller no part status Controller Part - bad input Controller Part - configuration failed Controller Part - no configuration Controller Part - no such type Controller thread not responding Download failed Download Failure Download Failure - file error Download Failure - Timeout Elevator HLI serial port not available Event buffer corrupt General Failure Hardware Fault Detected

Event Group	Event Type
Maintenance Failure **393 - Maintenance Alert** (cont'd…)	Image checksum failed Initialisation Failed Insufficient Reader Database Space Invalid Certificate Licence Expired - System is now read-only Local Drive Critically Low Disk Space Macro failed to run Report failed Re-sync Access Failed SQL Server Database Critical Space Shortage Unit Download Failure - Unit Offline Unit MAC Error (Access) Unit MAC Error (Level) Unit MAC Error (Zone) Unit Remote Diagnostic
Maintenance Mode **393 - Maintenance Alert**	Sensor Group in Maintenance Mode
Maintenance Warning **393 - Maintenance Alert**	Bad Packet Bad unit type Battery Low Biometric Reader Tampered Bulk Change Complete - Some Failures Bulk Change One Item Failed Command Centre Comms Interrupted Command Centre Link - No Carrier Command Centre Link Ceased Controller alarm buffer overflow Controller bad configuration parameter Controller bad message from unit Controller bad packet from unit Controller bad relay Controller Database - missing Controller disk space low Controller event buffer Configuration Changed Controller Incompatible configuration Controller IP Address in use by another device Controller IP Address Incorrect Controller kill no part Controller memory low Controller missing calendar Controller missing configuration parameter Controller missing configuration section Controller missing day Controller Network - encryption policy mismatch Controller Network - logon rejected Controller Network - new key and certificate

Event Group	Event Type
Maintenance Warning **393 - Maintenance Alert** (cont'd…)	loaded Controller Part - no such part Controller property out of range Controller shutdown no part? Controller unhandled message Controller unit command dropped Controller unknown packet from unit Controller Unknown version Controller unrecognised name type Controller WWW - send failed Controller WWW - unauthorised Deletion Conflict Detected Dialler message lost Download warning Duplicate Card Detected Duplicate Logon Name Detected Duplicate Personal Data Detected Duplicate User Code Detected Elevator HLI bad reply Elevator HLI protocol error Event buffer deleted General Warning Hardware mismatch Image lost Invalid Command Line in Macro Invalid User Account in Macro License Warning - Devices required to maintain your license validity are not responding. License Warning - License has expired License Warning - License is not valid for this version of Command Centre. License Warning - License limits have been exceeded. Local Drive Low Disk Space Notification Local Drive Low Disk Space Warning Macro misconfiguration Mains Power Failed Network auth timeout Network Overload Network trans timeout Replication Conflict Detected SQL Server Database Space Shortage Notification SQL Server Database Space Shortage Warning Unexpected Controller reset Unexpected request (special cardholder function) Unit Bad Version Unit Corrupt Setup Unit Lost Setup

Event Group	Event Type
Maintenance Warning **393 - Maintenance Alert** (cont'd…)	Unit MAC Error Unit Obsolete Database Unit Reset Unit Start Refresh Ignored
Network Attack **330 - System Peripheral trouble**	Network Attack
No Battery **311 – Battery Missing/Dead**	No battery
Non-Card Door Unlock **425 - Egress Granted**	Button Release Granted Code only Access Granted PPD Emergency Opening
Open/Off **130 - Burglary**	Input Open Logic Block Off Output Off
Perimeter Attack **131 - Perimeter**	Attack Detected
Point Not Tested **612 - Point not tested**	Input not Tested
Power Critical **311 - Battery Missing/Dead**	Unit stopped
Power Failure **305 - System reset**	Power failed
Power out of Range **302 - Low system battery**	Controller power high Controller power low Unit - power high Unit - power low
Power Severe **302 - Low system battery**	Unit going slow
Power Supply Failed **301 - AC Loss**	Power Supply failed
Power Warning **302 - Low system battery**	Low battery
Primary ethernet link **350 - Communication trouble**	Primary ethernet link failed
Primary ethernet link failed-over **393 - Maintenance Alert**	Secondary ethernet link failed-over

Event Group	Event Type
Repeated Login Failure **421 - Access denied**	Terminal: Max bad logins
Secondary ethernet link **350 - Communication trouble**	Secondary ethernet link failed
Security Breach **341 - Exp. Module Tamper**	Terminal: Code Tampered Terminal: Encryption Tampered
Sensor Abnormal **131 - Perimeter**	Sensor Abnormal Tension - High Sensor Abnormal Tension - Low Sensor Offline Sensor Power Low Sensor Tension Overload
Sensor(s) Reporting Abnormal Tension **393 - Maintenance Alert**	Sensor Group Abnormal Tension
Service Mode **140 - General Alarm**	Service Mode on
Shunted/Isolated **570 - Zone/Sensor bypass**	Controller Bus Automatically Shunted Controller Bus Shunted Device Shunted Input Isolated Input Shunted Sensor Group Shunted
State Unknown **393 - Maintenance Alert**	Logic items in unknown state
Tamper **145 - Expansion module tamper**	Controller tampered (front) Controller tampered (rear) Input Break Input Short Input Tampered Salto Door Tampered Unit Tampered Unit Tampered (Front) Unit Tampered (Rear)
Temperature Critical **393 - Maintenance Alert**	Unit stopped - Temperature
Temperature out of HVplus range **140 - General Alarm**	HVplus escalations disabled - high temperature
Temperature Out of Range **393 - Maintenance Alert**	Temperature too high Temperature too low

Event Group	Event Type
Unit On-line **531 - Module Added**	HBUS device detected
Unit Stopped Responding **143 - Expansion module failure**	Plug-in not responding Unit Not Responding
Walk Test Mode **393 - Maintenance Alert**	Sensor Group in Walk Test Mode
Walk Test Mode Attack **393 - Maintenance Alert**	Attack Detected
Wrong PIN **421 - Access denied**	Terminal: Bad PIN Wrong PIN Entered
Zone Count Maximum **140 - General Alarm**	Zone Count Maximum
Zone Count Mid-range **140 - General Alarm**	Zone Count Mid-range
Zone Count Minimum **140 - General Alarm**	Zone Count Minimum

Appendix C: CCC Identifiers

Introduction

This topic provides a list of what **CCC** will be sent when a particular **XYZ** event occurs. Each **XYZ** event below shows the data type in brackets beside it. There are two data types, as follows:

- ZONE: this means that the Hardware **CCC** is used, and
- USER: this means that the User **CCC** is used.

Note: In the case of Panic Alarms (Duress messages), if there is a reader on a door, Contact ID sends the Door's CCC code rather than the reader's CCC code.

ALARMS

Medical Alarms - 100

100 Medical	(ZONE)
101 Personal Emergency	(ZONE)
102 Fail to report in	(ZONE)

Fire Alarms - 110

110 Fire	(ZONE)
111 Smoke	(ZONE)
112 Combustion	(ZONE)
113 Water flow	(ZONE)
114 Heat	(ZONE)
115 Pull Station	(ZONE)
116 Duct	(ZONE)
117 Flame	(ZONE)
118 Near Alarm	(ZONE)

Panic Alarms - 120

120 Panic	(ZONE)
121 Duress	(USER)
122 Silent	(ZONE)
123 Audible	(ZONE)
124 Duress - Access granted	(ZONE)
125 Duress - Egress granted	(ZONE)

Burglar Alarms - 130

130 Burglary	(ZONE)
131 Perimeter	(ZONE)
132 Interior	(ZONE)
133 24 Hour (Safe)	(ZONE)
134 Entry/Exit	(ZONE)
135 Day/night	(ZONE)
136 Outdoor	(ZONE)
137 Tamper	(ZONE)
138 Near alarm	(ZONE)
139 Intrusion Verifier	(ZONE)

General Alarm - 140

140	General Alarm	(ZONE)
141	Polling loop open	(ZONE)
142	Polling loop short	(ZONE)
143	Expansion module failure	(ZONE)
144	Sensor tamper	(ZONE)
145	Expansion module tamper	(ZONE)
146	Silent Burglary	(ZONE)
147	Sensor Supervision Failure	(ZONE)

24 Hour Non-Burglary - 150 and 160

150	24 Hour Non-Burglary	(ZONE)
151	Gas detected	(ZONE)
152	Refrigeration	(ZONE)
153	Loss of heat	(ZONE)
154	Water Leakage	(ZONE)
155	Foil Break	(ZONE)
156	Day Trouble	(ZONE)
157	Low bottled gas level	(ZONE)
158	High temp	(ZONE)
159	Low temp	(ZONE)
161	Loss of air flow	(ZONE)
162	Carbon Monoxide detected	(ZONE)
163	Tank level	(ZONE)

Fire Supervisory - 200 and 210

200	Fire Supervisory	(ZONE)
201	Low water pressure	(ZONE)
202	Low CO2	(ZONE)
203	Gate valve sensor	(ZONE)
204	Low water level	(ZONE)
205	Pump activated	(ZONE)
206	Pump failure	(ZONE)

System Troubles - 300 and 310

300	System Trouble	(ZONE)
301	AC Loss	(ZONE)
302	Low system battery	(ZONE)
303	RAM Checksum bad	(ZONE)
304	ROM Checksum bad	(ZONE)
305	System reset	(ZONE)
306	Panel programming changed	(ZONE)
307	Self-test failure	(ZONE)
308	System shutdown	(ZONE)
309	Battery test failure	(ZONE)
310	Ground fault	(ZONE)
311	Battery Missing/Dead	(ZONE)
312	Power Supply Overcurrent	(ZONE)
313	Engineer Reset	(USER)

Sounder / Relay Troubles - 320

320 Sounder/Relay	(ZONE)
321 Bell 1	(ZONE)
322 Bell 2	(ZONE)
323 Alarm relay	(ZONE)
324 Trouble relay	(ZONE)
325 Reversing relay	(ZONE)
326 Notification Appliance Ckt. #3	(ZONE)
327 Notification Appliance Ckt. #4	(ZONE)

System Peripheral Trouble - 330 and 340

330 System Peripheral trouble	(ZONE)
331 Polling loop open	(ZONE)
332 Polling loop short	(ZONE)
333 Expansion module failure	(ZONE)
334 Repeater failure	(ZONE)
335 Local printer out of paper	(ZONE)
336 Local printer failure	(ZONE)
337 Exp. Module DC Loss	(ZONE)
338 Exp. Module Low Batt.	(ZONE)
339 Exp. Module Reset	(ZONE)
341 Exp. Module Tamper	(ZONE)
342 Exp. Module AC Loss	(ZONE)
343 Exp. Module self-test fail	(ZONE)
344 RF Receiver Jam Detect	(ZONE)

Communication Troubles - 350 and 360

350 Communication trouble	(ZONE)
351 Telco 1 fault	(ZONE)
352 Telco 2 fault	(ZONE)
353 Long Range Radio xmitter fault	(ZONE)
354 Failure to communicate event	(ZONE)
355 Loss of Radio supervision	(ZONE)
356 Loss of central polling	(ZONE)
357 Long Range Radio VSWR problem	(ZONE)

Protection Loop - 370

370 Protection loop	(ZONE)
371 Protection loop open	(ZONE)
372 Protection loop short	(ZONE)
373 Fire trouble	(ZONE)
374 Exit error alarm (zone)	(ZONE)
375 Panic zone trouble	(ZONE)
376 Hold-up zone trouble	(ZONE)
377 Swinger Trouble	(ZONE)
378 Cross-zone Trouble	(ZONE)

Sensor Trouble - 380

380	Sensor trouble	(ZONE)
381	Loss of supervision - RF	(ZONE)
382	Loss of supervision - RPM	(ZONE)
383	Sensor tamper	(ZONE)
384	RF Low battery	(ZONE)
385	Smoke detector Hi sensitivity	(ZONE)
386	Smoke detector Low sensitivity	(ZONE)
387	Intrusion detector Hi sensitivity	(ZONE)
388	Intrusion detector Low sensitivity	(ZONE)
389	Sensor self-test failure	(ZONE)
391	Sensor Watch trouble	(ZONE)
392	Drift Compensation Error	(ZONE)
393	Maintenance Alert	(ZONE)

OPEN/CLOSE/REMOTE ACCESS

Open/Close - 400, 440, 450

400	Open/Close	(USER)
401	O/C by user	(USER)
402	Group O/C	(USER)
403	Automatic O/C	(USER)
404	Late to O/C (*Note:* Use 453, 454 instead)	(USER)
405	Deferred O/C (*Note:* Obsolete - do not use)	(USER)
406	Cancel	(USER)
407	Remote arm/disarm	(USER)
408	Quick arm	(USER)
409	Keyswitch O/C	(USER)
441	Armed STAY	(USER)
442	Keyswitch Armed STAY	(USER)
450	Exception O/C	(USER)
451	Early O/C	(USER)
452	Late O/C	(USER)
453	Failed to Open	(USER)
454	Failed to Close	(USER)
455	Auto-arm Failed	(USER)
456	Partial Arm	(USER)
457	Exit Error (user)	(USER)
458	User on Premises	(USER)
459	Recent Close	(USER)
461	Wrong Code Entry	(USER)
462	Legal Code Entry	(USER)
463	Re-arm after Alarm	(USER)
464	Auto-arm Time Extended	(USER)
465	Panic Alarm Reset	(ZONE)
466	Service On/Off Premises	(USER)

Remote Access - 410

411 Callback request made	(USER)
412 Successful download/access	(USER)
413 Unsuccessful access	(USER)
414 System shutdown command received	(USER)
415 Dialler shutdown command received	(USER)
416 Successful Upload	(ZONE)

Access control - 420 and 430

421 Access denied	(USER)
422 Access report by user	(USER)
423 Forced Access	(ZONE)
424 Egress Denied	(USER)
425 Egress Granted	(USER)
426 Access Door propped open	(ZONE)
427 Access point Door Status Monitor trouble	(ZONE)
428 Access point Request To Exit trouble	(ZONE)
429 Access program mode entry	(USER)
430 Access program mode exit	(USER)
431 Access threat level change	(USER)
432 Access relay/trigger fail	(ZONE)
433 Access RTE shunt	(ZONE)
434 Access DSM shunt	(ZONE)

BYPASSES / DISABLES

System Disables - 500 and 510

501 Access reader disable	(ZONE)

Sounder / Relay Disables - 520

520 Sounder/Relay Disable	(ZONE)
521 Bell 1 disable	(ZONE)
522 Bell 2 disable	(ZONE)
523 Alarm relay disable	(ZONE)
524 Trouble relay disable	(ZONE)
525 Reversing relay disable	(ZONE)
526 Notification Appliance Ckt. #3 disable	(ZONE)
527 Notification Appliance Ckt. #4 disable	(ZONE)

System Peripheral Disables - 530 and 540

531 Module Added	(ZONE)
532 Module Removed	(ZONE)

Communication Disables - 550 and 560

551 Dialler disabled	(ZONE)
552 Radio transmitter disabled	(ZONE)
553 Remote Upload/Download disabled	(ZONE)

Bypasses - 570

570	Zone/Sensor bypass	(ZONE)
571	Fire bypass	(ZONE)
572	24 Hour zone bypass	(ZONE)
573	Burg. bypass	(ZONE)
574	Group bypass	(USER)
575	Swinger bypass	(ZONE)
576	Access zone shunt	(ZONE)
577	Access point bypass	(ZONE)

TEST / MISC.

Test/Misc. - 600 and 610

601	Manual trigger test report	(ZONE)
602	Periodic test report	(ZONE)
603	Periodic RF transmission	(ZONE)
604	Fire test	(USER)
605	Status report to follow	(ZONE)
606	Listen-in to follow	(ZONE)
607	Walk test mode	(USER)
608	Periodic test - System Trouble Present	(ZONE)
609	Video Xmitter active	(ZONE)
611	Point tested OK	(ZONE)
612	Point not tested	(ZONE)
613	Intrusion Zone Walk Tested	(ZONE)
614	Fire Zone Walk Tested	(ZONE)
615	Panic Zone Walk Tested	(ZONE)
616	Service Request	(ZONE)

Event Log - 620

621	Event Log reset	(ZONE)
622	Event Log 50% full	(ZONE)
623	Event Log 90% full	(ZONE)
624	Event Log overflow	(ZONE)
625	Time/Date reset	(USER)
626	Time/Date inaccurate	(ZONE)
627	Program mode entry	(ZONE)
628	Program mode exit	(ZONE)
629	32 Hour Event log marker	(ZONE)

Scheduling - 630

630	Schedule change	(ZONE)
631	Exception schedule change	(ZONE)
632	Access schedule change	(ZONE)

Personal Monitoring - 640

641	Senior Watch Trouble	(ZONE)
642	Latch-key Supervision	(USER)

Misc. - 650

651 Reserved for Ademco Use	(ZONE)
652 Reserved for Ademco Use	(USER)
653 Reserved for Ademco Use	(USER)
654 System Inactivity	(ZONE)

Glossary of Terms

A

Access Control

Restriction of entry or exit to access zones or elevator levels based upon specific criteria.

Access Criteria

The parameters which determine the access groups or individuals who are allowed access to an access zone or elevator level during specified times of the day.

Access Denied

The Cardholder does not have access to an access zone or elevator level.

Access Group

A group of cardholders with identical access criteria. An Access Group also has privileges other than access, including the ability to escort visitors and to do manual overrides. These can be found on the Access Groups Privileges tab in Command Centre.

Access Mode

The level of access restriction applying to an access zone at a certain time of day, (e.g. out of hours access mode may be 'Card plus PIN', and during work hours it may be 'Free Access').

Access Mode Change Event

This is an 'Access Zone state change' event and indicates an Access Zone has changed state. The state has two parts, the 'Access Mode' can be 'Free', 'Secure', 'Code or Card' or 'Dual-auth'; the PINs mode can be 'No PIN', '4 digit PIN' or '6 digit PIN'.

Access Point

Any point of entry or exit, such as an office door or car-park barrier arm which controls entry to an access zone.

Access Rights

Access rights determine the access zones and elevator levels to which a cardholder is allowed access. Access rights are assigned to Access Groups, and cardholders acquire access rights by joining Access Groups.

Access Zone

A single area within a site which has controlled points of entry or exit. There may be several controlled entry or access points into an access zone.

Access Zone Group

Individual Access Zones can be associated with a Master Zone so they become members of an Access Zone Group. Grouping Access Zones allows anti-passback to be applied to the group rather than individual zones.

Action Plan

An Action Plan defines what is going to happen when an event in the system occurs.

Alarm

Some activity taking place on your site which creates an entry in the Alarm Viewer window.

Alarm Escalation

Configurable setting so that if an alarm is not acknowledged within the set time, the alarm will automatically escalate in priority.

Alarm Flooding

Alarm Flooding occurs when the same alarm is generated numerous times and fills up the Alarm Viewer window. Command Centre allows these flood alarms to be summarised.

Alarm Instruction

A simple set of textual instructions which display when an operator views the details of an alarm.

Alarm State

The state of an alarm associated with an access zone. The alarm state may be 'set', 'unset', 'user1' or 'user2'.

Alarm Type

A category of alarm.

Alarm Zone

A grouping (normally geographical) of alarm points that are set and unset (or in user defined states) at the same times.

Alarm Zone State Change

This is an 'Alarm Zone state change' event and indicates that an Alarm Zone has been armed, disarmed or put into one of the other states.

Alarm Zone State Change Failed

Indicates an Alarm Zone State Change did not initiate and the Alarm Zone state has not changed.

Anti-Passback

The prevention of a cardholder from re-entering an access zone if they have not made a valid exit from that zone. Anti-passback is designed to prevent a cardholder 'passing' their credential 'back' to another person to allow them access into the zone at a later time.

Anti-Passback violation

The condition where the system has detected that a credential passback has occurred, (i.e. a cardholder has attempted to enter an Access Zone, or Access Zone Group, when they are already recorded as within it).

Anti-tailgating

Anti-tailgating means the ability to deny access through a controlled door when the current location of the cardholder is not within the area from which they are attempting to gain entry.

Anti-tailgating violation

The condition where the system has detected that a cardholder has tailgated, (i.e. a cardholder has attempted to enter an Access Zone when they are currently recorded as outside the Access Zone, or Access Zone Group, from which they are entering).

ARC

Alarm Receiving Centre. Usually a separate company used to receive and action alarms from an Intruder Alarm System (IAS) for use out of normal working hours.

Authorised Cardholder

A person who is authorised to exist in the system as a valid cardholder.

Auto-forgive

Allows an authorised cardholder to re-enter an anti-passback zone after the time set, even though they have not made a valid exit from that zone. The Auto-forgive time starts from the time of valid entry, (i.e. if set to 3 minutes and a cardholder presents their credential after 3 minutes from the original valid entry, they will be allowed back in the zone). See also 'Anti-Passback'.

Automatic Lock Type

When a Door is configured as an Automatic Lock the lock relay will always be activated for the user configured time. This time is set by the use of the "Door unlock time" option.

B

Backup

The systems working data can be backed up to a file. This can be done while the system is online and operators logged in.

C

Card

Any form of identifying token, such as a proximity token, mag-stripe card, insertion key, etc.

Card Activity

Use of cards within a Command Centre site to gain access through doors. Card Activity is recognised by the generation of events with the "Card Event" event group.

Card Expiry

The disabling of a card within the Command Centre system such that it may no longer be used to gain access.

Card Swipe Timeout

Maximum time allowed between card swipes. Applies for dual authorisation, escort, double-card overrides or any situation requiring dual card swipes. This timeout also applies to the time between pressing a function key on a keypad reader, (i.e. Arm, Mode, F1 or F2) and badging a card for a local override.

Card Trace

A message and/or alarm is generated each time a specific card is presented to a Reader.

Cardholder

Any person, vehicle or other identity issued with an access control token.

Challenge

The Challenge feature allows a Command Centre operator to contest Cardholders as they attempt to gain access through a Door, and either grant or deny access.

Class 5 End-of-Line Module (ELM)

The Class 5 End-of-Line Module (ELM) is an HBUS device that provides secure monitoring of alarm inputs for high security applications. The Class 5 ELM only works with a Gallagher PIV C6000HS Controller.

Closed

The contacts on an Input are closed. The Input is 'inactive'.

Confirmed Alarms

This uses the "Escalate if two events from different points in same zone within x seconds" feature on the **Armed** tab of the Action Plan. See Action Plans for further explanation of escalated alarms.

When a second alarm point is triggered within the same zone within the timeout, the first alarm has been confirmed by the second, which initiates a Contact ID notification using the "139 - Intrusion Verifier" code for the second event instead of the usual code, (i.e. any of the 130 to 138 codes). The first event uses a Contact ID code between 130 and 138 and the second event must be in the same Event Group as the first event.

Contact ID

Contact ID is a DTMF (Dual Tone Multi-Frequency) protocol for transmitting event/alarm occurrences to remote alarm monitoring stations over standard telephone lines.

Controller 6000

The Controller 6000, of which there are six variants, (i.e. Standard, Starter Kit, 2-Door, High Sec 2-Door, Enhanced and High Sec), is the central field controller for the Command Centre system. It is a processing board for an intruder alarm and access control system. All variants can operate on their own, or can have an optional Reader Module connected.

The Controller 6000 authenticates user access, logs it and carries out the required function, (e.g. opens the corresponding door). It is an Ethernet attached device which connects to a server, however it can operate autonomously.

The Controller 6000 has two RS-485 connections. Each connection may be individually configured to support HBUS, Sensor, Aperio, Schlage or OSDP communications.

Controller 7000 Single Door

The Controller 7000 Single Door, of which there are four variants, (i.e. 'RS485', 'Wiegand', 'PoE+, RS485' and 'PoE+, Wiegand'), is a processing board for an intruder alarm and access control system that can control a single door.

Count Zone

An Access Zone, or Access Zone Group, that the system must count cardholder entries into and exits from is known as a count zone.

Crypt Seed

The Crypt Seed number is used for the encryption/decryption of cards and PINs, and is supplied by Gallagher Group Limited.

D

Database Recovery Code

The Database Recovery Code is backed up and saved in a secure location during Command Centre installation. It protects the data stored in the Command Centre database, (e.g. encryption keys and user codes) and is required in the case of disaster recovery or when moving databases to a new server.
Note: Losing the recovery code prevents you from restoring your database in either of these cases.

Day Category

Day categories are assigned to days of the year, (e.g. Monday to Friday could be the "Weekday" category, and Statutory holidays could be the "Public Holiday" category). Day categories are then assigned to Schedules, so that the scheduled system behaviour occurs at the specified time on the day category type, (e.g. Monday, Weekday, Public Holiday).

Device

Devices include door readers and other interface hardware. Devices send information to the Controller and act upon information sent from the Controller.

Device Number

A unique code which identifies each device to the Controller, allowing it to 'address' messages to each.

Dialect

A combination of a language and sub-language. For instance, English (New Zealand) and English (United States) are dialects of the English language.

Digital Video Recording (DVR)

Digital Video Recording (DVR) equipment and software from a range of manufacturers can be integrated with Command Centre, and allows digital video to be stored to a hard disk.

Division

Division, (or system division), allows a site to be divided into smaller divisions and sub-divisions. Each sub-division can manage their own security needs without requiring access to other divisions' site configuration or access information.

Door

Any point of entry or exit, such as an office door or car-park barrier arm which controls entry to an access zone.

Door Not Locked

This is an alarm condition and indicates that the door should have locked but Command Centre has not detected the lock mechanism activation, indicating the lock may be faulty or being interfered with

Door Open Too Long

The door has been opened correctly, but has been left open longer than is allowed.

Door Reader

Any device, such as a swipe card or proximity reader which requires some form of identification from a cardholder.

Door Status

Indicates the current status on the door, (e.g. door closed and locked, door closed and unlocked, door open and unlocked).

Double card Override

Double card overrides are enabled in the reader properties. A double card override enables a cardholder to either:

- Override the access mode of an Access Zone (alternating between access mode 2 and scheduled) by badging their card twice at a card reader within a specified time frame, OR
- Override the Alarm Zone state to armed by badging their card twice at a card reader within a specified time frame.

Note: The double card override feature is not supported whilst an Access Zone is in Dual Authorisation mode.

DTMF (Dual Tone Multi-Frequency)

DTMF (Dual Tone Multi-Frequency) is a standard signalling method for dialling and data transmission using a combination of two sine waves at different frequencies. It is commonly referred to as Touch-Tone® signalling.

Dual Authorisation

An access mode which requires a valid access by two authorised cardholders to enter an access zone within a specified time period.
Note that this functionality is not supported for HLI or LLI elevator systems.

Duress Alarm

An alarm generated by a Cardholder entering a special code at a PIN to indicate that they are being threatened or forced to provide access under duress.

Duress Code

A special code entered at a PIN reader or Remote Arming Terminal by a Cardholder to indicate that they are being threatened or forced to provide access under duress. Entering such a code generates a duress alarm. To raise a duress logon alarm:

1. Enter your valid user code with the last digit incremented by one. **For example:** User code 1256 = Duress logon is 125**7** User code 1259 = Duress logon is 125**0**
2. Press the **Enter** key.

DVR (Digital Video Recording)

Digital Video Recording (DVR) equipment and software from a range of manufacturers can be integrated with Command Centre, and allows digital video to be stored to a hard disk.

E

Elevator Car HLI

Used to refer to an elevator car that is associated with a high level elevator interface (Elevator HLI). Access to floors from the elevator car is controlled by Command Centre using the high level communications link.

Elevator HLI

The Elevator HLI represents a high level communications link from Command Centre to the elevator system. Access to floors from elevator cars is controlled by Command Centre via the high level communications link.

Entry Delay

A time delay, during which an alarm will not be reported, to allow a person entering an area time to reach a Key Switch, Card Reader or Remote Arming Terminal that they can use to Unset the Alarm Zone without setting off any alarms.

Entry Delay expired

When an entry delay has started but the zone was not disarmed within the Entry Delay time-out, alarms will not be generated from devices contained in the "Device(s) to use as Entry Points" and "Device(s) to ignore when entering" but Confirmed Alarms can still occur. See ***Confirmed Alarms*** definition.

Entry Path

A set of points contained within a zone, and which have an entry delay that does not apply to the rest of the zone.

Entry Point

An Input that triggers an entry delay by opening. It does not have to be in the same zone as the zone that has the entry delay.

Entry Reader

A door reader which controls entry into an access zone.

Entry Zone

The access zone into which an entry reader allows access.

Escort

An access mode which requires a card-holder who is part of an escort authorised group, to make a valid access after a visitor cardholder has also made a valid access. Also, a cardholder belonging to an escort authorised group. Note that this function-ality is not supported for HLI or LLI elevator systems.

Event

Some activity taking place on your site which creates an entry in the Event Viewer window, (e.g. a cardholder swiping their card to enter a door would be a cardholder event).

Exit Delay

A time delay after setting a Zone, during which an alarm will not be reported, to allow a person who has just Set the Zone time to leave the area without setting off any alarms.

Exit Point

An Input that terminates an exit delay by closing. It does not have to be in the same zone as the zone that has the exit delay.

Exit Reader

A door reader which controls exit from an access zone.

Exit Zone

The access zone into which an exit reader allows access.

F

Facility Code

A Facility Code is an identification number stored on the access token. Each site or facility normally has their own unique facility code. Therefore, if cards are allocated identical card numbers, because the sites facility codes are different, access will not be allowed on both sites.

Find Tool

The Find Tool enables users to search for and locate items within Command Centre. There are four tabs to help users define their search criteria.

Flood Alarms

See 'Alarm Flooding'.

Floor Select Timeout

Time from when specific floor select buttons are enabled in an elevator car, following a cardholder being granted access, to when the floor select buttons are returned to the default access state.

Force Status Request

A pop-up menu option available for some items. Used to check the status of an item if it looks incorrect, (e.g. a guard can see that a door is open but the item does not show this). The status of an item will be up-to-date after selecting this option.

Forced Door

Forced door alarms are optionally enabled or disabled, and are generated if a door is detected as being open while the system thinks it is still locked.

Free Access

A state during which all doors into an access zone or elevator level are unlocked. A door into a free access zone is only unlocked however if the zone on the other side of the door is also in free access mode.

Free Handle

Doors that are controlled by a pushbutton for entry can also have an additional 'Free Handle' option. This option can be used for doors where the lock does not need to be unlocked for exit. When this option is enabled, and a valid exit request is made, the doors lock relay will not activate (doors outside handle will remain locked).

G

Global item

Global items can be viewed at, and edited from, any workstation connected to any server in a multi-server system by an operator with suitable privileges. Cardholders are the only Command Centre items that are global items.

Grace Period

The system will generate an event when the zone count reaches a threshold value or zero. The grace period is the time that the system must allow from determining

that the count has reached a threshold before generating the event. This is to allow time for the completion of relevant cardholder activity that may prevent the need for the event to be generated.

Grid view

Any view in Command Centre where information is presented as columns of data in list form. Users can adjust the columns in various ways and resort the information.

H

Hardware

An item which physically exists, such as a door reader or a Controller.

HBUS Alarms Only Terminal

The HBUS Alarms Only Terminal can be used by suitably authorised Command Centre operators to perform many of the alarm management operations normally available only from Command Centre workstations. An HBUS Alarms Only Terminal is connected to the Controller 6000. An HBUS Alarms Only Terminal uses the HBUS communications protocol to communicate with the Controller 6000.

HBUS I/O Interface

The HBUS I/O Interface is an input monitoring and output control unit. It is available in four hardware variants: 8-In Board, 8-In 2-Out Door Module, 8-In 4-Out Board, and 16-In 16-Out Board. The 8-In 2-Out Door Module allows the connection of HBUS Readers and HBUS Terminals. Making no high level decisions, the HBUS I/O Interface monitors the state of balanced inputs and switches the output relays as instructed by the Controller 6000.

HBUS Terminal

The HBUS Terminal can be used by suitably authorised Command Centre operators to perform many of the alarm management operations normally available only from Command Centre workstations. The HBUS Terminal can also be used as an access control terminal and smart card proximity reader. An HBUS Terminal is connected to the Controller 6000. An HBUS Terminal uses the HBUS communications protocol to communicate with the Controller 6000.

I

IAS

Intruder Alarm System

Icon

A small picture representing an object or action. May often be inter-acted with in some way, (e.g. shows the status).

Inactivity Timeout

The configurable period of card inactivity that will cause that card to expire.

Inhibit

After an Entry Delay has expired because the zone did not get unset (disarmed), confirmed alarms can be inhibited. The effect of this is that Contact ID code 139 will not be notified to the Alarm Receiving Centre (ARC) and events from devices contained in the "Device(s) to use as Entry Points" and "Device(s) to ignore when entering" will not cause an alarm.

Input

A four-state sensor (switch), in a device. The states are Open, Closed, Open Circuit and Short Circuit Tamper. This allows greater security if correctly wired because attempting to cut or short the wires will generate an open or short circuit tamper alarm instead of an Open or Closed event.

Input Isolated

See 'Isolating Inputs'.

Input Shunted

See 'Shunting Inputs'.

Insertion Tag

A tag that represents a small piece of information, (e.g. phone number) that can be inserted into an Alarm Instruction. (See 'Alarm Instruction'.).

Isolating Inputs

The Input's state is to be ignored while in an isolated state and will no longer trigger alarms. Isolation only persists until the next time the Alarm Zone is unset.
Note: Input Shunted and Input Isolated are both in the same Event Group, but shunting takes precedence. This means that is an Input has been shunted it will not also get isolated. If an Input has been isolated, it may however be shunted. The isolation ends when the Alarm Zone changes state, but the shunt will continue until the shunt is removed.

L

List Window

List Windows are used for navigation and management control. They are the starting point for creating new objects, editing existing objects and deleting old objects, (e.g. the Cardholder List Window provides a list of all the Cardholders).

Locale

An identifier Windows uses to specify a language. It can be set either at a Window Logon level or at the Thread level. The locale has a language identifier, (e.g English) and a dialect identifier, (e.g. New Zealand).

M

Macro

Macros allow an operator to schedule either a set of pre-programmed overrides or a bulk change. Macros provide the ability to group and schedule them for a specific time and duration, either on a one-off basis or for events that repeat on a daily basis.

Mag-Stripe Card

A plastic card with access control information encoded on a magnetic stripe on the side.

Maintenance Warning and Failure

Maintenance events all report unusual conditions from field devices. 'Failures' are more serious than 'Warnings'.

Master Zone

Individual Access Zones can be associated with a Master Zone so they become members of an Access Zone Group. Grouping Access Zones allows anti-passback to be applied to the group rather than individual zones.

Multi-breaks

The multi-breaks option determines how repeated alarm messages will be sent via Contact ID, to a remote alarm monitoring company. A site can choose to send multiple transmissions of the same alarm occurrence, (i.e. alarm floods), or to send just one and then wait for an Alarm Zone Set/Unset before sending another.

Multiple Client Code Reporting (Contact ID)

Multiple Client Code Reporting is when a different account code is assigned to each Alarm Zone for the purposes of sending Contact ID.

Example:
Account Code = 1234, so an arm area 1 will be 123418340201001 and the disarm 123418140201001.
Account Code = 1235, so an arm area 1 will be 123518340201001 and the disarm 123518140201001, and so on.

(Check with your monitoring station that they support Multiple Client Code Reporting before sending any data.)

N

No-Alone Zone

A count zone where, for security or safety reasons, cardholders are not allowed to be in the zone alone. It may or may not be acceptable to be completely empty.

When the zone is empty the only allowed access is two cardholders entering the zone together. The last two cardholders must leave together. Whilst the zone count is two or more, cardholders may enter one at a time. Whilst the zone count is more than two, cardholders may leave one at a time.

O

Open

The contacts on an Input are open. The Input is 'active'.

Operator

Any person authorised to use Command Centre.

Operator Group

A group of Cardholders who are authorised to use Command Centre. Each Operator Group defines the privileges members have as Command Centre operators, (e.g. View only access, editing ability).

Operator Privileges

Operator privileges restrict the functionality available to operators, (e.g. a receptionist may have access to fewer features than a person responsible for the system configuration and maintenance).

Output

A two-state relay in a device, which controls a device such as a magnetic lock, alarm bells or a warning light, etc. Also used to refer to the device controlled by such a relay.

Override

Overrides enable an operator to temporarily change the status of an item attached to their Command Centre system. They enable operators to respond to common, random events, (e.g. temporarily unlock a door to give access to a cardholder who has forgotten their card).

P

PACE

Gallagher Card-Reader Card or Key.

Passive InfraRed (PIR) Detector

A device that senses body heat to detect motion, and generates an alarm condition.

PDF (Personal Data Field)

Personal Data is information that is stored for an individual cardholder, (e.g. date of birth, company, photographs, etc.). Personal Data Fields are created as separate entities and are attached to Access Groups. They can be either textual fields or image fields. Cardholders inherit the Personal Data Fields from the Access Group(s) they belong to.

Photo ID

Photo ID is a licensable feature used within Command Centre to design and print card layouts.

PIN (Personal Identification Number)

Each cardholder has their own personal identification number, known only by them. Besides badging your card, the method of access to an access zone during certain times may include entering your PIN.

PIN Entry Timeout

Maximum time allowed for a cardholder to enter their PIN. Measured from card badge.

PIN Pad

A numeric key pad used to enter PINs.

PINs mode

A door state where access is granted by entering a single, system defined PIN number.

PIR (Passive InfraRed) Detector

A device that senses body heat to detect motion, and generates an alarm condition.

Polling

Sending messages between devices to ascertain their status.

Power Failure

Mains power to the Controller is lost.

Push Configuration

A pop-up menu option available for some items. This forces an update of the configuration of the site item to the Controller. This is most likely to be used after an upgrade of Command Centre.

R

Reader Module

The Reader Module is used with the Gallagher Controller 6000 to allow connection of readers, inputs and outputs. While the Controller 6000 is the processing board, the Reader Module handles I/O and reader communications.

Remote item

Remote items are only editable from workstations connected to the server they were created on in a multi-server system. Some remote items can be viewed from servers other than their home server, and behave as **read-only** representations of the original item when viewed from a remote server.

Restore

The working system can be restored from a backup file record.

S

Schedule

A schedule is a 'list of times and states that controls an item'.

Secure Access

A state during which only authorised card-holders are allowed access to an access zone or elevator level, and may require an optional PIN. The doors to a secure access zone will be in a normally locked state and elevator buttons normally disabled.

Server

The Command Centre Server runs on a personal computer (PC) under any of the following Microsoft operating systems:
- Windows Server 2022
- Windows 11 Pro/Enterprise,
- Windows 10 Pro/Enterprise,
- Windows Server 2019,

- Windows Server 2016,
The Command Centre Server is a background application which drives Command Centre workstations and enables the programming of the Controllers.

Shunting Inputs

The Input's state is to be ignored while in a shunted state and will no longer trigger alarms. When an Input is shunted, it is taken out of the system until such time as it is put back in. Shunting an Input is the same as doing a 'Stop Communications' override on an Input.
Note: Input Shunted and Input Isolated are both in the same Event Group, but shunting takes precedence. This means that if an Input has been shunted it will not also get isolated. If an Input has been isolated, it may however be shunted. The isolation ends when the Alarm Zone changes state, but the shunt will continue until the shunt is removed.

Single Client Code Reporting (Contact ID)

Single Client Code Reporting is when a single account code is used to send Contact ID, (i.e. each Alarm Zone will report under a single client code. The Alarm Zones are defined by the GG value).

Example:
Account Code = 1234, so an arm area 1 will be 123418340201001 and the disarm 123418140201001.
Account Code = 1234, so an arm area 2 will be 123418340202001 and the disarm 123418140202001, and so on.

(Check with your monitoring station that they support single client code reporting before sending any data.)

Site

The building(s) and areas controlled by the Command Centre system.

Site Plan

A window in Command Centre which displays the layout (a map of the site), and enables users to see the relationship of devices/site items to one another. Users can also monitor the status of site items and process alarms from this window.

Status

This refers to the current state of an item attached to the Command Centre system. The status displayed for each item will depend on the type of device, (e.g. an Input would normally be opened or closed, whereas a Door would be secure, free, etc.).

Swipe Card

A plastic access card which is swiped through a slot in a door reader to allow access.

System Division

Division, (or system division), allows a site to be divided into smaller divisions and sub-divisions. Each sub-division can manage their own security needs without requiring access to other divisions' site configuration or access information.

T

Tailgating

Following someone through a door without presenting one's own credential.

Tamper

Someone has either opened a device or a cabinet containing devices, or tried to remove them from their mountings, or the wiring to inputs has gone open or short circuit.

Tamper Return to Normal

The tamper condition has been corrected, (e.g. the cabinet door has been closed).

Tree view

A tree view displays information with branches representing the different levels in the hierarchy.

Turnstile

A door which only allows one person through between opening and closing. Tailgating is difficult with turnstiles.

V

Valid Access

Any attempt at entry or exit, such as presenting a card or entering a PIN, which would normally allow access.

Visitor Cardholder

A cardholder that has access to certain zones on a site, but only if an escort is present to validate their access.

W

Workstation

The Command Centre workstation is the user interface to the Command Centre system. Through workstations, operators can program and modify cardholder access and site set up information, monitor what is happening on your site, process alarms and generate reports.

Wrong PIN

The Cardholder has entered an incorrect PIN number and must enter the correct number before gaining entry. See also PIN.

Z

Zone Count Maximum

The number of Cardholders in the zone has reached the maximum threshold.

Zone Count Mid-Range

The number of Cardholders in the zone has reached the mid-range threshold.

Zone Count Minimum

The number of Cardholders in the zone has fallen to the minimum threshold.

Zone Counting

Zone counting is simply keeping count of the number of cardholders inside an Access Zone or an Access Zone Group.

Index

A

Access Command Centre • 2-2
Access Group Privileges, Inheriting • 34-2
Access Group Report • 39-31
Access Groups • 34-1
Access Groups and Lineage • 34-2
Access Groups, Configuring Privileges for Remote Arming Terminal Access • 34-13
Access Report • 39-33
Access Zone Lockdown • 10-9
Access Zones • 10-1
Access Zones, Adding • 10-3
Access Zones, Anti-Passback • 10-14
Access Zones, Configuring No-Alone Zones • 10-28
Access Zones, Configuring Personalised Actions • 10-36
Access Zones, Configuring Pushbutton Overrides • 10-34
Access Zones, Configuring Strict Anti-tailgating • 10-20
Access Zones, Enabling Zone Counting • 10-22
Access Zones, Lockdown • 10-9
Access Zones, Manually Resetting Zone Counts • 10-32
Access Zones, Understanding • 10-2
Acknowledging alarms via SMS or email • 35-27
Acknowledging an alarm • 42-16
Action on Access • 22-31
Action Plans • 15-1
Action Plans, Assigning to Events • 15-10
Action Plans, Creating • 15-4
Active Directory Single Sign-on • 57-1
Activity Report • 39-15
Adding a Background • 47-17
Adding a Barcode • 47-24, 47-51
Adding a Card to a Cardholder • 32-9
Adding a Card transformation • 54-47
Adding a Cardholder field transformation • 54-44
Adding a Competency transformation • 54-54
Adding a Magstripe object • 47-27
Adding a MIFARE Classic object • 47-33
Adding a MIFARE DESFire object • 47-37
Adding a MIFARE Plus object • 47-35
Adding a Morpho DESFire object • 47-29
Adding a Morpho FVP DESFire object • 47-31
Adding a Morpho FVP MIFARE Classic object • 47-32
Adding a Morpho MIFARE Classic object • 47-28
Adding a MorphoWave DESFire object • 47-30
Adding a new Access Zone • 10-3
Adding a new Cardholder • 32-2
Adding a new child to an external system • 24-11
Adding a new day category • 11-2
Adding a new external system • 24-7
Adding a new Interlock Group • 22-15
Adding a new server to a Star structure (Multi-Server systems) • 49-15
Adding a new Universal Card Format •26-2
Adding a new version of Device Software • 27-2
Adding a Non-diversified MIFARE DESFire object to a card layout • 47-46
Adding a Personal Data Field transformation • 54-45
Adding a Salto MIFARE Classic object to a card layout • 74-99
Adding Salto to the URL Tile • 74-105
Adding an Access Group transformation • 54-51
Adding an ASCII DESFire object • 47-44
Adding an ASCII MIFARE Classic object • 47-38
Adding an ASCII MIFARE Plus object • 47-41
Adding an Image • 47-22
Adding an Insertion Tag to an Alarm Instruction • 17-3
Adding Areas to Site Plans • 18-13
Adding Command Lines for Macros • 20-13
Adding Competencies to Access Zones • 52-15
Adding Day Categories to Schedules • 12-7
Adding external systems to a Site Plan • 24-72
Adding items to the Status Viewer • 45-5
Adding Lines to Site Plans • 18-13
Adding Reasons for printing • 47-57
Adding Rectangles to Site Plans • 18-13
Adding text objects • 47-20, 47-50
Advanced Drag and Drop feature • 2-26

Advanced Reports • 39-81
Advanced tab, Server Properties • 6-30
Alarm • 42-6
Alarm details, Viewing • 42-11
Alarm Flooding, Configuring • 42-7
Alarm Flooding tab, Server Properties • 6-9
Alarm Groups, Collapsing • 42-10
Alarm Instruction Defaults tab, Server Properties • 6-14
Alarm Instructions tab • 3-22
Alarm Notes tab, Server Properties • 6-17
Alarm Sounds • 42-23
Alarm Transmission tab, Server Properties • 6-15
Alarm Viewer window, Opening • 42-8
Alarm Viewer, Changing the behaviour • 42-26
Alarm Viewers • 42-6
Alarm Zone States tab, Server Properties • 6-11
Alarm Zones • 14-1
Alarm Zones, Adding multiple items • 14-18
Alarm Zones, Setting up • 14-3
Alarms, Acknowledging • 42-16
Alarms, Flooding • 42-7
Alarms, Force-Process all • 42-20
Alarms, Muting • 42-25
Alarms, Notify Restoral • 42-29
Alarms, Processing • 42-17
Alarms, Processing all in a Priority Group • 42-20
Alarms, Processing numerous alarms • 42-20
Alarms, Quick Processing • 42-18
Alarms, Sounds • 42-23
Alarms, Viewing from Site Plans • 43-4
Alarms, Viewing images associated with an alarm • 42-15
Allegion Engage Interface • 78-1
Allegion Engage Interface, Allegion Engage configuration • 78-8
Allegion Engage Interface, Command Centre configuration • 78-19
Allegion Engage Interface, Creating an Engage Site in Gallagher Configuration Client • 78-3
Answering a call (Intercom Systems) • 24-38
Anti-Passback • 10-14
Anti-Passback, Configuring • 10-15
Anti-Passback, Forgive a specific Cardholder • 10-20
Anti-Passback, Forgive All Cardholders • 10-18
Aperio Integration • 76-1
Aperio Integration, Command Centre Site Configuration • 76-29
Aperio Integration, Communication Hubs • 76-4
Aperio Integration, Configuration for Mobile Connect • 76-67
Aperio Integration, Configuring Override Credentials for Offline Access • 76-71
Aperio Integration, Configuring R100 Readers • 76-74
Aperio Integration, Configuring the Aperio Locks/Readers • 76-42
Aperio Integration, Configuring the Security Mode • 76-57
Aperio Integration, Connecting the communication hubs to a Gallagher Controller • 76-7
Aperio Integration, Enabling the Privacy Mode • 76-61
Aperio Integration, Enabling the Smart Credential cache • 76-64
Aperio Integration, Site Configuration • 76-10
Aperio Integration, Troubleshooting • 76-78
Aperio Mobile Access Integration • 31-20
Aperio Site Configuration • 76-10
Apple Employee Badge • 69-1
Apple Employee Badge, 1. Configure Apple Keys • 69-3
Apple Employee Badge, 2. Configure Mobile Wallet Readers • 69-4
Apple Employee Badge, 3. Configure the Apple Employee Badge Type • 69-6
Apple Employee Badge, 4. Enable In-app Apple Employee Badge Provisioning • 69-8
Apple Employee Badge, 5. Manage Apple Employee Badges • 69-10
Archives, Configuring • 40-3
Archives, Performing • 40-8
Archives, Restoring • 40-11
Archiving Image Sequences (DVR) • 24-31
Assigning a Commend Console to a Workstation • 60-8
Assigning a Fence Zone to a Terminal • 48-6
Assigning Action Plans to Events • 15-10
Assigning an escort • 50-125
Assigning an OSDP Compliant Reader to a Gallagher Controller • 79-7
Assigning an OSDP Veridt Stealth PIV Reader to a Gallagher PIV Controller 6000 • 56-27
Assigning Cardholders to Roles via Bulk Change • 35-19
Assigning Competencies to Cardholders • 52-12
Assigning Days to Day Categories • 13-5

Assigning Device Software to devices • 27-5
Assigning permanent cardholders to Cardholder Division • 50-46
Assigning Z20 and D10 sensors to a Controller 6000 • 55-20
Assigning Schlage devices • 77-19
Assigning the Alarm Transmitter/Dialler to a Controller • 29-25
Assigning the reader to the Controller, QR Code Readers • 80-2
Audit Trail, Salto Lock Interface • 74-66
Audit Trail of Cardholder changes • 32-28
Austco Intercoms • 58-1
Austco Intercoms, Assigning an Austco Console to a Workstation • 58-5
Austco Intercoms, Configuring an Austco Intercom Item • 58-4
Austco Intercoms, Configuring an Austco Intercom System • 58-3
Austco Intercoms, Locating an Austco Symbol • 58-6
Automatically Generated Reports • 39-62
Auto-Process all alarms • 42-20

B

Backups • 40-1
Backups, Performing • 40-14
Backups, Restoring • 40-19
Batch Printing and/or Encoding Cards • 47-63
Batch Printing/Encoding, Bureau Batch Jobs • 47-67
Batch Printing/Encoding, Cardholder Batch Jobs • 47-70
Biometric Integration • 65-1
Biometric Integration, Configuring Biometric Verification • 65-62
Biometric Integration, Encoding Morpho Cards for Verification • 73-67
Biometric Integration, Performing Overrides on a Morpho Biometric Reader • 73-69
Bulk Changes • 38-1
Bulk Changes, Assigning Cardholders to Roles • 35-19
Bulk Changes, Editing and Running • 38-24
Bulk Changes, Initiating Alarm Zone Bulk Changes • 38-26
Bulk Changes, Initiating Cardholder Bulk Changes • 38-3
Bulk Changes, Initiating Controller 6000 Bulk Changes • 38-30
Bulk Changes, Initiating Door Bulk Changes • 38-37
Bulk Changes, Initiating Division Bulk Changes • 38-15
Bulk Changes, Initiating Inactive Cardholder Bulk Purges • 38-19
Bulk Changes, Initiating Reader Bulk Changes • 38-34
Bureau Printing/Encoding, Setting a Card Type for • 47-65

C

Calendars • 13-1
Calendars, Assigning Days to Day Categories • 13-5
Calendars, Creating a Special Calendar • 13-3
Calendars, Resetting Dates • 13-7
Calendars, Viewing/Editing the Default Calendar • 13-2
Cameras tab • 3-24
Capturing an Image • 33-10
Card Editor Toolbar • 47-14
Card Layouts, Designing • 47-13
Card Security tab, Server Properties • 6-37
Card Trace, Enabling • 32-16
Card Types • 7-1
Card Types, Setting a Card Type for Bureau Printing/Encoding • 47-65
Card Types, Setting up • 7-2
Cardholders • 32-1
Cardholder Batch Jobs • 47-70
Cardholder Competencies • 52-1
Cardholder Competencies, Adding to Access Zones • 52-15
Cardholder Competencies, Configuring • 52-5
Cardholder Competencies, Overriding Operator Group Competencies • 52-20
Cardholder Competencies, Running a Cardholder Report from a Cardholder • 32-30
Cardholder Competencies, Scenario • 52-3
Cardholder Management across Divisions • 9-5
Cardholder Report •39-7
Cardholder Report, Running from a Cardholder • 32-30
Cardholders • 32-1
Cardholders, Adding • 32-2
Cardholders, Adding a Card to • 32-9
Cardholders, Assigning to Roles via Bulk Change • 35-18
Cardholders, Audit Trail of changes • 32-28
Cardholders, Configuring User Codes for access at Card Readers with keypads • 32-25

Cardholders, Configuring User Codes for Remote Arming Terminal Access • 32-23
Cardholders, Copying all Cardholders under a Role •35-21
Cardholders, Copying details • 32-7
Cardholders, Disabling the System Operator • 32-34
Cardholders, Editing Card details • 32-15
Cardholders, Editing PDF data • 32-20
Cardholders, Enabling Card Trace • 32-16
Cardholders, Reactivating Expired or Disabled cards • 32-17
Cardholders, Reading MIFARE Cards using a MIFARE USB Encoder • 32-31
Cardholders, Removing a Card from • 32-13
Cardholders, Running a Cardholder Report from a Cardholder • 32-30
Cards, Adding Cards to Cardholders • 32-9
Cards, Copying layouts • 47-54
Cards, Designing Layouts • 47-13
Cards, Editing details • 32-16
Cards, Re-issuing for a Cardholder • 32-20
Cards, Reactivating Expired or Disabled • 32-17
Cards, Removing from Cardholders • 32-13
CCC Identifiers (Contact ID) • Appx C-1
Challenge • 22-19
Challenge tab, Server Properties • 6-63
Challenge Viewer - Controlled Challenge mode • 22-27
Challenge Viewer - View-Only mode • 22-29
Challenge Viewer, Controlled Challenge mode • 22-27
Challenge, Configuring Challenge • 22-20
Challenge, Configuring Doors for Controlled Challenge mode • 22-24
Changing an expired password • 2-16
Changing Operator Passwords • 2-15
Changing registry values for PDF417 Barcodes • 47-25
Changing the Alarm Viewer behaviour • 42-26
Changing the Connection profile on the Intercel Sam3G+ module • 29-22
Changing the Day Category colour • 11-3
Changing times and states within Schedules • 12-8
Changing your password • 2-17
Changing your user name and password • 2-17
CipherToken Card Support • 71-1
CipherToken Card Support, CipherToken cards in Command Centre • 71-7
CipherToken Card Support, Configuring and printing CipherToken card layouts • 71-6
CipherToken Card Support, Enrolling a CipherToken configuration card • 71-2
CipherToken Card Support, Rolling configuration on a CipherToken card • 71-5
Class 5 End-of-Line Module (ELM) • 61-1
Class 5 End-of-Line Module (ELM), Configuring a Class 5 ELM • 61-2
Class 5 End-of-Line Module (ELM), Configuring Class 5 ELMs for Test Modes • 61-6
Class 5 End-of-Line Module (ELM), Performing Overrides for Class 5 ELMs • 61-8
Close Command Centre • 2-11, 2-13
Collapsing the alarm groups • 42-10
Column Headers, Repositioning • 3-6
Column Headers, Resizing • 3-5
Command Centre Site Configuration • 5-2
Command Centre Site Configuration for Visitor Management • 50-7
Command Centre Site Configuration for Salto Lock Interface • 74-71
Command Lines, Adding to Macros • 20-13
Commend Intercom Items, Configuring • 60-6
Commend Intercom Systems, Configuring • 60-4
Commend Intercoms, Using • 60-9
Common Regular Expressions • 33-8
Communications Encryption, Morpho Biometric Integration • 73-56
Compatibility, Salto Lock Interface • 74-3
Competency Bulk Changes • 52-31
Competency Messages tab, Server Properties • 6-24
Configurable Ports - NAT Solution • 21-40
Configuration Example, Enterprise Data Interface • 54-59
Configuration for Mobile Connect, Aperio Integration • 76-67
Configuration of OneLink • 21-18
Configuration Process, Recommended • 5-2
Configuration Wizard • 5-9
Configuring a Class 5 End-of-Line Module (ELM) • 61-2
Configuring a Commend Intercom Item • 60-6
Configuring a Commend Intercom System • 60-4
Configuring a Controller 7000 or 7000 Single Door for 802.1x • 21-22
Configuring a D10 Tautwire Sensor • 55-18
Configuring a Locker • 62-10
Configuring a Locker Bank • 62-3

Configuring a reader for Mobile Connect, Mobile Connect • 31-8
Configuring a Shift, Shifts • 70-3
Configuring a SIP Device, SIP Integration • 67-8
Configuring a ThyssenKrupp Elevator • 81-10
Configuring a ThyssenKrupp Elevator Group • 81-5
Configuring a ThyssenKrupp Insight Elevator System • 81-2
Configuring a ThyssenKrupp Kiosk • 81-14
Configuring a User Code for Terminal Access • 32-23
Configuring a Z10 Tension Sensor • 55-3
Configuring a Z20 Disturbance Sensor • 55-15
Configuring Access Group Privileges for Terminal Access • 34-13
Configuring Access Groups • 34-4
Configuring Access Groups for Test Modes • 46-9
Configuring Access Groups, Salto Lock Interface • 74-80
Configuring access to Salto Outputs • 74-89
Configuring Alarm Zones for Test Modes • 46-7
Configuring an Alarm Transmitter/Dialler • 29-10
Configuring and printing CipherToken card layouts • 71-6
Configuring an Elevator Car HLI • 23-19
Configuring an Elevator Kiosk Control Schedule • 81-12
Configuring an External System Server • 24-7
Configuring an F22 Fence Controller • 48-19
Configuring an F31/F32/F41/F42 Fence Controller • 48-9
Configuring an HBUS Contact Card Reader • 21-109
Configuring an HBUS I/O Interface • 21-127
Configuring an HBUS QuickSwitch Board • 21-132
Configuring an interface, Enterprise Data Interface • 54-3
Configuring an OSDP Reader • 79-3
Configuring an OSDP Veridt Stealth PIV Reader • 56-22
Configuring Anti-Passback, Access Zones • 10-14
Configuring Archives • 40-3
Configuring Biometric Verification • 65-62
Configuring Cardholder Competencies • 52-5
Configuring Cardholders for Test Modes • 46-11
Configuring Challenge • 22-20
Configuring Class 5 End-of-Line Modules (ELMs) for Test Modes • 61-6
Configuring Competencies • 52-5
Configuring DNS Servers for Controllers • 21-31
Configuring Doors for Controlled Challenge mode • 22-24
Configuring Elevator Cars • 23-2
Configuring Enrolment Templates • 8-2
Configuring Entra ID Single Sign-on and Automatic logon • 72-3
Configuring EOL Resistors for devices • 21-46
Configuring extended access time for a Door • 22-11
Configuring FTCAPI Trigger Strings and Reflected Outputs, External Systems • 24-24
Configuring HBUS Devices • 21-65
Configuring HBUS Terminals • 21-74
Configuring High Level Elevator Interfaces • 23-14
Configuring Inputs for Test Modes • 46-5
Configuring Items for Contact ID • 29-27
Configuring Local Overrides at Card Readers • 45-13
Configuring Multi-Break Alarms for Test Modes • 45-14
Configuring No-Alone Zones • 10-28
Configuring Offline Monitoring • 21-33
Configuring OneLink • 21-18
Configuring operators, Enterprise Data Interface • 54-2
Configuring Personalised Actions for Access Zones • 10-36
Configuring Printers for Reports automatically generated via Macros • 39-70
Configuring Pushbutton Overrides • 10-34
Configuring Report Scheduling • 39-65
Configuring Salto Access Zones • 74-86
Configuring Salto Doors • 74-84
Configuring Salto options for Cardholders • 74-88
Configuring Secondary Ethernet operation mode • 21-20
Configuring Single Sign-on and Automatic logon • 57-2
Configuring Strict Anti-tailgating • 10-20
Configuring terminals for Test Modes • 46-12
Configuring the Card Type, QR Code Readers • 80-3

Configuring the Controller RS-485 Bus for OSDP, Morpho Biometric Integration • 73-73
Configuring the SIP Service, SIP Integration • 67-3
Configuring the Tag Tracking feature • 66-3
Configuring User Codes for access at Card Readers with keypads • 32-25
Configuring User Codes for Terminal Access • 32-23
Configuring Visitor Management Kiosk • 51-16
Configuring Visitor Management setup • 50-7
Connecting and configuring a QR Code Reader • 80-1
Connecting to the Cloud • 28-7
Contact ID Assignment Report • 39-58
Contact ID, Configuring Items • 29-27
Contact ID, Creating Alarm Diallers • 29-10
Contact ID, Sample Messages • 29-33
Contact ID, Setting Country Codes • 29-6
Controller 6000, Creating • 21-2
Controller 7000, Creating • 21-2
Controller 7000 Single Door, Creating • 21-9
Controller Defaults tab, Server Properties • 6-59
Controller Web Server tab, Server Properties • 6-61
Controllers, Configuring EOL Resistors for • 21-46
Controllers, Configuring Offline Monitoring • 21-33
Controllers, Configuring Secondary Ethernet operation mode • 21-20
Controllers, Linking devices to • 21-48
Copying all Cardholders under a Role • 35-22
Copying an Elevator Car • 23-23
Copying Card Layouts • 47-54
Copying Cardholder details • 32-7
Country Codes, Setting for Contact ID • 29-6
Creating a Controller 7000 Single Door • 21-9
Creating a Fence Zone • 48-2
Creating a Guard Tour Report • 53-10
Creating a new Action Plan • 15-4
Creating a new Alarm Instruction • 16-2
Creating a new Custom Field • 6-83
Creating a new Guard Tour • 53-2
Creating a new Icon Set • 19-2
Creating a new Licensing Group • 30-2
Creating a new Logic Block • 25-15
Creating a new Macro • 20-2
Creating a new Morpho Biometric Card Type • 73-27
Creating a new Morpho Biometric Reader • 73-35
Creating a new Personal Data Field • 33-2
Creating a new report • 39-2
Creating a new Schedule • 12-2
Creating a new Site Plan • 18-4
Creating a new third party reader, QR Code Readers • 80-1
Creating a new Virtual Output • 25-21
Creating a new Workstation Item • 28-2
Creating a Notification Filter • 35-5
Creating a Reception • 50-10
Creating a Remote Server (Multi-Server systems) • 49-8
Creating a REST API Client Item • 28-13
Creating a Schlage Door • 77-14
Creating a Schlage PIM • 77-11
Creating a Special Calendar • 13-3
Creating a Temperature Report • 48-36
Creating a visit • 50-86
Creating a visitor • 50-90
Creating a Voltage Report • 48-34
Creating an Alarm Dialler • 29-10
Creating an Aperio Door • 76-30
Creating an Insertion Tag • 17-2
Creating Card Types • 7-2
Creating Cardholders • 32-2
Creating Controller 6000s • 21-2
Creating Controller 7000s • 21-2
Creating Devices • 21-45
Creating Divisions • 9-3
Creating Doors • 22-2
Creating Inputs and Outputs • 21-50
Creating Macros • 20-2
Creating Readers • 21-57
Creating Salto Doors or ESDs • 74-41
Creating Salto Lockers • 74-46
Creating Salto Outputs • 74-56
Creating Salto Rooms • 74-48
Creating Salto Suites • 74-51
Creating Salto Zones • 74-54
Creating Visitor Type and Host Type Groups • 50-15
Custom Field Types, Creating • 6-83
Custom Fields, Creating • 6-83
Custom Fields tab, Server Properties • 6-81
Customising Report Printouts • 39-75

D

D10 Tautwire Sensors, Configuring • 55-18
Z20 Disturbance Sensors, Configuring • 55-15
Data Retention tab, Server Properties • 6-72

Database Maintenance tab, Server Properties • 6-57
Day Categories • 11-1
Day Categories, Adding to Schedules • 12-6
Day Categories, Changing the colour • 11-3
Day Categories, Removing from Schedules • 12-7
DCOM Setup Utility • 4-1
Default Calendar, Viewing/Editing • 13-2
Deleting a child server from a Star structure (Multi-Server systems) • 49-24
Deleting a server from a Peer-to-Peer structure (Multi-Server systems) • 49-22
Deleting items • 3-27
Designing Card Layouts • 47-13
Device Software • 27-1
Device Software, Adding a new version • 27-2
Device Software, Assigning to devices • 27-5
Device Software, Loading to a Controller 6000 or 7000 using USB stick • 27-9
Devices, Creating • 21-45
Devices, Linking to Controllers • 21-48
Devices, Linking to Inputs and Outputs • 21-56
Digital ID Types, Setting up • 31-6
Digital ID Types, Working with Digital ID Type objects • 47-50
Digital Video Recording (DVR) • 24-25
Disability access for Doors • 22-11
Disabled cards, Reactivating • 32-17
Disabling the System Operator • 32-34
Disturbance Sensors, Configuring • 55-15
Divisions • 9-1
Divisions and Lineage • 9-2
Divisions, Cardholder Management across Divisions • 9-5
Divisions, Setting up • 9-3
DNS Servers, Configuring for Controllers • 21-31
Door Icons, Salto Lock Interface • 74-106
Doors • 22-1
Doors, Action on Access • 22-31
Doors, Challenge • 22-19
Doors, Creating • 22-2
Doors, Disability access • 22-11
Doors, Extended access time • 22-11
Doors, Interlocking • 22-13
Doors, Special access • 22-11
Double-card Override • 45-13
Drawing on Site Plans • 18-12
Dual Monitors • 2-24
Duplicating a Macro • 20-20
DVR (Digital Video Recording) • 24-25
DVR, Adding DVR Cameras • 24-10
DVR, Adding DVR Cameras to Site Plans • 24-24
DVR, Adding DVR Systems • 24-4
DVR, Archiving Image Sequences • 24-31
DVR, Editing Action Plans with DVR Cameras • 24-26

E

Edit and View modes, Site Plans •18-6
Editing Action Plans with DVR Cameras • 24-26
Editing Actions for a Macro • 20-10
Editing and Running a saved Cardholder Bulk Change • 38-24
Editing Card details • 32-15
Editing items • 3-26
Editing Scheduled run times for a Macro • 20-12
Editing settings of an existing report • 39-77
Editing/Removing Actions for a Macro • 20-10
Editing/Removing Scheduled run times for a Macro • 20-12
Editing the Salto Server • 74-73
Elevator Car HLI, Configuring • 23-19
Elevator Cars • 23-1
Elevator Cars, Configuring • 23-2
Elevator Cars, Copying • 23-23
Elevator HLI • 23-6
Enabling Card Trace • 32-16
Enabling DHCP for a new Controller using the wizard • 21-37
Enabling Event/Alarm Notifications for a Cardholder • 35-9
Enabling SIP Intercoms for a Workstation, SIP Integrations • 67-10
Enabling Zone Counting • 10-22
Encoding cards, Salto Lock Interface • 74-91
Encoding Morpho Cards for Verification • 73-67
Enrolling a CipherToken configuration card • 71-2
Enrolling a UK GovPASS configuration card • 64-2
Enrolling Users, Morpho Biometric Integration • 73-44
Enrolment Wizard and Templates • 8-1
Enrolment Wizard and Templates, Configuring Enrolment Templates • 8-2
Enrolment Wizard and Templates, Using the Enrolment Wizard • 8-7
Enterprise Data Interface, Configuration Example • 54-59

Enterprise Data Interface, Configuring an interface • 54-3
Enterprise Data Interface, Configuring operators • 54-2
Enterprise Data Interface, Manually running an interface • 54-55
Enterprise Data Interface, Stopping an interface • 54-56
Enterprise Data Interface, the failed file • 54-58
Enterprise Data Interface, the log file • 54-57
Enterprise Data Interface, Troubleshooting • 54-61
Entra ID admin center configuration • 72-3
Entra ID Single Sign-on • 72-1
Entra ID Single Sign-on, Configuring and Automatic logon • 72-3
Entra ID Single Sign-on, Entra ID admin center configuration • 72-4
Entra ID Single Sign-on, Linking operators to their Entra ID account • 72-5
Entra ID Single Sign-on, Migrating from Active Directory Single Sign-on • 72-7
EOL Resistors, Configuring for devices • 21-46
Evacuation Report • 39-23
Event Defaults tab, Server Properties • 6-12
Event Priorities tab, Server Properties • 6-7
Event Response tab • 3-20
Event Viewer • 42-1
Event Viewer window, Opening • 42-2
Events with Restorals • 42-5
Events, Viewing details • 42-3
Exception Report • 39-35
Existing Reports, Editing Settings • 39-77
Existing Reports, Printing • 39-73
Exiting Command Centre • 2-11, 2-13
Expanding an Object Box • 47-48
Expired cards, Reactivating • 32-17
Extended access time for a Door • 22-11
External System Server, Configuring • 24-7
External Systems • 24-1
External Systems, Adding a new child to an external system • 24-10
External Systems, Adding a new external system • 24-4
External Systems, Adding external systems to Site Plans • 24-72
External Systems, Configuring an External System Server • 24-7
External Systems, Configuring FTCAPI Trigger Strings and Reflected Outputs • 24-24
External Systems, SchindlerID • 24-28

F

Fence Configuration example • 55-8
Fence Controller, Configuring an F22 Fence Controller • 48-19
Fence Controller, Configuring an F31/F32/F41/F452 Fence Controller • 48-9
Fence Zone, Creating • 48-2
FIDO2 Credentials, Logon with • 2-7
Find Tool • 41-1
Find Tool, Search using 'Advanced' details • 41-9
Find Tool, Search using 'General' and 'Time' details • 41-5
Find Tool, Search using 'Related To' details • 41-7
Flexible Shift Pattern rules • 39-45
Flood Alarms, Configuring • 42-7
Formatting Cards for Photo ID • 47-16
FTCAPI Trigger Strings, Configuring for External Systems • 24-18
Functionality provided by Alarm Input Test Modes • 46-2

G

Gallagher Command Centre Site Configuration • 5-2
Gallagher Networked Perimeter Security Systems • 48-1
General tab • 3-18
Generic Properties Configuration • 3-14
Generic Properties, Alarm Instructions tab • 3-22
Generic Properties, Event Response tab • 3-20
Generic Properties, General tab • 3-18
GovPASS Card Support • 64-1
GovPASS Card Support, Enrolling a configuration card • 64-2
GovPASS Card Support, Rolling configuration • 64-5
GovPASS cards in Command Centre • 64-6
Granting Temporary Access by Access Group • 34-18
Granting Temporary Access by Cardholder • 34-21
Grid View • 3-4
Guard Tours, Creating • 53-2
Guard Tours, Creating a Report • 53-10
Guard Tours, Running • 53-6

H

HALO Smart Sensor Integration • 82-1
Hardware • 21-1
HBUS Devices, Configuring • 21-65
HBUS I/O Interface, Configuring • 21-127
HBUS QuickSwitch Board, Configuring • 21-132
HBUS Terminals, Configuring • 21-74
HBUS Terminal Defaults tab, Server Properties • 6-76
Help menu • 2-14
High Level Elevator Interfaces, Configuring • 23-14
High Level Interface Elevator Cars • 23-6
HLI Elevator Cars, Understanding • 23-7
How to configure a site • 5-2
HVplus mode, Using • 48-40

I

Icon Sets • 19-1
Icon Sets, Creating • 19-2
Icon Sets, Modifying • 19-5
Icons tab, Server Properties • 6-80
Icons, Removing from Site Plans • 18-24
Images, Capturing • 33-10
Import tab, Server Properties • 6-56
Incoming Email tab, Server Properties • 6-52
Inheritance of Access Group Privileges • 34-2
Initialising Alarm Zone functionality • 14-14
Initiating a new Alarm Zone Bulk Change • 38-26
Initiating a new Cardholder Bulk Change • 38-3
Initiating a new Controller 6000 Bulk Change • 38-30
Initiating a new Door Bulk Change • 38-37
Initiating a new Division Bulk Change • 38-15
Initiating a new Reader Bulk Change • 38-34
Initiating Alarm Zone Bulk Changes • 38-26
Initiating an Inactive Cardholder Bulk Purge • 38-19
Initiating Cardholder Bulk Changes • 38-3
Initiating Controller 6000 Bulk Changes • 38-30
Initiating Division Bulk Changes • 38-15
Initiating Inactive Cardholder Bulk Purges • 38-19
Inputs and Outputs, Creating • 21-50
Inputs and Outputs, Linking to devices • 21-56
Insertion Tags • 17-1
Insertion Tags, Adding to an Alarm Instruction • 17-3
Insertion Tags, Creating • 17-2
Installation Instructions for Salto Lock nterface • 74-5
Installation, Morpho Biometric Integration • 73-3
Installation, Salto Lock Interface • 74-5
Installing MorphoAccess Readers• 73-8
Installing the FTCAPI Middleware Framework (FMF) • 24-22
Installing the IP Alarms Receiver Software • 29-35
Intercoms, Austco • 58-1
Intercoms, Jacques • 59-1
Interlocking Doors • 22-13
Interlocking Doors, Adding a new Interlock Group • 22-15
Items, Adding to Status Viewer • 45-5
Items, Removing from Status Viewer • 45-6

J

Jacques Intercoms • 59-1
Jacques Intercoms, Answering a call • 59-11
Jacques Intercoms, Configuring an Intercom • 59-5
Jacques Intercoms, Configuring an Intercom System • 59-3
Jacques Intercoms, Opening the Intercom window • 59-7
Jacques Intercoms, Placing a call • 59-10
Joining Fields in the same Text Object • 47-21

K

Knowing your way around • 3-1

L

Licensing Groups • 30-1
Licensing tab, Server Properties • 6-4
Linking devices to Controllers • 21-48
Linking Inputs and Outputs to devices • 21-56
Linking operators to their Active Directory account • 57-3
Linking operators to their Entra ID account • 72-5
List Windows • 3-2
Loading Device Software to a Controller 6000 or 7000 using a USB stick • 27-9
Local Overrides, Configuring at Readers • 45-13
Locating the Cardholder for Encoding Cards • 47-4
Lockdown of Access Zones • 10-8

Locker Management Solution • 62-1
Locker Management Solution, Configuring a Locker • 62-12
Locker Management Solution, Configuring a Locker Bank • 62-3
Locker Management Solution, Locker Bank Status and Overrides • 62-11
Locker Management Solution, Locker Status and Overrides • 62-14
Logging on to the IP Alarms Receiver • 29-39
Logic Block and Virtual Outputs • 25-1
Logic Block and Virtual Outputs, Scenarios • 25-4
Logic Blocks, Creating a new Logic Block • 25-15
Logoff • 2-11
Logon • 2-2
Logon with FIDO2 Credentials • 2-7
Logout • 2-1

M

Macros • 20-1
Macros, Adding Command Lines • 20-13
Macros, Creating • 20-2
Macros, Duplicating • 20-20
Macros, Editing Actions • 20-10
Macros, Editing Scheduled run times • 20-12
Macros, Placing on Site Plans • 20-17
Macros, Removing Actions • 20-10
Macros, Removing Scheduled run times • 20-12
Macros, Running • 20-18
Macros, Scheduling • 20-7
Magnetic window snapping • 2-25
Manually Resetting Zone Counts • 10-32
Manually running an interface, Enterprise Data Interface • 54-55
Marking a visitor 'Off-Site' (Leave Site) • 50-117
Marking a visitor 'On-Site' • 50-115
Marking a visitor 'Temp Off-Site' • 50-116
Measurement Units tab, Server Properties • 6-28
MIFARE Site Key Migration • 6-43
Migrating from Active Directory Single Sign-on to Entra ID Single Sign-on • 72-7
Migrating Salto Legacy Cards to Salto Native, Salto Lock Interface • 74-36
Mobile Connect • 31-1
Mobile Connect, Aperio Mobile Access Integration • 31-20
Mobile Connect, Configuring a reader for Mobile Connect • 31-8
Mobile Connect, Performing Bluetooth® Actions • 31-14
Mobile Connect, SALTO Mobile Access Integration • 31-19
Mobile Connect, Setting up Digital ID Types • 31-6
Mobile Connect, Setting up Mobile Credential Types • 31-3
Mobile Connect Settings tab, Server Properties • 6-73
Mobile/SMS Notifications tab, Server Properties • 6-54
Modifying an existing Icon Set • 19-5
Monitoring Fence Alarms and Events • 48-29
Monitoring Fence Controller Status • 48-28
Monitoring Fence Zone Status • 48-27
More Challenge tab, Server Properties • 6-63
Morpho Biometric Integration • 73-1
Morpho Biometric Integration, Communications Encryption • 73-56
Morpho Biometric Integration, Configuring Biometric Verification • 73-65
Morpho Biometric Integration, Configuring the Controller RS-485 Bus for OSDP • 73-73
Morpho Biometric Integration, Creating a new Morpho Biometric Card Type • 73-27
Morpho Biometric Integration, Creating a new Morpho Biometric Reader • 73-35
Morpho Biometric Integration, Encoding Morpho Cards for Verification • 73-67
Morpho Biometric Integration, Enrolling Users • 73-44
Morpho Biometric Integration, Installation • 73-3
Morpho Biometric Integration, Installing MorphoAccess Readers • 73-8
Morpho Biometric Integration, Morpho OSDP Configuration • 73-71
Morpho Biometric Integration, Overrides on Morpho OSDP Readers • 73-76
Morpho Biometric Integration, Performing Overrides on a Morpho Biometric Reader • 73-69
Morpho Biometric Integration, QR Code authentication mode at Morpho Readers • 73-82
Morpho Biometric Integration, Supported Enrolment Devices • 73-25
Morpho Biometric Integration, Troubleshooting • 73-86

Morpho Biometric Integration, Wiring Morpho Readers for OSDP • 73-72
Moving Objects • 47-48
Moving or Resizing shapes • 18-14
Moving OSDP Readers between Controllers • 79-9
Moving text objects • 18-22
Multi-Server systems • 49-1
Multi-Server systems, Adding a new server to a Star structure • 49-15
Multi-Server systems, Creating a Remote Server • 49-9
Multi-Server systems, Deleting a child server from a Star structure • 49-24
Multi-Server systems, Deleting a server from a Peer-to-Peer structure • 49-22
Multi-Server systems, Event Aggregation • 49-19
Multi-Server systems, Important Issues • 49-4
Multi-Server systems, Overriding a Remote Server • 49-17
Multi-Server systems, Remote Command Centre items • 49-6
Multi-Server systems, Switching from Peer-to-Peer structure to Star structure • 49-13
Multi-Server systems, Switching from Star structure to Peer-to-Peer structure • 49-14
Mute Alarm • 42-25

N

NAT Solution - Configurable Ports • 21-40
Navigating between linked Site Plans • 18-23
Nedap ANPR Lumo Readers • 75-11
Nedap Booster DESFire feature • 75-5
Nedap Readers • 75-1
Nedap Transit Readers • 75-5
Nedap uPASS Readers • 75-2
Networked Perimeter Security Systems • 48-1
Networked Perimeter Security Systems, Assigning a Fence Zone to a Terminal • 48-6
Networked Perimeter Security Systems, Configuring a Fence Controller • 48-9, 48-19
Networked Perimeter Security Systems, Creating a Fence Zone • 48-2
Networked Perimeter Security Systems, Creating a Voltage Report • 48-34
Networked Perimeter Security Systems, Monitoring Fence Alarms and Events • 48-29
Networked Perimeter Security Systems, Monitoring Fence Controller Status • 48-28
Networked Perimeter Security Systems, Monitoring Fence Zone Status • 48-27
Networked Perimeter Security Systems, Overriding a Fence Controller • 48-32
Networked Perimeter Security Systems, Overriding a scheduled Fence Zone state • 48-30
Networked Perimeter Security Systems, Using HVplus mode • 48-40
Networked Perimeter Security Systems, Using Service mode • 48-38
New Cardholder, Add • 32-2
No-Alone Zone • 10-26
Notes tab, Server Properties • 6-85
Notification Examples • 35-25
Notifications • 35-1
Notifications tab, Server Properties • 6-47
Notifications, Acknowledging alarms via SMS or email • 35-28
Notifications, Assigning Cardholders to Roles via Bulk Change • 35-20
Notifications, Copying all Cardholders under a Role • 35-23
Notifications, Creating a Notification Filter • 35-5
Notifications, Enabling Event/Alarm Notifications for a Cardholder • 35-10
Notifications, Examples • 35-25
Notifications, Overall Process • 35-3
Notifications, Setting Expiry Notification Threshold Values • 35-14
Notifi cations, Setting up Roles • 35-17
Notify Restoral • 42-29
Numerous alarms, Processing • 42-20

O

Offline Monitoring, Configuring • 21-33
OneLink Configuration • 21-18
Open a Door Request • 45-12
Open Supervised Device Protocol (OSDP) Integration • 79-1
Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Readers • 56-21
Opening the Alarm Viewer window • 42-8
Opening the Card Editor window • 47-13
Opening the Event Viewer window • 42-2
Opening the Intercom window (Intercom Systems) • 24-34
Opening the Operator Sessions Viewer • 44-2
Opening the Salto List Window • 74-72
Opening the Server Properties window • 6-3
Opening the Status Viewer • 45-3

Operator Accounts, Unlocking • 2-22
Operator Defaults tab, Server Properties • 6-19
Operator Groups • 36-1
Operator Passwords • 2-15
Operator Passwords, Changing • 2-16
Operator Passwords, Resetting • 2-18
Operator Privileges, Which ones you require • 37-2
Operator Sessions • 44-1
Operator Sessions, Opening the Viewer • 44-2
Operator Sessions, Terminating • 44-4
Operators, Unlocking an Operator account • 2-20
OSDP Compliant Readers, Assigning to Gallagher Controllers • 79-7
OSDP Readers, Configuring • 79-3
OSDP Readers, Moving OSDP Readers between Controllers • 79-9
Outgoing Email tab, Server Properties • 6-49
Outputs and Inputs, Creating • 21-50
Outputs and Inputs, Linking to devices • 21-56
Overall Process - Setting up Notifications • 35-3
Overrides • 45-1
Overrides, Configuring at Card Readers • 45-13
Overrides, Open a Door Request • 45-12
Overrides, Performing • 45-7
Overrides on Morpho OSDP Readers, Morpho Biometric Integration • 73-76
Overriding a Fence Controller • 48-32
Overriding a Remote Server (Multi-Server systems) • 49-12
Overriding a scheduled Fence Zone state • 48-30
Overriding Operator Group Competencies • 52-20

P

Passwords, Changing • 2-16
Passwords, Preventing context specific passwords • 2-22
Passwords, Resetting • 2-18
PDF (Personal Data Field) • 33-1
PDF data, Editing a Cardholders • 32-20
Performing a Lockdown Override, Access Zones • 10-11
Performing a 'Log Tuning Data' override on a Z20 Disturbance Sensor • 55-22
Performing a Maintenance Mode Override • 55-9
Performing a Walk Test Mode Override • 55-12
Performing Archives • 40-8
Performing Backups • 40-14
Performing Bluetooth® Actions • 31-14
Perform ing Overrides • 45-7
Performing Overrides for Class 5 End-of-Line Modules (ELMs) • 61-8
Performing Overrides on a Morpho Biometric Reader • 73-69
Performing Overrides on the Salto Server • 74-76
Perimeter Sensors • 55-1
Personal Data Fields • 33-1
Personal Data Fields, Capturing Images • 33-10
Personal Data Fields, Creating • 33-2
Personalised Actions, Configuring for Access Zones • 10-34
Photo ID • 47-1
Photo ID objects, Adding a Barcode • 47-24, 47-51
Photo ID objects, Adding a Magstripe object • 47-27
Photo ID objects, Adding a MIFARE Classic object • 47-33
Photo ID objects, Adding a Non-diversified MIFARE DESFire object • 47-46
Photo ID objects, Adding an Image • 47-22
Photo ID objects, Adding Text • 47-20, 47-50
Photo ID objects, Deleting • 47-49
Photo ID objects, Expanding an Object Box • 47-48
Photo ID objects, Joining Fields in the same Text Object • 47-21
Photo ID objects, Selecting Multiple Objects • 47-49
Photo ID, Adding Reasons for Printing Cards • 47-57
Photo ID, Copying Card layouts • 47-54
Photo ID, Formatting Cards • 47-16
Photo ID, Opening the Card Editor window • 47-14
Photo ID, Printing and/or Encoding a Card from a Cardholder • 47-58
Photo ID, Working with Card Type objects • 47-19
Photo ID, Working with Digital ID Type objects • 47-50
Photo ID, Working with Objects • 47-18
Photo ID, Adding a Background • 47-17
PII Redaction • 68-1
PII Redaction, Redacted Cardholders • 68-8

PII Redaction, Redaction Configuration in Command Centre • 68-3
PII Redaction, Redaction events • 68-9
PII Redaction, Requesting a Cardholder Event Redaction • 68-6
PII Redaction, Requesting a Cardholder Information Redaction • 68-7
PIV Card Support • 56-1
PIV Card Support, Assigning an OSDP Veridt Stealth PIV Reader to a Gallagher PIV Controller 6000 • 56-27
PIV Card Support, Configuring an OSDP Veridt Stealth PIV Reader • 56-22
PIV Card Support, Configuring the PIV Card Reader • 56-18
PIV Card Support, Editing the PIV Card Type • 56-7
PIV Card Support, Enrolling PIV and PIV-I cards • 56-32
PIV Card Support, Installing the necessary applications/tools • 56-3
PIV Card Support, Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Readers • 56-21
PIV cards in Command Centre • 56-33
Placing a call (Intercom Systems) • 24-37
Placing a Macro on a Site Plan • 20-17
Pop-up Menu • 3-11
Pop-up Menu (Site Plans) • 18-3
Prepay Car Parking • 65-1
Prepay Car Parking, Configuration examples • 65-4
Prepay Car Parking, Configuring a low credit warning signal • 65-14
Prepay Car Parking, Configuring the Prepay Car Parking feature • 65-5
Prepay Car Parking, Understanding the Prepay Car Parking feature • 65-3
Pre-registration and Receptionist functions • 50-68
Preventing context specific passwords • 2-22
Printer Settings, Customising • 39-75
Printing a badge • 50-117
Printing a Find Visit report • 50-99
Printing a Visitor Status report • 50-112
Processing an alarm • 42-17
Processing numerous alarms • 42-20
Purging Shift history, Shifts • 70-6

Q

QR Code authentication mode at Morpho Readers • 73-82
QR Code Readers • 80-1
QuickSwitch Board, Configuring • 21-132
Quick Processing an alarm • 42-18

R

Re-issuing a Card for a Cardholder • 32-19
Reactivating Expired or Disabled cards • 32-17
Readers, Creating • 21-57
Readers, Nedap • 75-1
Reading MIFARE Cards using a MIFARE USB Encoder • 32-31
Receptionist functions • 50-103
Recommended Site Configuration Process • 5-2
Redacted Cardholders, PII Redaction • 68-8
Redaction Configuration in Command Centre, PII Redaction • 68-3
Redaction events, PII Redaction • 68-9
Regular Expression Settings • 33-6
Remote Command Centre items • 49-5
Removing a Card from a Cardholder • 32-13
Removing Actions for a Macro • 20-10
Removing an item from the Status Viewer • 45-6
Removing Icons from Site Plans • 18-24
Removing Scheduled run times for a Macro • 20-12
Removing, Cards from Cardholders • 32-13
Removing, Items from the Status Viewer • 45-6
Report Scheduling, Configuring • 39-64
Reporting on Cardholder Competencies • 52-23
Reports • 39-1
Reports, Access Group Report • 39-31
Reports, Access Report • 39-33
Reports, Activity Report • 39-15
Reports, Advanced • 39-81
Reports, Cardholder Report • 39-7
Reports, Configuring Report Scheduling • 39-65
Reports, Contact ID Assignment Report • 39-58
Reports, Creating • 39-2
Reports, Evacuation Report • 39-23
Reports, Exception Report • 39-35
Reports, Guard Tour Report • 53-10
Reports, Print Preview window • 39-78
Reports, Printing existing • 39-73
Reports, Site Configuration Report • 39-55
Reports, Time and Attendance Report • 39-40
Reports, Wiring Report • 39-61

Requesting a Cardholder Event Redaction, PII Redaction • 68-6
Requesting a Cardholder Information Redaction, PII Redaction • 68-7
Resetting Operator Passwords • 2-18
REST API • 63-1
REST API Client Item, Creating • 28-13
Resizing Column Headers • 3-5
Restoral Events • 42-5
Restoring Archives • 40-11
Restoring Backups • 40-19
Restricting System View • 2-9
Rolling configuration on a CipherToken card • 71-5
Rolling configuration on a UK GovPASS card • 64-5
Roles, Assigning Cardholders to Roles via Bulk Change • 35-18
Roles, Copying all Cardholders under a Role • 35-21
Roles, Setting up • 35-15
Running a Cardholder Report from a Cardholder • 32-30
Running a Guard Tour • 53-6
Running a Macro • 20-18

S

Salto Doors or ESDs • 74-41
Salto Ethernet Encoders/Dongles • 74-37
Salto Installation Instructions • 74-5
Salto Key Assignment • 74-107
Salto Lock Interface • 74-1
Salto Lock Interface, Adding Salto MIFARE objects to a card layout • 74-99
Salto Lock Interface, Advanced Parameter Options • 74-34
Salto Lock Interface, Audit Trail • 74-66
Salto Lock Interface, Command Centre Site Configuration • 74-71
Salto Lock Interface, Configuring Access Groups • 74-80
Salto Lock Interface, Configuring access to Salto Outputs • 74-89
Salto Lock Interface, Configuring Key to support Salto Sapce CUADAP 64 bit integration • 74-94
Salto Lock Interface, Configuring Salto Access Zones • 74-86
Salto Lock Interface, Configuring Salto Doors • 74-90
Salto Lock Interface, Configuring Salto options for Cardholders • 74-88
Salto Lock Interface, Editing the Salto Server • 74-73
Salto Lock Interface, Encoding cards • 74-91
Salto Lock Interface, Ethernet Encoders/ Dongles • 74-37
Salto Lock Interface, Initialising a door using the PPD • 74-64
Salto Lock Interface, Migrating Salto Legacy Cards to Salto Native • 74-36
Salto Lock Interface, Space Installation • 74-5
Salto Lock Interface, Opening the Salto List window • 74-72
Salto Lock Interface, Other Salto Configuration • 74-70
Salto Lock Interface, Performing Overrides on the Salto Server • 74-76
Salto Lock Interface, PPD Status • 74-40
Salto Lock Interface, Reason for using 64 bit Wiegand format • 74-93
Salto Lock Interface, Salto Doors or ESDs • 74-47
Salto Lock Interface, Salto Ethernet Encoders/ Dongles • 74-41
Salto Lock Interface, Salto Native Mode Migration • 74-35
Salto Lock Interface, Salto wireless RF devices • 74-59
Salto Lock Interface, Salto Zones • 74-54
Salto Lock Interface, SHIP settings • 74-32
Salto Lock Interface, Space Site Configuration • 74-31
Salto Lockers • 74-46
Salto Native Mode Migration • 74-36
Salto Outputs • 74-56
Salto Rooms • 74-48
Salto Server Connection, Salto Native Mode Migration • 74-36
Salto Site Configuration • 74-31
Salto Suites • 74-51
Salto to Command Centre Event Mapping • 74-113
Salto wired (online) devices • 74-57
Salto wireless RF devices • 74-59
Salto Zones • 74-54
Scanning business cards for visitors • 50-106
Scanning passports or driver licenses for visitors • 50-109
Scenarios using Logic and Virtual Outputs • 25-4
Schedules • 12-1
Schedules, Adding new day categories • 12-6

Schedules, Changing times and states within Schedules • 12-8
Schedules, Creating • 12-2
Schedules, Duplicating Day Category entries • 12-12
Schedules, Removing Day Categories • 12-7
Scheduling a Macro • 20-7
SchindlerID, External Systems • 24-28
Schlage Devices, Assigning • 77-19
Schlage Device Setup and Configuration • 77-5
Schlage Door, Creating • 77-14
Schlage PIM, Creating • 77-11
Schlage Lock Interface • 77-1
Secondary Ethernet operation mode, Configuring • 21-20
Sending Invitations • 50-126
Sensor Devices, D10 and Z10 • 55-1
Server Properties • 6-1
Server Properties window, Opening • 6-3
Server Properties, Advanced tab • 6-30
Server Properties, Alarm Flooding tab • 6-9
Server Properties, Alarm Instruction Defaults tab • 6-14
Server Properties, Alarm Notes tab • 6-17
Server Properties, Alarm Transmission tab • 6-15
Server Properties, Alarm Zone States tab • 6-11
Server Properties, Card Security tab • 6-37
Server Properties, Challenge tab • 6-63
Server Properties, Competency Messages tab • 6-24
Server Properties, Controller Defaults tab • 6-59
Server Properties, Controller Web Server • 6-61
Server Properties, Custom Fields • 6-81
Server Properties, Data Retention tab • 6-72
Server Properties, Database Maintenance tab • 6-57
Server Properties, Event Defaults tab • 6-12
Server Properties, Event Priorities tab • 6-7
Server Properties, HBUS Terminal Defaults tab • 6-76
Server Properties, Icons tab • 6-80
Server Properties, Import tab • 6-56
Server Properties, Incoming Email tab • 6-52
Server Properties, Licensing tab • 6-4
Server Properties, Measurement Units tab • 6-28
Server Properties, Mobile Connect Settings • 6-73
Server Properties, Mobile/SMS Notifications tab • 6-54
Server Properties, More Challenge tab • 6-63
Server Properties, Notes tab • 6-85
Server Properties, Notifications tab • 6-47
Server Properties, Operator Defaults tab • 6-19
Server Properties, Outgoing Email tab • 6-49
Server Properties, Standards tab • 6-64
Server Properties, State Names tab • 6-26
Server Properties, User Codes tab • 6-23
Server Properties, Web Services • 6-33
Service mode, Using • 48-38
Service or Workstation Items, Deleting • 28-6
Service or Workstation Items, Editing • 28-5
Services and Workstations • 28-1
Services and Workstations, Connecting to the Cloud • 28-7
Services and Workstations, Creating a new Workstation item • 28-2
Services and Workstations, Creating a REST API Client Item • 28-13
Services and Workstations, Server Migration • 28-12
Setting a Lockdown Source, Access Zones • 10-9
Setting Expiry Notification Threshold Values • 35-13
Setting up Access Groups • 34-4
Setting up Alarm Zones • 14-3
Setting up Card Types • 7-2
Setting up Digital ID Types • 31-6
Setting up Mobile Credential Types, Mobile Connect • 31-3
Setting up Operator Groups • 36-5
Setting up Roles • 35-15
Setting up System Divisions • 9-3
Setting up Tracking Tag Types • 66-7
Setting up your Site • 5-2
Shifts • 70-1
Shifts, Configuring a Shift • 70-3
Shifts, Purging Shift history • 70-6
Single Door Controller 7000, Creating • 21-9
SIP Integration • 67-1
SIP Integration, Configuring a SIP Device • 67-8
SIP Integration, Configuring the SIP Service • 67-3
SIP Integration, Enabling SIP Intercoms for a Workstation • 67-10
Site Configuration Report • 39-55
Site Plan Pop-up Menu • 18-3
Site Plans •18-1, 43-1

Site Plans, Adding Areas • 18-13
Site Plans, Adding Lines • 18-13
Site Plans, Adding Rectangles • 18-13
Site Plans, Creating • 18-4
Site Plans, Drawing on • 18-12
Site Plans, Editing • 18-8
Site Plans, Navigating between linked Site Plans • 18-23
Site Plans, Removing icons • 18-24
Site Plans, Viewing • 43-2
Site Plans, Viewing Alarms from Site Plans • 43-4
Sizing the windows • 3-9
Sorting information • 3-8
Sounds, Alarms • 42-23
Special access for Doors • 22-11
Special Calendars, Creating • 13-3
Standards tab, Server Properties • 6-64
Startup Wizard • 5-6
State Names tab, Server Properties • 6-26
Status and Overrides • 45-1
Status and Overrides, Understanding • 45-2
Status Viewer, Adding items • 45-5
Status Viewer, Opening • 45-3
Status Viewer, Removing items • 45-6
Supported Enrolment Devices, Morpho Biometric Integration • 73-25
Switching between windows • 3-10
Switching from Peer-to-Peer structure to Star structure (Multi-Server systems) • 49-13
Switching from Star structure to Peer-to-Peer structure (Multi-Server systems) • 49-14
System Division • 9-1
System Division, Setting up • 9-3
System Operator, Disabling • 32-34
System View, Restricting • 2-11

T

Tag Tracking • 66-1
Tag Tracking, Configuring the Tag Tracking feature • 66-3
Tag Tracking, Setting up Tracking Tag Types • 66-7
Tautwire Sensors, Configuring • 55-18
Terminals with Biometric Readers • 65-68
Terminating an Operator Session • 44-4
Temperature Report • 48-36
The IP Alarms Receiver Log Viewer • 29-39
The Report Print Preview window • 39-78
ThyssenKrupp Insight Elevator Systems • 81-1
ThyssenKrupp Insight Elevator Systems, Configuring an elevator • 81-10
ThyssenKrupp Insight Elevator Systems, Configuring a group • 81-5
ThyssenKrupp Insight Elevator Systems, Configuring a kiosk • 81-14
ThyssenKrupp Insight Elevator Systems, Configuring a system • 81-2
ThyssenKrupp Insight Elevator Systems, Configuring an Elevator Kiosk Control Schedule • 81-12
Time and Attendance Report • 39-40
Tree view • 3-3
Trigger Strings and Reflected Outputs, Configuring for FTCAPI • 24-18
Troubleshooting - Aperio Integration • 76-78
Troubleshooting - Morpho Biometric Integration • 73-86
Troubleshooting - Supported elevator systems • 23-26
Troubleshooting - Visitor Management Logon Failure • 50-133

U

UK GovPASS Card Support • 64-1
UK GovPASS Card Support, Enrolling a configuration card • 64-2
UK GovPASS Card Support, Rolling configuration • 64-5
UK GovPASS cards in Command Centre • 64-6
Understanding Access Zones • 10-2
Understanding Status and Overrides • 45-2
Understanding the High Level Elevator Interface • 23-7
Universal Card Format • 26-1
Universal Card Formats for'Use MIFARE Serial Number as Card Data' (CSN mode) • 26-11
Universal Card Formats, Adding • 26-2
Universal Card Formats, Deleting • 26-10
Unlocking an Operator account • 2-22
Updating Access Points, Salto Salto Lock Interface • 74-82
Upgrading a Controller 6000 to a Controller 7000 • 21-27
User Codes for access at Card Readers with keypads • 32-25
User Codes tab, Server Properties • 6-23
Using Commend Intercoms • 60-9
Using HVplus mode • 48-46
Using macros • 20-1
Using Service mode • 48-44
Using the advanced drag and drop feature • 2-26
Using the Enrolment Wizard • 8-7

Using the Find Tool • 41-2
Using USB stick to load Device Software to a Controller 6000 or 7000 • 27-9
Using Visitor Management • 50-66
Utilities • 4-1

V

Viewing a host's details • 50-102
Viewing a visitor's details • 50-100
Viewing alarm details • 42-11
Viewing alarms from Site Plans • 43-4
Viewing an existing Site Plan • 43-2
Viewing event details • 42-3
Viewing Images associated with an alarm • 42-15
Viewing item properties • 3-17
Viewing/Editing the Default Calendar • 13-2
Virtual Outputs and Logic Blocks • 25-1
Virtual Outputs, Creating • 25-21
Visit status • 50-85
Visitor Management • 50-1
Visitor Management Application Installation Instructions • 50-3
Visitor Management, Command Centre Site Configuration • 50-7
Visitor Management, Using • 50-66
Visitor Management Kiosk • 51-1
Visitor Management Kiosk Configuration • 51-7
Visitor Management Kiosk Document Scanning Process • 51-36
Visitor Management Kiosk Installation Instructions • 51-3
Visitor Management Kiosk screens • 51-39
Visitor Management Kiosk, Configuring Notifications for Hosts • 51-32
Visitor status • 50-111
Visitors displayed on the Home screen • 50-106
Voltage Report • 48-34

W

Web Services tab, Server Properties • 6-33
Which Operator Privileges you require • 37-2
Windows, Grid view • 3-4
Windows, Sizing • 3-9
Windows, Switching between • 3-10
Windows, Tree view • 3-3
Wiring Morpho Readers for OSDP, Morpho Biometric Integration • 73-72
Wiring Report • 39-61
Wizard Templates • 5-33
Wizards • 5-5
Working with Card Type objects • 47-19
Working with Digital ID Type objects • 47-50
Working with Objects • 47-18
Workstation Items, Creating • 28-2

X

XYZ Event Mappings • Appx B-1

Z

Z10 Tension Sensor Group Configuring • 55-3
Z20 Disturbance Sensor, Assigning to a Controller 6000 • 55-20
Z20 Disturbance Sensor, Configuring • 55-15
Z20 Disturbance Sensor, Performing a 'Log Tuning Data' override • 55-22
Zone Counting, Enabling • 10-20
Zone Counts, Manually Resetting • 10-30