Gallagher Command Centre

Configuration Client User Guide

Volume 3

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 Access 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 21-44
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 5: Licensable Features

Command Centre has a number of features that are licensable. Therefore, if your site does not have a particular feature included in their licence file, those options will not be available to you.

This part of the User Guide provides detail on what the licensable features are, and how to use them, in the following chapters:

- **Chapter 47: Card Layouts - Designing / Printing / Encoding**
- **Chapter 48: Perimeter Fence Controllers**
- **Chapter 49: Multi-Server systems**
- **Chapter 50: Visitor Management**
- **Chapter 51: Visitor Management Kiosk**
- **Chapter 52: Cardholder Competencies**
- **Chapter 53: Guard Tours**
- **Chapter 54: Enterprise Data Interface**
- **Chapter 55: Perimeter Sensors**
- **Chapter 56: PIV Card Support**
- **Chapter 57: Active Directory Single Sign-on**
- **Chapter 58: Austco Intercoms**
- **Chapter 59: Jacques Intercoms**
- **Chapter 60: Commend Intercoms**
- **Chapter 61: Class 5 End-of-Line Module (ELM)**
- **Chapter 62: Locker Management Solution**
- **Chapter 63: REST API**
- **Chapter 64: UK GovPASS Card Support**
- **Chapter 65: Prepay Car Parking**
- **Chapter 66: Tag Tracking**
- **Chapter 67: SIP Integration**
- **Chapter 68: PII Redaction**
- **Chapter 69: Apple Employee Badge**
- **Chapter 70: Shifts**
- **Chapter 71: CipherToken Card Support**
- **Chapter 72: Entra ID Single Sign-on**

Notifications

In addition to those licensable features mentioned above, there is also the **Notifications** feature. This feature allows administrators to configure Command Centre to automatically send notifications of significant events/alarms and card and competency expiry warnings.

This feature also relates to Cardholders, Roles and Personal Data Fields (all core features of Command Centre). Therefore, Notifications is covered in the Site Management part of this manual. Refer to Notifications for further detail.

OPC Data Access Server

In addition to those licensable features mentioned above, there is also the **OPC Data Access Server** feature. This feature enables the bi-directional transfer of information between Gallagher Command Centre and a third-party system. This integration allows security staff to manage all Command Centre alarms and events, view live status of Command Centre items and be able to change some parameters, such as overrides, from the third-party system. This requires Command Centre to be able to run unattended at all times.

If you require this feature, and have it included in your licence file, refer to the *Gallagher OPC Data Server Interface Specification* document (**Gallagher OPC Data Server Interface Spec.pdf**) provided with the Gallagher Command Centre Installation files for further information.

Chapter 47: Card Layouts - Designing / Printing / Encoding

Introduction

The following functions all relate to card layouts, and are available in Command Centre, providing your site has the correct license options. This chapter covers the following information:

- ***Overall Process*** (on page 47-2)
- ***Designing card layouts*** (on page 47-13)
  (using the Photo ID feature in Command Centre)
- ***Printing/Encoding Cards*** (on page 47-55)
- ***Batch Printing and/or Encoding*** (on page 47-64)
  (covers printing/encoding cards for multiple cardholders, and printing/encoding multiple cards of a particular Card Type)

Licensing

Each function related to card layouts, (i.e. designing card layouts, card printing and card encoding), is an individually licensable feature. There are a number of license options available depending on your site requirements. Therefore, depending on which option your site has could mean that one or more of the options mentioned in this topic may not be available to you. The following table indicates the license options available:

To...	the license file should include...

design and print card layouts	`[Features]`
	`Photo-ID=1`
	`CardPrinting=1`

design, print and encode card layouts	`[Features]`
	`Photo-ID=1`
	`Encoding=1`
	`CardPrinting=1`

batch print and encode cards for cardholders	`[Features]`
	`Encoding=1`
	`[Configuration]`
	`FacilityCode=<code>`
	Note: Batch printing and encoding will be restricted to Card Types whose Facility Code appears in the license file.

bureau print and encode cards	`[Features]`
	`BureauCard=1`
	`[Configuration]`
	`FacilityCode=<code>` OR
	`BureauFacilityCode=<code>`
	Note: Bureau printing and encoding will be restricted to Card Types whose Facility Code appears in the license file (either beside 'Facility Code' or 'Bureau Facility Code').

Overall Process

Introduction

This section describes the overall process for creating and designing card layouts and then printing and/or encoding cards, (e.g. Magstripe and MIFARE), using core Command Centre functionality. When necessary, this process refers to separate step-by-step procedures that are detailed elsewhere, (i.e. either as separate procedures in this section, or in other sections in this online help).

While this process covers all the options you may need, if you do not require a specific function then you can exclude it. This will not prevent you from proceeding to later steps.

Process

1. Create/edit a Card Type.
   Refer to ***Setting up Card Types*** (on page 7-2) for the procedure.

   Note: Ensure that the Facility Code in the Card Type matches that in the license file.

2. Create a card layout for the Card Type created in Step 1.
   Refer to ***Card Layouts*** (on page 47-13) for full details on configuring a card layout.

   Included in the Card Layout section are procedures for adding Magstripe objects and MIFARE objects to card layouts, which enables data to be encoded on the card.

   Note: MIFARE cards do not support 6-digit user PINs. If a 6-digit PIN is specified for a MIFARE card then the PIN will not work at the reader.

3. Does your site have "Enrolment Wizard" and "Enrolment Template" included in their license file?

If...	then...
no	go to Step 4.
yes	the Enrolment Wizard can be used for performing the remaining functions in this process, (i.e. to search for and identify cardholders, and then encode and print a card specific to that cardholder). Refer to ***Enrolment Wizard and Templates*** (on page 8-1) for detailed procedures.

4. What do you want to print and/or encode cards for?

If...	then...
for a cardholder	go to Step 5.
for multiple cardholders	perform a Cardholder Batch Job. Refer to ***Performing a Cardholder Batch Job*** (on page 47-70) for the procedure.
mulitple cards of a particular card type	perform a Bureau Batch Job. Refer to ***Performing a Bureau Batch Job*** (on page 47-67 for the procedure.

5. Locate the Cardholder.
   Refer to ***Locating the Cardholder*** (on page 47-4) for the procedure.
6. Edit the Cardholder data if necessary.
   Refer to ***Editing Cardholder Data*** (on page 47-7) for the procedure.
7. Preview the Card layout before printing/encoding to ensure the layout is acceptable. This gives you the opportunity to change anything if necessary.
   Refer to Previewing a card from a cardholder 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.
   Note: When you preview a card you will not see the magstripe or MIFARE object in the preview window.
8. Print and/or encode the card.
   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.
9. Repeat this process for all subsequent cardholders.
   If you used the Find Tool for locating cardholders, the **Find...** window remains open with the previous search selections. Enter the Student ID (or other search criteria) for the next person and continue from Step 6 in the ***Locating the Cardholder*** (on page 47-4) procedure.

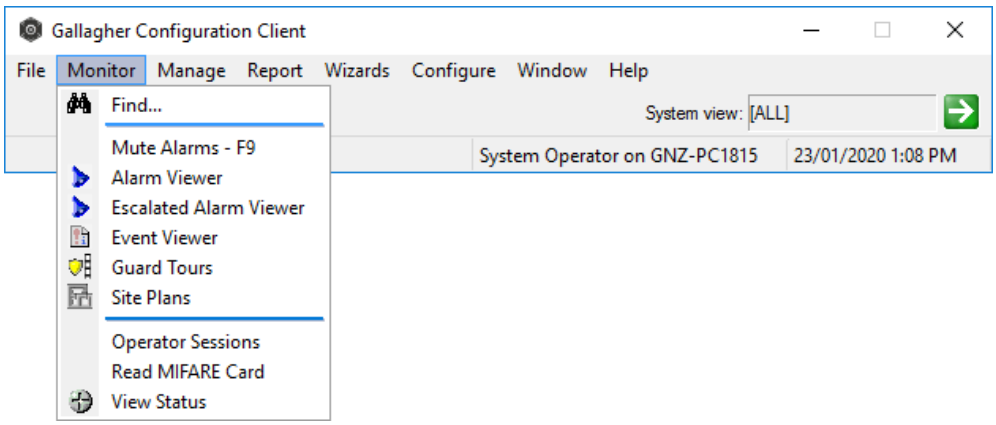
Locating the Cardholder

Introduction

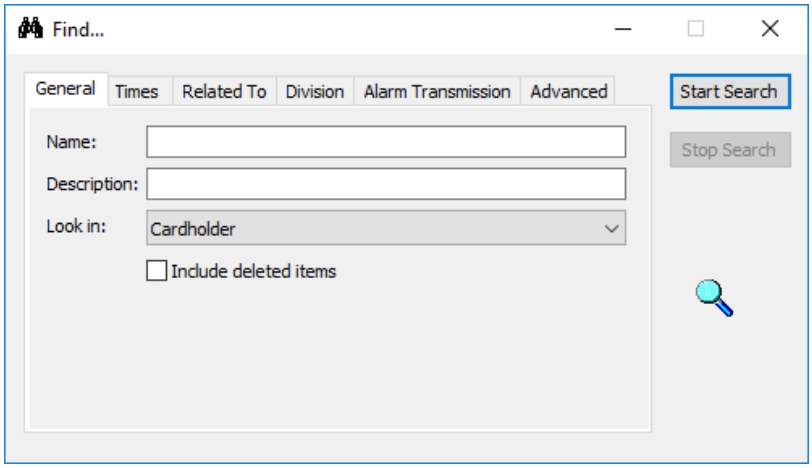
This procedure describes how to locate a Cardholder using the Find Tool. Although you could locate a Cardholder directly from the **Cardholder** List Window, the Find Tool allows you to search on something specific to a Cardholder, (e.g. Student ID), which can speed up the process.

Procedure

1. Click **Monitor** from the menu bar, then **Find...**
   The **Find** tool opens.



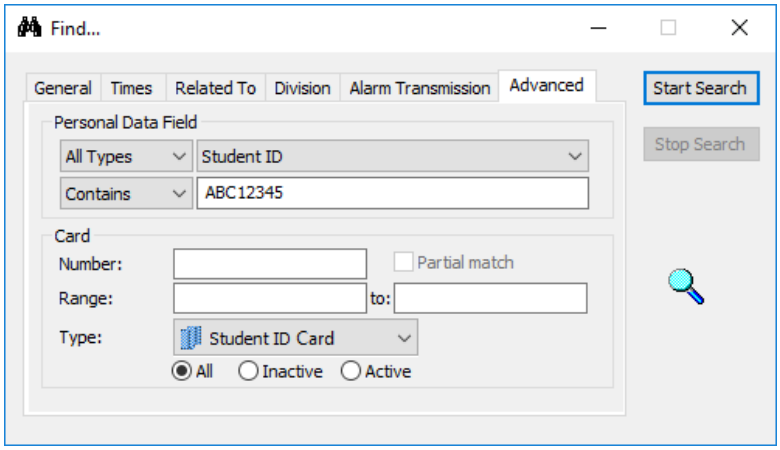
2. Click within the **Look in** field.
   From the displayed drop-down menu, click **Cardholder**.



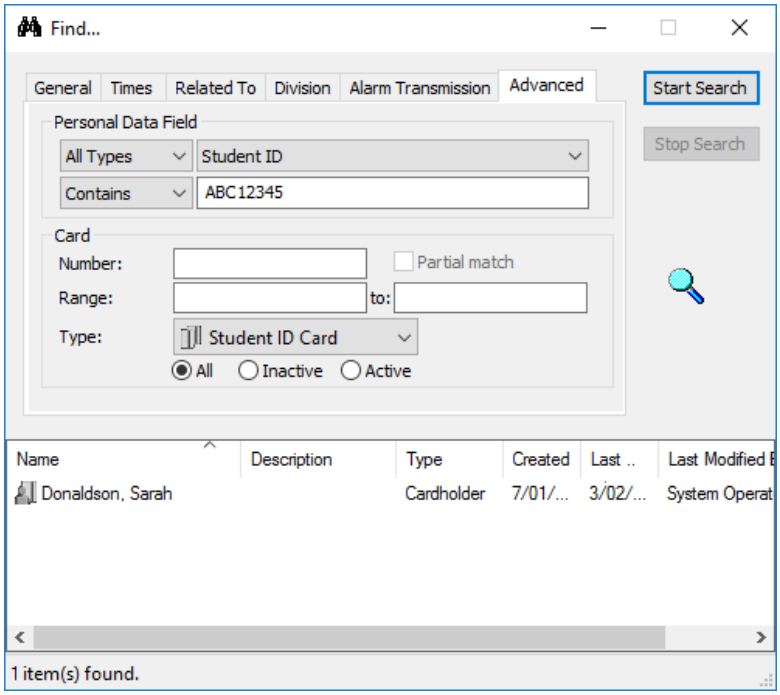
   For subsequent iterations, the **Find...** window remains open with the last selections that were made, and you will not need to perform Steps 1-2 again.

3. Click the **Advanced** tab.
   This tab allows you to define your search by using a personal data field, (e.g. "Student ID").

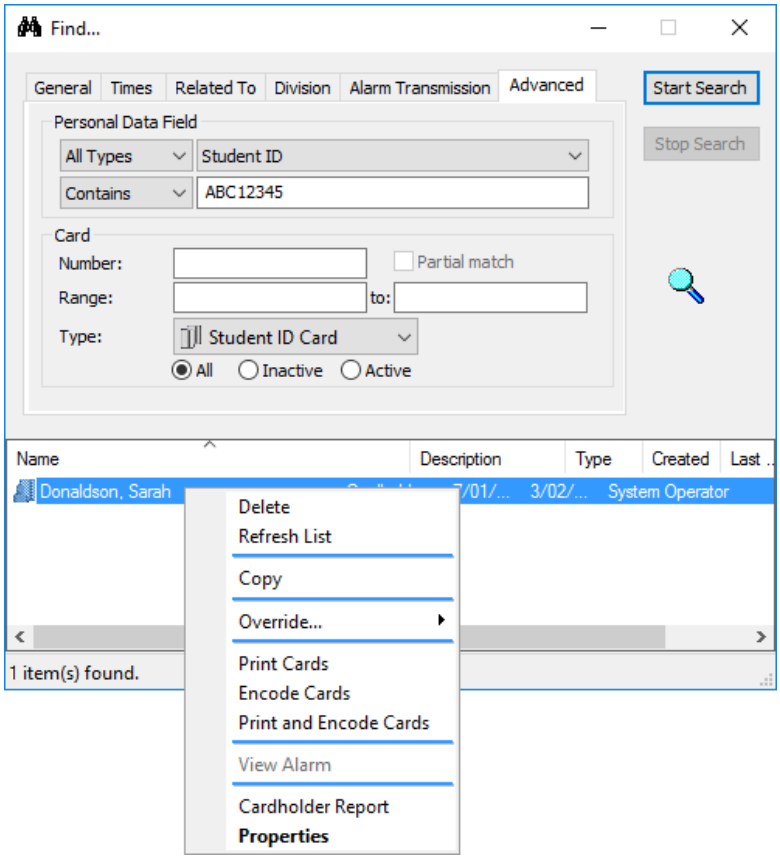
4. Select the **Personal Data Field** from the drop-down list, and if it is known, the **Card Type** from the drop-down list.
   Note:
   Once these options are selected you will not have to select them again when you search for the next cardholder.



5. If you are searching by Student ID, enter it in the blank field and click the **Start Search** button.
   The cardholder with that unique Student ID will display within the Search window.



6. **Right-click** on the Cardholder record to display the context menu.



7. To check or update cardholder data, go to ***Editing Cardholder Data*** (on page 47-7) next.
   If no cardholder or card data needs changing, return to Step 6 of the ***Overall Process*** (on page 47-2).

Editing Cardholder Data

Introduction

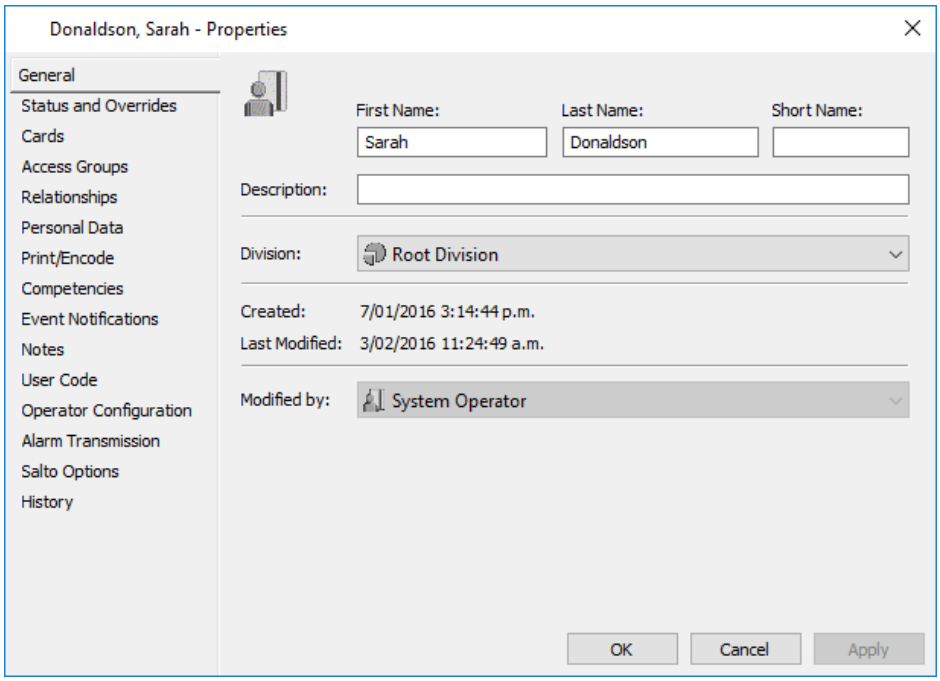
It may be a good idea to check that a cardholders data is correct prior to printing and/or encoding a card for them. This procedure allows you to check the data and change if necessary.

Before you begin

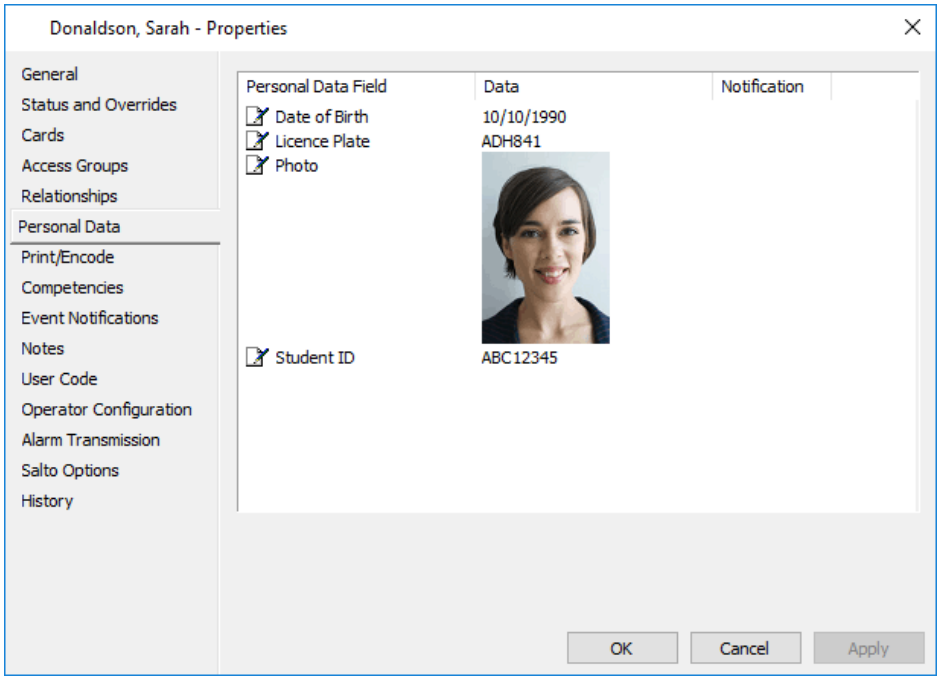
Before you begin this procedure ensure you have located the Cardholder using either the Find Tool or directly from the **Cardholder** List Window. From either window, you should have already right-clicked on the Cardholder record resulting in the context menu displaying.

Procedure

1. From the context menu, click on **Properties**.
   The **General** tab of the Cardholder properties displays.



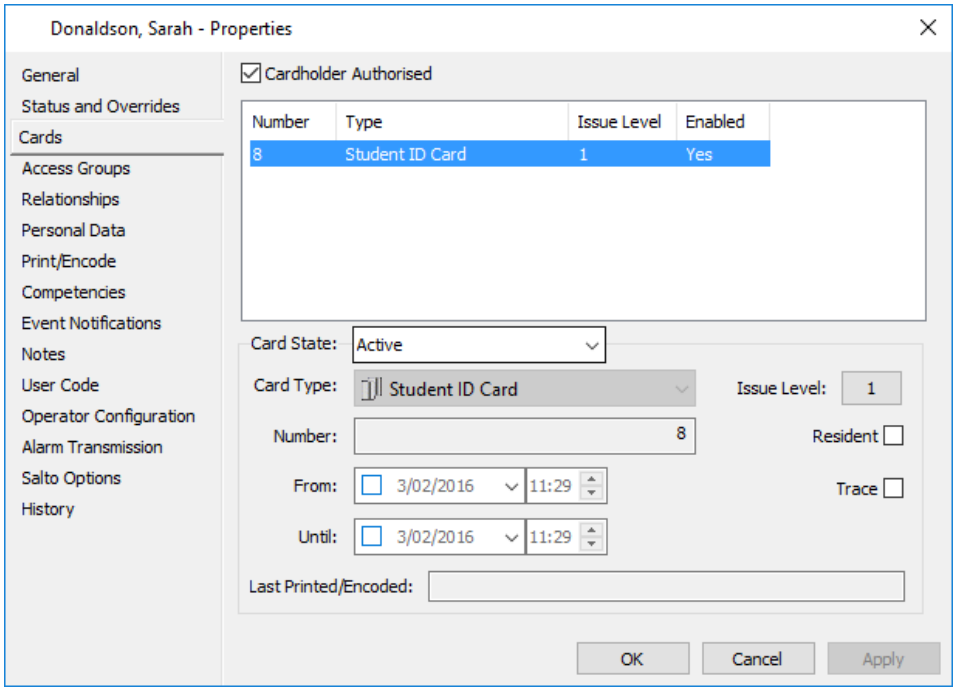
2. If you wish to update personal data, (e.g. capture a cardholder image), click on the **Personal Data** tab.



3. Double-click on the "Cardholder Image" personal data field to capture a new image. You can either capture an image from a camera installed on the workstation or upload an image from file. The former method lets you upload an image from a digital camera that installs as a removable drive on the workstation. If you use the latter method, a dialog box displays for you to path your way to the required folder. The path is remembered so that you do not need to repeat this step for the next cardholder.

   You can crop the image if necessary and then click **OK** to save it to the personal data field.

4. Other personal data fields can be edited by clicking on them.
5. If you need to add or check card data, click on the **Cards** tab.



From this window you can view existing card details and add or delete cards if required.

Note: Refer to ***Adding a Card to a Cardholder*** (on page 32-9) for a full explanation of the fields on this tab.

6. Click **OK** to return to either the **Cardholder** List Window or the **Find...** window.
7. Return to Step 7 of the ***Overall Process*** (on page 47-2).

Printer Installation

Introduction

This topic describes how to install the printer.

Before you begin

To view a list of supported printer integrations, view the ***Gallagher Security website*** (http://security.gallagher.co/products-and-systems/integrations/card-printers/) or contact Gallagher Technical Support.

Note: The printer integration may not support the latest printer and encoder drivers. Confirm the supported printer and encoder drivers with Gallagher Technical Support prior to installation.

Procedure

To install the printer, perform the following procedure:

1. Install the printer driver (provided by the printer manufacturer) on all Command Centre workstations that will be using the printer.

   Note: Some printer models may require you to connect the printer during the printer driver installation.

2. Install the encoder driver (provided by the printer manufacturer) on all Command Centre workstations that will be using the printer.

   Note: Printers using the SCM encoder module will need to install the MIFARE Encoder Driver on all Command Centre workstations that will be using the printer.
   Refer to the document *"3E0774 Install Note MIFARE Encoder.pdf"* for installation instructions. This document and the MIFARE Encoder Drivers are located in the **`Utilities/MIFARE Encoder Drivers`** folder of the Command Centre installation files.

3. Restart the Command Centre workstations after installing the printer and encoder drivers.

Editing the Encoder.ini file

This topic describes how to edit the Encoder.ini file.

Before you begin

Editing the Encoder.ini file should only be done under advisement from Gallagher Technical Support.

The Encoder.ini file references the encoding.dll used for each supported printer. If your printer is not a supported printer, you may be able to use the encoding.dll that belongs to a supported printer.

Procedure

Use the following procedure to edit the Encoder.ini file to allow another printer to be supported.

1. On the workstation with the printer attached, open Windows Explorer.
2. Go to the directory C:\Program Files\Gallagher\Command Centre\Bin
   Note: This is the default directory on Windows 32-bit, but may differ depending on your installation.
3. Double-click on the **Encoder.ini** file and open in Notepad.
4. From the **Start** menu or **Control Panel** go to **Devices and Printers**.
5. Right click on the printer and select **Properties**.
6. Take note of the **Printer Name** from the **General** tab.
7. In Notepad, press <**Enter**> twice after the last entry (to leave a space), then add the following:

   [**Printer Name**]

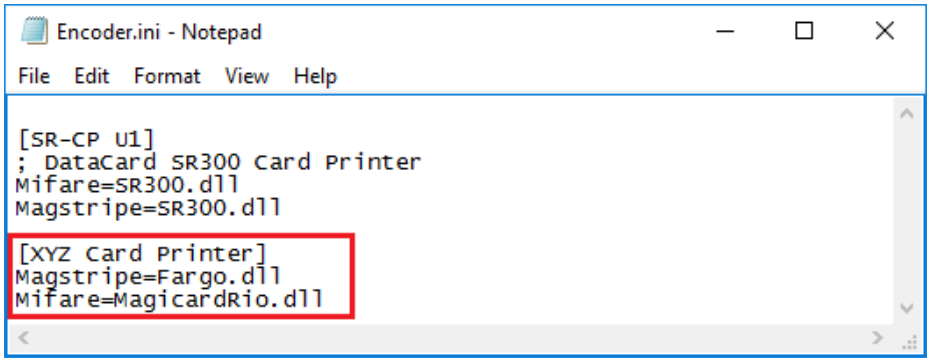
   MIFARE=encoding.dll

   Magstripe=encoding.dll

   Note: Remember to enter the Printer Name inside the square brackets.
8. Depending on the type of card you have, either:
   - type **Magstripe** = and the name of the **dll** file you wish to try, (i.e. DCSP55MIFARE.dll, Fargo.dll, FargoOmnikey.dll, CD800SingleWire.dll or SR300.dll)

     or

   - type **MIFARE** = and the name of the **dll** file you wish to try, (i.e. DCSP55MIFARE.dll, XID8300MIFARE.dll, FargoOmnikey.dll, CD800SingleWire.dll, MagicardRio.dll or SR300.dll)



9. Close Notepad and save the changes to the **Encoder.ini** file.
10. Try encoding and printing.
    If encoding is still unsuccessful, repeat this procedure but at Step 8 use the name of the other dll file. If still unable to print then, contact Gallagher Technical Support for further assistance.
11. Repeat this procedure to edit the Encoder.ini file located in the directories:
    - **`C:\Program Files\Gallagher\Command Centre\Client`**
    - **`C:\Program Files\Gallagher\Command Centre\ClientSetup\Client`** (server only)
12. Update **ClickOnceBuilder.exe** (server only).

    Once the **Encoder.ini** has been modified in the **`ClientSetup\Client`** directories, you will need to re-run the Click-Once executable (**ClickOnceBuilder.exe**) to include these additions in your next Click-Once deployment.

    The ClickOnceBuilder.exe is located in the directory `C:\Program Files\Gallagher\Command Centre\ClientSetup`
13. Update the Command Centre Client installation using Click-Once.

    Once the ClickOnceBuilder has been updated, you will need to update the Command Centre Client workstations that will be using the printer. When you launch the Command Centre Client you will be prompted to install the updated version. Click the **Install** button.

Designing Card Layouts

An operator with the correct privileges can create, edit and delete card layouts to existing card types. Refer to Setting up Card Types for procedure.

An operator must have the correct operator privileges to capture images for cardholders, and therefore edit cardholders. (Refer to ***Capturing an Image*** on page 33-10 under Personal Data Fields for procedure on capturing images.) They also require the correct privileges to be able to edit card layouts and to print cards. Refer to Operator Privileges to check.
Note: Any workstation running Photo ID needs to be configured for 24-bit colour to accurately display the cards on screen.

Select the item below that you require further detail on:

- ***Opening the Card Editor window*** (on page 47-14)
- ***Formatting Cards*** (on page 47-16)
- ***Adding a Background*** (on page 47-17)
- ***Working with Objects*** (on page 47-18)
- ***Copying Card Layouts*** (on page 47-54)

Opening the Card Editor window

Introduction

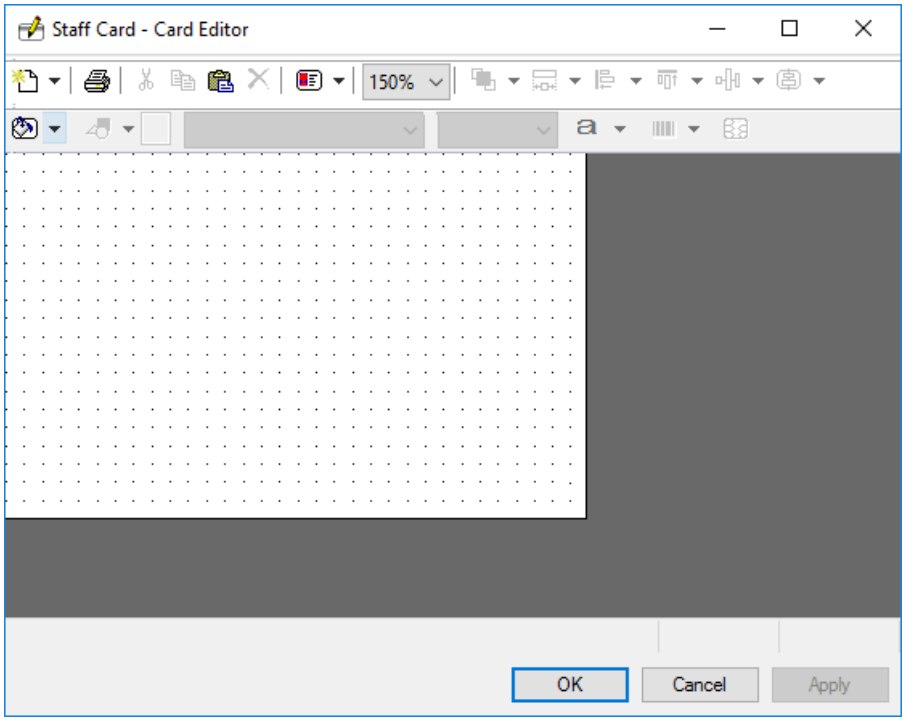
From within the Card Editor window you can format cards as necessary.

Procedure

1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens (in grid view).
2. **Right click** on the required card, and select **Edit Card Layout**.

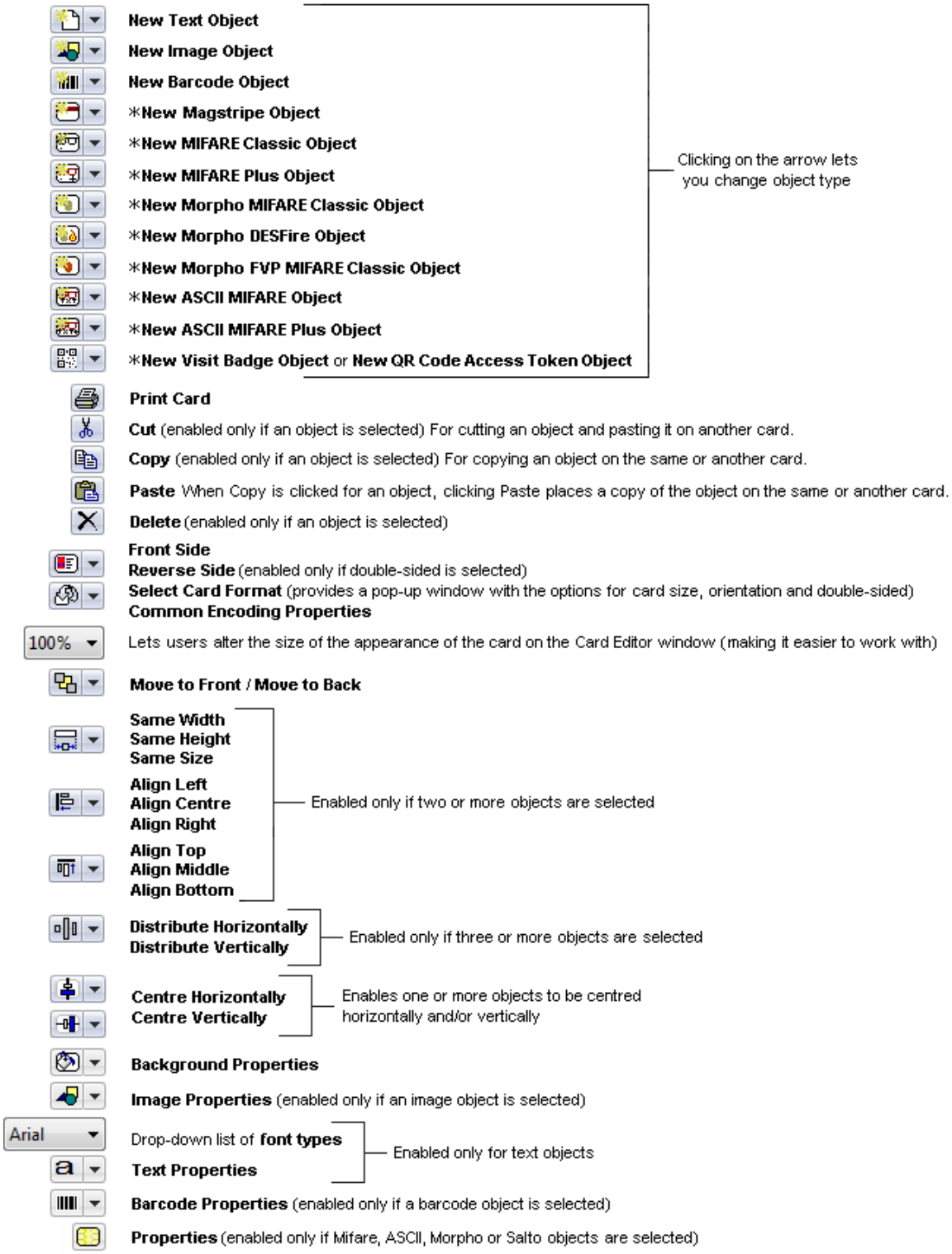
Result

The **Card Editor** window displays.
Not all the buttons on the Toolbar are enabled. Some of the formatting options are only available to specific object types, while other functions are available only when an object is selected, (i.e. when an object has placeholders around it).



Note:
The "Snap to Grid" option has been enabled on the screen above. You can turn this option on and off by clicking **Ctrl+G**. This grid can assist you to position objects exactly where you want them on a card.

Card Editor Toolbar



* **Note:** The **Magstripe**, **MIFARE** and **ASCII** objects will only be available if your Photo ID license includes card encoding. **Morpho** objects will only be available if your license includes Morpho. Likewise, **Salto** objects will only be available if your license includes Salto. **Visit Badge** objects are for sites using Visitor Management, and **QR Code Access Token** objects are for sites that have installed QR Code Readers as third-party readers.

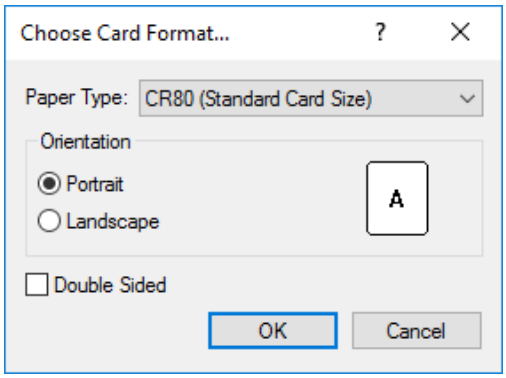
Formatting Cards

Introduction

This procedure describes how to format Card Type cards or Digital ID Type cards. It enables you to format the card size, orientation and whether the card is double-sided.

Procedure

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Click the  icon, then **Select Card Format**.
   The **Choose Card Format...** window displays.



3. Select the Paper Type from the drop-down list, (i.e. the size of the card).
   Note: For Digital ID Type cards the size affects its display on Mobile Devices.
4. Click the appropriate radio button to indicate the card orientation, i.e. Portrait (tall) or Landscape (wide).
5. Check the **Double Sided** checkbox if required.
   Note: The orientation has to be the same for both sides of a double-sided card, however by rotating text you could have one side portrait and the other side landscape. Rotation of images is not possible however, therefore if you wish to rotate an image you should do this in the source graphics package.
6. Click the **OK** button.
   Notes:
   - If Double Sided is checked, "Reverse Side" is now enabled on the drop-down list from the  icon.
   - "Common Encoding Properties" is another option available from the drop-down list, for MIFARE objects. If an object has not already been added to the card layout, when selected, the Common Card Encoding Properties dialog box opens with the **MIFARE Encoding Technology** field displaying 'None' and the following message:
     "Select a MIFARE encoding technology to continue".

     Encoding properties will display once a MIFARE technology is selected.

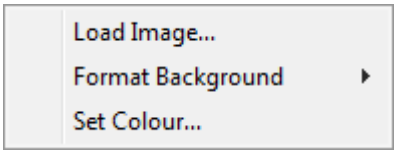
Adding a Background

Introduction

This procedure enables you to select a background for your card layout. You can select either a colour or an image as the background.

Procedure

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Click the **Background Properties** icon 
   A drop-down menu displays.



3. Depending on your requirements, click the appropriate option(s):

Option	Description
Load Image	Displays a window for you to locate the image file to load as a background on this card type. Path your way to the required image file and click the Open button. The image now displays as the background on the card layout. **Note:** The recommended maximum size for a background image is 2.5 MBytes.
Format Background	Provides a list of options of where and how to place the background image, (e.g. "Stretch" to make the image cover the entire card).
Set Colour	A colour swatch displays for you to select a background colour.

Note:
If you click the **OK** button now, the background image or colour you selected cannot be deleted. You can however select a new image or colour to replace the existing one.

Working with Objects

There are different object options for Card Types and Digital ID Types. Choose the appropriate procedure:

- ***Working with Card Type objects*** (on page 47-19)
- ***Working with Digital ID Type objects*** (on page 47-50)

Working with Card Type objects

Introduction

There are a number of objects you can add to a card layout:

- Text
- Image
- Barcode
- Magstripe
- Morpho MIFARE Classic
- Morpho DESFire
- Morpho FVP DESFire
- Morpho FVP MIFARE Classic
- MIFARE Classic
- MIFARE Plus
- MIFARE DESFire
- Salto MIFARE Classic
- Salto MIFARE Plus
- Salto MIFARE DESFire
- ASCII MIFARE Classic
- ASCII MIFARE Plus
- ASCII DESFire
- Non-diversified MIFARE DESFire
- Visit Badge
- QR Code Access Token

(**Note:** The Magstripe and MIFARE options will only be available if your Photo ID license includes card encoding. Likewise, the Morpho option is only available if your license includes Morpho, and the Salto option is only available if your license includes Salto. In addition to this, MIFARE objects can only be added to card types with a facility code that matches the one in your license.)

For each type, additional formatting options are available, some of which are common to all types, while other options are specific to individual types.
Note: Every time an object is added to a card layout it defaults to the same position on the card, (i.e. the top left corner of the card), thus making it difficult to identify new objects as they are added. For instructions on how to move objects on a card layout, refer to ***Moving Objects*** (on page 47-48).
Go to the item below that you require further detail on:

- ***Adding Text*** (on page 47-20)
- ***Joining Fields in the same Text Object*** (on page 47-21)
- ***Adding an Image*** (on page 47-22)
- ***Using the Transparency feature*** (on page 47-23)
- ***Adding a Barcode*** (on page 47-24)
- ***Adding a Magstripe object*** (on page 47-27)
- ***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)
- ***Adding a Morpho FVP MIFARE Classic object*** (on page 47-32)
- ***Adding a MIFARE Classic object*** (on page 47-33)
- ***Adding a MIFARE Plus object*** (on page 47-35)
- ***Adding a MIFARE DESFire object*** (on page 47-37)
- ***Adding an ASCII MIFARE Classic object*** (on page 47-38)
- ***Adding an ASCII MIFARE Plus object*** (on page 47-41)
- ***Adding an ASCII DESFire object*** (on page 47-44)
- ***Adding a Non-diversified MIFARE DESFire object*** (on page 47-46)

- ***Moving Objects*** (on page 47-48)
- ***Expanding an Object Box*** (on page 47-48)
- ***Selecting Multiple Objects*** (on page 47-49)
- ***Deleting Objects*** (on page 47-49)

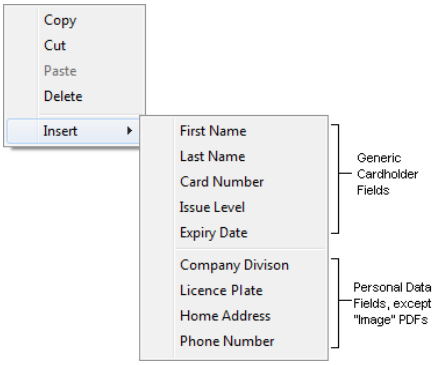
Notes:

- Adding Salto MIFARE objects is covered in the "Salto Lock Interface" section. Refer to ***Adding Salto MIFARE objects to a card layout*** for details.
- Adding visit badge objects is covered in the "Visitor Management" section. Refer to ***Adding Visitor details to cards/badges*** for details.
- Adding QR Code Access Token objects is covered in the process for QR Code Readers. Refer to ***QR Code Readers*** (on page 79-1) for details.

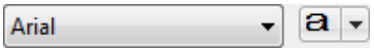
Adding Text

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Text Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. To add text, either:
   - type in the text,
   - insert text fields, as follows:

   (a) **Right click** within the text field, then click **Insert** from the drop-down menu. A drop-down menu displays.

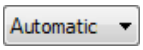


   (b) Click on the required item.
   The item now displays on the card layout.
   Note: You can insert more than one text field into the same text object. See ***Joining Fields in the same Text Object*** (on page 47-21) for procedure.

   - do a combination of both, i.e. type in text and insert text field(s). See ***Joining Fields in the same Text Object*** (on page 47-21) for procedure.
4. Format the text using the 

font options on the Toolbar. These options allow you to change the font type and alter the font properties as necessary. These properties include text colour, rotating the text on the card, and aligning the text within the placeholders.

Note: To alter the font size, you can either:

- place the cursor on one of the placeholders of the text object and drag to the desired size, or
- select the font size from the 

drop-down.
Note: The text will truncate if too much data is supplied to fit into the text object.

Joining Fields in the same Text Object

This procedure enables you to join text fields in the same text object, so they are treated as one entity on the card layout.

Example: To keep the appearance of cardholders 'First Names' and 'Last Names' the same, it is recommended to join these 2 fields in the 1 text object.

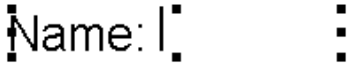
For cardholder Paul Stephenson-Hill, if you had his first name and last name as *two separate text objects*, on his card his name may appear as:



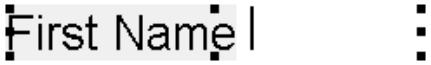
If you had his first name and last name *joined as one text object*, on his card his name would appear as:



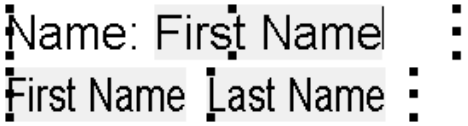
1. Select **New Text Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
2. Within the placeholders, either:
   - type in text, (e.g. Name:), or

   - **right click** and select **Insert**. Select the first field (either a 'Generic Cardholder Field' or a 'Personal Data Field') from the drop-down menu.

3. Press the 'spacebar' on your keyboard, or separate the fields some other way, (e.g. put a comma after the first field, then a space).
4. **Right click** within the placeholders, and repeat Step 2.
   Both fields now appear within the placeholders for this text object.

5. Repeat Steps 2-3 if necessary.
6. To allow for quite long fields, you may want to reduce the height of the text object, as follows:
   a) Place the cursor on either of the centre placeholders of the text object.
   b) When the cursor changes to a "double-headed arrow", click and hold down the mouse button.
   c) Move the mouse so the height of the text object reduces, and there is

more blank space within the placeholders of the text object.

d) Release the mouse button.

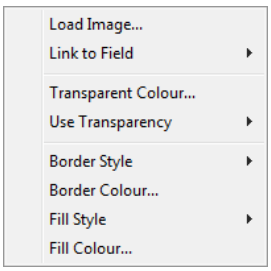


Note: The text object can also be left, centre or right aligned using the font options. The above example is left aligned.

Adding an Image

See ***Capturing an Image*** (on page 33-10) under Personal Data Fields for procedure on capturing images.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Image Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. Click the **Image Properties** icon 
   A drop-down menu displays.



4. Depending on your requirements, click the appropriate option:

Option	Description
Load Image	Displays a window for you to locate a previously saved image file to load on this card type, (e.g. Company logo). Path your way to the required image file and click the **Open** button. The image now displays on the card layout.
Link to Field	Displays a drop-down menu of all the "Image" PDFs. Click the appropriate PDF. The text in the "Image" box now indicates that it is linked to the "Image" PDF. **Note:** When you preview or print this card type for a cardholder, the actual image associated with that "Image PDF on their **Personal Data** tab will display.
Transparent Colour	A colour swatch displays for you to select a colour as the transparent background colour of the image.
Use Transparency	This enables you to make the background of an image transparent, so that the selected background of your card displays instead. **Note:** For more detail about using the transparency options, see ***Using the Transparency feature*** (next).

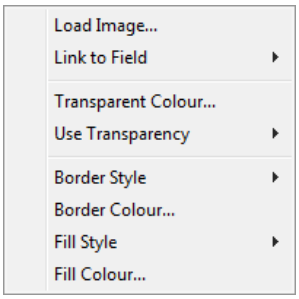
Option	Description
Border Style	Provides a list of border styles for you to select from if you wish to have a border around your image.
Border Colour	A colour swatch displays for you to select a border colour from.
Fill Style	Provides the option to have a solid fill within the border, (e.g. the border could be a blue line with a solid red fill inside it).
Fill Colour	A colour swatch displays for you to select a solid fill colour from.

Using the Transparency feature

The Transparency feature assumes you have:

- the card layout configured and you are trying to get better performance from the transparency feature
- a selection of photos taken at a dedicated photo station with consistent lighting and background colour (preferably blue)
- taken several colour samples of the colour you want set to 'transparent' and averaged the results for the Red, Green, Blue values (in general the defaults can be accepted for Hue, Saturation, Luminous)

1. Select the image object on the card layout.
   Placeholders appear around the object.
2. Click the **Image Properties** icon 
   A drop-down menu displays.



3. Select **Transparent Colour...**
   A colour swatch displays.
4. Select **Define Custom Colors** to update the colour values.
5. Accept the default values for **Hue**, **Sat** (saturation) and **Lum** (luminous).
6. Press **Add to Custom Colors** and click **OK**.
   This creates a 'custom colour' that is an 'average colour' of colour samples taken from images provided.
7. Click the **Image Properties** icon  again.
8. Select **Use Transparency...**, then **Custom Band**.
   This activates the Custom Band value box  beside the **Image Properties** icon, with a default value of 20.

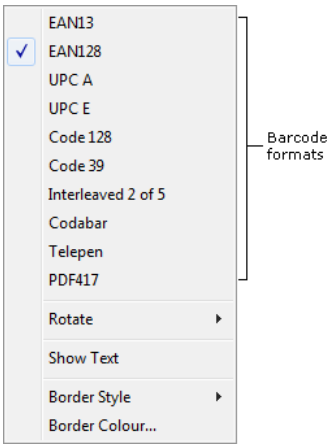
Notes:

- This value may need to be increased for people with spiky or curly hair.
- If you find that large amounts of black are being removed from your image you may want to check that you have defined the transparent colour correctly.

Adding a Barcode

It is possible to join barcode fields in the same object. See ***Joining Fields in the same Text Object*** (on page 47-21) for procedure.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Barcode Object**
   An object box displays with placeholders around it and a status message displays at the bottom of the **Card Editor** window. This message indicates the maximum number of characters that will print for the barcode you have entered. As you change the size of the barcode object, this value will increase/decrease, (i.e. the bigger you make the barcode the more characters are allowed). If the number of characters entered in the barcode object exceeds this amount, some barcodes will only print the number of characters indicated in the status message, while other barcodes shrink to include all characters. The Telepen format however has an **end** character, so all of the characters need to be printed, and the characters are a fixed width, so they cannot be shrunk to fit. Therefore, the size of the barcode must be big enough to include all characters (maximum of 12), otherwise it will be unreadable.
   Note: The size of the object box can be expanded if necessary, however to maintain readability of the barcode the Editor will adjust the barcode to the nearest readable size, (i.e. if you make it too big or too small). See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. Click the **Barcode Properties** icon
   A drop-down menu displays.



4. Select the type of Barcode format from the drop-down menu.
   The barcode format you select may alter the maximum number of characters shown in the status message.

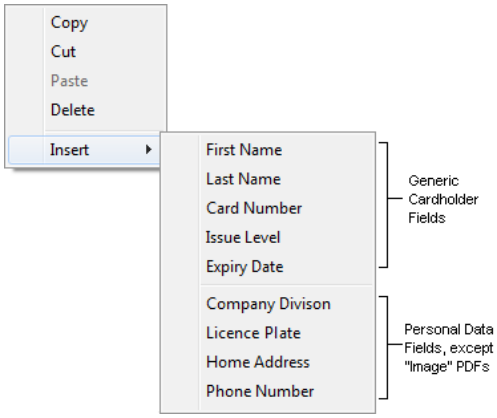
Notes:

- Barcode formats have set rules, (e.g. UPC codes require a set length of 11 digits). Go to the ***Taltech Web site*** for the rules applying to each of the formats (http://www.taltech.com/resources/barcode).
- For the PDF417 format, not only does the size of the barcode object limit the maximum number of the characters that will print, but so do the registry values. To change the registry values, see ***Changing registry values for PDF417 Barcodes*** (on page 47-25).

5. Use the other drop-down menu options if required:

Option	Description
Rotate	Enables you to rotate the Barcode on the card, (i.e. by 90, 180 or 270 degrees).
Show Text	Displays the text encoded underneath the Barcode.
Border Style	Provides a list of border styles for you to select from if you wish to have a border around your image.
Border Colour	A colour swatch displays for you to select a border colour from.

6. **Right click** on the barcode object, then click **Insert** from the drop-down menu. Another drop-down menu displays.
   Note: The actual amount of text which gets encoded in the barcode is limited by the size and type of the barcode. The smallest size barcode supports up to 8 characters for Code 39 barcode types and up to 12 characters for all other types. The largest size barcode supports up to 17 characters for Code 39 barcode types and up to 24 characters for all other types.



7. Click on the item you wish to display as a barcode on this card type.

Changing registry values for PDF417 Barcodes

Introduction

The registry values for the PDF417 barcode have been set so that the barcode will print with approximately 84 ASCII characters on a 35mm by 8mm area on a standard card with a redundancy level of 30%.

Note: The redundancy level is the level of corruption that can be present in the printed image, yet still allow for an accurate read.

The following table shows each registry value default for the PDF417 barcode:

Registry Value	Default	Min.	Max.	Description
BarcodePDFModuleHeight	30	10	100	Module (the smallest unit) height in mils (mil = 0.001 inches). Recommended to be three times larger than the Module Width so the barcode displays correctly.
BarcodePDFModuleWidth	10	7	100	Module width in mils (mil = 0.001 inches).
BarcodePDFSecurityLevel	best security level	0	8	Sets the Error Correction Level for PDF417 barcodes to a fixed value. 0 = error recognition only (no error correction) 8 = highest level of error correction.
BarcodePDFTruncatedSymbol	0	0	1	0 = false (full format). 1 = true (truncated format - no stop pattern).

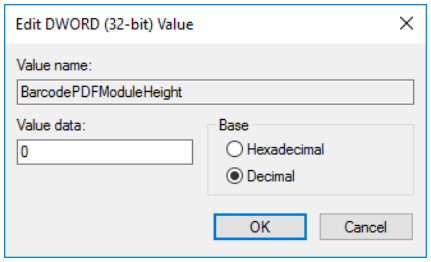
Warning: When changing the registry value for either **BarcodePDFModuleHeight** or **BarcodePDFModuleWidth**, Gallagher recommends that you make the value greater than the default already set. Anything less and you may have trouble scanning the barcode.

Where to change the registry values
Card Types are rendered on workstation PCs, but Digital ID Types are rendered on the Command Centre server. To have registry values affect PDF417 barcodes on Card Types, configure the registry values on all workstation PCs. To have registry values affect PDF417 barcodes on Digital ID Types, configure the registry values on all Workstations and the Command Centre server.

Procedure

To change a registry value, complete the following procedure:

1. From the **Start** menu, click **Run...**
2. Type in 'regedit' and click **OK**. The Registry Editor opens.
3. Path your way to **`HKEY_LOCAL_MACHINE\SOFTWARE\Gallagher\Command Centre`**.
   Notes:
   - If using a 64 bit system, browse to **`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Gallagher\Command Centre`**.
   - These directories are the default, but may differ depending on your installation.
4. **Right click** on **`Command Centre`**, and click **New**, then **DWORD Value**.
   A new DWORD Value appears at the bottom of the registry values list.
5. Enter the DWORD Value name, (e.g. BarcodePDFModuleHeight).
6. **Double-click** on the newly named DWORD Value.
   The Edit DWORD Value dialog displays:

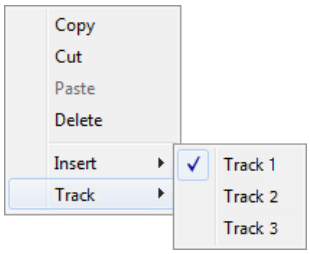


7. Click the **Decimal** radio button and enter your new value, (e.g. 10), then click the **OK** button.
   Note: The default value will be used if the value set is out of range.
8. Repeat Steps 4 - 7 to change each DWORD registry value, if required.
   For a changed registry value to take effect the **Card Editor** window must be closed and then re-opened.

Adding a Magstripe object

There are three tracks available for encoding data on Magstripe cards. Any or all of these three tracks can be used on a card layout, however each track can only be associated with one Magstripe object, (e.g. you cannot have two **Track 1** objects on a card).
It is possible to join magstripe fields in the same object. See ***Joining Fields in the same Text Object*** (on page 47-21) for procedure.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Magstripe Object** 
   An object box displays with placeholders around it. By default, this object is **Track 1** and Gallagher Encoded (with a vaild facility code included in your license file).
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the Magstripe object, then click **Track** from the drop-down menu. Another drop-down menu displays.



4. Click the appropriate "Track" for your requirements:
   Note: This allows you to add magstripe data and individually specify which data is to be encoded to Tracks 1, 2 and/or 3.

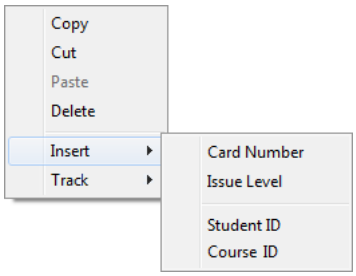
Option	Description
Track 1 (used for Cardax access)	a) "Gallagher Encoded" (this option is only available if your license file has a valid facility code) or b) select any non-image PDF, or c) enter any alpha-numeric string or other allowed

Option	Description
	characters (maximum of 76 characters), or d) nothing encoded. **Note:** "Gallagher Encoded" means the card number, facility code (as specified in the Card Type), and issue level will be encoded in Cardax format.
Track 2	a) select any non-image PDF, or b) enter digits or any of the characters **; : <=> ?** (maximum of 37 characters), or c) nothing encoded.
Track 3	a) select any non-image PDF, or b) enter digits or any of the characters **; : <=> ?** (maximum of 104 characters), or c) nothing encoded.

Notes:

- "Select any non-image PDF" means a text, number or list PDF is selected from those that are configured in the system, and visible to the operator. The content of the PDF will be encoded to the specified track, subject to data limitations for that track.
- "Nothing Encoded" means no data will be encoded to this track.

5. **Right click** within the object box, then click **Insert** from the drop-down menu. Another drop-down menu displays.



Note: This screen shot shows the data types available for Tracks 2 and 3. In addition to these data types, Track 1 also has another four, (i.e. 'First Name', 'Last Name', 'Expiry Date' and 'Gallagher Encoded').

6. Click on the required item.
   The item now displays on the card layout.
   Note: You can insert more than one text field into the same text object. See ***Joining Fields in the same Text Object*** (on page 47-21) for procedure.

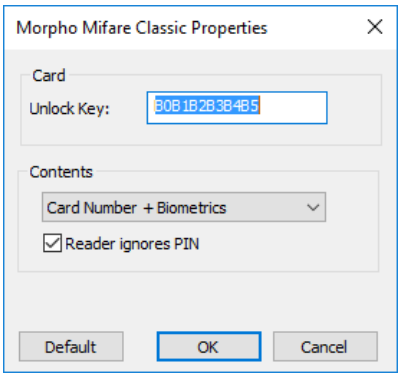
Adding a Morpho MIFARE Classic object

Morpho MIFARE Classic objects can only be added to card types with a facility code that matches the one in your license. This allows you to encode Morpho biometric information on a card.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Morpho MIFARE Classic Object** 

An object box displays with placeholders around it.
Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.

3. **Right click** on the Morpho MIFARE Classic object, then click **Properties** from the drop-down menu.
The Morpho MIFARE Classic Properties dialog box displays.



Note: The fields are populated with any previously configured values for existing Morpho MIFARE Classic objects.

4. Configure the Morpho MIFARE Classic properties as required:

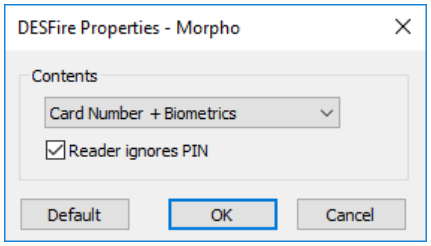
Option	Description
Unlock Key (Sector)	This is one of the standard values used to request write access for uninitialised cards. (Size Limit = 12 characters. Default = B0B1B2B3B4B5)
Contents	This drop-down list has only the following two options, (i.e. **Card Number Only** and **Card Number + Biometrics**). The option selected will define what will be encoded on the card.
Reader ignores PIN	This checkbox is enabled and by default will be checked. When checked, Morpho readers will ignore any PIN encoded on the card.

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

Adding a Morpho DESFire object

Morpho DESFire objects can only be added to card types with a facility code that matches the one in your license. This allows you to encode Morpho biometric information on a MIFARE DESFire EV1 /EV2 card.
Note: Only one Morpho DESFire object can be added to a card layout.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Morpho DESFire Object**
An object box displays with placeholders around it.
Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the Morpho DESFire object, then click **Properties** from the drop-down menu. The DESFire Properties - Morpho dialog box displays.



4. Configure the MIFARE DESFire properties as required:

Option	Description
Contents	This drop-down list has only the following two options, (i.e. **Card Number Only** and **Card Number + Biometrics**). The option selected will define what will be encoded on the card.
Reader ignores PIN	This checkbox is enabled and by default will be checked. When checked, Morpho readers will ignore any PIN encoded on the card.

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

5. Click the **OK** button to save the Morpho DESFire encoding properties.
The DESFire Properties - Morpho dialog box closes.

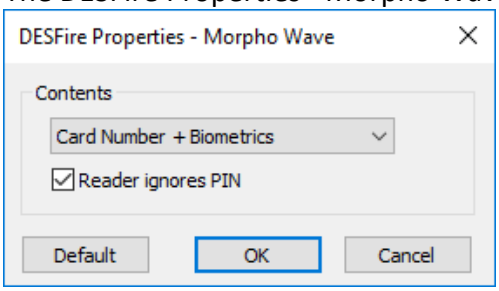
Adding a MorphoWave DESFire object

MorphoWave DESFire objects can only be added to card types with a facility code that matches the one in your license. This allows you to encode Morpho biometric information on a MIFARE® DESFire® EV1 or EV2 card.

Notes:

- The MorphoWave DESFire object will not encode "UNUSED" and "DURESS" fingerprints to a card. Only "ACCESS" fingerprints will encode to cardholder's card.
- Previously used DESFire cards should not be encoded for different cardholders.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New MorphoWave DESFire Object** 
An object box displays with placeholders around it.
Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the MorphoWave DESFire object, then click **Properties** from the drop-down menu.
The DESFire Properties - Morpho Wave dialog box displays.



4. Configure the MorphoWave DESFire properties as required:

Option	Description
Contents	This drop-down list has only the following two options: - Card Number Only - Card Number + Biometrics
Reader ignores PIN	This checkbox is enabled and by default is checked. When checked, MorphoWave readers will ignore any PIN encoded on the card.

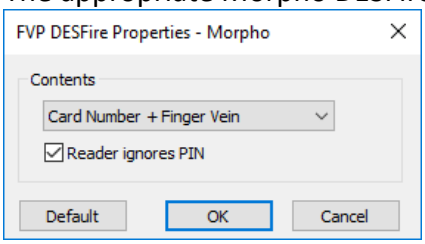
Note: The **Default** button allows you to reset the MorphoWave DESFire properties back to the default settings.

5. Click the **OK** button to save the MorphoWave DESFire encoding properties. The DESFire Properties - Morpho Wave dialog box closes.

Adding a Morpho FVP DESFire or Morpho VisionPass DESFire object

Morpho FVP FVP DESFire and Morpho VisionPass DESFire objects can only be added to card types with a facility code that matches the one in your license. This allows you to encode Morpho biometric information on a card.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Morpho FVP DESFire Object** or **New Morpho VisionPass DESFire Object** as appropriate.
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the Morpho DESFire object, then click **Properties** from the drop-down menu.
   The appropriate Morpho DESFire Properties dialog box displays.



   Note: The dialog box above is for the Morpho FVP DESFire Properties, however the same fields appear on the Morpho VisionPass DESFire Properties dialog box.
4. Configure the Morpho DESFire properties as required:

Option	Description
Contents	This drop-down list has only the following two options: - Card Number Only - Card Number + Finger Vein (for Morpho FVP) OR Card Number + Biometrics (for Morpho VisionPass)
Reader ignores PIN	This checkbox is enabled and by default will be checked. When checked, Morpho readers will ignore any PIN encoded on the card.

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

5. Click the **OK** button to save the Morpho DESFire encoding properties. The DESFire Properties - Morpho dialog box closes.

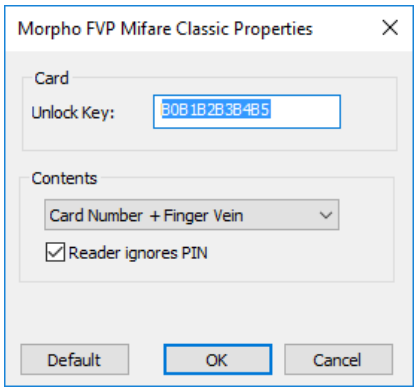
Adding a Morpho FVP MIFARE Classic object

Morpho FVP MIFARE Classic objects can only be added to card types with a facility code that matches the one in your license. This allows you to encode Morpho biometric information on a card.

Notes:

- When using Morpho FVP MIFARE Classic objects, the Gallagher object starting sectors should be earlier than the FVP starting sectors.
- Morpho FVP and Salto objects on the same card layout is not supported.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Morpho FVP MIFARE Classic Object**
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the Morpho FVP MIFARE Classic object, then click **Properties** from the drop-down menu.
   The Morpho FVP MIFARE Classic Properties dialog box displays.



   Note: The fields are populated with any previously configured values for existing Morpho FVP MIFARE Classic objects.

4. Configure the Morpho FVP MIFARE Classic properties as required:

Option	Description
Unlock Key (Sector)	This is one of the standard values used to request write access for uninitialised cards.
Contents	This drop-down list has only the following two options, (i.e. **Card Number Only** and **Card Number + Finger Vein**).
Reader ignores PIN	This checkbox is enabled and by default will be checked. When checked, Morpho readers will ignore any PIN encoded on the card.

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

5. Click the **OK** button to save the Morpho FVP MIFARE Classic encoding properties. The Morpho FVP MIFARE Classic Properties dialog box closes.

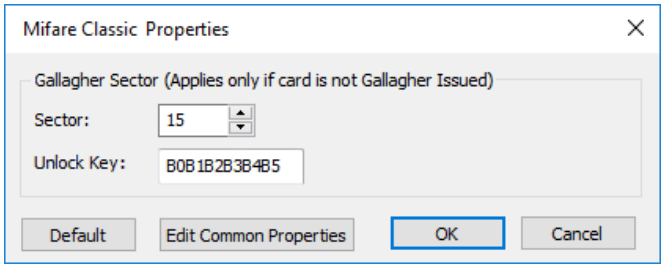
Adding a MIFARE Classic object

MIFARE Classic objects can only be added to card types with a facility code that matches the one in your license. There can also only be one MIFARE Classic object per card layout. Even though you can add (or copy) additional MIFARE Classic objects to a card, when you go to save it you will receive an error message.

Notes:

- MIFARE Classic cards do not support 6-digit user PINs. If a 6-digit PIN is specified for a MIFARE Classic card then the PIN will not work at the reader.
- The ***Cardholder Summary Report*** (on page 39-7), configured with the card type as an included column, can be used to determine which cardholders are using MIFARE Plus or MIFARE Classic cards. The card types should be clearly named to distinguish which card layouts contain MIFARE Plus objects and which contain MIFARE Classic objects.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New MIFARE Classic Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the MIFARE Classic object, then click **Properties** from the drop-down menu. The MIFARE Classic Properties dialog box displays with the options set by default for **Gallagher Issued** cards.

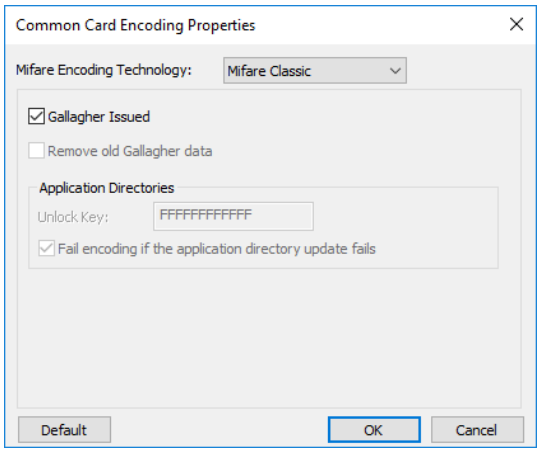


4. Configure the MIFARE Classic properties as required:

Option	Description
Sector	Only one sector of a MIFARE object can be populated. The drop-down list allows you to select which sector will be used. (Range = 1 - 15. Default = 15)
Unlock Key	This is the key used to unlock the sector that Gallagher data is written to. (Size Limit = 12 characters. Default = B0B1B2B3B4B5)

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

5. If you want to configure common encoding properties, click the **Edit Common Properties** button.
   The Common Card Encoding Properties dialog box displays.



6. If not already selected, select 'MIFARE Classic' from the **MIFARE Encoding Technology** drop-down list.
   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.
7. To alter the MIFARE properties, uncheck the **Gallagher Issued** checkbox.
   All fields become enabled.
8. Configure the MIFARE properties as required:

Option	Description
Remove old Gallagher data	This checkbox allows you to encode/re-encode to any sector and choose to either leave the Gallagher data on the card or remove it. Removing the Gallagher data from the card can cause performance issues. **Note:** If you write to the same sector as previously, the Gallagher data is removed and re-written.
Unlock Key	The Unlock Key fields allows you to access Sector 0 in the Application Directory. (Size Limit = 12 characters. Default = FFFFFFFFFFFF)
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.

   Note: The **Default** button allows you to reset the MIFARE Classic properties back to the default settings.
9. Click the **OK** button.
   The Common Card Encoding Properties dialog box closes.
10. Click the **OK** button to save the MIFARE Classic encoding properties.
    The MIFARE Classic Properties dialog box closes.

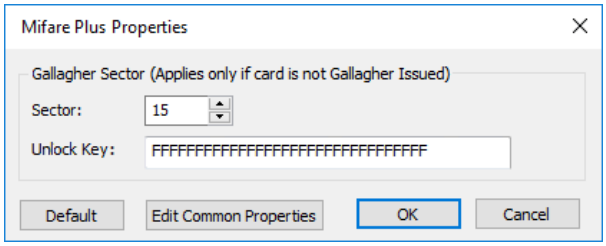
Adding a MIFARE Plus object

MIFARE Plus objects can only be added to card types with a facility code that matches the one in your license. There can also only be one MIFARE Plus object per card layout. Even though you can add (or copy) additional MIFARE Plus objects to a card, when you go to save it you will receive an error message.

Notes:

- Command Centre only encodes MIFARE Plus cards to Security Level 3.
- MIFARE Plus cards do not support 6-digit user PINs. If a 6-digit PIN is specified for a MIFARE Plus card then the PIN will not work at the reader.
- The ***Cardholder Summary Report*** (on page 39-7), configured with the card type as an included column, can be used to determine which cardholders are using MIFARE Plus or MIFARE Classic cards. The card types should be clearly named to distinguish which card layouts contain MIFARE Plus objects and which contain MIFARE Classic objects.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New MIFARE Plus Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the MIFARE Plus object, then click **Properties** from the drop-down menu.
   The MIFARE Plus Properties dialog box displays with the options set by default for **Gallagher Issued** cards.

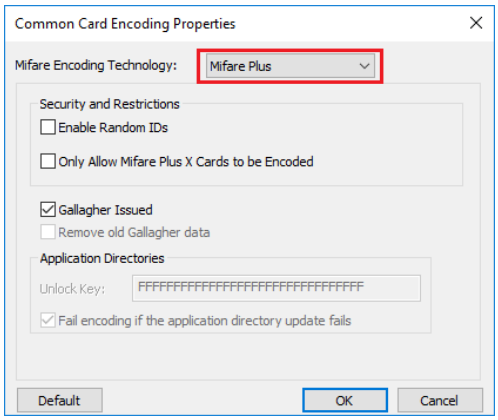


4. Configure the MIFARE Plus properties as required:

Option	Description
Sector	Only one sector of a MIFARE object can be populated. The drop-down list allows you to select which sector will be used. (Range = 2k cards: 1 - 15 and 17 - 31. 4k cards: 1 - 15 and 17 - 39. Default = 15)
Unlock Key	This is the key used to unlock the sector that Gallagher data is written to, (e.g. a third parties sector key should be entered in this field if the sector has been locked by the other party and hence the card manufacturer's key or Gallagher unlock key won't work.) **Note:** It must consist of 32 hexadecimal digits (0-9 and A-F). (Size Limit = 32 characters. Default = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)

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

5. If you want to configure common encoding properties, click the **Edit Common Properties** button.
   The Common Card Encoding Properties dialog box displays.
6. If not already selected, select 'MIFARE Plus' from the **MIFARE Encoding Technology** drop-down list.



   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.
7. To alter the MIFARE properties, uncheck the **Gallagher Issued** checkbox. All fields become enabled.
8. Configure the Security and Restrictions properties as required:

Option	Description
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 Plus/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.
Enable Random IDs	Checking this forces the card to use a random unique ID during collision detection.
Only Allow MIFARE Plus X Cards to be Encoded	Checking this prevents MIFARE Plus S cards from being encoded with this card type.
Unlock Key	The Unlock Key fields allows you to access Sector 0 in the Application Directory. (e.g. a third parties MAD write key should be entered in this field if the MAD has been locked

Option	Description
	by the other party and hence the card manufacturer's key or Gallagher unlock key won't work.) **Note:** It must consist of 32 hexadecimal digits (0-9 and A-F). (Size Limit = 32 characters. Default = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
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

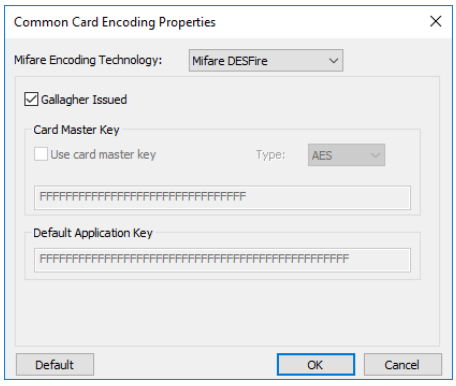
Note: The **Default** button allows you to reset the MIFARE Plus properties back to the default settings.

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

Adding a MIFARE DESFire object

MIFARE DESFire objects can only be added to card types with a facility code that matches the one in your license. There can also only be one MIFARE DESFire object per card layout. Even though you can add (or copy) additional MIFARE DESFire objects to a card, when you go to save it you will receive an error message.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New MIFARE DESFire Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the MIFARE DESFire object, then click **Common Encoding Properties** from the drop-down menu.
   The Common Encoding Properties dialog box displays.



4. If not already selected, select 'MIFARE DESFire' from the **MIFARE Encoding Technology** drop-down list.
   By default, the **Gallagher Issued** checkbox is enabled (ticked), which means that when you configure the MIFARE DESFire object on a card layout, all other configuration options are disabled. If a blank card is encoded with this option enabled, then the Card Master Key will be set to a unique 128 bit AES key derived from the MIFARE Plus/DESFire key seed.
5. To alter the MIFARE DESFire properties, uncheck the **Gallagher Issued** checkbox.
6. Configure the MIFARE DESFire properties as required:

Option	Description
Use card master key	When this checkbox is checked the Card Master Key specified is used to encode data onto the card. If this checkbox is unchecked, either the card to be encoded must be configured to not require Card Master Key authentication for application creation, or dummy Gallagher applications need to exist on 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.

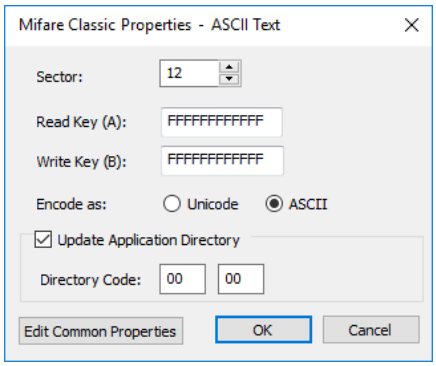
   Note: The **Default** button allows you to reset the MIFARE DESFire properties back to the default settings.
7. Click the **OK** button to save the MIFARE DESFire encoding properties.
   The Common Card Encoding Properties dialog box closes.

Adding an ASCII MIFARE Classic object

ASCII MIFARE Classic objects can only be added to card types with a facility code that matches the one in your license.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)

2. Select **New ASCII MIFARE Classic Object**
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the ASCII Text MIFARE object, then click **Properties** from the drop-down menu.
   The MIFARE Classic Properties - ASCII Text dialog box displays.

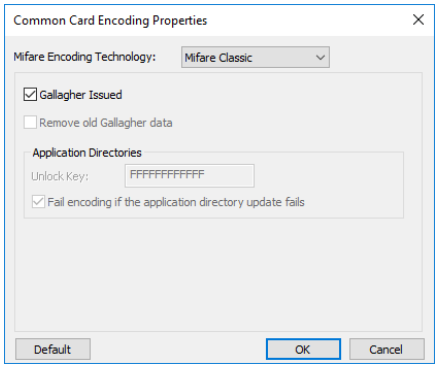


4. Configure the ASCII MIFARE Classic properties as required:

Option	Description
Sector	The drop-down list allows you to select the sector to be encoded with ASCII data. (Range = 1 - 15. Default = 12) **Notes:** • Sector 15 is usually reserved for Gallagher. • Choose your sector carefully. If you are using Morpho or Salto reader hardware, Morpho requires 10 consecutive sectors and Salto requires at least 5 consecutive sectors. • There is a constraint of a maximum of 48 bytes per sector.
Read Key (A)	Sets a read key used to read the sector that the ASCII data is written to. **Note:** It must consist of 12 hexadecimal digits (0-9 and A-F). (Size Limit = 12 characters. Default = FFFFFFFFFFFF)
Write Key (B)	Sets a lock/unlock key used to lock the sector that the ASCII data is written to. **Note:** It must consist of 12 hexadecimal digits (0-9 and A-F). (Size Limit = 12 characters. Default = FFFFFFFFFFFF)
Encode as	Click the appropriate radio button for what you want the data to be encoded as, (i.e. either **Unicode** or **ASCII**).
Update Application Directory	The MIFARE Application Directory (MAD) is the directory of all the sectors on the card. By default this checkbox is enabled (ticked), which means the Application Directory will be updated with a pointer to the sector containing the ASCII data. If you choose not to update the Application Directory, (i.e. uncheck the checkbox), the reader must search the whole card to locate the ASCII encoded sector.

Option	Description
Directory Code	Directory **Access** Code field and Directory **Application** Code field. This entry is unique to the application reading the ASCII data on this sector. Each field consists of two hexadecimal digits (0-9 and A-F).

5. If you want to configure common encoding properties, click the **Edit Common Properties** button.
   The Common Card Encoding Properties dialog box displays.

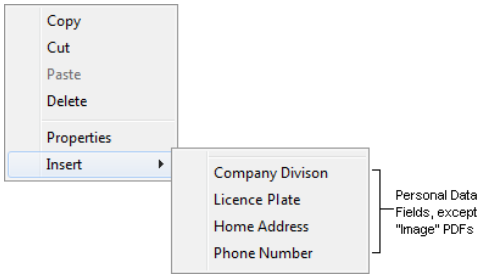


6. If not already selected, select 'MIFARE Classic' from the **MIFARE Encoding Technology** drop-down list.
   By default, the **Gallagher Issued** checkbox is enabled (ticked), which means that when you configure the MIFARE Classic object on a card layout, all other configuration options are disabled.
7. To alter the MIFARE properties, uncheck the **Gallagher Issued** checkbox.
   All fields become enabled.
8. Configure the MIFARE properties as required:

Option	Description
Remove old Gallagher data	This checkbox allows you to encode/re-encode to any sector and choose to either leave the Gallagher data on the card or remove it. Removing the Gallagher data from the card can cause performance issues. **Note:** If you write to the same sector as previously, the Gallagher data is removed and re-written.
Unlock Key	The Unlock Key fields allows you to access Sector 0 in the Application Directory. (Size Limit = 12 characters. Default = FFFFFFFFFFFF)
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.

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

9. Click the **OK** button.
   The Common Card Encoding Properties dialog box closes.
10. Click the **OK** button to save the ASCII MIFARE Classic encoding properties.
    The MIFARE Classic Properties - ASCII Text dialog box closes.
11. **Right click** within the object box, then click **Insert** from the drop-down menu. Another drop-down menu displays.

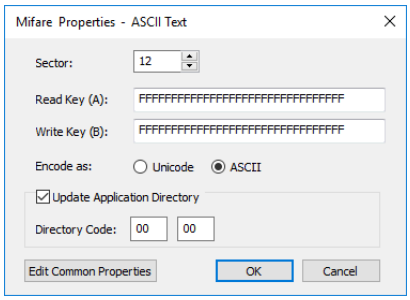


12. Click on the required item. The item now displays on the card layout.

Adding an ASCII MIFARE Plus object

ASCII MIFARE Plus objects can only be added to card types with a facility code that matches the one in your license.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New ASCII MIFARE Plus Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the ASCII Text MIFARE Plus object, then click **Properties** from the drop-down menu. The MIFARE Properties - ASCII Text dialog displays.

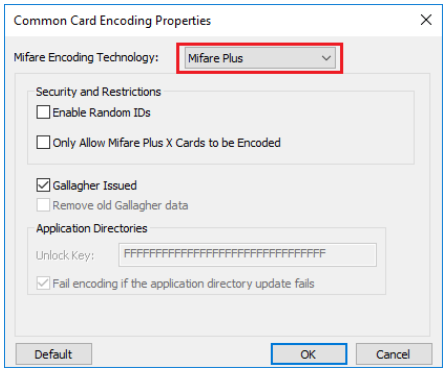


4. Configure the ASCII MIFARE Plus properties as required:

Option	Description
Sector	The drop-down list allows you to select the sector to be encoded with ASCII data. (Range = 1 - 15. Default = 12) **Notes:** • Sector 15 is usually reserved for Gallagher. • Choose your sector carefully. If you are using Morpho or Salto reader hardware, Morpho requires 10 consecutive sectors and Salto requires at least 5 consecutive sectors. • There is a constraint of a maximum of 48 bytes per sector.

Option	Description
Read Key (A)	Sets a read key used to read the sector that the ASCII data is written to. **Note:** It must consist of 32 hexadecimal digits (0-9 and A-F). (Size Limit = 32 characters. Default = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Write Key (B)	Sets a lock/unlock key used to lock the sector that the ASCII data is written to. **Note:** It must consist of 32 hexadecimal digits (0-9 and A-F). (Size Limit = 32 characters. Default = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Encode as	Click the appropriate radio button for what you want the data to be encoded as, (i.e. either **Unicode** or **ASCII**).
Update Application Directory	The MIFARE Application Directory (MAD) is the directory of all the sectors on the card. By default this checkbox is enabled (ticked), which means the Application Directory will be updated with a pointer to the sector containing the ASCII data. If you choose not to update the Application Directory, (i.e. uncheck the checkbox), the reader must search the whole card to locate the ASCII encoded sector.
Directory Code	Directory **Access** Code field and Directory **Application** Code field. This entry is unique to the application reading the ASCII data on this sector. Each field consists of two hexadecimal digits (0-9 and A-F).

5. If you want to configure common encoding properties, click the **Edit Common Properties** button.
   The Common Card Encoding Properties dialog box displays.
6. If not already selected, select 'MIFARE Plus' from the **MIFARE Encoding Technology** drop-down list.



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

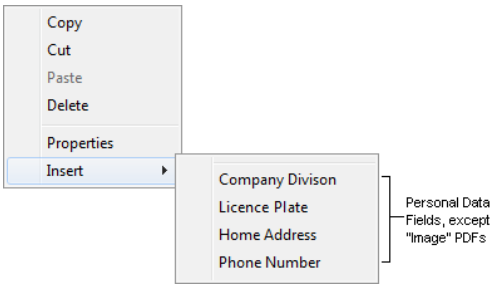
8. Configure the MIFARE properties as required:

Option	Description
Remove old Gallagher data	This checkbox allows you to either leave the old Gallagher data on the card or remove it. **Notes:** • Removing the Gallagher data will only succeed if the old card data was encoded with the same MIFARE Plus/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.
Enable Random IDs	Checking this forces the card to use a random unique ID during collision detection.
Only Allow MIFARE Plus X Cards to be Encoded	Checking this prevents MIFARE Plus S cards from being encoded with this card type.
Unlock Key	The Unlock Key fields allows you to access Sector 0 in the Application Directory. (e.g. 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.) **Note:** It must consist of 32 hexadecimal digits (0-9 and A-F). (Size Limit = 32 characters. Default = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
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.

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

9. Click the **OK** button.
   The Common Card Encoding Properties dialog box closes.
10. Click the **OK** button to save the ASCII MIFARE Plus encoding properties.
    The MIFARE Properties - ASCII Text dialog box closes.

11. **Right click** within the object box, then click **Insert** from the drop-down menu. Another drop-down menu displays.



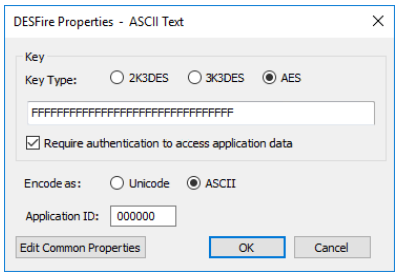
12. Click on the required item. The item now displays on the card layout.

Adding an ASCII DESFire object

ASCII DESFire objects can only be added to card types with a facility code that matches the one in your license. This allows you to encode ASCII data on a MIFARE DESFire EV1 / EV2 card.

Note: Multiple ASCII DESFire objects can be added to a Card Layout.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New ASCII DESFire Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. **Right click** on the ASCII DESFire object, then click **Properties** from the drop-down menu. The DESFire Properties - ASCII Text dialog box displays.

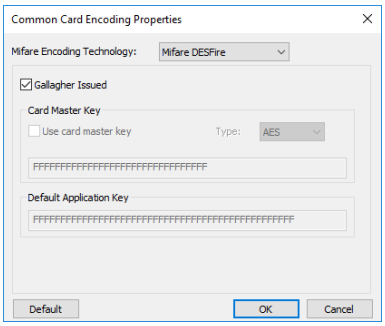


4. Configure the ASCII DESFire properties as required:

Option	Description
Key Type	Select the type of encryption used for the Card Master Key, either 2K3DES, 3K3DES or AES.
Application Master Key	This field must have either 32 hexadecimal characters for AES or 2K3DES encryption types, or 48 hexadecimal characters for the 3K3DES encryption type. Hexadecimal character validation occurs when the **OK** button is clicked. **Note:** If an application with a specified AppID has been encoded using this key, the AppID cannot be re-encoded using a different key.

Option	Description
Require authentication to access application data	Select this checkbox if authentication is required to access the application data. **Note:** If this checkbox is deselected, the authentication key is still written to the card, but is not required when reading the application data.
Encode as	Click the appropriate radio button for what you want the data to be encoded as, (i.e. either **Unicode** or **ASCII**).
Application ID	The UID. This entry is unique to the application reading the ASCII data on the card.

5. If you want to configure the common MIFARE DESFire encoding properties for the card, click the **Edit Common Properties** button.
The Common Card Encoding Properties dialog box displays.



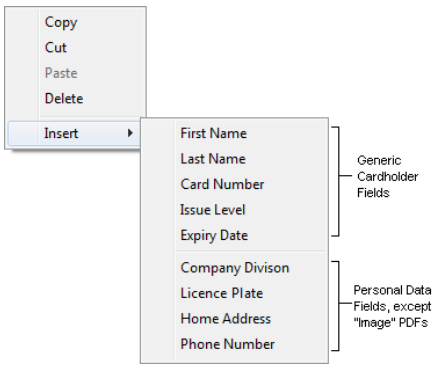
6. If not already selected, select **MIFARE DESFire** from the **MIFARE Encoding Technology** drop-down list. The MIFARE DESFire fields properties display with the options set by default for **Gallagher Issued** cards.
7. To alter the MIFARE DESFire properties, uncheck the **Gallagher Issued** checkbox. All the fields become enabled.

Option	Description
Gallagher Issued	By default this checkbox is enabled (ticked), which means that when you configure the MIFARE DESFire object on a Card Layout, all other configuration options are disabled. If a blank card is encoded with this option enabled, then the Card Master Key will be set to a unique 128 bit AES key derived from the MIFARE Plus/DESFire key seed.
Use card master key	When this checkbox is checked the Card Master Key specified is used to encode data onto the card. If this checkbox is unchecked, either the card to be encoded must be configured to not require Card Master Key authentication for application creation, or dummy Gallagher applications need to exist on 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.

Option	Description
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 hexadecimal 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 DESFire properties back to the default settings.

8. Click the **OK** button to save the MIFARE DESFire encoding properties.
   The Common Card Encoding Properties dialog box closes.
9. Click the **OK** button to save the ASCII DESFire properties.
   The DESFire Properties - ASCII Text dialog box closes.
10. Right click within the object box, then click **Insert** from the drop-down menu. Another drop-down menu displays.



11. Click on the required item. The item now displays on the Card Layout.

Adding a Non-diversified MIFARE DESFire object

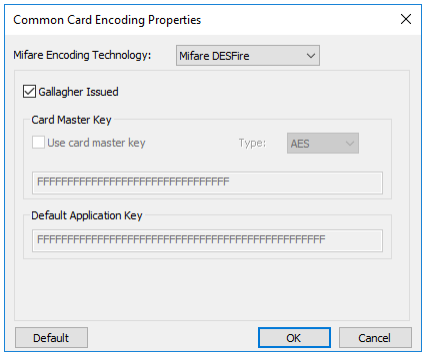
Non-diversified MIFARE DESFire objects can only be added to card types with a facility code that matches the one in your license. More than one non-diversified MIFARE DESFire object can be added to a card layout.

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Non-diversified MIFARE DESFire Object**
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.

3. **Right click** on the Non-diversified MIFARE DESFire object, then click **Properties** from the drop-down menu.
   The Non-diversified MIFARE DESFire Object Properties dialog box displays.
4. Configure the Non-diversified MIFARE DESFire properties as required:

Option	Description
AES Key	This field must have 32 hexadecimal characters for the AES encryption type. This can be done by either manually typing in a string, or by clicking the **Generate** button which will automatically populate the field with a random hexadecimal string.
Application ID	The UID. This entry is unique to the application reading the MIFARE data on the card. It must be 6 hexadecimal characters (0-9, A-F).

5. If you want to configure the common Non-diversified MIFARE DESFire encoding properties for the card, click the **Edit Common Properties** button.
   The Common Card Encoding Properties dialog box displays.



6. If not already selected, select **MIFARE DESFire** from the **MIFARE Encoding Technology** drop-down list.
   The MIFARE DESFire fields properties display with the options set by default for **Gallagher Issued** cards.
7. To alter the MIFARE DESFire properties, uncheck the **Gallagher Issued** checkbox. All the fields become enabled.

Option	Description
Gallagher Issued	By default, this checkbox is enabled (ticked), which means that when you configure the MIFARE DESFire object on a Card Layout, all other configuration options are disabled. If a blank card is encoded with this option enabled, then the Card Master Key will be set to a unique 128-bit AES key derived from the MIFARE Plus/DESFire key seed.
Use card master key	When this checkbox is checked the Card Master Key specified is used to encode data onto the card. If this checkbox is unchecked, either the card to be encoded must be configured to not require Card Master Key authentication for application creation, or dummy Gallagher applications need to exist on the card. When checked, the **Type** drop-down box and the **Card Master Key** field are enabled.

Option	Description
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.

8. Click the **OK** button to save the MIFARE DESFire encoding properties.
   The Common Card Encoding Properties dialog box closes.
9. Click the **OK** button to save the Non-diversified MIFARE DESFire properties.
   The Non-diversified MIFARE DESFire Object Properties dialog box closes.

Moving Objects

This procedure allows you to move an object to another position on a card layout.

1. Click on an object.
   Placeholders appear around the object.
2. Move the cursor over the edge of the object.
3. When the cursor changes to the 'object moving' icon , click and hold down the mouse-button.
4. Move the mouse and the object box moves to another position on the card layout.
5. When the object box is in the required position, release the mouse-button.

Expanding an Object Box

This procedure allows you to expand the size of an object box.

1. Place the cursor on one of the placeholders of an object box.
2. When the cursor changes to a double-headed arrow, click and hold down the mouse button.
3. Move the mouse and the object box resizes.
4. When the object box is the required size, release the mouse-button.

Selecting Multiple Objects

This procedure enables you to select multiple objects so you can format them the same, (e.g. you can change the font for multiple text objects rather than change them individually).

1. Click on one of the objects.
   Placeholders appear around the object.
2. Hold down the **Shift** key on your keyboard and click on the next object.
   The placeholders around the first object change to white, and the placeholders around the next object are black.
   

3. Repeat Step 2 for each additional object you wish to group together.
4. Format the objects as necessary.
   The  icons on the Toolbar are now enabled to allow you to do the following with the selected objects:
   - make the objects the same width / height / size
   - align the objects vertically
   - align the objects horizontally

   If you selected three or more objects, the 'Distribute Horizontally'  button is also enabled.

Deleting Objects

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Place the cursor on the object (text, image or barcode) you wish to delete so it displays with placeholders around it.
   The **Delete**  button is now enabled.
3. Either:
   - click the **Delete**  button, or
   - **right click**, then click **Delete** from the drop-down menu.

   The object is deleted from the card layout.
4. Click the **OK** button to permanently delete the object, or click the **Cancel** button to close the **Card Editor** window without saving your changes and recover the deleted objects.

Working with Digital ID Type objects

Introduction

There are just three objects you can add to a Digital ID Type card layout:
- Text
- Image
- Barcode

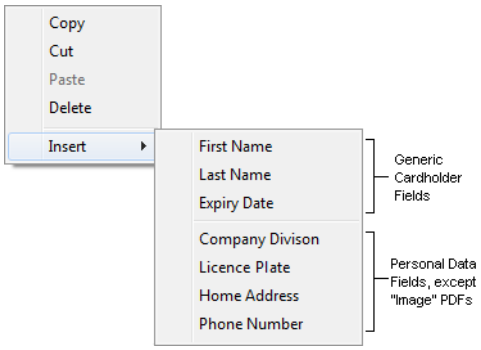
For each object, additional formatting options are available, some of which are common to all types, while other options are specific to individual types.
Note: Every time an object is added to a card layout it defaults to the same position on the card, (i.e. the top left corner of the card), thus making it difficult to identify new objects as they are added. For instructions on how to move objects on a card layout, refer to ***Moving Objects*** (on page 47-48).
Go to the item below that you require further detail on:

- ***Adding Text*** (on page 47-20)
- ***Joining Fields in the same Text Object*** (on page 47-21)
- ***Adding an Image*** (on page 47-22)
- ***Using the Transparency feature*** (on page 47-23)
- ***Adding a Barcode*** (on page 47-24)
- ***Moving Objects*** (on page 47-48)
- ***Expanding an Object Box*** (on page 47-48)
- ***Selecting Multiple Objects*** (on page 47-49)
- ***Deleting Objects*** (on page 47-49)

Adding Text - Digital ID

1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Text Object** 
   An object box displays with placeholders around it.
   Note: The size of the object box can be expanded if necessary. See ***Expanding an Object Box*** (on page 47-48) for procedure.
3. To add text, either:
   - type in the text,
   - insert text fields, as follows:

   (a) **Right click** within the text field, then click **Insert** from the drop-down menu. A drop-down menu displays.



(b) Click on the required Cardholder property.
The item now displays on the card layout.

Note: You can insert more than one text field into the same text object. See ***Joining Fields in the same Text Object*** (on page 47-21) for procedure.

- do a combination of both, i.e. type in text and insert text field(s). See ***Joining Fields in the same Text Object*** (on page 47-21) for procedure.

4. Format the text using the Arial font options on the Toolbar. These options allow you to change the font, style, and other text properties. These properties include text colour, rotating the text on the card, and aligning the text within the placeholders.
To alter the font size, you can either:
   - place the cursor on one of the placeholders of the text object and drag to the desired size (if the font size is Auto), or
   - select the font size from the Automatic drop-down.
   Note: The text will truncate if too much data is supplied to fit into the text object (unless the text size is Auto).

Adding a Barcode - Digital ID

It is possible to join barcode fields in the same object. See ***Joining Fields in the same Text Object*** (on page 47-21) for procedure.

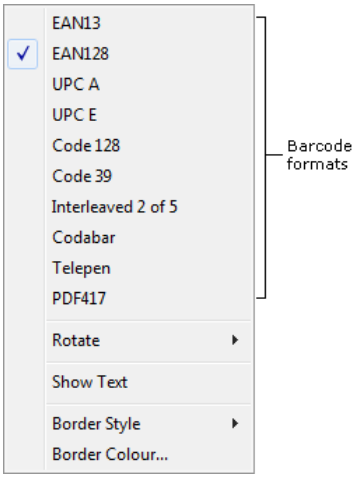
1. Open the **Card Editor** window. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. Select **New Barcode Object**
An object box displays with placeholders around it and a status message displays at the bottom of the **Card Editor** window. This message indicates the maximum number of characters that will print for the barcode you have entered.

   As you change the size of the barcode object, this value will increase/decrease, (i.e. the bigger you make the barcode the more characters are allowed). If the number of characters entered in the barcode object exceeds this amount, some barcodes will only print the number of characters indicated in the status message, while other barcodes shrink to include all characters.

   The Telepen format, however, has an **end** character; all of the characters need to be printed, and the characters are a fixed width, so they cannot be

shrunk to fit. Therefore, the size of the barcode must be big enough to include all characters (maximum of 12). Otherwise, it will be unreadable.
Note: The size of the object box can be expanded if necessary. However, to maintain readability of the barcode, the Editor will adjust the barcode to the nearest readable size, (i.e. if you make it too big or too small). See ***Expanding an Object Box*** (on page 47-48) for procedure.

3. Click the **Barcode Properties** icon
A drop-down menu displays.

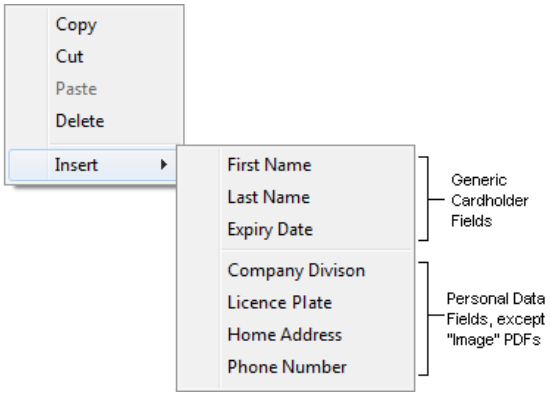


4. Select the type of Barcode format from the drop-down menu.
The barcode format you select may alter the maximum number of characters shown in the status message.
Notes:
   - Barcode formats have set rules, (e.g. UPC codes require a set length of 11 digits). Go to the ***Taltech Web site*** for the rules applying to each of the formats (http://www.taltech.com/resources/barcode).
   - For the PDF417 format, not only does the size of the barcode object limit the maximum number of the characters that will print, but so do the registry values. To change the registry values, see ***Changing registry values for PDF417 Barcodes*** (on page 47-25).

   IMPORTANT: To affect Digital ID barcode objects, registry values must be configured on the Command Centre server as well as on Workstations. Digital IDs are rendered on the Command Centre server.
5. Use the other drop-down menu options if required:

Option	Description
Rotate	Enables you to rotate the Barcode on the card, (i.e. by 90, 180 or 270 degrees).
Show Text	Displays the text encoded underneath the Barcode.
Border Style	Provides a list of border styles for you to select from if you wish to have a border around your image.
Border Colour	A colour swatch displays for you to select a border colour from.

6. **Right click** on the barcode object, then click **Insert** from the drop-down menu. Another drop-down menu displays.
   Note: The actual amount of text which gets encoded in the barcode is limited by the size and type of the barcode. The smallest size barcode supports up to 8 characters for Code 39 barcode types and up to 12 characters for all other types. The largest size barcode supports up to 17 characters for Code 39 barcode types and up to 24 characters for all other types.



7. Click on the item you wish to display as a barcode on this card type.

Copying Card Layouts

Introduction

To clone (copy) a card layout it is recommended you use the "Copy and Paste" method rather than "Drag and Drop", as this method positions details exactly where it should be on a card.

Procedure

1. Open the **Card Editor** windows for the card you wish to create a layout for, and the card whose layout you wish to copy. ***How?*** (see ***Opening the Card Editor window*** on page 47-14)
2. On the card layout you wish to copy from, place the cursor on the object (text, image or barcode) you wish to copy so it displays with placeholders around it.
   Note: If you wish to copy multiple objects, but **not all** objects from a card layout, see ***Selecting Multiple Objects*** (on page 47-49) for procedure.
   If you wish to copy **all** objects from a card layout, click on one of the objects, then press **Ctrl-A** on your keyboard.
   All the objects have placeholders around them.
   The **Copy** and **Paste** buttons are now enabled.
3. Click the **Copy** button.
4. On the **Card Editor** window of the card layout you are copying to, click the **Paste** button.
   If the card format is the same for both cards, the object(s) will display exactly where they were positioned on the original card.
5. Repeat Steps 2 - 5 as necessary.
6. Click the **OK** buttons to close both **Card Editor** windows.

Printing/Encoding Cards

Introduction

An operator with the correct privileges can configure card layouts, as well as print and/or encode card layouts.

Notes:

- To be able to encode cards, your site must have Photo ID with card encoding included in their license file. The license file must also include a valid Facility Code before you can encode cards with Gallagher data, and a key device, (e.g. Controller) must be on line.
- Gallagher Command Centre allows up to 256 Facility Codes.
- Printer/encoder drivers are **not** provided with the Command Centre installation files. Therefore, they need to be sourced and installed separately.
- If your site is using Gallagher, Salto and Morpho Biometric readers, cardholders can be issued with a single MIFARE SmartCard for access at all these readers. However, encoding of all three types together on the same card layout is only possible on 4k MIFARE cards. Refer to ***Working with Objects*** (on page 47-18) for further detail regarding adding these objects to card layouts.
- The EDIsecure RTP8500/XID8500 printer is capable of Magstripe encoding. If you require Magstripe encoding, open the Printing Preferences of the RTP8500/XID8500's Printer Properties, and for the Card Type, tick the **Magstripe** checkbox.

Notes regarding MIFARE Enhanced Security feature

- We recommend that all new Command Centre sites using MIFARE readers set a MIFARE Enhanced security key **before** any cards are encoded for the site, even if you do not intend using the MIFARE Enhanced Security feature. This gives you the option to implement the MIFARE Enhanced Security feature on your readers at a future date, whereas if you do not do it immediately, you will have to re-encode all cards. Refer to Card Security for further details.
- Sites using the MIFARE Enhanced Security feature, and purchasing pre-encoded cards from a third party, (either from Gallagher or from a supplier who encodes cards for them), need to provide the third party with the exported MIFARE Site Keys and password to allow the cards to be encoded with the enhanced MIFARE security.
- Cards encoded at sites using the MIFARE Enhanced Security feature can be used at sites that are not using this feature. However, cards not encoded with the high-security data or encoded using a different key seed will not work at a site using the MIFARE Enhanced Security feature, except on readers where the "Require Enhanced security MIFARE encoded cards" checkbox is unchecked (on the readers **Connections** property page).

When a card is printed, an event is generated in the Event Viewer window. The event details:

- the card type and the card number
- who printed the card
- which cardholder had a card printed, and
- the reason for printing the card, if this is configured for Photo ID.

Hint:

Before printing a card type for the first time, it is recommended you test the layout by previewing the card for a cardholder with quite a long name. This will ensure that the layout will display both long and short cardholder names in a presentable manner.

Select the item below that you require further detail on:

- ***Adding Reasons for printing*** (on page 47-57)
- ***Printing and/or Encoding a card from a cardholder*** (on page 47-58)
- ***Encoding MIFARE cards to operate on multiple Command Centre sites*** (on page 47-63)

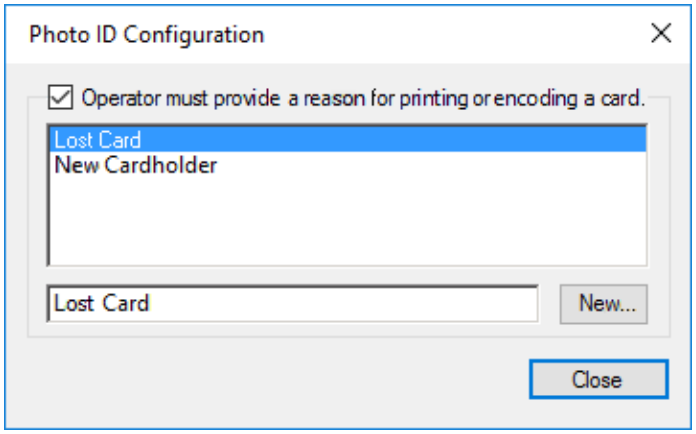
Adding Reasons for printing

Introduction

This procedure enables an operator with the "Edit Site" operator privilege in the root division to manage a list of reasons for printing a card.

Procedure

1. Click **Configure** from the menu bar, then **Photo ID**.
   The Photo ID Configuration window displays.



2. Check the **Operator must provide a reason for printing or encoding a card** box, if required.
3. Click the **New...** button, and type in your reason for printing a card.
4. Repeat Step 3 for each additional reason.
5. Click the **Close** button.

Result

A list of 'Reasons for Printing' cards is created.

Hints

Editing a Reason for Printing

1. Highlight the reason you wish to edit.
2. Edit as required and click the Close button.

Deleting a Reason for Printing

1. Highlight the reason you wish to delete.
2. Press the **Delete** key on your keyboard.
   Note: You are not asked for confirmation. The reason is deleted when you press **Delete**.
3. Click the Close button.

Printing and/or Encoding a card from a cardholder

Introduction

This procedure enables an operator to select a cardholder and either:
- print a card,
- encode a card, or
- print and encode a card.

You require either the "Print/Preview & Encode Card" or "Allows Re-Printing and Re-Encoding" operator privilege to view/edit a card, regardless of the card type setting. To print/preview and/or encode cards you must be in the same division as the Card Type of the card for the cardholder selected.

Operators with "View PINs" privilege in a division can view System Generated PINs assigned to cardholders. Whether this privilege works for User Defined PINs is controlled by a setting in the Server Properties, (i.e. the **Store PINs for later viewing** option on the **Card Security** tab), which controls whether the PIN is actually stored and encrypted for later decrypting and display.

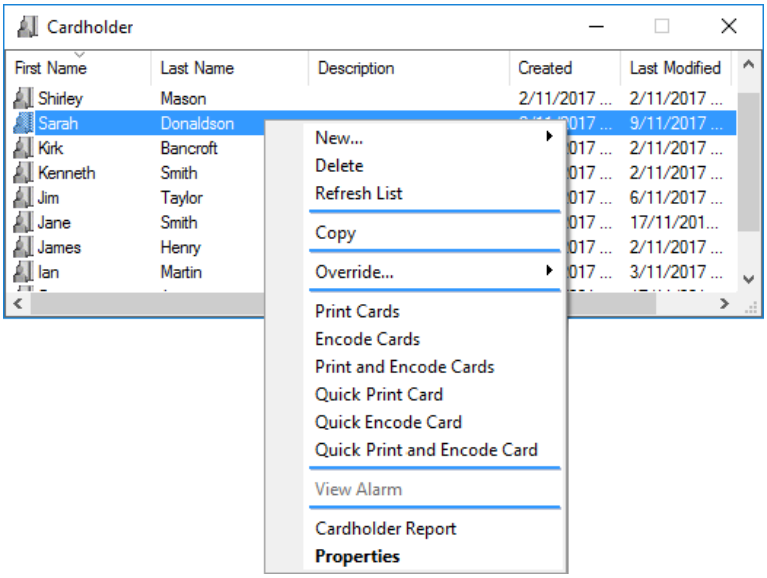
Note: If you are going to be encoding Morpho cards you do not need to have the Facility Code in the license file. However, if you are going to be encoding both Morpho **AND** Gallagher data, the Facility Code will need to be in the license file.

Procedure

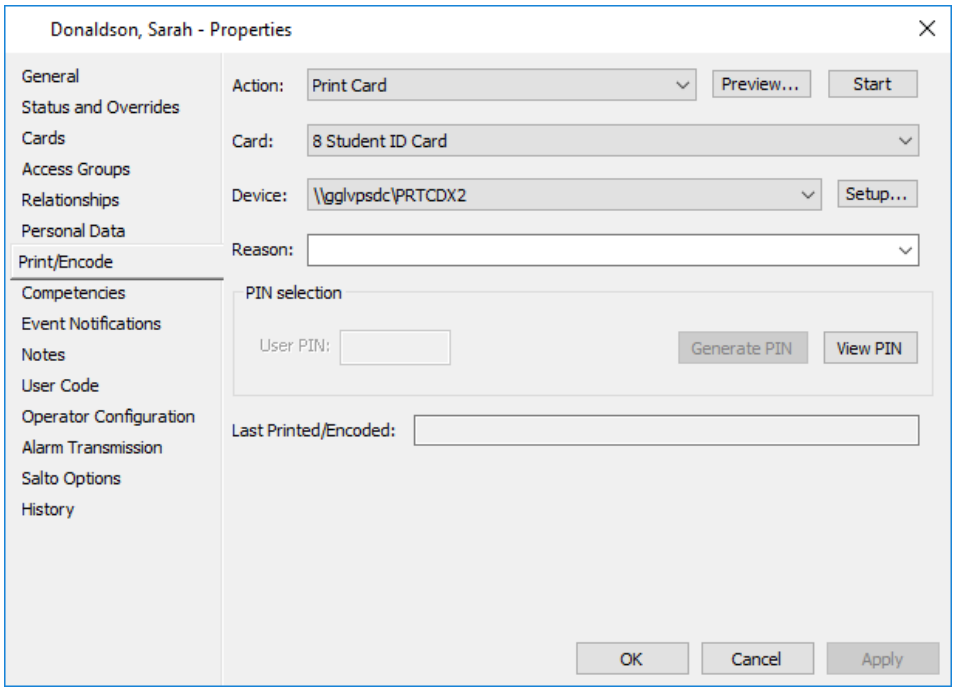
1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
   Note: Alternatively, you can locate the Cardholder by using the Find Tool. Refer to ***Find Tool*** (on page 41-1) for further detail.
2. **Right click** on the required cardholder, and select the required option from the context menu:
   - **Print Cards**
   - **Encode Cards**
   - **Print and Encode Cards**
   - **Quick Print Card**
   - **Quick Encode Card**
   - **Quick Print and Encode Card**

   Notes:
   - The Print/Encode options will be disabled if the Cardholder does not have any cards issued to them.
   - The “quick” options for printing and/or encoding cards are there to help speed up the process, however for them to work effectively the following configuration needs to be in place first:
     - the “Reason for printing” is not configured as compulsory
     - that a card has already been printed so that a default printer is known, and
     - the cardholder only has one card

- If the card has previously been printed or encoded the relevant "quick" options will not be available, unless the Card Type has **Allow re-printing** or **Allow re-encoding** enabled. You will not be able to re-print/re-encode a card using a Card Type that does not allow re-printing/re-encoding, unless you have the "Allows Re-Printing and Re-Encoding" privilege, in which case using **Print** or **Encode** will prompt you to 'Proceed' or 'Cancel'. With re-encoding, if you have the "Edit Cardholder" privilege you are prompted to increase the Issue Level, and if you have both the "Edit Cardholder" and "Allows Re-Printing and Re-Encoding" privileges you can either increase the Issue Level or 'Proceed'.



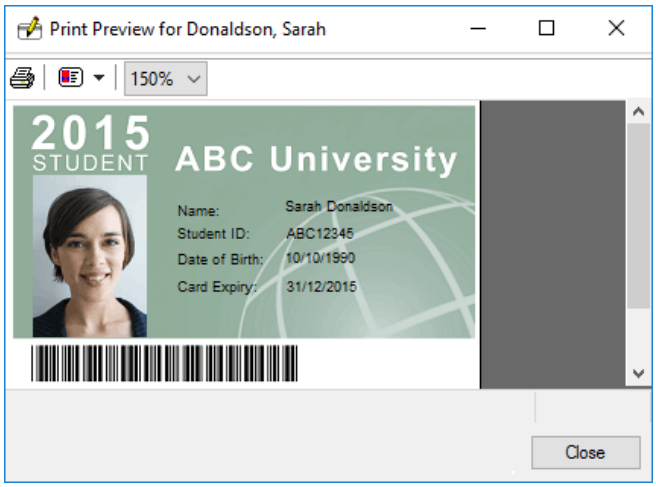
The **Print/Encode** tab of the Cardholders properties displays, showing the option you selected in the **Action** field.



3. If the Cardholder has several cards issued (via the **Cards** tab), select the card you want to preview from the **Card** drop-down list.

   Note: If you are not in the same division as the Card Type of the card, the following error message will display:
   "This card type is not available from the current division."

4. If you want to preview the card layout before printing/encoding it, click the **Preview** button.
   The **Print Preview** window displays.



   Note: If this card layout is double-sided, click the  icon to select the other side of the card so you can preview that also.

5. Is the card preview acceptable?

If...	then...
yes	click the **Close** button.
no	you will need to go to the Card Type to edit the layout. See ***Opening the Card Editor window*** (on page 47-14) for further details.

6. Select the required device to be used for card printing/encoding from the **Device** drop-down list of available printers/encoders.
   The system will remember this printer and default to it every time you preview/print a card until you change it again using the same procedure.

7. Click the **Setup...** button to alter the printer settings if necessary, then click the **OK** button.
   Note: If you are encoding a MIFARE card, using a serial MIFARE encoder, you need to select the port that the encoder is connected to. To do this:
   a) Click the **Setup...** button to display the Printer properties.
   b) Click the **Encoding** tab.
   c) Select the port the encoder is connected to from the drop-down list.

8. Select the appropriate reason for printing/encoding from the **Reason** drop-down list, or type your own reason into the text field. The reason selected will be logged in the event details.

Note: The **Start** button will be disabled until a reason is entered if the **Operator must provide a reason for printing or encoding a card** checkbox was checked on the Photo ID Configuration window when "Reasons for Printing" were configured.

9. The **PIN selection** section of the window will be enabled if you are encoding the card and PINs have not been disabled on the **PINs** tab of the Card Type. Either:
   - manually type a PIN number into the **User PIN** field, and then retype it into the **Confirm** field that displays.
     Note: As you enter the PIN it will display as a row of dots. The maximum PIN length is 8 digits. There is no mechanism to reduce the maximum size. Hence if a site sets minimum at 4, the user can enter PIN length anywhere from 4 to 8 digits, OR
   - click the **Generate PIN** button to automatically generate a random PIN.
     Note: Generated PINs will only display in the **User PIN** field while the window remains open. There will be no way of re-viewing the PIN number since the PIN itself is not stored. Generated PINs will be of length equal to the minimum PIN length set against the Card type.

   Note: The system prevents PINs with 3 consecutive or 3 repeating numbers from being either manually entered or automatically generated.
10. To view or hide the PIN click the **View PIN** / **Hide PIN** button.
    If you click the **View PIN** button, the User PIN displays and an event is logged to say you viewed PINs.
    By clicking the **Hide PIN** button, the PIN number disappears again.

    Note: If the PIN has not been stored and encrypted (via the setting in the Server Properties), the following dialog will display instead of the User PIN: *"The PIN for this card is not stored in a retrievable form."*
11. Click the **Start** button.
    Note: If this card has already been printed/encoded, the message *"The selected card details have already been [printed/encoded]."* displays. In addition to this:

If cards of this type...	the message will also say...
have **not** been configured to allow them to be re-printed and/or re-encoded,	*"Would you like to increase the issue level?".* Clicking the **Yes** button increases the issue level by 1.
have been configured to allow them to be re-printed and/or re-encoded, and you have the "Allow Re-Printing and Re-Encoding" operator privilege,	*"Would you like to proceed anyway?".* Clicking the **Yes** button re-prints and/or re-encodes the card with the same issue level.

Result

The result will depend on the option chosen at Step 3, as follows:

Option	The card...
Print Cards	prints to the default printer.
Encode Cards	is encoded by the default printer.
Print and Encode Cards	is encoded and prints to the default printer.

Encoding MIFARE cards to operate on multiple Command Centre sites

Introduction

A site may wish to grant access to MIFARE cards, (i.e. MIFARE Classic, MIFARE Plus and DESFire cards only) that are being used on another (third party) Command Centre site. There are three ways to achieve this:

- By reading the cards unique id (CSN) if the reader is configured to do so. Refer to the 'Use MIFARE Serial Number as Card Data' section, at Step 9 of the Creating Readers procedure.
- If the default MIFARE Plus/DESFire key seed is used by both sites, then it is possible to create a Card Type with the third parties Facility Code as per existing functionality. In this case it is possible to enrol a third-party card onto a site without creating a new card application.
- If the third-party site uses a unique key seed, the local site will need to encode their own data onto a sector on the third-party cards. This requires the third-party cards to have a spare sector available. In addition, the local Command Centre system must have the appropriate key(s) configured to enable encoding of the sector on the third-party card.

Notes:

- A document providing further detail on MIFARE mulitple applications (**Sharing MIFARE Classic and Plus cards between sites.pdf**) is located in the **`'Documentation'`** directory of the Command Centre installation files.
- Some higher security sites may be unwilling to share the Card Master Key (CMK) with another site. This would cause problems for sites using DESFire cards if the CMK is required for encoding. For further detail on the process, refer to **Sharing MIFARE DESFire cards between sites.pdf** located in the **`'Documentation'`** directory of the Command Centre installation files.

Batch Printing and/or Encoding

Introduction

Operators can set up a batch printing/encoding job for sending to a suitable combined printing and encoding device based on:

- A Card Type plus a range of Card Numbers (**Bureau Batch Job**)
- A selection of cardholders plus a given Card Type(s) (**Cardholder Batch Job**)

Note: The MIFARE USB encoder is supported.

Operator Privileges

Different operator privileges are required for the two types of batch jobs, as follows:

- To perform a **Bureau Batch Job** for a Card Type, the Card Type must belong to a division for which you have the "Bureau Batch Printing/ Encoding" operator privilege.
- To perform a **Cardholder Batch Job** for a selection of cardholders, the cardholders should all belong to a division for which you have the "Print/Preview & Encode Card" operator privilege. If the selection contains any cardholders belonging to another division, then the Batch Job will proceed but it will exclude these out-of-division cardholders.

Procedures

Before a Bureau Batch Job can be run, a Card Type needs to be configured so it can be used for Bureau Printing/Encoding. See ***Setting a Card Type for Bureau Printing/Encoding*** (on page 47-65) next for the procedure.

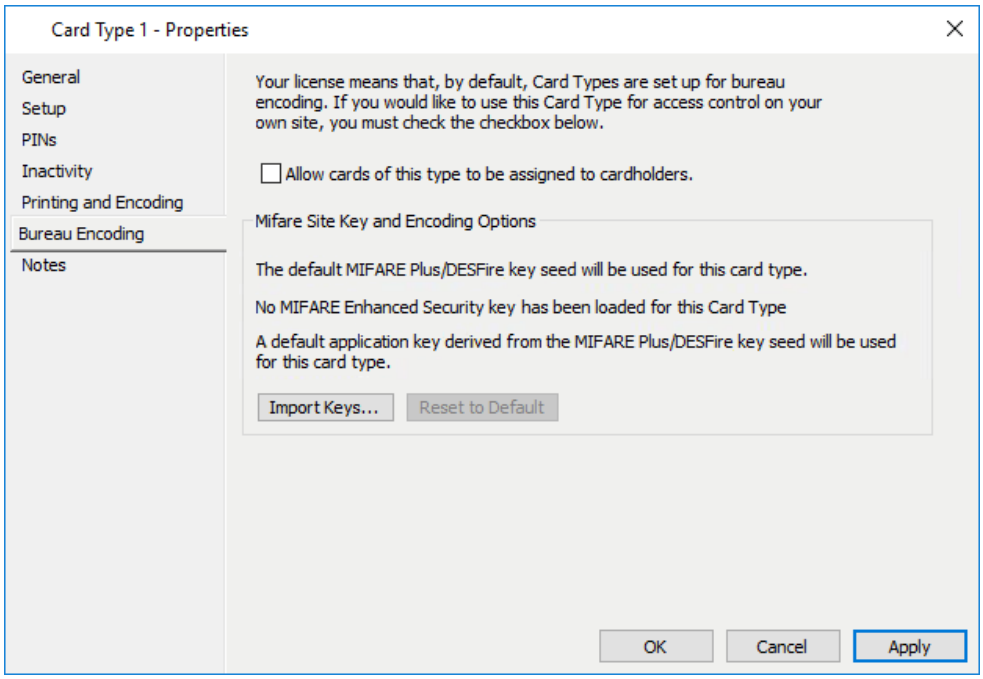
The procedure for performing a Batch Job has been split into two separate procedures for the two different types of Batch Jobs, (i.e. Bureau and Cardholder).
IMPORTANT: The encoder remembers the last cards serial number that it read or encoded. Therefore, if you set up a job and then cancel it without encoding any data onto the card, it records that cards serial number as being the last one and will not encode it again. In this situation you need to encode a different card first, then put the other card back on the encoder to encode it.

- ***Setting a Card Type for Bureau Printing/Encoding*** (on page 47-65)
- ***Performing a Bureau Batch Job*** (on page 47-67)
- ***Performing a Cardholder Batch Job*** (on page 47-70)

Setting a Card Type for Bureau Printing/Encoding

The main purpose of creating Card Types is for access control, however Card Types can also be created for encoding cards for other sites. This procedure describes how to configure a Card Type for Bureau Printing/Encoding.

1. Perform Steps 1 - 12 of the ***Setting up Card Types*** (on page 7-2) procedure and then go to Step 2 of this procedure.
2. Click the **Bureau Encoding** tab.
   Note: This tab will only appear if your site is licensed for Bureau Printing/Encoding.



3. Do you want this Card Type to be used for normal access control as well as Bureau Printing/Encoding?

If...	then...
yes	check the **Allow cards of this card type to be assigned to cardholders** checkbox. Cards of this Card Type will be able to be assigned to cardholders and used for normal access control, as well as being available for Bureau Printing/Encoding. **Note:** By clicking the **Apply** button now, the 'MIFARE Site Key' section disappears from this screen.
no	leave the **Allow cards of this card type to be assigned to cardholders** checkbox unchecked. This Card Type will be able to be used for Bureau Printing/Encoding only.

4. Is your site Bureau Encoding MIFARE cards?

If...	then...
no	go to Step 5.
yes	**a)** In the **MIFARE Site Key and Encoding Options** section, click the **Import Keys…** button. An 'Open File' dialog displays. **b)** Path your way to the appropriate MIFARE key file (that was configured on the **Card Security** tab of the Server Properties), and click the **Open** button. An 'Enter password' dialog displays. **Note:** If the file selected does not contain exported MIFARE keys, then the error message *"The file selected does not contain valid MIFARE site key data"* displays instead of the 'Enter password' dialog. **c)** Enter the password that was set for the MIFARE keys on the **Card Security** tab of the Server Properties, and click the **OK** button. **d)** Click the **OK** button. The selected file is imported and the encrypted MIFARE key within the file is loaded into memory. The message changes to: - *"The MIFARE Plus/DESFire key seed for this Card Type will be changed upon applying changes"*, AND/OR - *"The MIFARE Enhanced key for this Card Type will be changed upon applying changes".* **e)** Click the **Apply** button to send the change to the server. The message changes again to: - "A MIFARE Plus/DESFire key seed has been loaded for this Card Type", AND/OR - "A MIFARE Enhanced key has been loaded for this Card Type".

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.

   Note:
   If you decide that you do want this Card Type to be available for access control on your own site, you will need to delete this Card Type and start the procedure again, as it is not possible to re-enable the fields on this screen once they have been saved.

Performing a Bureau Batch Job

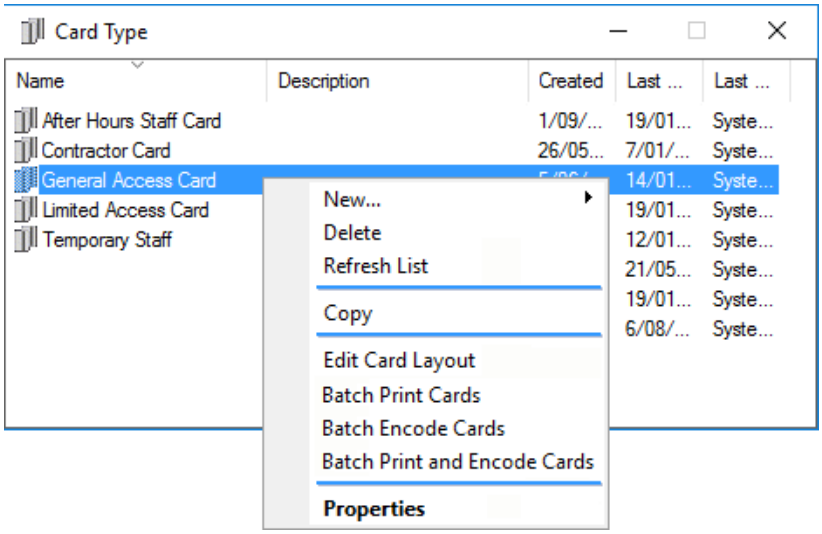
Note: Personal Data Fields (PDFs), First Names and Last Names should not be put on card layouts that will be used for bureau printing/encoding. The following items can be included:

- Text or barcode fields linked to a card number
- Issue level and expiry date
- Manually entered information on the card layout.

There are some exclusions however, as listed below:

- A Text Object or Barcode Object that contains First Name, Last Name or PDF link fields (Note that Card Number is allowed)
- Image Object field linked to a PDF
- Morpho object whose properties say "Card Number + Biometrics" or "Card Number + Finger Vein"

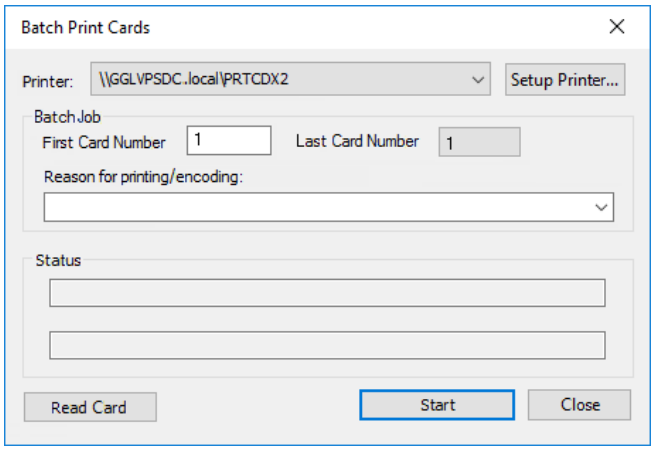
1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens (in grid view).
2. **Right click** on the required Card Type.



3. Select the appropriate option from the context menu:
   - **Batch Print Cards**
   - **Batch Encode Cards**
   - **Batch Print and Encode Cards**

   Note: These options are only enabled when **one** Card Type is selected, and only appear in the context menu when Facility Codes represented by the selected Card Type are licensed for Bureau Batch printing/ encoding.

   A Batch Job window displays.



Note: The title of this window will accurately reflect the option you selected, (i.e. 'Batch Print Cards', 'Batch Encode Cards' or 'Batch Print and Encode Cards').

4. Click the **Setup Printer…** button to alter the printer settings if necessary.
   Note:
   If you are encoding a MIFARE card with a printer connected via a serial port, you need to identify the port that the encoder is connected to. To do this:
   a) Click the **Setup Printer…** button to display the Printer properties.
   b) Click the **Encoding** tab.
   c) Select the port the encoder is connected to from the drop-down list.
5. Enter the **First Card Number** and **Last Card Number** of the cards to be printed/encoded.
   Note: You cannot print more cards than has already been set on the **Card Defaults** tab of the Card Type properties.
6. The **First Card Number** defaults to either:
   - what has been configured on the **Card Defaults** tab of the Card Type properties, or
   - if a Bureau Batch Job has already been performed previously for this Card Type, the last number used is remembered and it will be the next number.

   If required, change the card number to start at in the **First Card Number** field.
7. Select the appropriate **Reason for printing/encoding** from the drop-down list, or type your own reason into the text field. The reason selected will be logged in the event details.
   Notes:

   - The **Start** button will be disabled until a reason is entered if the **Operator must provide a reason for printing or encoding a card** checkbox was checked on the Photo ID Configuration window when "Reasons for Printing" were configured.

- The **Read Card** button allows you to read a newly encoded card to verify the contents of this encoding. When clicked, the **Read MIFARE Card** dialog appears which uses the custom keys used to encode the cards when attempting to re-read the data on the card.

8. Click the **Start** button.
   The Status bar indicates the progress of the batch job, identifying the completed card count and the total card count, along with the card number of the card currently being printed.

   Note:
   While a batch job is in progress the **Start** button is replaced by **Pause** and the **Close** button is replaced by **Cancel**. If a problem is encountered with a particular card(s), an error message displays and an additional **Skip Card** button appears, allowing you to ignore any card that causes the Batch Job to fail.

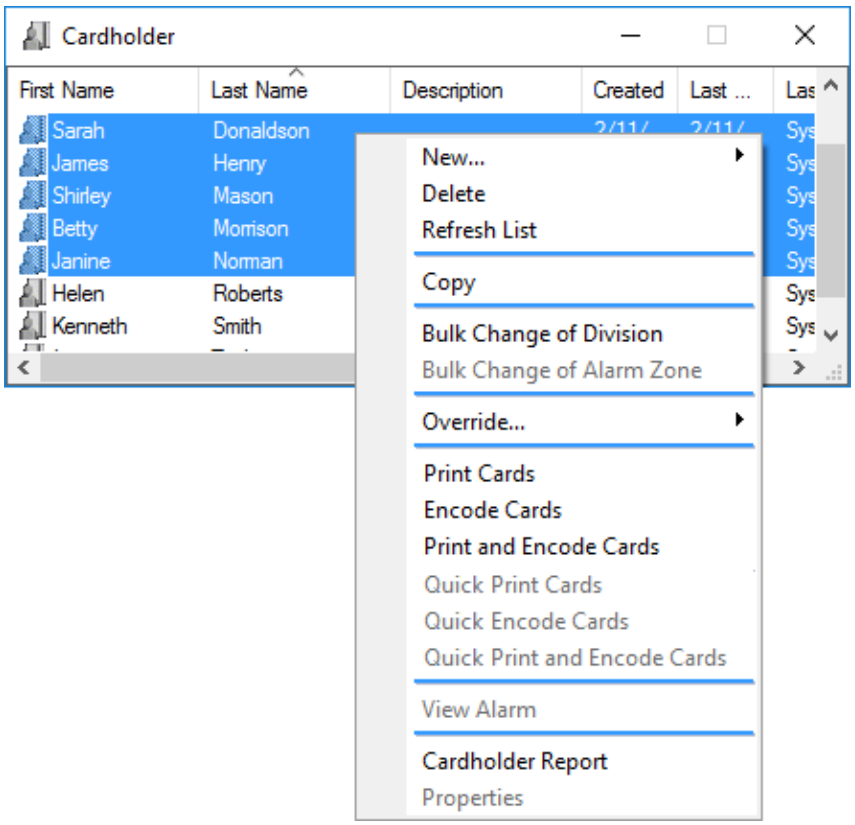
   The **Cancel** button allows the Batch Job to be stopped and the Batch Job window returns to its original state. The **Continue** button allows you to restart a paused Batch Job, (e.g. a Batch Job could pause due to the card hopper being empty).

Performing a Cardholder Batch Job

1. Click **Manage** from the menu bar.
2. Either:
   - Click **Cardholders**.
     The **Cardholder** List Window opens (in grid view).

   OR

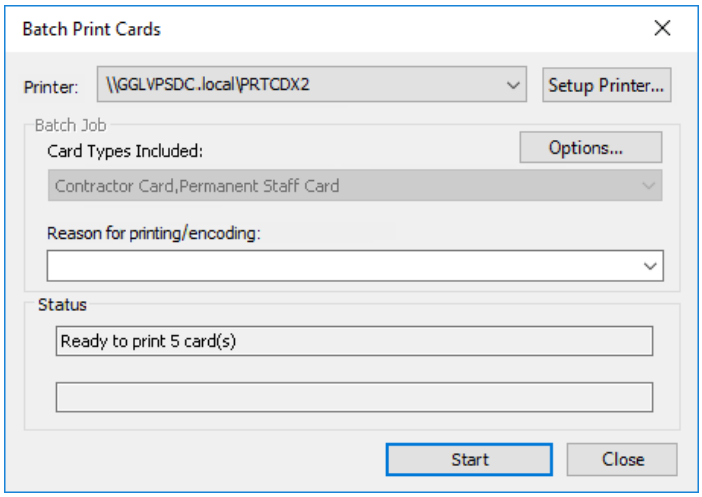
   - Click **Access Groups**.
     The **Access Group** List Window opens (in tree view).
3. Select the required Cardholders or Access Groups, and **right click**.



4. Select the required option from the context menu:
   - **Print Cards**
   - **Encode Cards**
   - **Print and Encode Cards**

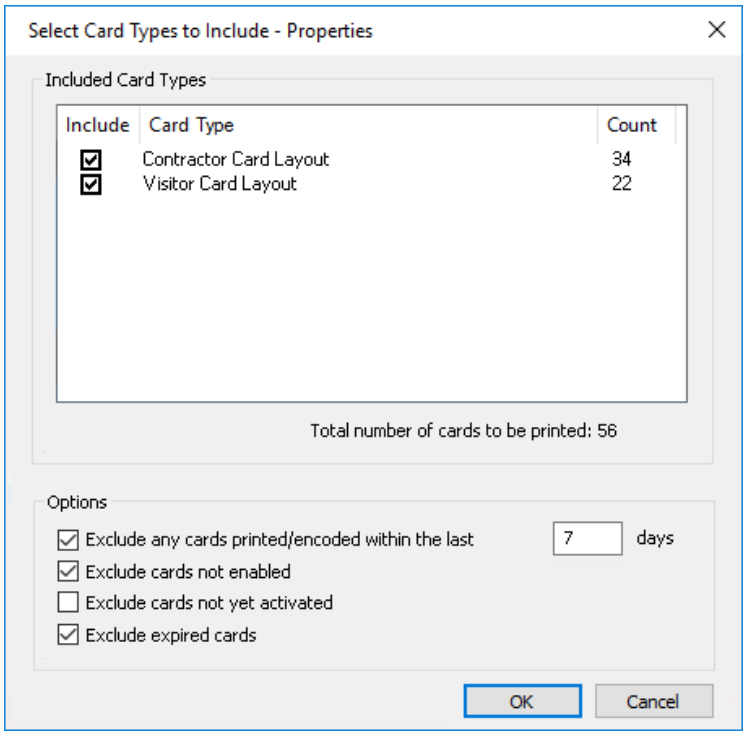
   Note:
   If the Batch Job includes any carhdolders that you do not have the "Print/Preview & Encode Card" operator privilege for, then a message will display indicating that they will be excluded.

   A Batch Job window displays.



Note: The title of this window will reflect the option you selected, preceded by the word 'Batch', (i.e. 'Batch Print Cards', 'Batch Encode Cards' or 'Batch Print and Encode Cards').

5. Click the **Setup Printer…** button to alter the printer settings if necessary.
   Note:
   If you are encoding a MIFARE card with a printer connected via a serial port, you need to identify the port that the encoder is connected to. To do this:
   a) Click the **Setup Printer…** button to display the Printer properties.
   b) Click the **Encoding** tab.
   c) Select the port the encoder is connected to from the drop-down list.
6. Click the **Options…** button.
   The **Select Card Types to Include** window displays to allow you to choose which Card Types to include in the batch printing/encoding job.



This window lists the unique Card Types represented by the current Cardholder selection. Each Card Type listed shows how many cards of that type will be printed if the Card Type is included.

7. Select which Card Types to include by ensuring the ☑ tick-box is checked for the required Card Types.
   Note:
   There may be Card Types listed that are unticked by default, and you are unable to select them. This occurs when your cardholder selection includes cardholders with a Card Type that is not licensed for encoding and you have chosen a Batch option that includes encoding.
8. Tick the appropriate checkboxes for the Exclude options you require.
   Notes:
   - The **Exclude recently printed cards** option (the first option) does not take into consideration any cards printed/encoded before the installation of the version that provides it.

     By turning this option ON (checked):
     - you can run the same batch job twice in immediate succession while ensuring that no duplicate cards are printed, (e.g. if you cancel part way through a batch job, or the job doesn't complete).
     - you can run two different batch jobs based on different selections without needing to worry about whether any cardholders appear in both selections, (e.g. cardholders that appear in more than one Access Group will not have duplicate cards printed/encoded).
   - Turning an **Exclude** option OFF (unchecked), does not necessarily mean that cards identified by that option are to be included. They will only be included if no other **Excluded** option dictates that they will be excluded.
   - The options selected are stored against the operator so that next time they do a Batch print/encode their previous selections are remembered.
9. Click the **OK** button.
10. Select the appropriate **Reason for printing/encoding** from the drop-down list, or type your own reason into the text field. The reason selected will be logged in the event details.
    Note:
    The **Start** button will be disabled until a reason is entered if the **Operator must provide a reason for printing or encoding a card** checkbox was checked on the Photo ID Configuration window when "Reasons for Printing" were configured.
11. Click the **Start** button.
    The Status bar indicates the progress of the batch job, identifying the completed card count and the total card count, along with the cardholders' name of the card currently being printed.

Once completed, the "Last Printed/Encoded" field on the **Cards** tab for each of the cardholders properties is updated.
The issue level and expiry settings are taken from the cardholder being printed/encoded.

Note:
While a batch job is in progress the **Start** button is replaced by **Pause** and the **Close** button is replaced by **Cancel**. If a problem is encountered with a particular card(s), an error message displays and an additional **Skip Card** button appears, allowing you to ignore any card that causes the Batch Job to fail.

The **Cancel** button allows the Batch Job to be stopped and the Batch Job window returns to its original state. The **Continue** button allows you to restart a paused Batch Job, (e.g. a Batch Job could pause due to the card hopper being empty).

Chapter 48: Perimeter Fence Controllers

Introduction

Command Centre allows for full configuration, control and monitoring of your perimeter fence system. Command Centre allows for the connection of the following Fence Controllers:

- Gallagher F31 and F32 Fence Controllers
- Gallagher F41 and F42 Fence Controllers
- Gallagher F51 and F52 Fence Controllers
- Gallagher F61 and F62 Fence Controllers
- Gallagher F22 Fence Controllers

Licensing

The use of Fence Controllers with Command Centre is a licensable feature. The total number of Fence Controllers in a system is governed by a single license file, (i.e. the license file specifies the total number of Fence Controllers that can be configured in Command Centre), as follows:

```
[Limits]
Fence Controllers=<nn>
Fence Zones=<nn>
```

FreeRTOS: The Gallagher F3x, F4x, F5x, F6x and F22 Fence Controllers use the real-time operating system FreeRTOSV6.0.4. This source code is available from the website: ***http://www.freertos.org/*** (***http://www.freertos.org/***)

Note: While you can have equipment configured across multiple Gallagher Controllers, it is not recommended as this may result in performance issues.

This chapter describes how to configure and monitor your perimeter fence system. This chapter covers the following topics:

- ***Creating a Fence Zone*** (on page 48-2)
- ***Assigning a Fence Zone to a Terminal*** (on page 48-6)
- ***Configuring an F3x/F4x/F5x/F6x Fence Controller*** (on page 48-9)
- ***Configuring an F22 Fence Controller*** (on page 48-19)
- ***Monitoring Fence Zone Status*** (on page 48-27)
- ***Monitoring Fence Controller Status*** (on page 48-28)
- ***Monitoring Fence Alarms and Events*** (on page 48-29)
- ***Overriding a scheduled Fence Zone state*** (on page 48-30)
- ***Overriding a Fence Controller*** (on page 48-32)
- ***Creating a Voltage Report*** (on page 48-34)
- ***Creating a Temperature Report*** (on page 48-36)
- ***Using Service mode*** (on page 48-38)
- ***Using HVplus mode*** (on page 48-40)

Creating a Fence Zone

Introduction

A Fence Zone is a section of perimeter fence (up to 300m length) which is assigned to a Fence Controller in Command Centre. Fence Zones can only be associated with one Alarm Zone, however each Alarm Zone can be associated with any number of Fence Zones belonging to any number of Fence Controllers. This procedure describes how to create a Fence Zone in Command Centre.

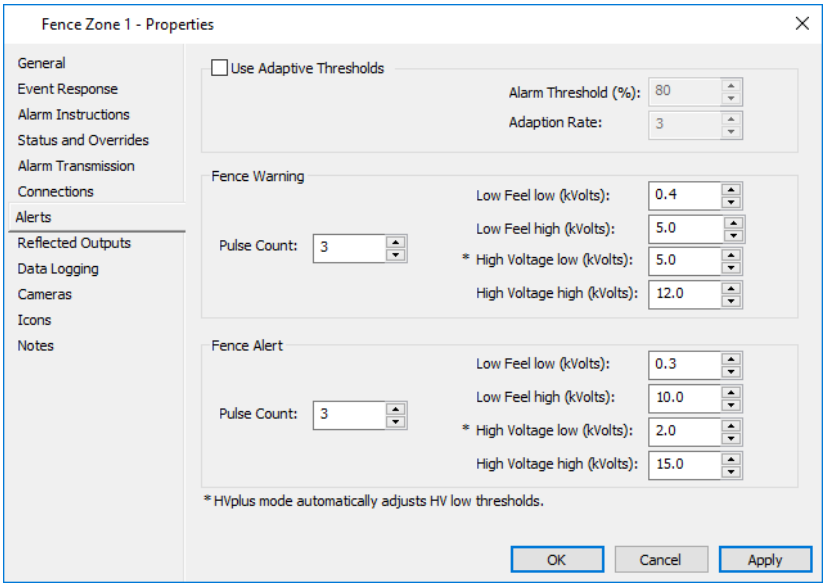
Before you begin

Before you begin this procedure, you need to be in the same or parent Division of the Command Centre items mentioned, and have the "Edit Site" operator privilege to perform this procedure.

Procedure

Creating a new Fence Zone

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Fence Zone**.
   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).
   Important: Fence Zones are energized in response to the state of the Alarm Zone they are associated with on the **Event Response** tab. Configuring a Fence Zone with an Alarm Zone that is not disarmed could unexpectedly energize the fence.
   Notes:
   - Each Fence Zone can only be associated with one Alarm Zone. However, each Alarm Zone can be associated with any number of Fence Zones belonging to any number of Fence Controllers.
   - If a Fence Zone is not associated with an Alarm Zone, the Fence Zone will only arm when overridden and will not log any events.
   - If a Fence Zone is assigned to an F3x, F4x, F5x, F6x or F22 Fence Controller, the Alarm Zone will control the HV/LF mode for this Fence Zone.
5. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
6. Click the **Alerts** tab.



7. Corrosion on the fence can cause the voltage to drop. The **Use Adaptive Thresholds** feature allows voltage alarm thresholds to adapt to their environment and prevent false alarms. Effectively, the Fence Controller will not report alarms that result in a gradual drop in voltage.
   Note: This feature will not work on F22 Fence Controllers.
   If required, check the **Use Adaptive Thresholds** checkbox.
   The **Alarm Threshold** and **Adaption Rate** options become enabled.
8. Adjust the **Alarm Threshold** percentage (Range = 0 - 100%) and **Adaption Rate** (Range = '1 - Slowest' to'9 - Fastest') as required.
   Notes:
   - An alarm will be generated when the return voltage drops below the adapted threshold. The threshold then adapts to the new level and when it does the alarm will be restored.
   - A Voltage Report run for this Fence Zone can show the adapted threshold compared to the actual voltage. Installers may use this report to confirm that they have the adaptive threshold settings suitably configured, (e.g. if they still get false alarms they can increase the settings).
9. Configure as appropriate.

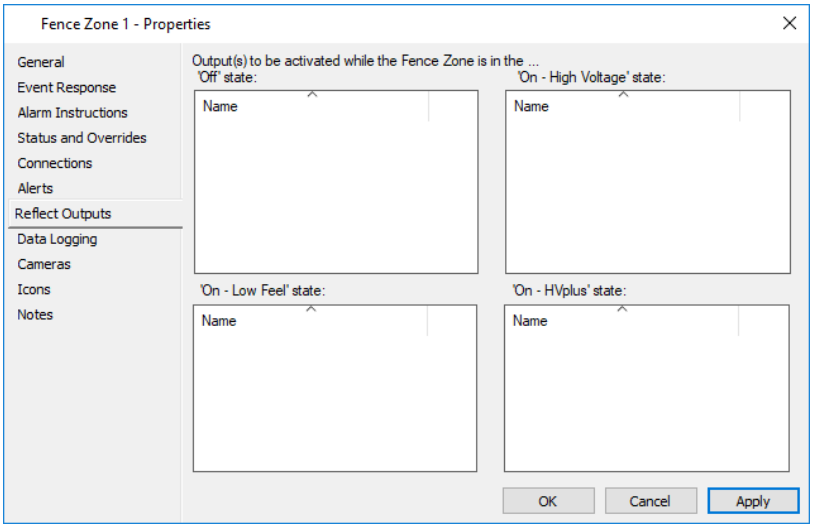
Field	Description
Fence Warning	When in Low Feel mode, if the Fence Controller reports a value less than the Low Feel low value or greater than the Low Feel high value, for three (default) consecutive pulses, a Fence Low Feel Warning is raised (Default = medium priority). When in High Voltage mode, if the Fence Controller reports a value less than the High Voltage low value or greater than the High Voltage high value, for three (default) consecutive pulses, a Fence Warning is raised (Default = medium priority).
Fence Alert	When in Low Feel mode, if the Fence Controller reports a value less than the Low Feel low value or greater than the Low Feel high value, for a period of three (default) consecutive pulses, a Fence Low Feel Alarm is raised (Default = very high priority). When in High Voltage mode, if the Fence Controller reports a value

Field	Description
	less than the High Voltage low value or greater than the High Voltage high value, for a period of three (default) consecutive pulses, a Fence Alarm is raised (Default = very high priority).

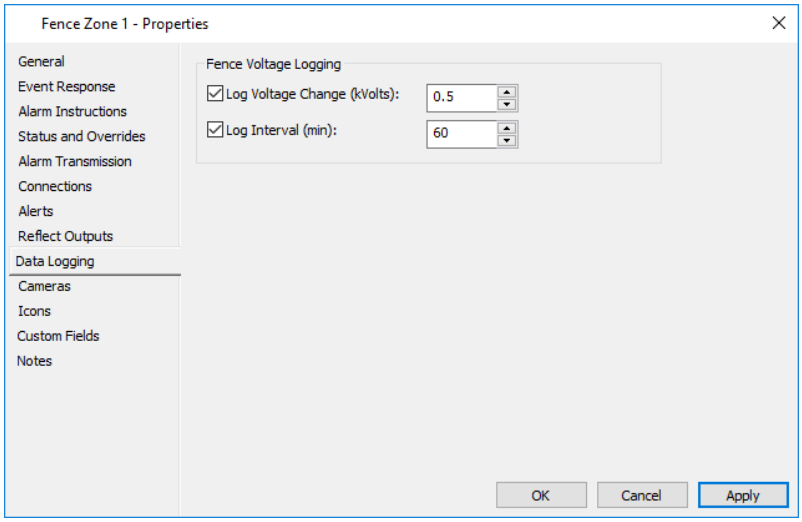
Notes:

- The **Low Feel low** and **Low Feel high** values are only applicable if the Fence Zone is assigned to an F31, F32, F41, F42 or F22 Fence Controller.
- The **Low Feel low** value must be less than or equal to the **Low Feel high** value (for both 'Fence Warning' and 'Fence Alert').
- The **High Voltage low** value must be less than or equal to the **High Voltage high** value (for both 'Fence Warning' and 'Fence Alert').
- The Fence Warning **High Voltage high** value must be greater than or equal to 12 kV and the Fence Alert **High Voltage high** value must be 15 kV when the Fence Zone is assigned to an F4X Fence Controller. The increase in values is due to the HVplus functionality of the F4X Fence Controller.
- If the Fence Zone is assigned to an F4X Fence Controller, the **High Voltage low** values will be automatically increased when HVplus mode is entered:
  If between 0 - 2.0 kV the value is increased 31%.
  If between 2.1 - 6.0 kV the value is increased 32%.
  If between 6.1 - 8.0 kV the value is increased 23%.
  If between 8.1 - 15.0 kV the value is increased 20%.
  Due to the automatic increase in values, a Fence Warning or Fence Alert may occur when the fence voltage is greater than the configured **High Voltage low** value.
  For example, if the configured **High Voltage low** value is 2.0 kV, when HVplus mode is entered, the value is automatically increased 31% to 2.6 kV. Hence a Fence Alert will occur when the voltage drops below 2.6 kV and not below the configured 2.0 kV value.

10. Click the **Reflect Outputs** tab.



11. Configure **Outputs** as required (drag and drop).
    Outputs turn on while in the Fence Zone state the outputs are placed in.
12. Click the **Data Logging** tab.



    This screen allows you to configure voltage logging for the Fence Zone. The events logged due to these settings will be used when a Voltage Report is run for this Fence Zone. Refer to ***Creating a Voltage Report*** (on page 48-34) for the procedure.
13. Configure the Data Log voltage change and/or time interval triggers as required.
14. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Fence Zone.
    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 Fence Zone.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
16. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Fence Zone.
    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 Fence Zone.
    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.

Result

A Fence Zone has been created.
Note: The Fence Zone is assigned to an F31, F32, F41, F42 or F22 Fence Controller. Once assigned to a Fence Controller, the following occurs:

- the Fence Zone will display within the Hardware window as a child of the Fence Controller, and
- on the **Connections** tab of the Fence Zone, the Fence Controller name will appear in the **Connected to** field.

Assigning a Fence Zone to a Terminal

Introduction

The Gallagher HBUS Terminal or HBUS Alarms Only Terminal can be used to monitor and control Fence Zones assigned to an F31, F32, F41, F42 or F22 Fence Controller.

A single Terminal can be used to monitor and control up to 50 Fence Zones.

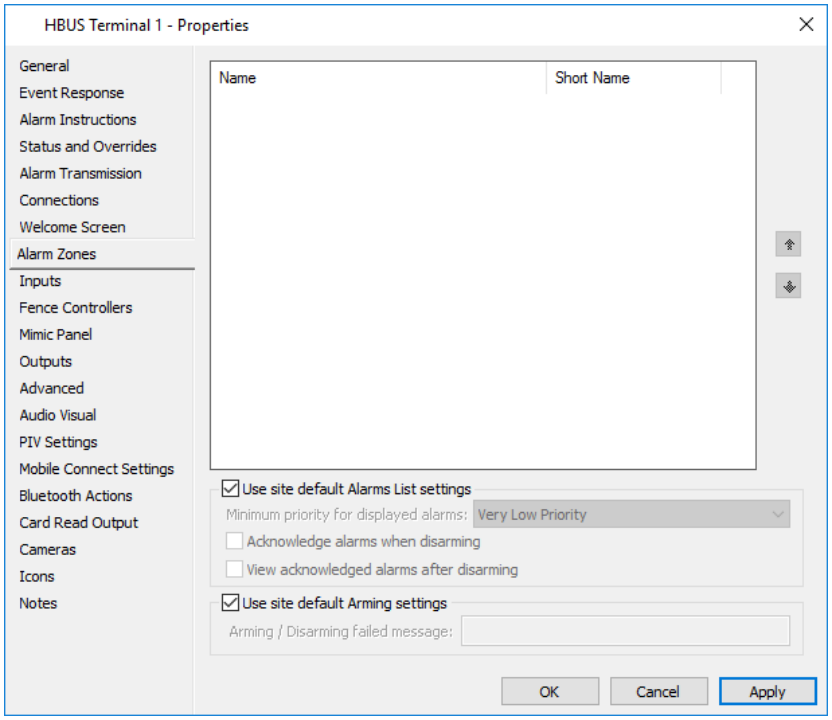
Before you begin

Before you begin this procedure:

- Ensure that the Fence Zone has already been assigned to a Fence Controller, which in turn has been assigned to a Gallagher Controller 6000 or 7000.(Fence Zones are assigned to Fence Controllers as part of the ***Configuring a Fence Controller*** procedure next.)
- You need to be in the same or parent Division of the Division holding all the items, and have the "Edit Site" operator privilege to perform this procedure.

Procedure

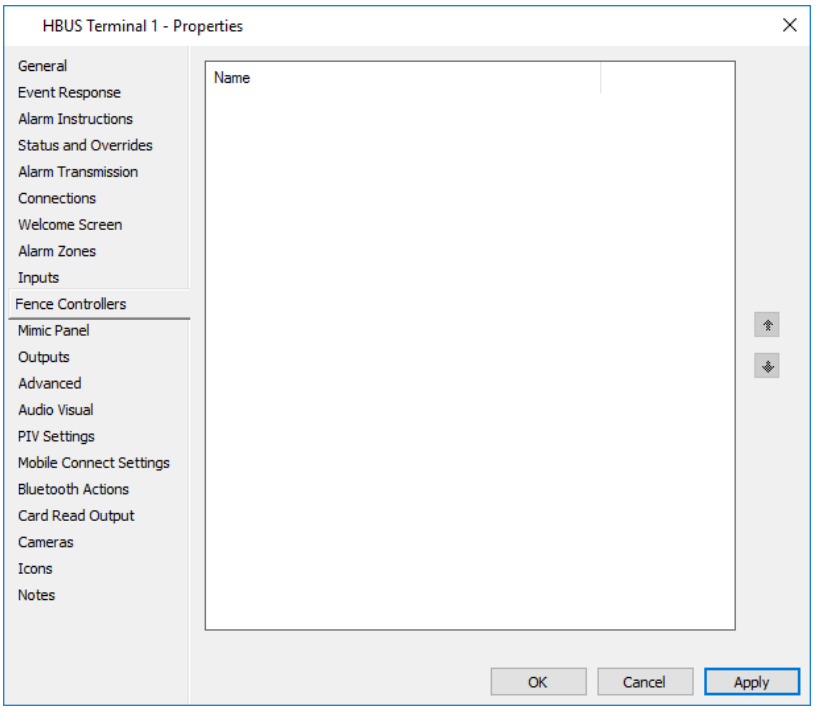
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Terminal you wish to assign a Fence Zone to.
3. **Right click** and select **Properties**.
4. Click the **Alarm Zones** tab.



5. Drag and drop the same Alarm Zone that is assigned to the Fence Zone (on the **Event Response** tab of the Fence Zones properties) into this grid.

   Note: The order you sort the Alarm Zones in here will be the order they appear in the terminal user interface.

6. Click the **Fence Controllers** tab so you can assign the Fence Controller (that has the assigned Fence Zones) to the terminal.



7. Drag and drop the F31, F32, F41, F42 or F22 Fence Controller that the Fence Zone is assigned to (on the **Devices** tab of the Fence Controller properties) into the grid. Go to Step 10.
   Note: The order you sort the Fence Controllers in here will be the order they appear in the terminal user interface.
8. 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 Fence Zone has been assigned to a Terminal.

Configuring an F3x/F4x/F5x/F6x Fence Controller

Introduction

An F3x, F4x, F5x or F6x Fence Controller can be operated in a networked mode, instead of stand-alone mode, by changing the Stand Alone/HBUS SW1 dipswitch 9 to ON and then connecting the Fence Controller via HBUS to a Controller 7000 or 6000 and Command Centre. In this configuration the Fence Controller's behaviour is configured and managed from Command Centre, replacing the Fence Controller's default stand-alone behaviour.

Within Command Centre up to 24 F3x, F4x, F5x, F6x or F22 Fence Controllers can be assigned to a single Gallagher Controller 7000 or 6000.

The difference between the Fence Controllers is shown below:

Fence Controller	Fence Channels	Inputs	Outputs	HV Sync	LV Sync	HVplus
F31	1	2	4	No	Yes	No
F32	2	3	5	Yes	Yes	No
F41	1	2	4	No	Yes	Yes
F42	2	3	5	Yes	Yes	Yes
F51	1	2	4	Yes	Yes	No
F52	2	3	5	Yes	Yes	No
F61	1	2	4	Yes	Yes	Yes (excl. EN variant)
F62	2	3	5	Yes	Yes	Yes (excl. EN variant)

This procedure describes how to create an F3x, F4x, F5x or F6x Fence Controller in Command Centre.

Before you begin

Before you begin this procedure:

- Ensure the following components have already been created:
  - a **Fence Zone**
    Refer to ***Creating a Fence Zone*** (on page 48-2)
  - a **Gallagher Controller 7000 or 6000**
    Refer to ***Creating Controllers*** (on page 21-2)
  - **Inputs and Outputs**
    Refer to ***Creating Inputs and Outputs*** (on page 21-33)
  - **Alarm Zones**
    Refer to ***Setting up Alarm Zones*** (on page 14-3)
- You need to be in the same or parent Division of the Command Centre items mentioned, and have the "Edit Site" operator privilege to perform this procedure.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**. The **Hardware** List Window opens (in tree view).

2. **Right click** and select **New...HBUS Devices** > **F31/32/41/42 Fence Controller** or **F5x/F6x Fence Controller**.
   Note: If **Fence Controller** is disabled in the context menu, this could be due to one of the following reasons:
   - the number of Fence Controllers already created has reached the limit as specified in the license, or
   - you do not have the privilege required to create Fence Controllers.

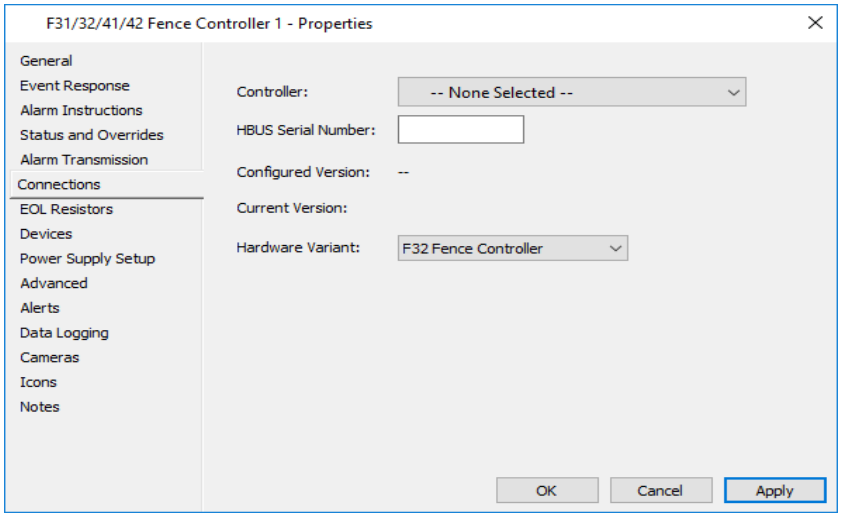
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
   Note: The Division must be the same as, or a parent of, the Division used for the new Fence Zone.
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).

   The Fence Controller needs to be placed in an Alarm Zone and have the Battery Alarms and Temperature Alarms settings configured to generate alarms for complete perimeter security.
   Note: It is possible to configure a "Pre-arm Timeout" (from 0-60 seconds) for Fence Controllers to ignore any alarms, via the **Alarm Warnings** tab of the Alarm Zone.
5. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
6. Click the **Status and Overrides** tab. **Notes:**
   - If a Fence Controller cover is removed, continuous tamper alarms will be generated. To prevent this from happening, tick the **Disable Tamper** checkbox.
   - The on-board optical tamper is re-calibrated:
     - 60 seconds after Service Mode SW1 dipswitch 1 has been changed from ON to OFF when the **Allow use of Service Mode for local control** checkbox is checked and the **Disable Tamper** checkbox remains unchecked. This allows time to replace the cover before re-calibration, or
     - 10 seconds after power up and the **Disable Tamper** checkbox remains unchecked, or
     - 10 seconds after a 'Reset' override has been performed and the **Disable Tamper** checkbox remains unchecked, or
     - 10 seconds after the **Disable Tamper** checkbox is unchecked.

     The Tamper LED located on the Fence Controller will enter a fast flash pattern that indicates the re-calibration countdown is in progress. Once the countdown timer for tamper re-calibration has started, if any SW1 dipswitch subsequently changes during the countdown period, the timer is restarted.
   - When a **'Reset'** override is performed, all inactive (historic) alarms shown on the Fence Controller are removed.

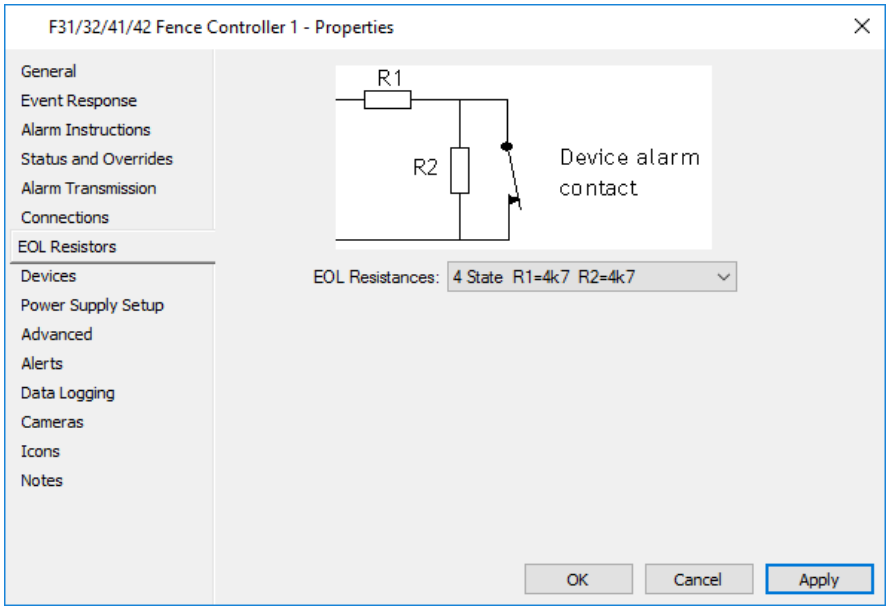
- When a **'Shunt'** override is performed Command Centre will stop communication to the Fence Controller. All Inputs and Outputs assigned to the Fence Controller will no longer respond to commands from Command Centre. It will remain this way until you 'Unshunt'. Alarms continue to be displayed on the Fence Controller.
- **'Initiate Battery Test' override:** Normally a battery test will only happen 24 hours after an energizer startup/reset. This override provides the ability to initiate a battery test immediately when needed, as long as at least one Fence Zone is operating.
- **'Reset LV Sync Secondaries' override:** When an energizer is removed or replaced, the Primary unit will continue expecting pulse acknowledgements from the previous Secondary. This causes the system to enter a 'sync-lost' state, preventing normal operation. Performing a 'Reset LV Sync Secondaries' override resolves this by removing any non-responsive Secondaries from the Primary's list and resyncing with active ones.
- The **Status and Overrides** tab displays the current battery voltage, the current temperature measured within the Fence Controller unit and the highest and lowest temperature recorded within the last 7 days.

7. Click the **Connections** tab.



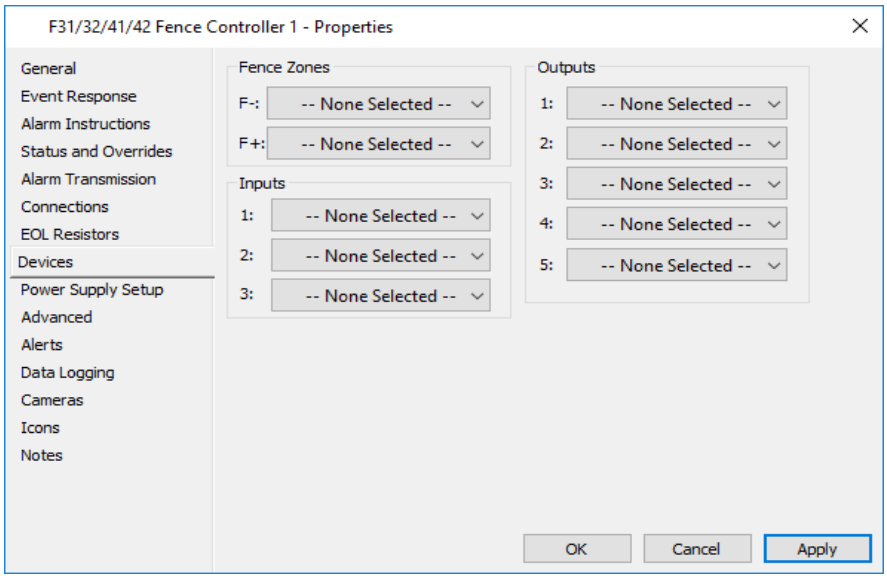
8. Select the Controller you want to assign this Fence Controller to, from the **Controller** drop-down list.
   Note: When an HBUS device is added to a Controller 7000 or 6000, it will appear on the **HBUS Devices** tab of the Controller. In this case, the **Controller** field will be pre-populated with that Controller name.
9. If not already present, enter the HBUS serial number (10 character hexadecimal string) into the **HBUS Serial Number** field.
   Note: The HBUS serial number is optional, however the Fence Controller will be considered as not properly configured unless one is entered.
10. If you click the **Apply** button, software version numbers display.
    The **Configured Version** is the version of the device software in the configured Controller 7000 or 6000 FTS file, (i.e. not the version of the Controller 7000 or 6000 software). The **Current Version** is the version of software as last reported by the Fence Controller itself.

11. Select the appropriate **Hardware Variant** from the drop-down list, (i.e. F3x, F4x, F5x or F6x Fence Controller).
12. Click the **EOL Resistors** tab.



This screen allows you to define the wiring and resistance values used on inputs that are connected to the Fence Controller.

13. Select the required resistor values from the drop-down list.
14. Click the **Devices** tab.



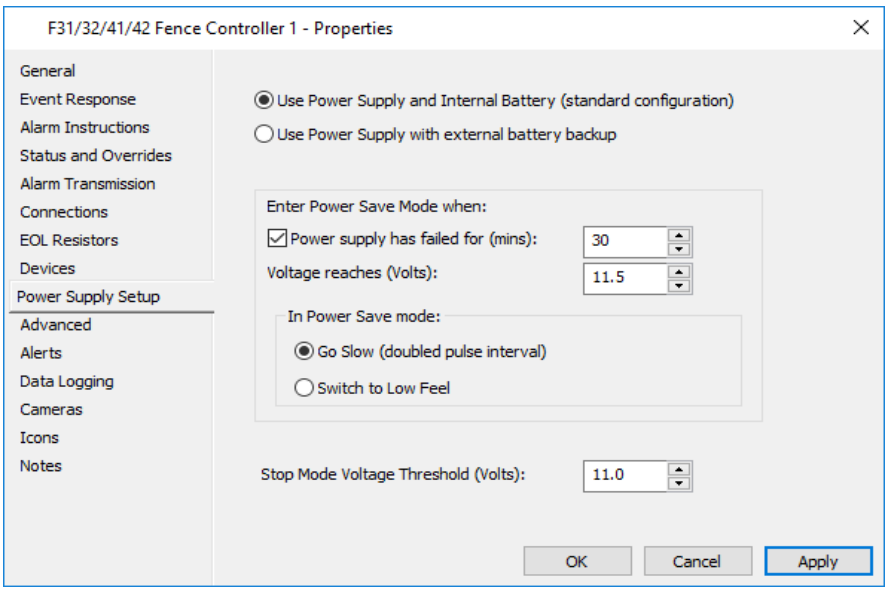
Note: The appearance of this screen may differ depending on the Fence Controller type selected.

15. Assign the appropriate Inputs, Outputs and Fence Zones to configure the Fence Controller.

Notes:

- Each Input, Output and Fence Zone can belong to only one Fence Controller.
- Fence Zones may or may not be connected to a physical fence.

16. Click the **Power Supply Setup** tab.



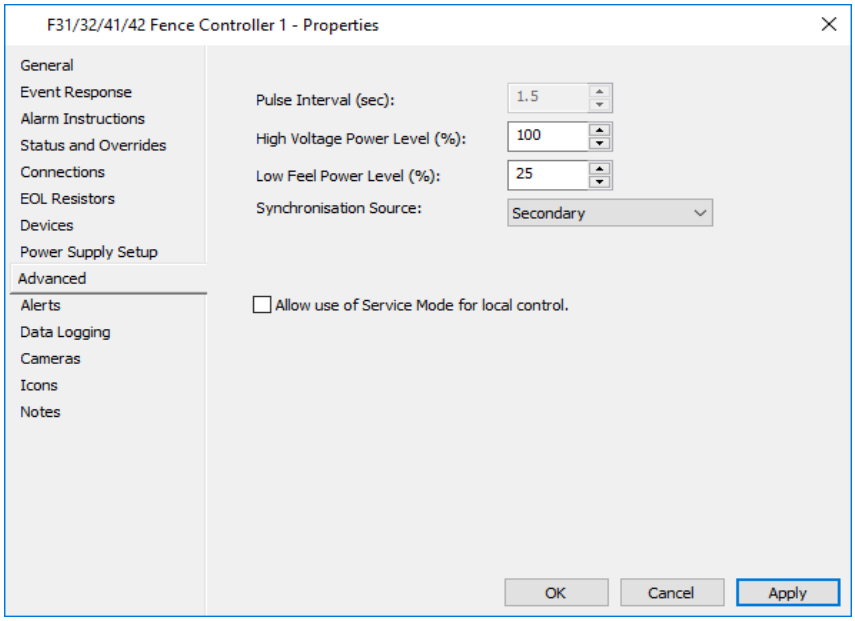
17. Click the appropriate radio button for the type of battery backup you want to use, (i.e. **Use Power Supply and Internal Battery (standard configuration)** or **Use Power Supply with external battery backup**).

    Note: When using an external battery backup, battery charging and testing is not supported, battery monitoring is supported. The **Power supply has failed for (mins)** option becomes disabled and Battery Alarms on the **Alerts** tab are disabled.

18. Configure as appropriate.

Field	Description
Enter Power Save Mode when	The Fence Controller will enter Power Save mode when: • the mains power has failed for a period of time greater than or equal to 30 minutes (default value), or • the mains power has failed and the battery voltage is less than or equal to 11.5 V (default value) for 7-10 seconds. **Note:** If the **Power supply has failed for (mins)** checkbox is un-ticked, the Fence Controller will continue to pulse as normal until the Power Save Voltage Threshold or Stop mode Voltage Threshold is reached.
In Power Save Mode	Select the appropriate behaviour when the Fence Controller enters Power Save mode. Either: • Go Slow (double pulse interval), or • Switch to Low Feel
Stop Mode Voltage Threshold (Volts)	The Fence Controller will enter Stop mode (cease producing pulses) when the battery voltage is less than or equal to 11.0 V (default value) for 7-10 seconds.

19. Click the **Advanced** tab.



Note: The appearance of this screen may differ depending on the Fence Controller type selected.

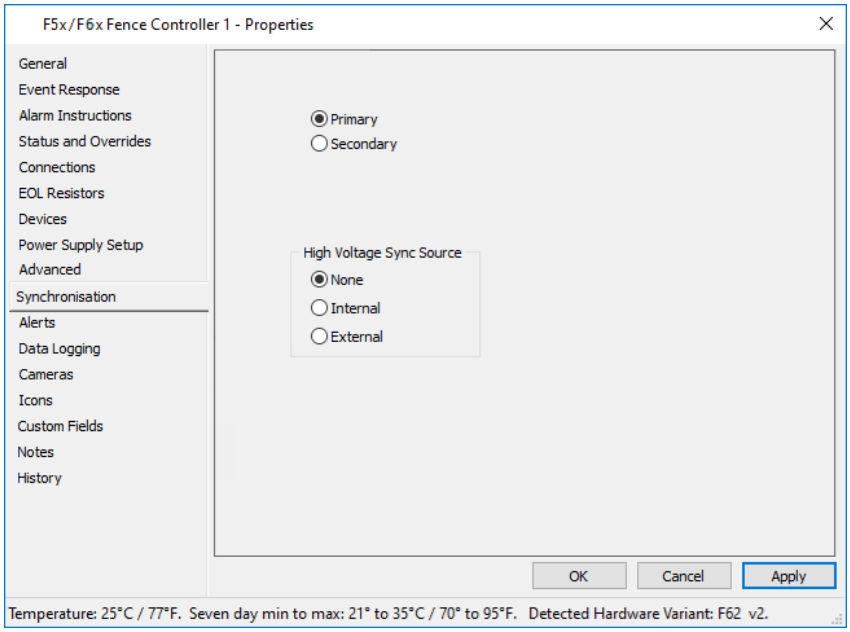
20. Configure as appropriate.

Field	Description
Pulse Interval (sec)	This is the pulse interval (period of time between pulses) for this Fence Controller. **Note:** If this Fence Controller has been configured as a secondary device the pulse interval will be set to that of the primary device.
High Voltage Power Level (%)	This is the percentage of high voltage power that will be delivered per pulse, by this Fence Controller (default = 100%). **Note:** An F41 or F4 Fence Controller in HVplus mode will be at 100% regardless of the value configured here. HVplus 100% = 10 kV.
Low Feel Power Level (%)	This is the percentage of low feel power that will be delivered per pulse, by this Fence Controller (default = 25%). The voltage chaser on the Fence Controller shows the measured return voltage delivered from the previous pulse, at or near its configured maximum.
Synchronisation Source	**Note:** This field is only applicable to F3x/4x Fence Controllers. For F5x/6x controllers, synchronisation is configured on the **Synchronisation** tab. Select the appropriate synchronisation source for this Fence Controller. If the Fence Controller is not synchronised to a primary device, the red synchronisation lost icon overlays the Fence Controller icon and a blue exclamation icon overlays the Fence Zone icons. **IMPORTANT:** If the F3x/4x Fence Controller is synced with an F5x/6x, the F3x/4x must be set as a secondary controller, with an F5x/6x as the primary. An F5x/6x will not sync from an F3x/4x primary controller.

21. Check the **Allow use of Service Mode for local control** checkbox if you want technicians to be able to use Service Mode SW1 dipswitch 1 for local arm/disarm control. For details about Service mode see ***Using Service mode*** (on page 48-38).
22. Are you configuring an F41/F42 Fence Controller?
    If **no**, go to the next step.
    If **yes**, deselect the **Enable HVplus Mode** checkbox if you do not want to use HVplus mode. For details about HVplus mode see ***Using HVplus mode*** (on page 48-40).
23. Are you configuring either an F5x or F6x Fence Controller?
    If **no**, go to the **Alerts** tab.
    If **yes**, go to the **Synchronisation** tab before continuing to the **Alerts** tab.
24. Click the **Synchronisation** tab and select 'Primary' or 'Secondary' as appropriate for this Fence Controller.
    Note: This tab only appears on the F5x/F6x properties.

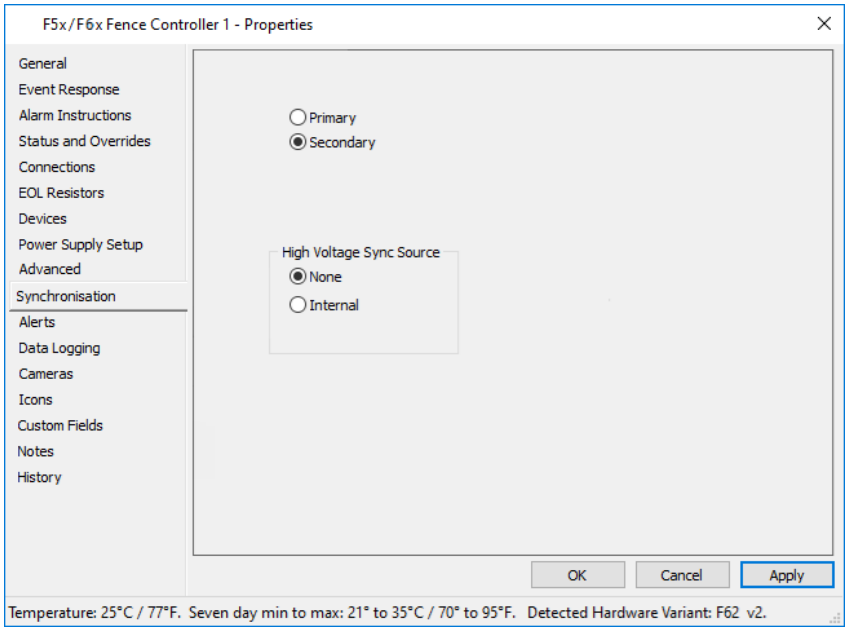
Option	Description
Primary	The Fence Controller that manages the LVSync bus and sends the PulseNow command to all Secondary devices connected.
Secondary	A Fence Controller on the LVSync bus that is managed by a Primary and pulses in response to a received PulseNow command.

25. If you select **Primary**, the Fence Controller will be assigned as the primary in the LV Sync Bus and will set the pulse timing for all connected secondaries.



Note: If a Fence Controller is removed, you can reinitialize the LV Sync bus by using the "Reset LV Sync Secondaries" override on the **Status and Overrides** tab. This action will automatically detect and register all connected Fence Controllers on the LV Sync bus.

26. If you select **Secondary**, the Fence Controller will be assigned as a secondary in the LV Sync Bus and will wait to receive the sync now command from the primary.



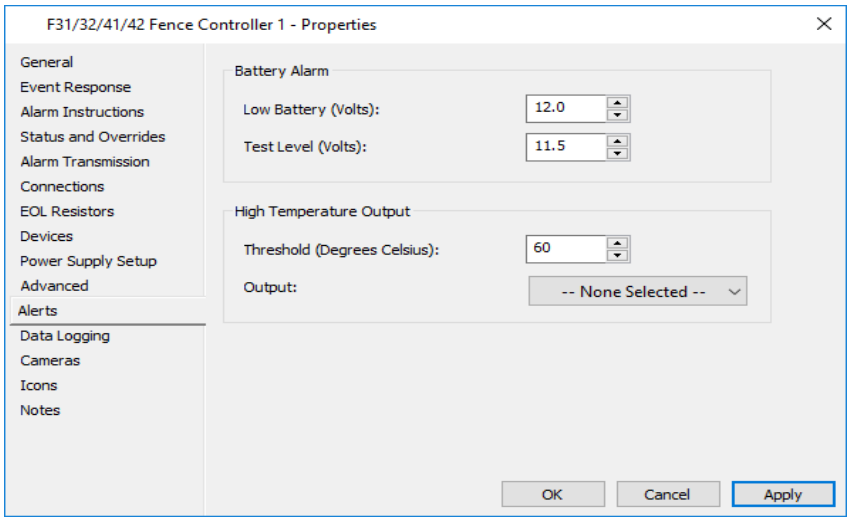
27. Select the appropriate High Voltage Sync Source:

Option	Description
None	No HV Sync source is connected. +ve channel is an output.
Internal	The HV Sync source is part of the same fence system, (i.e. synchronisation is mandatory). This is available on F52 and F62 Primaries, and Secondaries for bidirectional HV Sync.
External	This option only appears when the Fence Controller is set as **Primary**. It indicates the sync source is from a separate fence system, (e.g. synchronisation to a neighbouring Fence Controller is recommended but not mandatory).

IMPORTANT:

- If the F5x/6x Fence Controller is synced with an F3x/4x, an F5x/6x must be set as the primary controller. An F5x/6x will not sync from an F3x/4x primary controller.
- The maximum number of energisers connected to a primary F5x/6x Fence Controller is 100.

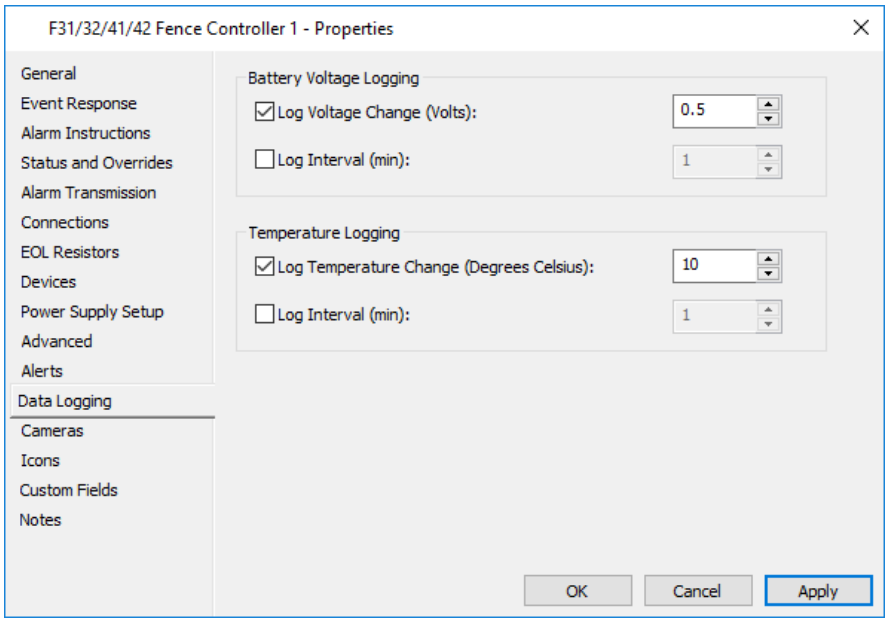
28. Click the **Alerts** tab.



29. Configure as appropriate.

Field	Description
Battery Alarm	If the battery voltage drops below the configured **Low Battery** level (Default = 12.0 V), an alarm is raised. This alarm is not reflected by the Battery icon on the Fence Controller. The Battery icon illuminates if the battery test has failed or a battery is not present. If the battery voltage drops below the configured **Test Level** (Default = 11.5 V) during the battery test, an alarm is raised. This alarm is reflected by the Battery icon on the Fence Controller. The **Test Level** can be used to change the value used when the Fence Controller is used in stand- alone mode. **Notes:** • The Fence Controller will automatically test the battery within 24 hours of switching on and every fortnight +/- a random 50 hours. An event is raised when the battery test starts and when the battery test finishes. • The Battery Alarm fields will be disabled if "Use custom Power Supply with external battery backup" is selected on the **Power Supply Setup** tab.
High Temperature Output	The Fence Controller is equipped with an on-board temperature sensor. This sensor measures the temperature within the Fence Controller unit. When the temperature exceeds the configured Threshold (default 60 °C), the Output, (e.g. fan or cooling unit) will activate. When the temperature has dropped by 10°C below the Threshold, the Output switches off. The optimal temperature measured within the Fence Controller unit is 40 °C. If the measured temperature exceeds 75 °C a very high temperature alarm is raised. The energizer will skip every alternate pulse (Go Slow mode). A hysteresis of 10 °C applies. If the measured temperature exceeds 85 °C a critical temperature alarm is raised. The energizer will stop pulsing (Stop mode). A hysteresis of 10 °C applies.

30. Click the **Data Logging** tab.



This screen allows you to configure voltage and temperature logging for the Fence Controller. The events logged due to these settings will be used when a Voltage Report or Temperature Report is run for this Fence Controller.

31. Configure the Data Log change and/or time interval triggers as required, for either Battery Voltage, Temperature, or for both.
32. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Fence Controller. For further details see ***Cameras tab*** (on page 3-24).
33. Click the **Icons** tab if you want to change the Icon Set for this Fence Controller.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
34. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Fence Controller.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
35. Click the **Notes** tab if you want to add a note(s) about this Fence Controller.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
36. 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 F3x, F4x, F5x or F6x Fence Controller has been created, with Fence Zone(s) assigned to it, and it has been assigned to a Gallagher Controller 7000 or 6000. As a result, the following occurs:

- the Fence Controller and Fence Zone(s) will display within the **Hardware** List Window. The Fence Zones as child(ren) of the Fence Controller, and the Fence Controller as a child of the Gallagher Controller 7000 or 6000.
- on the **Connections** tab of the Fence Controller, the Gallagher Controller 7000 or 6000 name will appear in the **Connected to** field.

Configuring an F22 Fence Controller

Introduction

An F22 Fence Controller monitors and controls two Fence Zones, actively deterring and detecting intruder attempts. F22 Fence Controllers use the encrypted HBUS communications protocol to communicate with the Gallagher Controller.

Within Command Centre up to 24 F3x, F4x, F5x, F6x or F22 Fence Controllers can be assigned to a single Gallagher Controller.

This procedure describes how to create an F22 Fence Controller in Command Centre.

Before you begin

Before you begin this procedure:

- Ensure the following components have already been created:
  - a **Fence Zone**
    Refer to ***Creating a Fence Zone*** (on page 48-2)
  - a **Gallagher Controller 7000 or 6000**
    Refer to **Creating Controllers** (on page 21-2)
  - **Inputs and Outputs**
    Refer to ***Creating Inputs and Outputs*** (on page 21-33)
  - **Alarm Zones**
    Refer to ***Setting up Alarm Zones*** (on page 14-3)
- You need to be in the same or parent Division of the Command Centre items mentioned, and have the "Edit Site" operator privilege to perform this procedure.

Procedure

Creating a new F22 Fence Controller

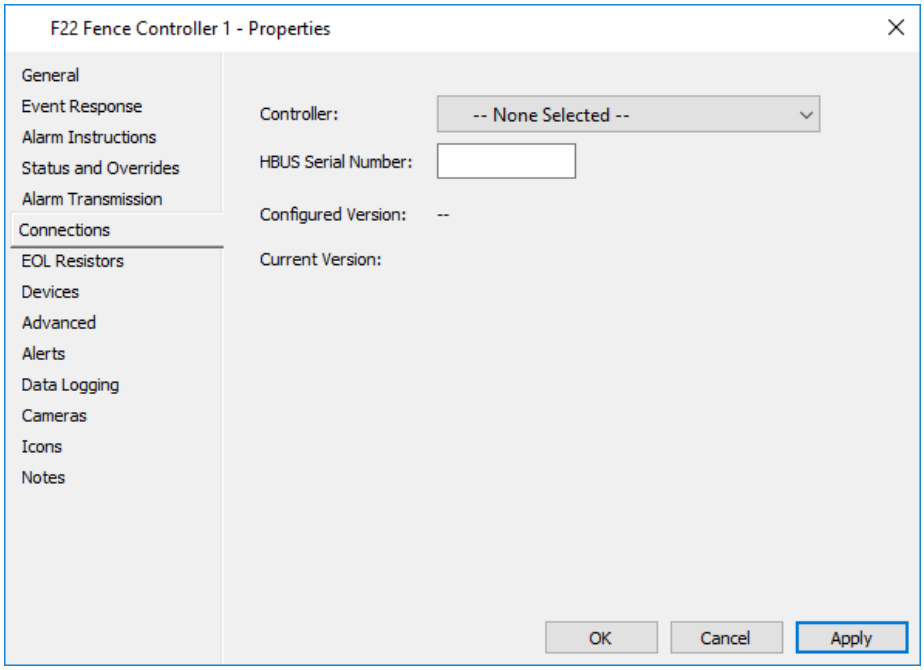
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...HBUS Devices**>**F22 Fence Controller**.
   Note: If **Fence Controller** is disabled in the context menu, this could be due to one of the following reasons:
   - the number of Fence Controllers already created has reached the limit as specified in the license, or
   - you do not have the operator privilege required to create Fence Controllers.

By default, the **General** tab displays.

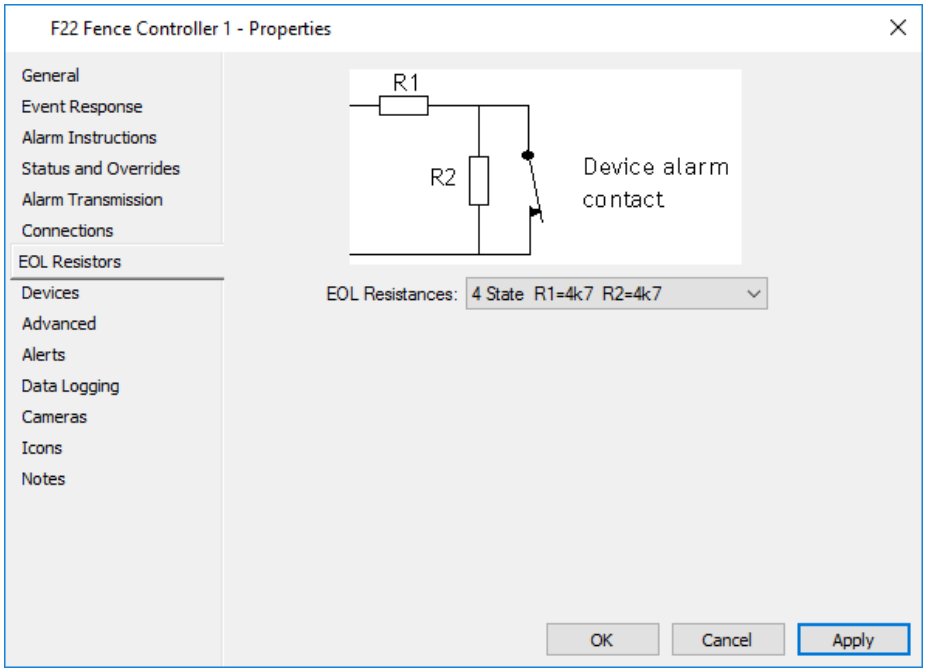
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
   Note: The Division must be the same as, or a parent of, the Division used for the new Fence Zone.
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).

   The Fence Controller needs to be placed in an Alarm Zone and have the Battery Alarms and Temperature Alarms settings configured to generate alarms for complete perimeter security.

   Note: It is possible to configure a "Pre-arm Timeout" (from 0-60 seconds) for Fence Controllers to ignore any alarms, via the **Alarm Warnings** tab of the Alarm Zone.
5. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
6. Click the **Status and Overrides** tab.
   Notes:
   - If a Fence Controller cover is removed, continuous tamper alarms will be generated. To prevent this from happening, tick the **Disable Tamper** checkbox.
   - When the Fence Controller is powered on, the tamper will automatically calibrate after a period of 10 seconds. Once fully installed and the cover mounted, an operator can reset the calibration of the tamper by re-booting the Fence Controller. To re-boot the Fence Controller, select **Reset** from the **Override** drop-down list and click **Override Now**. The Fence Controller will re-boot and the tamper will re-calibrate after a period of 10 seconds.
   - When a 'Shunt' override is performed Command Centre will stop communication to the Fence Controller. All Inputs and Outputs assigned to the Fence Controller will no longer respond to commands from Command Centre. It will remain this way until you 'Unshunt'. Alarms continue to be displayed on the Fence Controller.
   - The **Status and Overrides** tab displays the current battery voltage, the current temperature measured within the Fence Controller unit and the highest and lowest temperature recorded within the last 7 days.
7. Click the **Connections** tab.

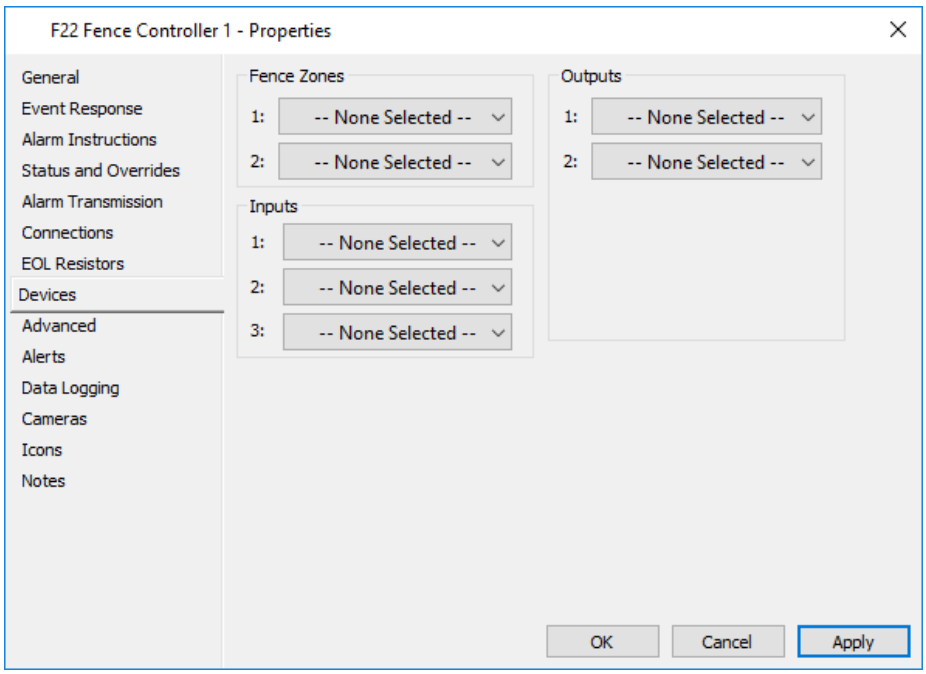


8. Select the Controller 6000 you want to assign this Fence Controller to, from the **Controller** drop-down list.
   Note: When an HBUS device is added to a Controller 6000, it will appear on the **HBUS Devices** tab of the Controller. In this case, the **Controller** field will be pre-populated with that Controller name.
9. If not already present, enter the HBUS serial number (10-character hexadecimal string) into the **HBUS Serial Number** field.
   Note: The HBUS serial number is optional, however the Fence Controller will be considered as not properly configured unless one is entered.
10. If you click the **Apply** button, software version numbers display.
    The **Configured Version** is the version of the device software in the configured Controller 6000 FTS file, (i.e. not the version of the Controller 6000 software). The **Current Version** is the version of software as last reported by the Fence Controller itself.
11. Click the **EOL Resistors** tab.



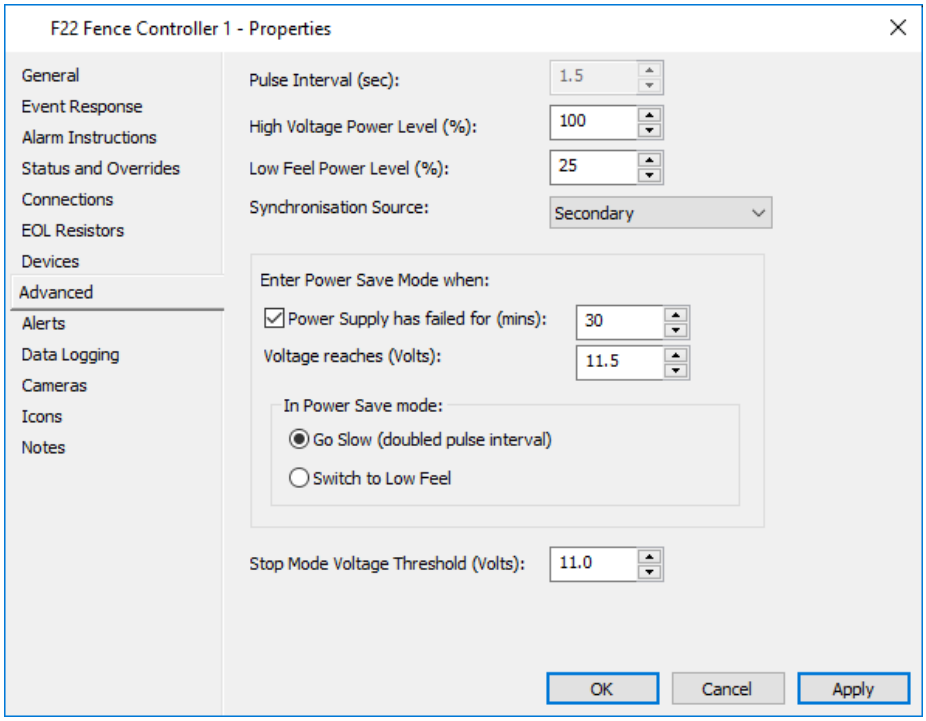
This screen allows you to define the wiring and resistance values used on inputs that are connected to the Fence Controller.

12. Select the required resistor values from the drop-down list.
13. Click the **Devices** tab.



14. Assign the appropriate Inputs, Outputs and Fence Zones to configure the Fence Controller.
    Notes:
    - Each Input, Output and Fence Zone can belong to only one Fence Controller.
    - Fence Zones may or may not be connected to a physical fence.

15. Click the **Advanced** tab.

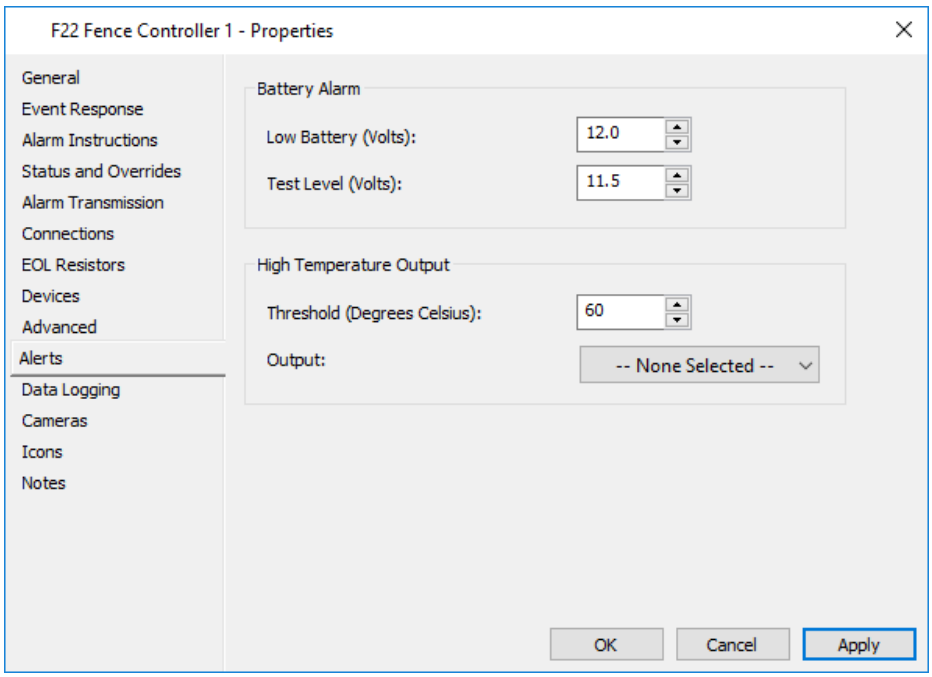


16. Configure as appropriate.

Field	Description
Pulse Interval (sec)	This is the pulse interval (period of time between pulses) for this Fence Controller. **Note:** If this Fence Controller has been configured as a secondary device, the pulse interval will be set to that of the primary device.
High Voltage Power Level (%)	This is the percentage of high voltage power that will be delivered per pulse, by this Fence Controller. (Default = 100%) 100% = 8.2 kV (without load) 50% = 5.8kV (without load) 30% = 4.5 kV (without load)
Low Feel Power Level (%)	This is the percentage of low feel power that will be delivered per pulse, by this Fence Controller. (Default = 25%) 25% = 0.9 kV (without load) 50% = 1.3 kV (without load) 100% = 1.8 kV (without load)
Synchronisation Source	Select the appropriate synchronization source for this Fence Controller.

Field	Description
Enter Power Save Mode	The Fence Controller will enter Power Save mode when: • the mains power has failed for a period of time greater than or equal to 30 minutes (default value), or • the mains power has failed and the battery voltage is less than or equal to 11.5 V (default value) for 7-10 seconds. **Note:** If the **Power supply has failed for (mins)** checkbox is un-ticked, the Fence Controller will continue to pulse as normal until the Power Save Voltage Threshold or Stop mode Voltage Threshold is reached.
In Power Save Mode	Select the appropriate behaviour when the Fence Controller enters Power Save mode. Either: • Go Slow (double pulse interval), or • Switch to Low Feel
Stop Mode Voltage Threshold	The Fence Controller will enter Stop mode (cease producing pulses) when the battery voltage is less than or equal to 11.0 V (default value) for 7-10 seconds.

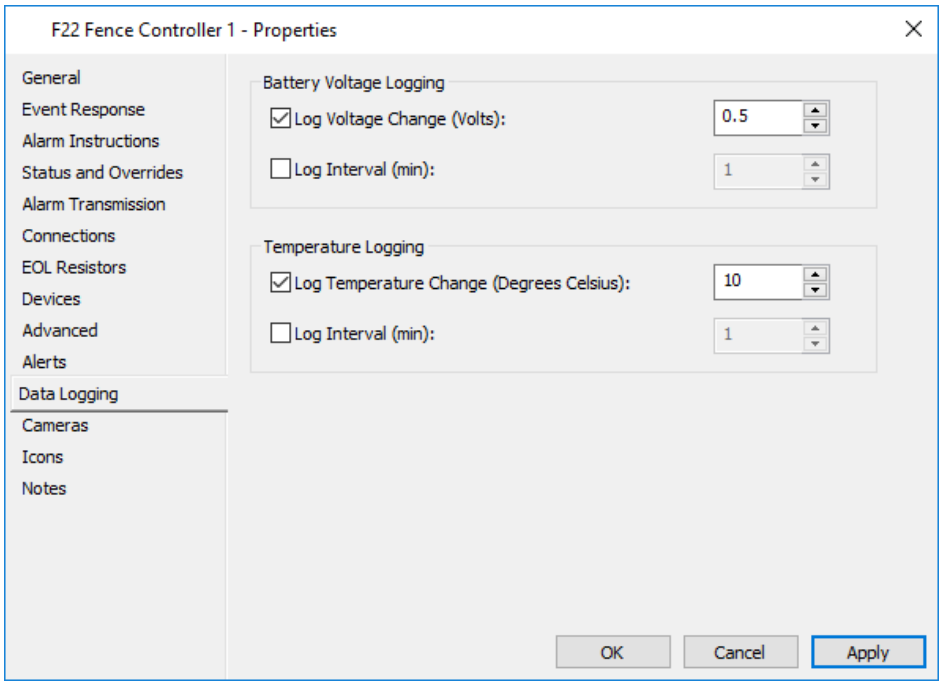
17. Click the **Alerts** tab.



18. Configure as appropriate.

Field	Description
Battery Alarm	If the battery voltage drops below the configured **Low Battery** level (Default = 12.0 V), an alarm is raised. If the battery voltage drops below the configured **Test Level** (Default = 11.5 V) during the battery test, an alarm is raised. **Note:** The Fence Controller will automatically test the battery within 24 hours of switching on and every fortnight +/- a random 50 hours. An event is raised when the battery test starts and when the battery test finishes.
High Temperature Output	The Fence Controller is equipped with an on-board temperature sensor. This sensor measures the temperature within the Fence Controller unit. When the temperature exceeds the configured Threshold (default 60 °C), the Output, (e.g. fan or cooling unit) will activate. When the temperature has dropped by 10 °C below the Threshold, the Output switches off. The optimal temperature measured within the Fence Controller unit is 40 °C. If the measured temperature exceeds 75 °C a very high temperature alarm is raised. The energizer will skip every alternate pulse (Go Slow mode). A hysteresis of 10 °C applies. If the measured temperature exceeds 85 °C a critical temperature alarm is raised. The energizer will stop pulsing (Stop mode). A hysteresis of 10 °C applies.

19. Click the **Data Logging** tab.



This screen allows you to configure voltage and temperature logging for the Fence Controller. The events logged due to these settings will be used when a Voltage Report or Temperature Report is run for this Fence Controller.

20. Configure the Data Log change and/or time interval triggers as required, for either Battery Voltage, Temperature, or for both.
21. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Fence Controller.
    For further details see ***Cameras tab*** (on page 3-24).
22. Click the **Icons** tab if you want to change the Icon Set for this Fence Controller.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
23. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Fence Controller.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
24. Click the **Notes** tab if you want to add a note(s) about this Fence Controller.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
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.

Result

An F22 Fence Controller has been created, with Fence Zone(s) assigned to it, and it has been assigned to a Gallagher Controller 6000. As a result, the following occurs:

- the Fence Controller and Fence Zone(s) will display within the **Hardware** List Window. The Fence Zones as child(ren) of the Fence Controller, and the Fence Controller as a child of the Gallagher Controller 6000.
- on the **Connections** tab of the Fence Controller, the Gallagher Controller 6000 name will appear in the **Connected to** field.

Monitoring Fence Zone Status

Introduction

This procedure describes how to monitor the status of a Fence Zone from Command Centre.

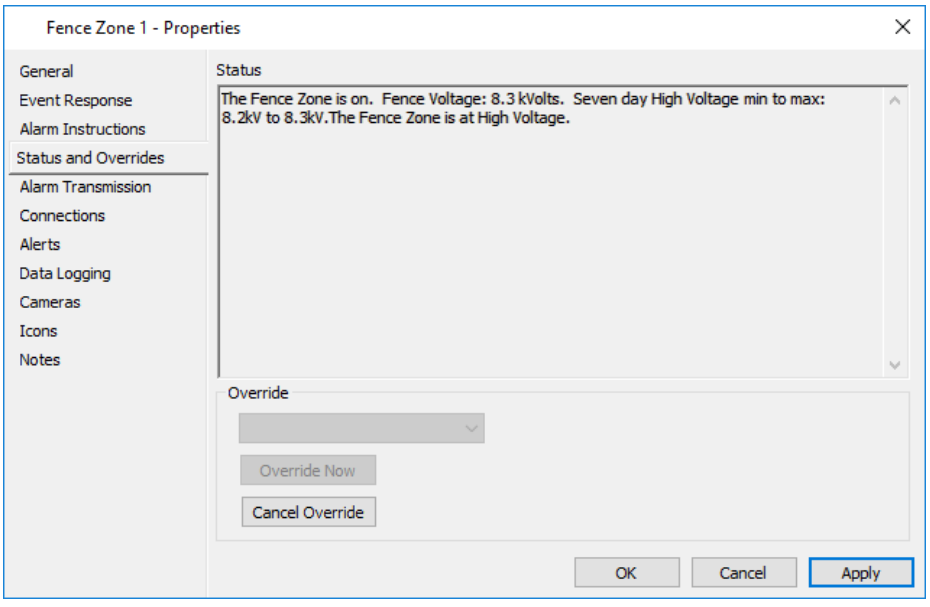
Before you begin

Before you begin this procedure:

- Ensure that the Fence Zone has been assigned to a Fence Controller, and the Fence Controller is assigned to a Gallagher Controller 6000 or 7000.
- You need to be in the same or parent Division of the Division holding the Fence Zone, and have the "View Site" operator privilege to perform this procedure.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Fence Zone you want to monitor.
3. **Right click** and select **Properties**.
4. Click the **Status and Overrides** tab.
   The status will be updated as soon as it is available.



If the Voltage reading changes, this could be due to some grass touching the fence, (e.g. grass).

If the Fence Controller that this Fence Zone is assigned to is offline the message *"Controller offline"* will display.

Monitoring Fence Controller Status

Introduction

This procedure describes how to monitor the status of a Fence Controller from Command Centre.

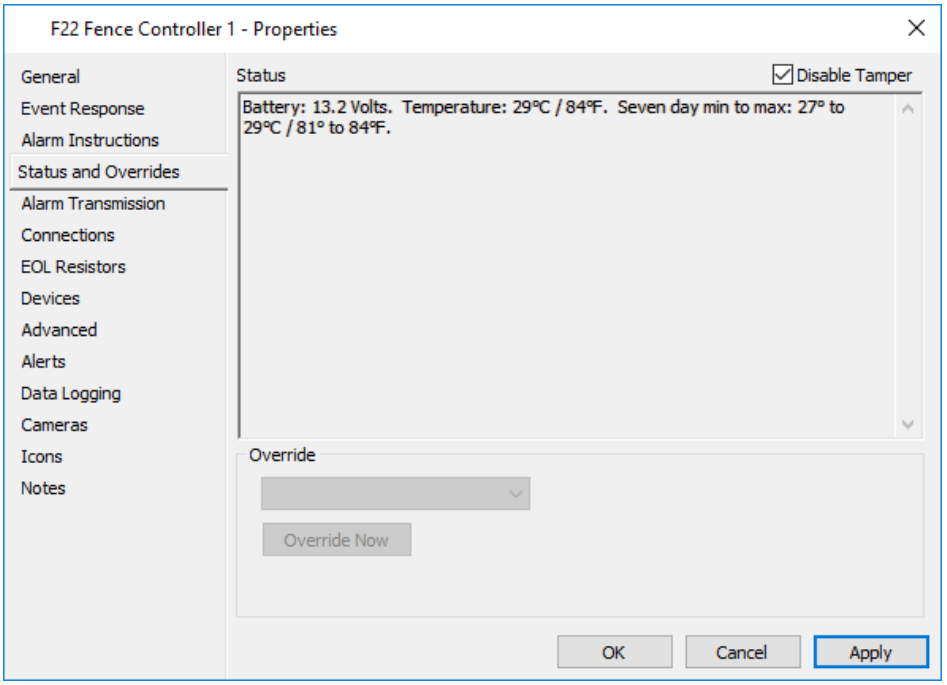
Before you begin

Before you begin this procedure:

- Ensure that the Fence Controller has been assigned to a Gallagher Controller 6000 or 7000.
- You need to be in the same or parent Division of the Division holding the Fence Controller, and have the "View Site" operator privilege to perform this procedure.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Fence Controller you want to monitor.
3. **Right click** and select **Properties**.
4. Click the **Status and Overrides** tab.
   The status will be updated as soon as it is available.



Monitoring Fence Alarms and Events

Introduction

Monitoring fence alarms and events can be done from either:

- the Command Centre **Alarm or Event window**, or
- a **Site Plan**
  Note: Only alarms can be monitored from a Site Plan, (i.e. events cannot be), and the procedure for this method is already described in ***Viewing Alarms from Site Plans*** (on page 43-4).

You can acknowledge alarms using the existing alarm acceptance capabilities in Command Centre.

Before you begin

Before you begin this procedure:

- Ensure that the Fence Zone has been assigned to a Fence Controller and has an Alarm Zone, and that the Fence Controller and Alarm Zone have been assigned to a Gallagher Controller 6000 or 7000.
- You need to be in the same or parent Division of the Division holding the Fence Zone, and have the "View Alarms" operator privilege to perform this procedure.

Procedure

1. Open either the **Alarm Viewer** window or the **Event Viewer** window, by clicking **Monitor** from the menu bar, and then either:
   - **Alarm Viewer**, OR
   - **Event Viewer**
2. Highlight the activity message.
3. Either:
   - **Right click** and select **Properties**, or
   - **Double-click** the alarm/event.

   The Alarm or Event Properties screen displays, providing more details.
   Note: The alarm can be acknowledged and/or processed if you have the "Edit Alarms" operator privilege. If you do not have this privilege, you can still add comments to the 'Notes' field.

Overriding a scheduled Fence Zone state

Introduction

This procedure describes how to temporarily override a Fence Zone in Command Centre to:

- "On" or "Off" (to allow voltages to be checked by a technician),
- "Shunt" or "Unshunt" (if the Fence Zone is creating false alarms), or
- "High Voltage" or "Low Feel" (to change the voltage level)
  Note: HV/LF mode is compatible with F3x, F4x, F5x, F6x and F22 Fence Controllers only.

Before you begin

Before you begin this procedure:

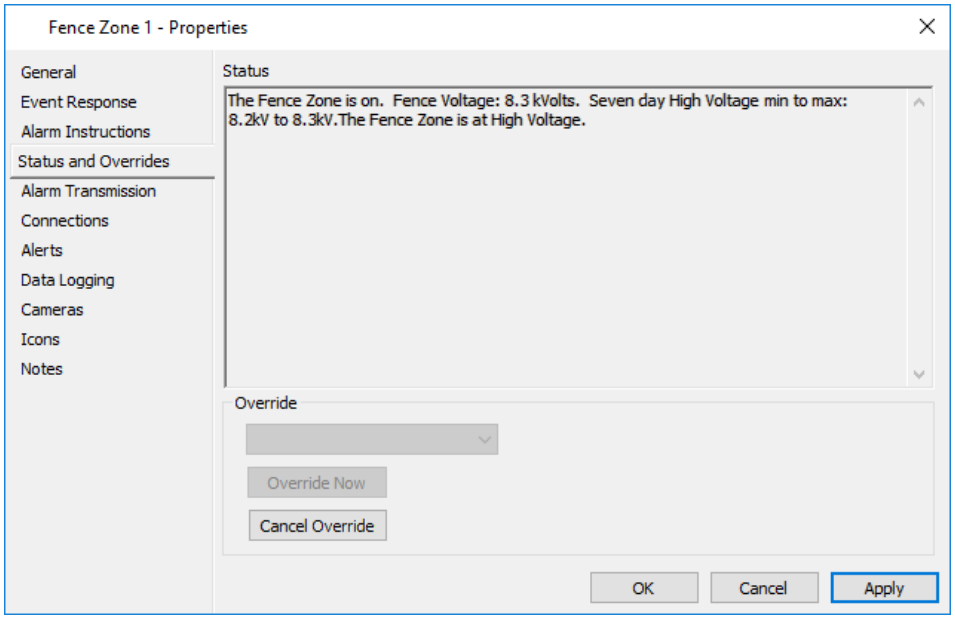
- Ensure that the Fence Zone has been assigned to a Fence Controller, and that the Fence Controller has been assigned to a Gallagher Controller 6000.
- You need to be in the same or parent Division of the Division holding the Fence Zone, and have the "Maintenance Override" operator privilege to perform this procedure.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Fence Zone you want to override.
3. Either:
   - **Right click** and select **Properties,** then click the **Status and Overrides** tab.

   OR

   - **Right click** and select **Override...**
     The **Status and Overrides** tab displays.



4. Click within the **Override** field and select the required override action from the drop-down list, (i.e. "Shunt", "Unshunt", "On", "Off", "High Voltage" or "Low Feel").
   Notes:
   - An "On" override causes the Fence Zone to become active, (i.e. pulsing), and an "Off" override causes the Fence Zone to become inactive, (i.e. not pulsing).
   - Fence Zones do not support timed overrides. All overrides are immediate and persist until specifically cancelled by an operator using Command Centre or from a Terminal. Cancelling an override cancels any existing "On" or "Off" override.
5. Click the **Override Now** button.

Result

The override is applied and will remain in place until the override is manually cancelled.
Notes:

- The Fence Zone turns on when its Alarm Zone is armed. This is not an override - it is normal behaviour.
- Fence logging events will still occur when a Fence Zone is shunted.

Overriding a Fence Controller

Introduction

You may choose to temporarily override a Fence Controller when testing the associated fences. Overrides that can be performed at a Fence Controller are:

- **Shunt**
  Stops communication with the Fence Controller. Alarms raised by the Fence Controller are suppressed. Command Centre will not send commands to the Fence Controller, Fence Zones, Inputs or Outputs until you 'Unshunt'.
- **Unshunt**
  Starts communication with the Fence Controller.
- **Reset**
  Performs a software reset on the Fence Controller. When performed on an F3x, F4x, F5x or F6x Fence Controller all inactive alarms (shown on the Fence Controller cover) will be reset (cleared).

Before you begin

Before you begin this procedure:

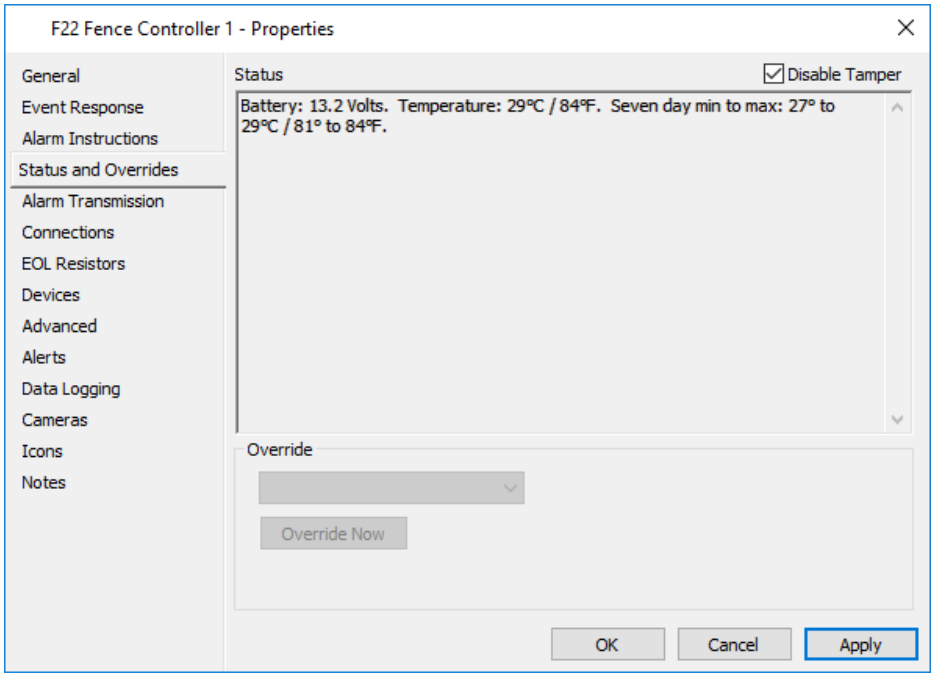
- Ensure that the Fence Controller has been assigned to a Gallagher Controller 7000 or 6000.
- You need to be in the same or parent Division of the Division holding the Fence Controller, and have the "Maintenance Override" operator privilege to perform this procedure.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Fence Controller you want to override.
3. Either:
   - **Right click** and select **Properties,** then click the **Status and Overrides** tab.

   OR

   - **Right click** and select **Override...**
     The **Status and Overrides** tab displays.



4. Click within the **Override** field and select the required override action from the drop-down list, (i.e. "Shunt", "Unshunt" or "Reset").
   Note: This function will not turn the associated Fence Zones on or off.
5. Click the **Override Now** button.

Result

An override has been applied to this Fence Controller.

Creating a Voltage Report

Introduction

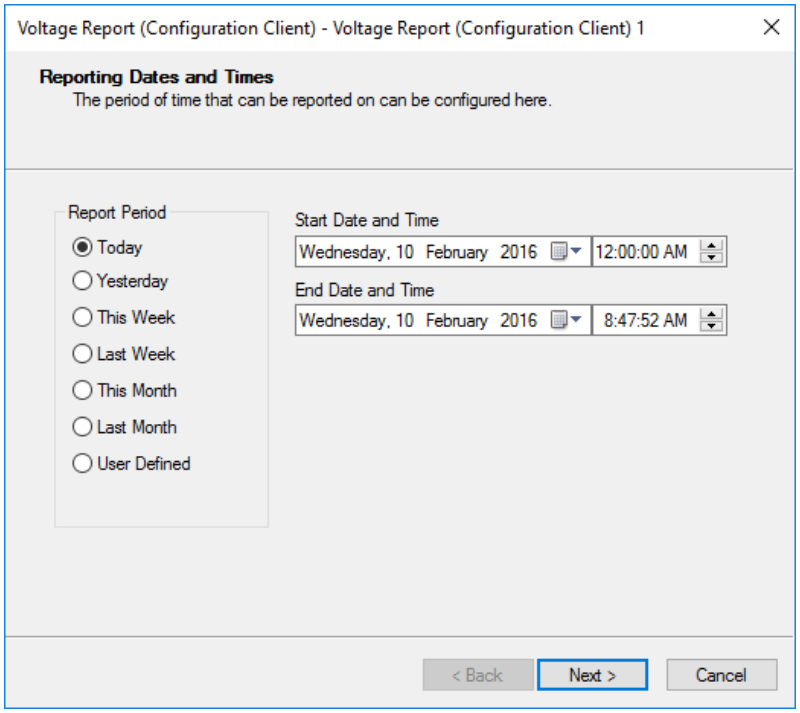
This procedure describes how to create a Voltage Report for either a Fence Zone or a Fence Controller. Voltage Reports use the settings configured on the **Data Logging** tab of the relevant Fence Zone or Fence Controller.

You need to be in the same or parent Division of the Division holding the Fence Zone, and have the "View Site" operator privilege to perform this procedure.

Note: The Voltage Report is only supported when the screen resolution is 1024 x 768 or higher. While it will run against a lower resolution, the results cannot be guaranteed.

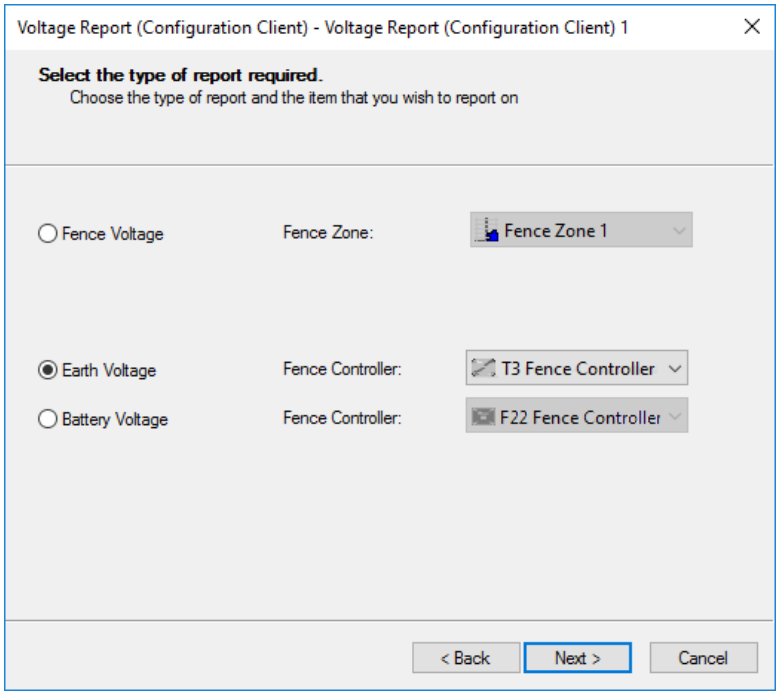
Procedure

1. Click **Reports** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
2. **Right click** and select **New...Voltage Report**.
   The **Reporting Dates and Times** page of the Voltage Report wizard displays.



This page allows you to enter a start and end time for the report. Pre-defined periods are provided for simplicity, or custom start and end times can be entered.

3. Configure the period required for the report, and click the **Next** button.
   The **Select the type of report required** page displays.



4. This page allows you to specify one of the following input combinations:

   - Click the **Fence Voltage** radio button and make a selection from the **Fence Zone** drop-down list,

   OR

   - Click the appropriate Voltage radio button, (i.e. either **Earth Voltage** or **Battery Voltage**) and make a selection from the **Fence Controller** drop-down list.

   Notes:

   - The F31, F32, F41, F42 and F22 Fence Controller does not support Earth Voltage Data Logging.
   - In a multi-server environment, for any given remote server with event aggregation enabled, remote Fence Controllers or remote Fence Zones will be available for selection from the drop-down lists.

5. Click the **Next** button.
   The **Report Generation and Saving** page displays. This wizard page is the same for all report types, and provides the same options. Refer to ***Report Generation and Saving*** (on page 39-3) in the *Creating a new report* procedure for further detail.

Result

The logged volts for the Fence Zone or Fence Controller are displayed on screen as a line graph, which can be printed out, or saved to file as a CSV format.

Creating a Temperature Report

Introduction

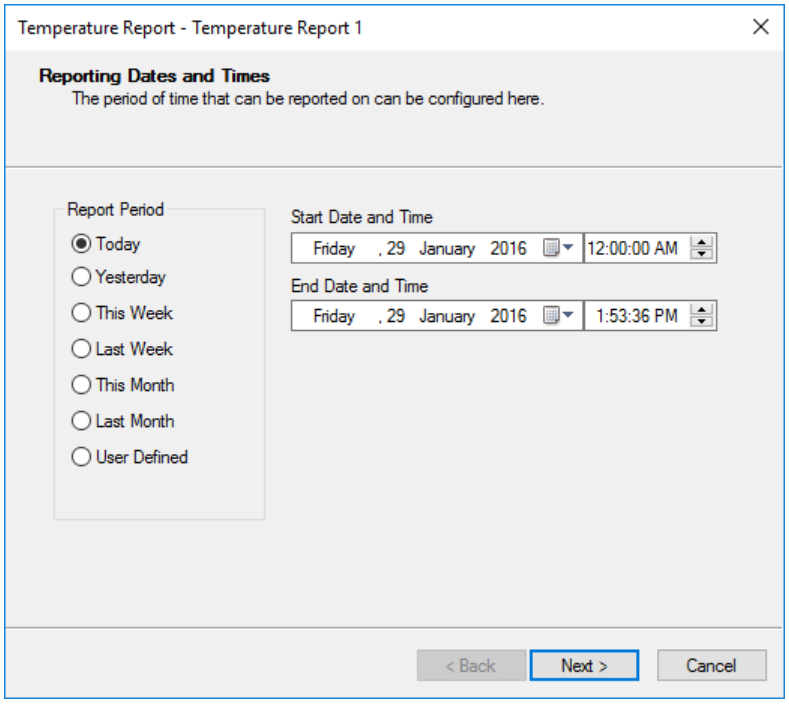
This procedure is applicable for the F31, F32, F41, F42 and F22 Fence Controller only. The Temperature Report details the temperature readings measured within the Fence Controller, and uses the settings configured on the **Data Logging** tab of the relevant Fence Controller.

You need to be in the same or parent Division of the Division holding the Fence Zone, and have the "View Site" operator privilege to perform this procedure.

Note: The Temperature Report is only supported when the screen resolution is 1024 x 768 or higher. While it will run against a lower resolution, the results cannot be guaranteed

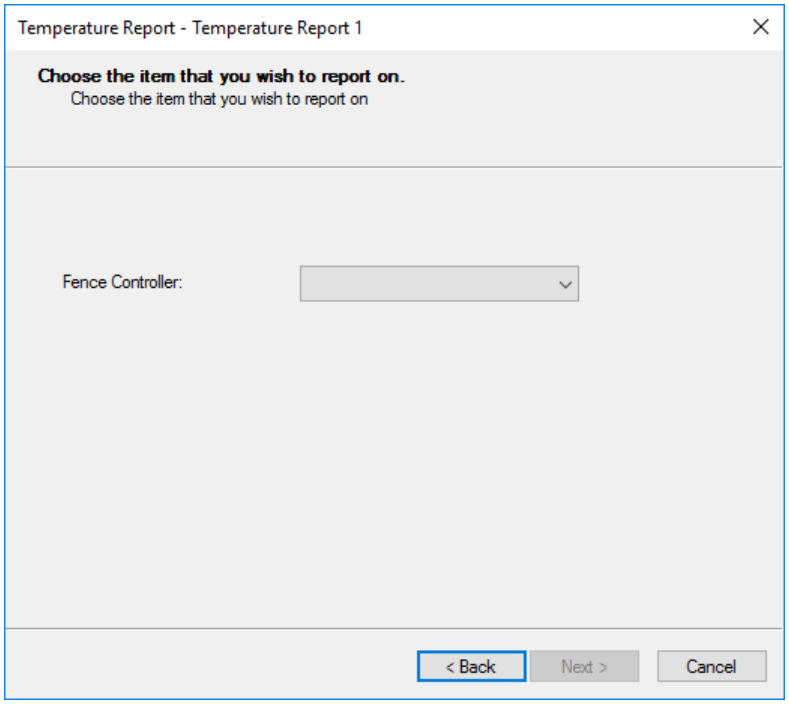
Procedure

1. Click **Reports** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
2. **Right click** and select **New...Temperature Report**.
   The **Reporting Dates and Times** page of the Temperature Report wizard displays.



This page allows you to enter a start and end time for the report. Pre-defined periods are provided for simplicity, or custom start and end times can be entered.

3. Configure the period required for the report, and click the **Next** button.
   The **Choose the item that you wish to report on** page displays.



4. Select the Fence Controller to report on from the drop-down list.
5. Click the **Next** button.
   The **Report Generation and Saving** page displays. This wizard page is the same for all report types, and provides the same options. Refer to ***Report Generation and Saving*** (on page 39-3) in the *Creating a new report* procedure for further detail.

Result

The temperature readings measured within the Fence Controller are displayed on screen as a line graph, which can be printed out, or saved to file as a CSV format.

Using Service mode

Introduction

Service mode is available on the F31, F32, F41 and F42 Fence Controllers only.

Service mode provides a convenient means for controlling Fence Zones at the Fence Controller, without using Command Centre or a terminal. It ensures the technician's safety when working on the fence by temporarily removing Fence Zone control from Command Centre and its associated terminals.

Procedure

1. To enable Service mode, check the **Allow use of Service Mode for local control** checkbox on the **Advanced** tab in the appropriate Fence Controller's properties.
2. To enter Service mode, set the Service Mode SW1 dipswitch 1 to ON.

   When Service mode is entered:

   - An active Service mode alarm is raised (the Service icon on the Fence Controller is lit, red and flashing while the Fence Controller is in Service mode). The alarm remains active and cannot be processed until you exit Service mode.
   - All system and fence alarms continue to be raised while in Service mode. The alarms are visible via the Fence Controller icons, in Command Centre and at a terminal.

     Inactive alarms reset at the Fence Controller will remain visible in Command Centre and at a terminal. Inactive alarms processed in Command Centre but not reset at the Fence Controller, remain visible at the Fence Controller.
   - The Fence Zones are initially disarmed.
   - The Fence Controller no longer responds to Command Centre or terminal state changes to arm or disarm the Fence Zones.
   - The Fence Controller continues to follow the set HV/LF mode and responds to any changes made to the HV/LF mode.
   - The Fence Zone control via the magnetic key operates on a toggle; arming the Fence Zone if it is currently disarmed; disarming the Fence Zone if it is currently armed. Each Fence Zone operates independently by presenting the magnetic key to each Fence Zone icon "+" or "-".

     Presenting the magnetic key to the Fence Controller will reset all inactive alarms displayed on the Fence Controller.

Inactive alarms reset at the Fence Controller will remain visible in Command Centre and at a terminal. Inactive alarms processed in Command Centre but not reset at the Fence Controller, remain visible at the Fence Controller.

When Service mode is exited:

- The Service icon on the Fence Controller is restored (solid red).
- The Service mode alarm changes to inactive and can be processed.
- The Fence Zones immediately follow the status as set by Command Centre.
- Presenting the magnetic key no longer arms or disarms the Fence Zones but will reset all inactive alarm conditions.

Notes:

- If a Fence Zone is placed in Lockout mode from a terminal, no indication of Lockout mode is visible on the Fence Controller. When subsequently placed in Service mode, the magnetic key cannot be used to arm/disarm Fence Zones that are in Lockout. The magnetic key will clear all inactive alarms.
- Placing the Fence Controller in Service mode when the Fence Controller is offline or shunted has no effect on behaviour, (i.e. Fence Zones cannot be controlled via the magnetic key), even if Service mode was enabled prior to the Fence Controller going offline or being shunted.
- If the Fence Controller is in HBUS mode (not Stand-Alone mode) and not connected to Command Centre, Service mode cannot be entered.

Using HVplus mode

Introduction

HVplus mode is only available on the F41 and F42 Fence Controllers, and the F61 and F62 Fence Controllers (excluding the EN variants). HVplus mode is enabled by default (the **Enable HVplus Mode** checkbox is checked on the **Advanced** tab in the Fence Controller's properties).

HVplus mode is triggered when either Fence Zone (armed in High Voltage mode) drops below the configured High Voltage low Fence Alert threshold. The move to HVplus mode occurs after a single pulse below the configured threshold.

HVplus mode increases the high voltage on both Fence Zones to approximately 10 kV (load dependent) for a period of 20 minutes.

Notes:

- Only Fence Zones armed in High Voltage mode can transition to HVplus mode.
- The stated time of 20 minutes remains, even if the fence voltage returns to above the High Voltage low Fence Alert threshold.
- After an HVplus escalation, the fence voltage must return to above the High Voltage low Fence Alert threshold, then drop to below the High Voltage low Fence Alert threshold to trigger another HVplus escalation.
- The Fence Controller will enter HVplus mode at 100% power (10 kV), regardless of the High Voltage Power Level, (e.g. 50%) configured on the **Advanced** tab in the Fence Controller's properties.
- To exit HVplus mode, both Fence Zones must be disarmed or changed to Low Feel mode.

HVplus indications

- When the Fence Controller enters HVplus mode, the event "HVplus escalation has occurred" is raised in Command Centre.
- When a Fence Zone enters HVplus mode, the event "[Fence Zone name] – HVplus" is raised in Command Centre.
- Indications that a Fence Zone is in HVplus mode is shown on a terminal.
- When a Fence Zone is in HVplus mode, the Fence Zone icon (in Command Centre) changes to indicate HVplus mode and the HV icon (located on the Fence Controller cover) for the applicable Fence Zone flashes orange.

Synchronisation

- If the Fence Controller has a synchronization loss active alarm it will still transition to HVplus mode, if the trigger condition occurs.
- HVplus mode is not persisted across synchronised Fence Controllers.

Temperature management

- If the temperature measured within the Fence Controller unit is less than 72 0C (162 0F) the Fence Controller will transition to HVplus mode, if the trigger condition occurs.
- If the temperature measured within the Fence Controller unit is greater than 72 0C (162 0F) the Fence Controller will not transition to HVplus mode, if the trigger condition occurs. If an HVplus escalation is currently in progress, it is allowed to complete normally.

When powered by the battery

- If an HVplus escalation condition occurs while the Fence Controller is running on the battery (mains failure has occurred) the Fence Controller will still enter HVplus mode.
- If the Fence Controller enters Stop mode from HVplus mode, the HVplus escalation is cancelled. Once pulsing resumes, it is in High Voltage mode (assuming the unit has remained armed in High Voltage mode throughout).

Service mode

- If the Fence Controller is in Service mode it will still transition to HVplus mode, if the trigger condition occurs.
- If the Fence Controller is in Service mode and HVplus mode, then both Fence Zones are disarmed or placed in Low Feel mode, the Fence Controller will exit HVplus mode.
- If the Fence Controller is in HVplus mode and Service mode is entered or exited, the Fence Controller will exit HVplus mode.

Moving from Low Feel mode to HVplus mode

A Macro can be used to override a Fence Zone into High Voltage mode. For example, if a Fence Zone which is armed in Low Feel mode generates an event, the event can be used to drive an Action Plan that has the Macro assigned to override the Fence Zone into High Voltage mode. If fence voltage drops below the configured High Voltage low Fence Alert threshold when in High Voltage mode, the Fence Zone will enter HVplus mode.

Chapter 49: Multi-Server systems

Introduction

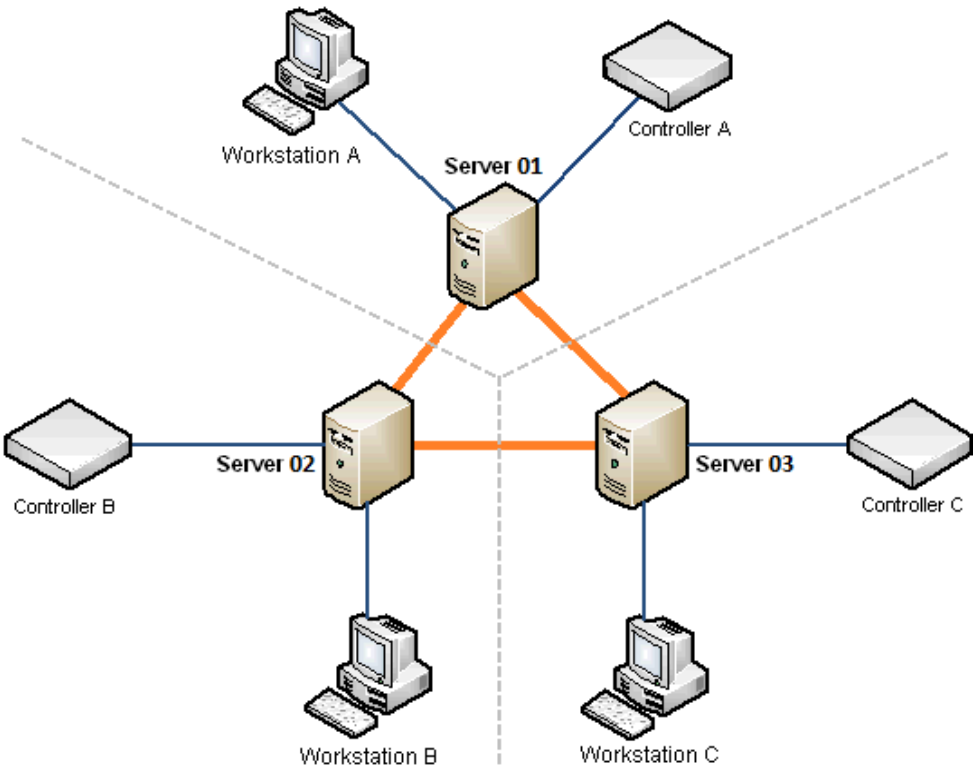
The Multi-Server systems feature improves the ability of Command Centre to operate effectively in a distributed environment. This “distributed environment” may include multiple sites separated by large geographical distances and connected via low bandwidth and/or intermittently available networks.

A Multi-Server User Guide is located in the '`Documentation`' directory of the Command Centre installation files, which provides further information regarding multi-server functionality.

There are two different types of Multi-Server system structures, (i.e. 'Peer-to-Peer' structure and 'Star' structure).

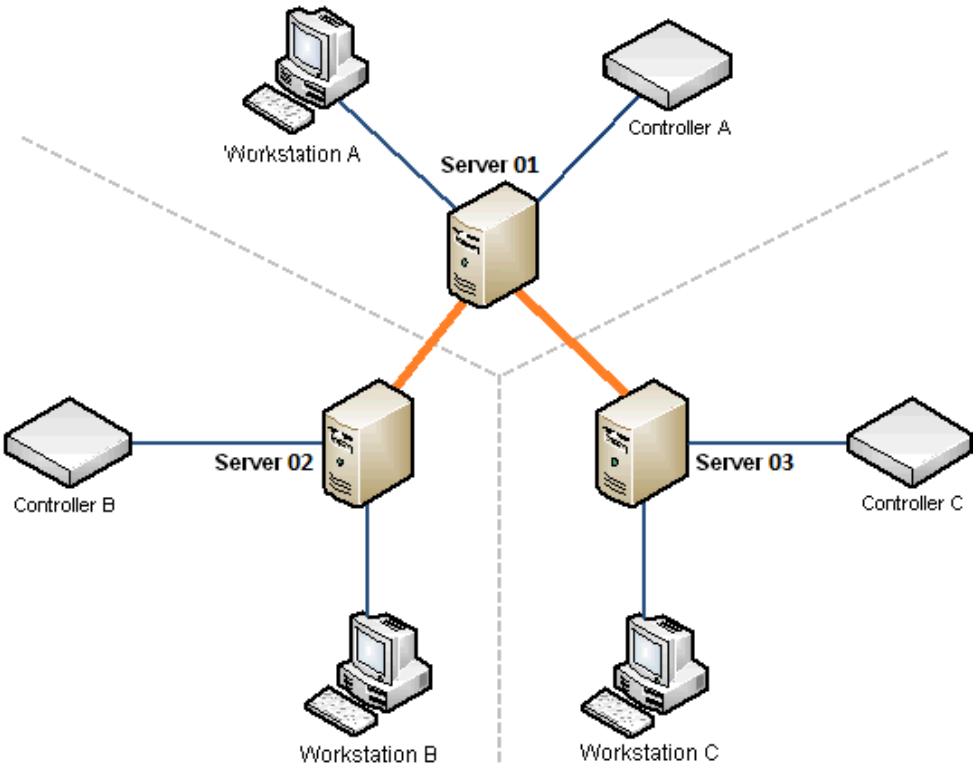
Peer-to-Peer structure

In a Peer-to-Peer structured multi-server system, each server communicates directly with every other server in the multi-server environment, as shown:



Star structure

In a Star structured multi-server system, each server only communicates with the Parent server, (e.g. Server 02 and 03 are child servers of Parent Server 01), as shown:



Licensing

Multi-server functionality is a licensable feature of Gallagher Command Centre. Each server in the Multi-server environment must have its own unique license file, (which means that license limits are applied locally on each server), containing the following entry:

```
[Features]
MultiServer=1
```

There are two additional entries that may also be required:

To allow…	License entry
the site to change multi-server structure, (i.e. from 'Peer-to-Peer' to 'Star' structure, or vice versa), the license file for each server must also contain,	MultiServerHierarchy=1
a parent server to delete child servers from the system, the license file for the parent server must contain,	`MultiServerRemoval=1` **Note:** Child servers cannot delete other servers.

A server will not be able to participate in a multi-server system if its License File does not grant that privilege. Licensing is used to control which other servers a server can be connected to. A server cannot be connected to other servers unless the License File has the following:

- Multi-server enabled
- The same system Serial Number
- A unique server Serial Number

License restrictions for Command Centre items only apply to the local items on the server to which the License File applies. Remote items are not counted when determining how many instances of a Command Centre item exist for the purpose of licensing. However, this is not so with global items, for example: *If two servers in a multi-server system both use Photo ID, each server will need to be enabled with a valid Photo ID license.*

This chapter covers the following topics:

- ***Important Issues*** (on page 49-4)
- ***Remote Command Centre items*** (on page 49-6)
- ***Creating a Remote Server*** (on page 49-9)
- ***Switching from Peer-to-Peer structure to Star structure*** (on page 49-13)
- ***Switching from Star structure to Peer-to-Peer structure*** (on page 49-14)
- ***Adding a new server to a Star structure*** (on page 49-15)
- ***Overriding a Remote Server*** (on page 49-17)
- ***Event Aggregation*** (on page 49-19)
- ***Deleting a remote server from a Peer-to-Peer structure*** (on page 49-22)
- ***Deleting a child server from a Star structure*** (on page 49-24)

Important Issues

Introduction

When configuring a multi-server system, it is important to be aware of the following issues:

Setup

- Connecting Command Centre Servers to the Internet is not recommended as this would introduce potential security risks.
- All servers in a multi-server system need to be configured to get replication functioning, and they must all have their time-clocks synchronised.
- Crypt Seeds must be the same on all servers in order for cardholder's PINs to work correctly at all locations.
- The **Minimum User Code Length** (on the **User Codes and PINs** tab of the Server Properties) should be set to a higher value on all servers in a multi-server system.
- If your site has Morpho Biometric Readers installed, 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.
- From a security standpoint, all servers in a multi-server system are considered as a single system with no trust boundary between the individual servers.

Divisions

- Every Division in the multi-server system will be permanently linked to the server it is created on and cannot span across other servers, (i.e. it cannot be assigned to any server other than the one it is created on).
- Items other than cardholders created on one server cannot be assigned to a Division not associated with its 'Home' server.
- A cardholder created on one server **can** be assigned to a Division on a different server in a Multi-server environment.

Operators

- In a multi-server system there is a separate "system operator" for each server and they cannot be renamed. This makes it difficult to identify what activities have been performed by each system operator, (e.g. in an Activity Report). Therefore, once you have used the "system operator" to initially set up operators access in a multi-server system, it is recommended that you do not use the "system operator' again.

You cannot logon as a remote "system" account, (i.e. if the local system account is disabled, the logon will not try to use a remote system account even if it is enabled).

You cannot disable remote system accounts. You must logon locally to the server in order to disable the system account.

Refer to ***Disabling the System Operator*** (on page (32-34) for further detail.

- Configuration conflicts, (e.g. duplicate Card Numbers are used) may occur. If this happens, a configuration conflict alarm will be raised, prompting an operator to resolve the conflict manually.
- Password restrictions (set on the **Operator Defaults** tab of the Server Properties) are only applied at the server where a password is created. This means that unless password restrictions are set up identically on all servers, a non-compliant password can be used to log onto a workstation connected to any server other than the server the password was created on. For this reason, it may be advisable to set password restrictions up to be the same on all servers in the system.
- When an operator is logged onto a remote server, (e.g. monitoring remote alarms), they will show as a "Remote" session on the **Operator Sessions** tab of the Server Properties.
- Sites need to be aware that any sensitive information created and stored local to one particular server will be accessible by anyone with access to any server in the multi-server system.
- Operator lockout state does not get replicated to remote servers in a multi-server environment.

Limitations

- In a multi-server system that uses Visitor Management (a licensable feature), visit data does not get replicated between servers. Therefore, the Evacuation Report cannot report on remote visitors.
- It is the intention to enhance OPC in future releases so that it can function with either a single server or multiple server events. However, currently OPC Bridge, OPC CCTV and OPC Contact ID will work only using a single server within a Multi-Server environment. Each server will allow multiple OPC operators, and events will be obtained for individual servers only.
- In a multi-server system that has Morpho Biometric Readers installed, biometric inactivity is managed by each server independently, using the Morpho Biometric Type configuration unique to each server.
- You cannot connect two servers in a multi-server system if they have been created from the same template.

Remote Command Centre items

Introduction

When Command Centre items are viewed on a server other than their home server, (i.e. a remote server), they may behave slightly differently than they do on their home server. Command Centre items in a multi-server system are split into two groups, as the following table shows:

Item Type	Definition	Command Centre items
Global items	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
Remote items	Remote items are only editable from workstations connected to the server they were created on. 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.	**Access Groups *** **Card Types** **Personal Data Fields **** **Divisions** **Operator Groups** **Macros ***** **Site Plans** **Remote Server** Icon Sets Alarm Instructions Insertion Tags Workstations

Note: The remote items above in **bold** text can be viewed from the appropriate List Window. However, the other remote items, or any item on another server, can be located by using the Find Tool. See Searching using Divisions for further detail.

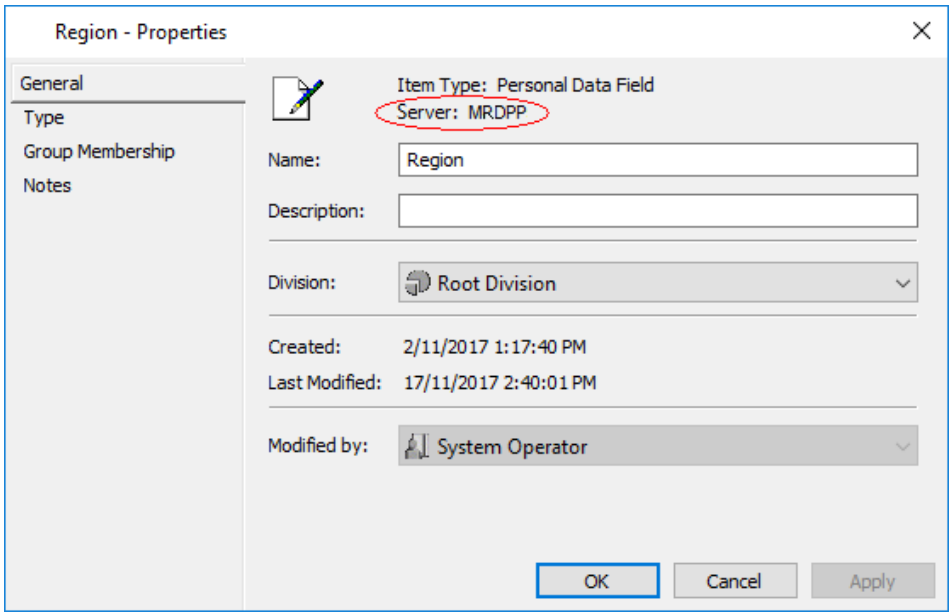
***** Some **Access Group** properties are editable remotely. Local access can be assigned to remote Access Groups in the same way as for local Access Groups. Any access assigned on other servers is visible from all servers by suitably privileged operators, but cannot be removed.
Note: "Access" includes Access Zones, Alarm Zones, Salto Doors and Salto Zones.

**** Personal Data Fields** should have unique names across servers.

***** Macros** can be scheduled remotely while the home server of the Macro is online.

Identifying an item's server

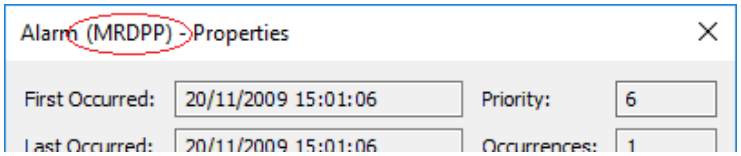
It is possible to identify which server a remote item belongs to from the **Server** field on the **General** tab of the item's property pages.
Note: The **Server** field is only visible for remote items. It does not display for cardholders.



You can give the server a more user friendly name by adding a 'Short Name' on the **General** tab of the Server Properties. The short name is then used instead of the hostname configured against the remote item.

Remote items have a restricted set of property page tabs from what would normally be visible for that item type. Only those tabs necessary for remote monitoring, (e.g. for editing or performing an override) will display. Operator privileges will also determine what information appears as 'read-only' within those tabs.

The Alarm Viewer window appears the same between servers, (i.e. there is no way of telling which server an alarm was generated by). However, when you view the alarm details, if a server name appears in the title bar in brackets, this indicates that the alarm was generated by a remote server.



Notes:

- When a remote server is off-line, a user will not be able to acknowledge the alarm and it will be marked as off-line if they attempt to do so. All other remote alarms from that remote server will appear as off-line, read only and the user will not be able to process or enter details against them.

- If you are viewing off-line remote alarms in the Alarm Viewer and the Alarm Viewer is refreshed, (e.g.**F5**), all off-line alarms will be removed and will not reappear until the remote server comes online again.

Deleting remote Command Centre items

Remote Command Centre items cannot be deleted manually, instead they need to be deleted from the home server of the item.

Creating a Remote Server

Introduction

This procedure describes how to add a remote server to a multi-server system. Typically, an operator will set up a connection between an existing server and the new server (referred to as Server 1 and Server 2 in this procedure), and the system will ensure that the information about the new server is distributed to any other servers in the system.

Notes:

- The connection can be configured in either direction so Server 1 could be either the new server or the existing server.
- Remote Server items can only be created if your system is licensed for multi-server, and each server in a multi-server system must have compatible license files.

Before you begin

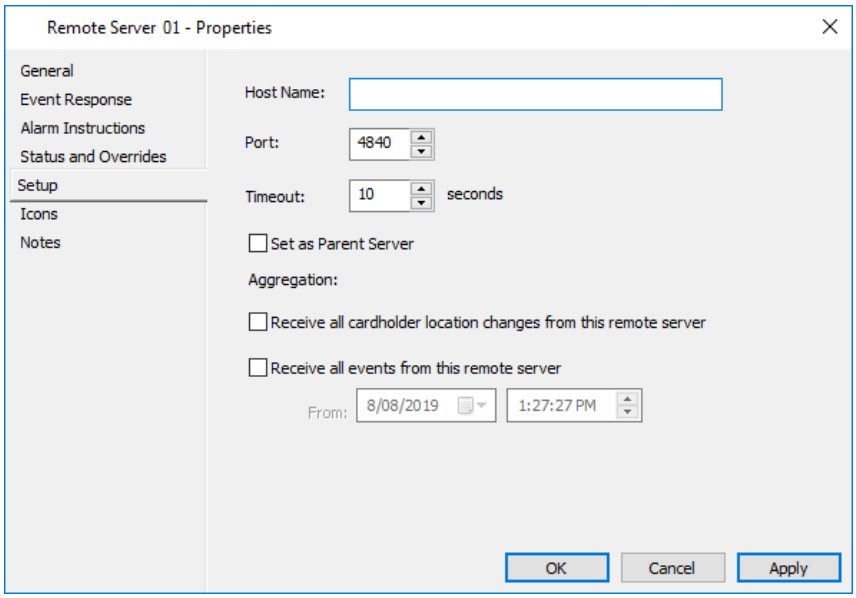
Before you begin this procedure ensure:

- you know the name and password of an operator on the other system with sufficient privileges to create a Remote Server.
- the remote server is running.
- you are logged on as an operator with the "Advanced User" privilege.
  Note: While the "Advanced User" privilege is required to create remote servers, to edit the properties of remote servers you only need the "Edit Site" privilege.

Procedure

Create a 'Remote Server' for Server 2 on Server 1

1. On Server 1, click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens (in grid view).
2. **Right click** and select **New...Remote Server**.
   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 **Setup** tab.



7. Enter the host name or IP address of the remote server in the **Host Name** field. (Limit = 255 characters)
   Note: The host name can be specified in any form that can be resolved by the operating system, (e.g. host name, fully qualified domain name or IP address). However, the host name should be entered in a form that can be resolved by other servers as they will need to connect to the new server.

8. Is the remote server listening on the default port?

If...	then...
yes	go to Step 9.
no	you may need to specify the port number as well, in the **Port** field. (Limit = 5 digits; Range = 1 to 65535)

9. Alter the **Timeout** period if required. (Limit = 2 digits; Range = 1 to 99)
   Note: The Timeout period should not be set to anything too large as it is used by other parts of the multi-server system and could slow down multi-server functionality.

10. The **Set as Parent Server** checkbox only applies to 'Star' structure multi-server systems, where one of the remote servers is the parent server, (i.e. all the other remote servers only communicate with the parent server).

    Note: The 'Star' structure multi-server is a licensed feature. The **Set as Parent Server** checkbox will be disabled if your site is not licensed for the 'Star' structure.

    Is your multi-server system a 'Star' structure?

If...	then...
no	go to Step 11.
yes, and this server is to be the Parent server,	a) Check the **Set as Parent Server** checkbox. The message *"Setting this as the Parent Server will disable communication with all other servers. Do you wish to continue?"* displays.

If...	then...
	b) Click the **Yes** button. The Aggregation fields become disabled. c) Go to Step 13.

11. To receive all cardholder location changes from this remote server, check the **Receive all Cardholder location changes from this remote server** checkbox.
    Notes:
    - This is usually only used for the purpose of Evacuation Reporting. Enabling this feature will cause increased network traffic.
    - This setting is not replicated to other sites, as it is up to the operators of those other sites to decide if they wish to receive cardholder location information from the new server, and check the checkbox.
12. Do you want to enable event aggregation?

If...	then...
yes	refer to ***Event Aggregation*** (on page 49-14) for the procedure.
no	go to Step 12.

13. To make the initial connection to the Remote Server, click the **Apply** button.
    Note: A message will display if a connection cannot be established, for any of the following reasons:
    - the Remote Server is not running.
    - the Remote Server is inaccessible because of some firewall or network configuration.
    - the Remote Server does not have a compatible license, or is not running a compatible version of Command Centre.
    - the Remote Server has already been added to the system.
    - the Remote Server's certificate was not trusted by the system. If the certificate is correct, then click the **Yes** button and the Remote Server's certificate will be added to the list of trusted certificates.

Create a 'Remote Server' for Server 1 on Server 2

14. Repeat Steps 2 - 10 from Server 2's workstation to create a Remote Server Command Centre item for Server 1.

Wait for Replication to complete

If the initial connection was successful, the servers will begin replicating their configuration.
Note: Replication can take quite a while.

15. To monitor the progress of the replication, click the **Status and Overrides** tab of the Remote Server's property pages.
    During replication, the following progress messages appear in the **Status** field:

Message	Description
"<number> change(s) waiting to be replicated"	This is the number of changes on the remote server that have not yet been replicated to the local server. It may be greater than zero after servers are reconnected after being offline if changes were made.
"<number> change(s) waiting to be applied"	This is the number of changes that have been replicated to the local server but have not yet been applied. It may be greater than zero due to temporary delays in replication, or dependencies on not yet replicated changes, etc.

Configure Operator Privileges

Initially, operators will only have access to the server they were created on. To give operators access to multiple servers if required, follow the steps below:

16. Create and configure an Operator Group entirely on the remote server (including divisions and privileges). Then from the local server, using the System Operator, drag the operators on to the **Cardholders (Operators)** tab of the Operator Group.

    See ***Setting up Operator Groups*** (on page 36-5) for further detail.

Result

A Remote Server has been created.

Hints

Deleting Remote Servers
Remote servers can be removed from a multi-server system, providing the license file contains `MultiServerRemoval=1` and the operator has the "Advanced User" privilege in the appropriate division.

In a 'Star' structure, child servers cannot delete other servers. Only parent servers can delete a child server from the system.

Refer to Deleting ***a server from a Peer-to-Peer structure*** (on page 49-22) or Deleting ***a child server from a Star structure*** (on page 49-23) as appropriate for the procedure.

Switching from Peer-to-Peer structure to Star structure

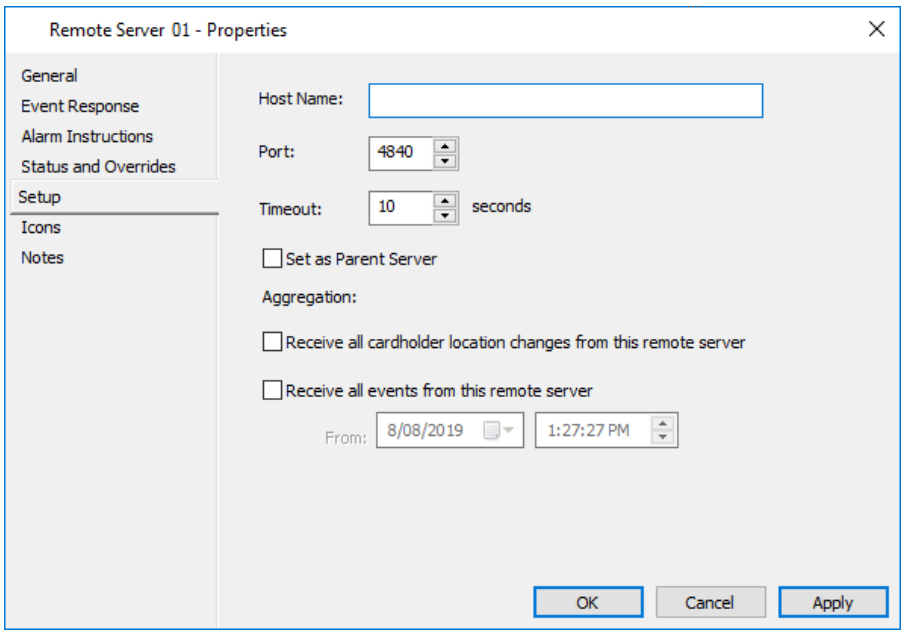
Introduction

To suit operational needs better, sites with a large number of servers may want to switch their current system from 'Peer-to-Peer' structure to 'Star' structure.

This procedure describes how to switch a 'Peer-to-Peer' structured multi-server system to a 'Star' structure.

Procedure

1. Click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens.
2. **Right click** on the Remote Server that you want to have as the Parent Server, (i.e. all other remote servers in the system will communicate with that server only).
3. Click the **Setup** tab.



4. Check the **Set as Parent Server** checkbox.
   The following message displays:

   "Setting this as the Parent Server will disable communication with all other servers. Do you wish to continue?"
5. Click the **Yes** button.
   The Aggregation fields become disabled.
6. Click the **OK** button.

Switching from Star structure to Peer-to-Peer structure

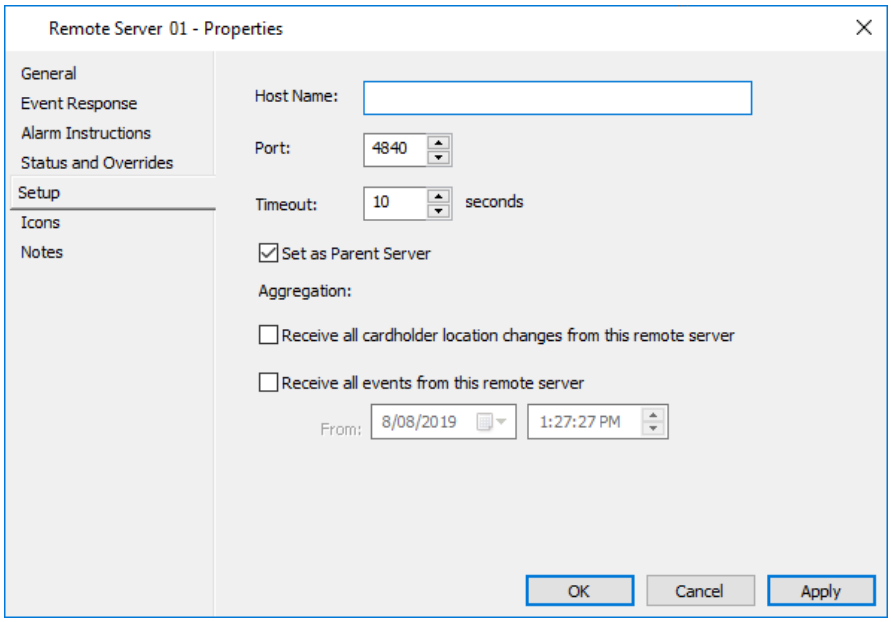
Introduction

A site may want to switch from a 'Star' structure back to a 'Peer-to-Peer' structure if the wrong server was set as the Parent, and therefore needs to be reset.

This procedure describes how to switch a 'Star' structured multi-server system to a 'Peer-to-Peer' structure.

Procedure

1. Click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens.
2. **Right click** on the Remote Server that is currently set as the Parent Server, and click **Properties**.
3. Click the **Setup** tab.



4. Uncheck the **Set as Parent Server** checkbox.
   The following warning message displays:

   "Un-selecting Parent Server option means communications with every other remote server will be completely enabled again. Do you want to continue?"
5. Click the **Yes** button.
   The Aggregation fields become enabled.

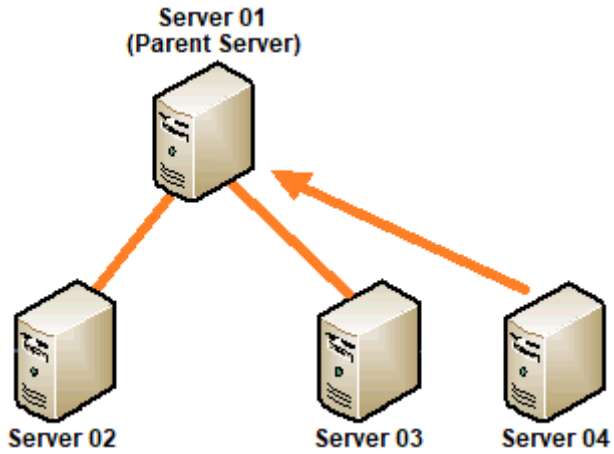
   Note: The local server can only have one parent server. Therefore, once a remote server has been made the parent server, the **Set as Parent Server** checkbox becomes disabled for all other remote servers (existing or new).
6. Click the **OK** button.

Adding a new server to a Star structure

Introduction

This procedure describes how to add a new remote server (as a child server of the parent server), to a 'Star' structured multi-server system.

For example: Server 02 and 03 are already children of Server 01, and you want to add new Server 04 as a child of Server 01 also.



Note: Adding a new child server to a 'Star' structure requires a new remote server to be created on the parent server and the parent server to be created on the new child server.

Procedure

Creating new child server

1. On the parent server, click **Configure** from the menu bar, then **Services & Workstations**. The **Services and Workstations** List Window opens.
2. **Right-click** and select **New…Remote Server**.
   By default the **General** tab displays.
3. Enter the **Name o**f the new child server, (e.g. Server 04).
4. Click the **Setup** tab.
5. Enter the IP address of the new remote server in the **Host Name** field. (Limit = 255 characters)
6. Click the **OK** button.

Creating parent server on new child server

7. On the new remote server, click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens.

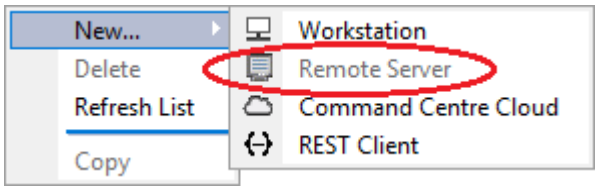
8. **Right-click** and select **New…Remote Server**.
   By default the **General** tab displays.
9. Enter the **Name o**f the parent server, (e.g. Server 01).
10. Click the **Setup** tab.
11. Enter the IP address of the parent server in the **Host Name** field.
    (Limit = 255 characters)
12. Check the **Set as Parent Server** checkbox.
    The following message displays:

    "Setting this as the Parent Server will disable communication with all other servers. Do you wish to continue?"
13. Click the **Yes** button.
    The Aggregation fields become disabled.
14. Click the **OK** button.

Result

A new Remote Server has been added to a 'Star' structured multi-server system as a child server.

Note: The **Remote Server** option is now disabled, as remote servers cannot be added to a child server.



Overriding a Remote Server

Introduction

This procedure describes how to temporarily override a Remote Server. Operators with permission to perform local overrides will be able to trigger a remote override.

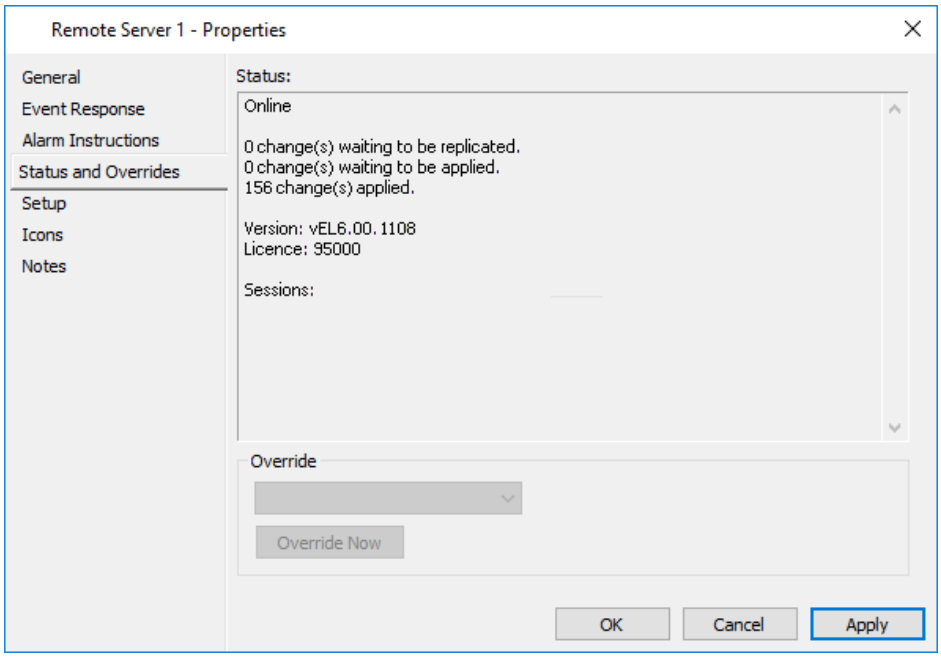
Note: Overriding a child remote server is not allowed in a 'Star' structured multi-server system.

Procedure

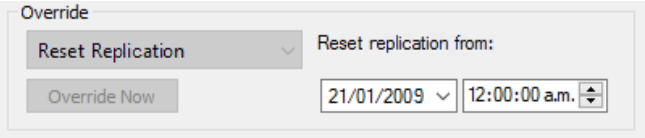
1. Click **Configure** from the menu bar, then **Services & Workstations**. The **Services and Workstations** List Window opens (in grid view).
2. Highlight the Remote Server you want to override.
3. Either:
   - **Right click** and select **Properties,** then click the **Status and Overrides** tab.

   OR

   - **Right click** and select **Override...**
     The **Status and Overrides** tab displays.



4. Click within the **Override** field and select the required override action from the drop-down list:
   Note: "Advanced User" privilege is needed to perform an **Accept Certificate** override, while "Maintenance Override" privilege is needed for the other three types of remote server overrides.

Option	Description
Disable Communication	Stops communication with the Remote Server.
Enable Communication	Resumes communication with the Remote Server.
Accept Certificate	When selected, a **View Certificate** button appears to the right of the overrides list. Clicking this button displays the remote server's certificate using a standard Windows certificate dialog. Starting the override will cause the local server and any other servers trusted by the local server to start trusting the remote server's current certificate. This only needs to be done if the status of the remote server is "The Remote Server does not have the correct certificate". **Note:** You will not be able to start the **Accept Certificate** override if the local server already trusts the remote server's certificate.
Reset Replication	When selected, extra date and time controls appear for setting when you require replication to start from:  The time displayed by default is today at midnight. If you start the override then all changes since that date and time will be re-retrieved from the remote server(s). Any changes that have not previously been received will be applied.

5. Click the **Override Now** button.

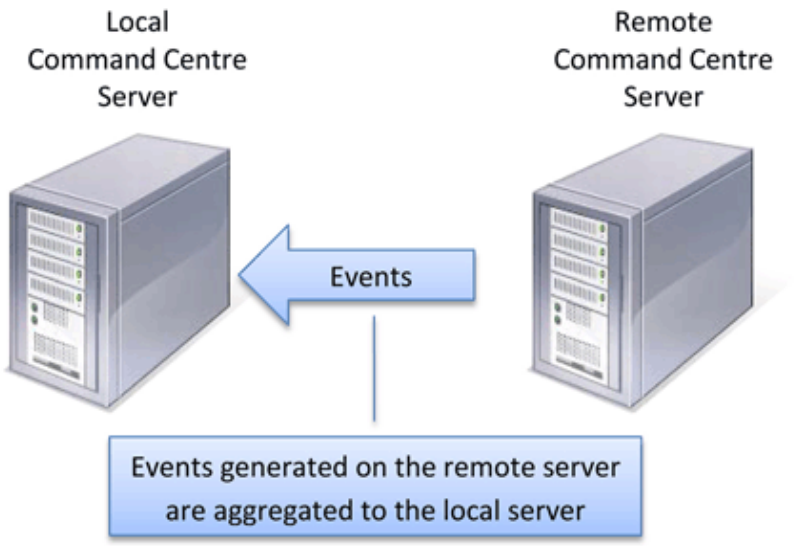
Result

The Remote Server has been overridden. Disable and Enable Communication overrides remain in place until the override is manually cancelled.

Event Aggregation

Introduction

In a multi-server environment, event aggregation allows remote server events to be aggregated on the local server. This allows for centralized reporting and provides a central location for event backup and data maintenance purposes.



Note: The events that are displayed to an operator will depend on the operator's privileges.

Network Disconnection

If an event aggregation server is offline, remote server events will be aggregated at the earliest time possible upon restoration of the device. The Status and Overrides tab of a Remote Server item indicates the number of events waiting to be aggregated.

Archived Events

Remote server events that have been archived and deleted will not be aggregated to the local server. Only events in the remote event database are available for aggregation.

In 'Star' structured multi-server systems:

- child servers can receive/view local events only.
- The parent server can receive events from all child servers.
- A child server cannot aggregate events from the parent server or other child servers.
- Once a server becomes a child server, it must log off and log back in again. Otherwise the child server can still see the events from other servers just like the parent server.

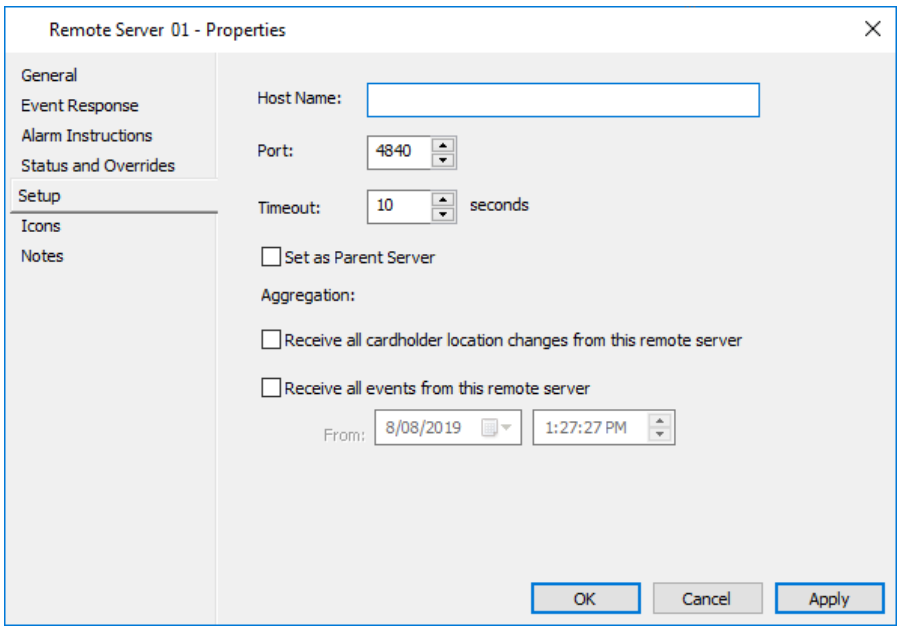
Before you begin

- You will need to have a multi-server environment installed and configured before enabling event aggregation.
- All servers must be on the same build of Command Centre. All servers must be on Command Centre vEL7.10 or later.
- You will need to nominate a server that will receive events from the remote server(s). This nominated server is referred to as an event aggregation server. Any number of servers can be nominated as event aggregation servers. An event aggregation server will receive events from all remote server(s) that have been configured to aggregate events (via the **Setup** tab of each remote server).

Procedure

To enable event aggregation, perform the following procedure on the event aggregation server:

1. Click **Configure** from the menu bar, then **Services & Workstations**. The **Services and Workstations** List Window opens (in grid view).
2. Highlight the Remote Server you want to receive events from.
3. **Right click** and select **Properties**.
4. Click the **Setup** tab.



5. Check the **Receive all events from this remote server** checkbox.
6. The **From** date indicates the date that all events (that are not 'archived and deleted') will aggregate from.
   What events do you want aggregation to apply to?

If...	then...
past events,	set the date/time control to the required date in the past. This causes historical events to commence aggregation 'from this past time' forward.
all future events,	leave the date/time control as the current date. All events 'from this current time forward' will commence aggregation.

Note: The **From** date can only ever be applied as a current or past date. Setting the date in the future generates an error message.

7. To commence aggregation, click the **Apply** button.

Viewing the number of events waiting to be aggregated

To view the number of events waiting to be aggregated from the remote server, click the **Status and Overrides** tab of the Remote Server's property pages.
When event aggregation is enabled, the following message displays in the **Status** field:

Message	Description
"<number> event(s) waiting to be aggregated."	This is the number of events on the remote server that have not yet been aggregated to the local server.

8. Repeat Steps 2 - 7 for each server you want to aggregate events for.
   Note: Event aggregation can be stopped at any time by unchecking the **Receive all events from this remote server** checkbox and applying the change. If re-enabled, no duplicate events will be aggregated.

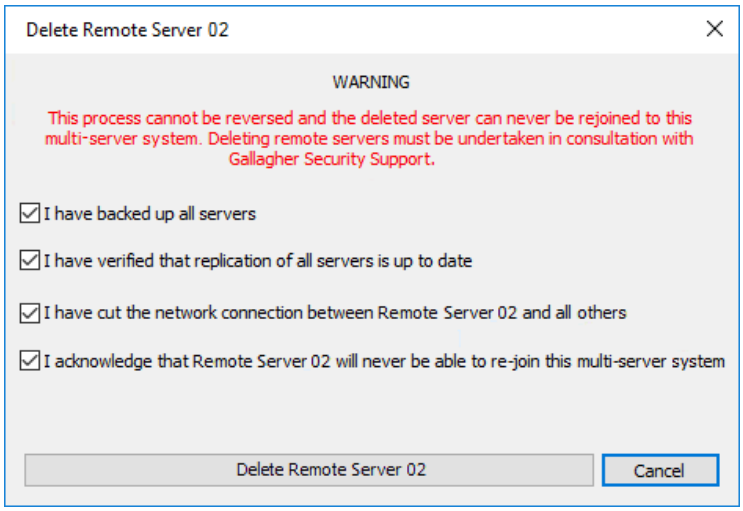
Deleting a server from a Peer-to-Peer structure

Introduction

In a 'Peer-to-Peer' structure, a remote server can be removed from the system, providing the license file contains `MultiServerRemoval=1`, and the operator has the "Advanced User" privilege in the appropriate division.

Procedure

1. Check all servers are online, and the time is synced on all of them.
2. Make sure there are no pending updates of each server, and backup all the servers in the multi-server system.
3. Disconnect the network on the server to be deleted.
   Note: NOT disable communications.
4. Shutdown the server to be deleted.
5. From a server in the multi-server system, click **Configure** from the menu bar, then **Services & Workstations**.
   The Services and Workstations List Window opens.
6. Highlight the remote server you want to delete.
7. **Right click** and select **Delete**.
   A warning window displays with a checklist of the actions that need to be performed prior to deleting the server.



8. Go through the checklist and tick each checkbox to indicate the action has been completed, and click the **Delete <Remote Server>** button.
   Notes:
   - It is recommended that operators do not add, delete or modify items (including cardholders) in a multi-server environment on any servers while running the deletion process.

- The deletion process can be monitored by opening the properties of the server which is performing the deleting function.

9. Backup all the servers in the multi-server system again.

Result

The server is deleted and disappears from the Services and Workstations List Window.
Note: Sometimes it takes a few minutes depending on how many items the server has to process.

All hardware and hardware related items from the deleted server are removed, (e.g. hardware components, Access Zones, Alarm Zones, Doors), and all other items are moved to the parent server, (e.g. Cardholders, Card Types, Access Groups, Operator Groups).

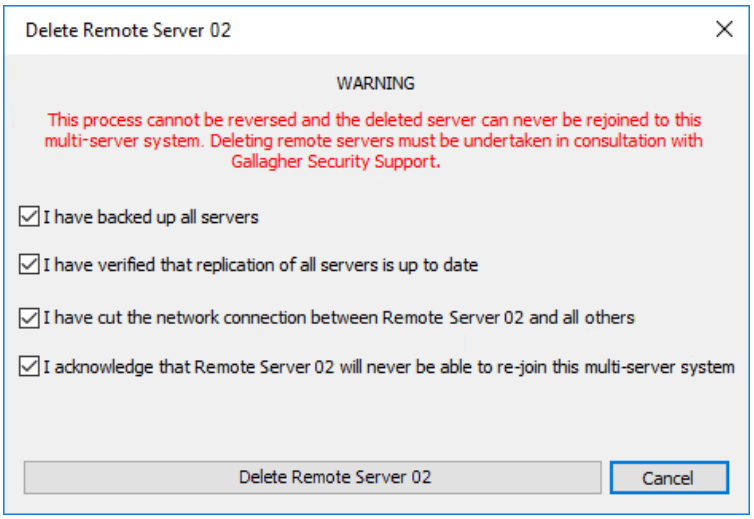
Deleting a child server from a Star structure

Introduction

In a 'Star' structure, child servers cannot delete other servers. Only parent servers can delete a child server from the system, providing the license file contains `MultiServerRemoval=1`, and the operator has the "Advanced User" privilege in the appropriate division.

Procedure

1. Check all servers are online, and the time is synced on all of them.
2. Make sure there are no pending updates of each server, and backup all the servers in the multi-server system.
3. Disconnect the network on the server to be deleted.
   Note: NOT disable communications.
4. Shutdown the child server to be deleted.
5. From the parent server in the multi-server system, click **Configure** from the menu bar, then **Services & Workstations**.
   The Services and Workstations List Window opens.
6. Highlight the child server you want to delete.
7. **Right click** and select **Delete**.
   A warning window displays with a checklist of the actions that need to be performed prior to deleting the server.



8. Go through the checklist and tick each checkbox to indicate the action has been completed, and click the **Delete <Remote Server>** button.
   Notes:
   - It is recommended that operators do not add, delete or modify items (including cardholders) in a multi-server environment on any servers while running the deletion process.

- The deletion process can be monitored by opening the properties of the server which is performing the deleting function, (i.e. the parent server).
- Once the deletion process is finished, all child servers need a RESTART to remove all cached FT items from memory.

9. Backup all the servers in the multi-server system again.

Result

The child server is deleted and disappears from the Services and Workstations List Window.
Note: Sometimes it takes a few minutes depending on how many items the server has to process.

All hardware and hardware related items from the deleted server are removed, (e.g. hardware components, Access Zones, Alarm Zones, Doors), and all other items are moved to the parent server, (e.g. Cardholders, Card Types, Access Groups, Operator Groups).

Chapter 50: Visitor Management

Introduction

Visitor Management is a visitor management access control system.

Visitor Management is closely integrated with Gallagher Command Centre and is configured by your Command Centre administrator to meet the requirements of your business.

Visitor Management is a mechanism for supporting visitors to companies:

- with single receptions
- with multiple locations (sites)
- with multiple receptions
- in tenanted buildings, where there is a building reception and company reception using the same Command Centre system.

It can be used to: identify visitors, print visitor badges, issue visitor access cards, assign escorts to visitors, manage visitors and create visitor reports.

Licensing

Visitor Management is a licensable feature. Customers requiring the Visitor Management application must purchase a Visitor Management license enabling them to configure Gallagher Command Centre for Visitor Management, as follows:

```
[Features]
VisitorManagement=1
```

Access to the Receptionist Visitor Management client will be controlled by a workstation license within Command Centre. This will be a concurrent workstation license which operates across the suite of Command Centre applications. Visitor Management Pre-registration users do not require a workstation license.

To use the 'Visit Count' licensable feature, the license must also contain the following option:

```
[Features]
VisitCounting=1
```

Roles in Visitor Management

There are a number of roles involved in the Visitor Management module:

Role	Description
Systems Administrator	The person who is responsible for configuring and managing Visitor Management in Command Centre. They have the ability to add, delete and modify user accounts and user privileges.

Role	Description
Receptionist	The person who will be stationed in a Reception area where they will: • greet visitors, • contact the escorts, • mark visitors on and off site, and • provide name badges and access cards for the visitors
Host	A member of the company with whom a visit may be arranged, or who is authorised to escort visitors. They will pre-register a visit, (i.e. book a meeting), with one or more visitors. The "Host" role can be further split into: • "Meeting with", (i.e. the person a visitor plans to see on their visit), and • "Escort", (i.e. someone who escorts a visitor to the person they are visiting).
Visitor	The person who visits a site to meet with someone, (i.e. the escort). **Note:** This can be a permanent cardholder.
Gallagher Operator/Guard	The person operating the Command Centre system and monitoring alarms. As part of this function they will manage "overdue visitors".

This chapter covers the following topics:

- ***Visitor Management Application Installation Instructions*** (on page 50-3)
- ***Command Centre Site Configuration*** (on page 50-6)
- ***Using Visitor Management*** (on page 50-66)
- ***Visitor Management Barcode Scanner Process*** (on page 50-148)
- ***Visitor Management Passport/Drivers License Scanning Process*** (on page 50-161)

Visitor Management Application Installation Instructions

Introduction

Initial installation of the Visitor Management application should be performed by a user who has administrative rights on both the server and client PC. The Visitor Management client then needs to be installed by each user individually, (i.e. there is no option to install for all users of the client PC). These subsequent Visitor Management client installs do not need to be performed by Administrators, the users just need to have access to the `VMClientUpdate` shared folder on the server, (i.e. `\\[ServerName]\VMClientUpdate`). **Notes:**

- This procedure is for a clean install of Visitor Management **only**. If you are upgrading from a previous version, refer to the Command Centre Release Note provided with the installation files for the upgrading instructions.
- It is recommended that you run the Visitor Management Server Installer locally, (i.e. not across the network).

Before you begin

Before installing the Visitor Management Application log on to the server machine as an Administrator.

Procedure

The following procedure for installing the Visitor Management application has been split into two parts:
- Server Installation, and
- Client Installation.

Server Installation

1. Install Gallagher Command Centre.
   Refer to the appropriate release note on the Gallagher Command Centre installation DVD, (i.e. either the "New Installations" release note or the "Upgrade Procedures" release note), for the procedure.
2. At the time Command Centre is installed, the Visitor Management Client is automatically built to the default location of `'C:\Program Files\Gallagher\Command Centre\VMClient\VMClientUpdate'`. Although we recommend sites leave the Visitor Management Client in this default location with the default TCP port, it can be built to a different location and/or run on a different TCP port. Do you want to build it to a different location or change the TCP port?

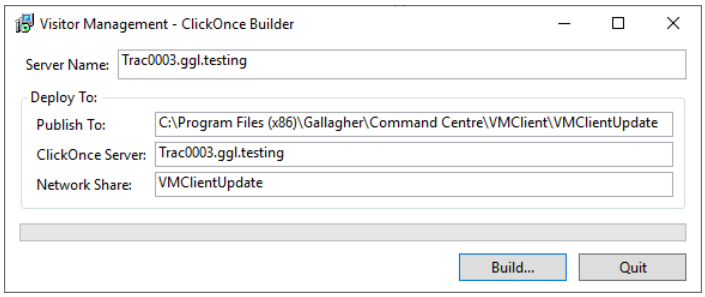
If…	then…
no	the Server Installation is complete. Go to the **Client Installation** procedure below.
yes	go to Step 3.

3. If you would like to change the TCP port, complete the following steps:
   a) Open the **Command Centre Server Properties** window.
   b) Click the **Web Services** tab.
   c) Change the port in the **Server Base Port** field.

d) Click **OK** to exit and save your changes.
IMPORTANT: If the TCP port is changed, The Visitor Management - ClickOnce Builder configuration file will also need to be modified, as follows:

a) Go to the `'C:\Program Files\Gallagher\Command Centre\VMClient\Files'` folder.
b) Open the **VMCABClient.exe.config** file, in the <appSettings> section, modify the port value to match the Server Base Port:
<add key="Port" value="4243"/>
c) Save the file and proceed to Step 4.

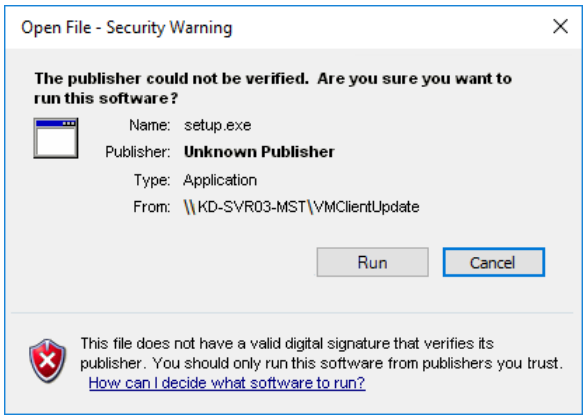
4. Go to the `'C:\Program Files\Gallagher\Command Centre\VMClient'` folder and double-click on **ClickOnceBuilder.exe**.
The Visitor Management - ClickOnce Builder screen displays.



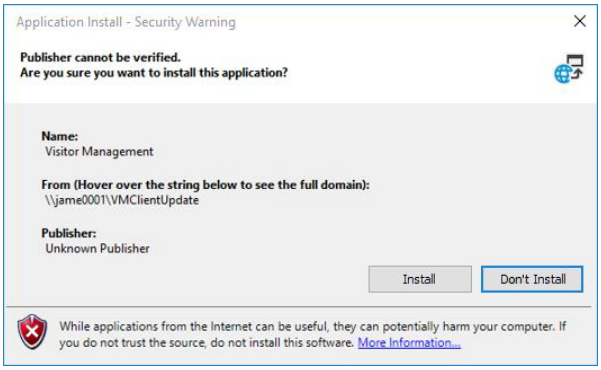
5. Change the 'Deploy To' settings to the required location if the location has changed, and click the **Build…** button.
The Client build may take a few minutes.
Note: ClickOnce supports deployment via HTTP/HTTPS. You can specify a URL instead of a machine name for the **ClickOnce Server** name.
6. Ensure the folder indicated in the **Publish To** field is shared, and the path is set correctly in the **Network Share** field. This allows the Visitor Management application to be installed on other computers.
7. Click the **Quit** button.

Client Installation

1. Browse to the **`VMClientUpdate`** shared folder on the server, (i.e. `\\[ServerName]\VMClientUpdate`).
2. Run the Visitor Management installation executable, (i.e. **ClickOnceVisitorManagementSetup.exe**).
The following Open File Security Warning displays:

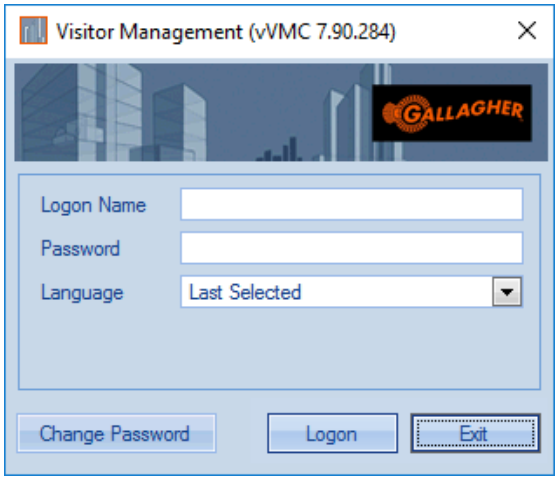


3. Click the **Run** button.
4. Does the following Application Install - Security Warning screen display?



If...	then...
yes	go to Step 6.
no	Microsoft .NET Framework 4.5 is not installed on the PC, which is needed for Visitor Management. A License Agreement dialog displays for the application(s) which is not installed. **Note:** If only one License Agreement dialog displays, then the other application is already installed.

5. Click the **Accept** button to accept the license agreement.
   A series of dialog boxes display indicating which application(s) is being installed, followed by the Application Install Security Warning screen displaying (shown at Step 4).
6. Click the **Install** button.
   The Visitor Management application installs, and launches automatically.



Notes:

- Command Centre needs to be configured before any users can log on to the Visitor Management application.
- It is recommended that you create a shortcut on your desktop for the Visitor Management application.

Command Centre Site Configuration

Introduction

The following process is recommended so you perform each activity in the correct order when setting up Visitor Management for your site, and therefore the relationships between the various entities in Command Centre are maintained.

Where necessary, this process refers to step-by-step procedures that are either detailed in this section or elsewhere in this document.

Notes:

- Functionality specific to Visitor Management is only available in Command Centre if your site is licensed for Visitor Management.
- Visits that have been created in the Visitor Management application can be viewed in Command Centre. This is not part of the configuration process, but may be of use. See ***Viewing Visits*** (on page 50-48) for details.
- Many actions performed in the Visitor Management application will generate events and/or alarms in Command Centre. See the Event Viewer and Alarm Viewers sections for details on how to process these alarms.
- An automated purge will run daily to purge expired visits from the system. See ***Purging Expired Visits*** (on page 50-53) for details.
- In a multi-server system that uses Visitor Management, visit data does not get replicated between servers. Therefore, the Evacuation Report cannot report on remote visitors.

Configuration Process

The configuration required in Command Centre involves a number of procedures:

Note: This list can be used as a checklist to ensure you have configured all the necessary components for Visitor Management.

"System" related	✓	Procedure
Base system configuration (mandatory)	☐	***Create Cardholder Division*** (on page 50-8)
	☐	***Create Visitor Division*** (on page 50-8)
	☐	***Create a Reception*** (on page 50-9)
	☐	***Assign Reception Workstation(s)*** (on page 50-11)
	☐	***Define Visitor Types*** (on page 50-13)
	☐	***Define Host Types*** (on page 50-13)
	☐	***Configure Visitor Management set up*** (on page 50-15)

"System" related	✓	Procedure
If you intend using image capture device(s) other than the default	☐	See ***Using Image Capture Devices*** (on page 50-40) for supported devices
If you intend scanning business cards	☐	Configure the fields to be displayed on the ***Cardscan Configuration tab*** (on page 50-25)
If you intend printing badges	☐	***Create a Card Type*** (on page 50-41)
	☐	***Add Visitor details to cards/badges*** (on page 50-42)
If access cards are to be issued	☐	***Configure Access Groups*** (on page 34-4)
If Reception readers are going to be used	☐	***Configure Doors*** (on page 50-44)
If Macros will be available for a Receptionist	☐	***Configure Macros*** (on page 50-45)

"People" related	✓	Procedure
Allow permanent cardholders to be visitors.	☐	***Assign to Cardholder Division*** (on page 50-46)
If you require contact details for "Host" Cardholders	☐	***Add Contacts to "Host" Cardholders*** (on page 50-47)
Assign privileges to cardholders able to pre-register visits.	☐	See ***Configuration Examples*** (on page 50-54) for recommended Operator Groups
Assign privileges to Receptionists who can create/edit visits and Visitors and perform the Visitor Management actions.	☐	See ***Configuration Examples*** (on page 50-54) for recommended Operator Groups
Assign privileges to Receptionists who can only view Visit and Visitor details. They cannot perform the Visitor Management actions.	☐	See ***Configuration Examples*** (on page 50-54) for recommended Operator Groups

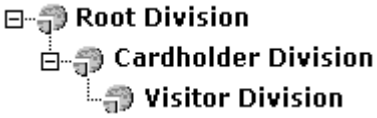
Creating Divisions

Introduction

The **Cardholder Division** should contain all permanent cardholders who can be visitors.

The **Visitor Division** is the division in which visits and visitors for a reception will be created automatically by the system.

The **Visitor Division** should be a child division of the **Cardholder Division**.



See ***Configuration Examples*** (on page 50-54) if installing Visitor Management on a site with multiple tenants.

Procedure

This procedure allows you to provide the minimum information required to create a new Division.

1. Click **Configure** from the menu bar.
2. Click **Divisions**.
   The **Division** List Window opens.
3. **Right click** and select **New...Division**.
   By default the **General** tab displays.
4. Type the appropriate name in the **Name** field, for the type of division you are creating, (i.e. either "Cardholder Division" or "Visitor Division").
5. Click the **Lineage** tab.
6. What type of division are you creating?

If a...	select from the 'Immediate Parent' drop-down list...
Cardholder Division	"Root Division".
Visitor Division	"Cardholder Division".

7. Click the **OK** button.
   The new division is created, and appears on the **Division** List Window, (i.e. the "Cardholder Division" appears as a child division of the "Root Division", and the "Visitor Division" appears as a child division of the "Cardholder Division").

Creating a Reception

Introduction

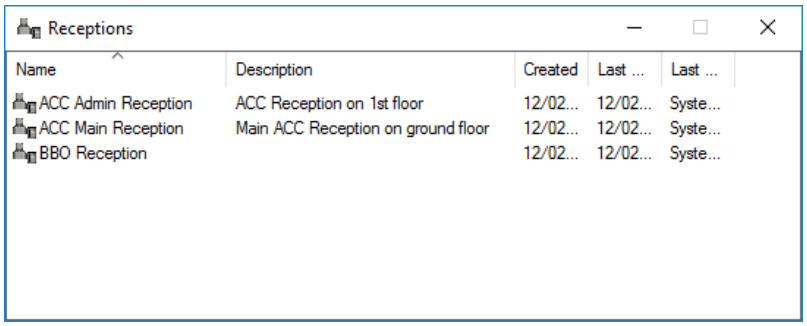
This procedure describes how to create a Reception in Command Centre.

Operator Privileges

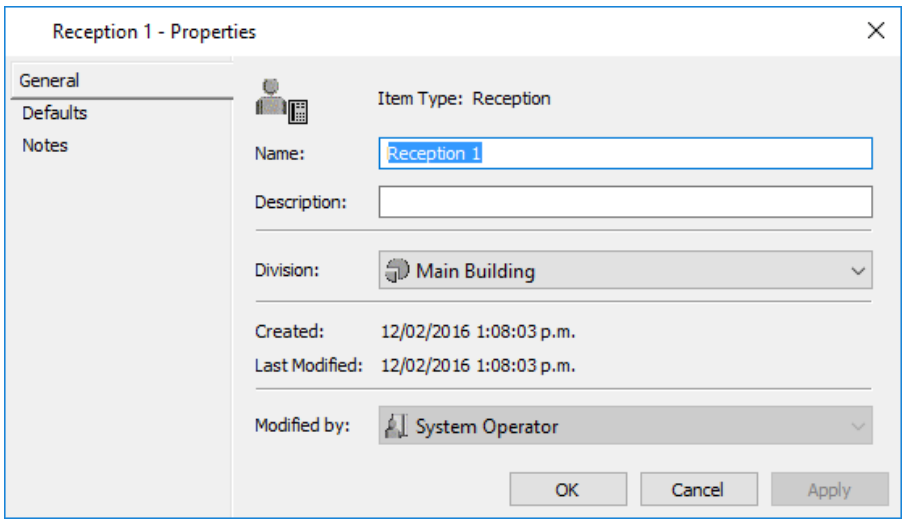
Privilege	is required to...
“View Site”, "View Visits", "Edit Visits" or "Manage Receptions"	view a Reception's properties.
“Edit Site”	create and/or change a Reception's properties.

Procedure

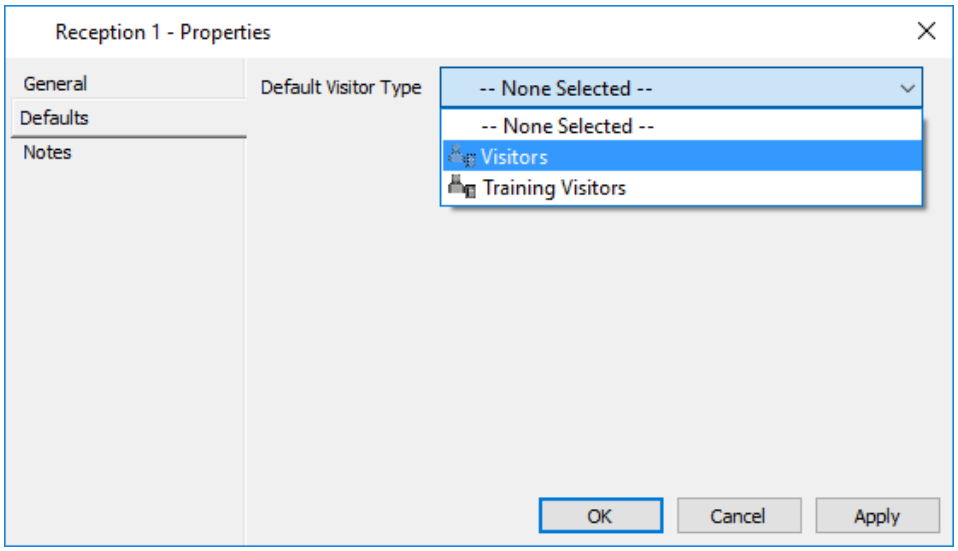
1. Click **Configure** from the menu bar.
2. Click **Receptions**.
   The **Receptions** List Window opens, displaying the Receptions that the operator can view or edit.



3. **Right click** and select **New…Reception**.
   By default the **General** tab displays.



4. Type in a **Name** for the Reception and a logical **Description**.
   Note: Use meaningful names for Receptions, as they will appear throughout the Visitor Management application.
5. Assign the Reception to a Division.
   Notes:
   - Each Reception can only be assigned to a single division.
   - Divisions are used to configure the way the Visitor Management application operates for each Reception. Receptions that share the same configuration should be held in the same division, (i.e. usually in the **Visitor Division**, however for more complicated setups refer to ***Configuration Examples*** (on page 50-54) to determine which division the Receptions should be assigned to).
   - Receptions should be saved in the Division with the configuration.
6. Do you want to configure a default visitor type for this Reception?
   If **yes**, go to Step 7.
   If **no**, got to Step 9.
7. Click the **Defaults** tab.



8. Select a **Default Visitor Type** from the drop-down list for this Reception. The visitor type selected will be used by default when creating a new visit in Visitor Management.
9. Click the **OK** button to exit and save your changes.

Deleting Receptions

A Reception can not be deleted if it is the:

- default reception for a Workstation (see ***Setting default Receptions for Workstations*** on page 50-11), or
- reception for a visit.

Setting default Receptions for Workstations

Introduction

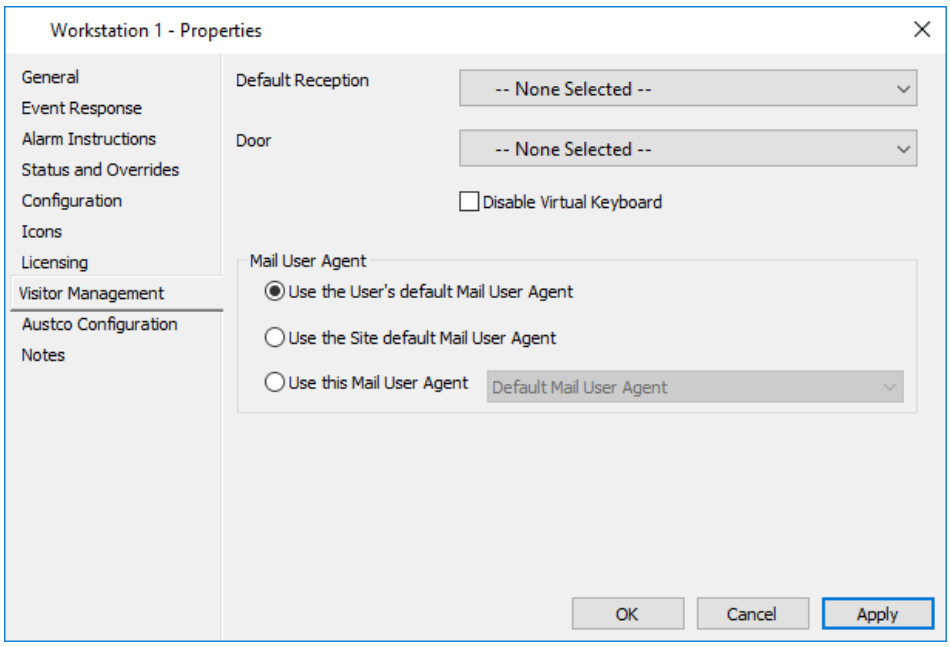
The default Reception that displays in the Visitor Management application (on the **Home** screen and when creating a new visit), when a Receptionist logs on is determined by the workstation they have logged onto.
This procedure allows you to set a default Reception for a workstation, and an associated door, as well as configure whether or not a physical or on screen (soft) keyboard will be used for Visitor Management Kiosk.

Operator Privileges

Privilege	is required to...
"Edit Site" or “View Site”	view this page.
“Edit Site”	edit properties.

Procedure

1. Click **Configure** from the menu bar.
2. Click **Services & Workstations**.
   The **Services and Workstations** List Window displays.
3. Select the Workstation you want to set the default Reception for.
4. **Right click** and select **Properties**.
   By default the **General** tab displays.
5. Click the **Visitor Management** tab.



6. From the **Default Reception** drop-down list, select the Reception that this workstation is located at.

   Note: This field is disabled if the operator does not have the privilege to edit the workstation.

7. The **Door** field allows you to assign the door that the Visitor Management application will monitor for card events. However, this cannot be done until you have created the door. Therefore, this step is covered later in ***Creating Doors*** (on page 50-44).
   Notes:
   - The door (reader) that you select enables the host to sign in at the kiosk, and the same door can be used to assign visitor cards.
   - Remote (multi-server) Doors can be selected.
   - It is recommended that you turn the readers sound off.

8. If the Kiosk is in an area that needs to be recorded for Evacuation Report purposes, then the reader must be configured as either the entry or exit reader (normally the former) on the Door assigned here.
   It is recommended that the site set up an Access Zone on the Kiosk Door, then give the Kiosk Host Access Groups access to that door, (i.e. put the Access Zone and Schedule on the actual Host Access Groups).
   We recommend sites do the following:
   a) Configure the Kiosk reader on the **Entry Zone** tab of the Kiosk's Door.
   b) Configure an Access Zone on the **Entry Zone** tab of the virtual Kiosk Door.
   c) Add the Access Zone to the Kiosk Admin and Host Type Access Groups (for the Kiosk Visitor Types), so that everyone in that Group will be granted access to the zone, and therefore will be able to sign in.

9. The Visitor Management Kiosk feature is touch screen capable and supports the use of a physical or on screen (soft) keyboard.
   If an external keyboard is going to be used for the Kiosk, check the **Disable Virtual Keyboard** checkbox to disable the soft (virtual) keyboard for the kiosk workstation.

   Note: It is recommended that if the kiosk is to have a physical keyboard, the virtual keyboard should be disabled.

10. The **Mail User Agent** section provides the ability to use the VM Operators client email to send an invitation to a Visitor during the Hosts Visit creation and edit process.
    Click the appropriate radio button if required.

11. Click the **OK** button.

Creating Visitor Type and Host Type Groups

Definitions

Visitor Types are used to determine the:
- details to be captured for a visitor of that type
- Host Types valid for a visitor of that type
- access which may be assigned to a visitor of that type
- layout of the badge to be printed for a visitor of that type

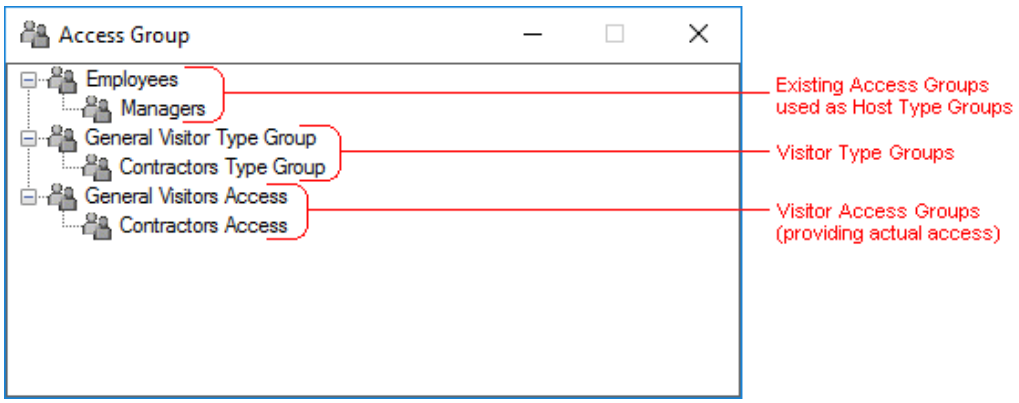
Host Types determine which cardholders may meet with or escort a visitor of a particular visitor type. A Host Type may be assigned to one or more Visitor Types, and more than one Host Type can be assigned to a Visitor Type.

Introduction

Visitor Types and Host Types are implemented in Command Centre using Access Groups. This procedure describes how to create an Access Group to be used as a Visitor Type Group or Host Type Group.

IMPORTANT:
Access Groups are typically used to control access to Access Zones. Access Groups created for Visitor Types cannot be used to control access to Access Zones. No real access should be assigned to Visitor Type Groups as they will be assigned to the visitors when they are added to the visit. They will not be removed from these groups when the visit is finished.

To avoid having to maintain Host Type Groups when new permanent cardholders get added to the system, existing Access Groups can be used as Host Type Groups. However, within Visitor Management, any one group cannot be a Visitor Type group, a Host Type group and the Visitor Access group, (i.e. the actual group that provides access for visitors). Therefore, if you do elect to use existing Access Groups as your Host Type Groups, you will need to create separate groups to provide visitors with access on site.



Procedure

To configure Access Groups which provide access to zones, use the ***Setting up Access Groups*** (on page 34-4) procedure. To configure Visitor Type and Host Type Groups, use the following procedure:
Note: Configuring Membership Defaults (on the **Cardholder Membership** tab) for a Visitor Type or Visitor Access access group is not recommended as Visitor Management adds and removes cardholders from Visitor Type and Visitor Access access groups on a daily basis.

1. Click **Manage** from the menu bar.
2. Click **Access Groups**.
   The **Access Group** List Window opens.
3. **Right click** and select **New...Access Group**.
   By default the General tab displays.
4. Enter an appropriate **Name** for the group.
   Note: Each Visitor Type Group should be given a meaningful name as this will appear in both the Command Centre configuration and in the Visitor Management application.
   If you have used existing Access Groups as your Host Type Groups, there is no need to alter these names.
5. Click the **OK** button to save the group.
6. Repeat Steps 3 to 5 for every Visitor Type and Host Type required.

Important

For Visitor Type Groups:

- Do **not** assign any cardholders. Instead, this is done when visitors are added to "Visits" in the Visitor Management application.
- When you get to the **Personal Data** tab, any Personal Data Fields (PDFs) that you assign to the Access Group must not have the "Required Field" checkbox checked on the **Type** tab of the PDF properties.

Configuring Visitor Management setup

Introduction

The configuration for a Reception is defined against a division. If your site has a single Reception this will be configured on the **Visitor Division** (created earlier for assigning available visitors for a visit). For all other setups refer to ***Configuration Examples*** (on page 50-54) to determine which division the Receptions should be configured on.

The configuration of a Reception determines the following options:

- Visitor Types available
- Visitor fields available: Visitor First Name, Visitor Last Name, Escort, Contacts, Notes, Personal Data Fields applicable to the Visitor Type
- Host Types (Meeting With) available
- Badge Texts available
- Access (access groups) available
- Actions available: Send Invitation, Sign In, Print badge, Assign access card, Assign escort, Mark On-Site, Mark Temp Off-Site and Mark Off-Site (Leave Site)
- Overdue grace period
- Time zone for a Reception
- Home screen columns and timeframe shown
- 'Find' screen columns
- Macros.

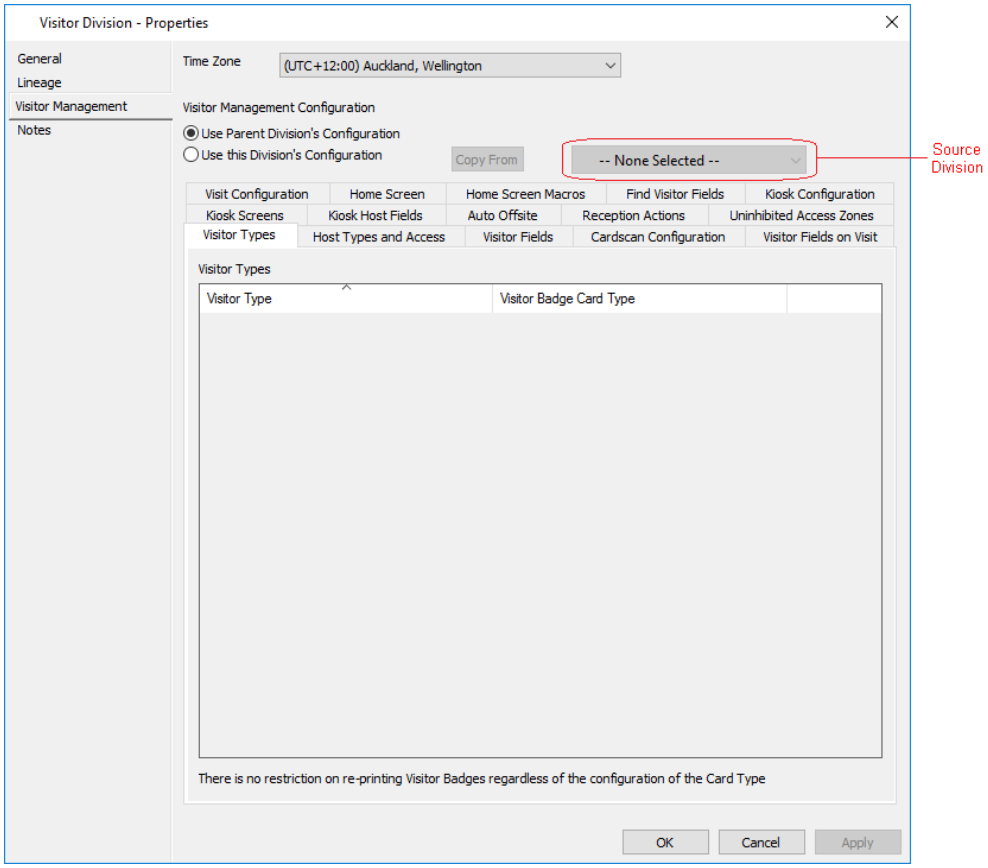
Operator Privileges

Privilege	is required to...
“Configure Site” or “View Site”	view this page.
"Configure Site"	edit properties.
"View Access Groups"	view the **Visitor Types** tab.
"View Cardholders"	see PDF's on the **Visitor Fields** tab and the **Visit Fields on Visit** tab.
"View Site"	see macros on the **Home Screen Macros** tab.

Procedure

1. Click **Configure** from the menu bar.
2. Click **Divisions**.
   The **Division** List Window opens.

3. **Right click** on the "Visitor Division", and select **Properties**.
4. Type in the Name and Description.
5. Click the **Visitor Management** tab.



This screen is split into two sections. The top section allows you to set the time zone and which Division's configuration to use in the Visitor Management application. The lower section of this screen has nine tabs for configuring the different features of the Visitor Management application.

6. Complete the fields in the top section as required:

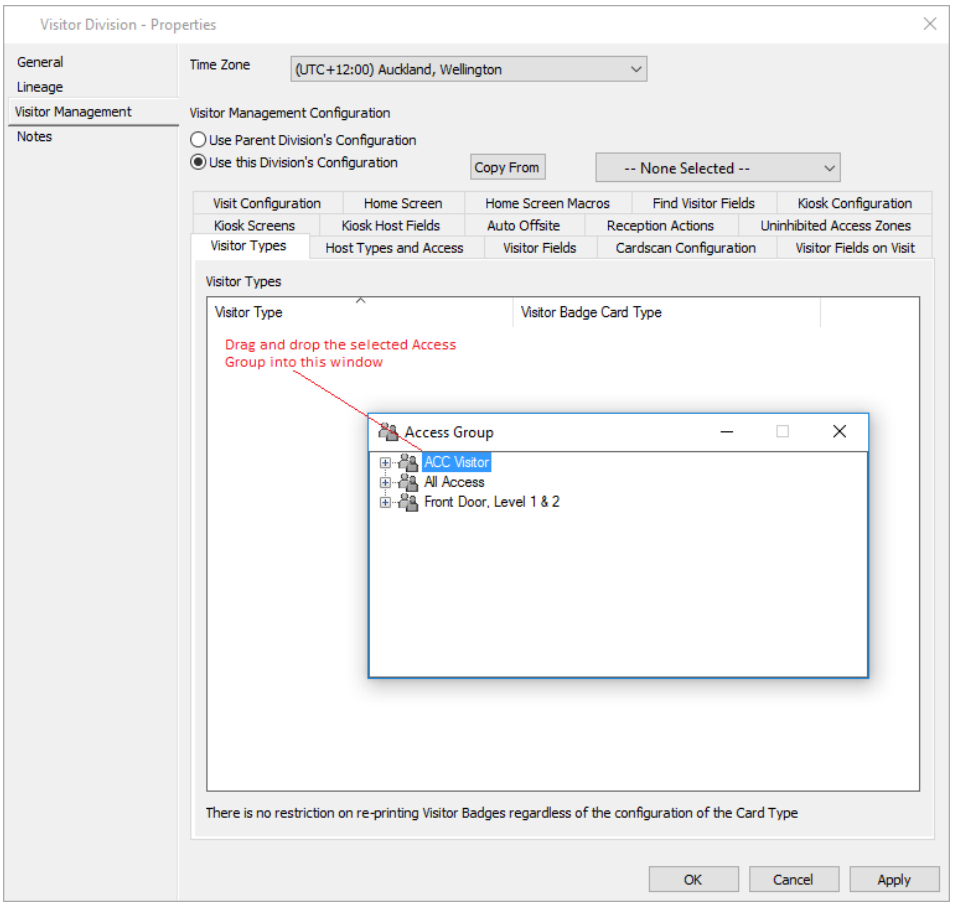
Field / Button	Description
Time Zone	A drop-down list of all the time zones that are installed on the computer. The time zone selected should be the one that receptions in this division are situated in. **Note:** You can create visits for Receptions in different time zones. (Default = The computer's time zone)
Use Parent Division's Configuration	Click this radio button if the parent division's Visitor Management configuration is to be used. (Default = Checked if the division is not the Root division) **Note:** When checked, the configuration options on

Field / Button	Description
	all the other tabs on this screen are disabled, as the properties will be defined on the Parent Division.
Use this Division's Configuration	This radio button should be set if this division's division Visitor Management configuration is to be used. (Default = Checked if the division is the Root division)
Copy From	This button copies the configuration from the division selected from the Source division drop-down list, preventing you having to repeat the set up.
Source Division	A drop-down list which allows the selection of a division. This is only available if the **Use this Division's Configuration** radio button is checked.

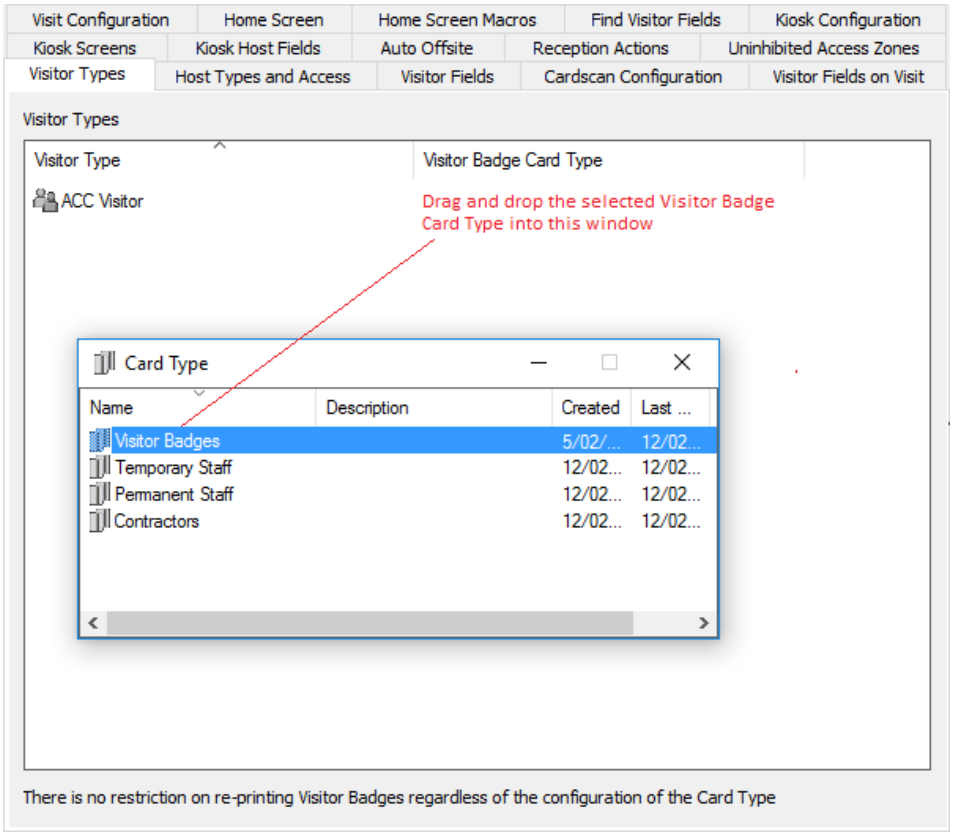
7. Which radio button did you select?

If the...	then...
Use Parent Division's Configuration	no further Visitor Management configuration is required, as this will be defined on the Parent Division.
Use this Division's Configuration	the **Visitor Types** grid on the lower section of this screen is enabled. Go to Step 8.

8. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens.
9. Select the Visitor Type Access Group that is applicable for the Reception(s) that are in this division, and drag and drop them into the **Visitor Types** tab, under the "Visitor Type" column.
   The Visitor Type(s) you include here will appear on the **Visit** screen for the Reception in the Visitor Management application.
   Note: The 'Root Division' is the exception, as it is envisaged it will not be used for Visitor Management configuration.

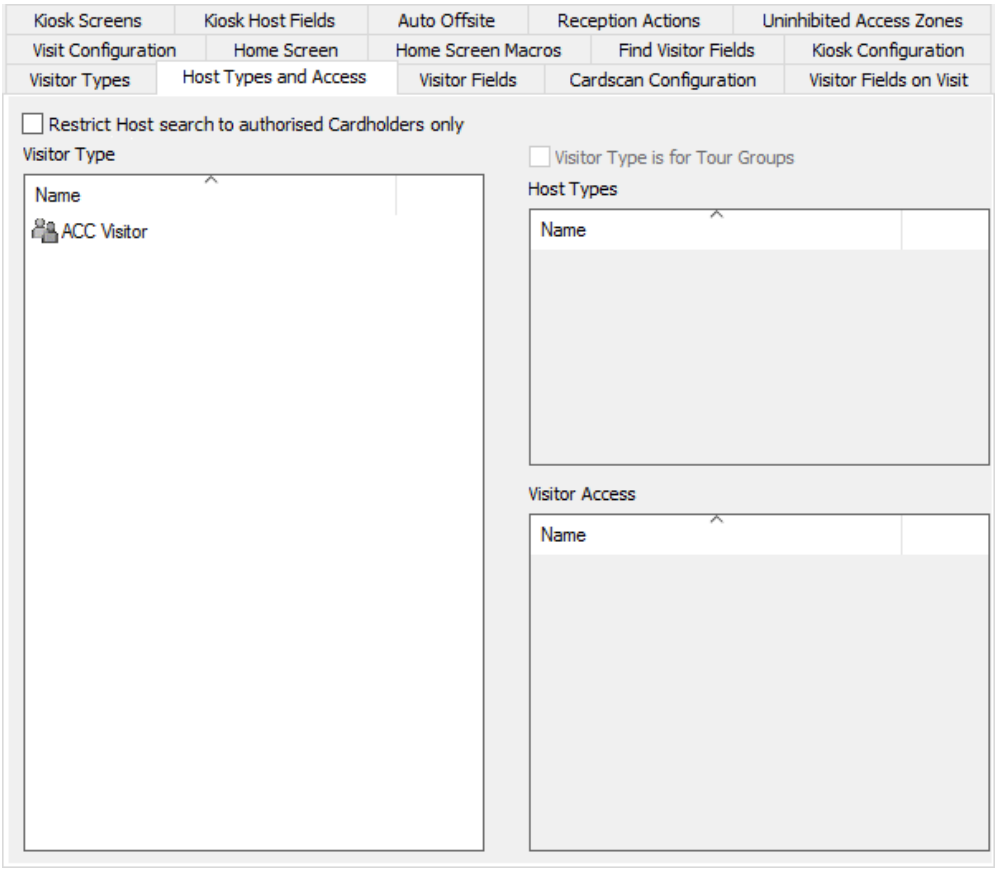


10. Close the **Access Group** List Window.
11. Select (highlight) a Visitor Type Group if you want to assign a Visitor Badge Card Type to this group, (i.e. if using the 'Print Badge' action).
12. Click **Configure** from the menu bar, then **Card Types**.
    The **Card Type** List Window opens.
13. Select the required Visitor Badge Card Type, and drag and drop it into the **Visitor Types** tab, under the "Visitor Badge Card Type" column.
    The Visitor Badge Card Types you include here specify the badge layout to be used for the visit for that Visitor Type.



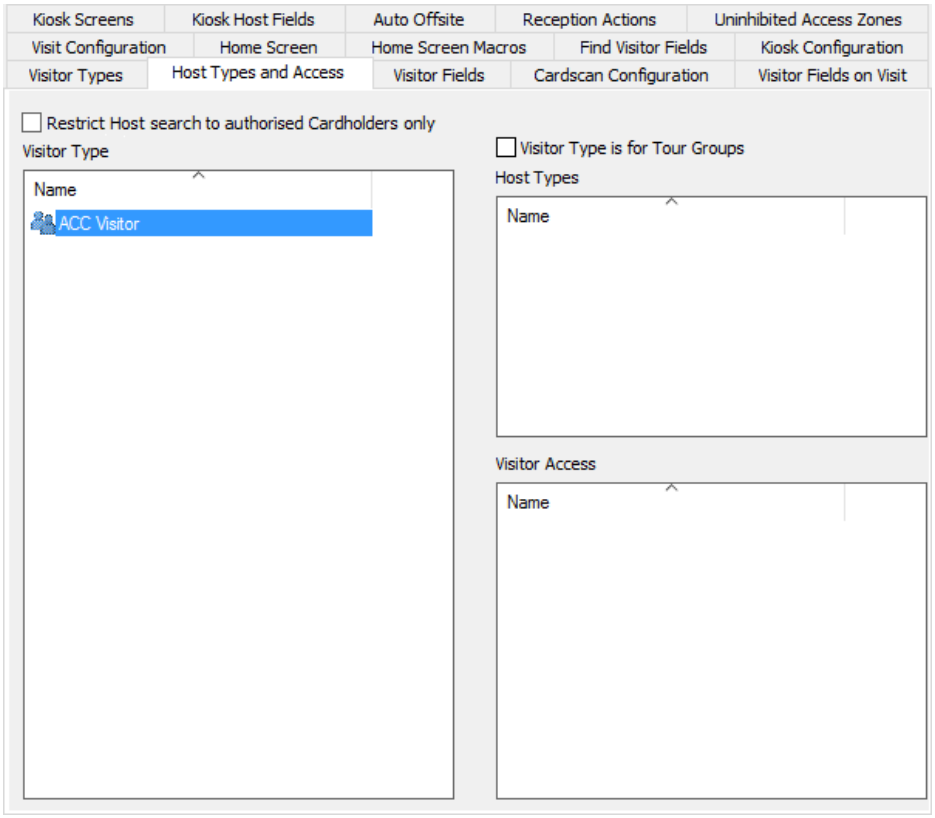
14. Repeat Step 13 if there are other Visitor Types requiring Visitor Badge Card Types.
15. Close the Card Type list window.
16. Click the appropriate sub-tab(s) required to configure the division, and complete the setting information.
    Note: The minimum configuration required before you can save is Visitor Type and Host Type.
    - ***Host Types and Access tab*** (on page 50-20)
    - ***Visitor Fields tab*** (on page 50-22)
    - ***Cardscan Configuration*** (on page 50-25)
    - ***Visitor Fields on Visit tab*** (on page 50-26)
    - ***Visit Configuration tab*** (on page 50-28)
    - ***Home Screen tab*** (on page 50-31)
    - ***Home Screen Macros tab*** (on page 50-33)
    - ***Find Visitor Fields tab*** (on page 50-34)
    - ***Reception Actions tab*** (on page 50-36)
    - ***Auto Offsite tab*** (on page 50-38)
    - ***Uninhibited Access Zones*** (on page 50-39)

Host Types and Access tab



The Visitor Type(s) that you dragged and dropped onto the **Visitor Types** tab appear in the Visitor Type grid on this screen.

1. Select the **Restrict Host search to authorised Cardholders only** checkbox to only allow authorised Host Cardholders to be viewed and selected in the Visitor Management Client. This restricts the 'Meeting With' field (when creating a visit) and the 'Find Host' search (on the 'Home' screen). **Note:** 'Authorised' Cardholders are those with the **Cardholder Authorised** checkbox checked on the **Cards** tab in their properties.
2. Select the Visitor Type you want to assign a Host Type to.



The Host Types and Visitor Access Groups grids become enabled.

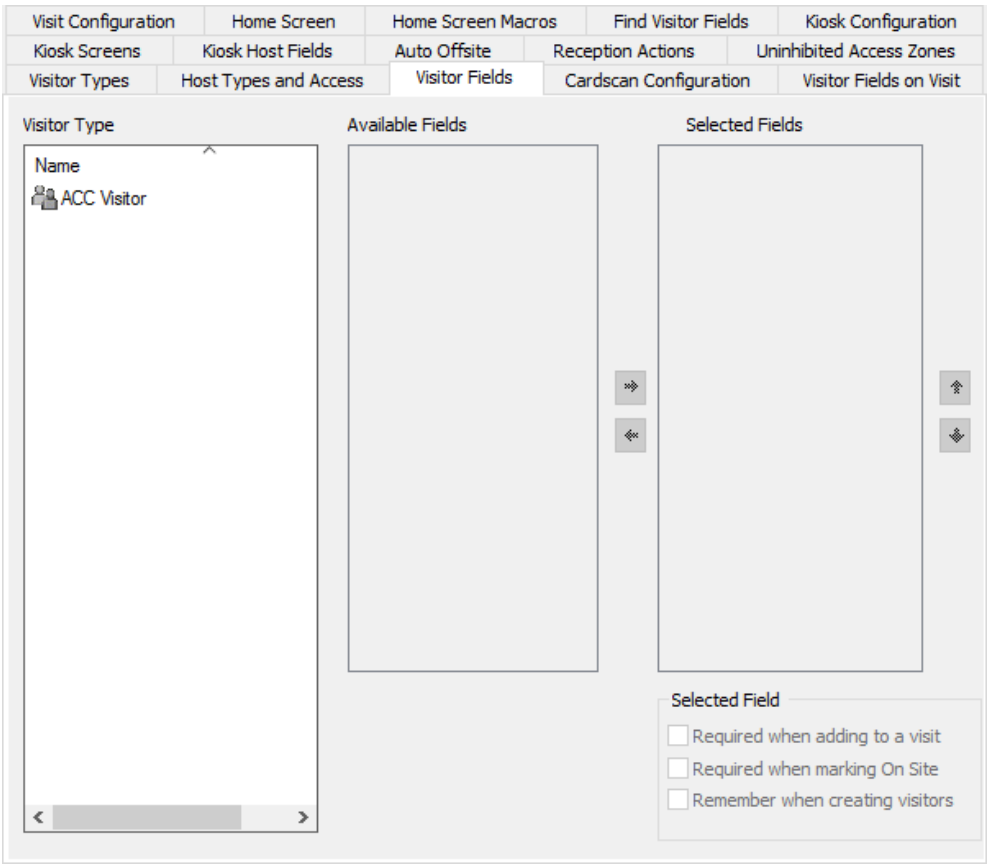
Notes:

- Each Visitor Type can have more than one Host Type assigned to it.
- The **Visitor Type is for Tour Groups** checkbox is for sites using the Visitor Management Kiosk feature that intend using this Visitor Type for Tour Group visits. See ***Host Types and Access tab (Kiosk)*** (on page 51-33) for further detail.

3. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens.
4. Select the required Host Type Access Group(s), and drag and drop it into the **Host Types** grid.
5. **Visitor Access** is the Access Groups that actually give access in the Visitor Management application. It forms a list of access that can be selected on a visit.
   Select any required Access Groups, and drag and drop them into the **Visitor Access** grid.
6. Repeat Steps 3 and 4 if there are other Visitor Types requiring Host Types and/or Visitor Access Groups.

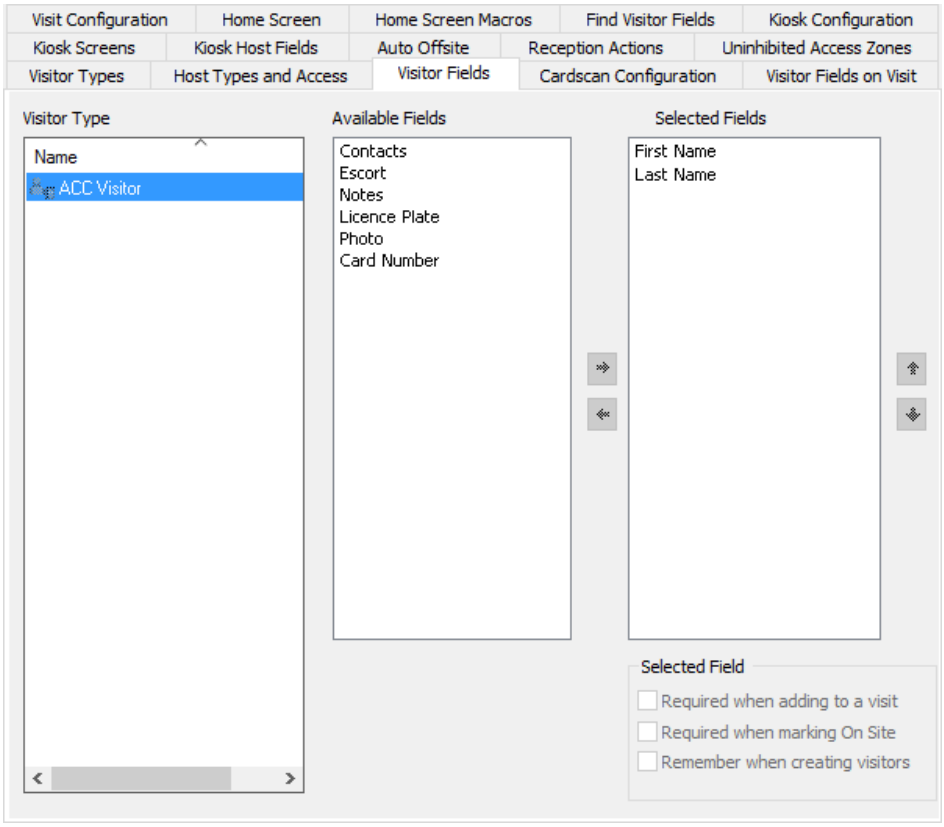
Visitor Fields tab

This tab allows you to configure what will appear on the **Visitor** screen for each Visitor Type in the Visitor Management application.



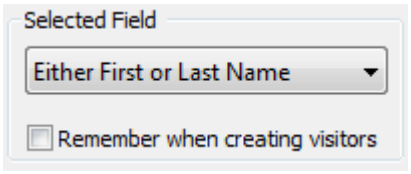
The Visitor Type(s) that you dragged and dropped onto the **Visitor Types** tab appear in the Visitor Type grid on this screen.

1. Select the Visitor Type you want to select the visitor fields for.
   The visitor fields are a combination of some mandatory fields, (e.g. Visitor **First Name** and **Last Name**), and Personal Data Fields (PDFs) that are assigned to the Visitor Type, (i.e. Visitor Type Access Group).



The ‘Available Fields’ and ‘Selected Fields’ grids become enabled.
The ‘Available Fields’ grid is populated with the fields which are available to display on the **Visitor** screen in the Visitor Management application, but have not been selected.

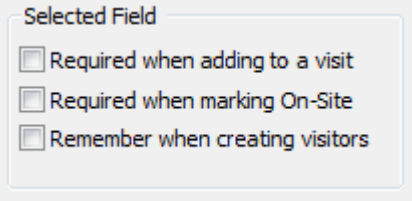
The ‘Selected Fields’ grid is populated with the mandatory fields, (e.g. **First Name** and **Last Name**, are always in the 'Selected Fields' list), and cannot be removed.
Note: If you click on either the **First Name** or **Last Name** fields the options in the 'Selected Field' section change as shown. The options available in the drop-down are 'Either First or Last Name' or 'Both First and Last Name'.



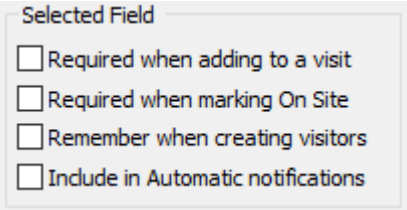
2. Move any of the fields you require from the ‘Available Fields’ grid to the ‘Selected Fields’ grid by selecting the field and clicking the button.
Note: If "Card Number' is selected a read-only **Card Number** field, showing cards assigned to visitors, will appear on the Visitor window.
3. Once you have all the fields you require in the ‘Selected Fields’ grid, you can re-order the fields if required by using the **up** and **down** arrow buttons to the right of the ‘Selected Fields’ grid.

   Note: The order you sort these fields in here will be the order they appear in the Visitor Management application.

4. By clicking on a field in the 'Selected Fields' grid, the checkboxes below become enabled.



If you click on a **PDF** in the 'Selected Field' grid, an additional **Include in Automatic notifications** checkbox displays.



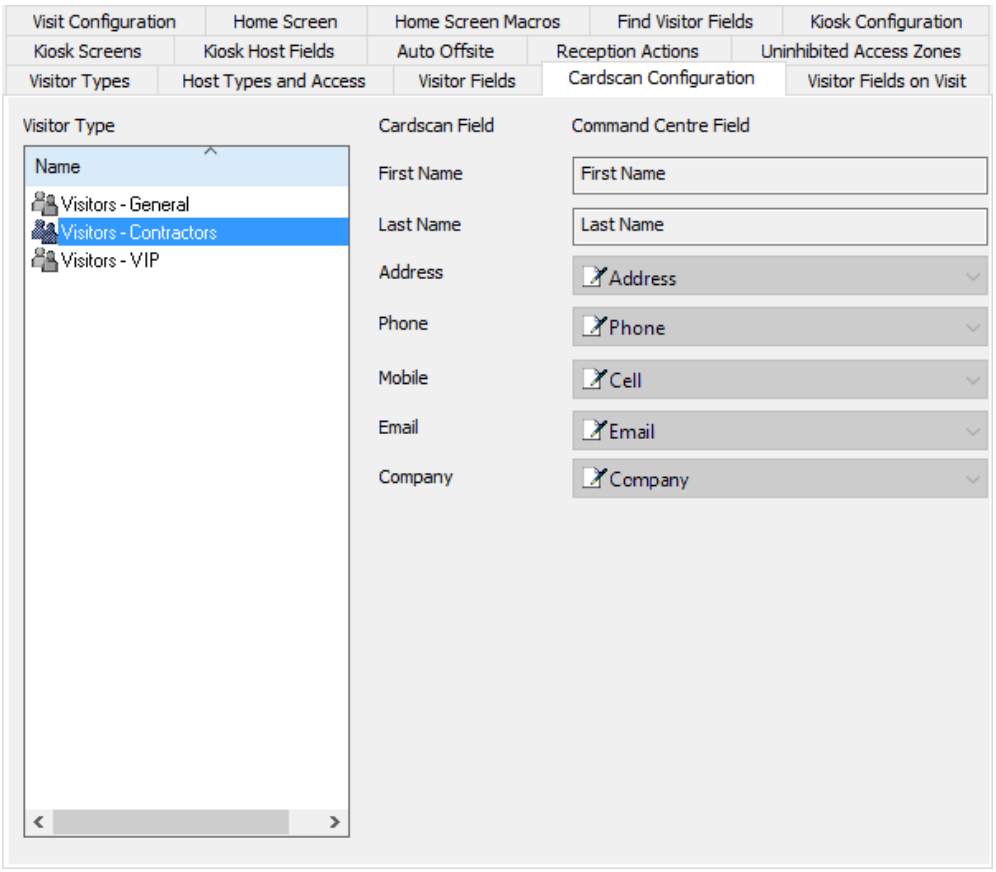
Note: If you have moved **Escort** to the 'Selected Fields' grid, and click on it, all the checkboxes are disabled.

5. Check the required checkbox(es) for each selected field as appropriate.

Checkbox	Checking this means…
Required when adding to a visit	the value of the field must be entered at the time you add a visitor to a visit. **Notes:** • Checking this control disables the "Required when marking On Site" control. You get the mandatory On Site automatically. • Any PDFs with the 'Required Field' ticked (on the **Type** tab) must have 'Required when adding to a visit' here checked also.
Required when marking On Site	the value of the field does not have to be entered until the visitor is on site, (e.g. a photo of the visitor would usually not be able to be taken until the visitor arrives on site). This is only mandatory before marking On Site.
Remember when creating visitors	the system will remember the value of the field for each visitor, (e.g. if all visitors on a visit are from the same Company, this option saves re-entering the Company name for each visitor).
Include in Automatic notifications	that the PDF will be included in automatic arrival and departure overdue notifications sent to hosts/escorts. **Notes:** • Departure notifications are managed by the server and privileges cannot be applied to them. Therefore, if you have sensitive data in these PDF's do not configure departure overdue notifications, or do not include these PDF's as Automatic Notifications. • This option will be disabled for Image PDFs.

Cardscan Configuration tab

Configure the fields on this tab if you have a Business Card scanner attached for the purpose of scanning visitor business cards.

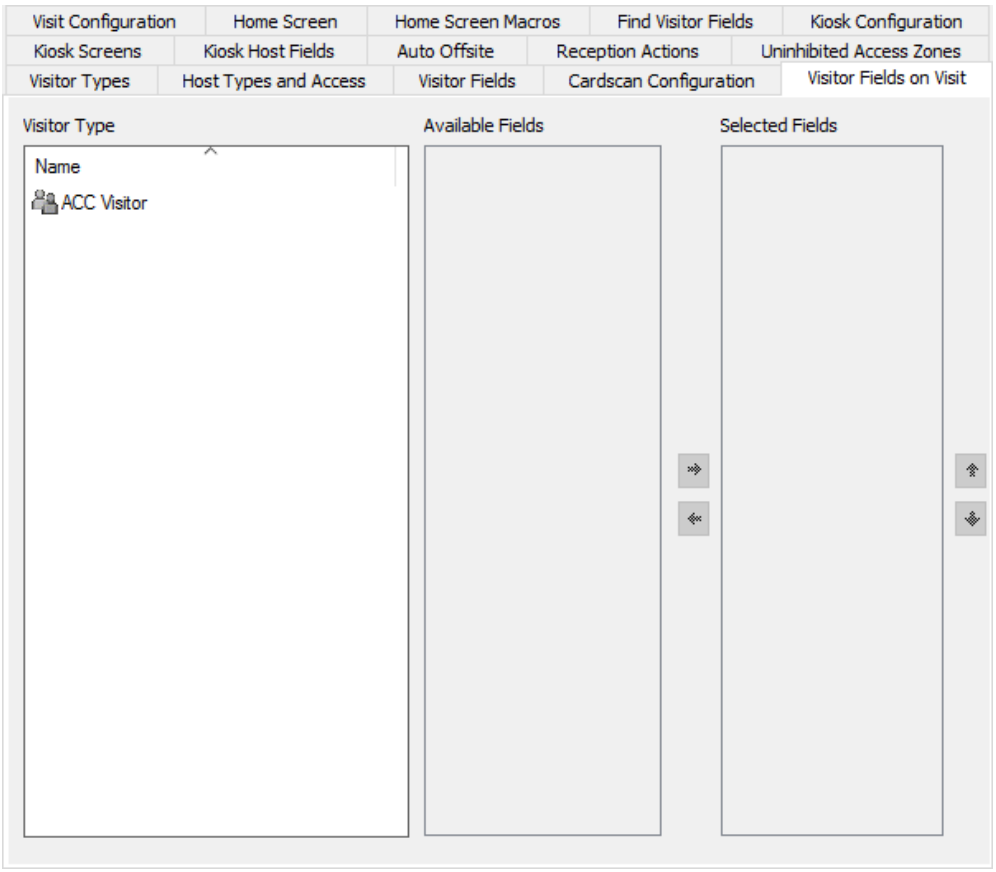


The Visitor Type(s) that you dragged and dropped onto the **Visitor Types** tab appear in the Visitor Type grid on this screen.

1. Select the Visitor Type that you want to configure Business Card scan capability for.
   The Cardscan configuration for that Visitor Type displays.
2. Select the required PDFs from the drop-down lists as appropriate.

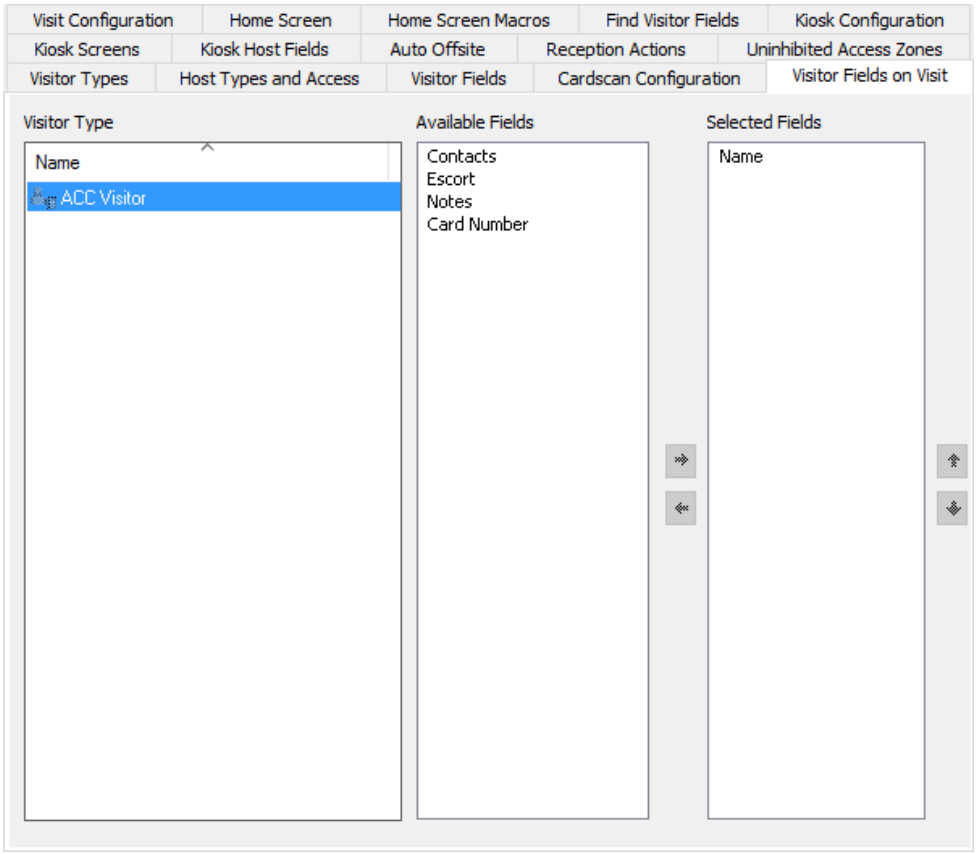
Visitor Fields on Visit tab

This tab allows you to configure what columns will appear on the **Visit** screen for a particular Visitor Type, in the Visitor Management application.



The Visitor Type(s) that you dragged and dropped onto the **Visitor Types** tab appear in the Visitor Type grid on this screen.

1. Select the Visitor Type you want to select the visitor fields for.
   The visitor fields are a combination of some mandatory fields, (e.g. Visitor **Name**), and Personal Data Fields (PDFs) that are assigned to the Visitor Type, (i.e. Visitor Type Access Group).



The ‘Available Fields’ and ‘Selected Fields’ grids become enabled.

The ‘Available Fields’ grid is populated with the fields which are available to display for each visitor on the **Visit** screen in the Visitor Management application, but have not been selected.

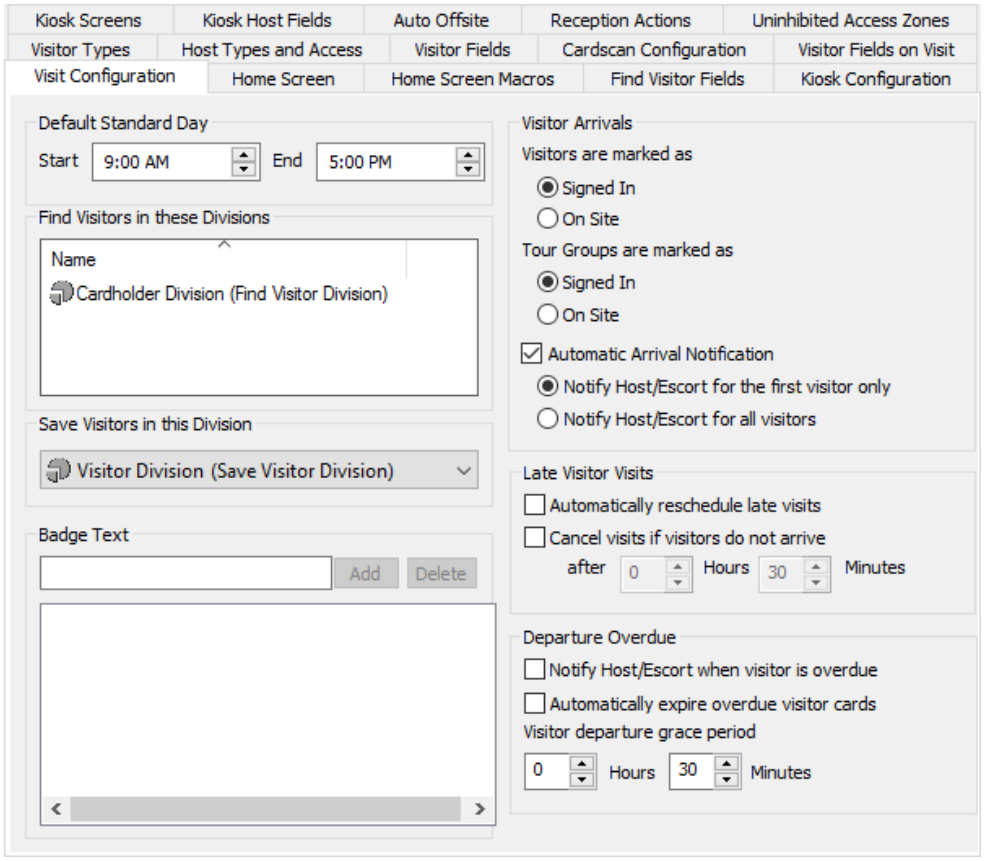
The ‘Selected Fields’ grid is populated with the mandatory fields, (e.g. **Name** is always in the 'Selected Fields' list), and cannot be removed.

2. Move any of the fields you require from the ‘Available Fields’ grid to the ‘Selected Fields’ grid by selecting the field and clicking the button.

   Note: If "Card Number" is selected, a read-only **Card Number** column (which can be sorted on), showing cards assigned to visitors, will appear on the Visit screen.

3. Once you have all the fields you require in the ‘Selected Fields’ grid, you can re-order the fields if required by using the **up** and **down** arrow buttons to the right of the ‘Selected Fields’ grid.
   Note: The order you sort these fields in here will be the order they appear in the Visitor Management application.

Visit Configuration tab



Configure as appropriate:

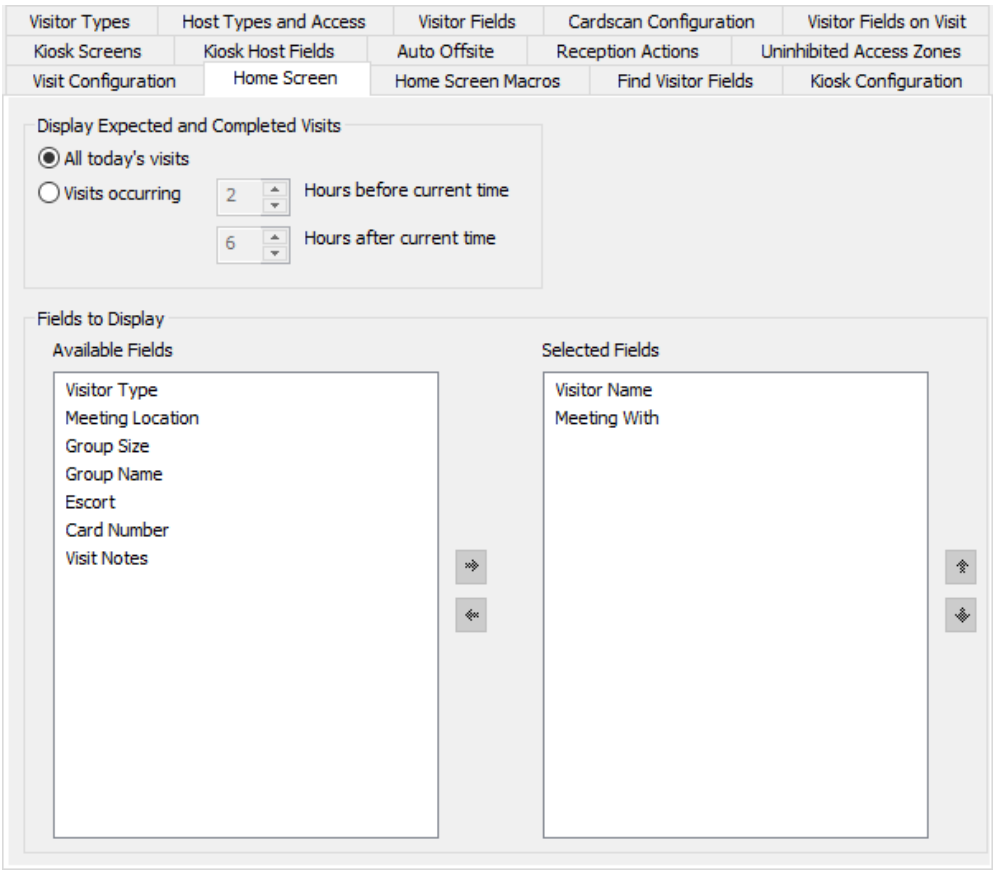
Field / Button	Description
Start Time	This is the standard start of day time. (Default = 9:00am)
End Time	This is the standard end of day time, and is used to set a default departing time for the visit. (Default = 5:00pm)
Find Visitors in these Divisions	The division(s) from which the list of available visitors for a visit will be built. For a simple site setup this will be the Cardholder Division(s). (Default = The name of the division being configured and can be changed to any other division you have the ability to see.)
Save Visitors in this Division	The division in which visits and visitors for that reception will be created. This will be the Visitor Division. (Default = The name of the division being configured and can be changed to any other division you have the ability to see.)

Field / Button	Description
Badge Text	You can specify a list of items which can then be selected for a visit and printed on a badge. You can type in the actual text that you want to appear on visitor badges or copy items in, clicking the **Add** button after each line of text, (e.g. a "VIP" badge marking, or an area the visitor is allowed to visit).
Visitors are marked as	Check the appropriate radio button for how you want Visitors to be marked as on arrival, (i.e. either **Signed In** or **On Site**).
Tour Groups are marked as	Check the appropriate radio button for how you want Tour Groups to be marked as on arrival, (i.e. either **Signed In** or **On Site**).
Automatic Arrival Notification	Check this option if you want a notification to be automatically sent to the Host/Escort(s) when the Receptionist chooses the 'Sign In' action, when a visitor arrives on site, and then click the appropriate radio button. **Notes:** • This setting applies to both the Visitor Management client and Visitor Management Kiosk. • A Host/Escort is the person a visitor is meeting with. • Clicking the **Notify Host/Escort for the first visitor only** radio button means that the host will only be sent one notification when the first visitor in a Visit arrives, rather than them receiving notifications for every member of a Visit.
Automatically reschedule late visits	Check this option if you want late visits to be automatically rescheduled. When enabled, if a visitor arrives for a visit after the visit is scheduled to start the system will change the scheduled start and end time for the visit, so that the visitor's visit is still for the same length of time, e.g. A visit is scheduled to start at 2:00pm and end at 3:30pm. The visitor arrives, (i.e. is marked on-site) at 2:10pm. The visit is automatically updated to start at 2:10pm and end at 3:40pm

Field / Button	Description
Cancel visits if visitors do not arrive	Check this checkbox and enter a time in hours and/or minutes, if you want to specify a grace time, after which if a visitor has not arrived, their visit will be cancelled.
Notify Host/Escort when visitor is overdue	Check this option if you want a notification to be automatically sent to the Host/Escort(s), (i.e. the person a visitor is meeting with), when a visitor becomes overdue.
Automatically expire overdue visitor cards	Check this option if you want overdue visitor cards to be automatically expired. When enabled, a cards expiry time becomes the expected departure time for the visitor plus the departure grace period.
Visitor departure grace period	A grace period can be specified allowing a visitor extra time on site if their visit goes over the expected length. If a grace period is not required, this can be set to 0. (Default = 30 minutes) **Notes:** • In the Visitor Management application, once a visitor goes past their expected visit **End Time** plus the "Grace Period", the visitors status changes to “Overdue” on the **Home** screen, they appear in the **Exceptions** tab, and an alarm is raised. • If the grace period is changed in Command Centre, it will not update visits already created, unless the visit end time is edited.

Home Screen tab

This tab allows you to configure the columns that will display on the **Home** screen in the Visitor Management application. There is a single configuration which applies regardless of which status the Receptionist is viewing.



Configure as appropriate:

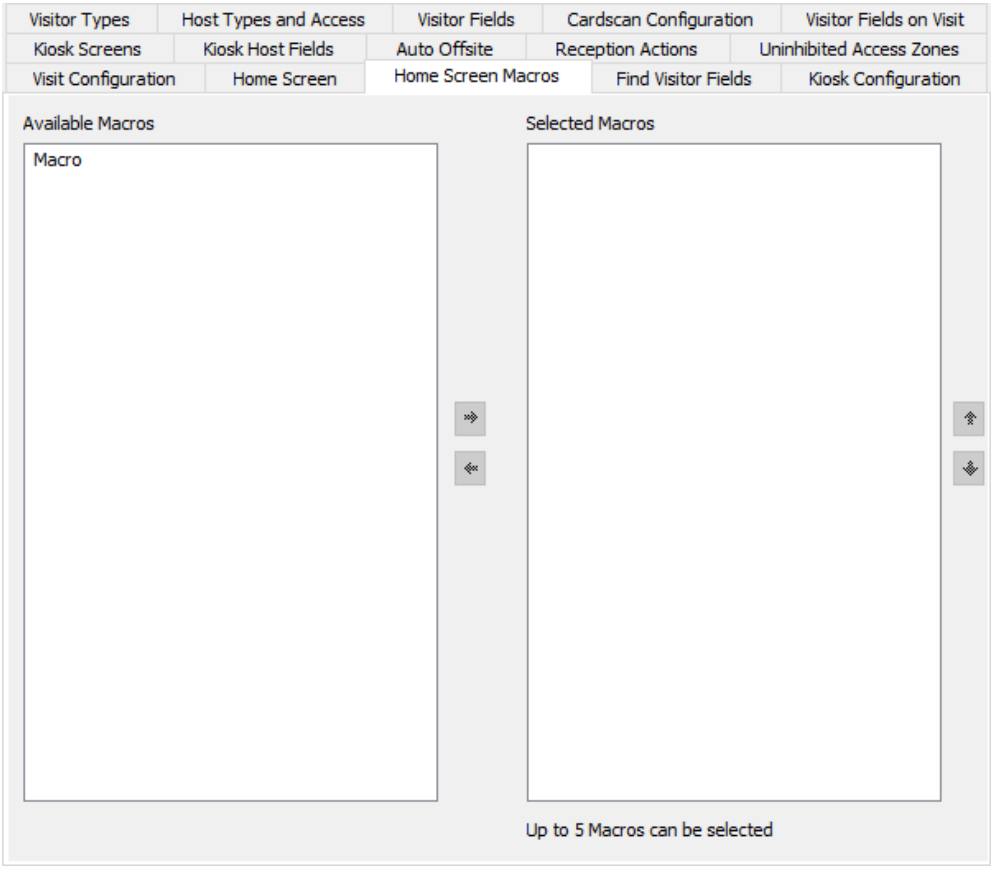
Field / Button	Description
Display Expected and Completed Visits	These radio buttons allow you to configure the time slot used to determine which visitors on a visit will be shown on the **Expected** and **Completed** tabs in the Visitor Management application. The time slots available are: • All today's visits • Visits occurring (Default = The **All today's visits** radio button is selected)

Field / Button	Description
Fields to Display	Using the arrow buttons, place the fields that you require from the **Available Fields** grid to the **Selected Fields** grid. **Notes:** • Although "Arriving Date and Time", "Departing Date and Time", "Visitor Status", "Next Action" and "Visit" do not appear in the **Selected Fields** grid, they will automatically appear on the Home screen. • If "Card Number" is selected a read-only **Card Number** column (which can be sorted on), showing cards assigned to visitors, will appear on the Home screen. • If "Visit Notes" is selected, a **Visit Notes** column will appear on the Home screen. A read-only dialog can be accessed from this column which shows notes relating to visitors visits.

Home Screen Macros tab

This tab allows you to select a macro (already configured in Command Centre), to be run from a button on the Visitor Management application toolbar.

Note: A maximum of five macros can be selected, and there will be one button per macro in the Visitor Management application.



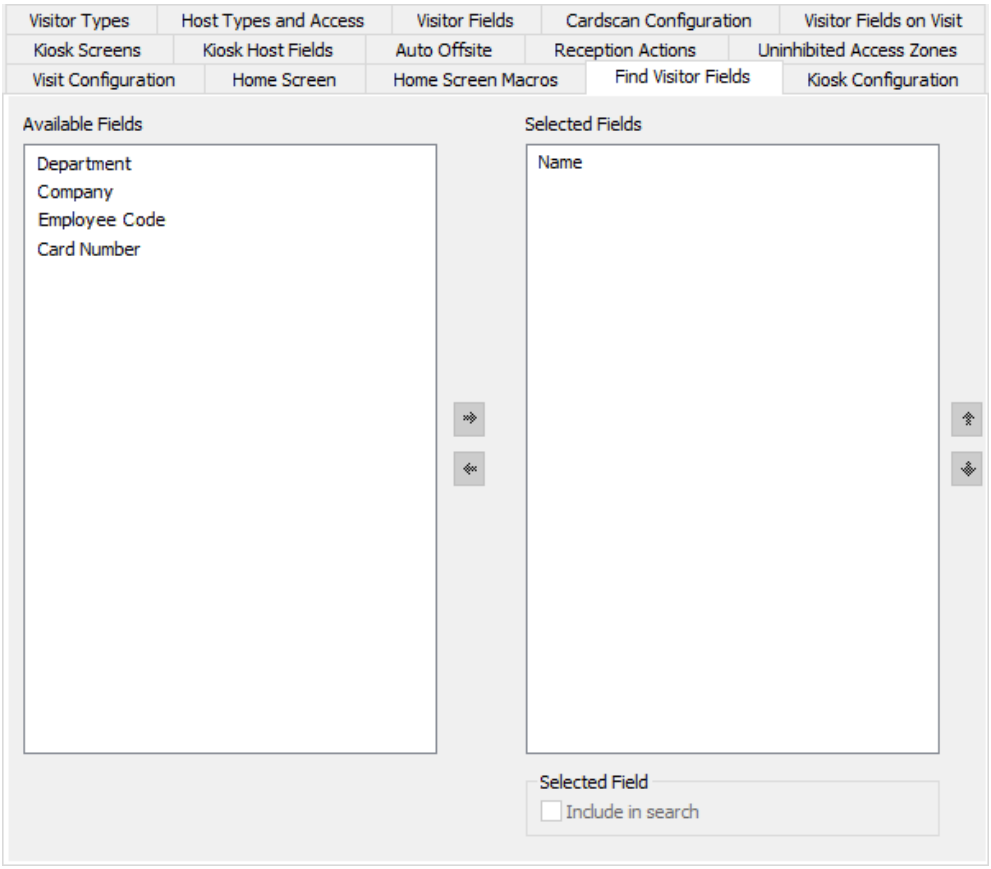
1. Move any of the fields you require from the 'Available Macros' grid to the 'Selected Macros' grid by selecting the macro and clicking the button.
2. Once you have all the macros you require in the 'Selected Macros' grid, you can re-order them if required by using the **up** and **down** arrow buttons to the right of the 'Selected Macros' grid.
   Note: The order you sort these macros in here will be the order they appear as buttons in the Visitor Management application.

Find Visitor Fields tab

This tab allows you to configure what columns will appear on the **Find Visitor** screen in the Visitor Management application, from the following:

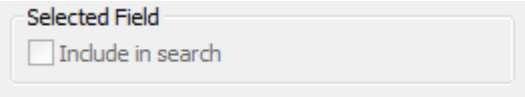
- Visitor (made up of Last Name, First Name)
- Visitor Last Name
- Visitor PDFs
- Card Number

This configuration will also determine the columns to be included in the list of visitor matches displayed when searching for a visitor to add to a visit in the Visitor Management application.



1. Move any of the fields you require from the 'Available Fields' grid to the 'Selected Fields' grid by selecting the field and clicking the  button.
2. Once you have all the fields you require in the 'Selected Fields' grid, you can re-order the fields if required by using the **up** and **down** arrow buttons to the right of the 'Selected Fields' grid.
   Note: The order you sort these fields in here will be the order they appear in the Visitor Management application.

3. By default, searching and matching is only performed on the visitor name. By clicking on a PDF in the 'Selected Fields' grid, the checkbox below becomes enabled, allowing you to include the PDF in the search and match.

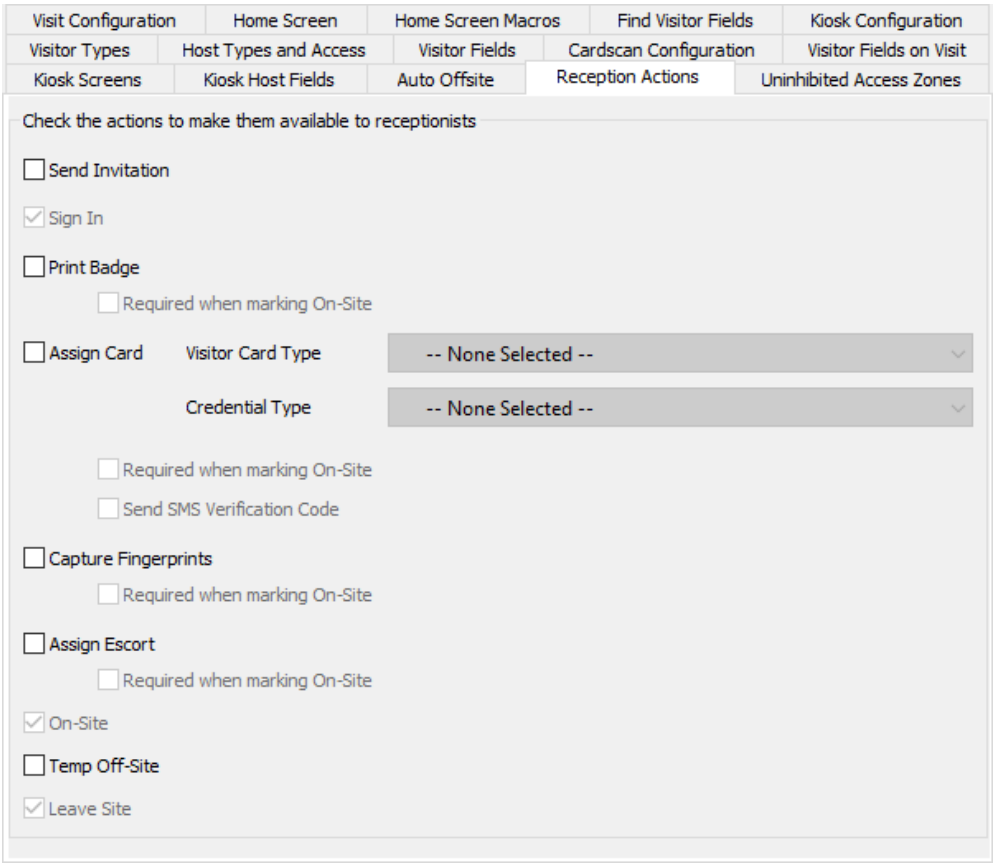


Note: If you want to be able to search by card number on the Visitor Search window, move "Card Number" into the 'Selected Fields' grid. From there, highlight it and check the **Include in search** checkbox.

4. Check the **Include in search** checkbox for each of the PDFs, if any, that you want to have included in the search and match in addition to the visitor name.
Note: There is no limit to the number of PDFs you can include for searching. While the **Visit** screen in the Visitor Management application will only display the Name field plus four PDFs, searching will still be performed on all the PDFs included.

Reception Actions tab

This tab allows you to configure the actions that will be available to Receptionists.



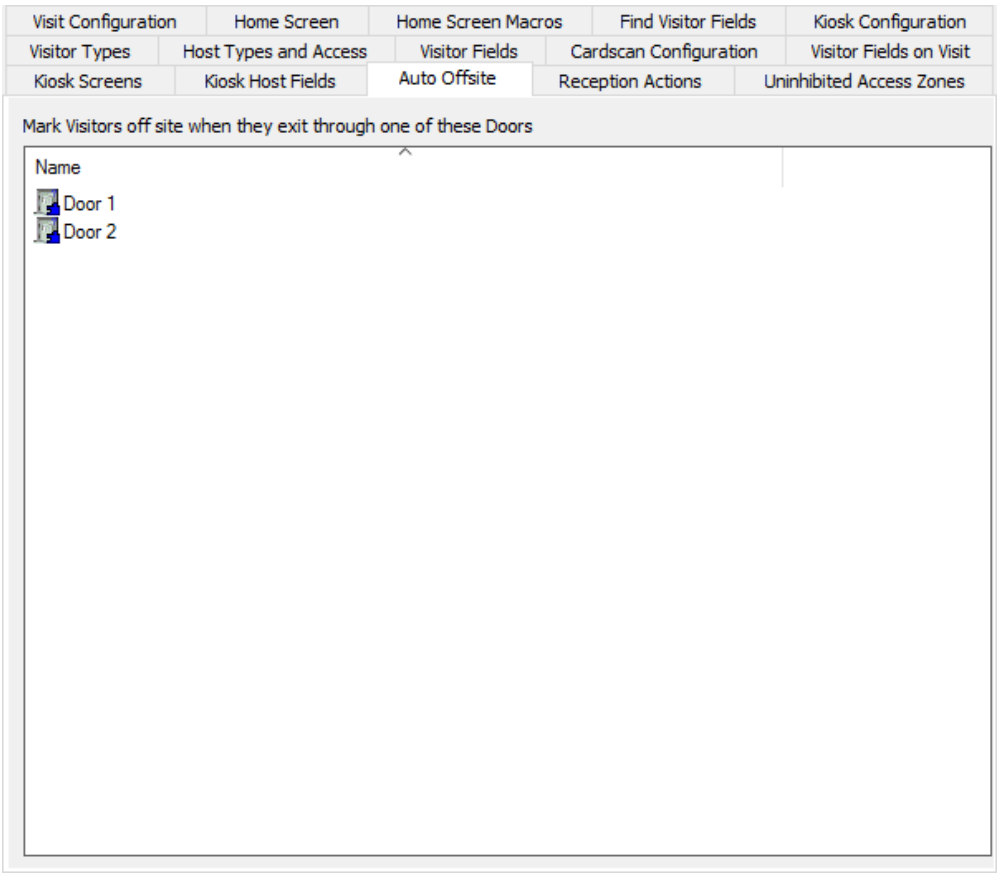
Configure as appropriate:

Field / Checkbox	Description
Action	By default the following actions are not available to receptionists: - Send Invitation - Print Badge - Assign Card - Capture Fingerprints - Assign Escort - Temp Off-Site If you require any of them to be available to receptionists, check the checkbox to the **left** of the required action(s). **Notes:** • The "Sign In", "On-Site" and "Leave Site" actions are permanently checked and disabled so they cannot be unchecked.

Field / Checkbox	Description
	• Enabling the "Capture Fingerprints" option results in a **Biometrics** action button appearing on the Visitor Management Visit or Home screens. If this button is clicked when biometric functionality has not been set up an error displays and Visitor Management closes. For further detail on configuring biometrics, see ***Morpho Biometric Integration*** (on page 64-1).
Required when marking On-Site	The "Print Badge", "Assign Card", "Capture Fingerprints" and "Assign Escort" actions can be set as mandatory prior to a visitor being recorded on-site. To do this, check the **Required when marking On-Site** checkbox directly below the required action(s). **Note:** The **Required when marking On-Site** option cannot be selected for "Assign Card", "Capture Fingerprints" or "Assign Escort" if the visitor has been configured to be marked automatically onsite.
Visitor Card Type Credential Type	These drop-down lists are only enabled when the “Assign Card” action has been checked. If enabled, a Card Type and/or Credential Type must be selected, (e.g. a card type for recyclable visitor cards). **Note:** Only one Card Type and Credential Type per Division can be selected.
Send SMS Verification Code	Checking this option allows the Registration Server to authorise cardholders’ mobile phones. **Note:** This makes a **Mobile** field appear on the Assign Credential pop-up in the Command Centre Client when registering mobile credentials for cardholders.

Auto Offsite tab

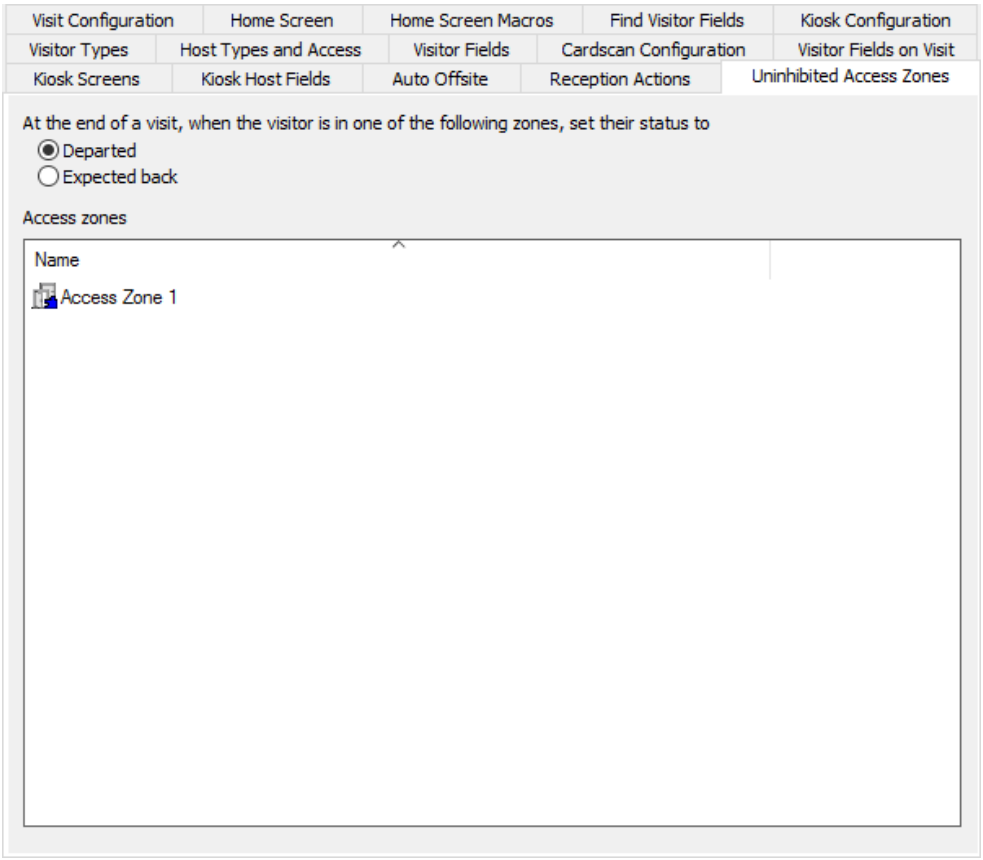
This tab allows you to configure the system so that visitors will be marked "off site" when they badge their visitor access card at a designated exit reader.



1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens.
2. Select the required Door(s), and drag and drop it into the grid.
   Notes:
   - Alternatively, the Find Tool can be used to select multiple doors to drag and drop into the grid.
   - Doors included here need to have been specifically configured for exit readers.

Uninhibited Access Zones tab

This tab allows a list of Access Zones to be configured as "Uninhibited Access Zones", so that when a visitor is in one of the listed zones at the end of their visit, (i.e. at the scheduled departure time) they are automatically marked as being either "off-site" (departed), or "temporarily off-site" (expected back).



1. Drag and drop the Access Zones you want included as uninhibited zones into the grid.
2. Click the appropriate radio button, (i.e. **Departed** or **Expected back**) for what status visitor should appear as when they enter one of these zones at the end of a visit.
   Important:
   The use of Uninhibited Access Zones will also apply to subsequent visits if the visitor's status still shows them as being in one of the Uninhibited Access Zones.

Using Image Capture Devices

It is possible to capture multiple images for visitors, (e.g. a photo of the visitor, the visitor's business card, a letter of recommendation, etc.). Sites have the ability to configure the type of device to be used for capturing images, and visitor details can be captured by scanning a business card.

The following APIs are supported for image capture:

- Direct Show
- TWAIN
- Cardscan (**Note:** This option will not be available if your site has installed/ upgraded with `NPSA=1` in the licence file.)
- Acuant SDK (for ScanShell 800NR)

Not all devices work with these APIs, therefore a modification may be required to get a particular device to work. As a result, the devices supported are:

- Plustek OptiCard 821 (Business Card scanner based on the TWAIN API)
- Avision AVA6 (An A6 sized scanner based on the TWAIN API)
- CardScan 800C (Business Card scanner using the CardScan API)
- ScanShell 800NR (Business Card scanner using the Acuant SDK)

Notes:

- Other devices than those listed above may also work (using these APIs), but there is no guarantee of how well.
- It is recommended that sites have no more than five capture devices connected.

Creating Card Types

Introduction

A Visitor Badge Card Type needs to be configured in Command Centre if you intend printing badges or using visitor access cards.

Note: Bureau card types cannot be used in Visitor Management.

Procedure

1. Click **Configure** from the menu bar.
2. Click **Card Types**.
   The **Card Type** List Window opens.
3. **Right click** and select **New...Card Type**.
   By default the **General** tab displays.
4. Configure the new Card Type as required.
   See ***Setting up Card Types*** (on page 7-2) for further detail.
   Note: The maximum Card Number normally allowed in Command Centre (on the **Setup** tab of the Card Type), is approximately 605 characters in decimal format, (i.e. 2008 bits). However, for Visitor Management the maximum Card Number allowed is 20 digits, (i.e. 18,446,744,073,709,551,615).

Using recyclable visitor access cards

Recyclable access cards can be held by Receptionists for issuing to visitors when they arrive for a visit. When visitors leave, they return the access cards to the Receptionist so they can be reused for other visitors when required.

If you intend assigning cards to visitors, using recyclable access cards, you need to:

1. Encode all of the cards to be used for visitors.
   See ***Printing and/or Encoding a card from a cardholder*** (on page 47-52) for further detail.
2. Remove these cards from the cardholder so they can be reassigned to visitors as and when required.

Adding Visitor details to cards/badges

Introduction

The Photo ID feature has been enhanced so that additional information can be printed onto visitor cards. The details to be added are new fields that are associated with a visit in Command Centre.

An operator with the suitable privilege will have the option to include visit badge objects and/or the following fields, (i.e. text objects) on a card:

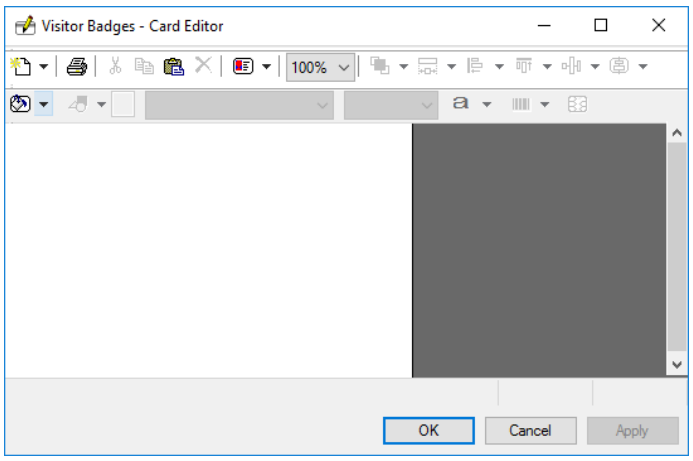
- Visit Start Date and Time
- Visit End Date and Time
- Meeting With (this is the person that the meeting is planned with)
- Visitor Type
- Badge Text
- Group Name.

Notes:

- All other functionality for Photo ID (including editing, layout, etc.) has remained the same.
- Visitor Management does not require Photo ID licensing to print visitor badges.

Procedure

1. Click **Configure** from the menu bar.
2. Click **Card Type**.
   The **Card Type** List Window displays.
3. **Right click** on the Visitor Badge card type created earlier (see ***Creating Card Types*** on page 50-41), and select **Edit Card Layout**.
   The Card Editor window displays.

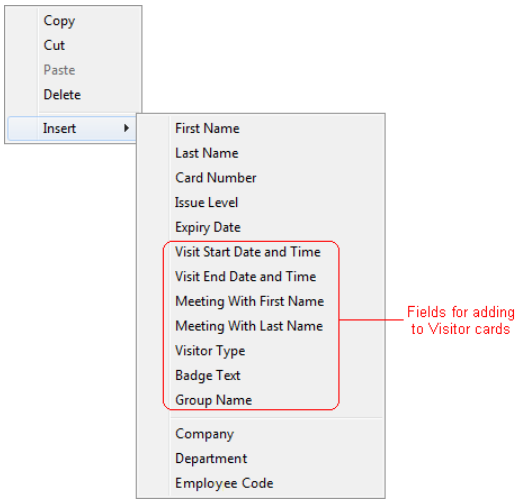


4. Visitors can be assigned a QR Code (Quick Response Code format) or barcode, to allow them to sign in and sign out as fast as possible. See ***Visitor Management Barcode Scanner Process*** (on page 50-148) for further detail.

Do you want to add a QR Code or barcode to the visitor badge?

If…	then…
no,	go to Step 5.
a QR Code,	a) Select **New QR Code Access Token Object**  A QR barcode image displays with placeholders around it.  b) Resize and reposition the barcode as required. See ***Expanding an Object Box*** (on page 47-47) and/or ***Moving Objects*** (on page 47-46) for the procedure. c) Make further modifications to the card, (e.g. add a background or another object), if necessary. See ***Designing Card Layouts*** (on page 47-13) for further details.
a barcode,	select **New Barcode Object**  See ***Adding a Barcode*** (on page 47-23) for the procedure.

5. Select **New Text Object** 
   An object box displays with placeholders around it.
6. **Right click** within the text field, then click **Insert** from the drop-down menu.
   A drop-down menu displays.



   Note: The seven additional fields for adding to Visitor cards only appear if your site is licensed for Visitor Management.
7. Click on the required item. The item now displays on the card layout.
8. If you want to add other items, repeat Steps 4 to 6.
   Notes:
   - For further details about adding objects to cards, see Designing card layouts.
   - The recommended maximum size for a background image for a badge is 2 MBytes.
9. Click the **OK** button.
   The Card Editor window closes.

Creating Doors

Introduction

A Door needs to be configured in Command Centre if your site intends using reception readers.
Notes:

- If access cards are to be assigned to visitors or will be used for identifying and assigning escorts, a Door will need to be configured for each Reception workstation requiring such functionality.
- If visitor access cards are to be used, and visitors will be leaving the site through a different reception from the one they arrived at, a Door needs to be configured for the exit reader.
- Doors should be created in the "Visitor Division" as the Receptionist will need the "Events and Alarms" privilege to see the Door and the result of the card swipe.

Procedure

1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens.
2. **Right click** and select **New...Door**.
3. Configure the new Door as required.
   See ***Creating Doors*** (on page 22-2) for further detail.
4. Click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens.
5. Double-click on the Reception workstation.
6. Click the **Visitor Management** tab.
7. From the **Door** drop-down list, select the applicable Door. Remote (multi-server) Doors can be selected.
   The Visitor Management application will monitor this door for card events.

   Notes:

   - Where more than one workstation is configured for a single reception and access cards are used, it is advisable to configure one reader per workstation to prevent unexpected events occurring at another workstation when a card is badged.
   - Ensure escorts (in the Host Type Groups) have access to the door selected.

Creating Macros

Introduction

A Macro needs to be configured in Command Centre if you require macros to be available to Receptionists.

Note: Any Macros which the Receptionist can run from buttons on the Visitor Management toolbar should be stored in the *Save Visitor in this Division* as the user must have the "Run Macro" privilege in order to run them.

Procedure

1. Click **Configure** from the menu bar.
2. Click **Macros**.
   The **Macro** List Window opens.
3. **Right click** and select **New...Macro**.
   By default the **General** tab displays.
4. Configure the new Macro as required.
   See ***Creating a new Macro*** (on page 20-2) for further detail. **Notes:**
   - When naming macros, be aware that only 20 characters fit on the macro buttons in the Visitor Management application.
   - If you configure a macro to present a confirmation dialog prompt before the macro runs (on the **Operator Confirmation** tab), no confirmation dialog will appear when it is run from the Visitor Management application.

Assigning permanent cardholders to Cardholder Division

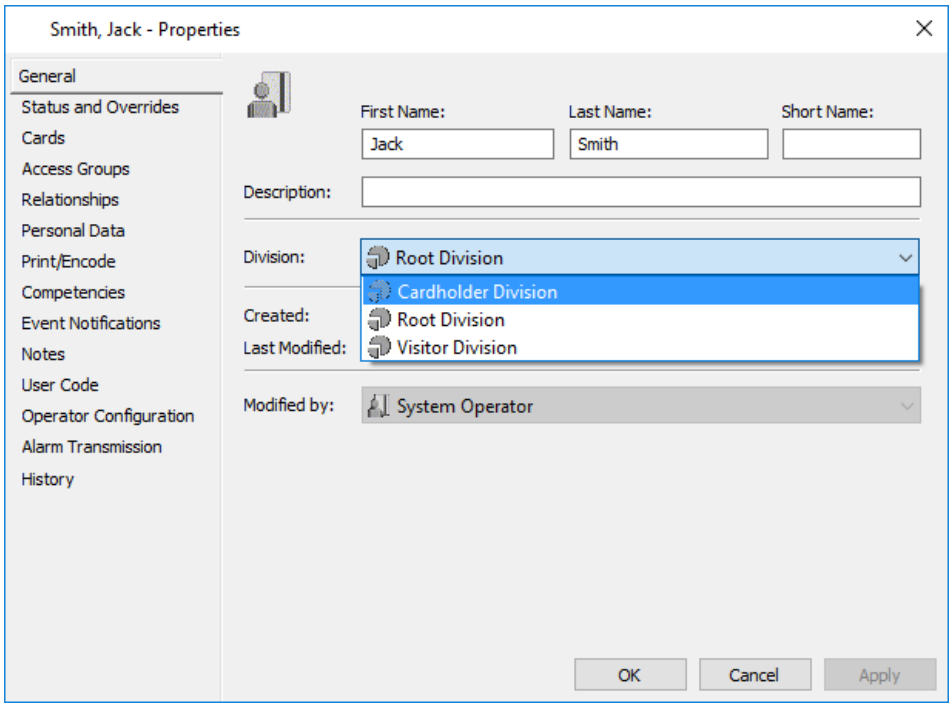
Introduction

This procedure describes how to assign permanent cardholders to the **Cardholder Division**, allowing them to be potential visitors, (e.g. visiting a site within the same organisation).

Note: The bulk changes feature can be used if you want to change the division for a large number of cardholders. Refer to Initiating a new Cardholder Bulk Change for the procedure.

Procedure

1. Click **Manage** from the menu bar.
2. Click **Cardholders**.
   The **Cardholder** List Window opens.
3. **Right click** on the Cardholder you want to assign to the Cardholder Division, and select **Properties**.
   By default the **General** tab displays.



4. Select the "Cardholder Division" from the **Division** drop-down list.
5. Click the **OK** button.
6. Repeat Steps 3 to 5 for every cardholder you want to assign to the Cardholder Division.

Adding Contacts to "Host" Cardholders

Introduction

A "Host" is the person responsible for visitors for the duration of their visit, and must be a non-visitor cardholder. Potentially, the "Host" can be either the "Meeting with" person or the "Escort".

Contact details for cardholders who are “Hosts” in the Visitor Management application are required so that they can be easily contacted by Reception if a visitor arrives to see them.

There are four Contact type Personal Data Fields (PDFs) that can be configured for holding cardholder contact details. Contact details for individual cardholders are then entered against these PDFs on the **Personal Data** tab of the Cardholder properties. They are then available from the **Host** screen in the Visitor Management application as "read-only", (i.e. they cannot be altered in the Visitor Management application).

Refer to...	for the procedure on...
Creating a new Personal Data Field (on page 33-2)	creating Contact type PDFs.
Editing a Cardholders PDF data (on page 32-20)	adding contact details for individual cardholders.

Viewing Visits in Command Centre

Introduction

When visits have been created in the Visitor Management application, their details can be viewed in Command Centre by using the Find tool and searching for visits. However, visits are not available from a List Window, like most Command Centre Items.

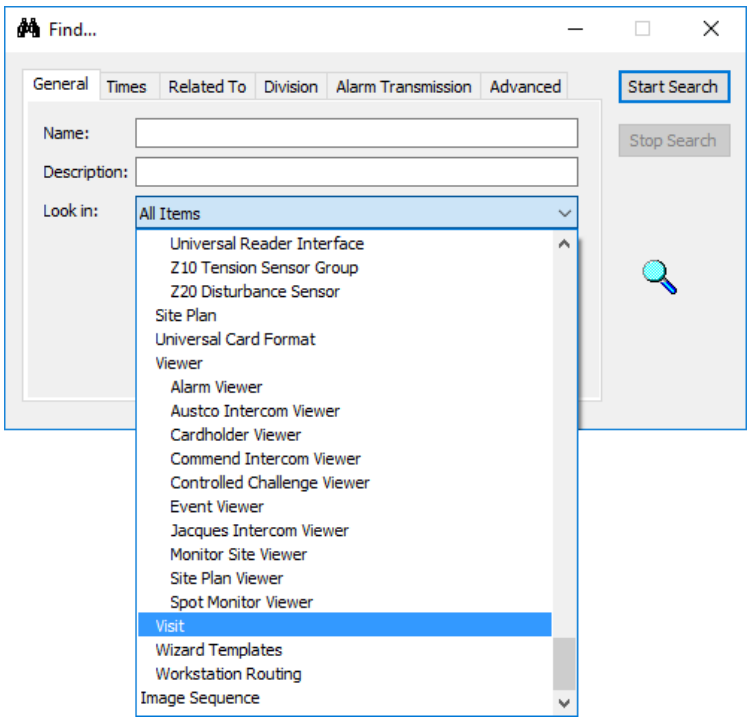
Note: Visits cannot be included in macros, or appear on Site Plans.

Operator Privileges

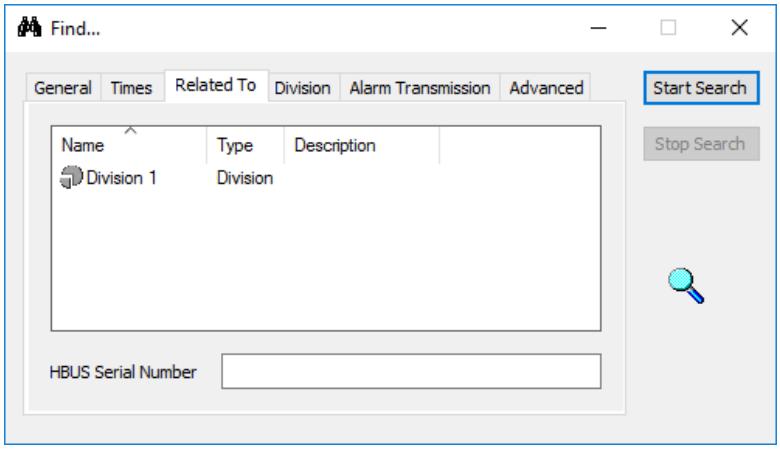
“View Visits” is required to view a Visit's properties.

Procedure

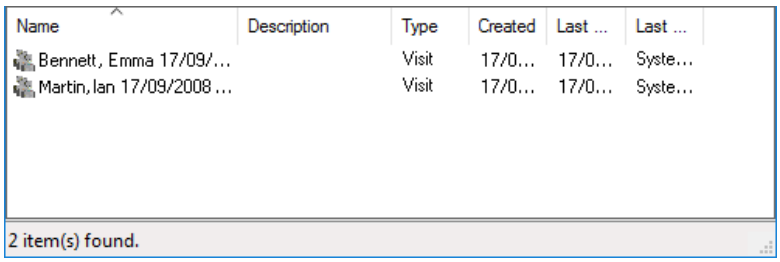
1. Click **Monitor** from the menu bar.
2. Click **Find...** to open the Find window.
3. Click the "Look In" field and select the option **Visit**.



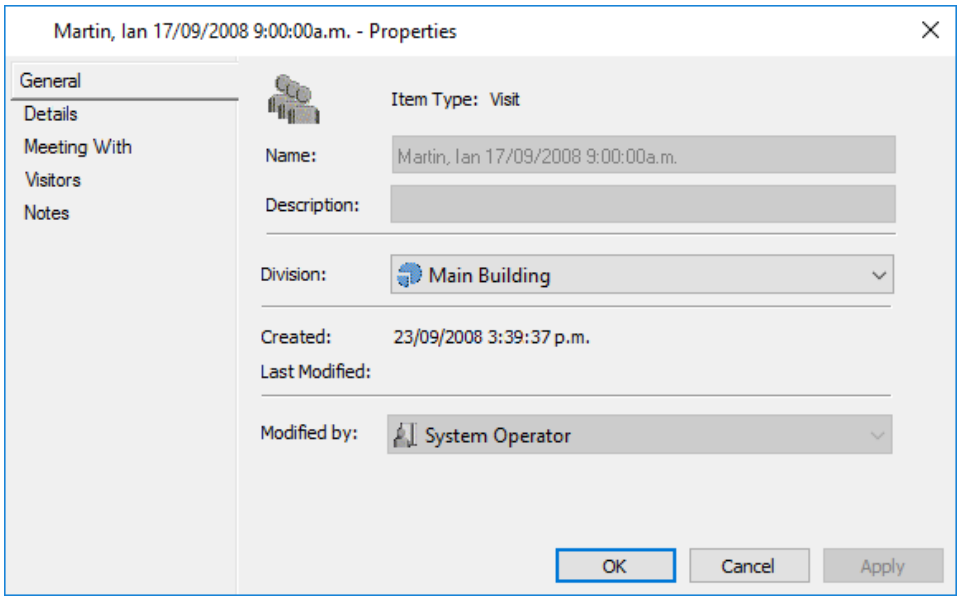
4. Click the **Related To** tab.
   The **Related To** tab searches for items in the "Look In" field on the **General** tab that are related to the item in this window.
5. Open the **Division** List Window.
6. Select the relevant Division(s) and drag and drop it into the "Related To" window.



7. Click the **Start Search** button.
   The Search window opens and displays all those pre-registered Visit(s) that are related to the Division(s) selected.

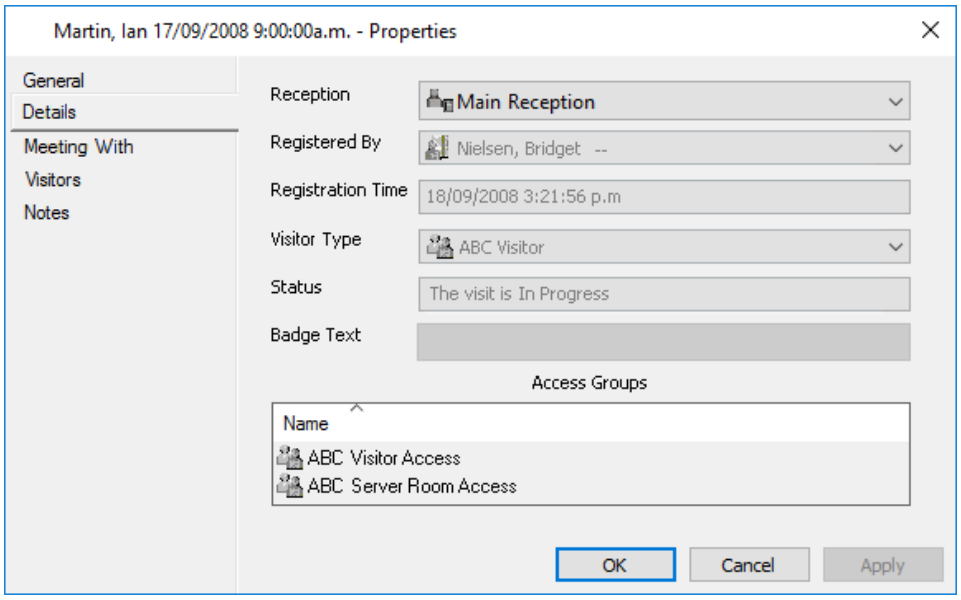


8. Double-click on the Visit you want to look at the details of.
   The **General** tab of the Visit property pages displays.



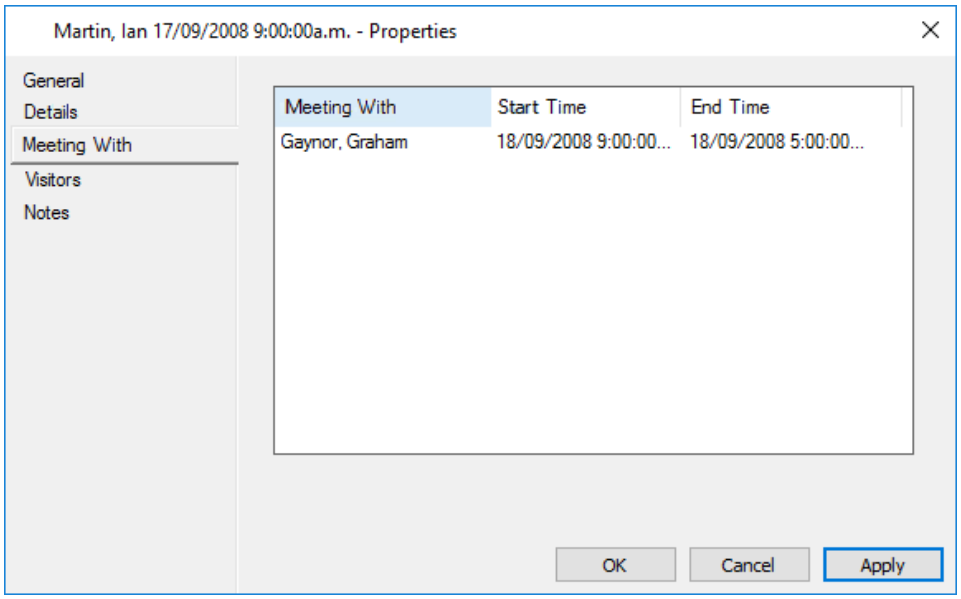
   All the fields on this screen are "read-only".

9. Click the **Details** tab.



All the fields on this screen are "read-only".

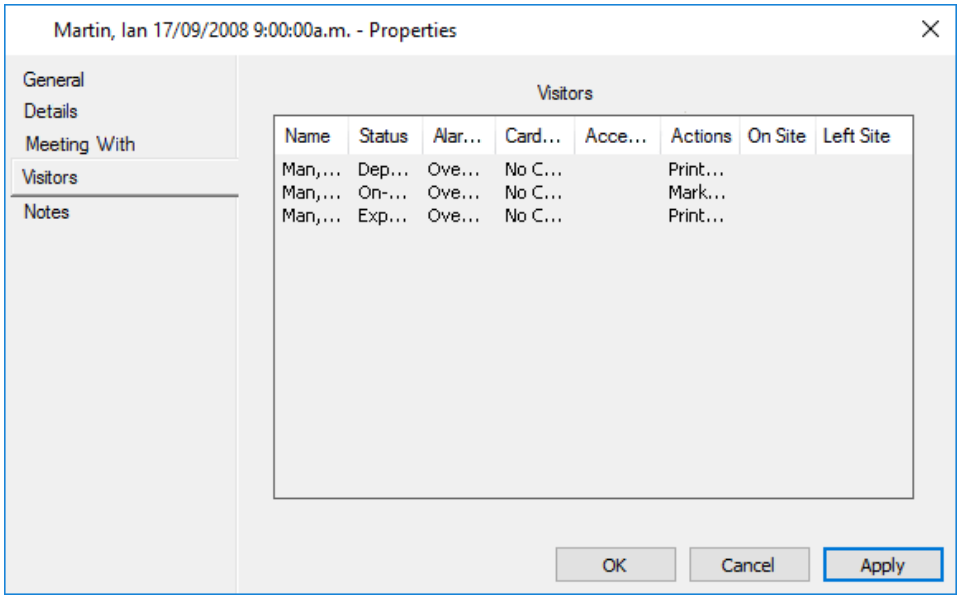
10. Click the **Meeting With** tab.



All the fields on this screen are "read-only". There are three columns of information:

- Meeting With
- Start Time
- End Time

11. Click the **Visitors** tab.

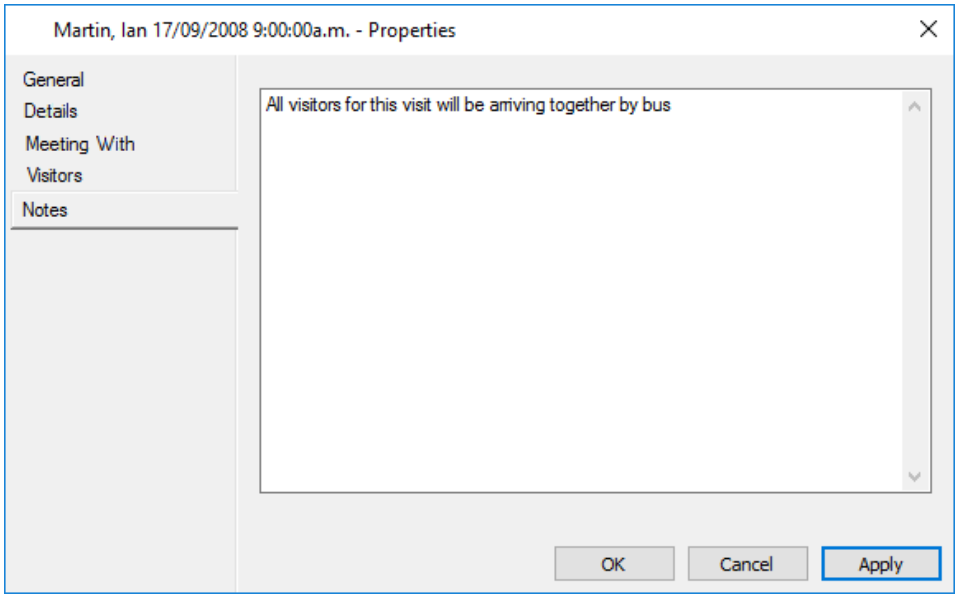


All the fields on this screen are "read-only". There are eight columns of information:

Column	Description
Name	The name of the visitor.
Status	The visitor's status for this visit. Available statuses are: • Expected • On-Site • Expected Back • Departed • Cancelled
Alarm State	The visitor's alarm state for this visit. Available alarm states are: • Ok • Due to Leave • Over Due
Card Issued	Available options for this column are: • **[Card Type Name] [card number]** This displays if a card has been issued to the visitor. • **No Card allocated** This displays if a card has not been issued to the visitor.

Column	Description
Access Groups	A comma separated list of the names of Access Groups that have been assigned to the visitor as part of the "Mark On-site" action.
Actions	A comma separated list of the names of actions that have been performed for this visitor. Action names are: • Print Badge • Assign Card • Mark On-Site • Temp Off-Site • Leave Site
On Site At	The actual time the visitor was marked as "On-site".
Left Site At	The actual time the visitor was marked as "Left Site".

12. Click the **Notes** tab.



If any "Notes" were entered in the Visitor Management application for this visit, they will appear on this screen. However, unlike the other tabs, this screen is **not** "read-only", (i.e. you can add a note(s) about this Visit if required).

For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).

Purging Expired Visits

Introduction

An automated purge runs daily to purge expired visits from the system. The ability to purge visits is only available at system level, therefore where the system is used by multiple companies, it will not be possible for them to purge visits according to different "number of days" settings.

You can configure the parameters for when expired visits will get purged from the system, (i.e. the time of day the purge will run, and the length of time visits are kept before they are eligible for purging), via the **Database Maintenance** tab in the Server Properties. See ***Database Maintenance*** (on page 6-57) for details.

Notes:

- The "purge process" cannot be disabled.
- In a multi-server system visits are not being replicated, so the purge needs to be run on each server running Visitor Management.

Operation

Only the visit information itself gets deleted. The following do **not** get deleted as part of the purge:

- Visitors assigned to the visit
- Events generated as part of the visit

An event is logged when the purge starts and another when the purge completes.

If the purge process encounters a visit which cannot be deleted, it will skip that visit and continue deleting the other visits. A message will be logged to the log file showing any available information why the visit failed to delete, and the "purge process" will try to delete the visit again during it's next run, (i.e. the next day).

Configuration Examples

The following examples show the recommended configuration and associated privileges necessary to perform certain Receptionist and Pre-registration functions. Also to help simplify your setup there are suggested Operator Groups for each example.

Note: With these examples, we recommend that you assign the "View Cardholders" privilege in the permanent cardholder division. If you are going to make certain PDFs 'required' for a visit, then the suggestion is to ensure that permanent cardholders already have PDF data for fields which are mandatory for a visit before attempting to add them to a visit.

- ***Example 1:***
  Single Company installation, single Visitor Management configuration (on page 50-55)
- ***Example 2:***
  Single Company installation, different Visitor Management configuration for Receptions (on page 50-59)
- ***Example 3:***
  Multi-tenanted installation, no common lobby Reception, data separation for the Companies (on page 50-64)
- ***Example 4:***
  Multi-tenanted installation, common lobby Reception, no data separation for the Companies (on page 50-65)

Example 1: Single Company installation, single Visitor Management configuration

Introduction

The following scenarios show the recommended set up where the system is for a single company with multiple Receptions. The Visitor Management configuration requirement is the same for all Receptions.

Scenario 1

The table below shows the privileges required for the Receptions where the Receptionist has the ability to:

- create and edit visits,
- create and edit visitor cardholder records,
- manage the Reception(s), (i.e. view the Home screen, perform the Visitor Management actions and print reports).

Additionally, it shows the privileges required if the Reception is set up for the badging of cards and the running of Macros (which is optional).

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
· contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes" "Manage Visitor Attributes" (needed if assigning escorts)
Visitor Division (has the *Visitor Management configuration* and is the *Save Visitors Division*)	
· contains Receptions · may contain the workstations, (i.e. located in Reception)	"Manage Receptions"
· contains Visits	"Edit Visits"
· contains Visitor Cardholders	"Edit Cardholders" / "Edit Cardholder Notes"
· Visitor Type Access Groups	"Modify Access Control" (needed for creating/editing visits)
· Access Groups (contains Access Zones and Schedules)	
· Visitor Card Type	(covered by the "Manage Reception" privilege)
· contains Doors (1 per workstation for Reception readers)	"View Event and Alarms" and "View Site" (needed if card badging is applicable for the Reception)
· Macros	"Run Macros" (needed if the Receptionist can run Macros)

To assign an access card to a cardholder the operator needs the "Create and Edit Cardholders" privilege in the division that the cardholder is stored. To prevent a permanent cardholder's existing access from fraudulently being given to a visitor the Visitor Management application will not allow a second card to be assigned to someone who already has a card assigned in the system. Therefore, the only circumstance where the system would allow the assignment of a Visitor Card to a permanent cardholder, and therefore require "Create and Edit Cardholders" privilege in the permanent cardholder division, would be where they did not already have a card assigned.

Scenario 2

The table below shows the privileges required for the Receptions where the Receptionist only has the ability to:

- view visits and visitor cardholder records,
- view the Home screen, and
- print reports.

To perform any actions the Receptionist would need "Edit Visits" privileges, so it is not possible to configure the system to allow the user to perform the Visitor Management actions but not directly edit the visit.
Note: In this sceanrio, the ability to View Visitors is inherited from the "View Cardholders" privilege in the parent division.

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
· contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes"
Visitor Division (has the *Visitor Management configuration* and is the *Save Visitors Division*)	
· contains Receptions · may contain the workstations, (i.e. located in Reception)	"Manage Receptions"
· contains Visits	"View Visits"
· contains Visitor Cardholders	No additional privilege required
· Visitor Type Access Groups	No privilege
· Access Groups (contains Access Zones and Schedules)	No privilege
· Visitor Card Type	No privilege
· contains Doors (1 per workstation for Reception readers)	No privilege
· Macros	No privilege

Scenario 3

The table below shows the recommended set up for users who can only pre-register visits.

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
• contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes"
Visitor Division (has the *Visitor Management configuration* and is the *Save Visitors Division*)	
• contains Receptions • may contain the workstations, (i.e. located in Reception)	
• contains Visits	"Edit Visits"
• contains Visitor Cardholders	"Edit Cardholders" / "Edit Cardholder Notes"
• Visitor Type Access Groups	"Modify Access Control"
• Access Groups (contains Access Zones and Schedules)	
• Visitor Card Type	No privilege
• contains Doors (1 per workstation for Reception readers)	No privilege
• Macros	No privilege

Recommended Operator Groups for Example 1

For the setup described in Example 1, (i.e. scenarios 1, 2 and 3), it is recommended that the following Operator Groups are created in order to simplify the allocation of user privileges:

Operator Group Name	Privileges / Divisions
Group 1	"View Cardholders" and "View Cardholder Notes" in the *Find Visitor in this Division*
Group 2	"Manage Visitor Attributes" in the *Find Visitor in this Division* **Note:** Where a Receptionist will be assigning escorts to visitors in a Division for which they only have "View Cardholder" privileges, (likely where the visitor is a permanent cardholder), the "Manage Visitor Attributes" privilege should be granted in that Division to enable them to perform that action.

Operator Group Name	Privileges / Divisions
Group 3	"View Visits" in the *Save Visitor in this Division*
Group 4	"Edit Visits", "Create and Edit Cardholders", "Edit Cardholder Notes" and "Modify Access Control" in the *Save Visitor in this Division*
Group 5	"Manage Receptions" in the *Save Visitor in this Division* Optionally: (in the *Save Visitor in this Division*) • "View Events and Alarms" – for card badging • "Run Macros" – for running macros

For a Reception where a Receptionist can create and edit visits, Groups 1, 2 (optional), 4 and 5 are required.

For a Reception where a Receptionist can only view visits, Groups 1, 3 and 5 are required.

For a Reception where the user only has the ability to pre-register visits, Groups 1 and 4 are required.

Example 2: Single Company installation, different Visitor Management configuration for Receptions

Introduction

The following example shows the recommended set up where the system is for a single company, but there is a requirement to configure the Receptions differently for Visitor Management.

Scenario 1

This table shows the privileges required assuming that the Receptionist has the ability to:

- create and edit visits,
- create and edit visitor cardholder records,
- manage the reception, (i.e. view the Home screen, perform the Visitor Management actions, and print reports for the Receptions shown).

Additionally the table shows the privileges required if the Reception is set up for the badging of cards and the running of Macros (which is optional).

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
• contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes" "Manage Visitor Attributes" (needed if assigning escorts)
Division 1 (has the *Visitor Management config*)	
• Reception 1, Reception 2 • Workstations for Reception 1 and Reception 2	"Manage Receptions"
Division 2 (has the *Visitor Management config*)	
• Reception 3 • Workstations for Reception 3	"Manage Receptions"
Visitor Division (is the *Save Visitors Division*)	"Manage Receptions"
• contains Visits	"Edit Visits"
• contains Visitor Cardholders	"Edit Cardholders" / "Edit Cardholder Notes"
• Visitor Type Access Groups	"Modify Access Control" (needed for creating/editing visits)
• Access Groups (contains Access Zones and Schedules)	
• Visitor Card Type	(covered by the "Manage Reception" privilege)
• contains Doors (1 per workstation for Reception readers)	"View Event and Alarms" and "View Site" (needed if card badging is applicable for the Reception)
• Macros	"Run Macros" (needed if the Receptionist can run Macros)

Note: In this setup the "Manage Receptions" privilege is required in the following divisions:

a) each Division containing a Reception, (e.g. Division 1 and/or Division 2) for which the user can act as a Receptionist. This determines the Receptions available for the Receptionist on their Home screen.

b) the Visitor Division. This indicates that the user is a Receptionist rather than someone who can only pre-register visits, and will allow them to see the Visitor Card Type details, required for validating that the card they have assigned to a visitor is valid, and is needed to perform the necessary configuration validation at logon.

Scenario 2

The table below shows the privileges required for the Receptions where the Receptionist only has the ability to:

- view visits and visitor cardholder records
- view the Home screen, and
- print Reports.

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
· contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes" "Manage Visitor Attributes" (needed if assigning escorts)
Division 1 (has the *Visitor Management config*)	
· Reception 1, Reception 2 · Workstations for Reception 1 and Reception 2	"Manage Receptions"
Division 2 (has the *Visitor Management config*)	
· Reception 3 · Workstations for Reception 3	"Manage Receptions"
Visitor Division (is the *Save Visitors Division*)	"Manage Receptions"
· contains Visits	"View Visits"
· contains Visitor Cardholders	No additional privilege required
· Visitor Type Access Groups	No privilege
· Access Groups (contains Access Zones and Schedules)	No privilege
· Visitor Card Type	No privilege
· contains Doors (1 per workstation for Reception readers)	No privilege
· Macros	No privilege

Note: In this setup the "Manage Receptions" privilege is required in the following divisions:

a) each Division containing a Reception, (e.g. Division 1 and/or Division 2) for which the user can act as a Receptionist. This determines the Receptions available for the Receptionist on their Home screen.

b) the Visitor Division. This indicates that the user is a Receptionist rather than someone who can only pre-register visits, and is needed to perform the necessary configuration validation at logon.

Scenario 3

The table below shows the recommended set up for users who can only pre-register visits.

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
• contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes"
Division 1 (has the *Visitor Management config*)	
• Reception 1, Reception 2 • Workstations for Reception 1 and Reception 2	"View Visits"
Division 2 (has the *Visitor Management config*)	
• Reception 3 • Workstations for Reception 3	"View Visits"
Visitor Division (is the *Save Visitors Division*)	
• contains Visits	"Edit Visits"
• contains Visitor Cardholders	"Edit Cardholders" / "Edit Cardholder Notes"
• Visitor Type Access Groups	"Modify Access Control" (needed for creating/editing visits)
• Access Groups (contains Access Zones and Schedules)	
• Visitor Card Type	No privilege
• contains Doors (1 per workstation for Reception readers)	No privilege
• Macros	No privilege

The "View Visits" privilege is required in Divisions 1 and 2 so that users can see Receptions in those divisions.

Recommended Operator Groups for Example 2

For the setup described in Example 2, (i.e. scenarios 1, 2 and 3), it is recommended that the following Operator Groups are created in order to simplify the allocation of user privileges:

Operator Group Name	Privileges / Divisions
Group 1	"View Cardholders" and "View Cardholder Notes" in the *Find Visitor in this Division*

Operator Group Name	Privileges / Divisions
Group 2	"Manage Visitor Attributes" in the *Find Visitor in this Division*
Group 3	"View Visits" in the *Save Visitor in this Division*
Group 4	"Edit Visits", "Create and Edit Cardholders", "Edit Cardholder Notes" and "Modify Access Control" in the *Save Visitor in this Division*
Group 5	"Manage Receptions" in the *Save Visitor in this Division*
Group 6	"View Events and Alarms" – for card badging, and "Run Macros" – for running macros in the *Save Visitor in this Division*
Group(s) 7	"Manage Receptions" in Division 1 **Note:** There should be one group for each division which has a Reception. Alternatively a single group could be used to assign the "Manage Receptions" privilege for all the Visitor Management configuration divisions.
Group(s) 8	"View Visits" in Division 1 This provides someone who can only pre-register visits with the privileges to see the Receptions in that Division without the ability to Manage those Receptions. **Note:** There should be one group for each division which has a Reception. Alternatively a single group could be used to assign the "View Visits" privilege for all the Visitor Management configuration divisions.

For a Reception where a Receptionist can create and edit visits, Groups 1, 2 (optional), 4, 5, 6 (optional) and 7 (whichever group contains the Reception) are required.

For a Reception where a Receptionist can only view visits, Groups 1, 3, 5 and 7 (whichever group contains the Reception) are required.

For a Reception where the user only has the ability to pre-register visits, Groups 1, 4 and 8 (whichever group contains the Reception) are required.

Example 3: Multi-tenanted installation, no common lobby Reception, data separation for the Companies

Introduction

The following example shows the recommended set up where the system is for a multi Company installation where it is important that the members of one company cannot see the visits and visitors for another company.

Scenario

This table shows the configuration recommended for this scenario:

Configuration	Privileges
Root Division **Company A Division** (is the *Find Visitors Division* for Company A) • contains Permanent Cardholders this can be configured as shown in Example 1 (if all Receptions for this company share the same configuration requirements), or as shown in Example 2 (if some Receptions for this company have different configuration requirements) **Company B Division** (is the *Find Visitors Division* for Company B) • contains Permanent Cardholders this can be configured as shown in Example 1 (if all Receptions for this company share the same configuration requirements), or as shown in Example 2 (if some Receptions for this company have different configuration requirements)	See previous Examples 1 and 2 for privileges

Recommended Operator Groups

The Operator Groups to be used will depend upon how the divisions for the individual companies are configured, but should be based on those shown in ***Recommended Operator Groups for Example 1*** (on page 50-57) and ***Recommended Operator Groups for Example 2*** (on page 50-62), taking into account they should be restricted by company.

Example 4: Multi-tenanted installation, common lobby Reception, no data separation for the Companies

Introduction

The following example shows the recommended set up where the system is for a multi Company installation and visitors are shared across companies.

Scenario

This table shows the configuration recommended for this scenario:

Configuration	Privileges
Root Division **Lobby Division** (is the *Find Visitors Division*) **Company A Cardholder Division** • contains Permanent Cardholders **Company B Cardholder Division** • contains Permanent Cardholders **Visitor Division** (has the *Visitor Management config* and is the *Save Visitors Division*) • contains Receptions • may contain the workstations, (i.e. located in Reception) • contains Visits • contains Visitor Cardholders • Visitor Type Access Groups • Access Groups (contains Access Zones and Schedules) • Visitor Card Type • contains Doors (1 per workstation for Reception readers) • Macros	The Lobby Receptionists will be given "View Cardholder" privileges either in the Lobby Division (which is the *Find Visitors Division*) or individual Company A and Company B Cardholder Divsions

Recommended Operator Groups

The Operator Groups will be based on those shown in ***Recommended Operator Groups for Example 1*** (on page 50-57).

Using Visitor Management

Introduction

This section provides instructional information for the Pre-registration users and Receptionist users of the Command Centre Visitor Management application.

This section has been divided into two parts:

- **Pre-registration and Receptionist functions:**

  This section is for Pre-registration users and Receptionists users. The role of a Pre-registration user is to create visits.

  Refer to ***Pre-registration and Receptionist functions*** (on page 50-68)

- **Receptionist functions:**

  This section is for Receptionist users only. The role of a Receptionist user is to create visits and process visitors.

Refer to ***Receptionist functions*** (on page 50-113)

Managing visitors

Below is an overview of the process you will need to perform in order to manage visitors on your site.

This process is divided into the two roles each user can perform.

User	Process
Pre-registration and Receptionist users	**Create visits:** • Create a visit in advance or when visitors arrive at the reception. • Add visitors to the visit. You can add an existing visitor or create a new visitor.

User	Process
Receptionist users only	**Process visitors:** When a visitor arrives: • Capture additional details about the visitor. • Optionally, issue a visitor badge, access card or assign an escort. • Mark the visitor 'On-Site'. When a visitor departs: • If issued, retrieve the visitor's badge and access card. • If required, mark the visitor 'Off-Site'. • When a visitor is overdue an alarm is raised in Command Centre.

Working with visitors

While this process describes how to manage visitors using Visitor Management, it is important to follow your company's visitor guidelines when interacting with visitors for your site.

Pre-registration and Receptionist functions

This section describes the functions you can perform if you are a Pre-registration or Receptionist user.

Select the topic below that you require further detail on:

- ***Getting started*** (on page 50-69)
- ***Knowing your way round*** (on page 50-77)
- ***The Visit screen*** (on page 50-83)
- ***The Find Visit screen*** (on page 50-96)

Getting started

This section describes a number of operations you will perform regularly when using Visitor Management.

Select the topic below that you require further detail on:

- ***Logon*** (on page 50-70)
- ***Logout*** (on page 50-75)
- ***Exit*** (on page 50-76)

Logon

Introduction

Your username and password will allow you to access Visitor Management. Your username and password are configured in the Command Centre Configuration Client. It is the responsibility of your Command Centre administrator to provide you with a username and password. If you wish to change your password, refer to ***Changing your password*** (on page 50-73).

Notes:

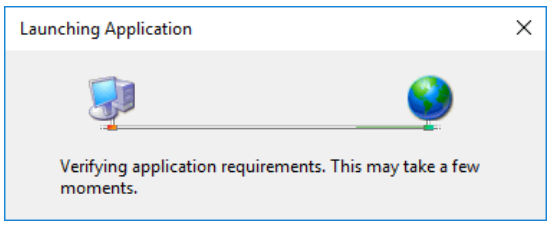
- If your Visitor Management configuration has changed in the Configuration Client, you need to log off and on again for the changes to take effect.
- When Visitor Management is launched, if the server to which the work-station is trying to connect to is enabled for Active Directory single sign-on (a licensable feature), the system will try to log the operator onto the Visitor Management client. If Active Directory single sign-on is being used, ensure you have a domain account, (e.g. Windowsuser@Gallagher.Local).

Procedure

Follow this procedure to log on and open Visitor Management:

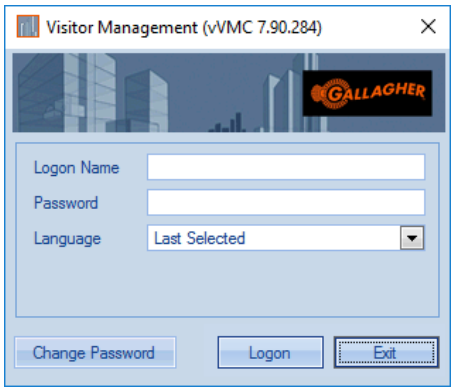
1. Either:
   - Double-click the **Visitor Management** icon on your Desktop, OR
   - From the **Start** menu, click **All Programs** > **Gallagher** > **Visitor Management**.

   The Launching Application window displays.



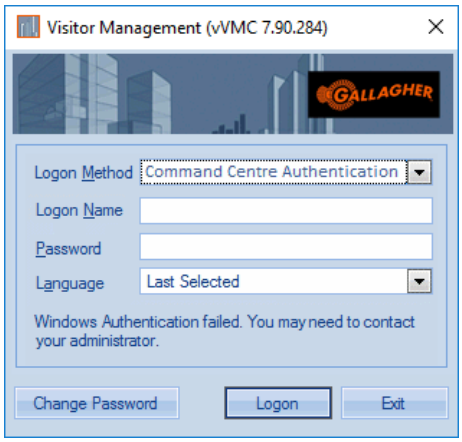
2. Is your site licensed for Active Directory single sign-on?

If...	then...
no	the following logon screen displays:



Go to Step 4.

If...	then...
yes	a progress dialog displays briefly. If automatic logon is possible, the Visitor Management main window displays. If not, an error message informing the user of the reason logon has failed displays, followed by the logon screen below:



Note: For the system to automatically log the operator onto Visitor Management the following must apply:

- the Active Directory is available
- the domain account used to log onto the network has not been disabled, deleted or locked out in Active Directory
- the domain account is linked to an operator in Command Centre.

Go to Step 3.

3. Select the appropriate Authentication Logon method from the **Logon Method** drop-down box.

If you click...	then...
Windows Authentication,	the system will find the operator linked to the user's domain account and log onto the workstation as that operator.
Command Centre Authentication,	this allows the operator to enter a Visitor Managment Logon Name and Password. Go to Step 4.

4. Type your **Logon Name**.
5. Click in the **Password** field (alternatively, press the **Tab** key).
6. Type your password.
   If your password has expired the Expired Password window displays, refer to ***Changing an expired password*** (on page 50-74).
7. The **Language** drop-down box provides a list of available languages.
   If you have previously logged in, **Last Selected** will be the first option, and this is selected by default.
   Select another language if required.

8. Click **Logon**.
   (Alternatively, press the **Enter** key).

   Note: If you are unable to log on, please contact your Command Centre administrator, or see ***Troubleshooting - Visitor Management Logon errors*** (on page 50-144) for further detail.

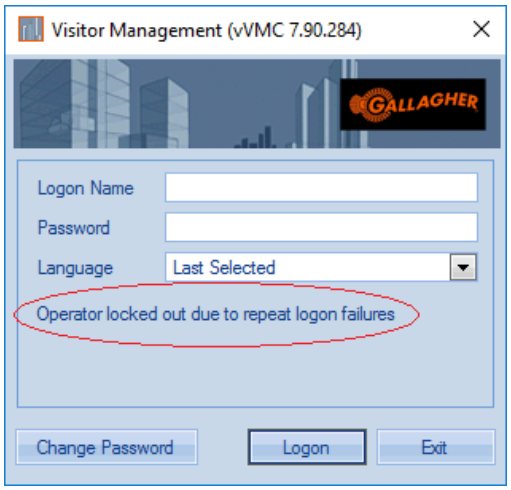
Result

Visitor Management opens. Your username is displayed on the Visitor Management status bar on the bottom right hand side.

- For Pre-registration users the Visit screen is displayed.
- For Receptionist users the Home screen is displayed.

Hint

Failed logons
If an operators' successive attempts reaches the configured 'number of failed attempts before lockout', then they will be locked out for the configured lockout period (or permanently if this option is set). A message will display on the logon screen indicating that the operator is locked out.



The lockout period (if any) will not be displayed. When the lockout period has completed, the logon name and password can be re-entered and authenticated successfully. If the operator needs the account unlocked, a privileged operator can do so via the **Operator Configuration** tab of the Cardholder properties.

Note: Lockout state does not get replicated to remote servers in a multi-server environment.

Changing your password

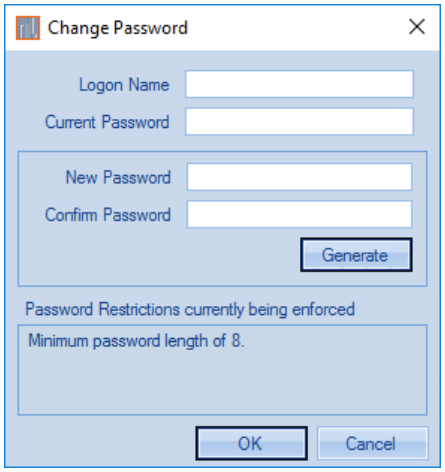
Introduction

If desired, you can change your current password. If password restrictions have been configured in Command Centre, these restrictions will be enforced. Your new password must meet all password restrictions.

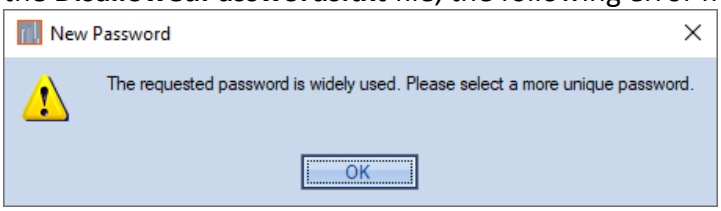
Procedure

Follow this procedure to change your current password:

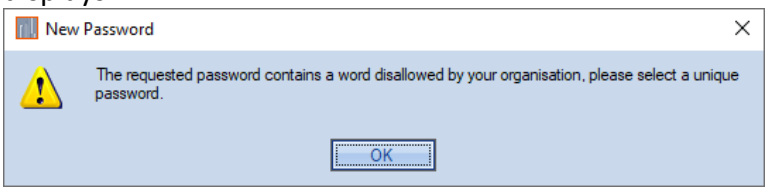
1. Click **Change Password**, located on the Logon window.
   The Change Password window displays.



2. Type your username in the **Logon Name** field.
3. Click in the **Current Password** field (alternatively, press the **Tab** key) then type your current **password**.
4. Generate a new password by either:
   - manually typing a password into the **New Password** field, and re-typing it in the **Confirm Password** field, OR
   - clicking the **Generate** button to generate a random password.
     A system generated password populates the **New Password** field and the **Confirm Password** field is disabled.
5. Click **OK** (alternatively, press the **Enter** key).
   A message box displays confirming your password has changed, or if it did not change then it provides a reason why.
   Note: The system will not allow the new password if it is commonly used or contains a specific string, as listed in the **DisallowedPasswords.txt** or **ContextSpecificPasswords.txt** files that are pre-installed with Command Centre.
   - If the new password is one of the commonly used passwords listed in the **DisallowedPasswords.txt** file, the following error message displays:



- If the new password is not allowed due to containing a word(s) listed in the **ContextSpecificPasswords.txt** file, the following error message displays:



For For further details see ***Preventing context specific passwords*** (on page 2-22).

Changing an expired password

Introduction

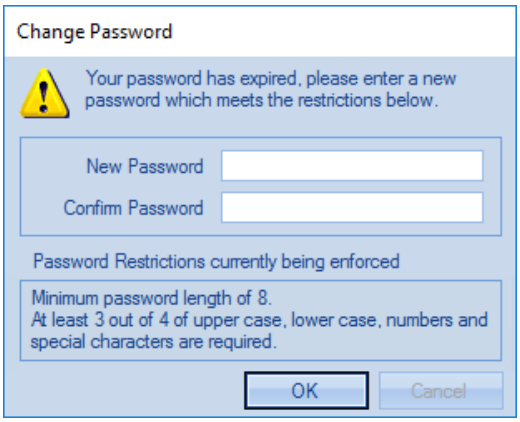
When you attempt to log on using an expired password, the Expired Password window displays. This window enables you to change your expired password.

If password restrictions have been configured in Command Centre, these restrictions will be enforced. Your new password must meet all password restrictions.

Procedure

Follow this procedure to change an expired password:

1. When you attempt to log on using an expired password, the Expired Password window displays.



2. Type your **new password**. Your new password must meet the password restrictions currently being enforced.
3. Click in the **Confirm Password** field (alternatively, press the **Tab** key).
4. Re-type your **new password**.
5. Click **OK** (alternatively, press the **Enter** key).

Logout

Introduction

For security and integrity, it may be important to log out when you are away from the computer.

Procedure

Click **Logout** on the toolbar.

Result

- Visitor Management closes.
- The logon window automatically displays; waiting for the next user to logon.

Automatic Logout

An "automatic logout" time can be configured by your Command Centre administrator, so that operators are logged off Visitor Management after a specified period of inactivity, closing all windows and discarding any unsaved changes.

See ***Automatic Logoff*** (on page 2-12) for a full explanation.

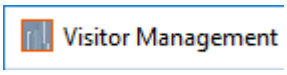
Exit

Introduction

In one procedure, you can log off and close Visitor Management.

Procedure

Either:

- Click  on the Visitor Management window, or
- Click 

on the Visitor Management window.

  A drop down command list displays. Click **Close**.

Result

Visitor Management closes.

Hint: Logout instead of exiting, to avoid having to restart Visitor Management.

Knowing your way round

This section describes a number of procedures that may make your life easier when using Visitor Management. If you are familiar with the Windows Operating System you may have already encountered some of these procedures.

Select the topic below that you require further detail on:

- ***Sizing the windows*** (on page 50-78)
- ***Selecting visitor records*** (on page 50-79)
- ***Viewing confirmation messages*** (on page 50-80)
- ***Using the toolbar*** (on page 50-81)
- ***Using macros*** (on page 50-82)

Sizing the windows

Introduction

If a window is too big or too small, you can change its size.

This is particularly useful if you want to view all displayed information.

Hint: It is recommended that you resize the Visitor Management window to maximum size. To maximise the window, click the  on the Visitor Management window.

Procedure

1. Move the mouse cursor to an edge of the window.
2. When the cursor changes to a "double-headed arrow", click and hold down the mouse button.
3. Move the mouse and the window resizes.
4. When the window is the required size, release the mouse button.

Result

The window is resized.

Hint: You can size the window vertically, horizontally or both directions at the same time.

Selecting visitor records

Introduction

You can select more than one visitor record (row) at a time.

This is particularly useful if you want to perform an action for more than one visitor.

Procedures

- To select multiple consecutive rows, click on the top and bottom row required while holding down the Shift key. The two rows clicked on and all rows in between are highlighted to show they have been selected.
- To select multiple rows which are not consecutive, click on each row required while holding down the Control key. All rows clicked on are highlighted to show they have been selected.
- To deselect a row, click the row required while holding down the Control key. The row will display as deselected.
- To select all rows shown in the grid, hold down the Control 'A' keys. All rows are highlighted to show they have been selected.

Example

Davis, Stephen	Avery, Kahlia	ReadDX Limited	10:00	12:00
Hale, Jennifer	Jennings, Mark	InfoTech Limited	09:00	17:00
Hamilton, Karen	Jennings, Mark	InfoTech Limited	09:00	17:00
Robinson, Peter	Avery, Kahlia	ReadDX Limited	10:00	12:00
Singh, Suniel	Jennings, Mark	InfoTech Limited	09:00	17:00
Withers, Kate	Avery, Kahlia	ReadDX Limited	10:00	12:00

Viewing confirmation messages

Introduction

When a function or action is performed, a confirmation message displays on the status bar. For example:

- If you are a Pre-registration user who is searching for a visit and you want to verify the number of visits found that match the search criteria you entered, (e.g. Found 10 Visits).
- If you are a Receptionist user who has performed an action and you want to verify the number of visitors the action was performed for, (e.g. 2/3 on-site actions were successful and 1/3 were unsuccessful).

Procedure

View the status bar to confirm your most recently performed function or action. The status bar is located at the bottom of the Visit, Find Visit and Home screens.

Example



Using the toolbar

Description

The toolbar is located at the top of the screen and displays when you first log on. Your user role determines what toolbar is displayed.

The Pre-registration user's toolbar



This table explains the function of each button shown on the Pre-registration user's toolbar:

Button	Function
Visit	Click to create a visit
Find Visit	Click to find a visit
Help	Click to display the Help, alternatively press F1
	Hover the mouse over the Help button to view the version number of the Visitor Management application installed.
Logout	Click to log off

The Receptionist user's toolbar



This table explains the function of each additional button shown on the Receptionist user's toolbar:

Button	Function
Home	Click to display visitors on a visit
Macros	Click to perform a pre-programmed operation in Command Centre. Note, macros will only display if configured by your Command Centre administrator.

Using macros

Introduction

Macros are valid for Receptionist users only.

A macro is a pre-programmed override configured in Command Centre by your Command Centre administrator. Macros can be used to perform various functions, (e.g. lockdowns, generate a silent alarm or evacuation report).

If your Command Centre administrator has configured a macro for your reception workstation, this macro will display as a button on your toolbar.

Procedure

To activate a macro, click the **button** for the macro you want to activate.

Your selected macro will be activated automatically. A confirmation message is not displayed.



The Visit screen

Description

The Visit screen enables you to create, edit, copy, cancel, restore and view a visit. This screen displays details about the visit and lists each visitor on the visit.

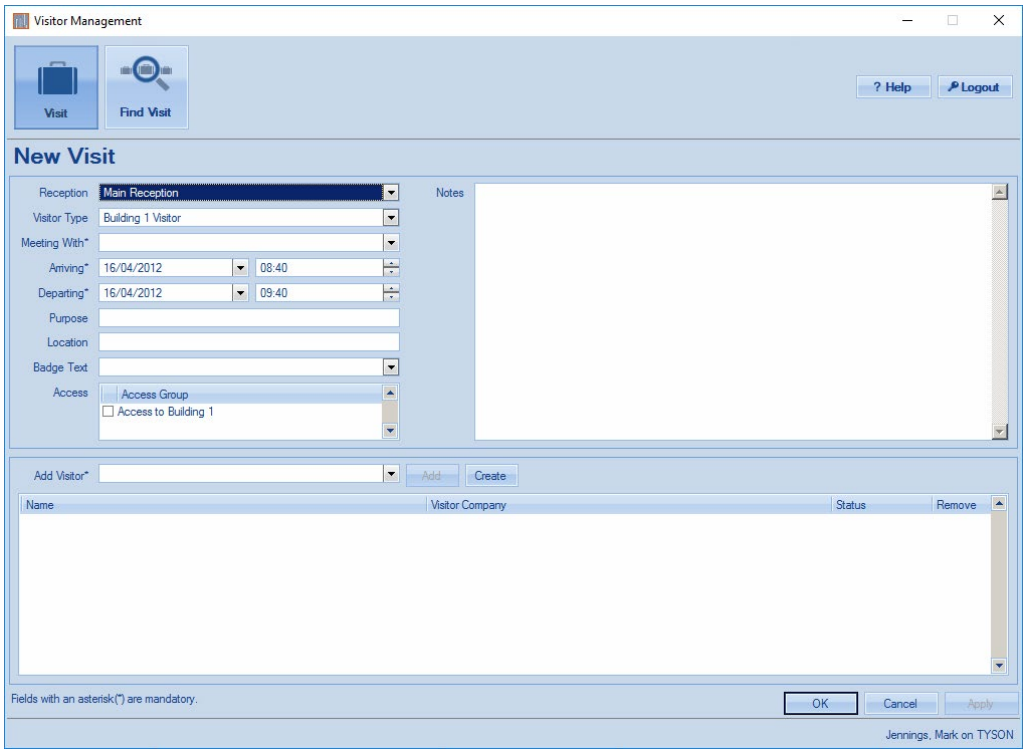
Notes:

- If you are a Pre-registration user, this screen displays automatically at logon.
- Pre-registration users require the "Edit Visits" operator privilege to create and edit visits.

To open the Visit screen either:

- click the **Visit** button located on the toolbar (which creates a new visit), or
- double click a visitor record, or
- click the visit icon 

The Visit screen



The Visit screen displays your default reception, the columns and action buttons (if applicable) for this reception, as configured in Command Centre.

Fields on the Visit screen

This table describes the mandatory (*) fields on the Visit screen.

Field	Description
Reception	This drop down is populated with a list of receptions you can edit or view visits for. The reception selected determines if the Badge Text and Access fields are displayed.
Visitor Type	This drop down is populated with a list of visitor types valid for the selected reception.
Meeting With	This drop down is populated with a list of cardholders who can host visits for the selected visitor type for this reception (once you have started typing a value into the field).
Arriving	This is the planned start date and time for the visit. **Note:** This field defaults to the current date and time.
Departing	This is the planned end date and time for the visit. **Note:** The date defaults to the current date. The time defaults to the standard end of day time. If the visit is created after the standard end of day time and before the standard start of day time on the following day, the time will default to 1 hour after the arriving time.

This table describes the non-mandatory fields on the Visit screen.

Field	Description
Purpose	Enter a purpose for the visit.
Location	Enter a free text location for the visit.
Badge Text	This field will only appear if configured in Command Centre. This field enables you to select text to be printed on the visitor's badge.
Access	This field will only appear if configured in Command Centre. This field enables you to specify what access will be given to the visitors on this visit when they are marked on-site.
Notes	Enter a note for the visit.

Visit status

The visit status is shown in the top left corner of the Visit screen.

This table describes each visit status.

Visit status	Description
New Visit	The visit is being created.
Visit Scheduled	The visit has been saved but no visitors have been marked on-site.
Visit In Progress	At least one visitor has been marked on-site.
Visit Completed	All visitors have been marked off-site or cancelled.
Visit Cancelled	The visit has been cancelled.

Note: In the event that some visitors on a visit have not arrived before the last on-site visitor has been marked off-site, it is assumed the remaining visitors won't be coming.

If it is assumed the remaining visitors won't be coming the visit status will be set to 'Completed' and the expected visitors 'Cancelled'. However, if one of the expected visitors has been assigned an access card the visit status will remain 'In Progress'.

Creating a visit

Introduction

When a visitor plans to arrive or arrives at your reception you will need to create a visit.
Hint: It is recommended that you create a visit before the visitor arrives. This saves check-in time and informs the person at the reception or security gate that one or more visitors are expected.

Procedure

Perform the following procedure to create a visit:

1. Click the **Visit** button located on the toolbar or click the **New Visit** button on the Visit screen. A new visit is created and the status of the visit is set to 'New Visit'.
2. Select a **Reception** from the Reception drop down. This is where the visitor will arrive. Refer to ***Managing multiple receptions*** (on page 50-88).
   Note: Changing the reception may affect the information already entered for the visit.
3. Select a **Visitor Type** from the Visitor Type drop down. This drop down is populated with a list of visitor types valid for the selected reception.
   Notes:
   - Only one visitor type can be selected per visit.
   - If the visitor type is changed and an access group has been selected, the access group may not be valid for the new visitor type.
   - If the visitor type is changed the Meeting With field will be set to blank.
4. To enter a Host in the **Meeting With** field, either:
   - badge a valid Host card at the reception reader. The Host displays. Or,
   - present a valid Host biometric sample at the reception reader. The Host displays. Or,
   - enter the first 3 characters of the Host's name and select the Host from the Meeting With drop-down list. This drop-down is populated with a list of cardholders who can host visits for the selected visitor type.
5. Enter the **Arriving** date and time for the visit.
6. Enter the **Departing** date and time for the visit.
7. Optionally, enter a **Purpose** for the visit.
8. Optionally, select a **Badge Text** entry from the Badge Text drop down. This text will be printed on the badge label for each visitor for this visit. This drop down is populated with a list of badge text entries valid for the selected reception.
9. Optionally, select one or more **Access Groups**, refer to ***Assigning access*** (on page 50-89).

10. Optionally, enter a **Note** for the visit. A note could be information about the visit, information about the visitors, instructions for the visit or preparations required for the visit.
11. **Add Visitors** to the visit. To create a visit at least one visitor must be added to the visit.

If you want to…	then…
Add a visitor (visitor previously created)	a) Enter a minimum of three characters into the **Add Visitor** field. A list of possible matches display. As more characters are entered the list becomes further refined. Configuration in Command Centre determines what the search and match is performed on. It will be either: • visitor name only, or • visitor name and any of the PDFs selected in the Find Visitor configuration. • Visitor names are checked for matches and the system returns entries where there is a match on any part of the name. If PDF searching is included, not only is the name checked for matches but the system also includes in the match list any visitors where the characters entered match the characters at the beginning of any of those PDF fields. **Note:** The **Visit** screen only displays the Name field plus four PDFs. If there are more than four PDFs selected for inclusion in searching, even though they will not all display, searching will still be performed on all of them. b) Select a visitor from the list and click **Add**. The visitor displays below.
Create a visitor	click **Create**. The Create Visitor screen displays. Refer to ***Creating a visitor*** (on page 50-90).

12. Ensure all mandatory (*) fields have been completed for the visit then click **OK** or **Apply** to save the visit. The status of the visit is set to 'Scheduled'. The status of each visitor is set to 'Expected'.

Managing multiple receptions

Introduction

Your system may have been configured with multiple receptions. If so, you may be able to view or manage multiple receptions from the one computer.

Note: The receptions you can view or manage are configured by your Command Centre administrator in Command Centre.

Definition

A reception is where visitors arrive and are processed. Visits and visitor data is specific to a reception, hence visits and visitors are saved within a reception.

Multiple reception examples

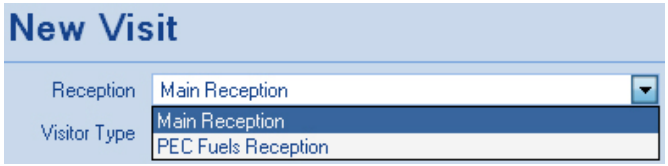
- A multi-tenanted building may have multiple receptions (a reception for each tenant).
- An international organisation may have multiple receptions (a reception in each country). Note, if a reception is in a different country the time zone will be different.

Selecting a reception

Receptions can be selected on each of the following screens:

- **Visit screen**

  Select a reception from the **Reception** drop down list. This list displays the receptions you can view or manage.



- **Home screen**

  Select a reception from the **Reception** drop down list. This list displays the receptions you can view or manage.



Multiple users managing the same reception

In the event you cannot perform an action for an item, due to another user editing the item, a message displays "Locked for editing". Please wait then try again.

Defining access for a visit

Introduction

The access defined for a visit controls what secure areas a visitor can access on-site, using the access card they have been assigned by the receptionist.

Access is defined in the visit but only granted once a visitor has been marked on-site. When a visitor is marked off-site or temporarily off-site, access is removed from the visitor.

Notes:

- When access is changed for a visit, access is changed for all visitors on the visit.
- If your site has designated exit readers for visitors to badge their cards at when leaving, they will need access to the exit zones, otherwise they will be denied access and will not be marked off-site.
- When defining access it may be important to have a generic access group selected that enables visitors to exit the site during an emergency.
- In the event some visitors require different access for the visit, these visitors should be assigned to a different visit.

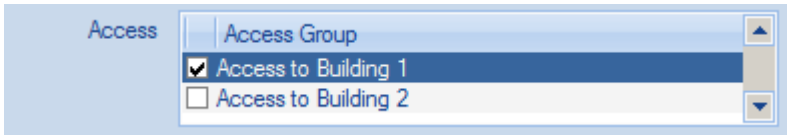
Procedure

To define access for a visit, select one or more access groups by ticking the corresponding checkbox for each access group.

Note: This field is populated with a list of access groups valid for the selected visitor type.

Example

In the example below access has been defined for building 2.



Creating a visitor

Introduction

You will need to create a new visitor record when someone who has not visited before (not in the system) arrives at your site.

When a visitor is created personal details are recorded about the visitor. Personal details are items such as: visitor name, visitor company, contact details, notes, photograph, etc.

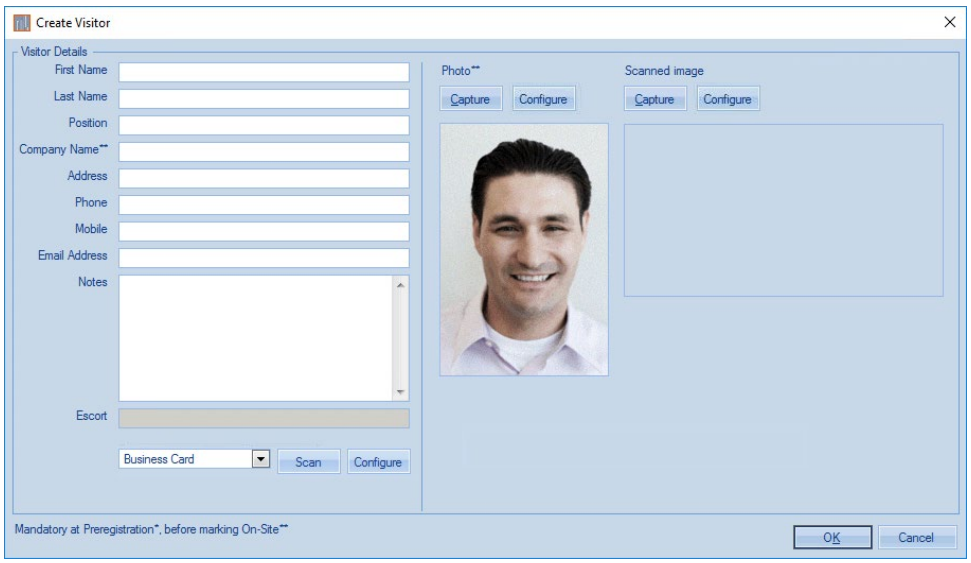
The visitor type determines what visitor details can be recorded for the visitor and what details are mandatory (*must be recorded in order to save the visitor). Hence, the fields shown on the Create Visitor screen can vary depending on the visitor type.

Note: Your Command Centre administrator will configure what personal details can be recorded for each visitor type.

Procedure

Perform the following procedure to create a visitor:

1. Click the **Create** button located on the Visit screen.
   The Create Visitor window opens.



   Note: Fields marked with an asterisk (*) are mandatory in order to save the visitor. Fields marked with two asterisks (**) are mandatory before marking a visitor on-site.

2. Enter the **First Name** of the visitor into the First Name field. This field is limited to 50 characters.
3. Enter the **Last Name** of the visitor into the Last Name field. This field is limited to 50 characters.

4. Optionally, enter the visitors **Contact Details** into any Contact Details fields that appear, (e.g. Phone, Mobile, Email or Address).
5. Optionally, enter a **Note** for this visitor into the Notes field.
   This field is limited to 2500 characters.
6. Optionally, click **Capture** to capture an image to store against the visitor, (e.g. a photo of the visitor).
   See ***Capturing images to store against a visitor*** (on page 50-102) for a detailed procedure.

   Note: A capture device must be connected and configured.
7. Optionally, visitor details can be captured by scanning their business card, passport or driver's license.
   See the appropriate topic for a detailed procedure. Either:

   - ***Scanning business cards for visitors*** (on page 50-106), OR
   - ***Scanning passports or driver licenses for visitors*** (on page 50-109)

   Note: The appropriate capture device for the form of ID being scanned must be connected and configured.
8. Complete any additional fields as required by the visitor type.
9. Click **OK** to save the visitor. The visitor is stored in the system and added to the current visit.

   Note: If configured an Escort field may be displayed. The Escort field is read-only and is updated when an escort has been assigned to the visitor.

Removing a visitor from a vist

Introduction

Only a visitor whose status is set to 'Expected' can be removed from a visit.

Note: If an access card has been assigned to the visitor, you will need to unassign the access card before the visitor can be removed.

Procedure

To remove a visitor, click the remove visitor icon of the visitor you want to remove from the visit.



Editing a visit

Introduction

Only a visit with a status of 'Scheduled' or 'In Progress' can be edited.
Notes:

- The reception cannot be changed if a visitor has been marked on-site.
- The visitor type cannot be changed once the visit has been saved.
- Changing the access will change the access for all visitors on the visit.

Procedure

To edit a visit, complete the following procedure:

1. Find the appropriate visit. Refer to ***Finding a visit*** (on page 50-97).
2. Open the visit. The Visit screen will display all fields as previously entered.
3. Edit the necessary fields, as required.
4. Click **OK** or **Apply** to save your changes.

Copying a visit

Introduction

Copying a visit creates an exact copy of the visit.

It is recommended that you copy visits for frequent visitors to your site. Once copied you can simply change the visit date and time as required.

Procedure

To copy a visit, click the **Copy Visit** button located on the Visit screen. The status of the visit is set to 'New Visit' and the status of each visitor is set to 'Expected'.

Cancelling a visit

Introduction

Only a visit with a status of ‘Scheduled’ can be cancelled.

Note: If a card has been assigned to a visitor in advance of them arriving for a visit, it must be removed before the visit can be cancelled.

Procedure

To cancel a visit, click the **Cancel Visit** button located on the Visit screen. The status of the visit is set to ‘Cancelled’. The status of each visitor is set to 'Cancelled'.

Restoring a cancelled visit

Only a visit with a status of ‘Cancelled’ can be restored.

To restore a cancelled visit, click the **Restore Visit** button located on the Visit screen. The status of the visit is set to ‘Scheduled’. The status of each visitor is set to ‘Expected’.

The Find Visit screen

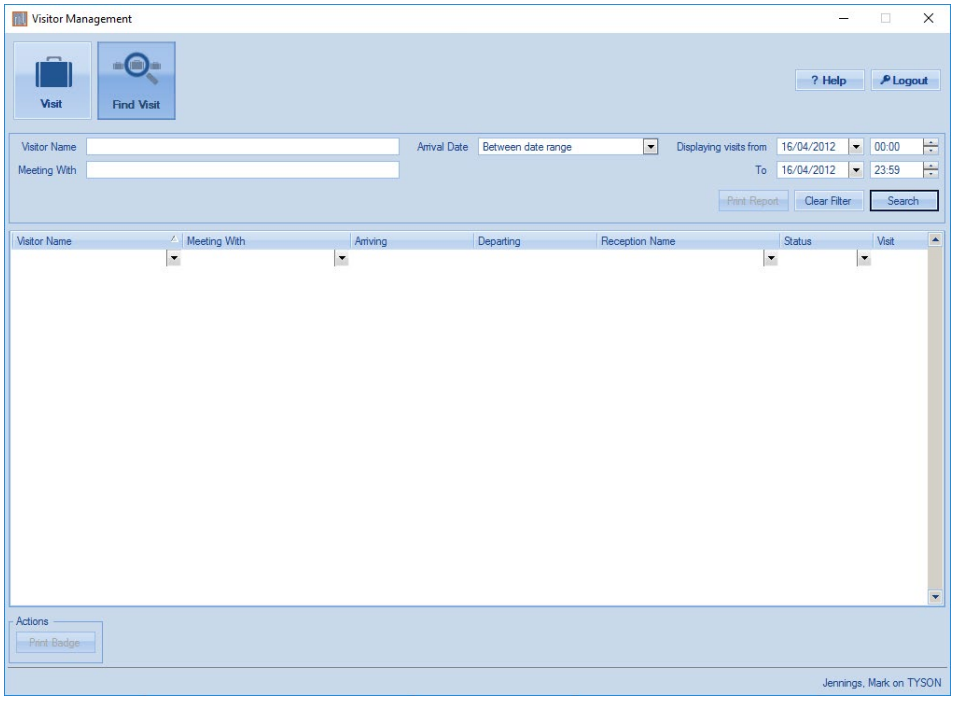
Description

The Find Visit screen enables you to search for a visit. You can enter different search criteria to help you find a visit.

Search results will display the visitors on the visit. If required you can use the filter to filter your search results. Refer to ***Filtering visitor records*** (on page 50-98).

To open the Find Visit screen click the **Find Visit** button located on the toolbar. The Find Visit screen displays the search criteria and results from your previous search.

The Find Visit screen



Fields on the Find Visit screen

This table describes the fields on the Find Visit screen.

Field	Description
Visitor Name	Enter the name of a visitor who is on the visit you want to find.
Meeting With	Enter the name of the person meeting with the visitors for the visit you want to find.
Arrival Date	Select the arrival date of the visit that you want to find or enter a 'Between date range' to find all visits that occurred within a specific timeframe.

Finding a visit

Introduction

This topic describes how to find a visit. You may want to find a visit in order to:

- view a visitor on the visit
- edit the visit, (e.g. departure time)
- print visitor badges, if applicable (e.g. at the end of the day, print visitor badges for visitors that are due to arrive the following day)

Procedure

Perform the following procedure to find a visit:

1. Click the **Find Visit** button located on the toolbar. The Find Visit screen displays. This screen displays the search criteria and results from the last search.
2. Either:
   - enter the name of a visitor on the visit into the Visitor Name field, or
   - enter the name of the person meeting with the visitors, for the visit into the Meeting With field, or
   - select an arrival date from the Arrival Date drop down list. If 'Between date range' is selected, date and time fields are displayed, you will need to enter a date range and time

     Note: Name matching is not case sensitive.
3. Click **Search**. Results are displayed for each visitor on a visit (including visits which have been cancelled or where the visitor has not turned up) which match the search criteria entered.

   Visitor search results are displayed in ascending visitor name order. To sort rows by ascending or descending order, click the column header.
4. To view the visit, click the visit icon  or double click the visitor record.

Filtering visitor records

Introduction

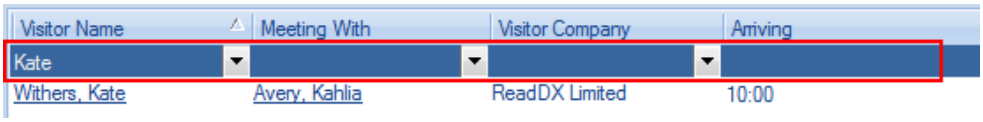
This topic describes how to filter visitor records. The filter works by filtering records shown on either the Find Visit or Home screens. You may want to filter visitor records in order to quickly find a visitor, host or visit.

Procedure

Perform the following procedure to filter visitor records:

1. Enter the criteria you want to search for into the 'Visitor Name' column of the filter row.

   The filter row is the blank row shown at the top of the Find Visit and Home screens.



2. The filter starts filtering after the first character has been typed. Entry of additional characters will further refine the search.

   To clear the data displayed in the filter row, click **Clear Filter**.

Printing a Find Visit report

Description

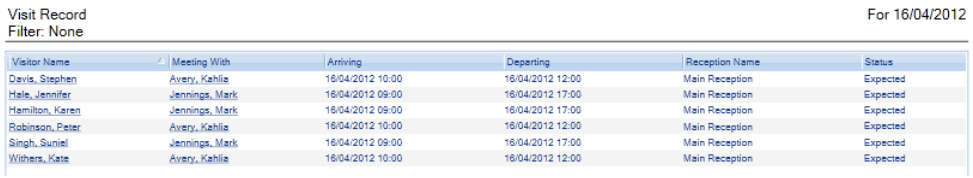
The Find Visit report records the information shown on the Find Visit screen. The Find Visit report takes into account the filtering used on the Find Visit screen.

You may want to print a Find Visit report to record the time and attendance of a particular visitor, or record the visits that occurred on a particular date.

To print a Find Visit report, click the **Print Report** button located on the Find Visit screen.

The Find Visit report

This report shows all visits that are expected to occur on the: 16/04/2012.



Visit Record
Filter: None

For 16/04/2012

Visitor Name	Meeting With	Arriving	Departing	Reception Name	Status
Davis, Stephen	Avery, Kahlia	16/04/2012 10:00	16/04/2012 12:00	Main Reception	Expected
Hale, Jennifer	Jennings, Mark	16/04/2012 09:00	16/04/2012 17:00	Main Reception	Expected
Hamilton, Karen	Jennings, Mark	16/04/2012 09:00	16/04/2012 17:00	Main Reception	Expected
Robinson, Peter	Avery, Kahlia	16/04/2012 10:00	16/04/2012 12:00	Main Reception	Expected
Singh, Suniel	Jennings, Mark	16/04/2012 09:00	16/04/2012 17:00	Main Reception	Expected
Withers, Kate	Avery, Kahlia	16/04/2012 10:00	16/04/2012 12:00	Main Reception	Expected

Note: The user who requested the report and the date and time the report was generated is displayed at the bottom.

Viewing a visitor's details

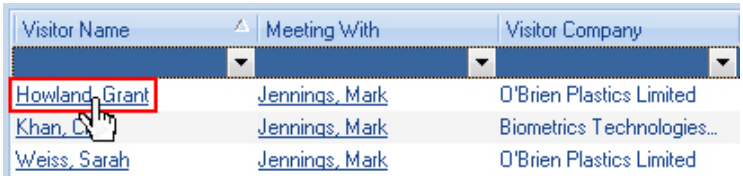
Introduction

You can view a visitor's details when you open the visitor.

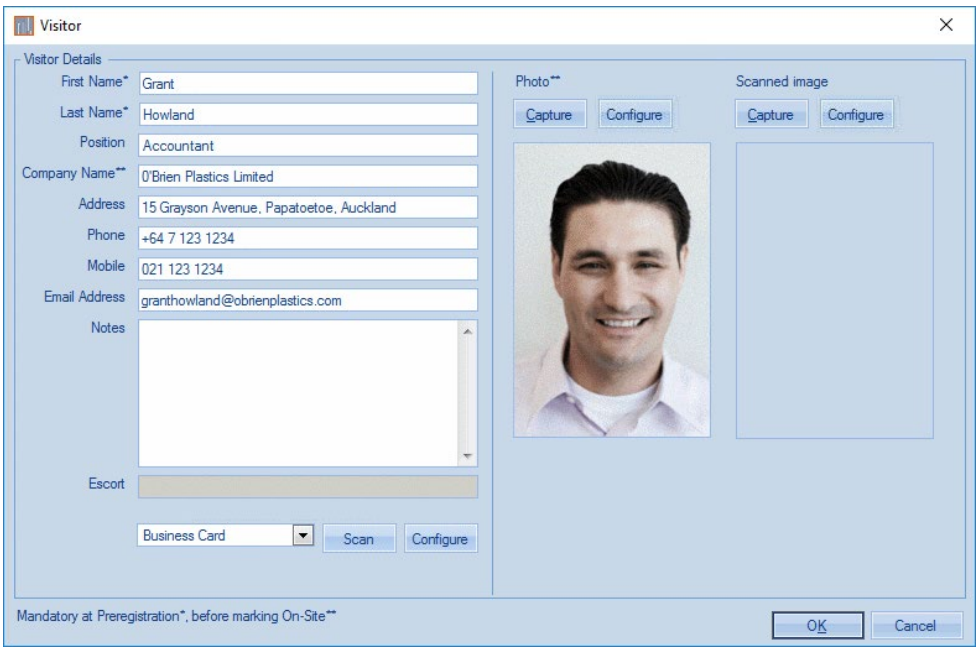
Viewing a visitor's details

Perform the following procedure to view a visitor's details:

1. Click the **Visitor Name** hyper-link located on either the Visit, Find Visit or Home screens.



2. The visitor's details are displayed in the Visitor window.



Note: All data captured for a visitor is displayed when a Receptionist user views the visitor's details via the Visitor Search window. For example, a visitor may have attended multiple visits that required different personal details to be captured for each visit. If you are viewing visitor details from a visit, only the visitor details applicable to the visitor type for the visit will display.

Editing a visitor's details

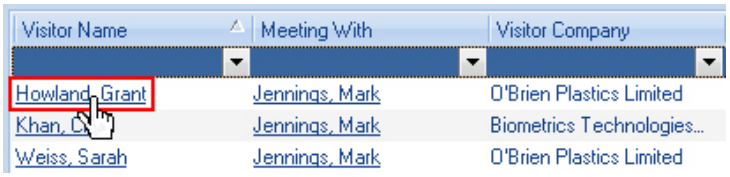
Introduction

You can edit a visitor's details when you open the visitor, if you have the required user privileges.

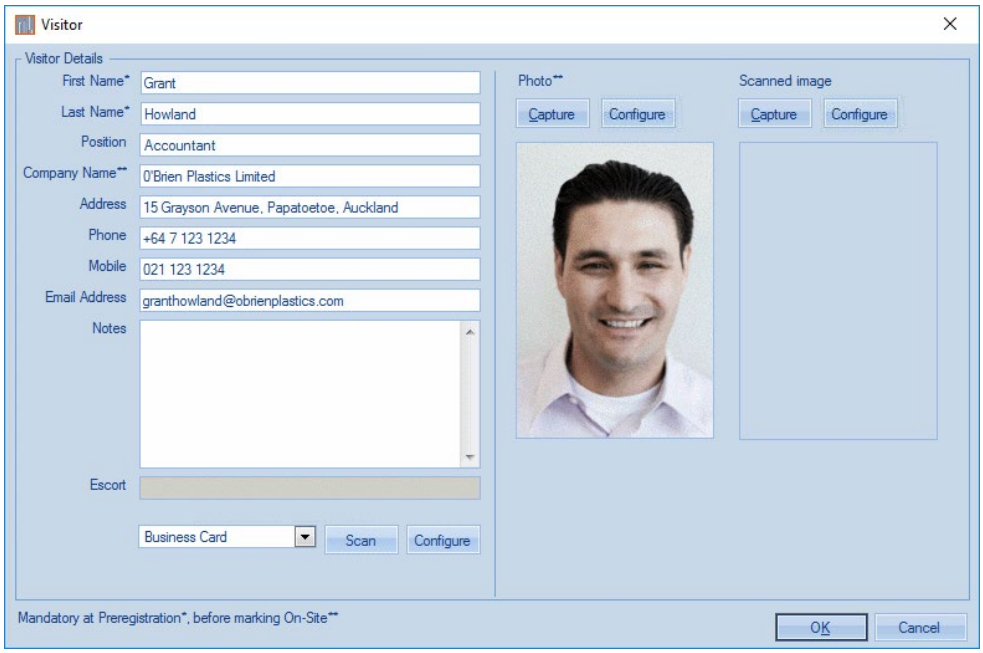
Editing a visitor's details

Perform the following procedure to edit a visitor's details:

1. Click the **Visitor Name** hyper-link located on either the Visit, Find Visit or Home screens.



2. The visitor's details are displayed in the Visitor window.



Note: If you don't have the required user privileges, the visitor's details display as read-only.

3. Edit the visitor's details as required.
4. Click **OK** or **Apply** to save your changes.

Capturing images to store against a visitor

Introduction

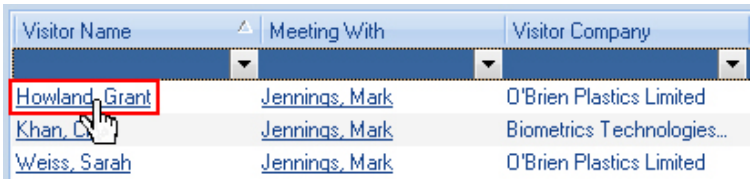
Multiple images can be captured and stored against a visitor, and the type of device to be used for capturing images can be configured. The options available are:

- to capture an image of the Visitor via a supported digital camera or a web cam;
- to capture an image of the Visitor's business card from a supported document scanner;
- to capture an image of the Visitor's supporting documentation (e.g. letter of recommendation, Passport, National ID card, etc.) from a supported document scanner.
  Note: Up to A4 size will be supported.

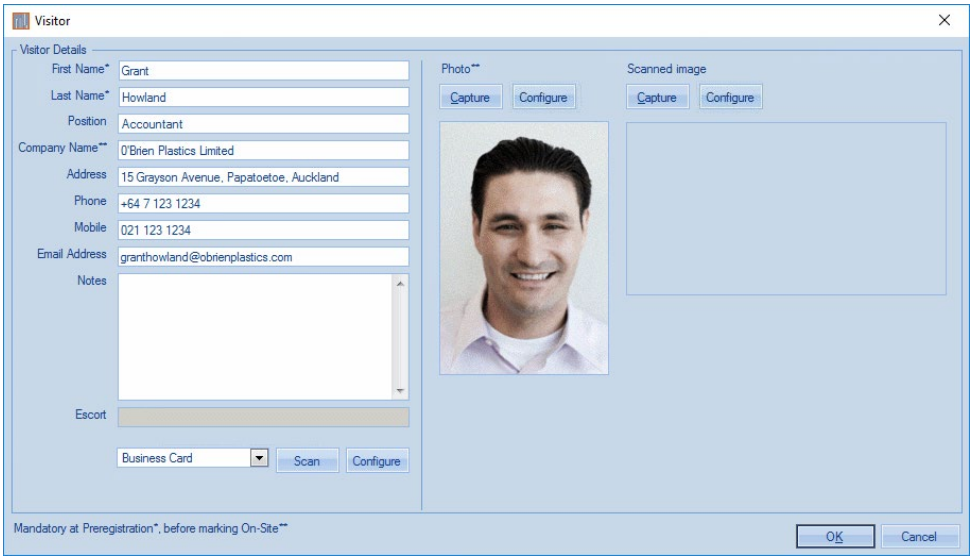
Procedure

Perform the following procedure to configure an image PDF using a specific image capture device:

1. Click the **Visitor Name** hyper-link located on either the Visit, Find Visit or Home screens.



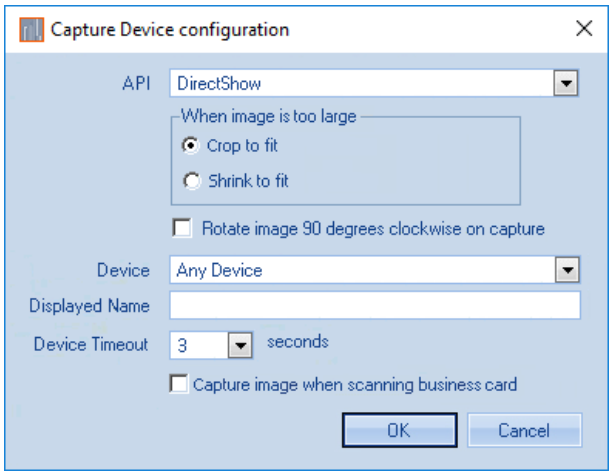
2. The visitor's details are displayed in the Visitor window.



Note: The size of this window will automatically resize depending on the number and size of image PDFs configured up to a maximum, based on the size of the workstation monitor, (or the primary monitor if a workstation

has multiple monitors), on which the user is looking at this window. A scroll bar appears if all the image PDFs cannot be seen on the resized screen.

3. If required for an image PDF, configure the image capture device settings by clicking the **Configure** button.
The Capture Device configuration dialog displays.



Note: The options for "When image is too large" and the "Rotate image 90 degrees clockwise on capture" checkbox only appear when the **DirectShow** API is selected.

4. Configure the settings as appropriate:

Field	Description
API	The options available from the drop-down are: - DirectShow (Legacy) - DirectShow - TWAIN - Cardscan (**Note:** This option will not be available if your site has installed/ upgraded with `NPSA=1` in the licence file.) (Default = DirectShow)
Device	This drop-down populates with relevant devices associated with the API selected. The default "Any Device" option may use an imaging device not currently connected to the workstation.
Displayed Name	This is an optional string that can be displayed as a Tool Tip when the mouse pointer hovers over the **Capture** button on the Visitor window. This can be useful as an indication of which imaging device to use. (Maximum = 200 characters)

Field	Description
Device Timeout	This option is useful for allowing sufficient time to get an image from some slower devices, (e.g. the timeout value may need to be set to 6 seconds for the iBall Document Scanner). (Default = 3 seconds. Range = 1 - 30)
Capture image when scanning business card	If you check this box for any of your configured images, then when a 'Scan Business Card' is done (via the Visitor window), it will update each of those image PDFs with the scanned image of this card.

5. Click the **OK** button.
   The Capture Device configuration dialog closes.
6. Click the **Capture** button.
   The type of imaging device associated with the Image PDF determines what window will display, as follows:

If a...	and the API is...	then a...
digital camera or web cam,	DirectShow (Legacy)	**Camera** Viewer displays.  Click the **Capture** button. The Camera Viewer closes, and the captured image appears on the Visitor screen, cropped to fit the image PDF.

If a...	and the API is...	then a...
	DirectShow	**Camera** Viewer displays.  This screen gives you the opportunity to adjust the image before capturing it, as follows: • Clicking **Rotate Left** turns the image 90 degrees anti-clockwise. • Clicking **Rotate Right** turns the image 90 degrees clockwise. • **Crop to fit** (which changes to **Shrink to fit** when clicked), allows the image to either be cropped or shrunk to fit. Make adjustments (if required), and click the **Capture** button. The Camera Viewer closes, and the captured image appears on the Visitor screen.
	TWAIN or Cardscan scanner,	**Scanner Properties** dialog displays, with a **Scan** button on it. **Note:** The user interface will be device specific. Click the **Scan** button. The Scanner Properties dialog closes, and the captured image appears on the Visitor screen. Images captured by these devices always resize to fit the image PDF.

Notes:

- Images captured will always maintain their aspect ratio.
- If an image is a mandatory field you will get an error if you try to click **OK** without capturing the image, but you may need to scroll along to find the required image, which will be highlighted in yellow.

7. Click the **OK** button to save the visitor.

Scanning business cards for visitors

Introduction

You can scan a visitor's business card and details taken from the card will automatically populate the visitor fields using Optical Character Recognition (OCR). You can also select whether an image of the business card will be captured and stored against the visitor.

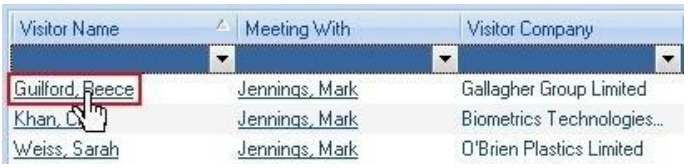
Notes:

- The OCR functionality for business cards supports English language only.
- The ability to capture a business card image is supported using the Plustek OptiCard 821, the Avision AVA6 Plus or the Dymo CardScan scanner. Other devices may also work, but there is no guarantee of how well.

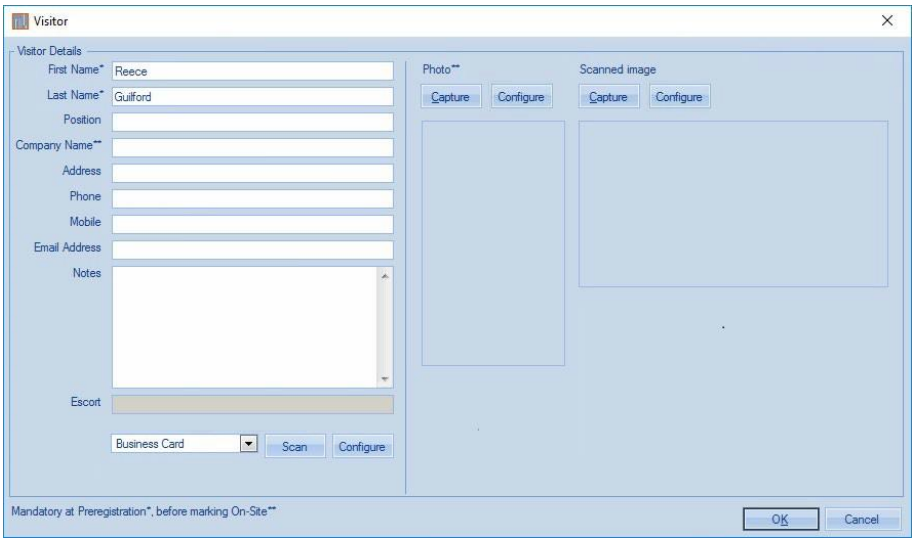
Procedure

Perform the following procedure to scan a visitor's business card:

1. Click the **Visitor Name** hyper-link located on either the Visit, Find Visit or Home screens.



2. The visitor's details are displayed in the Visitor window.



Notes:

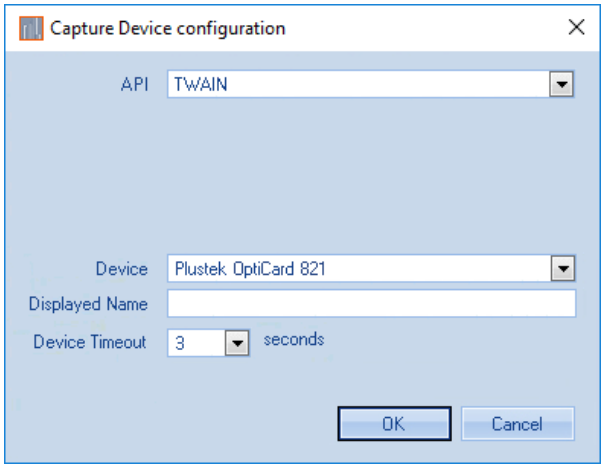
- If you don't have the required user privileges, the visitor's details display as read-only.
- The **Scan** and **Configure** buttons (at the lower left of the window) do not appear if you accessed this window via the **Find Visitor** search (on the Home screen).

3. Select **Business Card** from the document type drop-down list.

4. Are you using ScanShell 800NR?

If…	then…
no,	go to Step 5.
yes,	a. Install using the procedure in ***Visitor Management Kiosk Installation Instructions*** (on page 51-3). b. Go to Step 8.

5. If required, configure the scanner settings by clicking the **Configure** button. The Capture Device configuration dialog displays.



6. Configure the settings as appropriate:

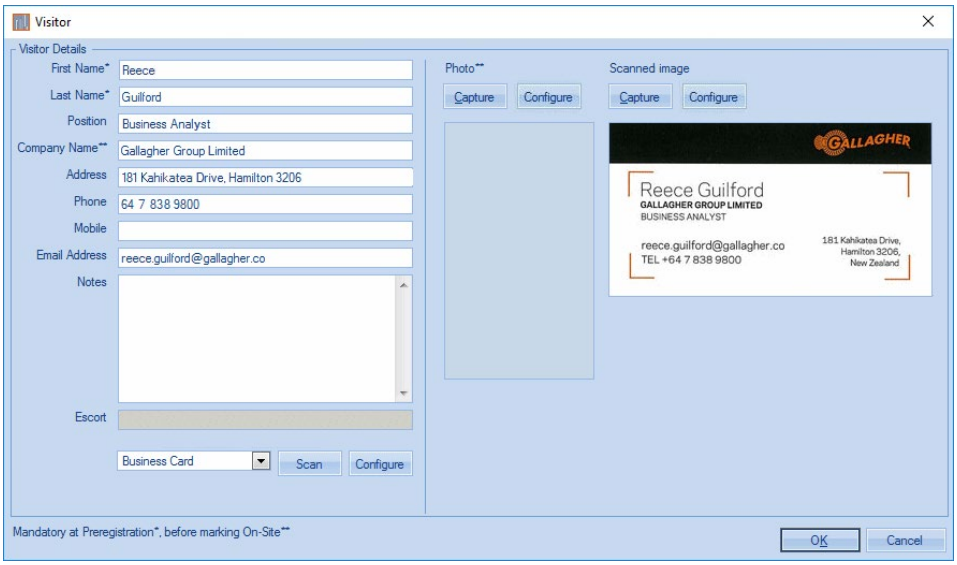
Field	Description
API	The options available from the drop-down are: - DirectShow (Legacy) - DirectShow - TWAIN - Cardscan (**Note:** This option will not be available if your site has installed/ upgraded with `NPSA=1` in the licence file.) (Default = DirectShow)
Device	This drop-down populates with relevant devices associated with the API selected. The default "Any Device" option may use an imaging device not currently connected to the workstation.
Displayed Name	This is an optional string that can be displayed as a Tool Tip when the mouse pointer hovers over the **Capture** button on the Visitor window. This can be useful as an indication of which imaging device to use. (Maximum = 200 characters)

Field	Description
Device Timeout	This option is useful for allowing sufficient time to get an image from some slower devices, (e.g. the timeout value may need to be set to 6 seconds for the iBall Document Scanner). (Default = 3 seconds. Range = 1 - 30)

7. Click the **OK** button.
   The Capture Device configuration dialog closes.
8. Place the business card in the scanner, and click the **Scan** button.
   Note: For TWAIN scanners, business cards need to be placed the right way up (as indicated in the scanner documentation). The Visitor management software will not flip the image if a card is placed sideways or upside down.

For…	then business cards need to be placed…
TWAIN scanners,	the right way up (as indicated in the scanner documentation). The Visitor management software will not flip the image if a card is placed sideways or upside down.
ScanShell 800NR,	in the scanner facing down, with the top of the card in first.

   The visitor fields are populated with details from the business card, and if configured to do so, an image of the business card appears on the Visitor screen.



9. Check that the details mapped to the visitor fields have been captured correctly.
   Correct any mistakes manually.
10. Click the **OK** button to save the visitor.

Scanning passports or driver licenses for visitors

Introduction

You can scan a visitor's passport or driver's license and the details taken will automatically populate the visitor fields using Optical Character Recognition (OCR). You can also select whether an image of the passport or driver's license will be captured and stored against the visitor.

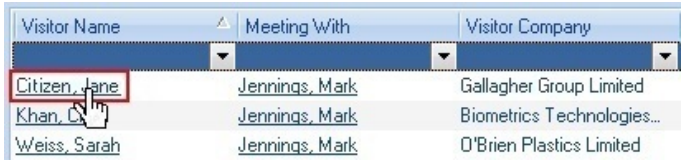
Notes:

- The OCR functionality for passports and driver's licenses supports English language only.
- The ability to capture a passport or driver's license image is supported using the SnapShell Passport Scanner, which supports Microsoft Windows 8 and 10 (32 & 64 bits).
  Note: The SnapShell Passport Scanner is End of Life, and no longer available for purchase.

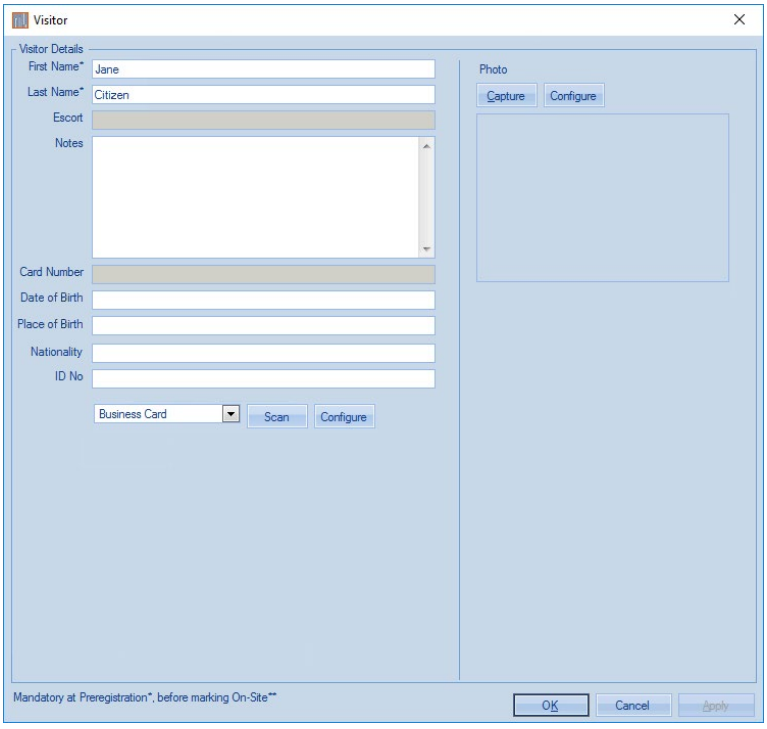
Procedure

Perform the following procedure to scan a visitor's passport or driver's license:

1. Click the **Visitor Name** hyper-link located on either the Visit, Find Visit or Home screens.



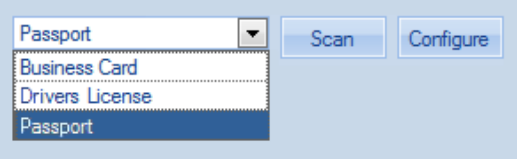
The Visitor screen displays.



Notes:

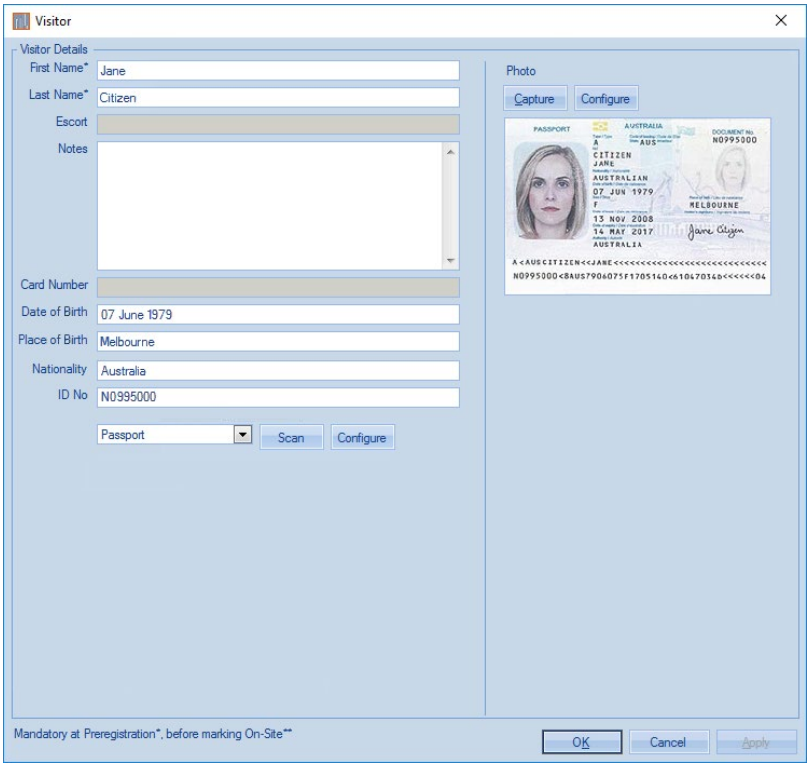
- If you don't have the required user privileges, the visitor's details display as read-only.
- The **Scan** and **Configure** buttons (at the lower left of the window) do not appear if you accessed this window via the **Find Visitor** search (on the Home screen).

2. Select the appropriate document type, (e.g. Driver's License, Passport), from the drop-down list.
   Note: The document types that appear in the drop-down are determined by what Data Maps have been created in Command Centre Client.



3. Place the passport or driver's license in the scanner, and click the **Scan** button.
   Note: To ensure passports scan properly, we recommend you hold the lid of the scanner down so they lie flat.

   The visitor fields are populated with details from the passport or driver's license, and if configured to do so, an image of the document appears on the Visitor screen.



4. Check that the details mapped to the visitor fields have been captured correctly.
   Correct any mistakes manually.
   Notes:
   - If no information or only partial fields are captured, you may want to try re-scanning before manually populating fields.
   - The system does not verify that the document scanned is either a valid or current form of ID.
5. Click the **OK** button to save the visitor.

Viewing a host's details

Introduction

The host is responsible for the visitor for the duration of their visit. A host can be either:

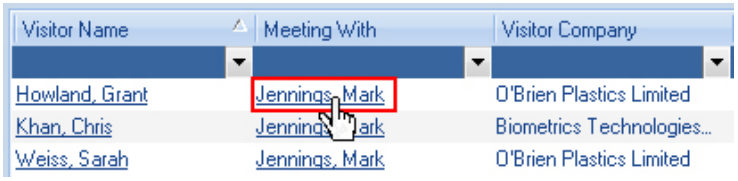
- **Meeting With**. The person a visitor plans to meet with, or
- **Escort**. The person physically escorting the visitor to the meeting venue.

Note: Hosts are created in Command Centre and should be permanent cardholders. It is the responsibility of your Command Centre administrator to configure hosts who can meet with or escort visitors of a particular visitor type.

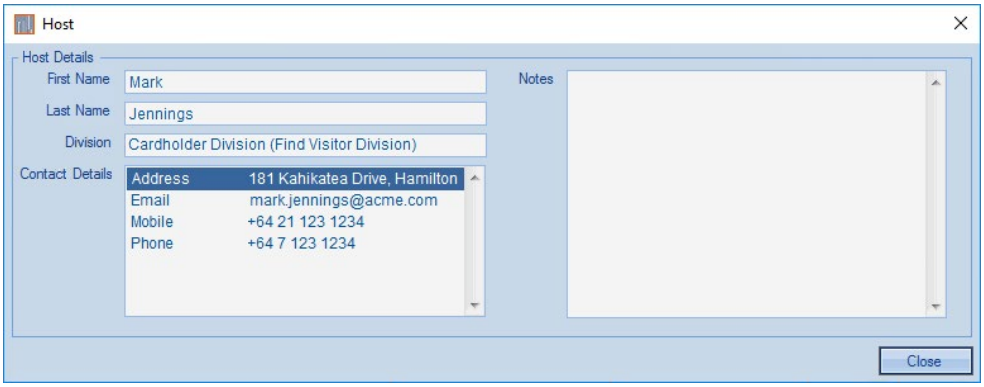
Procedure

Perform the following procedure to view a host's details:

1. Click the **Meeting with** hyper-link located on the Find Visit or Home screens.



2. The host's details are displayed as read-only in the Host window.



Note: If you don't have the required user privileges, only the host's name displays.

Receptionist functions

This section describes the functions you can perform if you are a Receptionist user.

Select the topic below that you require further detail on:

- ***The Home screen*** (on page 50-114)
- ***Performing visitor actions*** (on page 50-125)
- ***Grace period and overdue alarm*** (on page 50-142)

The Home screen

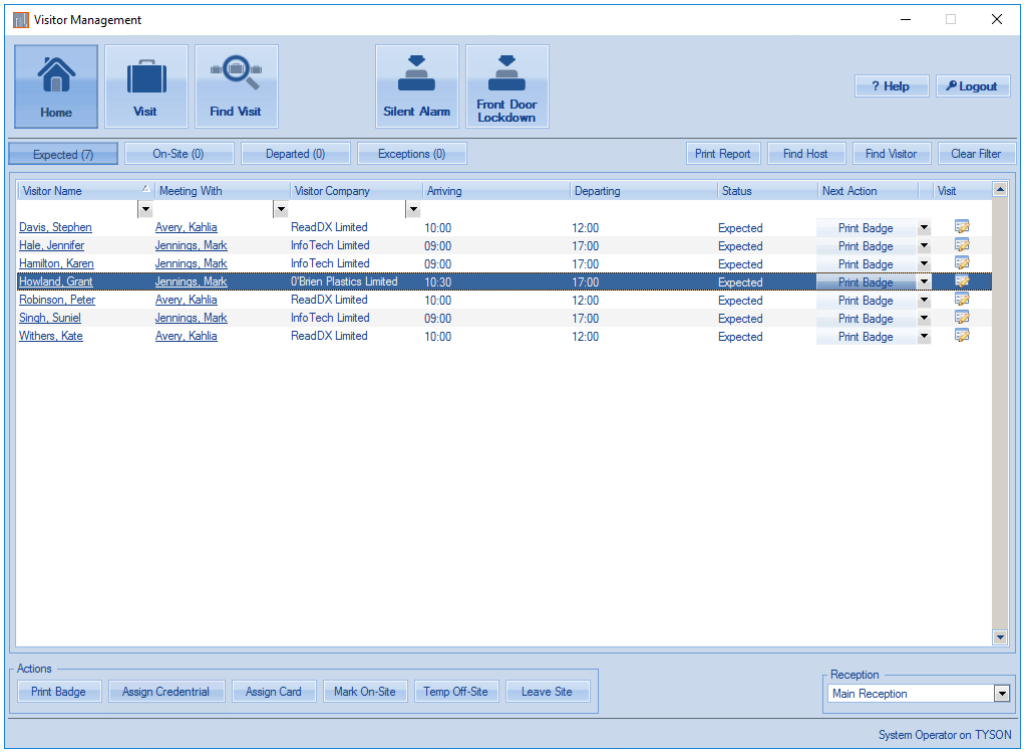
Description

The Home screen enables you to perform an action for a visitor and change a visitor's status.

Note: If you are a Receptionist user, this screen displays automatically at logon. The Home screen is available for Receptionist users only.

To open the Home screen, click the **Home** button located on the toolbar. Expected visitors for the selected reception are displayed on the 'Expected' status tab.

The Home screen



The Home screen displays your default reception, the columns and action buttons for this reception, as configured in Command Centre and the visitors on a visit for this reception.

Columns on the Home screen

This table explains the columns on the Home screen:

Column	Function
Visitor Name	Click the hyper-link to view the visitor's details.
Meeting With	Click the hyper-link to view the meeting with person's details.
Escort	Displays the Escort assigned to this visitor.
Arriving	Displays the arrival date and time for the visit for this visitor.
Departing	Displays the departure date and time for the visit for this visitor.
Status	Displays the current status for this visitor.
Next Action	Click to perform the next action recommended for this visitor, or click the drop-down arrow and select an action to perform for this visitor.
Visit	Click the visit icon to view the visit for this visitor.

Notes:

- Two additional columns, (i.e. **Card Number** and **Visit Notes**) will also appear if configured to do so in Command Centre. The **Card Number** column (which can be sorted on) shows cards assigned to the visitor. When the **Visit Notes** icon is clicked, a dialog displays showing the notes relating to the visitor's visit. The content of this dialog is read-only, and cannot be changed.
- An additional **Send Message** button will be available in the Action buttons if the site is licensed for Notifications. This button allows a Receptionist to send a manual notification (via email and/or SMS message) to a Host and/or Escort for a visitor or Tour Group.

Visitors displayed on the Home screen

Introduction

A time slot can be configured by your Command Centre administrator that determines which visitors are displayed on the 'Expected' and 'Departed' Home screen status tabs.

Time slot options

The time slot is configured using one of the following options:

- show all today’s visits

  OR:

- show all visits occurring ‘x’ hours before the current time and ‘y’ hours after the current time, (e.g. minus 'x' hours plus 'y' hours)

Time zones

Where the time slot is 'show all today’s visits' the reception will show all today's visits, for the reception's time zone.

Where the time zone is 'show all visits occurring **x** hours before the current time and **y** hours after the current time' the reception will show all visits relative to the workstation's time zone.

Time zone example

Two reception locations:

- New Zealand (UTC +13)
- South Africa (UTC +2)

  New Zealand is 11 hours ahead of South Africa.

If the time slot is 'show all today's visits'

Workstation time zone	Receptions
New Zealand Date: 02-02-09 Time: 9:00a.m.	**New Zealand Reception** You will see all visits for the 02-02-09 **South Africa Reception** You will see all visits for the 01-02-09

If the time slot is 'show all visits occurring 2 hours before the current time and 4 hours after the current time':

Workstation time zone	Receptions
New Zealand Date: 02-02-09 Time: 9:00a.m.	**New Zealand Reception** You will see all visits due between 7:00a.m. and 1:00p.m. on the 02-02-09 (New Zealand Time) **South Africa Reception** You will see all visits due between 7:00p.m. on the 01-02-09 and 2:00a.m. on the 02-02-09 (South African Time)

Status tabs

Description

There are four tabs shown on the Home screen: 'Expected', 'On-Site', 'Departed' and 'Exceptions'. These tabs display visitors according to their status.

Tabs



The visitor count per status, is shown in brackets on each tab.

Function

This table explains the function of each tab.

Tab	Function
Expected	Click to display all visitors who are expected to arrive.
On-Site	Click to display all visitors who have been marked on-site at some time.
Departed	Click to display all visitors who have left the site.
Exceptions	Click to display all visitors who are overdue.

Action buttons

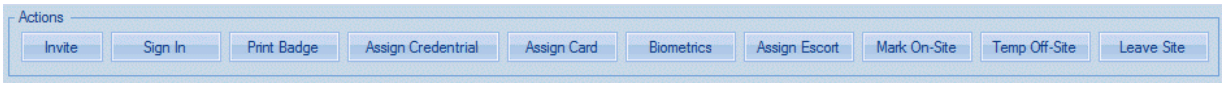
Description

The action buttons are located at the bottom of the Visit or Home screens. These buttons enable you to perform an action for the selected visitor.

Notes:

- The selected reception controls what actions are displayed. This means that if you manage more than one reception the actions available may vary.
- Sign In, Mark On-Site and Leave Site actions are compulsory, all other actions are configured in Command Centre by your Command Centre administrator. If configured, some actions may be required before a visitor can be marked on-site, (e.g. A badge may need to be printed before a visitor can be marked on-site).

Actions



Function

This table explains the function of each action.

Action	Function
Invite	Click to email a QR Code barcode (in an attached **.png** file) to a visitor.
Sign In	Click to sign a visitor in.
Print Badge	Click to print a badge for a visitor.
Assign Credential	Click to assign an access credential for a visitor.
Assign Card	Click to assign an access card for a visitor.
Biometrics	Click to capture the biometrics, (i.e. fingerprints or finger veins) of a visitor on a visit. **Note:** If biometric functionality has not been set up and this button is clicked, an error will display and Visitor Management closes.
Assign Escort	Click to assign an escort for a visitor.
Mark On-Site	Click to mark a visitor on-site.
Temp Off-Site	Click to mark a visitor temporarily off-site.
Leave Site	Click to mark a visitor off-site.

Note: An additional **Send Message** button will be available in the Action buttons if the site is licensed for Notifications. This button allows a Receptionist to send a manual notification (via email and/or SMS message) to a Host and/or Escort for a visitor or Tour Group.

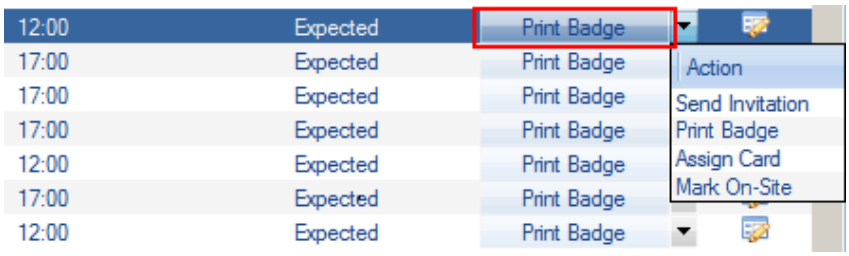
Next Action buttons

Description

The Next Action buttons are located in the Next Action column of the Home screen. These buttons show the next allowable action you can perform for the visitor, on this row.

To perform a different action for the visitor, click the Next Action drop down arrow. A list of allowable actions displays. Select an action. The action selected is performed for the visitor on this row.

Actions



Visitor status

This table provides an explanation for each visitor status.

Visitor status	Explanation
Expected	Is the status of a visitor when their visit has been scheduled but they have not been marked on-site. Visitor record colour: **Blue**
Signing In	Is the status when a visitor is at a Kiosk and is in the process of signing in. Visitor record colour: **Blue**
Signed In	Is the status when the Receptionist has chosen the 'Sign In' action and also where a visitor using a Kiosk has completed the sign in process and are waiting for a host to sign them in. Visitor record colour: **Blue**
On-Site	Is the status of a visitor when they have been marked on-site. Visitor record colour: **Green**
Expected Back	Is the status of a visitor when they go off-site during a visit, intending to return. Visitor record colour: **Blue**
Due to Leave	Is the status of a visitor when they are still on-site after the departure time of the visit but the overdue grace period has not expired. Visitor record colour: **Orange**
Overdue	Is the status of a visitor when they are still on-site after the departure time of the visit plus the grace period has expired. Visitor record colour: **Red**
Departed	Is the status of a visitor when they have been marked off-site. Once marked off-site the visitor's status cannot be changed. Visitor record colour: **Black**
Cancelled	Is the status of a visitor when their visit has been cancelled. Visitor record colour: **Black**

Printing a Visitor Status report

Description

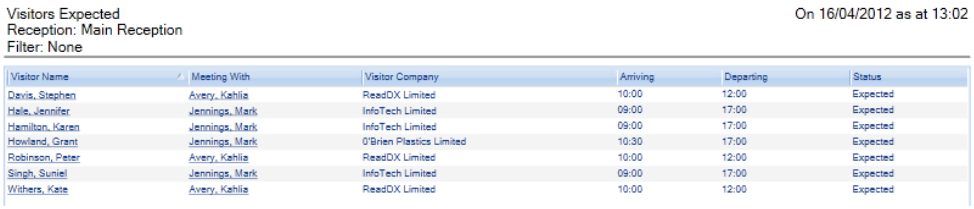
The Visitor Status report records the information shown on the Home screen. You can print a separate report for each of the status tabs: 'Expected', 'On-Site', 'Departed' or 'Exceptions'. The Visitor Status report takes into account the filtering used on the Home screen.

You may want to print a Visitor Status report that records all visitors who are expected for the current day, or all visitors who are currently on-site.

To print a Visitor Status report, click the **Print Report** button located on the Home screen.

The Visitor Status report

This report shows all visitors who are 'Expected' at the time the report was generated: 16/04/2012 at 13:02



Visitors Expected
Reception: Main Reception
Filter: None

On 16/04/2012 as at 13:02

Visitor Name	Meeting With	Visitor Company	Arriving	Departing	Status
Davis, Stephen	Avery, Kahlia	ReadDX Limited	10:00	12:00	Expected
Hale, Jennifer	Jennings, Mark	InfoTech Limited	09:00	17:00	Expected
Hamilton, Karen	Jennings, Mark	InfoTech Limited	09:00	17:00	Expected
Howland, Grant	Jennings, Mark	O'Brien Plastics Limited	10:30	17:00	Expected
Robinson, Peter	Avery, Kahlia	ReadDX Limited	10:00	12:00	Expected
Singh, Suniel	Jennings, Mark	InfoTech Limited	09:00	17:00	Expected
Withers, Kate	Avery, Kahlia	ReadDX Limited	10:00	12:00	Expected

Notes:

- The user who requested the report and the date and time the report was generated is displayed at the bottom.
- The information shown in the report is the same as the information shown on screen. If you require additional information to be shown in your report, refer to your Command Centre administrator, with regards to configuring different columns on the Home screen.

Finding a visitor

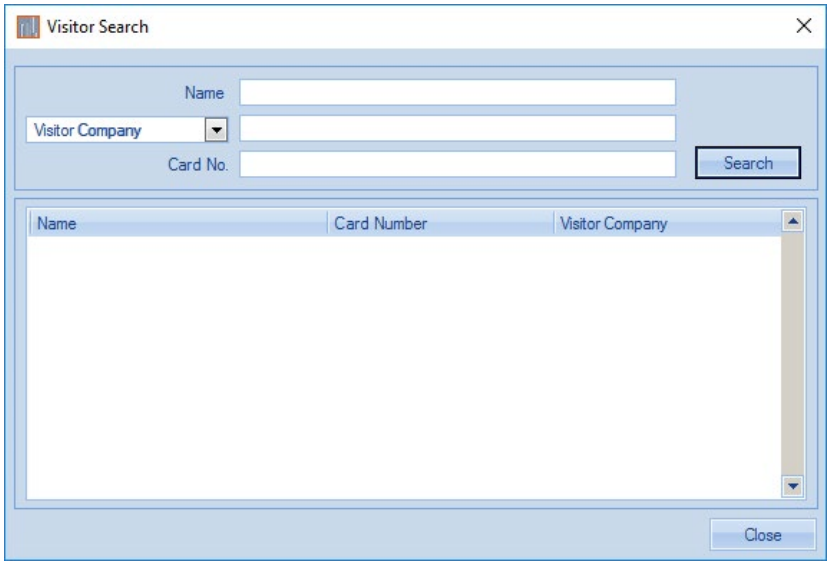
Introduction

This topic describes how to find a visitor. You may want to find a visitor in order to view the visitor's details or edit the visitor's details, (e.g. add additional information to the visitor's details, when the visitor arrives).

Procedure

Perform the following procedure to find a visitor:

1. Click the **Find Visitor** button located on the Home screen.
   The Visitor Search window displays.



   Note: The reception selected on the Home screen determines the configuration of the columns shown in the Visitor Search window and the personal detail fields that can be searched.

2. Search using one of the following methods:
   - Enter the visitor name into the **Name** field.
     Note: Name matching is not case sensitive.
   - Select a personal detail from the drop down list and enter a value in the field opposite.
   - Enter a card number in the **Card No.** field.
     Note: Searching by card number is only possible if it has been configured in Command Centre, in which case the **Card No.** field and **Card Number** column will appear.
3. Click **Search**. Visitor search results are displayed in ascending visitor name order. To sort rows by ascending or descending order, click the column header.
4. To view the visitor's details, click the **Name** hyper-link or double click the **visitor record**.

Finding a host

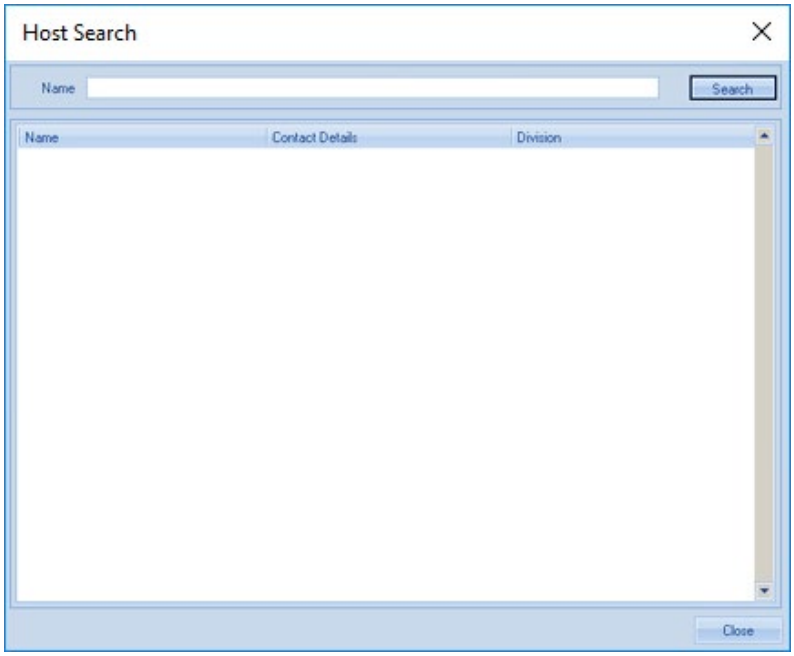
Introduction

This topic describes how to find a host. You may want to find a host in order to view the host's details, (e.g. authenticate the host).

Procedure

Perform the following procedure to find a host:

1. Click the **Find Host** button located on the Home screen.
   The Host Search window displays.



2. Enter the host name into the Name field.

   Note: Name matching is not case sensitive.

3. Click **Search**.

   Search results are displayed for each host, who matches the search criteria entered and who belong to one of the host type groups (access groups) specified in the Visitor Management configuration.

   Host search results are displayed in ascending host name order. To sort rows by ascending or descending order, click the column header.

4. To view the host's details, click the **Name** hyper-link or double click the **host record**.

Performing visitor actions

Introduction

This topic describes the actions you can perform, in order to process visitors on your site.

Actions

Actions that can be performed are:

- ***Sending Invitations*** (on page 50-126)
- ***Signing in*** (on page 50-127)
- ***Printing a badge*** (on page 50-128)
- ***Assigning a credential*** (on page 50-130)
- ***Assigning a card*** (on page 50-131)
- ***Capturing Biometrics*** (on page 50-132)
- ***Assigning an escort*** (on page 50-136)
- ***Marking a visitor 'On-Site'*** (on page 50-137)
- ***Marking a visitor 'Temp Off-Site'*** (on page 50-138)
- ***Marking a visitor 'Off-Site' (Leave Site)*** (on page 50-139)
- ***Sending a Message*** (on page 50-140)

Sending Invitations

Introduction

Sending an invitation is an action that a Host would perform during the creation of a new Visit, or selecting an existing visit.

Prerequisites

Sending invitations to visitors requires the following:

- the Visitor to be the correct Visitor Type and have a configured Email Personal Data Field with a valid Email in it. If not, an email will still be created but the **To** field will be blank.
- the Email Personal Data Field has the **Default Notifications** checkbox ticked (on the **Type** tab).
- a card type has been created with barcodes.

Procedure

1. Select the visitor record on either the Find Visit, Visit or Home screens.
2. Click the **Invite** action button.
   Note: The reception configuration determines if the Invite action is displayed, or not.

   The Visitor receives the email with an attached **.png** file containing the QR Code barcode, and the Host is cc'd on the email if email is configured.
   When the visitor arrives for their visit:

   a) They scan the Barcode directly from their cell phone or printed on a piece of paper.
      This either marks them as ‘signed In’ or ‘on site’, depending on configuration.

   b) A Badge is printed that contains the Barcode (this is a manual action).

   c) When they leave, they swipe the Barcode on their Badge and they are marked ‘off site’.

Signing In

Introduction

The **Sign In** button allows a visitors status to change to 'Signed In'. This status is used at the Visitor Management Kiosk. If a receptionist 'Signs In' a visitor the host can badge their card at a Kiosk reader and mark the visitor on-site.

Procedure

1. Select a visitor record.
   Note: The visitor's status must be either 'Expected' or 'Expected Back'.
2. Click the **Sign In** action button.
   The visitor's status prior to signing them in determines the result, as follows:

If a Visitor has an...	then...
'Expected' status,	their visit status will remain as 'Visit Scheduled', and they will remain on the **Expected** tab.
'Expected Back' status,	their visit status will remain as 'Visit in Progress', and they will move from the **On-Site** tab to the **Expected** tab.

Note: If configured in Command Centre, a notification will automatically be sent, (i.e. an e-mail and/or sms message) to the Host and the Escort, if there is one.

Printing a badge

Introduction

A badge is a printed label given to a visitor which displays information about the visitor and/or visit.

A badge can be used to identify who a visitor is and where a visitor is allowed to be on-site (access area/badge text).

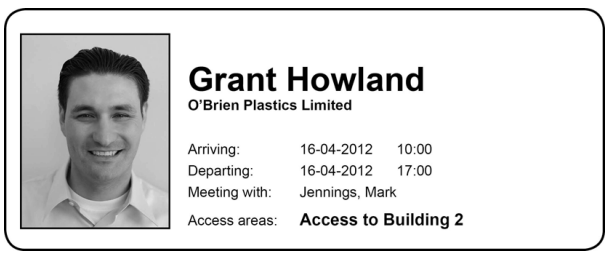
A badge label can be printed in advance or when a visitor arrives. It is recommended that the badge be printed as a self adhesive sticker and attached to a visitor's garment, lapel or tag.

What information can the badge display?

A badge can display the following information:

- **Visitor Details** (e.g. visitor name, company name, photograph)
- **Visit Details** (e.g. the person they are meeting with, visit arriving date and time, visit departing date and time)
- **Visitor Type** (e.g. contractor, supplier)
  The visitor type controls what information is displayed on the badge and the appearance of the badge, (e.g. a contractor's badge may have a different layout compared to a supplier's badge).
- **Badge Text** (e.g. area of access)
  Badge Text is a piece of text added to the badge. A list of Badge Text options is configured in Command Centre. Select a Badge Text option when you create a visit.
- **Group Name**
  Group Name is the name of the Tour Group, (e.g. the organisation the group is from).
- **Barcode**
- **QR Code**

Examples





Recommended printer

The recommended printer is the Dymo LabelWriter 400.

When printing a badge for the first time, the system will prompt you to select a printer. The printer selected will then become the default printer for all subsequent print requests. To change the default printer, select a visitor record and click **Alt+P**. The Print window displays. Select an alternative printer.

Note: A different default printer can be set for each reception.

Procedure

To print a badge, complete the following procedure:

1. Select a visitor record.

   Note: Multiple records can be selected.

2. Click the **Print Badge** action button.

   Note: The reception configuration determines if the Print Badge action is displayed, or not.

3. The badge label is printed. A message on the status bar shows how many badges were successfully printed out of the number of records which were selected.

   Note: The visitor row will be updated to show the next available action.

Assigning a credential

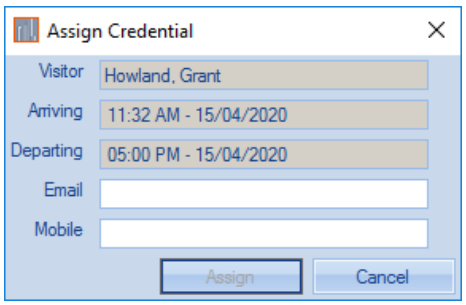
Introduction

You can assign an access credential to a visitor on a visit. A credential is used to open secure doors on-site. What areas the visitor has access to are defined by the 'Access Groups' selected on the visit.

Procedure

To assign a credential to a visitor, complete the following procedure:

1. Select the visitor record. The visitor's status must be either 'Expected', 'On-Site' or 'Expected Back'.
   Note: If more than one visitor is selected, the **Assign Credential** action is disabled.
2. Click the **Assign Credential** action button.
   The Assign Credential window displays.



   This window displays the Visitor's name, Arriving information, Departing information and Email address if previously assigned.
   Notes:
   - The **Mobile** field only appears if SMS verification has been enabled for Mobile Credential assignments made from this workstation.
   - The reception configuration determines if the Assign Credential action is displayed, or not.
3. Enter the visitor's email address in the **Email** field if not already populated.
   Note: If the format of the email address is not entered correctly, the tool tip icon displays. Hover the mouse over the tool tip icon to view the tip.
4. If the **Mobile** field appears and is not already populated, enter the visitor's mobile phone number.
5. Click **Assign** to save the credential assigned to the visitor for this visit.

Assigning a card

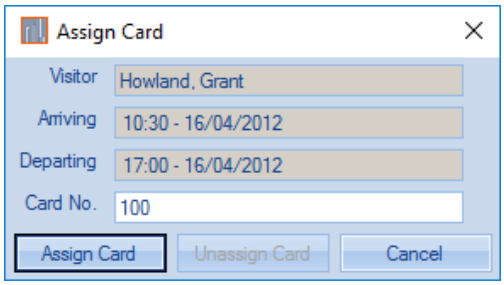
Introduction

You can assign an access card to a visitor on a visit. A card is used to open secure doors on-site. What areas the visitor has access to are defined by the 'Access Groups' selected on the visit.

Procedure

To assign a card to a visitor, complete the following procedure:

1. Select the visitor record. The visitor's status must be either 'Expected', 'On-Site' or 'Expected Back'.
   Note: If more than one visitor is selected, the **Assign Card** action is disabled.
2. Click the **Assign Card** action button.
   The Assign Card window displays.



   This window displays the Visitor's name, Arriving information, Departing information and Card Number, if previously assigned.
   Notes:
   - The reception configuration determines if the Assign Card action is displayed, or not.
   - If a card is badged at the reception reader prior to the Assign Card action being selected, the card number will display in the Card Number field, unless a card has previously been assigned to the visitor for this visit.
   - If a card has previously been assigned to the visitor for this visit, this card will display beneath the Card Number field.

   To remove a previously assigned card from the visitor for this visit, click the **Unassign Card** button.
3. Either:
   - badge a card at the reception reader. The card number displays in the Card Number field, or
   - enter a card number into the Card Number Field. This option can be used if a reader is unavailable

   If an invalid card number is entered, the tool tip icon displays. Hover the mouse over the tool tip icon to view the tip.
4. Click **Assign Card** to save the card assigned to the visitor for this visit.

Capturing Biometrics

Introduction

You can capture the biometric credentials (fingerprints / finger veins) of a visitor on a visit. The biometrics are used to open secure doors on-site. What areas the visitor has access to are defined by the 'Access Groups' selected on the visit.

Before you begin

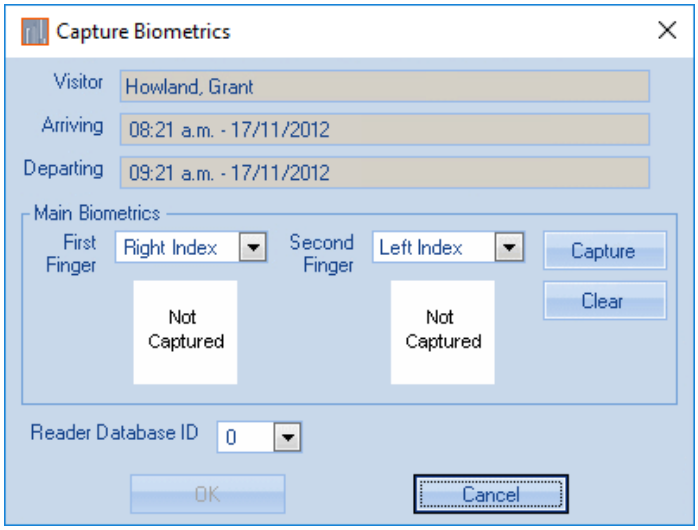
Before you begin this procedure:

- A Morpho Biometric Type must already be created. Refer to ***Creating a New Morpho Biometric Type*** (on page 64-3) for the procedure.
- A suitable enrolment device (for capturing fingerprints or finger veins) must be connected to Visitor Management via a USB connection.

Procedure

To enrol a visitor for a Morpho Fingerprint or Finger Vein, complete the following procedure:

1. Select the visitor's record.
2. Click the **Biometrics** action button.
   The Capture Biometrics window displays.



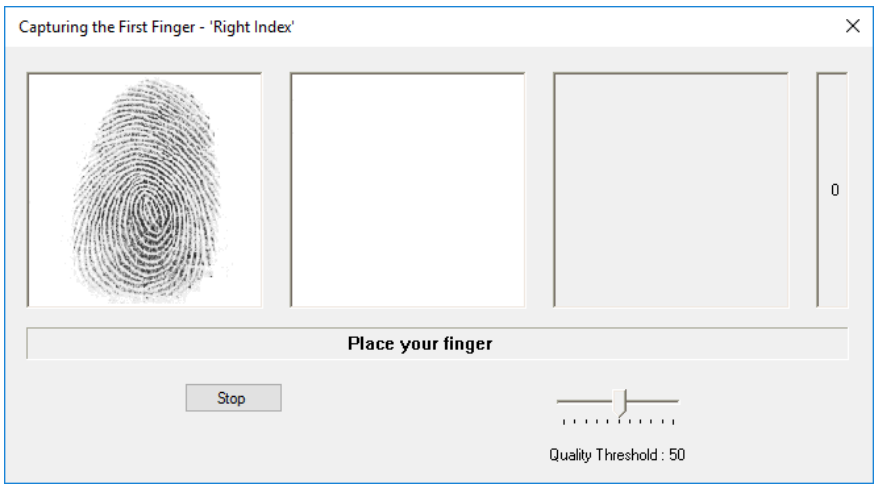
This window displays the Visitor's name, Arriving and Departing information, and Biometrics, if previously assigned.

Notes:

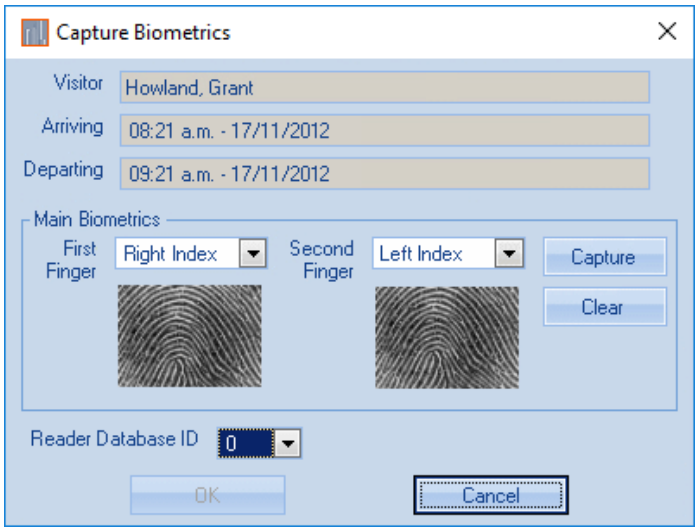
- The reception configuration determines if the Biometrics action is displayed or not.
- To remove a previously assigned fingerprint/vein from the visitor for this visit, click the **Clear** button.

- The Privacy Settings selected (via the **Advanced** tab of the Morpho Biometric Type) affect what appears on the bottom of this window.

3. Click the **Capture** button.
   The Morpho Finger Capture screen displays.



4. Place the appropriate finger on the enrolment device.
   The percentage bar on the right of the screen indicates how successful the capture is.
5. Repeat Step 4 twice so you have three captures of the same finger.
6. Repeat Steps 3 - 5 for the second finger.
   On capturing two fingers successfully:
   - an image displays under the appropriate Finger on the Capture Biometrics screen to indicate that something has been captured,
   - the **Clear** button (used for deleting the captured biometrics) is enabled, and
   - the **OK** button is enabled.



7. What model of Morpho Biometric readers do you have?

If...	then...
MA1xx, **MA Sigma**, **MA J**, **MA VP** or **MA5xx** without an IDENTPLUS licence	these readers only have one database, therefore the **Reader Database ID** field can be ignored. Go to Step 9.
MA5xx with an IDENTPLUS licence	these multi-database readers have 5 databases that each hold 10,000 sets of fingerprints/veins. Go to Step 9.

8. Do you expect to capture biometrics for more than 3000 visitors?

If...	then...
no	enter 0 in the **Reader Database ID** field.
yes	select an appropriate value in the **Reader Database ID** field between 0 - 15 to indicate which of the 16 databases is to be used. The number of fingerprints/veins in each database can be determined from the reader status screen. A value greater than zero will mean that visitors will be required to enter this Database ID using the reader's keypad before placing their finger for identification. For databases 10 - 15, a '#' needs to be entered in place of the '1', (e.g. for database 14, a visitor would enter '#4').

9. Do you expect to capture biometrics for more than 10,000 visitors?

If...	then...
no	enter 0 in the **Reader Database ID** field.
yes	select an appropriate value in the **Reader Database ID** field between 0 - 4 to indicate which of the 5 databases is to be used. The number of fingerprints/veins in each database can be determined from the reader status screen. A value larger than 4 will be accepted but the fingerprints/veins will be stored in database 0. A value greater than zero and less than 5 will mean that visitors will be required to enter this Database ID using the reader's keypad before placing their finger for identification.

Notes:

- The general rule is that database 0 is used to store fingerprints/veins if the Reader Database ID is the same or larger than the number of databases supported by a particular reader. For instance, if a visitor

has a Reader Database ID of 10, and has access to both a MA3xx and MA5xx (with IDENTPLUS licence), then database 10 will be used on the MA3xx and database 0 will be used on the MA5xx.

- The larger an Access Group, the longer it takes to sort and send to the reader.

10. Click the **OK** button to exit and save your changes.
    Notes:
    - You will not be able to save the visitor's biometrics if only one 'Main' biometric has been captured.
    - It is possible to report on biometric details in a Cardholder Report. On the first page of the Cardholder Report wizard, (i.e. the 'Report Style' page), there is an **Include Biometric Details** checkbox that can be turned off/on as required.

Assigning an escort

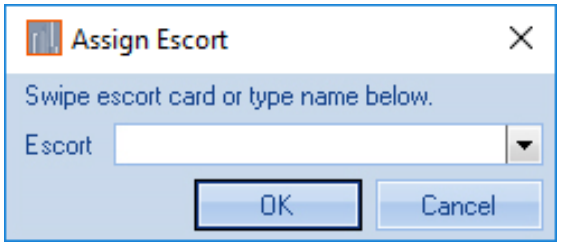
Introduction

An escort is a person who accompanies a visitor(s) on a visit. An escort is a cardholder who belongs to the host type access group, for the selected visitor type.

Procedure

To assign an escort to a visitor, complete the following procedure:

1. Select the visitor's record.
2. Click the **Assign Escort** action button.
   The Assign Escort window displays.



   Notes:
   - The reception configuration determines if the Assign Escort action is displayed, or not.
   - If a valid escort card was badged at the reception reader prior to this action being selected the name of the escort displays.
   - If a valid escort biometric sample, (e.g. a person's fingerprint or finger vein) was presented at the reception reader prior to this action being selected the name of the escort displays.
3. Either:
   - badge a valid escort card at the reception reader. The escort displays, or
   - present a valid escort biometric sample at the reception reader. The escort displays, or
   - enter the first 3 characters of the escorts's name and select the escort from the Escort drop down list. This option can be used if a reader is unavailable.
4. Click **OK** to save the escort assigned to this visitor. If an escort was previously assigned to this visitor a confirmation window displays. Click **OK** to confirm the new escort assigned.
   Note: In Command Centre, the escort that has been assigned displays as 'read-only' on the **Status and Overrides** tab of the visitor's cardholder properties.

Marking a visitor 'On-Site'

Introduction

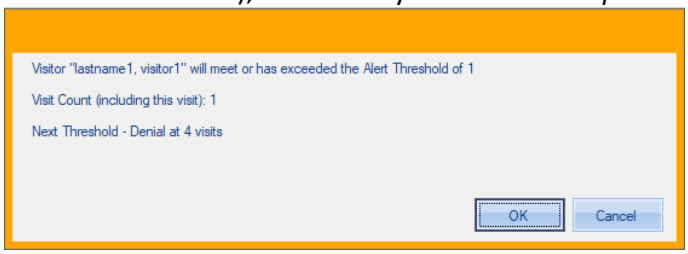
When a visitor checks-in at the reception the visitor will need to be marked on-site. Before a visitor can be marked on-site, the reception may require one or all of the following actions to be carried out:

- Print badge
- Assign access card
- Assign escort
- Capture biometrics

Note: The availability of these actions may vary depending on the configuration of your system in Command Centre.

When a visitor is successfully marked on-site the system will:

- check that all mandatory visitor details have been entered, for this visitor
- check that all mandatory actions have been performed, for this visitor
- set the visitor's status to on-site
- move the visitor's record to the 'On-Site' status tab
- set the visitor's visit status to 'Visit In Progress'
- assign site access to the visit, if access groups have been selected for the visit
- if the site is licensed for the 'Visit count' feature, the visit count for this visitor will be incremented when they are marked on-site for the first time per visit. **Notes:**
  - The 'Visit counting' thresholds are configured on the **Advanced** tab of the Command Centre Server Properties.
  - Events are generated in Command Centre, and prompts appear in Visitor Management when thresholds, (i.e. Warning, Alert and Denial Thresholds), are already met. *For example:*



Procedure

To mark a visitor on-site, complete the following procedure:

Note: Only a visitor whose status is 'Expected', 'Expected Back' or 'Signed In' can be marked on-site.

1. Select the visitor record on either the Visit or Home screens.
2. Click the **Mark On-Site** action button. **Notes:**
   - When the first visitor on a visit is marked on-site, the arrival time for the visit is changed to the marked on-site time.
   - You can mark multiple visitors on-site at the same time.
   - You cannot mark a visitor on-site after the departing date and time of their visit.
   - In the event that a mandatory action has not been completed, the visitor will not be marked on-site and an appropriate error message displays.

Marking a visitor 'Temp Off-Site'

Introduction

When a visitor checks-out temporarily at the reception the visitor will need to be marked temporarily off-site. The visitor can be marked back on-site at a later stage.

When a visitor is successfully marked temporarily off-site the system will:

- set the visitor's status to 'Expected Back'
- remove the access card and access assigned to this visitor
- remove the escort assigned to this visitor

Note: The reception configuration determines if the **Temp Off-Site** button or **Temp Off-Site** Next Action button is displayed, or not.

Procedure

To mark a visitor temporarily off-site, complete the following procedure:

Note: Only a visitor whose status is on-site can be marked temporarily off-site.

1. Select the visitor record on either the Visit or Home screens.
2. Click the **Temp Off-Site** action button.

   Note: The visitor should return their access card, if issued to the reception.

Marking a visitor 'Off-Site' (Leave Site)

Introduction

When a visitor leaves, having completed their visit, they need to be marked off-site. There are two ways that this can be achieved, as follows:

1. The Receptionist can manually record them as having left the site, or
2. If visitor access cards are used, the Visitor or the Receptionist can badge the card at a designated exit reader, which triggers the system to automatically complete the leave site process.

When a visitor is successfully marked off-site the system will:

- set the visitor's status to ‘Departed’
- move the visitor's record to the 'Departed' status tab
- remove the access card and access assigned to this visitor
- remove the escort assigned to this visitor
- set the visit status to 'Completed' if the visitor is the last person remaining on the visit

Note: The visitor’s status cannot be changed once marked off-site.

Procedure

This procedure describes how a Receptionist manually marks a visitor off-site in Visitor Management:

1. Select the visitor record, on either the Visit or Home screens.
2. Click the **Leave Site** action button.

   Note: The visitor should return their access card, if issued to the reception.

Sending a Message

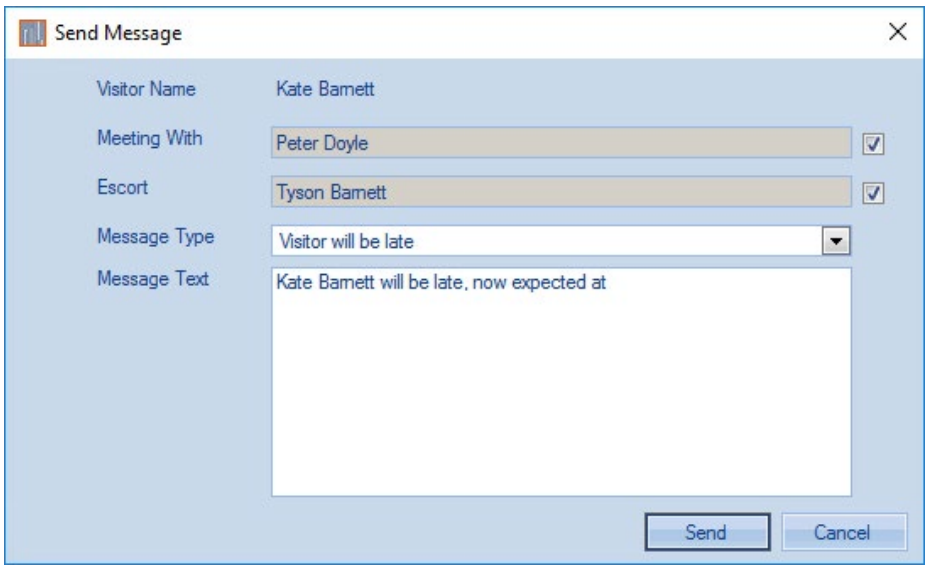
Introduction

The **Send Message** button is only visible if the site is licensed for Notifications. It allows a Receptionist to send a manual notification (via e-mail and/or sms message) to a Host and/or Escort for a visitor or Tour Group.

Note: The format of the date is from the system default locale. To display correctly the **Region and Language** format should be set to "English (New Zealand)".

Procedure

1. Select the visitor record.
2. Click the **Send Message** button.
   The Send Message window displays if either the Host or Escort are configured to receive messages.



   Note: If only one of the Host or Escort is configured to receive messages, only that person's name will show. If either the Host and/or Escort is not configured to receive messages, a message will display indicating this.
3. Select the appropriate option from the **Message Type** drop-down list.
   The pre-formatted **Message Text** will change according to the **Message Type** you select, as follows:

Message Type	Message Text
Visitor/Tour Group will be late	[Visitor name]/[Tour Group name] will be late, now expected at

Message Type	Message Text
Visitor/Tour Group advises cancellation	[Visitor name]/[Tour Group name] has cancelled
For your information	[Visitor name]/[Tour Group name]

4. Edit the message if required.
5. Click the **Send** button.
   The Send Message window closes and the visit now has a notification icon next to it on the Home screen.
   Note: By hovering over the visit, a message displays indicating who has been manually notified.

Grace period and overdue alarm

Introduction

This topic defines what the grace period and overdue alarm is and when they occur.

Definitions

- **Grace Period**
  The grace period is the length of time (default 30 minutes) between when a visitor's status is set from 'Due to Leave' to 'Overdue'.

  Note: Your Command Centre administrator can configure, in Command Centre, a different grace period for each reception. If the grace period has been changed, this change will only affect newly created visits.

- **Overdue Alarm**
  When a visitor's status is set to 'Overdue' an alarm is raised in Command Centre.

  IMPORTANT: A visitor must be marked off-site before the Command Centre Operator/Guard can process the alarm. Alternatively the visit details can be changed, (e.g. visit departure time) so that the visitor is no longer considered overdue.

Example

Situation:

A visitor on a visit, has not checked-out and the departure time plus grace period has expired.

Result:

The following occurs:

- The visitor's status is set to 'Overdue' and an overdue alarm is raised.
- A copy of the visitor record is created on the 'Exceptions' status tab on the Home screen.
- If it has been configured in Command Centre, Hosts and Escorts will automatically receive a notification (via e-mail and/or sms message) that the visitor has become overdue, and the visit will have a notification icon next to it on the Home screen.
  Note: By hovering over the visit, a message displays indicating who has been automatically notified.

FAQs - Visitor Management

Q: Can two users edit the same visit?
A: No. A visit can only be edited by one user at a time.

Q: Why am I unable to cancel a visit?
A: If a card has been assigned to a visitor on a visit, the visitor needs to be marked off-site or their access card unassigned before the visit can be cancelled.

Q: Why am I unable to assign a card?
A: Either:

- This card has already be assigned to a visitor. View the status bar to confirm who this card has been assigned to.

OR:

- This person may already have a card assigned, (e.g. this person is already on a visit or this person is a permanent cardholder).

Q: Can I control what access the visitor is granted?
A: Yes, if your reception and user privileges have been configured in Command Centre to grant access, you can control what access is assigned to a visit, for a visitor.

Q: Can I grant a visitor additional access while on a visit?
A: Yes, if you have the required user privileges, you can assign additional access to the visit that the visitor is on, either before the visit starts or while the visit is in progress.

Q: Can I pre-register visitors and groups of visitors?
A: Yes, create a visit, add visitors and set the visit date for the future.

Q: Can I customise the badge label?
A: Yes, a badge label can be customised in Command Centre to incorporate a background template, (e.g. colour), visit details, visitor details, visitor photograph, company name, company logo or badge text.

Q: When does the access card assigned to a visitor expire?
A: Access is granted when the visitor is marked on-site. Access is removed when the visitor is marked off-site or temp off-site. Access can also be removed from the visitors visit, at any stage of their visit.

Q: Can I use a biometric reader?
A: Yes, a biometric reader, (e.g. fingerprint reader) can be used to identify hosts (permanent cardholders in Command Centre).

Q: Can I use passwords to protect the data?
A: Yes, a username and password is required to logon. User privileges determine what you can see and what actions you can perform.

Q: What reports can I produce?
A: You can generate a report that records the information on the Home and Find Visit screens. What information is shown on these screens is up to you, (e.g. display the time and attendance for a particular visitor).

Troubleshooting - Visitor Management Logon Failure

Failure to log on to Visitor Management is usually due to configuration errors. The following tables list some of the error messages that can appear on the Visitor Management Logon screen, and the reason why logon has failed:

Message	Cause(s)
"You require Visitor Management vVMC x.xx.xxxx".	The Visitor Management client version is different from the server version. Upgrade the client version to match the server version.
"Your workstation's time is out of sync with the server. Please contact your administrator"	If the server time or workstation time differs by more than 5 minutes, then the Visitor Management client will not log onto the server.
"The Visitor Management system is unavailable. Please contact your administrator"	The Command Centre services have not been started. Start the Command Centre services and Visitor Management services (Microsoft Windows Services).
"No Visitor Management receptions are available. Please contact your administrator"	The user does not have the privileges required to see any Receptions, (i.e. they do not have either the "Manage Reception" or the "Edit Visits", or the "View Visits" privilege in any Division which contains a Reception, in either the same division or sub division).
"The system cannot find any configuration for the reception called <reception name>. Please contact your administrator"	At least one of the receptions that the visitor can see does not have a division which has been configured for Visitor Management. The divisions checked for Visitor Management configuration will be the division specified on the Reception Command Centre item or any other division higher up the hierarchy of that division. At least one of those divisions checked must have the 'Visitor Management Configuration' flag set to 'Use this division's configuration' and have at least one Visitor Type on the 'Visitor Type' tab (of the Visitor Management tab).

Message	Cause(s)
"You do not have the appropriate privilege to create visitors in the division <division name>. Please contact your administrator" **Note:** <division name> is the Save Visitor Division name.	The user does not have the privileges they need for the receptions they can see. They have the "Edit Visits" privilege for the Save Visitor Division (it is assumed therefore that they are authorised to create/edit visits for this reception), but they cannot "Create and Edit Cardholders" in the same division.
"You do not have the appropriate privilege to assign escorts to visitors in the division <division name>. Please contact your administrator" **Note:** <division name> is the Find Visitor Division name.	The user does not have the privileges they need for the receptions they can see. They have the "Edit Visits" and "Manage Reception" privileges for the Save Visitor Division, and the Assign Escort action is enabled, but they do not have the "Manage Visitor Attributes" privilege for the Find Visitor Division.
"You do not have the appropriate privilege to assign visitors to the access group <access group>. Please contact your administrator" **Note:** <access group> is either the Visitor Type access group name, or the access group name.	The user does not have the privileges they need for the receptions they can see. They have the "Edit Visits" privilege for the Save Visitor Division, but they do not have the ability to add or remove cardholders from one of the visitor type access groups.
"You do not have the appropriate privilege to view visitors in the division <division name>. Please contact your administrator" **Note:** <division name> is the Save Visitor Division name.	The user does not have the privileges they need for the receptions they can see. They have the "View Visits" privilege for the Save Visitor Division (it is assumed therefore that they are only authorised to view visits for this reception), but they cannot view Cardholders in the same division.

Message	Cause(s)
"You do not have the appropriate privilege to view or create visits in the division <division name>. Please contact your administrator" **Note:** <division name> is the Save Visitor Division name.	The user does not have the privileges they need for the receptions they can see. Either: • they have the "Manage Reception" privilege for the Save Visitor Division (it is assumed that they are a receptionist for this reception), but they do not have either the "Edit Visits" or "View Visits" privilege in the same division (which means they cannot create/edit or view visits for this reception), OR, • they have the "Edit Visits" or "View Visits" privilege in the division which contains the Reception (in either the same division or sub division), but they do not have the "Edit Visits" privilege in the Save Visitor Division (which means they cannot create/edit visits for this reception).
"You do not have the appropriate privilege to view the card type <card type>. Please contact your administrator" **Note:** <card type> is the name of the card type for which the user does not have the required privilege.	The user does not have the privileges they need for the receptions they can see. They have the "Edit Visits" and "Manage Reception" privileges for the Save Visitor Division, and the Assign Card action is enabled, but they do not have the privileges to view the selected Card Type.
"You do not have the appropriate privilege to edit a mandatory visitor field for the visitor type <visitor type> for reception <reception name>. Please contact your administrator" **Note:** <visitor type> is the first visitor type for which the user's access fails the test for the pdf, and <reception name> is the reception for which the user access check failed.	The user does not have edit access for a visitor field that is mandatory at pre-registration, for any visitor type for a reception for which they have the "Edit Visits" privilege. Additionally, if the user is a receptionist and they do not have edit access for a visitor field which is mandatory at on-site, for any visitor type for a reception for which they have the "Edit Visits" privilege.

Message	Cause(s)
"The following Personal Data Fields are required and must be configured in the division <division name> for Visitor Management: <pdf name1>, <pdf name2>" **Note:** <division name> is the division for which the Visitor Type has been configured but the required pdf has not been selected. <pdf name1>, <pdf name2> are the names of the required pdfs which have not been selected and marked as required. There can be as many pdfs listed as there are pdfs which meet this condition for the named division.	A required PDF which does not have a default value has been added to a Visitor Type access group that has been configured for Visitor Management, BUT the PDF has not been selected on the Visitor Fields tab and has not been marked as 'Required when adding to a visit'. **Note:** This scenario only occurs if the PDF is added to the Visitor Type access group after the Visitor Type has been configured for Visitor Management on a Division, AND no visitors of that (Visitor) Type have yet been scheduled for meetings).
"The visitor access group <access group name> contains at least one required Personal Data Field without a configured default value" **Note:** <access group name> is the name of the access group which has been configured as a visitor access group for Visitor Management, but contains at least one required pdf without a default value.	A required PDF which does not have a default value has been added to an access group that has been configured as a 'Visitor Access' group for Visitor Management.
"Operator logged out due to repeated logon failures"	A users successive logon attempts has reached the configured 'number of failed attempts before lockout'. They are locked out for the configured lockout period (or permanently if this option is set). The user can re-enter their logon name and password, and authenticate successfully once the lockout period (which is not displayed) has completed. A privileged operator can unlock the account for the user if need be.

Visitor Management Barcode Scanner Process

Introduction

Visitors can be assigned a QR Code barcode (Quick Response Code format), to allow them to sign in and sign out as fast as possible.

Prerequisites

In order for the Visitor Management Client and Kiosk to use barcodes to sign visitors in or sign out, additional software must be installed on any workstation that runs the Visitor Management Client or Kiosk.

See ***Software required for Barcode Scanner Support*** (next) for details.

Procedure

Creating a Badge with barcode

1. Create a visitor card/badge with barcodes in Configuration Client.
   See ***Adding Visitor details to cards/badges*** (on page 50-42) for the procedure.

Setting up email for sending invitation

Configure email in Configuration Client so the Reception is able to send an email from Visitor Management.

2. Set the site default mail user agent, as follows:
   a) Click **File** from the menu bar, then **Server Properties**.
   b) Click the **Advanced** tab.
   c) Select the appropriate **Site Default Mail User Agent** from the drop-down list.
3. Set the email programme to use for sending invitations to Visitors during the Hosts Visit creation and edit process, as follows:
   a) Open the default Reception for the Workstation.
   b) Click the **Visitor Management** tab.
   c) Click the appropriate **Mail User Agent** radio button for the mail programme you want to use to access the email software.
   Note: If the option you select is not available when invoked, the 'Default Mail User Agent' (configured on the **Operator Defaults** tab of the Server Properties) will be used.

Enabling the Send Invitation action for Receptionists

Allow Receptionists to send invitations in Configuration Client.

4. Click **Configure** from the menu bar, then **Divisions**.
5. Open the "Visitor Division", (i.e. the Visitor Management Configuration Division), and click the **Visitor Management** tab. The **Visitor Types** sub-tab displays by default.
6. Click the **Reception Actions** sub-tab.
7. Check the **Send Invitation** checkbox.
8. Click the **OK** button to exit and save your changes.

Creating an Invitation

Create an invitation in the Visitor Management application.

9. From either the Visit or Home screen, select a visitor record and click the **Invite** action button.

   Note: This requires the Visitor to be the correct Visitor Type and have a configured Email PDF with a valid Email in it. If not, an email will still be created but the To field will be blank.

   The Visitor receives the email with an attached **.png** file containing the QR Code barcode.

Visitor Arrival

When the Visitor arrives for the visit:

- they can scan the Barcode directly from the cell phone or printed out on a piece of paper, this will either mark them as signed in or on site depending on configuration.
- a Badge is printed that contains a Barcode (this is a manual action).
- when the Visitor is ready to leave, they swipe the Barcode on their Badge and they are marked off site.

Software required for Barcode Scanner Support

Introduction

The Visitor Management Client and Kiosk support the use of barcode scanners that implement the OPOS Protocol. There are several software components that need to be installed for barcode scanners to work with Command Centre applications. These applications have been tested with the following barcode scanners:

- Zebra DS457 Fixed Mount Barcode Scanner
- Zebra DS9208 Digital Scanner
- Honeywell 1400g Hand Held Barcode Scanner
- Zebex Z-6112SR Barcode Scanner
- Zebex Z-5652 Barcode Scanner
- Datalogic GFS-440 Barcode Scanner

Procedure

Perform the following procedures in the order specified, to install the required software on all workstations that run the Visitor Management Client or Kiosk.

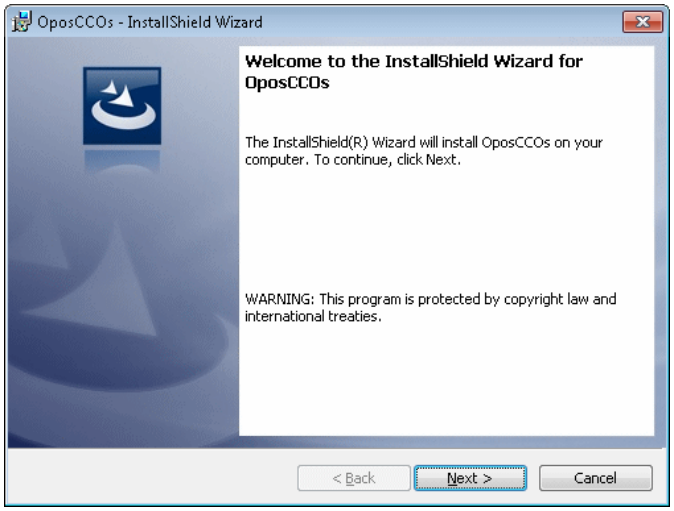
Install and configure the Scanner

1. What type of barcode scanner are you installing?

If a...	then...
Zebra DS457 scanner,	see ***Zebra DS457 Barcode Scanners*** (on page 50-152) for the procedure.
Zebra DS9208 scanner,	see ***Zebra DS9208 Scanner*** (on page 50-157) for the procedure.
Honeywell 1400g scanner,	see ***Honeywell 1400g Barcode Scanner*** (on page 50-160) for the procedure.
Zebex Z-6112SR scanner,	see ***Zebex Z-6112SR Barcode Scanner*** (on page 50-163) for the procedure.
Zebex Z-5652 scanner,	see ***Zebex Z-5652 Barcode Scanner*** (on page 50-167) for the procedure.
Datalogic GFS-440 scanner,	See ***Datalogic GFS-440 Barcode Scanner*** (on page 50-169) for the procedure.

Installing the OPOS Common Control Objects

2. Run the **OPOS_CCOs_1.14.001.msi** installer located in the **`'Utilities\Visitor Management Drivers'`** folder of the Command Centre files. The 'Welcome' screen of the OposCCOS InstallShield Wizard displays.



3. Click the **Next** button.
   The 'Destination Folder' screen displays.
4. Click the **Next** button.
   The 'Setup Type' screen displays.
5. Click the **Next** button.
   The 'Ready to Install the Program' screen displays.
6. Click the **Install** button.
   The 'Installing OposCCOS' screen displays. Once OposCCOS has finished installing, the 'InstallShield Wizard Completed' screen displays.
7. Click the **Finish** button to close the Installer.

Installing the Visitor Management Client or Kiosk

8. Install the Visitor Management Client or Kiosk.
   See ***Visitor Management Application Installation Instructions*** (on page 50-3) or ***Visitor Management Kiosk Installation Instructions*** (on page 51-3) as appropriate for the procedure.

Zebra DS457 Barcode Scanners

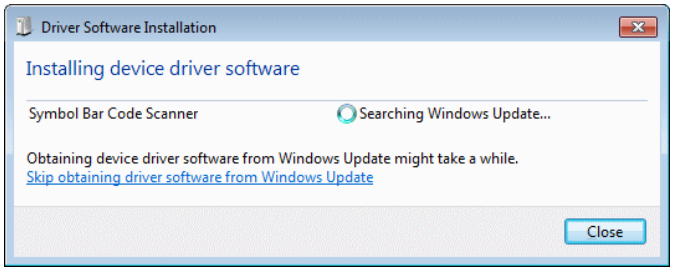
Procedure

Install and configure the required software for a **Zebra DS457 Fixed Mount Barcode Scanner** on all workstations that run the Visitor Management Client or Kiosk, as follows:

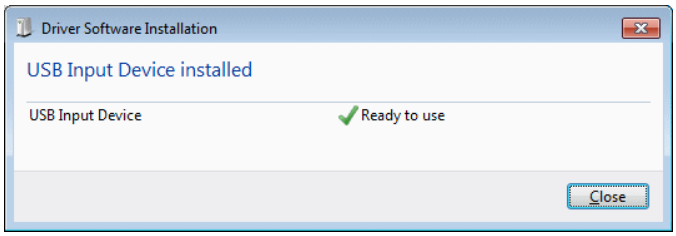
Install and configure the Scanner

Most scanners use a USB connection. Install and configure the scanner as follows:

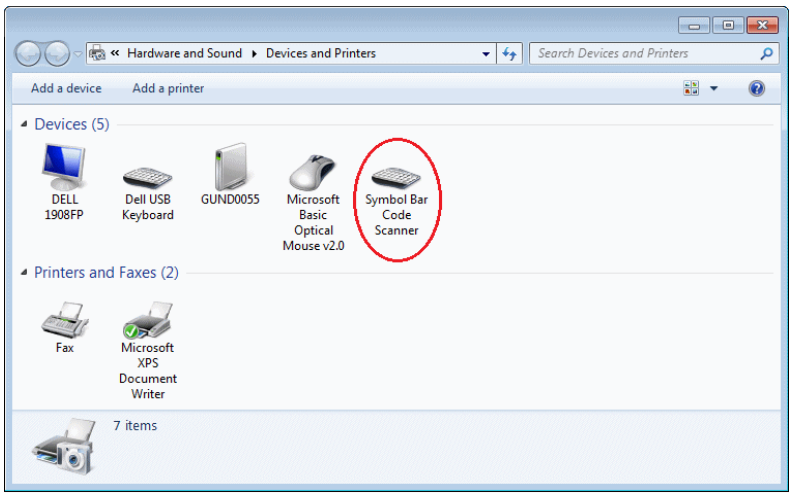
1. Plug the scanner in.
   The 'Installing Device Driver Software' dialog displays.



   The Windows Update service is used to download the software. When the drivers have been downloaded the dialog changes, as follows:



   The Devices and Printers windows should now look like this:



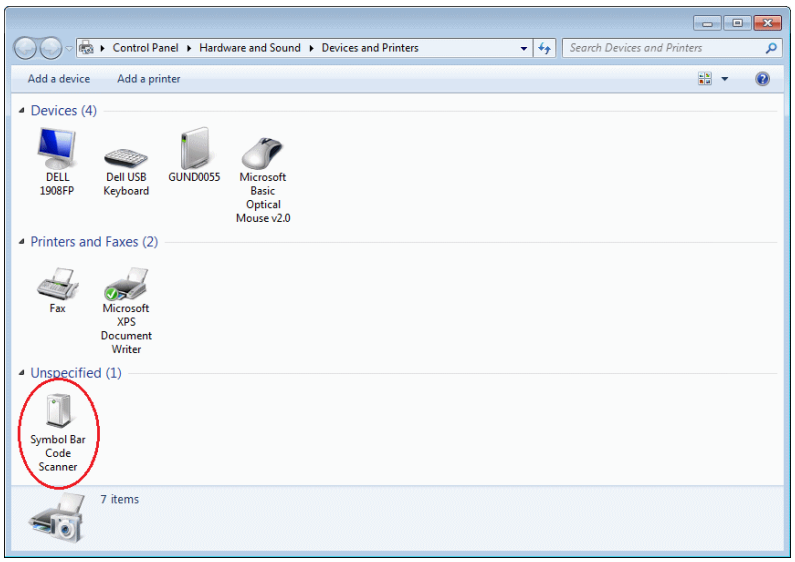
2. Typically, a scanner is configured by default to insert scanned data in to the keyboard stream. The Command Centre applications require the scanner to act as a SNAPI or IBM HAND-HELD USB scanner. This avoids inadvertantly scanning barcodes into data entry fields. Change the scanner

configuration by scanning the Symbol Native API (SNAPI) without Imaging Interface programming barcode from the DS457 Quick Reference Guide.

In addition to this, if the scanner is going to be used to scan the QR Code from a screen, (i.e. cell phone or tablet), then it may need to be programmed to handle this.

This is achieved by downloading the appropriate document from the Zebra Support Portal, and scanning the Mobile Phone/Display Mode barcode on page 6-22 of the **DS457 Fixed Mount Imager Integration Guide** (https://www.zebra.com/content/dam/zebra_new_ia/en_us/manuals/barcode-scanners/ds457-integration-guide-en-us.pdf)

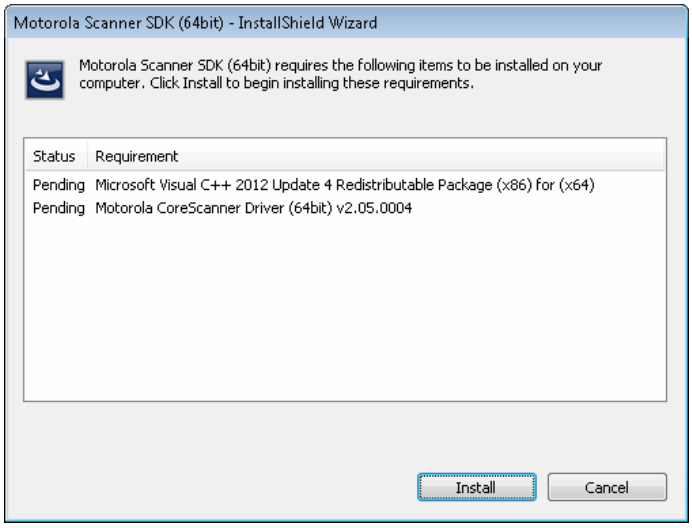
The drivers used to access the scanner are changed, and the Devices and Printers control should now look like this:



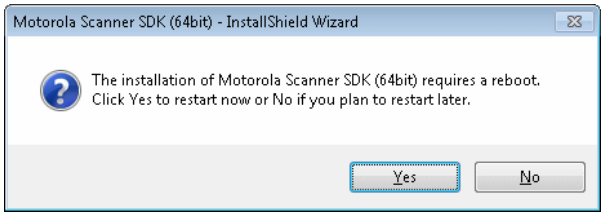
Installing the Zebra Scanner SDK for Windows

3. Download and install the latest version of the Zebra Scanner SDK for Windows, from the ***Zebra Support and Downloads*** (https://www.zebra.com/us/en/support-downloads/software/developer-tools/scanner-sdk-for-windows.html).
   Notes:
   - The SDK can also be found in the **`'Utilities\Visitor Management Drivers\QRcode Scanner'`** folder of the Command Centre files.
   - Select either the 32 or 64 bit version as appropriate.

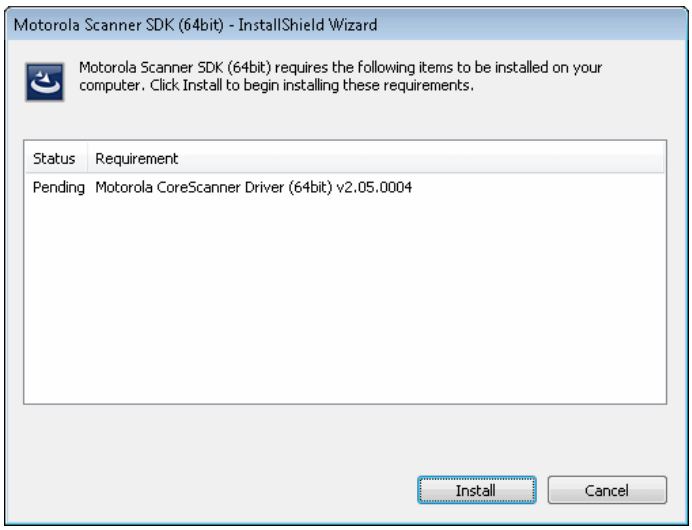
   The following screen displays, indicating the Scanner SDK requires some additional items to be installed, (i.e. C++ Redistributable package and the CoreScanner Driver).



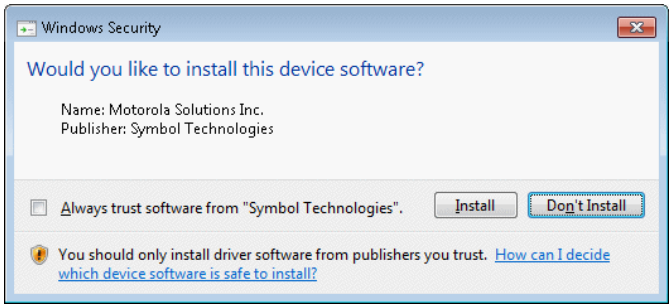
4. Click the **Install** button.
   After installing the C++ Redistributable package, the following message displays indicating that a reboot is required.



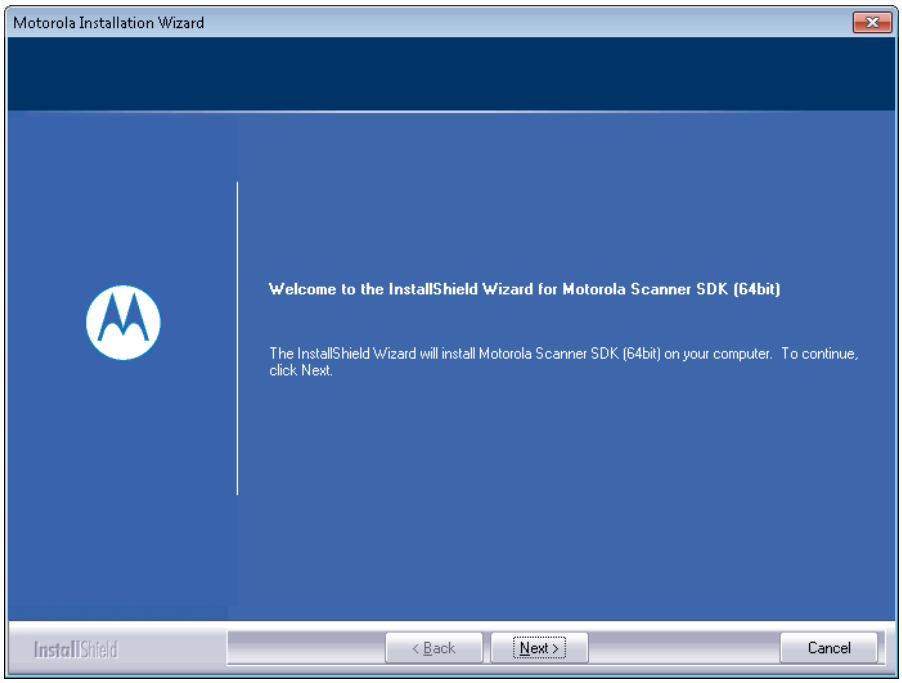
5. Click the **Yes** button. The Installer continues after the reboot.



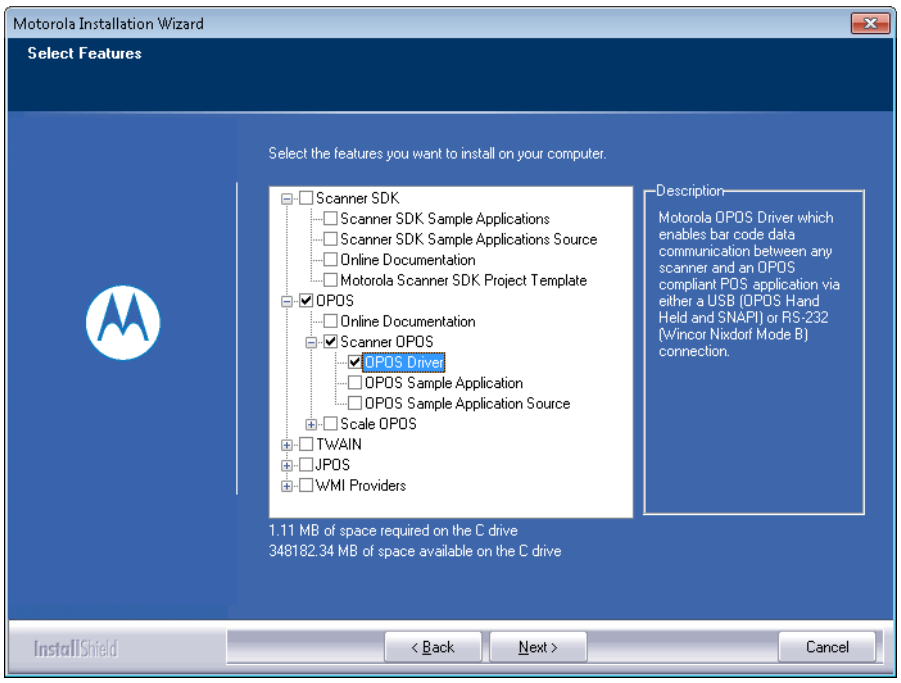
6. Click the **Install** button.
   A second reboot is required after installing the Core Scanner Driver.
7. Click the **Yes** button.
   The following dialog displays after the second reboot. The Scanner SDK Installer must be invoked again to continue the installation.



8. Click the **Install** button.
   The 'Welcome' screen of the Motorola Scanner SDK InstallShield Wizard displays.



9. Click the **Next** button.
   The 'License Agreement' screen displays.
10. Read the 'End User License Agreement' and click the **Yes** button.
    The 'Setup Type' screen displays.
11. Select the **Custom** radio button and click the **Next** button.
    The 'Select Features' screen displays.



12. The only required feature is the Scanner OPOS Driver, as shown in the above screen shot.
    Click the **Next** button.
    The 'Start Copying Files' screen displays.
13. Click the **Next** button.
    The 'Setup Status' screen displays. Once the Scanner SDK has finished installing, the 'InstallShield Wizard Complete' screen displays.
14. Click the **Finish** button to close the Installer.
    Note: The ReadMe file will be displayed but is targeted to an Application Developer.
15. Return to Step 2 of the ***Software required for Barcode Scanner Support*** (on page 50-150) procedure.

Zebra DS9208 Scanner

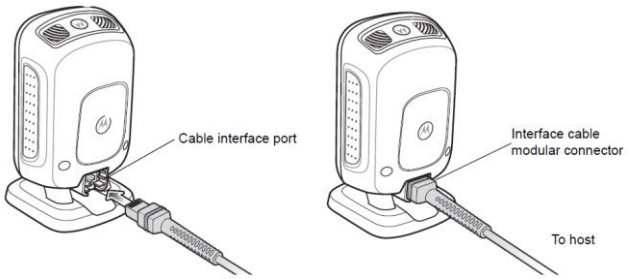
Procedure

Install and configure the required software for a **Zebra DS9208 Digital Scanner** on all workstations that run the Visitor Management Client or Kiosk, as follows:

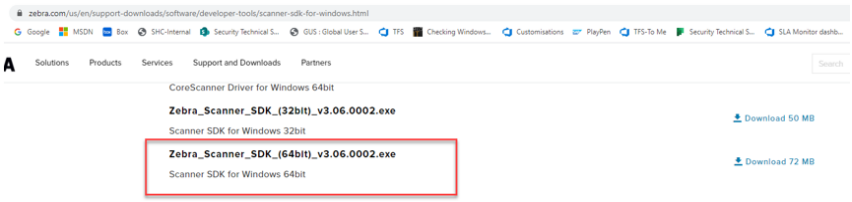
Setup Scanner and install SDK

Most scanners use a USB connection. Install and configure scanner as follows:

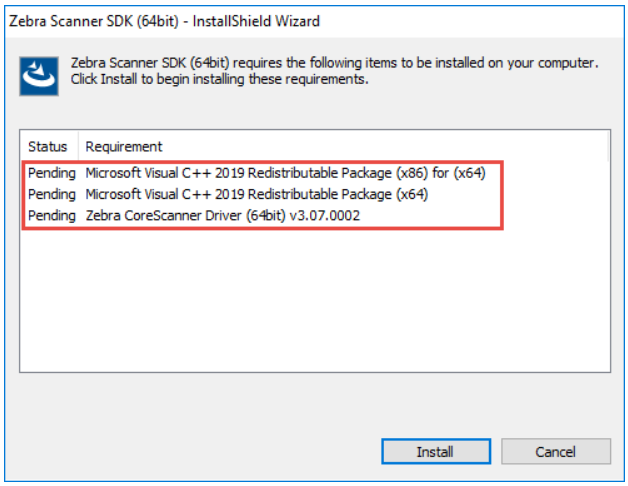
1. Install the interface cable.



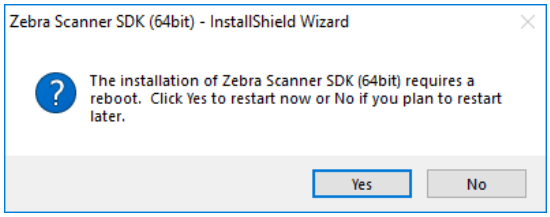
2. Plug the USB to the Visitor Management Kiosk PC.
3. Download and install the latest version of the Zebra Scanner SDK for Windows, from ***Zebra Support and Downloads***. (https://www.zebra.com/us/en/support-downloads/software/developer-tools/scanner-sdk-for-windows.html).
   Notes:
   - The SDK can also be found in the **`'Utilities\Visitor Management Drivers\QRcode Scanner'`** folder of the Command Centre files.
   - Select either the 32 or 64 bit version as appropriate.



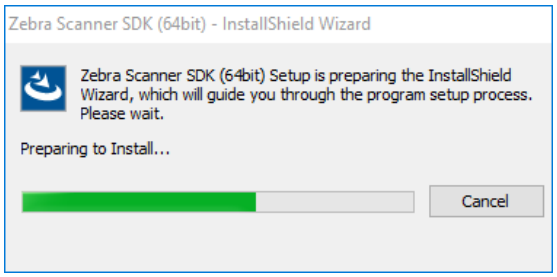
4. Double-click the installation file.
   The following screen displays, indicating the Scanner SDK requires some additional items to be installed, (i.e. Microsoft Visual C++ 2019 Redistributable Package and Zebra CoreScanner Driver).



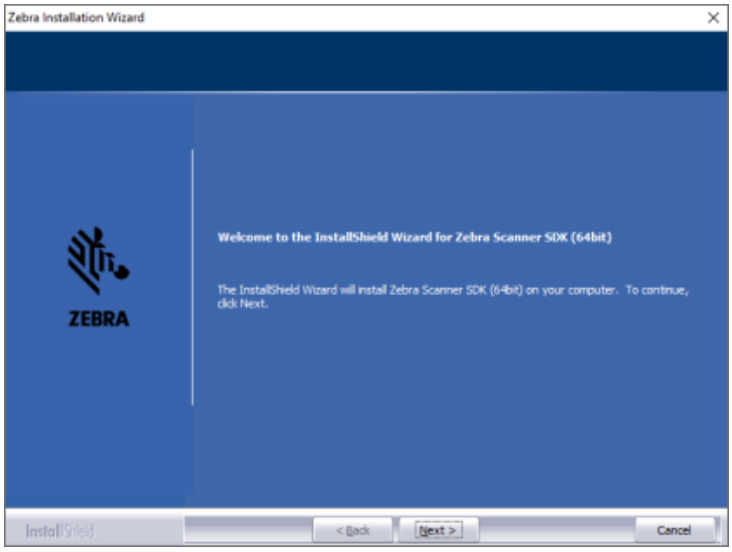
5. Click the **Install** button.
   After installing the C++ 2019 Redistributable package, the following message displays indicating that a reboot is required.



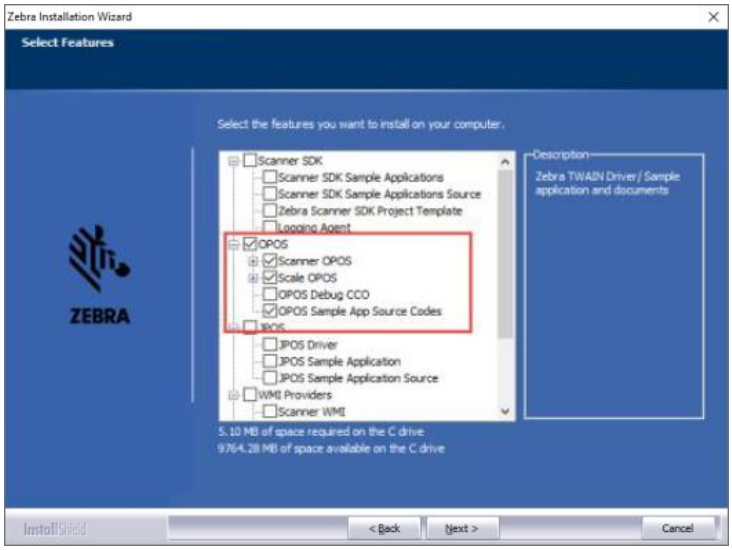
6. Click the **Yes** button. The Installer continues after the reboot.
7. Click the **Install** button.
   A second reboot is required after installing the Core Scanner Driver.



'Welcome' screen of the Zebra Scanner SDK InstallShield Wizard displays.



8. Click the **Next** button.
   The 'License Agreement' screen displays.
9. Read the 'End User License Agreement' and click the **Yes** button.
   The 'Setup Type' screen displays.
10. Select the **Custom** radio button and click the **Next** button.
    The 'Select Features' screen displays.



11. Choose **OPOS** driver for the scanner by ticking 'OPOS', 'Scanner OPOS', 'Scale OPOS' and 'OPOS Sample App Source'., and click the **Next** button.
    The 'Start Copying Files' screen displays.
12. Choose the path for installation and click the **Next** button.
    The 'InstallShield Wizard Complete' screen displays.
13. Click the **Finish** button to close the installer.
14. Set the scanner to defaults by scanning the following barcode.



***Set Defaults**

15. Set emulation mode to Symbol Native API (SNAPI) with Imaging Interface by scanning the following barcode.



Symbol Native API (SNAPI) with Imaging Interface

16. Return to Step 2 of the ***Software required for Barcode Scanner Support*** (on page 50-150) procedure.

Honeywell 1400g Barcode Scanner

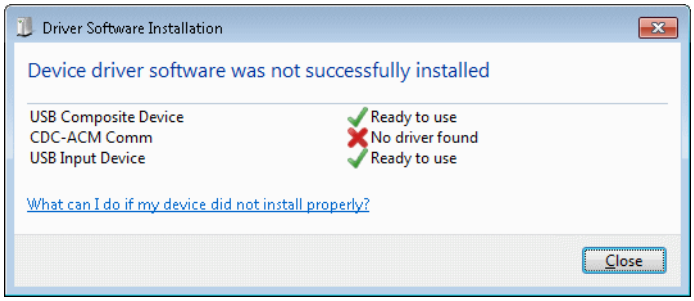
Procedure

Install and configure the required software for a Honeywell 1400g Hand Held Barcode Scanner on all workstations that run the Visitor Management Client or Kiosk, as follows:

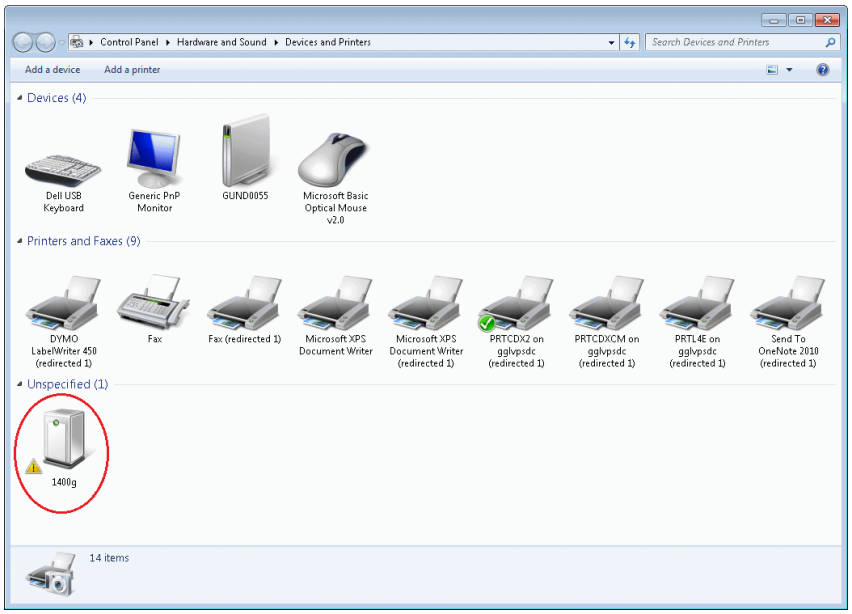
Install and configure the Scanner

Most scanners use a USB connection. Install and configure the scanner as follows:

1. Plug the scanner in.
   The 'Driver Software Installation' dialog displays.



2. Click the **Close** button.
   The Devices and Printers control should now look like this:



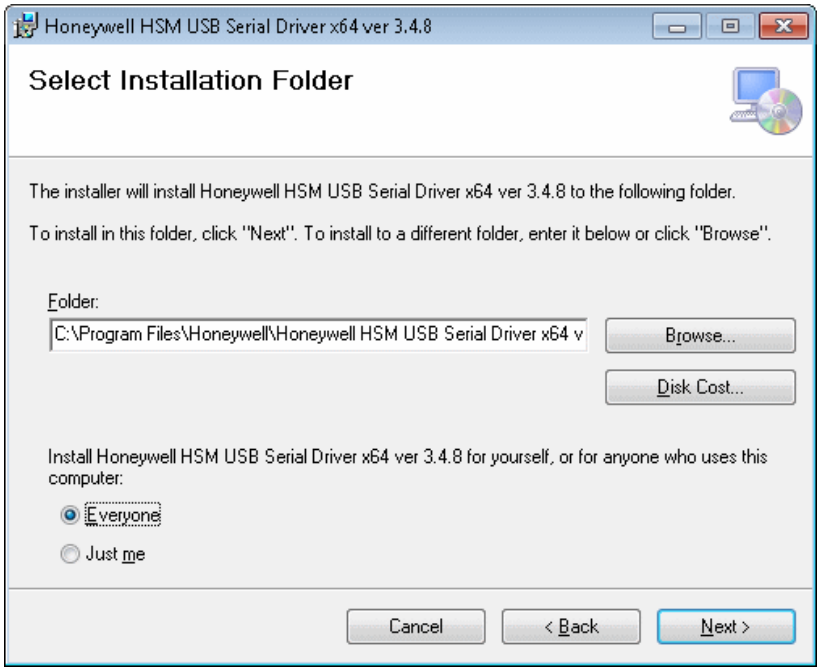
Installing the HSM USB Serial Driver

3. The HSM USB Serial Driver is available from the ***Honeywell Scanning and Mobility website*** (http://www.honeywellaidc.com), by searching for HSM USB Serial Driver and clicking the **Web Site Content** tab.

   Right click on **Setup.bat** and choose the 'Run as Administrator' menu option.

The 'Welcome' screen of the Honeywell HSM USB Driver Setup Wizard displays.

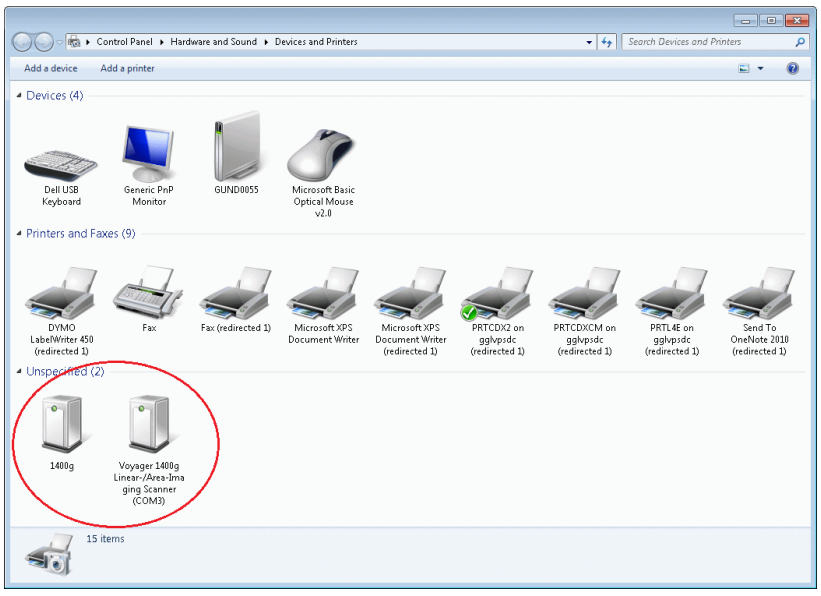
4. Click the **Next** button.
   The 'Select Installation Folder' screen displays.



5. Click the **Everyone** radio button, and then the **Next** button.
   The 'Confirm Installation' screen displays.

6. Click the **Next** button.
   The 'Installing Honeywell HSM USB Serial Driver' screen displays. Once the Serial Driver has finished installing, the 'Installation Complete' screen displays.

7. Click the **Close** button to close the Installer.
   The Devices and Printers control should now look like this:



Installing the Honeywell OPOS Suite_1.13.4.17

8. Download and run the Honeywell OPOS Suite application from the **Software** tab of the ***Honeywell Scanning and Mobility website*** (http://www.honeywellaidc.com/en-AP/Pages/Product.aspx?category=hand-held-barcode-scanner&cat=HSM&pid=Voyager1400g).
   The 'Welcome 'screen of the Honeywell OPOS Suite InstallShield Wizard displays, followed by the 'License Agreement' screen.
9. Read the 'End User License Agreement' and click the appropriate radio button to accept the terms of the license agreement.
10. Click the **Next** button.
    The 'Destination Folder' screen displays.
11. Click the **Next** button.
    The 'Setup Type' screen displays.
12. Click the **Next** button.
    The 'Ready to Install the Program' screen displays.
13. Click the **Next** button.
    The 'Installing Honeywell OPOS Suite' screen displays. Once the Honeywell OPOS Suite has finished installing, the 'InstallShield Wizard Completed' screen displays.
14. Click the **Finish** button to close the Installer.
15. If the scanner is going to be used to scan the QR Code from a screen, (i.e. cell phone or tablet), then it may need to be programmed to handle this. This is achieved by downloading the **Voyager 1400g Series Area-Imaging Scanner User's Guide** from the ***Honeywell Scanning and Mobility website*** (http://www.honeywellaidc.com/en-AP/Pages/Product.aspx?category=hand-held-barcode-scanner&cat=HSM&pid=Voyager1400g), and scanning the **Presentation Scanning - Mobile Phone** barcode (PAPPSC) provided on page 3-10.
16. Return to Step 2 of the ***Software required for Barcode Scanner Support*** (on page 50-150) procedure.

Zebex Z-6112SR Barcode Scanner

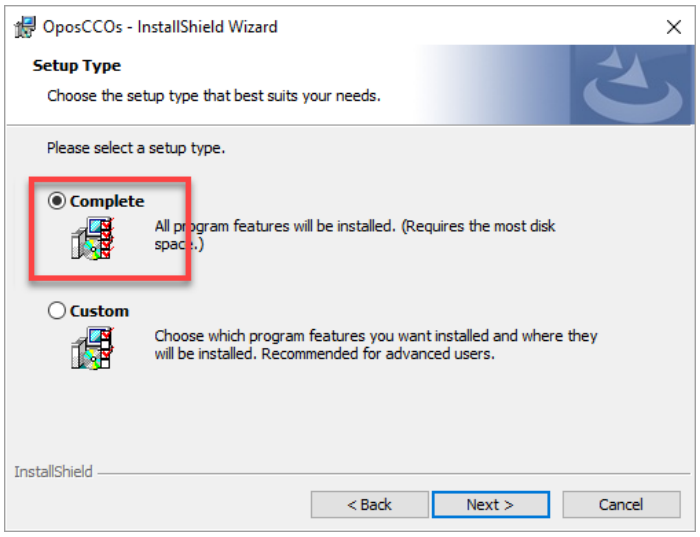
Prerequisite

You will need to print a hardcopy of this topic to be able to physically scan the various barcodes shown below, at the Zebex Z-6112SR Barcode Scanner you are installing.

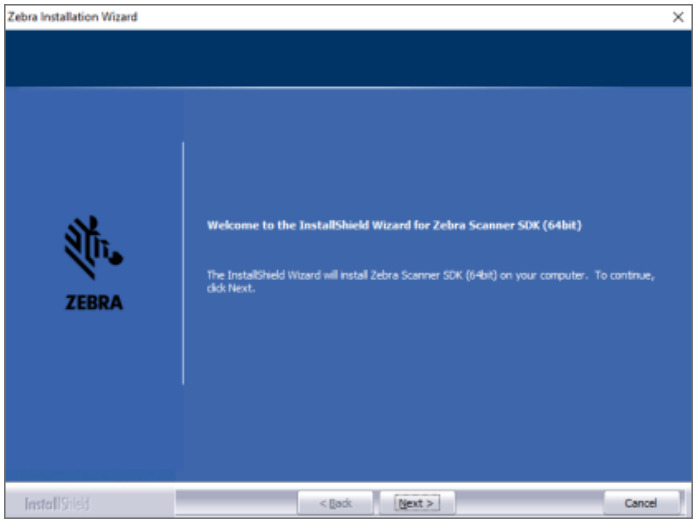
Procedure

Install and configure the Zebex Z-6112SR Barcode Scanner on all workstations that run the Visitor Management Client or Kiosk, as follows:

1. Run the **OPOS_CCOs_1.14.001.msi** installer located in the `'Utilities\Visitor Management Drivers'` folder on the Visitor Management Kiosk PC.

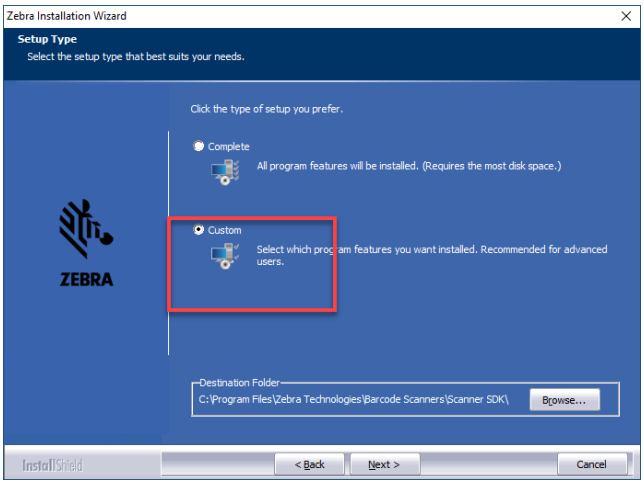


2. Install the **Zebra_Scanner_SDK_(64bit or 32bit)_v3.06.0002** located in the `'Utilities\Visitor Management Drivers\QRcode Scanner'` folder.
   The Core Scanner Driver installs and the 'Welcome' screen of the Zebra Scanner SDK InstallShield Wizard displays.

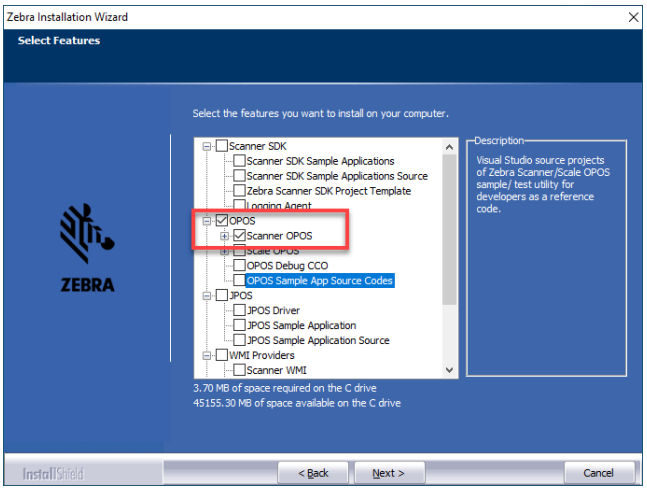


3. Click the **Next** button. The 'License Agreement' screen displays.

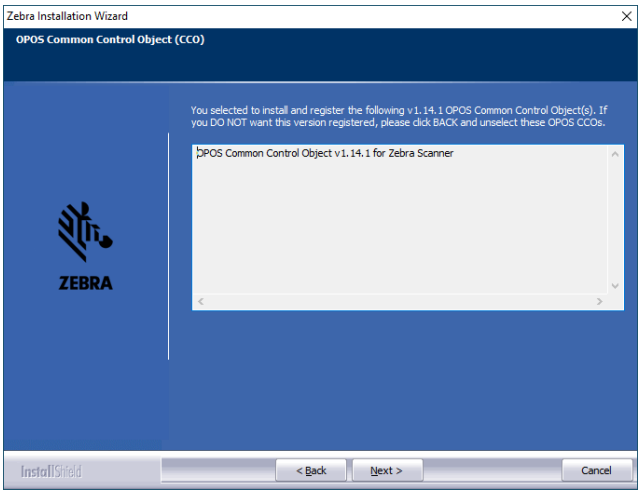
4. Read the 'End User License Agreement' and click the **Yes** button.
   The 'Setup Type' screen displays.



5. Select the **Custom** radio button and click the **Next** button.
   The 'Select Features' screen displays.



6. Choose **OPOS** driver for the scanner by ticking 'OPOS' and 'Scanner OPOS', and click the **Next** button.
   The 'OPOS Common Control Object (CCO)' screen displays.



7. Click the **Next** button. The 'InstallShield Wizard Complete' screen displays.
8. Click the **Finish** button to close the installer.

9. Plug the scanner into a USB port on the Visitor Management Kiosk PC.
10. Set the scanner to defaults by scanning the following barcode.



11. Enable parameter scanning by the following barcode.



12. Set emulation mode to Symbol Native API (SNAPI) with Imaging Interface by scanning the following barcode.



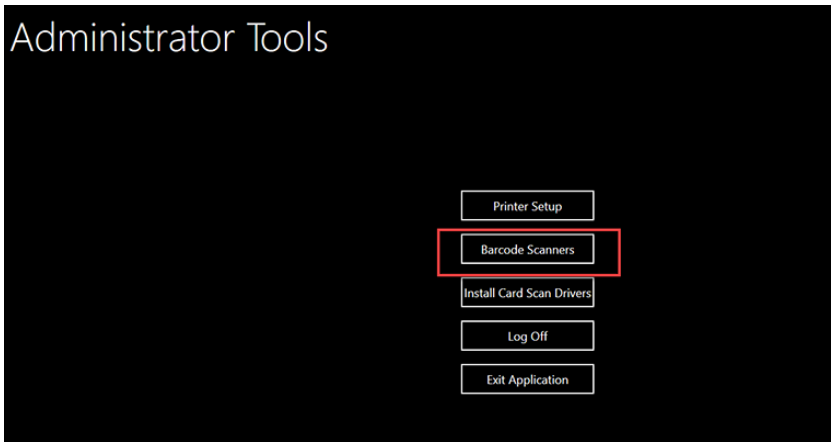
13. Take the scanner out of parameter mode by scanning the following barcode.



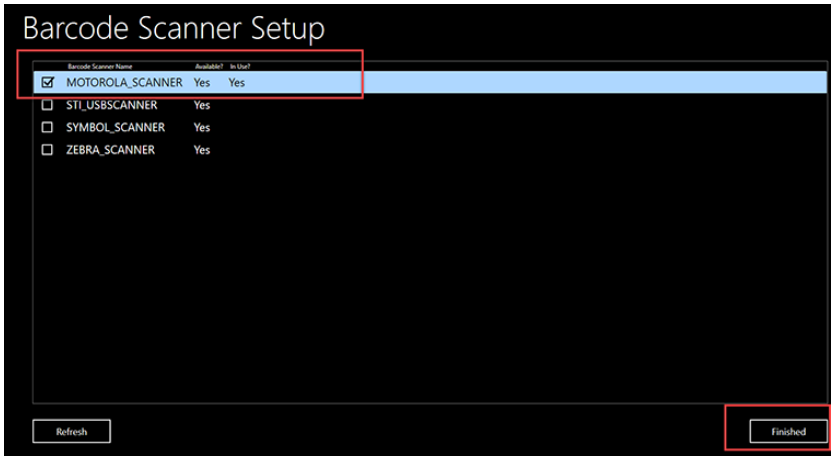
14. Enter the Kiosk Host action screen as a Kiosk Administrative user and select the **Tools** button.



15. Select the **Barcode Scanners** button on the Administrator Tools screen.



16. Ensure the MOTOROLA_SCANNER is recognised.



17. Select the **Finished** button.
    You can check the installed applications on the kiosk machine:



Zebex Z-5652 Barcode Scanner

Prerequisite

You will need to print a hardcopy of this topic to be able to physically scan the various barcodes shown below, at the Zebex Z-5652 Barcode Scanner you are installing.

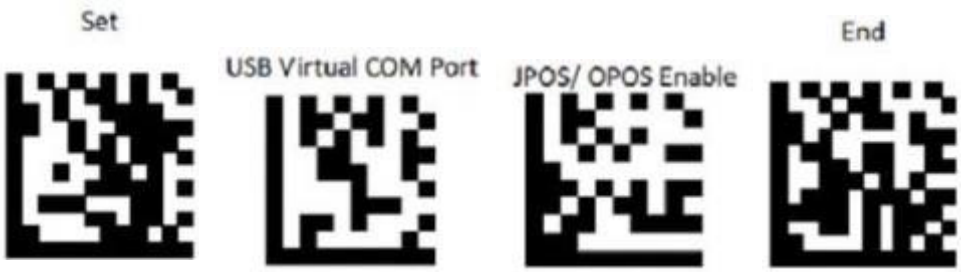
Procedure

Install and configure the Zebex Z-5652 Barcode Scanner on all workstations that run the Visitor Management Client or Kiosk, as follows:

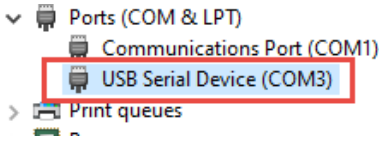
1. Connect the driver USB to computer port.
2. For Windows XP, install the attached VCOM Driver (**VCOM_Driver_ Installation_v1.0.0.1.zip**) located in the `'Utilities\Visitor Management Drivers\Zebex Drivers'` folder of the Command Centre installation files.
   Note: This step is not necessary for Windows 10.
3. Install the OPOS Driver (**ZOPOS_V3.2.0.0_Setup.zip**) located in the `'Utilities\Visitor Management Drivers\Zebex Drivers'` folder of the Command Centre installation files.
   a) Extract file ZOPOS_V3.2.0.0_Setup file to local PC or VM.
   b) Run **ZOPOS_V3.2.0.0_Setup.exe**
   The 'Welcome' screen of the OPOS Service Control Setup Wizard displays.



   c) Click the **Next** button. The 'Select Destination Location' screen displays.
   d) Click the **Next** button. The 'Ready to Install' screen displays.
   e) Click the **Install** button.
   The 'Completing the OPOS Service Control Setup Wizard' screen displays.
   f) Click the **Finish** button to close the Installer.
4. Scan the following barcodes in the sequence below to configure the scanner to USB-Serial Mode.
   Note: As you scan each individual barcode, you may need to cover the others to ensure they each get read correctly.



5. Go to `'C:\Program Files (x86)\OPOS Service Control V3.2.0.0'` and run **ConfigOPOS.exe**
   The 'ZOPOSConfig 3.2.0.0' dialog displays.
6. Select the related COM **Port** (which is what shows for this device in Device Manager as shown below).





7. To create a new scanner, click the **New** button.



   The 'Create a new device...' dialog displays.
8. Enter the **Device Name** and select the "2D Scanner [USB]" from the **Scanner Type** drop-down list.



9. Click the **OK** button.
   The scanner setup is complete.

Datalogic GFS-440 Barcode Scanner

Procedure

Install and configure the required software for a Datalogic GFS-440 Barcode Scanner on all workstations that run the Visitor Management Client or Kiosk, as follows:

1. Download and install the OPOS Drivers from Datalogic on all workstations running the Visitor Management Client or Kiosk where the barcode scanner will be used. Follow the install instructions bundled with the drivers to run the installation. Select **Yes** (typical) when asked to install the control objects.

   OPOS 1.14.199 Drivers:
   https://cdn.datalogic.com/Download?iddwnfile=35971
2. Connect the barcode scanner to the workstation via USB.
3. From the *Datalogic Quick Reference Guide* document, using the barcode scanner, scan the 'USB-OEM (for use with OPOS/UPOS/ JavaPOS)' configuration QR code under the 'Setting Up the Reader' section.
4. Return to Step 2 of ***the Software required for Barcode Scanner Support*** procedure (on page 50-150).

Visitor Management Passport/Drivers License Scanning Process

Introduction

The 'Visitor Management OCR Passport / Drivers License Interface' allows the Gallagher Visitor Management Client to support an interface to a number of scanners, such that Visitor fields in the Visitor Management Client can be automatically populated when a form of ID is scanned, (e.g. Passport or Driver's License). The aim is to reduce the amount of manual data entry required by an Operator and improve Visitor processing time.

The scanners that Visitor Management interface with are:
- SnapShell Passport Scanner,
- Gemalto QS1000 Passport Scanner, and
- Acuant i-Dentify ID-150 Card Scanner.

Notes:

- The SnapShell Passport Scanner supports Microsoft Windows 8 and 10 (32 & 64 bits).
- SnapShell Passport Scanners cannot be used for the Visitor Management Client and the Visitor Management Kiosk at the same time.
- The SnapShell Passport Scanner is End of Life, and no longer available for purchase.

Prerequisites

- If you already have version vEL.7.30.2014 with this feature installed, you must first uninstall the ScanShell SDK before Gallagher Command Centre can be upgraded, as follows:
  1. Exit Command Centre and stop the Command Centre Services.
  2. Uninstall the ScanShell SDK, (i.e. **CSSN SDK Version 10.05.20.05**), using the Windows **Programs and Features** utility.
- Visitor Management Scanning requires the following Interface (**Accuant OCR Scanner Interface - C12716**) and Licence file entry - (**Visitor Management ID Scanning=1**) to enable the capture of:
  - Passports, Drivers Licenses and National Identity Cards, and
  - information from visitors at the Visitor Management workstation, when integrated with Command Centre.

Procedure

To configure and use this feature, perform the following procedures in the order specified.

Creating a Personal Data Field

1. Create a Personal Data Field (e.g. Date of Birth) that will be used by the Passport Scanner, in Configuration Client or Command Centre Client.

See ***Creating a new Personal Data Field*** (on page 33-2) for the procedure if using Configuration Client.

Note: If using Command Centre Client, see "Creating a new Personal Data Field" in the Command Centre User Guide for the procedure.

Adding the Personal Data Field to Visitor Types

2. Add the Personal Data Field (configured in Step 1) to the appropriate Access Groups (Visitor Types), in Configuration Client or Command Centre Client. See Step 27 of ***Setting up Access Groups*** (on page 34-4) for the procedure if using Configuration Client.

   Note: If using Command Centre Client, see Step 10 of "Creating a new Access Group" in the Command Centre User Guide for the procedure.

Adding the Personal Data Field to the Visitor screen

3. Add the Personal Data Field (configured in Step 1) to the Selected Fields grid on the **Visitor Fields** tab of the Visitor Management Division Configuration, in Configuration Client.
   See ***Visitor Fields tab*** (on page 50-22) for the procedure.

   Note: The order of the Personal Data Fields listed in the Selected Fields grid will match the order of the Personal Data Fields shown on the Visitor screen in the Visitor Management client. If required, check the **Required when adding to a visit** or **Required when marking On Site** checkboxes.

Creating Data Maps

The scanning software must be configured to automatically populate the Visitor fields (within Visitor Management) when a Passport or Driver's License is scanned.

4. Create Data Maps in Command Centre Client.
   See "Creating a Data Map" for the procedure in the Command Centre User Guide.

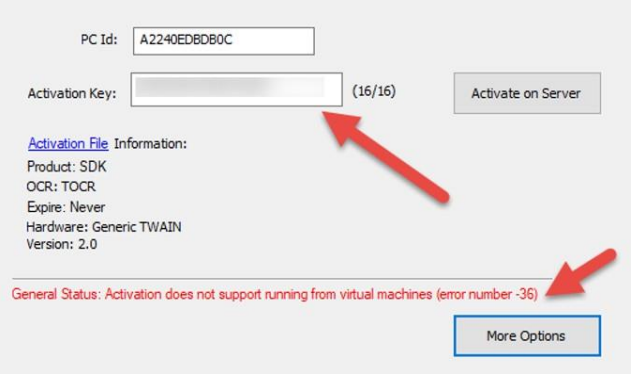
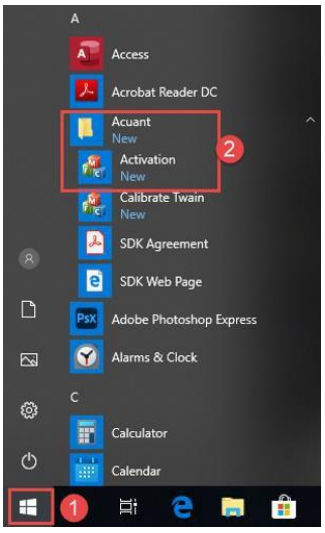
Installing the Scanner

Installing a document scanner installs the necessary SDK and drivers for the specific scanner. Log on as an Administrator, and install for each client as follows:

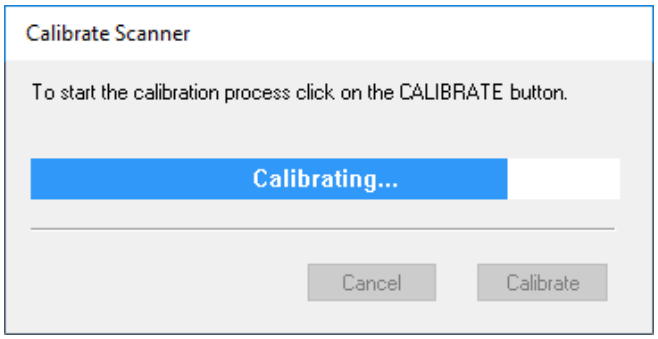
5. Ensure the Scanner is not connected to the PC.
6. Run the **OPOS_CCOs_1.14.001.msi** installer located in the **`'Utilities\Visitor Management Drivers'`** folder of the Command Centre installation files.
7. Install the Card Scan Drivers (**DPInst.exe**) located in the **`'Utilities\Visitor Management Drivers\Card Scan Drivers\Drivers'`** folder.

8. From the **'Utilities\Visitor Management Drivers\ScannerDrivers'** folder, run the relevant silent install patch file for the type of scanner you are installing.

   Note: The patch files install all the drivers for the scanner from the **SDK_setup_is.exe** file automatically.

Scanner type	Install patch file…
SnapShell,	InstallerForSnapShellScanner.bat
Gemalto QS1000,	InstallerForGemaltoScanner.bat **Note:** The QS1000 scanner is the only one that the following ActivatedSDK window displays after the **SDK_setup_is.exe** finishes installing.  Type in the **Activation Key** and click the **Activate on Server** button to activate the key. The QS1000 scanner will not work without this activation key. **IMPORTANT:** Gallagher do not provide this activation key for users. Please contact Acuant company for this key. The Activation Application can be found from **Start** > **Acuant** > **Activation**. 
Acuant i-Dentify ID-150,	InstallerForID150Scanner.bat

9. Restart the PC.
10. Make sure all the drivers have installed correctly by checking the Windows **Programs and Features** list.
11. Plug the scanner into the PC.
12. Manually start the Visitor Management Client.
13. Go to the Visitor window and click the **Scan** button.
    Note: You require the "Edit Visits" operator privilege to scan.
14. Place the calibration sheet provided with the scanner into the scanner.
    A Calibrate Scanner screen displays.
15. Click the **Calibrate** button.
    Calibration starts.



When the progress bar reaches 100% calibration is complete, and a pop-up message *"Calibration done successfully"* displays.

Note: The scanner needs to be calibrated before being used for the first time, and may need recalibrating if unplugged.

Scanning a Passport or Driver's License for a Visitor

16. Scan a visitor's passport or driver's license in the Visitor Management application.
    See ***Scanning passports or driver licenses for visitors*** (on page 50-109) for the procedure.

Chapter 51: Visitor Management Kiosk

Introduction

The Visitor Management Kiosk, which is a licensable feature, allows visitors to a site to register their details from a self-service touch screen kiosk, and to automatically notify the host of the visitor's arrival without intervention by a reception. Hosts retain the responsibility for meeting the visitors and marking them on or off site, to ensure evacuation reports are up to date at any time. The Visitor Management Kiosk supports:

- **Individual visitors** arriving for a visit, who may or may not be pre-registered by the host.
- **Tour Groups** which have been pre-registered by the host. All members of a Tour Group must arrive and leave together.
- **Rapid Entry**, where existing cardholders who belong to specific Access Groups can use the 'Fast Track" process to gain quick entry.

The following general functionality is included to support the Visitor Management Kiosk:

- Automated logon (also known as 'single sign on') for hosts to the Gallagher Visitor Management client (this is the main client, not the kiosk) using the host's Windows logon credentials. This will allow hosts to pre-register visits. Command Centre configuration is required for each host to allow single sign on to the Visitor Management client.
- A Click-once installer to allow for installation of the Visitor Management Kiosk software.
- Visitor records are stored within the Command Centre database and their details can be viewed, updated or reported on from Command Centre.
- Configuration required for the kiosk, including configuration of the operator logon credentials for the kiosk will be achieved via Command Centre.
- A touch screen Visitor Management Kiosk. See ***Visitor Management Kiosk screens*** (on page 51-39) for further detail on the screens that a self-service kiosk provides.

The following features can be configured:

- Cards can be assigned to single visitors.
- Visitors can scan their business cards at a kiosk to simplify and speed up the data entry process.

- Capturing images.
- Support for Tour Groups.

Licensing

Visitor Management Kiosk is a licensable feature. The license file must contain the following options:

License option	Description
[Features] **VisitorManagement=1**	Allows you to see and configure the Kiosk in Configuration Client on the Division setup.
[Limits] **Visit Kiosk=n**	The number [n] indicates how many Kiosk Clients can be connected at one time.

In addition to these two options, if you want Hosts to be automatically notified of their visitor's arrival, your site licence file must also contain the option:

[Features]
Notifications=1

This chapter covers the following topics:

- ***Visitor Management Kiosk Installation Instructions*** (on page 51-3)
- ***Visitor Management Kiosk Configuration*** (on page 51-7)
- ***Configuring Visitor Management Kiosk*** (on page 51-15)
- ***Visitor Management Kiosk Document Scanning Process*** (on page 51-36)
- ***Visitor Management Kiosk screens*** (on page 51-39)

Visitor Management Kiosk Installation Instructions

Introduction

Initial installation of the Visitor Management Kiosk should be performed by a user who has administrative rights on both the server and client PC. The Visitor Management Kiosk then needs to be installed by each user individually, (i.e. there is no option to install for all users of the client PC). These subsequent Visitor Management Kiosk client installs do not need to be performed by Administrators, the users just need to have access to the VMClientUpdate shared folder on the server, (i.e. \\[ServerName]\ VMClientUpdate).

Note: When installing Visitor Management Kiosk, make sure the operator logged into the kiosk has the privilege to view all cardholders who might badge at the kiosk for rapid entry.

Procedure

The following procedure for installing the Visitor Management Kiosk has been split into three parts:
- Server Installation,
- Client Installation, and
- Card Scan Driver Installation (if business card scanning capability is going to be used).

Visitor Management Kiosk Server Installation

1. Ensure the site licence file **CommandCentre.lic**:
   - is accessible on the PC. It is recommended that this file be copied to `'C:\Windows'` prior to commencing the installation, and
   - contains the following options:

License option	Description
`[Features]` `VisitorManagement=1`	Allows you to see and configure the Kiosk in Configuration Client on the Division setup.
`[Limits]` `Visit Kiosk=n`	The number [n] indicates how many Kiosk Clients can be connected at one time.

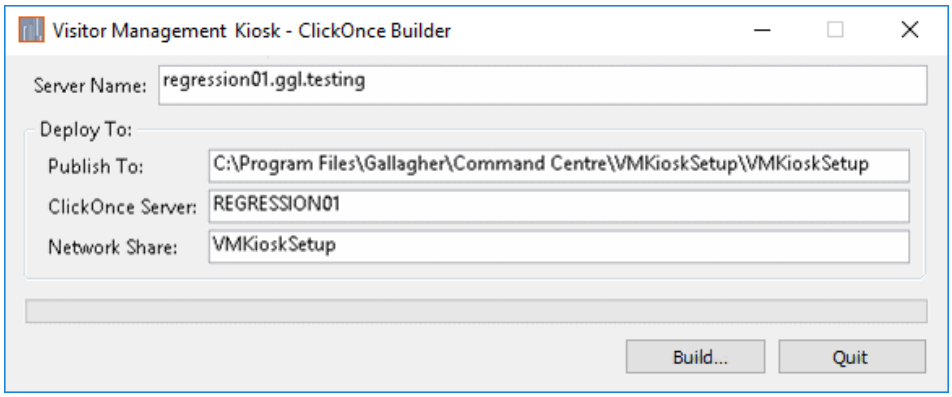
In addition to these two options, if you want Hosts to be automatically notified of their visitor's arrival, your site licence file must also contain the option:

```
[Features]
Notifications=1
```

2. Install Gallagher Command Centre.
   Refer to the appropriate release note with the Gallagher Command Centre installation files, (i.e. either the "New Installations" release note or the "Upgrade Procedures" release note), for the procedure.
3. At the time Command Centre is installed, the Visitor Management Kiosk Client is automatically built to the default location of **`'C:\Program Files\Gallagher\Command Centre\VMKioskSetup\VMKioskSetup'`**. Although we recommend sites leave the Kiosk Client in this default location, it can be built to a different location.
   Do you want to build it to a different location?

If...	then...
no	the Server Installation is complete. Go to the **Visitor Management Kiosk Client Installation** procedure below.
yes	go to Step 4.

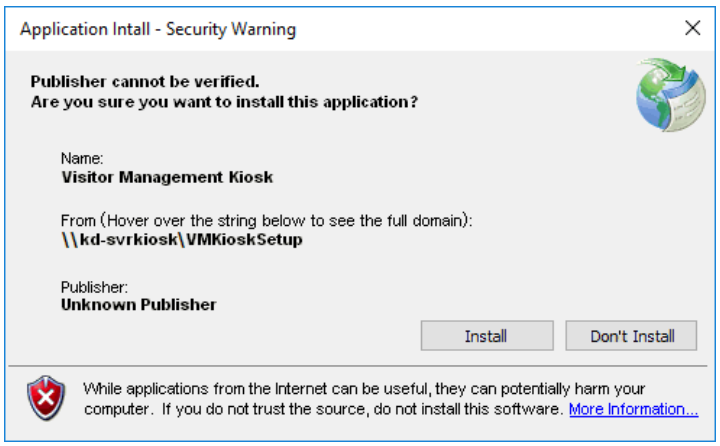
4. Go to the **`'C:\Program Files\Gallagher\Command Centre\VMKioskSetup`**' folder and double-click on **ClickOnceBuilder.exe**.
   The Visitor Management Kiosk - ClickOnce Builder screen displays.



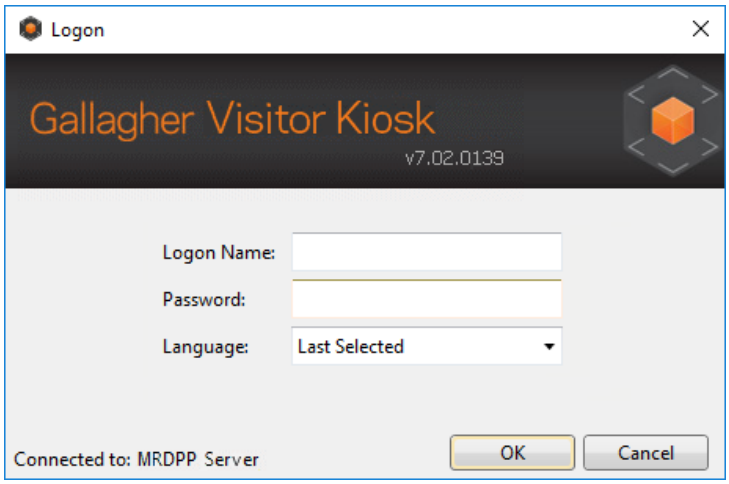
5. Change the 'Deploy To' settings to the required location, and click the **Build** button.
   The Client build may take a few minutes.
   Note: ClickOnce supports deployment via HTTP/HTTPS. You can specify a URL instead of a machine name for the **ClickOnce Server** name.
6. Ensure the folder indicated in the **Publish To** field is shared, and the path is set correctly in the **Network Share** field.
   This allows the Visitor Management Kiosk application to be installed on other computers.
7. Click the **Quit** button.

Visitor Management Kiosk Client Installation

1. Browse to the **`'\\[ServerName]\VMKioskSetup'`** folder and run the installation executable, (i.e. **ClickOnceVMKioskSetup.exe**) to initiate the client install. The following Application Install Security Warning displays:



2. Click the **Install** button.
   The Visitor Management Kiosk client installs and the logon screen displays:



3. Type your **Logon Name**.
4. Click in the **Password** field (alternatively, press the **Tab** key), and type your password.
5. Select another language from the **Language** drop-down box if required.
6. Click the **Logon** button (alternatively, press the **Enter** key).
   Note: If you enter successive invalid logon name and password combinations equal to the configured 'number of failed attempts before lockout', then you will be locked out for the configured lockout period (or permanently if this option is set). The message *"Operator locked out due to repeat logon failures"* will display on the logon screen.

Card Scan Driver Installation

Before the card scan drivers are installed, all the necessary Visitor Management Kiosk configuration work in Command Centre should be performed. Once all the components are configured, the card scan drivers need to be installed by a member of the Kiosk Administrator Access Group, as follows:

1. While the 'Welcome screen' is displayed, present your card at the Kiosk Door/Reader.
2. Open the **Tools** screen, if not already open.
3. Click the **Install Card Scan Drivers** button.
   The card scan drivers install.

It may not be possible to install the card scan drivers via the Kiosk application. This could be because the logged in user is not an Administrator or User Account Control is switched on. To install the drivers manually:

1. Browse to the **'Utilities\Visitor Management Drivers\Card Scan Drivers'** folder of the installation files.
2. Copy the drivers folder from the installation files to **'C:\Program Files\ Gallagher\Command Centre\VMKioskSetup\ VMKioskSetup'** on the server.
3. On the Client PC browse to **'\\[Server_name]\VMKioskSetup\Drivers'**, double click on **dpinst.exe** and follow the on screen prompts.
   Note: For 64 bit machines browse to **'\\[Server_name]\VMKioskSetup\Drivers\x64'**.

Visitor Management Kiosk Configuration

The Visitor Management Client (Classic) is designed around the concept of Receptions. The configuration relating to visits for each Reception is stored on a Reception's Division. All Receptions utilising the same configuration can be stored in the same Division to minimise the configuration required.

A Visitor Management Kiosk is represented in Configuration Client as a Workstation with the configuration for each of these Workstations determined by their default Reception.
Important: This applies even if there is no physical Reception with the Kiosks.

Visitor Divisions

Two types of Divisions are used by the Visitor Management system for visits and visitors:

- **Find Visitor Divisions** (Cardholder Division)
  This division or divisions are where permanent Cardholders who are potential visitors on a visit will be found. Normal inheritance rules apply.
- **Save Visitor Division** (Visitor Division)
  This division is where the system saves visits and newly created visitors. So that visitors in this are available for future visits this Division will either be the same or a child division of the Find Visitor Divisions.

Whilst the configuration of the Save Visitor Division and the Find Visitor Divisions have nothing to do with determining who can be a host or escort, it is likely that hosts and escorts will be stored in the Find Visitor Divisions.

These Divisions are configured on the **Visit Configuration** sub-tab (which is on the **Visitor Management** tab of the Visitor Division), as follows:

- Drag and drop the appropriate Divisions into the **Find Visitors in these Divisions** grid, so that people from these divisions can be added to visits.
- Select a Division from the **Save Visitors in this Division** drop-down list.

See ***Visit Configuration tab*** (on page 50-28) for further detail.

Configuration Process

The configuration process required in Command Centre involves a number of components listed below. Each component refers to a step-by-step procedure that is either detailed in this section, or those procedures marked with an * are located in the 'Visitor Management' section.

Some of the components are base configuration for both Named Visitor visits and Tour Group visits, while others are specific to only one of the visit types.
Notes:

- This list can be used as a checklist to ensure you have configured all the necessary components for Visitor Management Kiosk.

- To configure a Division for Visitor Management at least one Visitor Type must be specified on the **Visitor Types** tab. While multiple types can be configured for use at a Reception, only one type can be used for Named Visitors checking in at a Kiosk. Multiple types can be used for Tour Groups regardless of whether they are checking in at a Reception or Kiosk.

Base Kiosk configuration	✓	**Procedure**
Create Find Visitor and Save Visitor Divisions	☐	Creating Divisions (on page 50-8) *
Create a Reception	☐	Creating a Reception (on page 50-9) *
Set a default Reception for a Workstation, (i.e. Kiosk)	☐	Setting default Receptions for Workstations (on page 50-11) *
Create Visitor Types and Host Types. **Note:** To host a visit, (i.e. named visitor or Tour Group visit), a Cardholder must belong to a Host Type Access Group.	☐	Creating Visitor Type and Host Type Groups (on page 50-13) *
Configure text for the Welcome screen start options buttons, on the **Kiosk Configuration** tab.	☐	***Kiosk Configuration tab*** (on page 51-17)
Specify the Welcome screen background, Privacy Statement, Induction Material, Conditions of Entry and Timeouts on the **Kiosk Screens** tab.	☐	***Kiosk Screens tab*** (on page 51-20)
If you require badges to be printed at the Kiosk:		
• Configure a Visitor Badge Card Type	☐	Creating Card Types (on page 50-41) *
• Indicate this on the **Reception Actions** tab	☐	Reception Actions tab (on page 50-36) *
• Specify the Badge Layout on the **Visitor Types** tab	☐	Configuring Visitor Management setup (on page 50-15) *
Configure the columns to display on the Kiosk 'Host Actions screen', on the **Home Screen** tab.	☐	***Home Screen tab*** (on page 50-31) *
If you require notifications to be sent to Hosts when they have a visitor signed in at a Kiosk. **Note:** Notifications are subject to licence.	☐	***Configuring Notifications for Hosts*** (on page 51-35)

Specific Named Visitor Visits configuration	✓	**Procedure**
(Named Visitor visits can be created by the visit Host in the Visitor Management (VM) Client or by the visitor at the Kiosk.)		
Create a Visitor Type to be used for named visitors signing in at a Kiosk. **Note:** Many Visitor Types can be configured for a Reception (via the **Visitor Types** tab), and	☐	Configure details on the **Visitor Types** tab. See ***Configuring Visitor Management setup*** (on page 50-15) *

Specific Named Visitor Visits configuration	✓	Procedure
the Kiosk Visitor Type can be used for visitors checking in at a Reception where the VM Client is used. However, only one Visitor Type can be used for named visitors signing in at a kiosk.	☐	***Kiosk Configuration tab*** (on page 51-17)
Specify the Access Groups containing cardholders who can host visits for the Kiosk Visitor Type.	☐	Configure 'Host Type' details on the ***Host Types and Access tab*** (on page 51-33)
If access cards will be assigned to named visitors:		
• Configure the type of card to be assigned	☐	Creating Card Types (on page 50-41) *
• Indicate this on the **Reception Actions** tab	☐	Reception Actions tab (on page 50-36) *
• Configure the Access Groups available for assignment for the Kiosk Visitor Type	☐	Configure 'Visitor Access' details on the ***Host Types and Access tab*** (on page 51-33)
When visitors sign in at a Kiosk they are expected to identify themselves. PDFs can be configured for use in the search. **Note:** This configuration is also used by the Find Visitor search in the VM Client. PDF privileges can be used to hide information at the Kiosk that you want a Receptionist to see in the VM Client.	☐	Configure the PDF to be used, and whether it is mandatory for the search, on the ***Kiosk Configuration tab*** (on page 51-17)
	☐	Configure the columns to be shown in the search results on the ***Find Visitor Fields tab*** (on page 50-34) *
Create/update visitor details. **Note:** This config is shared with the visitor details displayed/captured in the VM Client. Created visitors will be stored in the Save Visitor Division, and existing visitors will be stored in either the Save Visitor Division or one of the Find Visitor Divisions (if a permanent Cardholder). Privileges can be used to control the details that are visible and editable by the visitor, allowing different rules to be applied for permanent Cardholders and adhoc visitors. Where a Cardholder is stored in a Division in which the kiosk operator does not have the privilege to edit their details any required field checks will be bypassed.	☐	Configure the fields to be displayed on the ***Visitor Fields tab*** (on page 51-31)
	☐	If an image PDF is configured on the Visitor Fields tab, instructions can be configured for the camera on the Kiosk Screens tab

Specific Named Visitor Visits configuration	✓	Procedure
If you want visitors to be able to scan a personal document, (e.g. Passport, Drivers License), to initiate a cardholder search.	☐	Configure on the ***Kiosk Screens tab*** (on page 51-20)
If you want visitors to be able to scan their business card, to simplify and speed up the data entry process.	☐	Configure the fields to be displayed on the ***Cardscan Configuration tab*** (on page 51-32)
'Your Visits screen', which shows pre-registered visits for the visitor. (See ***Visitor Management Kiosk screens*** on page 51-35 for an example of this screen.)	☐	The information shown on this screen comes from the visit and is not configurable.
There are two steps to creating a visit:		
• Identify the person (Host) the visitor is meeting with on the **Kiosk Host Fields** tab. **Note:** This configuration is also used on the 'Sign In Complete screen'. (See ***Visitor Management Kiosk screens*** on page 51-35 for an example of this screen.)	☐	Configure the host fields to be displayed on the ***Kiosk Host Fields tab*** (on page 51-30)
• Enter details of the visit.	☐	This is not configurable.

Specific Tour Group Visits configuration	✓	Procedure
(Tour Group Visits can only be created by the visit Host in the Visitor Management Client.)		
Create a Visitor Type to be used for Tour Group visits signing in at a Kiosk. **Note:** It is possible to have more than one Tour Group Visitor Type.	☐	Configure details on the Visitor Types tab. See ***Configuring Visitor Management setup*** (on page 50-15) *
	☐	Check the 'Visitor Type is for Tour Groups' checkbox on the ***Host Types and Access tab*** (on page 51-33)
Specify the Access Groups containing cardholders who can host visits for each Tour Group Visitor Type. **Note:** If you have different types of Tours, you can specify different Host Type Access Groups for the different Tour Group Visitor Types.	☐	Configure 'Host Type' details on the ***Host Types and Access tab*** (on page 51-33)
'Tour Group Visits screen' (See ***Visitor Management Kiosk screens*** (on page 51-39) for an example of this screen.)	☐	The information shown on this screen comes from the visit and is not configurable.

Specific Rapid Entry Visits configuration	✓	Procedure
Create a Visitor Type to be used for Rapid Entry visits signing in at a Kiosk.	☐	Configure details on the Visitor Types tab. See ***Configuring Visitor Management setup*** (on page 50-15) *
	☐	To use Rapid Entry, cardholders must be a member of the Rapid Visitor Type and Rapid Host Type Access Group, specified on the ***Host Types and Access tab*** (on page 51-33). Also, the Cardholder's division must be included in the **Find Visitors in these Divisions** grid on the Visit Configuration tab *

Sign In Complete

When an individual visitor or Tour Group leader has completed the sign in process at a Kiosk the following occurs:

- A badge is printed if configured.
- A notification will be sent to the Host subject to licence and configuration.
- The status of the visitor/Tour Group leader will change to 'signed in' or 'on-site' depending on configuration.
- The 'Sign In Complete screen' will display. The host details on this screen will be as configured on the **Kiosk Host Fields** tab.

Hosts

A Host will 'sign in' at the Kiosk by badging at the reader when the 'Welcome screen' is displayed. A valid Host will be a member of any of the Host Type Access Groups configured for the Kiosk Visitor Type and/or Tour Group Visitor Types as configured on the **Host Types and Access** tab.

Configuration Example

The Visitor Management Kiosk uses a single operator to act as both the visitor signing in and the host 'logging on' to perform actions.
The following example shows the recommended set up where the system is for a single Company, and the Visitor Management configuration requirement for all Kiosks is the same. At least one Reception must be configured regardless of whether physical Receptions exist or not.

Permanent Cardholders may be treated as visitors when they visit another part of the organisation. In the example below the **Cardholder Division** represents an existing Division (which may be at the top of a hierarchy of Divisions) containing Cardholders who could be visitors. Where there are Cardholders who can act as visit hosts, that are not in any of the 'Find Visitor' Divisions, privileges will be required to view Cardholders in the additional (host) Divisions.

Configuration	Privileges	Purpose
Root Division		
Cardholder Division (is the *Find Visitors Division*)		
• contains Permanent Cardholders	"View Cardholders"	Required to allow a permanent Cardholder checking in as a visitor to search for and find themselves. Also required when displaying a list of signed in/on site visitors on the Host Actions screen (if more than just the name is required). The fields to be displayed in both cases can be controlled by PDF privileges if required.
	"Manage Visitor Attributes" (renamed Assign Escort privilege)	Only required if induction material is configured.
Visitor Division (has the *Visitor Management configuration* and is the *Save Visitors Division*)		
• contains Receptions • may contain the workstations, (i.e. located in Reception)		
• contains Visits	"Edit Visits"	Required for creating/editing visits.
• contains Visitor Cardholders	"Edit Cardholders"	Required for creating/editing visitors. This privilege also covers the ability to read the card badge where cards are to be assigned and the card type of the visitor cards is stored in this Division.
	"Edit Cardholder Notes"	Only required if the visitor will be given the opportunity to enter notes for themselves.
• Visitor Type Access Groups	"Modify Access Control" (needed for creating/editing visits)	Required
• Access Groups (access assigning) - optional		
• Visitor Card Type - optional		
• Visitor Badge Card Type - optional		
• contains Doors (1 per workstation for Reception readers)	"Event and Alarms" (needed if card badging is applicable for the kiosk)	Required for reading the result of the host's card badge. Required if assigning a card by badging at the reader.

Notes:

- To allow 'visiting' permanent Cardholders to edit their details, the "Edit Cardholders" privilege must be granted in the (permanent) Cardholder Division.
- It is possible to restrict the information that could be seen/edited using PDF privileges. If the kiosk operator only has the privilege to view Cardholders in these Divisions, their details will be displayed but will not be editable.
- To allow a site to stop permanent Cardholders (on a visit) from editing their details, the kiosk will allow Cardholders in the Find Visitor Divisions to either sign in for an existing visit or to create new visits for themselves with just a view Cardholders privilege. The implication is that there may be visitor fields which have been marked as required when adding to a visit / marking on site that cannot be entered or updated. To allow for this, when the visitor signs in, the screen that presents the visitor details for checking and update will appear read only and all validation around required fields and format will be ignored. Similarly when a visitor in a read only Division is marked on site, any validation around required fields will be ignored.
- The "Manage Visitor attributes" privilege allows the Cardholder to be updated with the last time they read the induction material. This privilege will only be required if induction material has been configured and the operator does not have the "Edit Cardholders" privilege in that Division.
- If it is not possible to put the Kiosk Visitor Type Access Group and all access granting Access Groups in the Save Visitor Division, the "Modify Access Control" privilege will be required in the Divisions in which those Groups are stored AND either the "Edit Cardholders" or a view Cardholders privilege will be required in each of the Divisions containing Cardholders who may be assigned to these Groups.
- Assuming that the kiosk operator has the ability to view the details of the Cardholder badging at the 'Welcome screen', the system will be able to establish whether the Cardholder is a member of any of the Host Type Access Groups for the kiosk visitor type or Tour Group visitor types and therefore a host.

Recommended Operator Groups

For the setup described it is recommended that at least the first two Operator Groups be created:

Operator Group	Privileges / Divisions
Group 1	Visitor Attributes, and either "Edit Cardholders" or view Cardholders in Find Visitor Division. If Cardholder Notes have been configured for the kiosk

Operator Group	Privileges / Divisions
	visitor type and are to be displayed/editable via the kiosk, either the "View Cardholder Notes" or "Edit Cardholder Notes" privilege in the Find Visitor Division.
Group 2	"Edit Visits", "Edit Cardholders", "Modify Access Control", and "View Events and Alarms" in the Save Visitor Division. If Cardholder Notes have been configured for the kiosk visitor type and are to be editable via the kiosk, the "Edit Cardholder Notes" privilege in the Save Visitor Division.
Group 3	Only applicable if there are hosts in Divisions that have not been configured as Find Visitor Divisions. The privilege to view Cardholders in each of the Divisions that could contain a host.
Group 4	Only applicable if any of the access granting Access Groups is not in the Save Visitor Division. "Modify Access Control" in the Save Visitor Division.

Note: If you will be using the Visitor Management client, it is possible that a combination of the Groups created for Receptionists may be used.

See ***Configuration Examples*** (on page 50-54 in the 'Visitor Management' chapter) for suggestions where different configuration is required for different Kiosks or Receptions.

Configuring Visitor Management Kiosk

The Command Centre configuration procedures that are particular to Visitor Management Kiosk areas follows, whereas the procedures relating to Visitor Management Client can be found in the 'Visitor Management' section.

- Setting default Receptions for Workstations (on page 50-11) *
- ***Configuring Visitor Management for the Kiosk*** (on page 51-16) (on the Kiosk workstation's default Reception Division)
- ***Configuring Notifications for Hosts*** (on page 51-35)
  Note: This step is only necessary if your site is licensed for Notifications, and you want Hosts to be automatically notified of their visitor's arrival.

Recommendations for Kiosk configuration

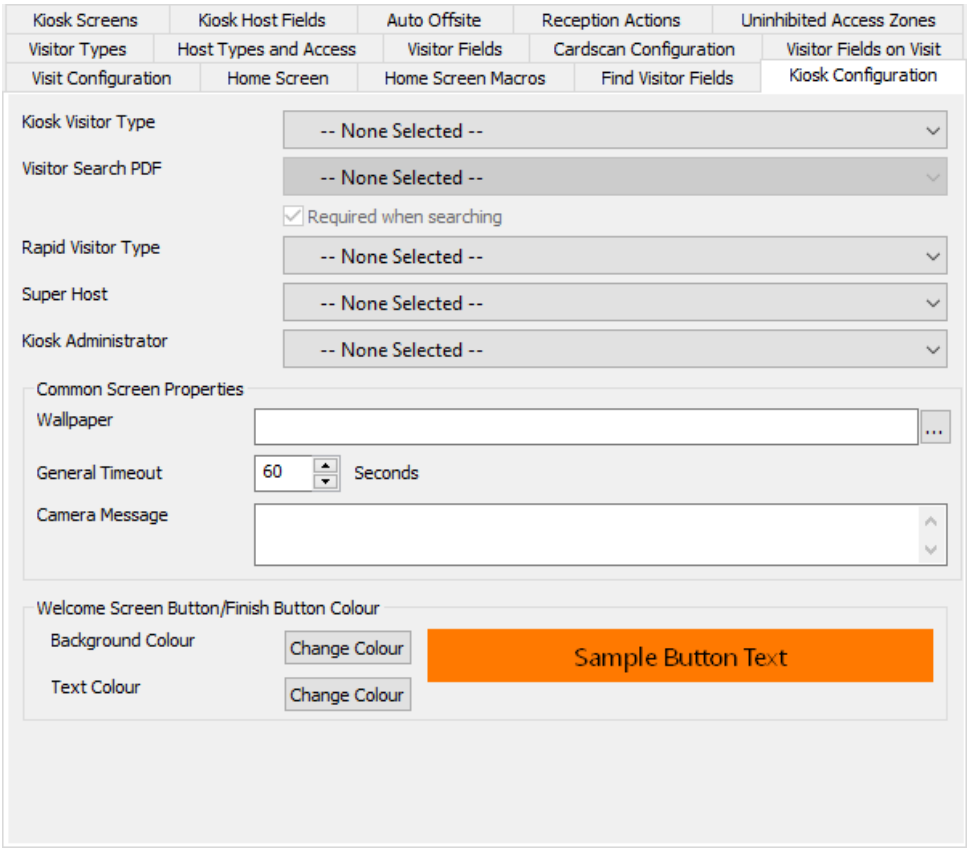
We recommend you configure the following for Visitor Management Kiosk:

- Due to visual space restrictions in the Kiosk, when Personal Data Fields (PDFs) are being used we recommend the length of PDF names do not exceed 20 characters. How well these names display on the Kiosk depends on the screen resolution used.
- If Regular Expressions are used for text and contact type PDFs, (i.e. Address, Phone, Mobile and Email) a **Description** for the data format is recommended.
- If text-list type PDFs are used for the Kiosk, they must be restricted to the text-list, (i.e. "Restrict to List" must be checked on the **Type** tab of the PDF properties).
- The PC used to run the Kiosk should have the following Windows settings (via Control Panel):
  - the **Region and Language** format set to "English (New Zealand)", which sets the time to 12 hour time and displays the date correctly, and
  - the **Personalization** Basic and High Contrast Theme Settings should remain on Windows 7 Basic. Changing the theme to 'Windows Classic' or one of the 'High Contrast' options, will slightly change the Kiosk appearance and may make the visitor entered data difficult to read.

Configuring Visitor Management for the Kiosk

1. Click **Configure** from the menu bar, then **Divisions**.
   The **Division** List Window opens.
2. Open the "Visitor Division", (i.e. the Visitor Management Configuration Division), and click the **Visitor Management** tab.
   The **Visitor Types** sub-tab displays by default.
3. Select the Visitor Type Access Groups intended to be used for the Kiosk.
4. Click the appropriate sub-tab(s) required to configure the division, and complete the setting information (refer to the Configuration Process checklist in ***Visitor Management Kiosk Configuration*** on page 51-7):
   - ***Kiosk Configuration tab*** (on page 51-17)
   - ***Kiosk Screens tab*** (on page 51-20)
   - ***Kiosk Host Fields tab*** (on page 51-30)
   - ***Visitor Fields tab*** (on page 51-31)
   - ***Cardscan Configuration tab*** (on page 51-32)
   - ***Host Types and Access tab*** (on page 51-33)

Kiosk Configuration tab



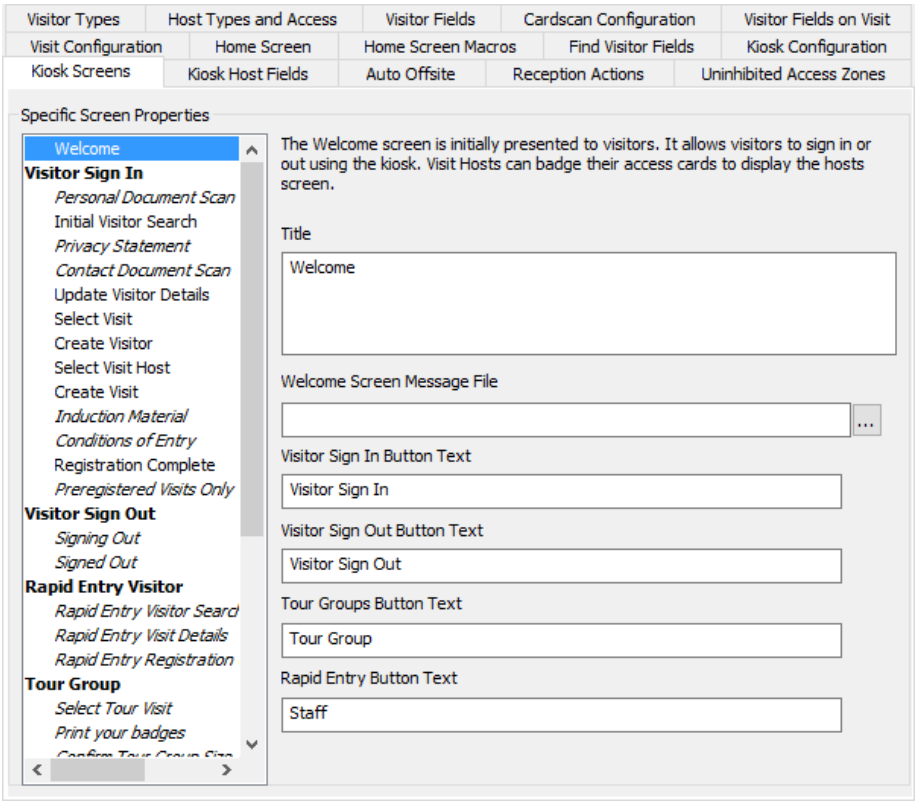
This tab supports some of the additional configuration required for the Kiosk. Configure as appropriate:

Field / Checkbox	Description
Kiosk Visitor Type	This is the Visitor Type to be used when creating visits via the kiosk, and to determine which visits created in the VM client will display at the Kiosk. Selecting a Kiosk Visitor Type enables the **Visitor Search PDF** field. **Notes:** • Changing the **Kiosk Visitor Type** to a different Visitor Type or back to --None Selected-- will set the **Visitor Search PDF** field back to --None Selected--. • If the Visitor Type specified here is removed as a Visitor Type for the Division, this field will be set back to -- None Selected --.
Visitor Search PDF	The list is populated with all non-image PDFs belonging to the 'Kiosk Visitor Type' Access Group that the user has the privilege to see.

Field / Checkbox	Description
	Notes: • The **Visitor Search PDF** should also be configured as a **Visitor Field** for the Kiosk Visitor Type to allow the visitor to capture this PDF data. • If the option selected in the **Kiosk Visitor Type** field is changed, the **Visitor Search PDF** value is set back to --None Selected--. • If the search PDF is removed from the 'Kiosk Visitor Type' Access Group, this field returns to the default of --None Selected--. The **Required when searching** checkbox applies to the Visitor Search PDF. Check this if you require the visitor to enter something in the Visitor Search PDF before a search is run.
Rapid Visitor Type	This is the Visitor Type to be used for visitors that have the ability to host themselves, (i.e. be unescorted visitors). It allows internal employees who are visiting a site to use their access credential to enable quick entry to the site. The list is populated with all visitor types configured for the division. **Note:** Neither the Kiosk Visitor Type or the Tour Group Visitor Type can be used as the Rapid Visitor Type.
Super Host	Super Hosts can see and manage all visitors/Tour Groups at the kiosk (depends on the host also belonging to the relevant Host Access Groups for either single visitor and/or Tour Group visits).
Kiosk Administrator	The Kiosk Administrator is able to access the Tools to perform Kiosk Admin functions, (i.e. Amend/select the printer details, log off Kiosk and configure card scan).
Wallpaper	This is the file location for a logo and splash screen content to be displayed on the background of each screen.
General Timeout	The period of time you indicate in the Time Box will be the length of time the Kiosk has been inactive, before showing the inactivity timeout and returning to the Welcome screen.

Field / Checkbox	Description
Camera Message	If you intend capturing visitor images at the Kiosk, instructions can be configured for the camera here, (e.g. where the camera is positioned).
Welcome Screen Button/Finish Button Colour	This section allows you to change both the **Background** and **Text Colour** of the Kiosk Start and Finish buttons. By clicking the **Change Colour** button for either the Background or Text, the standard colour swatch displays allowing you to select a different colour. The Example image to the right of this section previews how the buttons will appear at the kiosk.

Kiosk Screens tab



This tab supports more additional configuration options for screen presentation and content within the Visitor Management Kiosk.

The Screen navigation list (on the left) displays all available screens that can be displayed on the kiosk, in order of appearance.
Clicking on an item in the list reveals the properties associated for you to configure, as follows:

Notes:

- The default text in the **Title** field for each screen can be changed.
- The **Display This Screen** checkbox is available for some of the screens, giving sites the option whether or not a screen will display at the kiosk.
- All the fields with a browse button allow you to either type in the name of the file containing the information to be displayed or to browse for the file. When browsing for a file, the default file type is Rich Text Files, (i.e. .rtf), but includes Image Files, (i.e. .png, .bmp, .jpg, .jpeg, .jpe, .jfif, .tif, .tiff and .gif), Video Files, (i.e. .wmv, .mp4 and .api), and All Files. The files need to be stored in a location accessible to the kiosk. It is recommended that once files are configured, the kiosk is checked to ensure the material is presented as intended. With the number of possible file types available, there can be variations in the appearance. For example, when using **.rtf** files, careful consideration should be given to the use of font colours against a black background. The colour automatically applied will appear white, where as black will not change and will not be visible.

Standard Visits

Screen	Description
Welcome	You can configure the text on the start option buttons that appear on the Welcome screen at the Kiosk. By default they are labelled Visitor Sign In, Visitor Sign Out, Tour Group and Staff. **Notes:** • These fields are each limited to 60 characters. • A 'Tour Groups' button will only appear on the Welcome screen if Tour Groups are configured, and a 'Rapid Entry' button will only appear if a **Rapid Visitor Type** is configured (on the **Kiosk Configuration** tab).
Personal Document Scan	If configured to display, this screen allows visitors to scan a personal document to initiate a cardholder search. The types of personal documents that appear on the screen is determined by which Data Maps are selected during configuration. **Note:** If the Kiosk cannot detect a scanner and associated SDK when this is configured to display, a failure message will display on the 'Initialisation screen' and the operator will not be able to logon to the Kiosk.
Initial Visitor Search	Additional sign in instructions can be added to the initial search screen. For example, if there is a card scan device installed and configured for the kiosk, you could enter *"To sign in either insert your business card in the scanner or enter your details below"*.
Privacy Statement	If configured to display, this screen provides visitors with a disclaimer regarding the privacy of visitor information.
Contact Document Scan	If configured to display, this screen allows visitors to scan a secondary document containing further information about them. The types of personal documents that appear on the screen is determined by which Data Maps are selected during configured. **Note:** If the Kiosk cannot detect a scanner and associated SDK when this is configured to display, a failure message will display on the 'Initialisation screen' and the operator will not be able to logon to the Kiosk.
Update Visitor Details	If configured to display, this screen allows visitors to update their details.
Select Visit	A visitor can either select a pre-registered visit or create a new visit on this screen.
Create Visitor	New visitors can enter their details on this screen.

Screen	Description
Select Visit Host	Visitors can search for and select the host they intend visiting on this screen.
Create Visit	This screen allows visitors to enter their visit start and end times, and reason for visiting. The configuration options for this screen allow the operator to set the Kiosk to: • Display this screen • Allow visits to be created without seeing this screen, using default values. • Restrict the visits to pre-registered visits only.
Induction Material	If required, this screen can be configured to display information that visitors must read before their visit can proceed. See ***Configuring Induction Material*** (on page 51-24) for further detail.
Conditions of Entry	If configured to display, this screen can provide visitors with useful information relating to local site conditions, (e.g. safety rules).
Registration Complete	This screen indicates that sign-in is complete. A **Completion Message** can be entered if required, and the **Completion Timeout** is the period of time before the kiosk returns to the Welcome screen after visitor sign-in is complete.
Preregistered Visits Only	This screen displays when visitors have no preregistered visits and the Create Visit screen is configured to not display.
Signing Out	If configured to display, this screen allows visitors to identify themselves and mark themselves off-site.
Signed Out	This screen, which only displays if the Signing Out screen is configured to display, indicates to visitors that they have completed the Sign Out process.

Rapid Entry Process

The following screens are displayed to visitors that are configured as Rapid Visitor Type on the **Kiosk Configuration** tab.

Screen	Description
Rapid Entry Visitor Search	This screen allows visitors to badge their access card to identify themselves. If configured to display, by checking the **Enable Rapid Entry Process** checkbox, the **Allow self hosting visitors to skip entering visit details** checkbox is also enabled. If this is checked, the Rapid Entry Visit Details screen will be skipped for self hosting visitors (only).

Screen	Description
Rapid Entry Visit Details	This screen, which only displays if the Rapid Entry Visitor Search screen is configured to display, allows rapid entry visitors to enter visit details. It will be skipped for self hosting visitors (only) if the **Allow self hosting visitors to skip entering visit details** checkbox was checked on the Rapid Entry Visitor Search screen.
Rapid Entry Registration Complete	This screen, which only displays if the Rapid Entry Visitor Search screen is configured to display, indicates to rapid entry visitors that they have completed the registration process.

Tour Groups

Screen	Description
Select Tour Visit	If configured to display, this screen allows a tour group leader (visitor) to select a pre-registered tour group visit and sign in their tour group.
Print your badges	This screen, which only displays if the Select Tour Visit screen is configured to display, allows the tour group leader to print badges for all members of the tour group.
Confirm Tour Group Size	This screen, which only displays if Tour Groups are configured to be marked on-site and "Print Your Badges" is not enabled, allows a tour group leader to specify the number of members in a tour group.

Host Screens

The following screens are displayed to operators that are part of Host Access Groups, displaying only visits that are specific to them. An all visits view is available to a Super Host, as configured on the **Kiosk Configuration** tab.

Screen	Description
Display Visitors	This screen displays the visitors for a host and allows access to other host action screens.
Display Tour Groups	This screen displays the tour groups for a visit host, allowing the host to mark the tour group on or offsite.
Mark Tour Group Offsite	This screen allows a host to mark a Tour Group offsite.
Mark Tour Group Onsite	This screen allows a host to mark a Tour Group onsite.
Change Visit Host	This screen allows a visit host to change the host for a visit to themselves or some other host.

Screen	Description
Host Assign Card	This screen allows a visit host to assign an access card to a visitor.
Update Visit Details	This screen allows a visit host to update the details of a visit.
Print Your Badges	This screen allows a visit host to reprint tour group visitor badges.
Administrator Tools	This screen is displayed to operators that are part of a Host Access Group that is selected as the Kiosk Administrator on the Kiosk Configuration tab. It provides Kiosk Administrators with access to various administrative functions.
Barcode Scanners	This screen allows a Kiosk Administrator to view the available barcode scanners.
Printer Setup	This screen allows a Kiosk Administrator to configure the printer used to print visitor badges.

Configuring Induction Material

The "Induction Material" screen properties option on the **Kiosk Screens** tab allows you to configure induction material, if required. The two types of induction material are:
- Simple, (i.e. showing a rich text, image or video file only), or
- Advanced, (i.e. rich text, image or videos and questions), if you want to test visitors knowledge after viewing the induction material.

Note: All Induction material should be checked on a configured kiosk prior to implementation.

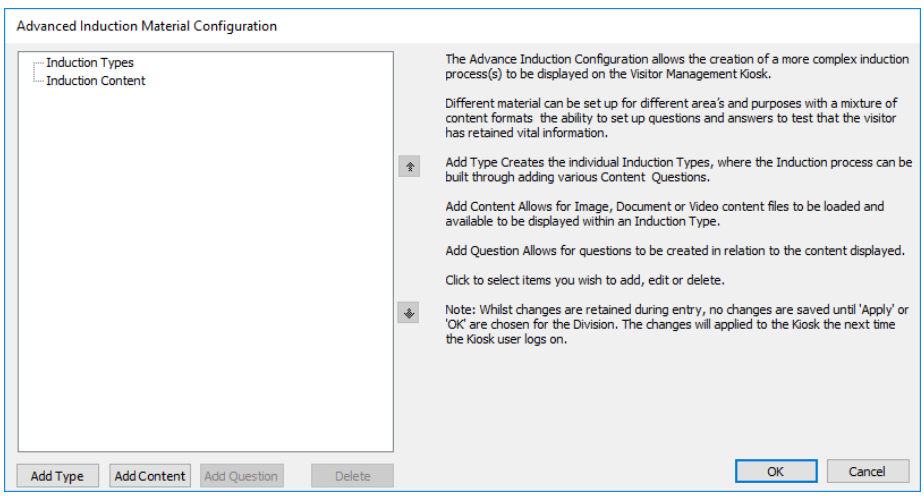
1. Do you want induction material to appear as part of the screens on a Kiosk?

If...	then...
yes	check the **Display This Screen** checkbox and go to Step 2. **Note:** The **Use this Division's Configuration** radio button must be selected at the top of this screen for you to be able to configure videos and questions for induction material.
no	ensure the **Display This Screen** checkbox is unchecked. All the Induction Material fields are disabled.

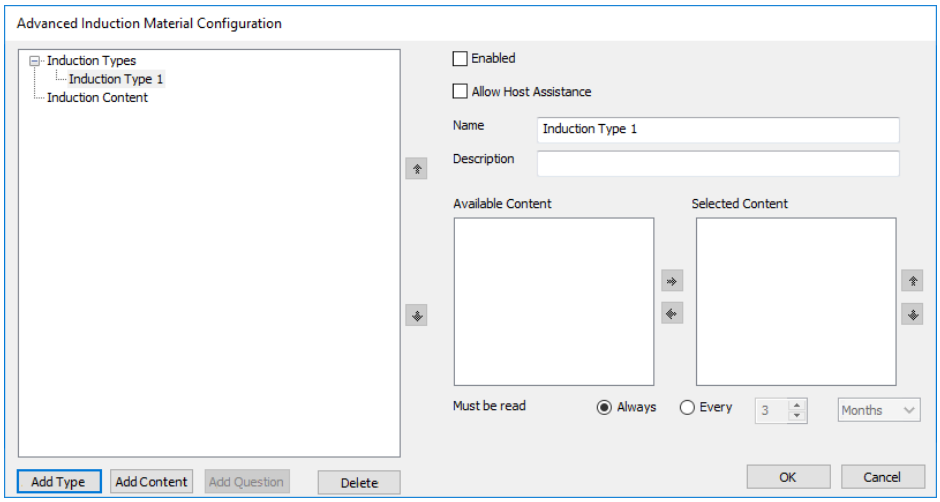
2. Do you want only a rich text, image or video file to appear on the Induction screen, or any of these file types as well as questions?

If...	then...
rich text, image or video file only,	**a)** Click the **Simple Induction Material File** radio button. The **Must be read** options, and the empty file location field are enabled. **b)** Either type in the name of the file containing the information to be displayed, or browse for the file by clicking the ... button. **Note:** When browsing for a file, the default file type will be **.rtf** but the content of image files, (i.e. .png, .bmp, .jpg, .jpeg, .jpe, .jfif, .tif, .tiff, .gif, plus video files .wmv, .mp4 and .avi) can also be displayed. **c)** Click the appropriate radio button for how often the induction material must be read, (i.e. either **Always** or **Every**). If the **Every** radio button is selected, the frequency can be specified in days, weeks or months. (Default = 3 Months) **d)** In the **Induction Timeout** field, enter the required time (in seconds) that you want for the Kiosk to return to the Welcome screen after a period of inactivity. **Note:** The timeout will be stalled until the video is finished playing or the video is paused. Procedure is complete.
rich text, image or video file and questions,	go to Step 3.

3. Click the **Advanced** radio button.
   The **Maintain Advanced Induction Material** button is enabled.
4. Click the **Maintain Advanced Induction Material** button.
   The **Advanced Induction Material Configuration** dialog displays.



5. Click the **Add Type** button.
   This option allows you to create a process path for visitors to step through, (i.e. determine the order in which videos are displayed and when questions are to be answered if there are a number) on the Kiosk Induction screen.



6. Check the **Enabled** checkbox, and enter a name for the Induction Type in the **Type Name** field.
   Notes:

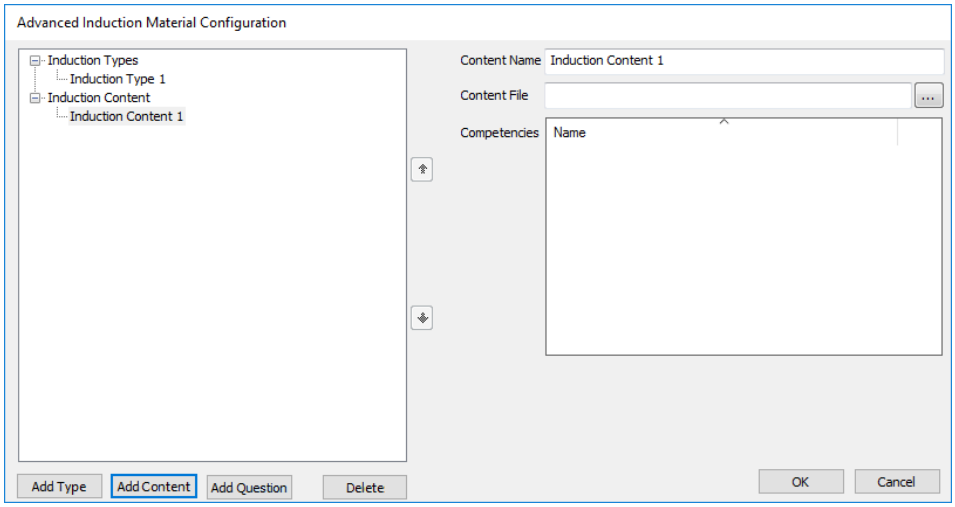
   - When an Induction Type is first created, the **Type Name** defaults to the item type name, plus a number on the end to ensure that there are no duplicate names, (e.g. Induction Type 1). The number increments by one if an item of that type already exists with that number on the end.
   - If there is only one Induction Type, it will go straight to the Kiosk Induction screen. However, if there are multiple Types, the **Type Name** will appear on button(s) displayed on the Kiosk Induction screen. For this reason, the **Type Name** field is limited to 20 characters, to ensure the button text remains within its fixed size.

7. If you want explanation text to be presented next to the button on the Kiosk (to give the visitor more information about what Induction Type to choose), enter a suitable explanation in the **Description** field.

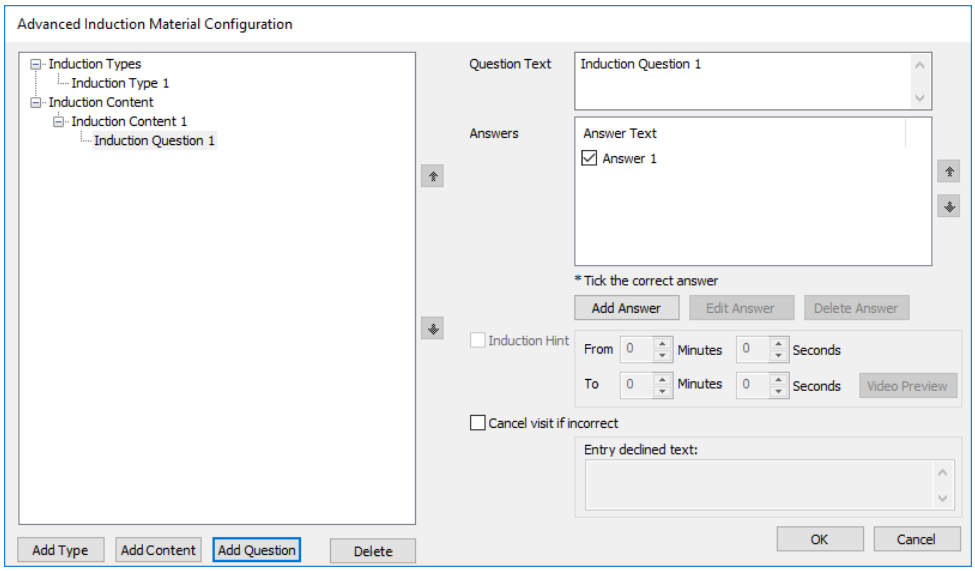
8. The rich text, image and/or video files that populate the 'Available Content' grid is determined by what is stored using the **Add Content** option.
   Move any of the files you require from the 'Available Content' grid to the 'Selected Content' grid by selecting the file and clicking the  button.

9. Once you have all the rich text, image and/or video files you require in the 'Selected Content' grid, you can re-order them if required by using the **up** and **down** arrow buttons to the right of the 'Selected Content' grid.
   Note: The order you sort these files here will be the order they appear on the Kiosk Induction screen.

10. Click the appropriate radio button for how often the induction material must be read, (i.e. either **Always** or **Every**).
    If the **Every** radio button is selected, the frequency can be specified in days, weeks or months. (Default = 3 Months)
11. Click the **Add Content** button.
    This option allows you to load and select rich text, image and/or video file(s) to display on the Kiosk Induction screen.



12. Enter a name for the rich text, image or video file in the **Content Name** field.
    Note: When an Induction file is first added, the **Content Name** defaults to the item type name, plus a number on the end to ensure that there are no duplicate names, (e.g. Induction Content 1). The number increments by one if an item of the type already exists with that number on the end.
13. In the **Content File** field, either type in the name of the rich text, image or video file to be displayed, or browse for the file by clicking the ... button.
14. From the **Competency** List Window, drag and drop any required competencies into the **Competencies** grid.
    These competencies will be applied to a person after they have viewed the Induction material, and the expiry for the competency will be based on the 'Must be read' setting.
15. Click the **Add Question** button.
    This option allows you to configure and display induction questions (and/or sets of questions).



16. Enter the question in the **Question Text** field.
17. Click on "Answer 1", which by default populates the **Answers** grid.
    The **Edit Answer** button is enabled.
18. Click the **Edit Answer** button, and type what the answer should be.
19. Click the **Add Answer** button.
    A new entry appears in the **Answers** grid.
20. Type what the answer should be for the new entry.
21. Repeat Steps 20 - 21 for each answer you require.
    Notes:
    - You can re-order the answers if required by using the **up** and **down** arrow buttons to the right of the **Answers** grid.
    - It is recommended that answers are reasonably concise to fit on the screen (taking into consideration the screen orientation, i.e. landscape or portrait).
      All Induction material should be checked on a configured kiosk prior to implementation.
22. Tick the checkbox beside the correct answer.
23. A segment of the video footage can be configured to play if a visitor answers the question incorrectly, providing a clue to what the correct answer is.
    Do you want a segment of the video to play if a visitor answers incorrectly?

If...	then...
no	go to Step 24.
yes	**a)** Check the **Induction Hint** checkbox. The **Video Preview** button becomes enabled. **b)** Click the **Video Preview** button. An **Induction Hint** screen displays.

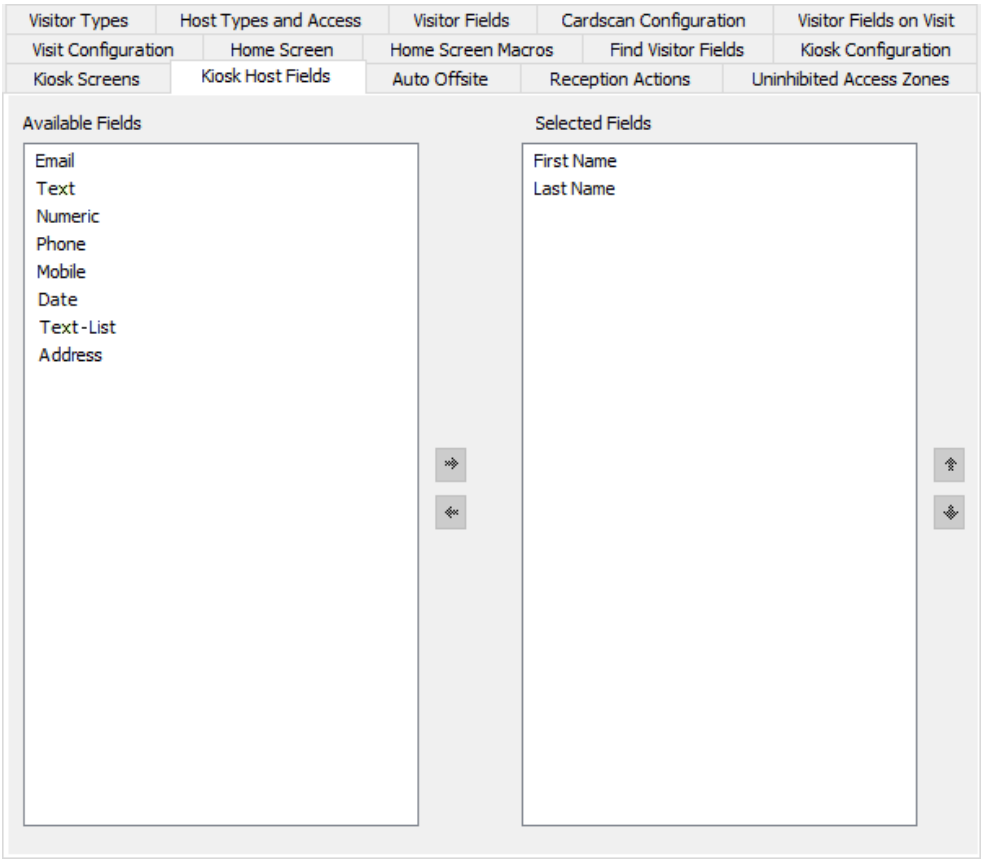
If...	then...
	c) Enter the **From** and **To** time (minutes/seconds) of the part of the video you want to play as a clue. **d)** Click the **Play Hint** button. The segment of the video plays. Alter the **From** and/or **To** times if required to get the exact segment of the video to play, by repeating Steps c. and d. **e)** Click the **OK** button. The **Induction Hint** screen closes and the **From** and **To** times appear on the **Advanced Induction Material Configuration** dialog. A visitor at a kiosk will now be able to view the relevant video segment as a clue if they answer the question incorrectly. Once the segment plays the visitor will be returned to the question for another attempt.

24. Do you want the visit to be cancelled if a visitor answers incorrectly?

If...	then...
no	go to Step 25.
yes	**a)** Check the **Cancel visit if incorrect** checkbox. This disables the **Induction Hint** checkbox. **b)** Enter the message you want visitors to be presented with in the **Entry declined text** field. This message will display at a kiosk when a visitor answers a question incorrectly, before the system cancels the visit.

25. Click the **OK** button.
    The **Advanced Induction Material Configuration** dialog closes.
26. In the **Induction Timeout** field, enter the required time (in seconds) that you want for the Kiosk to return to the Welcome screen after a period of inactivity.
    Note: The timeout will be stalled until the video is finished playing or the video is paused.

Kiosk Host Fields tab



This tab is used to define the Host fields that will be used when a visitor searches for a host (on the 'Who are you meeting with? screen' of the Kiosk), and will appear on the 'You are signed in screen' of the Kiosk.

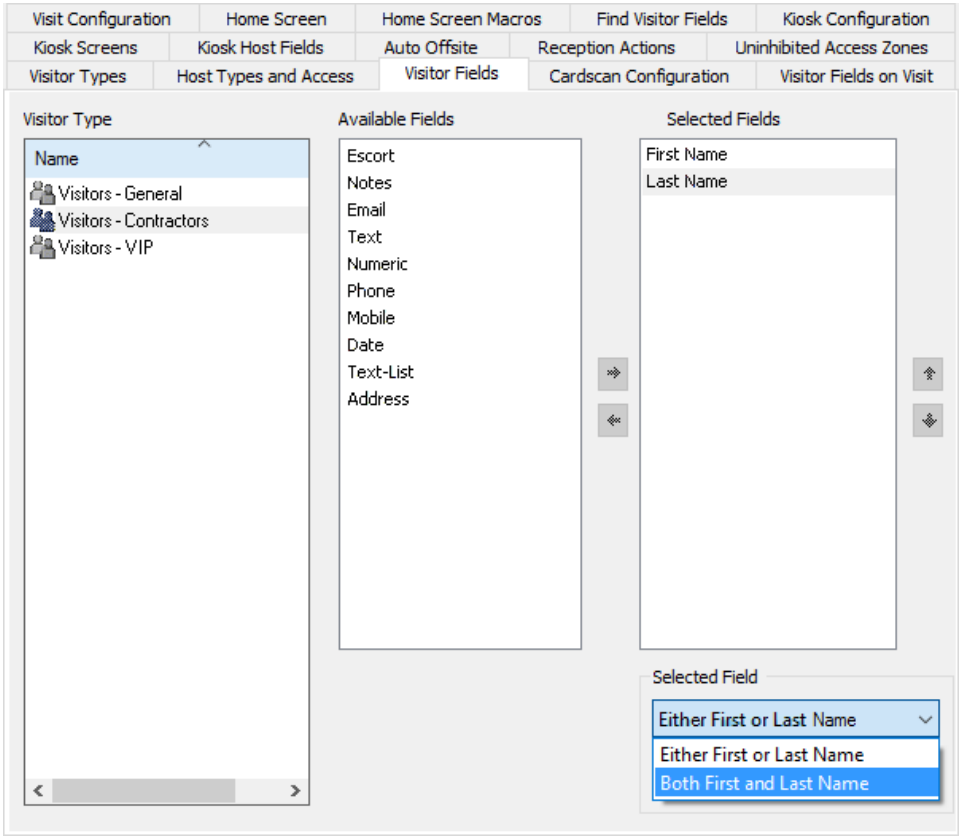
Note: There is no limit to the number of items you can select.

1. Move any of the fields you require from the 'Available Fields' grid to the 'Selected Fields' grid by selecting the PDF and clicking the button.
   Notes:
   - Host fields that display contact information are recommended, (e.g. email, phone number, mobile), as well as departmental information so that a visitor can verify the correct Host.
   - The 'Available Fields' grid displays all non-image PDFs that the operator is privileged to view.
   - First and Last Name are configured by default and cannot be removed.
2. Once you have all the PDFs you require in the 'Selected Fields' grid, you can re-order them if required by using the **up** and **down** arrow buttons to the right of the 'Selected Fields' grid.

Visitor Fields tab

This tab is used to define the visitor fields that appear on the 'Your Details screen' of the Kiosk, which is used for capturing/updating visitor details when they sign in

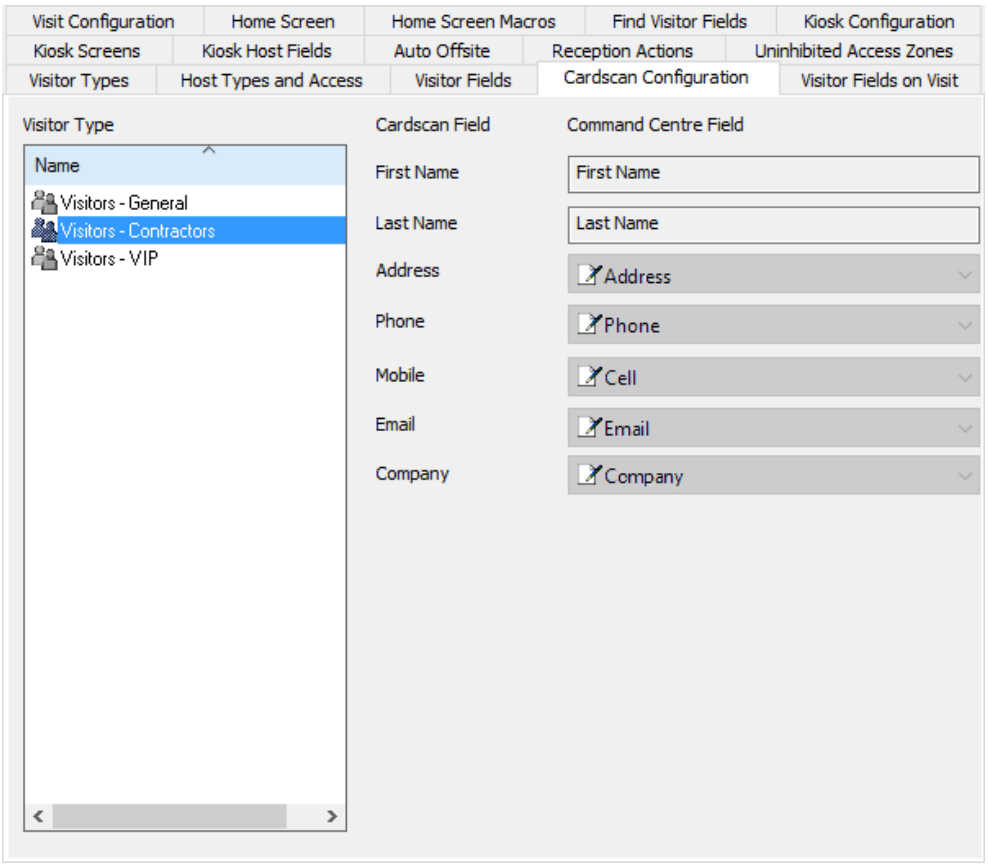
1. In the Kiosk both First and Last Names are mandatory for visitor searches. Therefore, once you have selected the Visitor Type, click on either **First Name** or **Last Name** in the 'Selected Fields' grid, and select 'Both First and Last Name' from the drop-down list in the **Selected Field** section.



Note: The 'Escort' and 'Notes' fields can be selected and used for the Visitor Management client, however they will be ignored at the Kiosk.

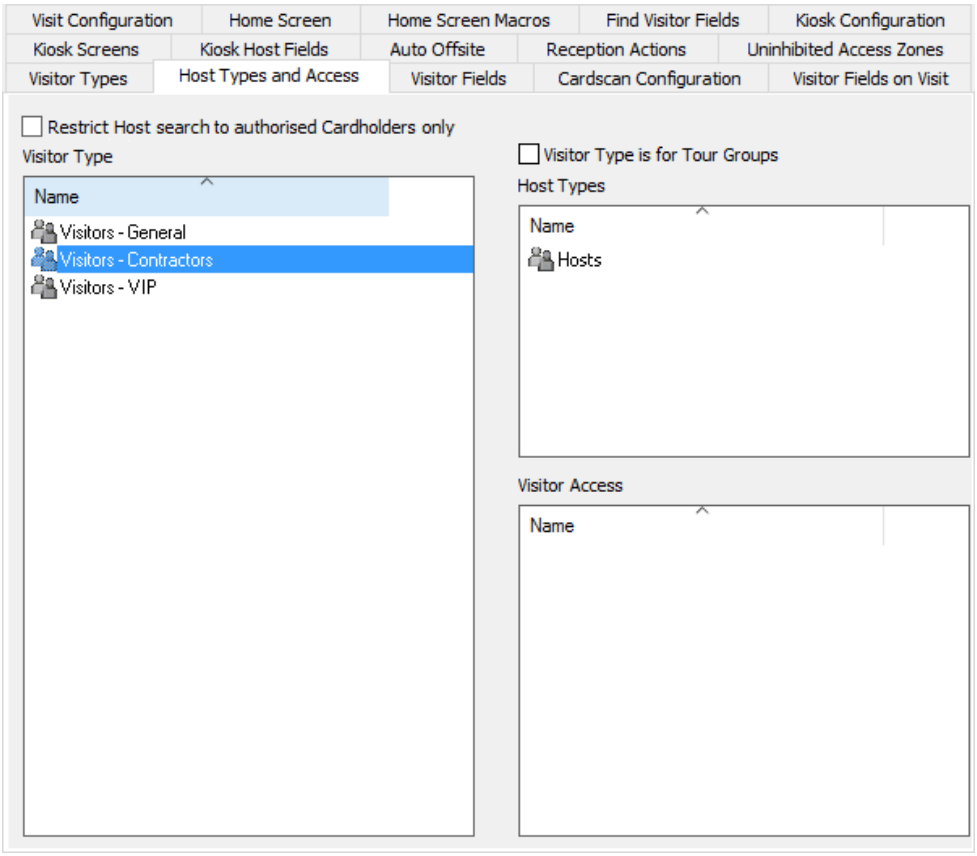
Cardscan Configuration tab

Configure the fields on this tab if you have a Business Card scanner attached to the kiosk for the purpose of allowing visitors to scan their business cards.



1. Select the Kiosk Visitor Type that you want to configure Business Card scan capability for.
   The Cardscan configuration for that Visitor Type displays.
2. Select the required PDFs from the drop-down lists as appropriate.

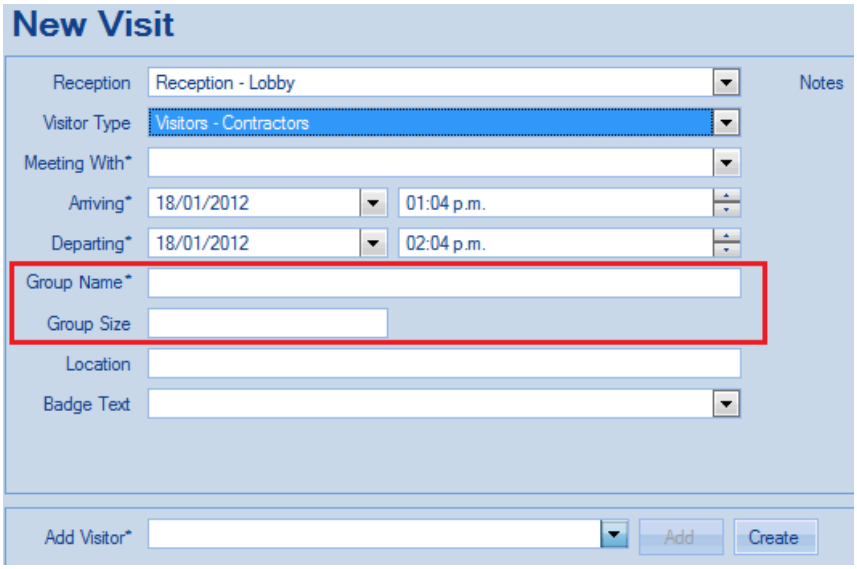
Host Types and Access tab



1. Select the **Restrict Host search to authorised Cardholders only** checkbox to only allow authorised Host Cardholders to be viewed and selected in the Visitor Management Client. This restricts the 'Meeting With' field (when creating a visit) and the 'Find Host' search (on the 'Home' screen). **Note:** 'Authorised' Cardholders are those with the **Cardholder Authorised** checkbox checked on the **Cards** tab in their properties.
2. Select the Kiosk Visitor Type that you want to assign a Host Type to.
3. Select the required Host Type Access Group (from the **Access Group** List Window), and drag and drop it into the **Host Types** grid.

If access cards are to be assigned to named visitors, the Access Groups available for assignment must be configured for the Kiosk Visitor Type. Select and drag and drop any required Access Groups into the **Visitor Access** grid.

1. If your site intends to use this Visitor Type for Tour Groups visit, check the **Visitor Type is for Tour Groups** checkbox.
   This results in a **Group Name** field (which is mandatory) and a **Group Size** field appearing on the Visit screen in the Visitor Management application. The number of people in a Tour Group may not be known until they physically come on-site, therefore it is not necessary to populate this field. However, the Host must confirm/record at the start of the visit how many people will be going on-site as part of the Tour Group. This then filters through to the Visitor Management application and populates the **Group Size** field.



   The name of the Tour Group leader or primary contact from the group needs to be entered in the **Add Visitor** field on the Visit screen.

2. Click the **OK** button.

Configuring Notifications for Hosts

Notifications (via email and/or SMS) can be configured to be sent to Hosts (cardholders) when they have a visitor who has signed in and is ready to be collected from a Visitor Management Kiosk.
This procedure allows you to configure the system so that the "Message for Host" field will appear during registration on the Kiosk.

1. Ensure your site is licensed for Notifications, i.e. your site licence file **CommandCentre.lic** contains the option:
   ```
   [Features]
   Notifications=1
   ```
2. Configure the **Outgoing Email** and/or **Mobile/SMS Notifications** tabs of the Server Properties to facilitate the sending of email and/or SMS text messages to Hosts (cardholders).
   For detailed instructions refer to ***Outgoing Email*** (on page 6-50) and/or ***Mobile/SMS Notifications*** (on page 6-54).
3. Configure an appropriate email and/or SMS PDF, with the Notifications options selected, for the Host (cardholder).
   For detailed instructions refer to ***Setting Cardholder "Email" and "Mobile" PDFs*** (on page 35-8).

Visitor Management Kiosk Document Scanning Process

Introduction

The Gallagher Visitor Management Kiosk supports an interface to a number of scanners allowing visitors to scan a form of ID, (e.g. Passport, Driver's License, Business Card) during the "sign in" process at a self-service Kiosk. The aim is to reduce the amount of manual data entry required and improve Visitor processing time.

The scanners that the Visitor Management Kiosk interface with are:

- ScanShell 800NR Business Card Scanner,
- SnapShell Passport Scanner,
- Gemalto QS1000 Passport Scanner, and
- Acuant i-Dentify ID-150 Card Scanner.

Notes:

- The SnapShell Passport Scanner and ScanShell 800NR support Microsoft Windows 8 and 10 (32 & 64 bits).
- SnapShell Passport Scanners cannot be used for the Visitor Management Kiosk and the Visitor Management Client at the same time.
- The SnapShell Passport Scanner is End of Life, and no longer available for purchase.

Prerequisites

Unless you are using the ScanShell 800NR which is a business card scanner only, Visitor Management Kiosk Scanning requires the following Interface (**Accuant OCR Scanner Interface - C12716**) and Licence file entry - (**Visitor Management ID Scanning=1**) to enable the capture of:

- Passports, Drivers Licenses and National Identity Cards, and
- information from visitors at the Visitor Management workstation, when integrated with Command Centre.

Procedure

To configure and use this feature, perform the following procedures in the order specified.

Creating Data Maps

The scanning software must be configured to automatically populate the Visitor fields (within Visitor Management Kiosk) when a visitor scans a document at a Visitor Management Kiosk.

1. Create a set of Data Maps, one for each document type, (e.g. Passport, Driver's License, Business Card), in Command Centre Client. See "Creating a Data Map" for the procedure in the Command Centre Client Help.

Adding Data Maps to the Visitor Details screen

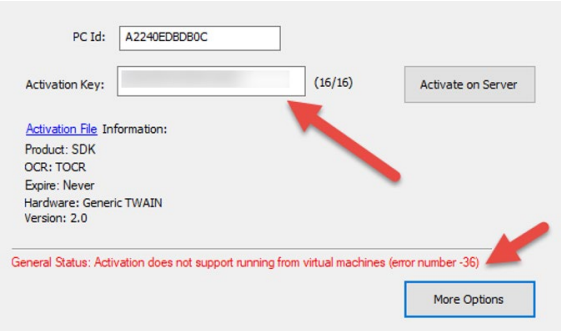
2. Add the Data Maps (configured in Step 1) to the Selected Data Maps grid on the **Kiosk Screens** tab of the Visitor Management Kiosk Division

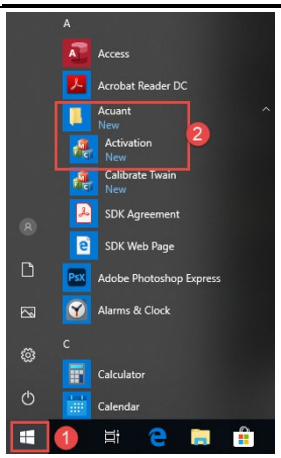
Configuration, in Configuration Client.
See ***Kiosk Screens tab*** (on page 51-20) for the procedure.
Note: The order of the Data Maps listed in the Selected Data Maps grid will match the order of the personal identification type buttons shown on the 'Visitor Details screen' in Visitor Management Kiosk.

Installing the Scanner

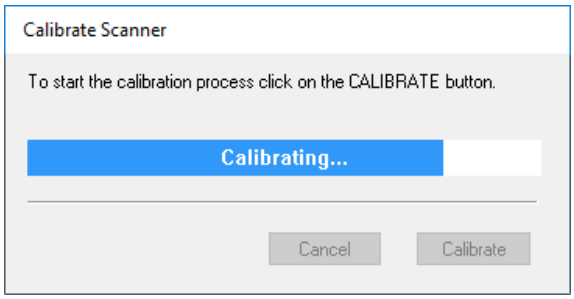
Installing a document scanner installs the necessary SDK and drivers for the specific scanner. Log on as an Administrator, and install for each client as follows:

3. Ensure the Scanner is not connected to the PC.
4. Run the **OPOS_CCOs_1.14.001.msi** installer located in the **`'Utilities\Visitor Management Drivers'`** folder of the Command Centre installation files.
5. Install the Card Scan Drivers (**DPInst.exe**) located in the **`'Utilities\Visitor Management Drivers\ Card Scan Drivers\Drivers'`** folder.
6. From the **`'Utilities\Visitor Management Drivers\ ScannerDrivers'`** folder, run the relevant silent install patch file for the type of scanner you are installing.
   Note: The patch files install all the drivers for the scanner from the **SDK_setup_is.exe** file automatically.

Scanner type	Install patch file…
ScanShell 800 NR,	InstallerFor800NRScanner.bat
SnapShell,	InstallerForSnapShellScanner.bat
Gemalto QS1000,	InstallerForGemaltoScanner.bat **Note:** The QS1000 scanner is the only one that the following ActivatedSDK window displays after the **SDK_setup_is.exe** finishes installing.  Type in the **Activation Key** and click the **Activate on Server** button to activate the key. The QS1000 scanner will not work without this activation key. **IMPORTANT:** Gallagher do not provide this activation key for users. Contact Acuant company for this key. The Activation Application can be found from **Start** > **Acuant** > **Activation**.

Scanner type	Install patch file...
	
Acuant i-Dentify ID-150,	InstallerForID150Scanner.bat

7. Restart the PC.
8. Make sure all the drivers have installed correctly by checking the Windows **Programs and Features** list.
9. Plug the scanner into the PC.
10. Manually start the Visitor Management Client.
11. Go to the Visitor window and click the **Scan** button.
    Note: You require the "Edit Visits" operator privilege to scan.
12. Place the calibration sheet provided with the scanner into the scanner.
    A Calibrate Scanner screen displays.
13. Click the **Calibrate** button.
    Calibration starts.



When the progress bar reaches 100% calibration is complete, and a pop-up message *"Calibration done successfully"* displays.

Note: The scanner needs to be calibrated before being used for the first time, and may need recalibrating if unplugged.

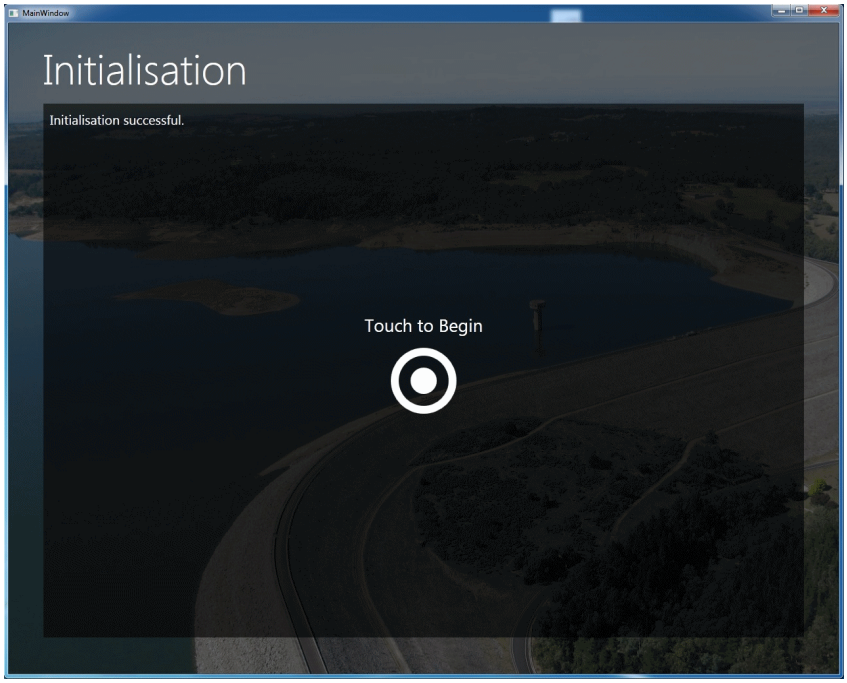
Scanning documents at a self-service Visitor Management Kiosk

14. A visitor clicks the **Visitor Sign In** button at a Visitor Management Kiosk, is presented with a 'Scan Personal Document screen', and scans a document (form of identification).
    Any fields that are mapped to Data Maps are populated with the scan data.
    See ***Visitor Management Kiosk screens*** (on page 51-39) for examples of the screens and the screen flow.

Visitor Management Kiosk screens

The screens that appear on a self-service Visitor Management Kiosk, and the order they appear in, are as follows:

Initialisation screen



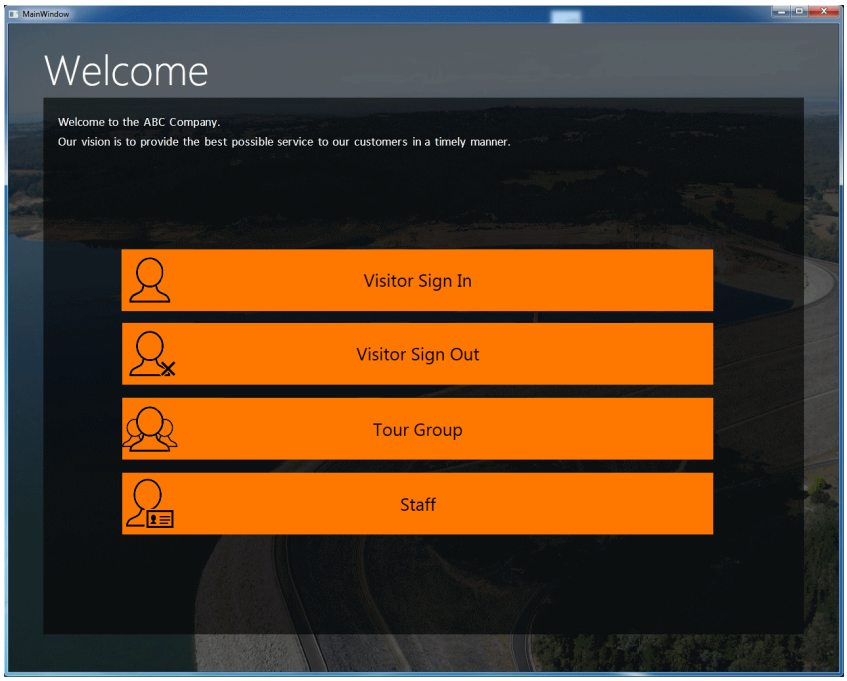
When the Visitor Kiosk application is launched either the 'Logon screen' displays or logon occurs automatically if the Kiosk's Windows user account is configured for Active Directory single sign-on within Command Centre.

Note: If either 'Personal Document Scan' or 'Contact Document Scan' option are enabled, the Visitor Kiosk will check for the scanner and associated SDK. If the Visitor Kiosk cannot detect them, the following message will appear on the 'Initialisation screen', and the operator will not be allowed to logon:

"Failed to initialise Acuant Scanner. Ensure the Acuant SDK has been installed correctly and the scanned is connected to the workstation."

Check the scanner connection and install the SDK before starting the Visitor Management Kiosk application.

Welcome screen



The 'Welcome screen' is the default screen for the Kiosk and the screen returned to after visitor sign-in or other processes at the Kiosk have completed. It is the screen that is returned to whenever a process is cancelled, or if the Kiosk has been inactive for a predetermined time.

The screens that follow depend on what start option button you select.
Note: The screen shot above shows the default names of the start option buttons, however the text on these buttons may differ as they are configurable in Command Centre. Also, the 'Visitor Sign Out', 'Tour Group' and 'Staff' buttons will only appear if configured to do so.

Visitor Sign In (on page 51-41)

Visitor Sign Out (on page 51-49)

Tour Group (on page 51-51)

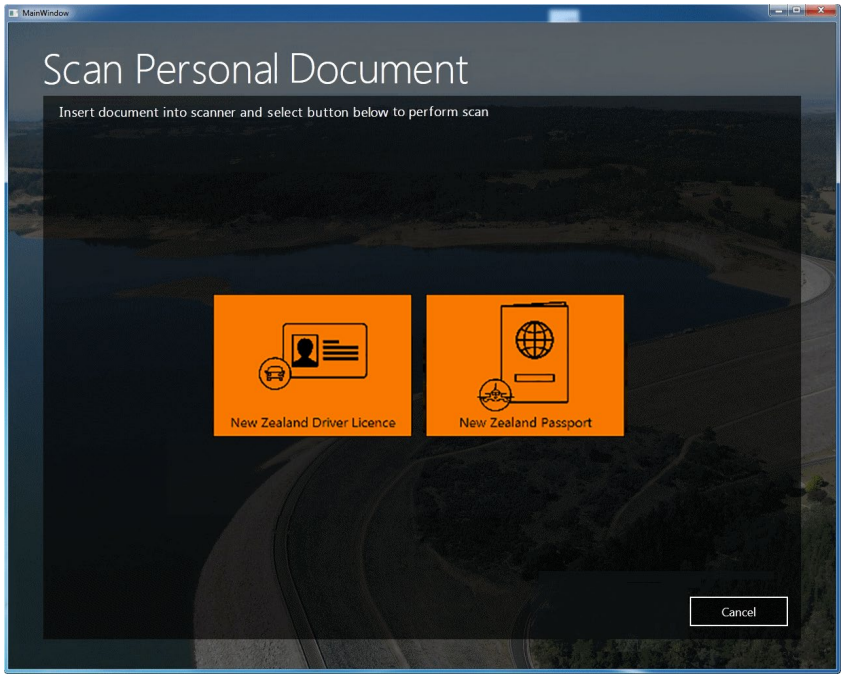
Staff (Rapid Entry) (on page 51-54)

Host Actions

A Host can log on at the Kiosk when the 'Welcome screen' is displayed, by badging their card at the reader. See ***Host Actions*** (on page 51-57) for sample screens.

Visitor Sign In

Scan Personal Document screen



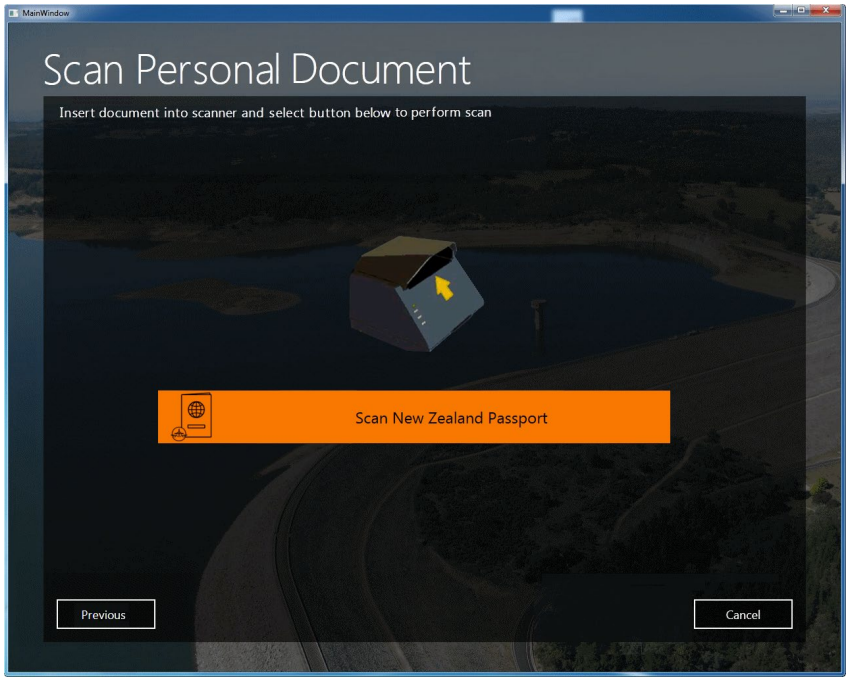
The ‘Scan Personal Document screen’ allows a visitor to scan a personal document to initiate a cardholder search. It is the first step of the single visitor registration process (entered from the 'Welcome screen') if:

- it is configured to display; and
- a Card scan device is installed and configured for the kiosk.

Otherwise the ‘Sign In screen’ displays.

Note: This screen is bypassed if there is only one type of personal identification able to be scanned, and will go directly to the next ‘Scan Personal Document screen’ with the **Scan <document type>** button to start scanning.

The visitor can only select one type of personal identification. When they insert the appropriate document into the scanner and click the corresponding button, the following screen displays:

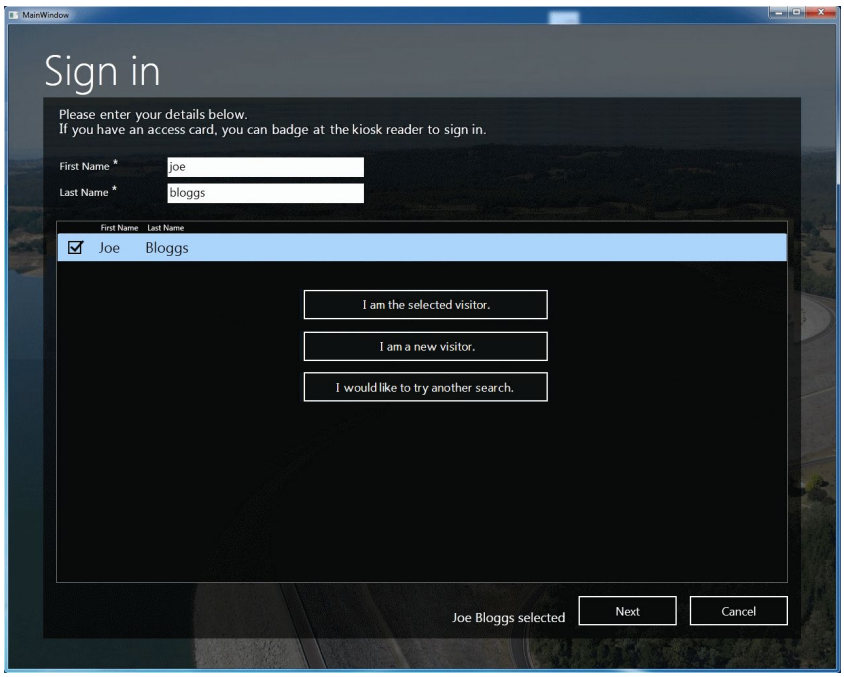


The visitor then clicks the **Scan <document type>** button to start scanning. A spinning wheel displays while scanning is in progress.

Notes:

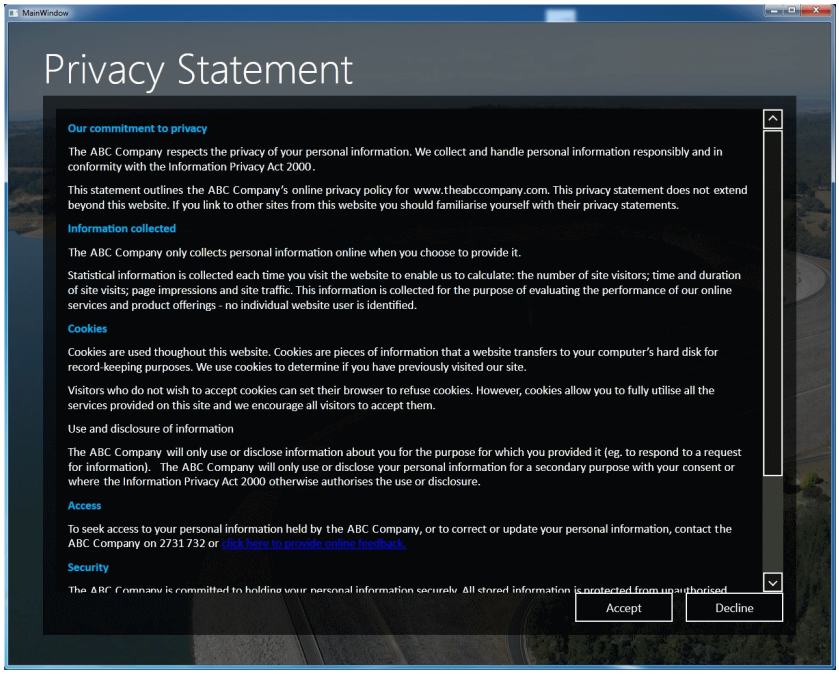
- The screens that appear, and the order they appear in, will vary depending on configuration.
- For visitors that are emailed an invite barcode, when they arrive and scan the barcode (either directly from their cell phone or printed on paper), a number of the screens will be bypassed, making the sign in process much quicker.

Sign in screen



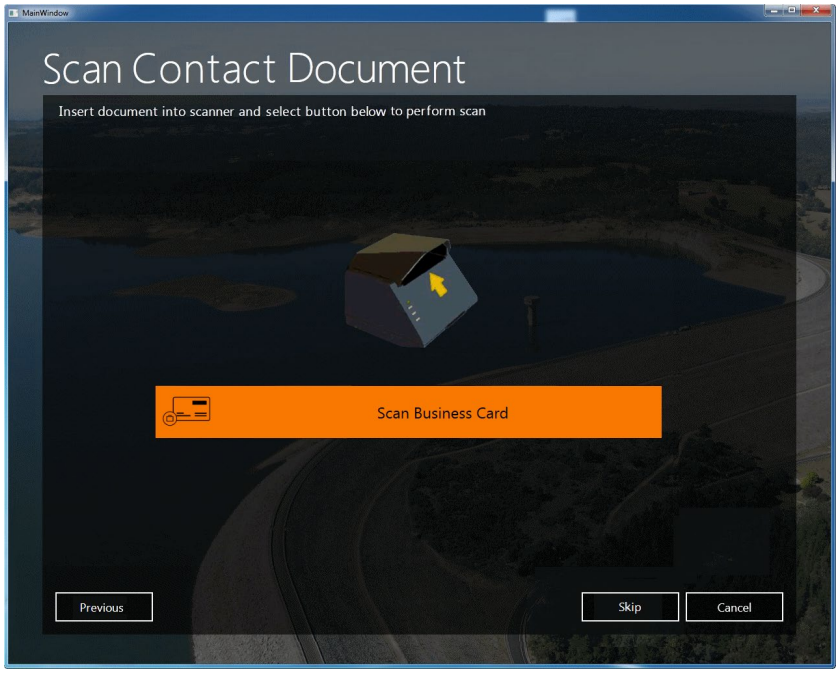
The 'Sign in screen' allows a visitor to identify themselves. If the ‘Scan Personal Document screen’ is NOT configured to display, this screen is the first step of the single visitor registration process entered from the 'Welcome screen'. Visitors can either manually enter their details or badge their access card if they have one.

Privacy Statement screen



The 'Privacy Statement screen' is entered from the 'Sign in screen' (if configured).

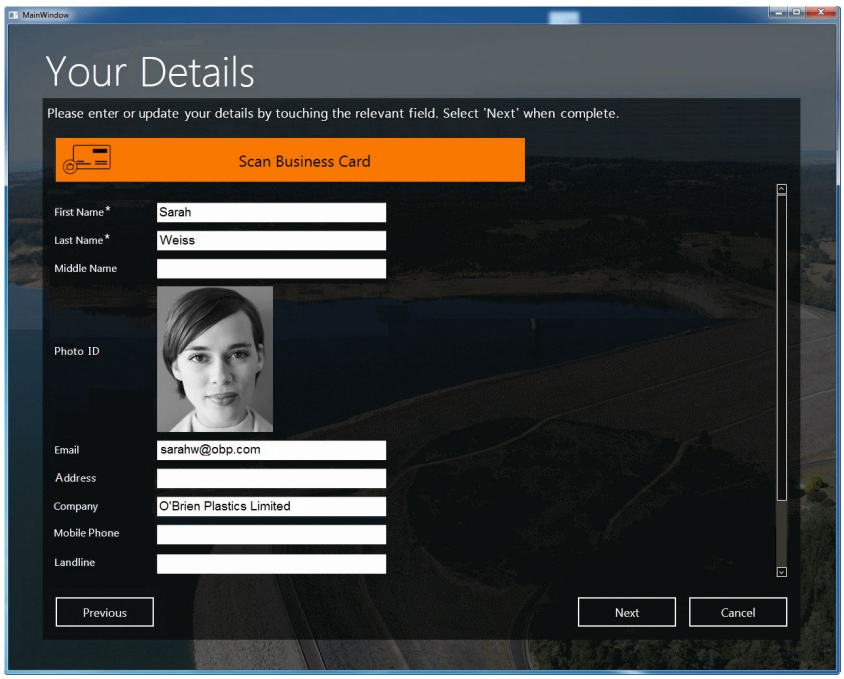
Scan Contact Document screen



The ‘Scan Contact Document screen’ allows a visitor to scan a secondary document containing further information about them, (e.g. contact details). If configured to display, it is entered from the ‘Privacy Statement screen’, but will only appear for a newly created visitor, (i.e. the **I am a new visitor** button was clicked on the ‘Sign in screen’).

The visitor inserts their personal identification into the scanner and clicks the **Scan <document type>** button to start scanning. A spinning wheel displays while scanning is in progress.

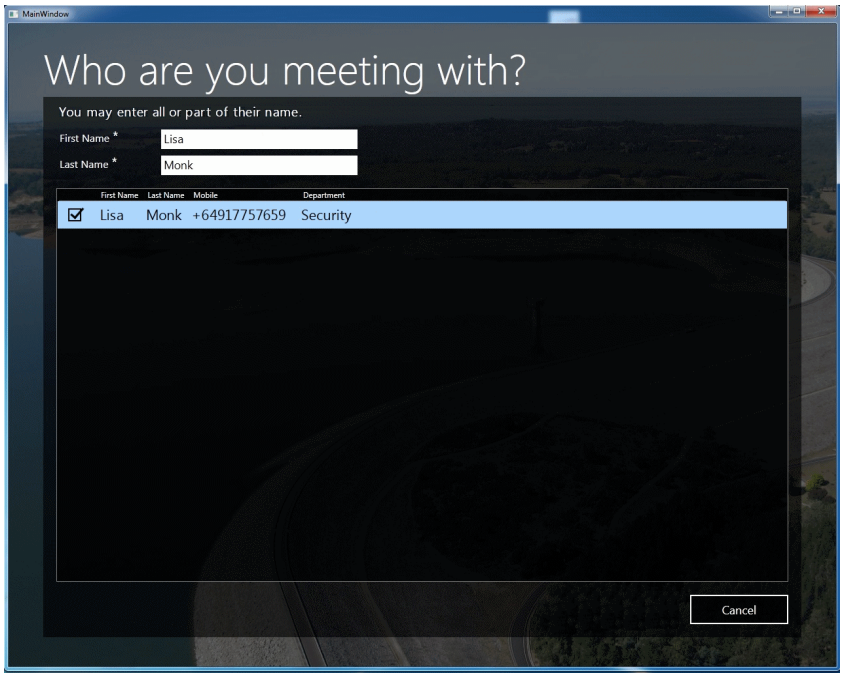
Visitor Details screen



The 'Visitor Details screen' is entered from the 'Privacy Statement screen' (if configured).

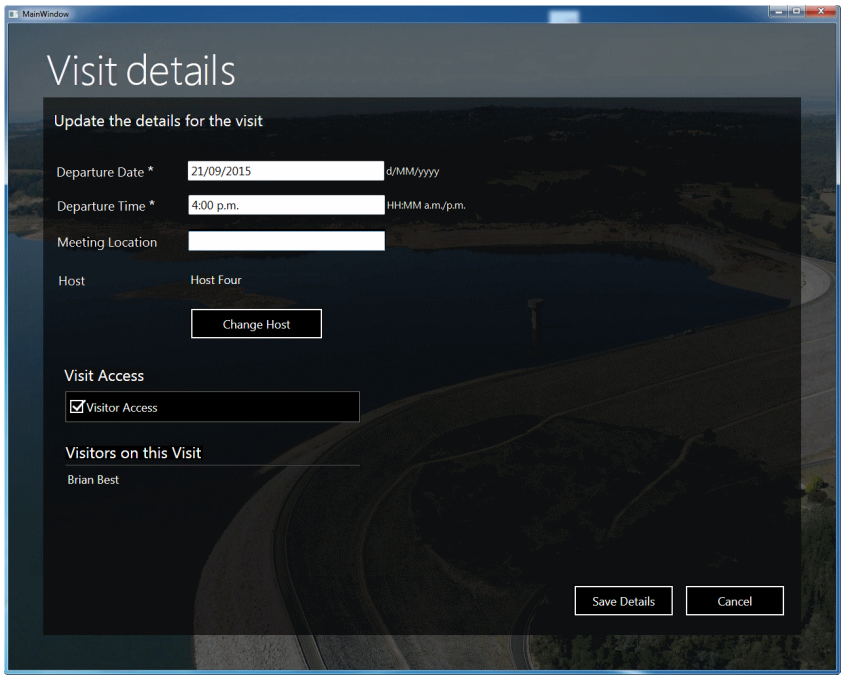
If an existing visitor was selected, (i.e. the **I am the selected visitor** button was clicked on the ‘Sign in screen’), a **Scan <document type>** button will be available for the visitor to re-scan their personal identification or make updates to their details on this screen as necessary. If the visitor does click the **Scan <document type>** button the ‘Scan Contact Document screen’ will appear, allowing them to scan their document.
Important: From the ‘Scan Contact Document screen’, if the visitor clicks the **Previous** button without scanning, the ‘Visitor Details screen’ will re-display but the **Scan <document type>** button will be missing. Therefore, the visitor will no longer have the option to scan unless they return to the 'Sign in screen' (via the **Previous** button) and start the sign in process again.

Find Host screen



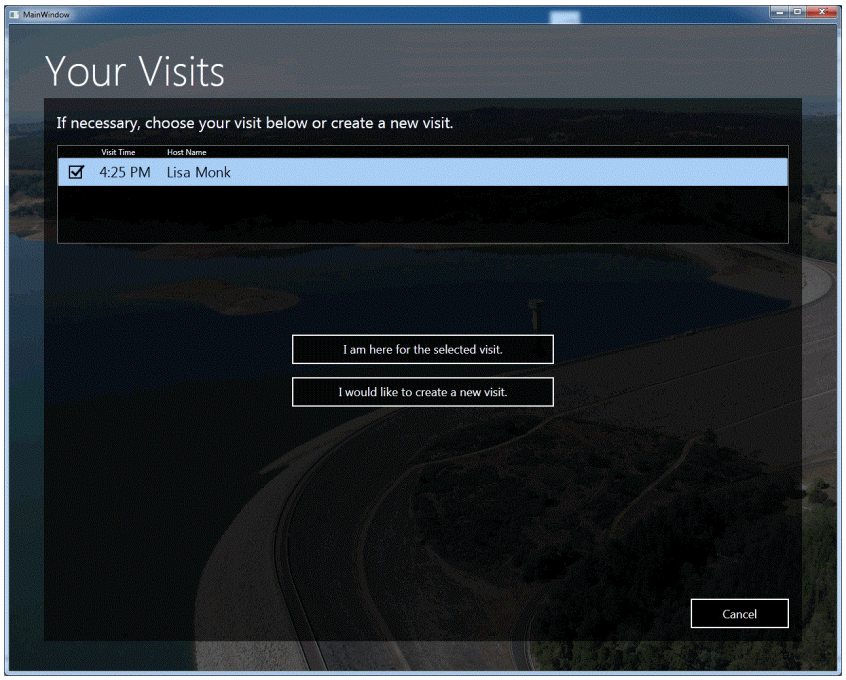
If a pre-registered visit for the visitor who is signing in cannot be found, the 'Find Host screen' is entered from the 'Visitor Details screen'. It allows the visitor to identify the person (host) they are meeting with. They can enter all or part of the person's name that they are meeting with. For example, if you are meeting with someone and you do not know how to spell their first name you could enter the first character of their first name followed by their surname, (e.g. A Thompson).

Visit Details screen



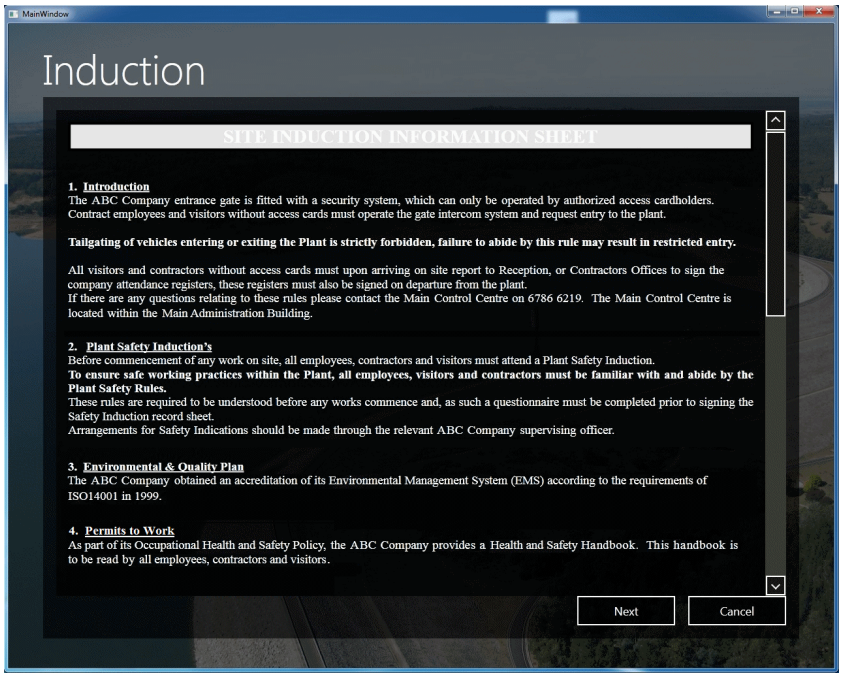
The 'Visit Details screen' is entered from the 'Find Host screen'. It is displayed only if a pre-registered visit cannot be found for the visitor who is signing in.

Alternatively, if a pre-registered visit can be found the 'Your Visits screen' is displayed to the visitor.



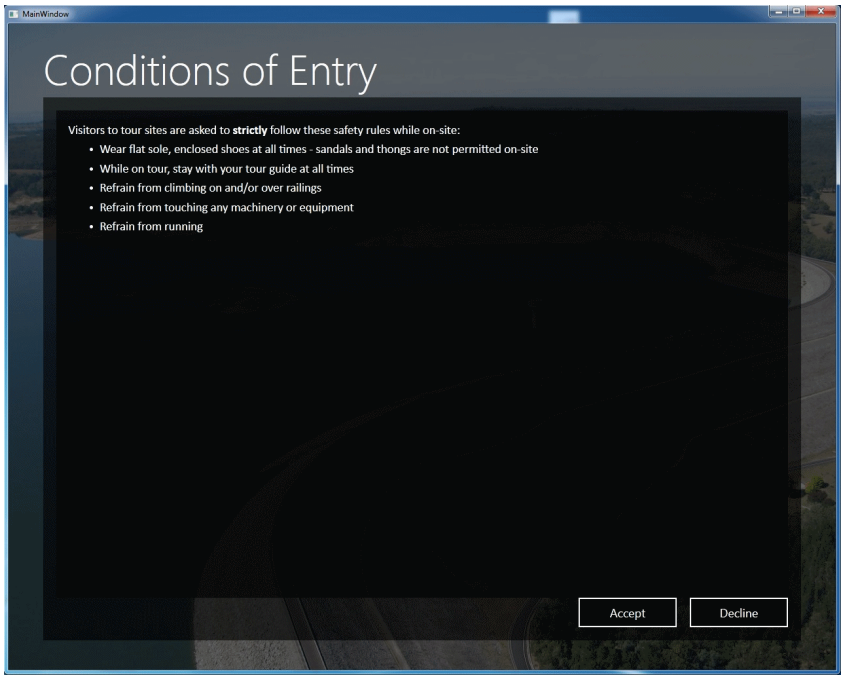
The 'Message for Host' field will appear on both of these screens if your site is licensed for Notifications and they have been configured, and the Host has an email or SMS configured. This field allows the visitor to enter additional information for the Host.

Induction screen



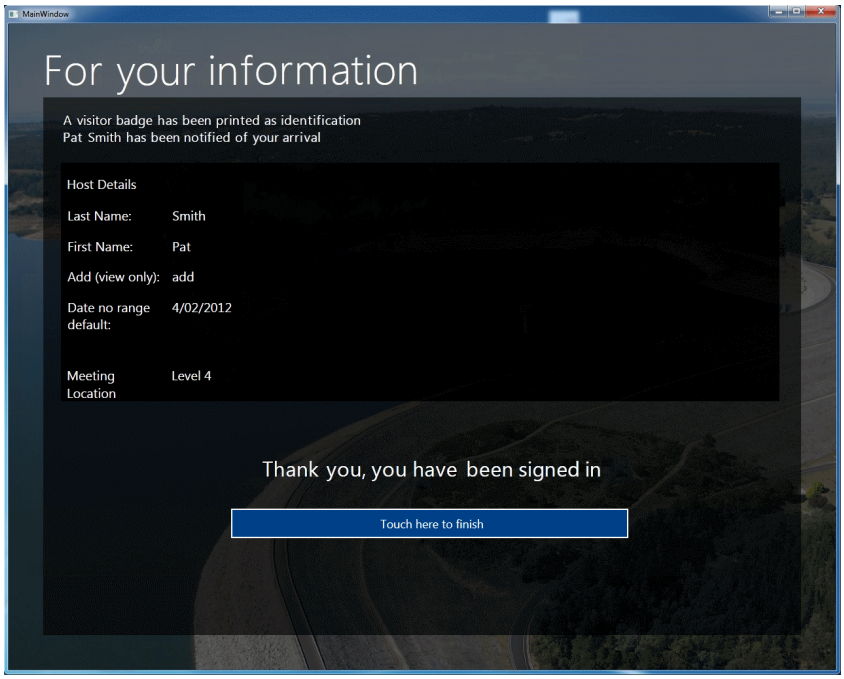
The 'Induction screen' is entered from either of the Visit Details screens, (i.e. either the 'Enter Visit Details screen' or the 'Your Visits screen'), if configured.

Conditions of Entry screen



The 'Conditions of Entry screen' is entered from the 'Induction screen' (unless this screen has been skipped), if configured.

Registration Complete screen



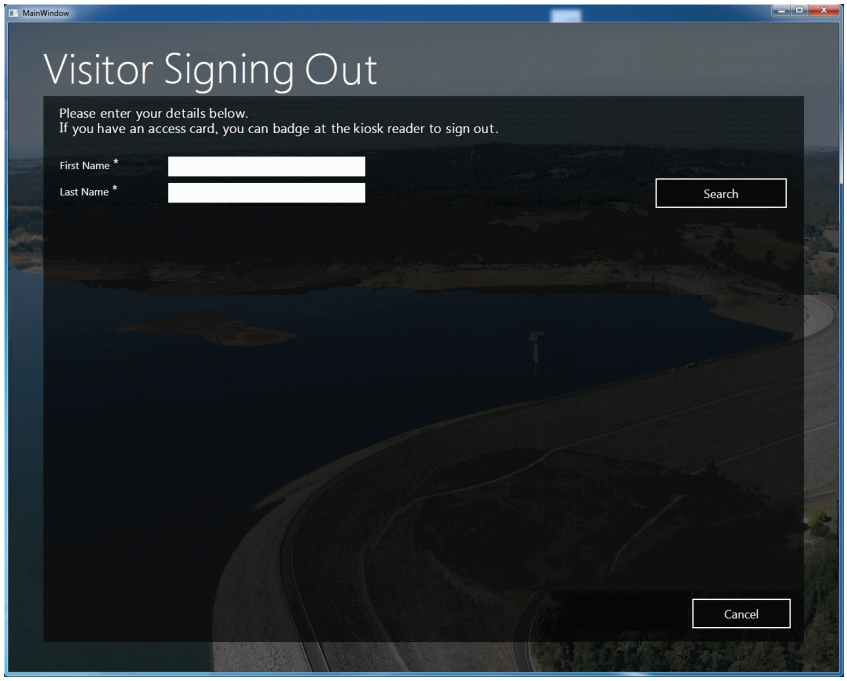
The 'Registration Complete screen' is entered from the 'Conditions of Entry screen' (unless this screen is skipped), and indicates that sign-in is complete. The following actions occur:

- The label is printed if label printing is configured for the kiosk,
- The visitor is automatically marked 'on site' or 'signed in', depending on configuration,
- Any Access Groups configured for this visitor type are assigned to the visitor,
- Host Notifications will occur if configured for the kiosk AND the visitor has chosen a host other than themselves,
- A message displays on screen to confirm actions taken, (e.g. *"Thank you, you have been signed in"*).

Selecting the **Touch here to finish** button returns the kiosk to the 'Welcome screen'.

Visitor Sign Out

Signing Out screen

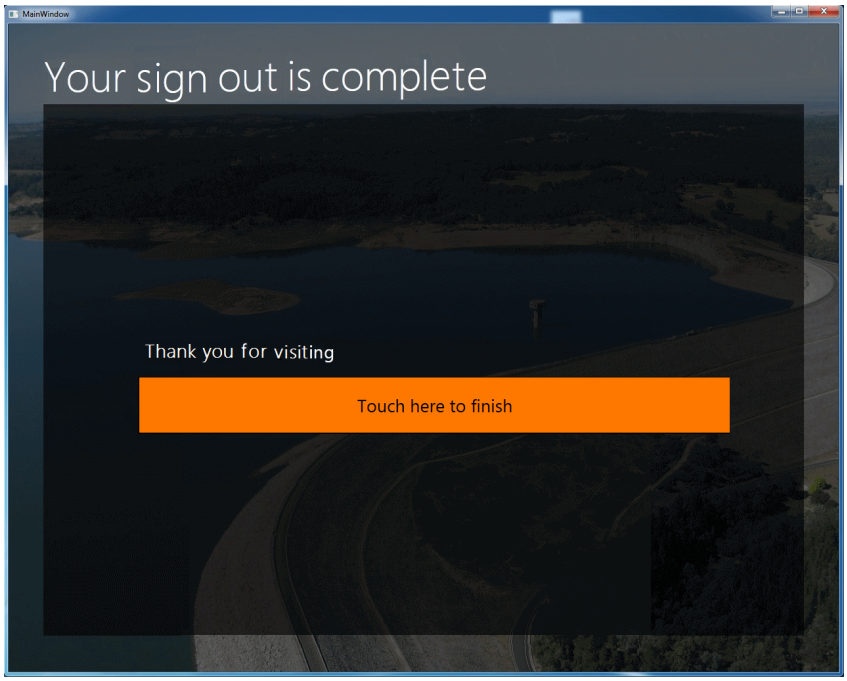


The 'Visitor Signing Out' screen allows visitors to identify themselves and mark themselves off site. It is the first step of the single visitor signing out process, entered from the 'Welcome Screen'.

They can either:

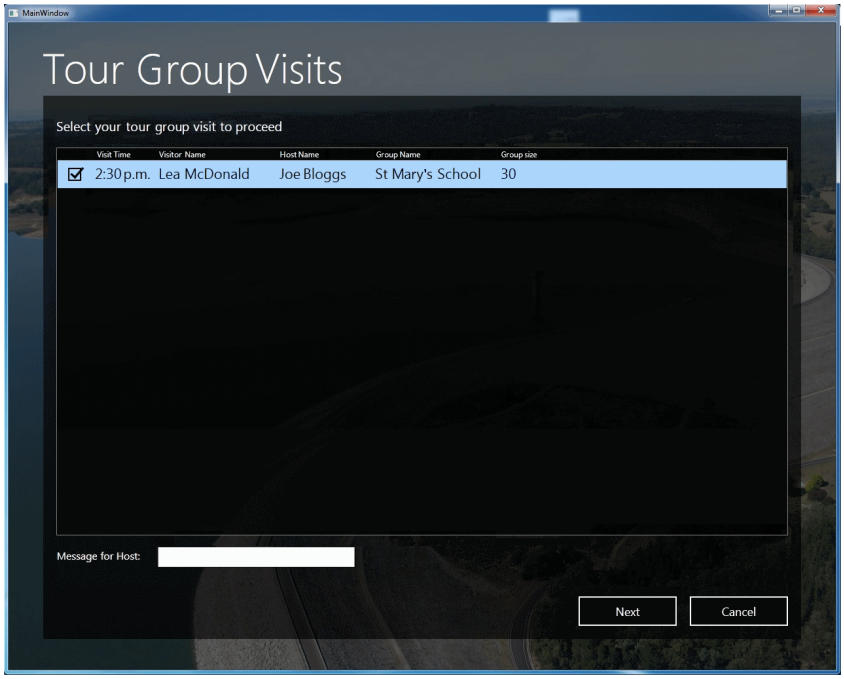
- manually enter their details,
- badge their access card (if they have one), or
- scan the barcode on their printed badge.

Signed Out screen



The 'Signed Out' screen is entered from the 'Signing Out' screen (if configured), and indicates to visitors that they have completed the Sign Out process.

Tour Group

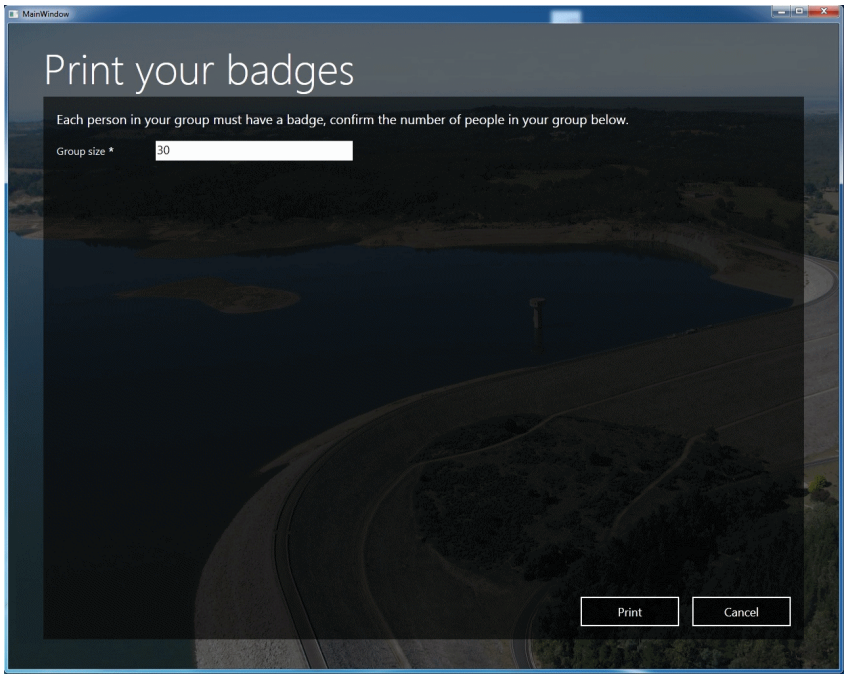


Tour Groups can sign in at the Kiosk by selecting the **Tour Group** button (or similar) on the 'Welcome screen'.

Notes:

- While 'Tour Group' is the default name of this button, the text is configurable in Command Centre.
- Tour Group visits cannot be created at the Kiosk. Tour Group visits must be pre-registered by their host using the Visitor Management client.

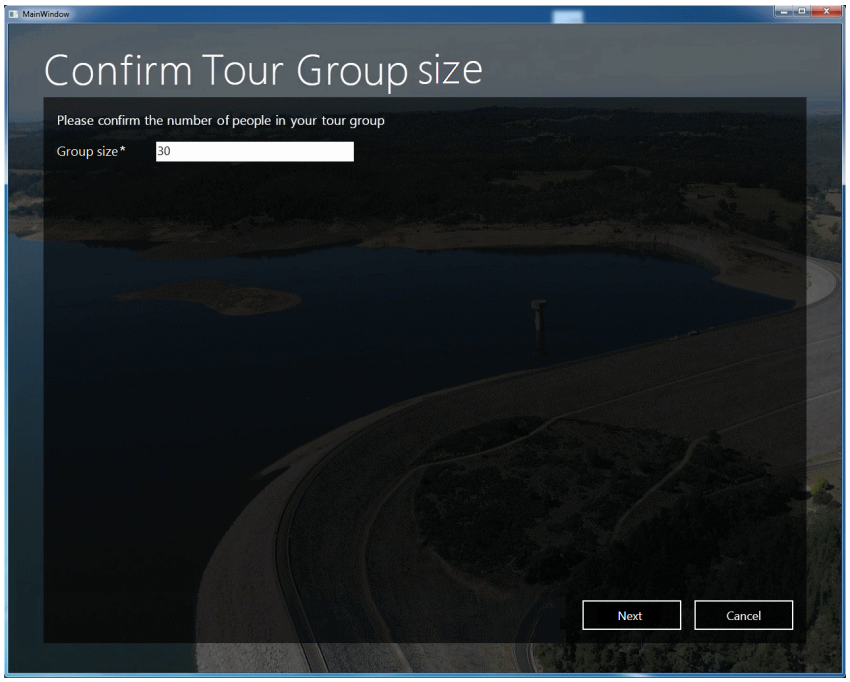
Tour Group - Print badges



A Tour Group leader prints a label for each member of the tour group from this screen. The supported label printer is the Dymo 450 label writer.

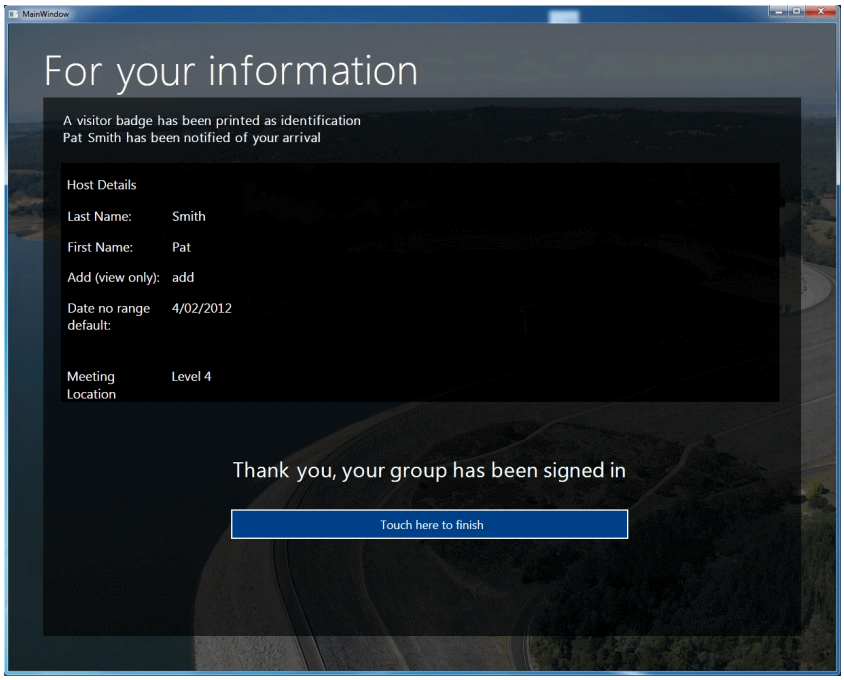
This screen only appears if the Kiosk is configured to print badges.

Tour Group - Confirm group size



This screen only appears if Tour Groups are configured to be marked on site and 'Print Your Badges' is not enabled.

Tour Group - Sign in complete

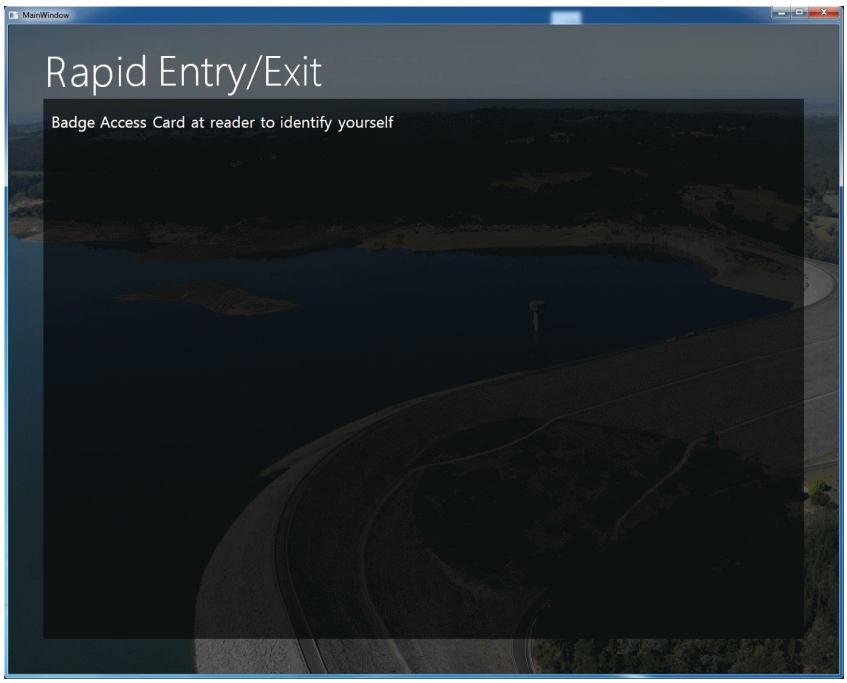


The final screen for Tour Groups indicates that sign-in is complete. The following actions occur:

- The label is printed if label printing is configured for the kiosk,
- The Tour Group is automatically marked "on site" or "signed in", depending on configuration,
- Host Notifications will occur if configured for the kiosk AND the visitor has chosen a host other than themselves,
- A message displays on screen to confirm actions taken, (e.g. *"Thank you, your group has been signed in"*).

Selecting the **Touch here to finish** button returns the kiosk to the 'Welcome screen'.

Staff (Rapid Entry)



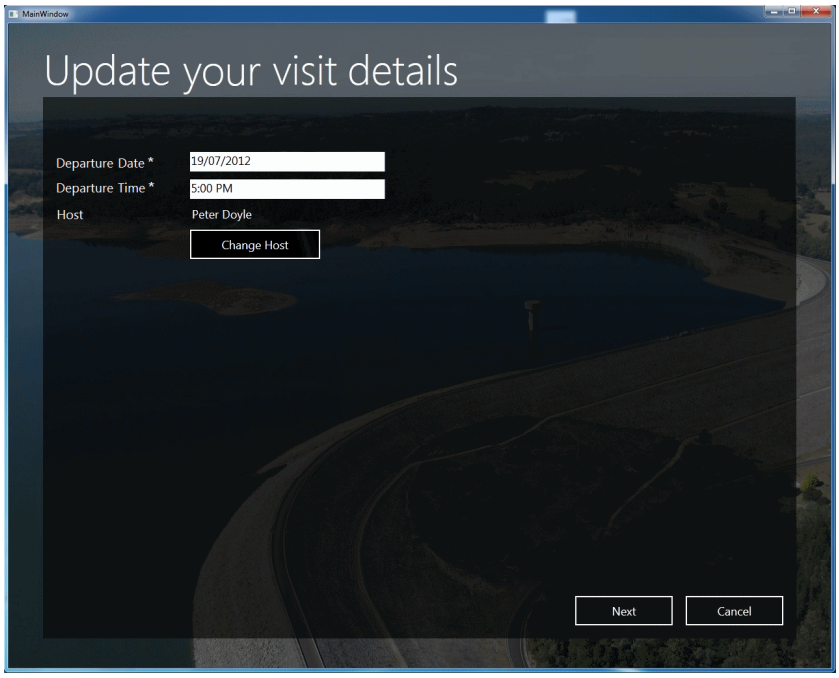
Internal employees who are visiting a site can gain quick entry to the site by selecting the **Staff** button (or similar) on the 'Welcome screen', then badging their card.

Notes:

- While 'Staff' is the default name of this button, the text is configurable in Command Centre.
- If the card badge does not identify a visitor then the following message displays:
  "Your access card is not recognised at this kiosk. Press Cancel to sign in manually."

  This often happens if the cardholder's division is not included in the **Find Visitors in these Divisions** grid on the ***Visit Configuration tab*** (on page 50-28), or the logged in operator does not have privilege to view the cardholder of the badged card.
- If they change host and the site host is configured for Notifications, the host will be notified.
- If the card badge identifies the person but they are not a member of the Rapid Visitor Type and the Rapid Host Type, they will be automatically sent to the standard visitor sign-in process.

Rapid Staff Entry - Update your visit details



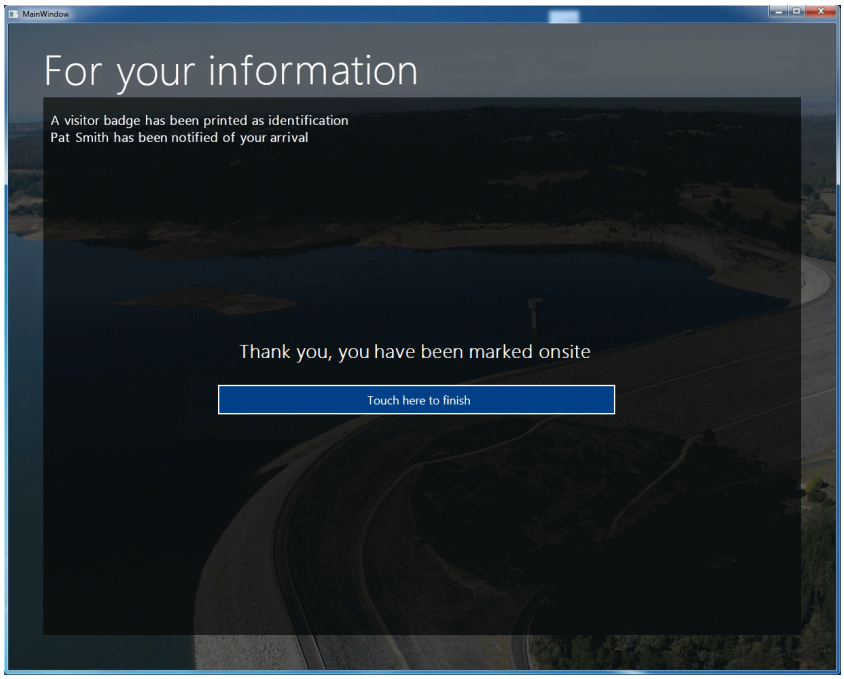
When the card badge identifies a visitor who is allowed to fast track their entry, then a visit is automatically created, with the visitor hosting themselves. The departure time for the visit is displayed on screen and can be updated if necessary (defaults to today).

The visitor can also change their host from this screen, if they want to be hosted by someone else, by clicking the **Change Host** button which opens the 'Who are you meeting with screen'.

If configured, this screen will not display for self-hosting visitors (only).

The 'Induction screen' displays (if configured), or is skipped if the visitor has already viewed this material within the configured time-frame. Likewise, the 'Conditions of Entry screen' displays if configured.

Rapid Entry - For your information

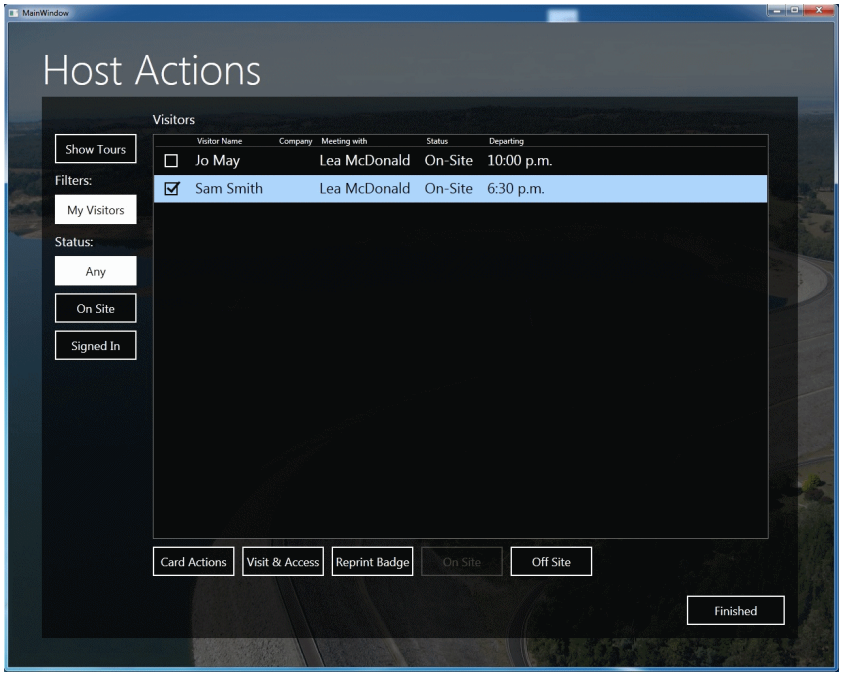


The final screen for Rapid Staff Entry indicates that sign-in is complete. The following actions occur:

- The label is printed if label printing is configured for the kiosk,
- The visitor is automatically marked on site,
- Any Access Groups configured for this visitor type are assigned to the visitor,
- Host Notifications will occur if configured for the kiosk AND the visitor has chosen a host other than themselves,
- A message displays on screen to confirm actions taken, (e.g. *"Thank you, you have been marked onsite"*).

Selecting the **Touch here to finish** button returns the kiosk to the 'Welcome screen'.

Host Actions



The 'Host Actions screen' allows a valid host to:

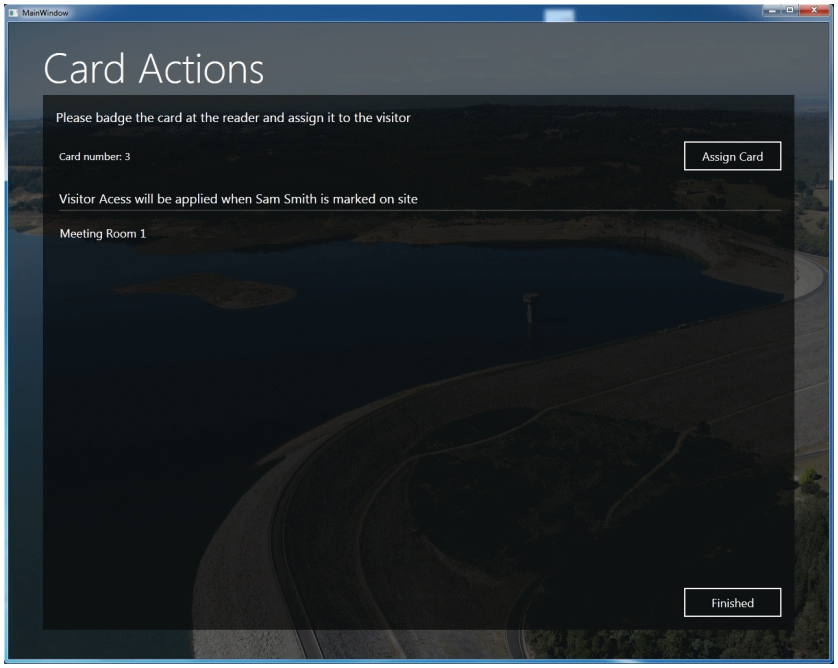
- mark visitors on or off site,
- to amend the departure time for a visit,
- reprint visitor labels if required, (e.g. where the label has been ruined or did not print), or
- assign visitor cards and access.

A privileged host, (i.e. one who belongs to the Kiosk Administrator Access Group configured on the Kiosk's reception) can also:

- select the label printer for the Kiosk,
- setup the business card scanner, or
- log off or exit from the Kiosk application from this screen, (i.e. use the **Tools** button).

Host Actions - Assigning a card

This feature allows a host to assign a card to a visitor, from a pool of visitor cards available at the Kiosk. Card assignment is optional. When a host selects a single visitor and clicks the **Card Actions** button, the following screen displays:

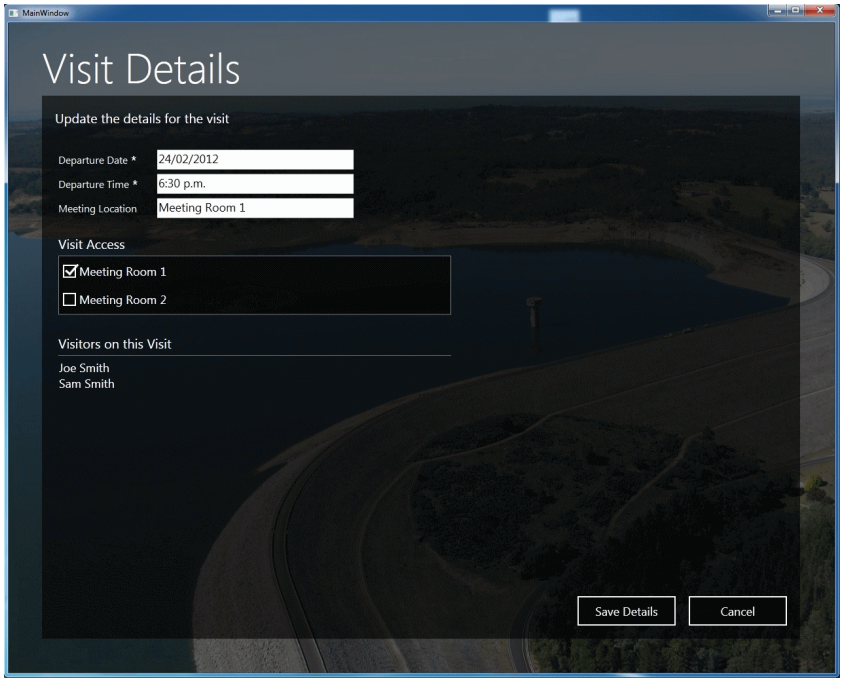


Note: If there are any card(s) already assigned through Command Centre, they will be mentioned as a note. A Visitor Management card can still be assigned here, and existing cards will be ignored.

Host Actions - Visit and access

This feature allows a host to assign access to a visitor (if configured) or update details of the visit, such as departure time or meeting location. Assigning access is optional if a visitor is using a pre-assigned card, (e.g. a permanent card rather than one assigned at the Kiosk). If a visitor card is assigned at the Kiosk, some access must also be assigned.

When a host selects a single visitor and the **Visit & Access** button the following screen displays:



Chapter 52: Cardholder Competencies

Introduction

Cardholder Competencies address a gap in the way Cardholder's access to zones can be specified. Using Access Groups a Cardholder need only belong to any group providing access to the zone. However, there is a need (especially in the mining industry) to be able to block access to a Cardholder who lacks some certification or whose certification has expired (for example Health and Safety certificate, qualification to operate equipment, etc.).

Notes:

- It is envisaged that cardholders in the emergency services would be put in an Access Group that has "competency-exempt" status configured for all Access Zones. All other cardholders would be required to have the competencies, whatever Access Group they belonged to, or at least somewhat less general competency exceptions.
- A competency once created is never 'removed' from the system, regardless of whether it has been assigned to anything or not. It can always be found by using the "Include deleted items" option (on the **General** tab) of the Find Tool.
- The **Times** tab of the Find Tool includes a cardholder "Competency Expiry" option. Choosing this option returns all Cardholders who have competencies that are due to expire within the specified time-frame.
- Competency requirements are additional the normal access schedule restrictions.
- Each Cardholder Competency requires the following to be specified:
  - Competency Type
  - Expiry Date (defaults to blank to indicate that it does not expire)
  - Advance Notification Period in days (defaults to zero if no Expiry Date, otherwise defaults to seven days).
- Messages can be configured to display at HBUS Terminals and Remote Arming Terminals (when used in conjunction with a reader) or secondary displays via the Gallagher Controller API (FTCAPI), when cardholders present their cards, to inform them of upcoming expiry of competencies or competencies they are missing. However, messages will not display when the reader is assigned to an elevator car.
- In a multi-server system Competencies and Cardholder Competencies are replicated between servers according to the same rules as any other replicated items.
- The Cardholder Report, Access Report and Site Configuration Report all have the option to include competencies.

- Access granted or denied events from a reader that is assigned to an elevator car will not contain any competency details.

Licensing

The use of competencies is controlled by a server license option which specifies the number of competencies allowed to be created in the system, as follows:

```
[Limits]
Competencies=<nn>
```

where <nn> is the number of competencies your site is allowed.

Note: Base license files include the use of one competency, (i.e. the license file entry will be Competencies=1). Sites with this type of license file will have access to the competency functionality, but will only be able to create one competency.

In a multi-server environment each server is independently licensed and the server of origin can create as many competencies as it is licensed for. Competencies can only be edited on the server they were created on, but are replicated across all other servers in the system. A competency can be assigned to any cardholder whether it was created on the local server or a remote server.

Operator Privileges

Privilege	is required to...
"View Site"	to display a competency.
"Configure Site" and "View Site"	create, update or delete a competency.

Select the item below that you require further detail on:

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

Scenario: Accessing a zone restricted by cardholder competencies

Introduction

On many sites cardholders are required to have specific competencies before they can enter a particular Access Zone. These competencies may be as simple as the successful completion of a training programme, or may be associated with a specific credential, (e.g. a driver's license). The competency may be a permanent competency once attained or it may be valid only between specified dates and requires renewal if the cardholder still requires access after the expiry date.

Scenario

1. A cardholder presents a card at a reader controlling access to an Access Zone which is currently in a secure state.
2. The cardholder belongs to an Access Group, the members of which are allowed into the secure Access Zone at that time according to the Command Centre schedule.

The Access Zone has...	A cardholder...	Result
no competencies stipulated	Cardholder competencies are not checked in this scenario	• Access is granted, • Cardholder is notified, • Door unlocks.
a single competency stipulation that all cardholders must have: • **completed site induction training**	has the competency of "Site Induction" and this is still current	• Access is granted, • Cardholder is notified, • Door unlocks.
	does not have the competency of "Site Induction"	• Access is denied, • Cardholder is notified with the configured message, • Door remains secure.
	has the competency of "Site Induction" but this has expired, (e.g. 6 month employment contract)	• Access is denied, • Cardholder is notified with message *"Access denied. Employment expired"* or similar, • Door does not unlock.

The Access Zone has...	A cardholder...	Result
a competency stipulation that all cardholders must have: • **completed site induction training, and** • **have a current medical certificate**	has the current competency of "Site Induction" and the competency of a valid "Medical Certificate" that has not expired	• Access is granted, • Cardholder is notified, • Door unlocks.
	has the current competency of "Site Induction" but has never had a valid "Medical Certificate" competency	• Access is denied, • Cardholder is notified with message *"Access denied. Medical Cert missing. Contact HR Dept"* or similar, • Door remains secure.
	has the current competency of "Site Induction" and does have the competency of a valid "Medical Certificate" but this has expired	• Access is denied, • Cardholder is notified with message *"Access denied. Medical Cert expired. Contact HR Dept"* or similar, • Door remains secure.
at least one **Access Group** defined as being **competency-exempt**. The cardholder does not have any of the competencies required for access to the zone	is a member of the **competency-exempt** Access Group	• Access is granted, • Cardholder is notified, • Door unlocks. (The cardholder's competencies are not checked in this scenario)
	is not a member of a **competency-exempt** Access Group for the Access Zone	• Access is denied, • Cardholder is notified with appropriate *"Access denied"* message, • Door remains secure.
a competency stipulation that all cardholders must have completed at least one of: • **site induction training, OR** • **company induction training**	has the current competency of "Site Induction" and the competency of "Company Induction"	• Access is granted, • Cardholder is notified, • Door unlocks.
	has the current competency of "Company Induction" but does not have the "Site Induction" competency	• Access is granted, • Cardholder is notified, • Door unlocks.
	has neither the competency of "Site Induction" nor "Company Induction"	• Access is denied, • Cardholder is notified with the configured message, • Door remains secure.

Configuring Competencies

Introduction

This procedure describes how to configure a new competency. The "Configure Site" or "Edit Competency Definitions" operator privilege is required to configure a competency.

Note: Your license file contains the maximum number of competencies that your site is allowed. Once that number has been reached the option to create additional competencies will be disabled.

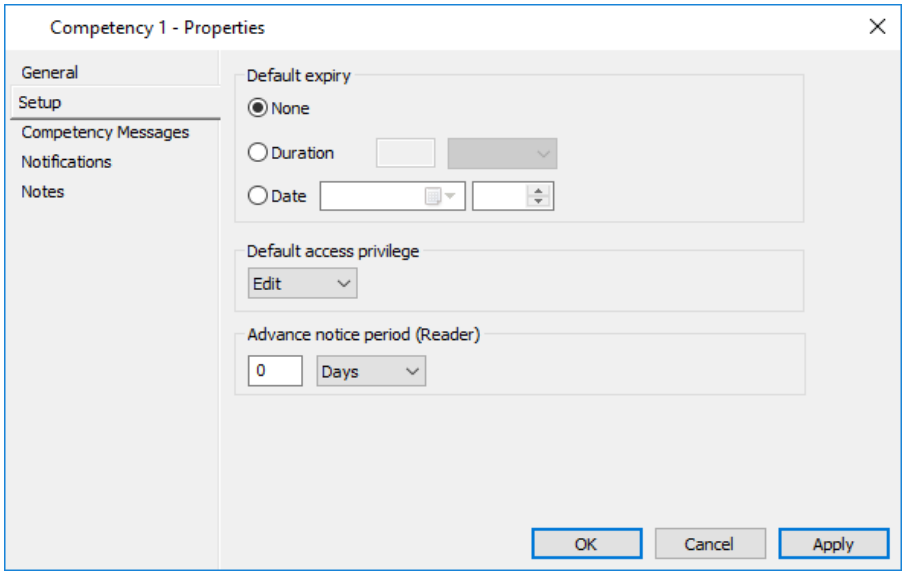
Considerations

- Deletion of a Competency is only allowed if it is not currently assigned to a Cardholder or an Access Zone.
- Competency expiry notifications are sent each day at the **Expiry Notification Time** set in **File > Server Properties > Notifications**.
- If notifications cannot be sent at an **Expiry Notification Time** (e.g. due to server being down), *all* unsent notifications will be sent at the next possible **Expiry Notification Time**.

Configuration

To configure a Competency, perform the following procedures in Gallagher Configuration Client:

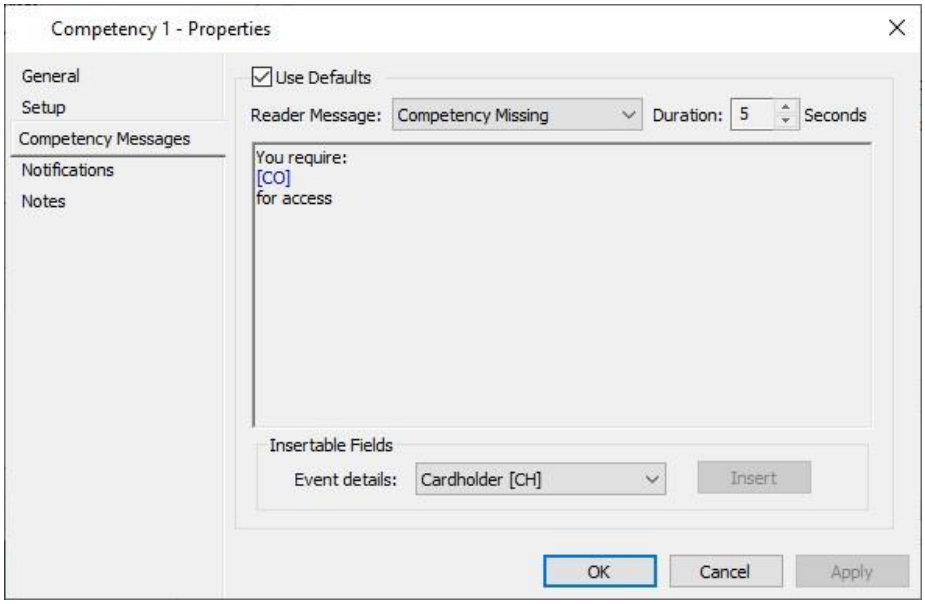
1. Click **Configure** from the menu bar, then **Competencies**.
   The **Competency** List Window opens (in grid view).
2. **Right click** and select **New...Competency**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Setup** tab.



5. Configure as appropriate:

Field	Description
Default Expiry	The default expiry can change between three states: - No expiry, (i.e. none), - a duration, or - a date/time. When one is selected, the others are disabled and the controls are blanked out. If editing the default expiry as a duration, or editing the advance notice period, the user will be able to choose the units in the adjacent combo box - choosing between days, weeks, months and years, and the edit boxes will only accept values up to 999. The duration and date expiry options will not be kept in sync - when one changes, the other will not change to reflect the updated date or duration. (Default = None) **Note:** If an Expiry Date is set in the past a message displays alerting you that the date is before the current date.
Default access privilege	The options available in this drop-down list are: - Edit (the default) - View, and - Hidden
Advance notice period (Reader)	Defines when Cardholders will be given competency expiry warnings at Terminals. Once this time has been reached (e.g. 1 week) before a Cardholder's competency is due to expire, the Competency Expiry Due message will display on a 'Message display device' (e.g. HBUS Terminal or secondary devices via the Gallagher Controller API) the next time a Cardholder badges at one. (Default = 0 days).

6. Click the **Competency Messages** tab to alter the messages displayed by this competency.



This screen allows you to specify how competency notifications are to be structured for each type of 'Message display device' that is required to show these messages. 'Message display devices' are:
- HBUS Terminal, or
- a secondary display via the Gallagher Controller API.

When a cardholder presents their card, one of the following messages may be displayed:
- Competency Missing
- Competency Expired
- Competency Expiry Due

Notes:

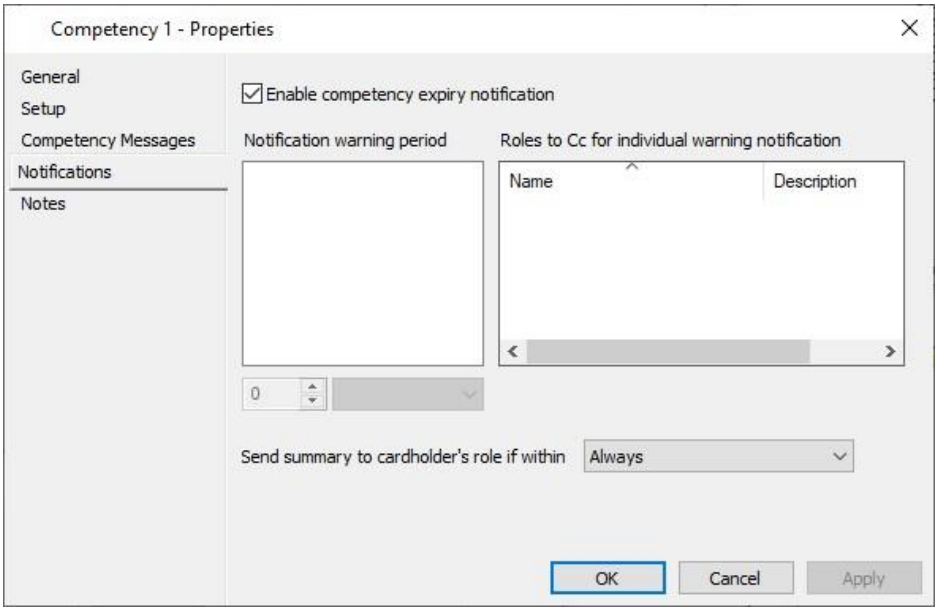
- When creating a new competency, the options on this tab are set to the system-wide defaults (via the Server Properties). Altering messages defined on this property page will only apply to this specific competency.
- Competency messages are not displayed on a reader, when the reader is associated with an elevator car.

7. Deselect the **Use Defaults** checkbox.
   The competency message becomes editable.
8. Select the type of message string you wish to modify from the **Reader message** drop-down list. The options are:
   - Competency Missing
   - Competency Expired
   - Competency Expiry Due
9. Enter a string into the grid.
   This is achieved by typing in text and selecting the appropriate “Insertable Fields”, from the **Event details** drop-down list where necessary, and clicking the **Insert** button.
   Notes:
   - There is no limitation on how many of each **Event detail** can be inserted, nor on how many different types of details can be put in the message.
   - The message string is limited to 2000 characters (one byte characters or Latin characters). Four lines of text are displayed. A user can access the remaining text by pressing the 'More' function key on the HBUS Terminal, then scrolling the message.
   - The contents of the **Event details** drop-down list will vary based on what **Reader message** has been selected for modifying.
     The following **Event details** represent entities that can be named within Command Centre, and will all appear in the drop-down list for each message, except for numbers 3 and 4, which will only appear for the “Competency expiry due” message:

1. Cardholder name [CH]
2. Competency name [CO]
3. Date of expiry [DA]
4. Days to expiry [#D]

- The message will display for the length of time configured in the **Duration** field (Default = 5 seconds) or until the next card is presented, whichever comes first. If the 'More' function key is pressed on the HBUS Terminal and there is less than 10 seconds until the display is due to expire, the time will be increased to 10 seconds.
- Only one cardholder competency message is displayed on the reader. The message that is displayed is decided as follows:
  - If there is one or more Competency Expiry Due message, the message for the competency that will expire soonest is displayed on the reader.
  - If there are messages for competencies that are due to expire at the same date and time, the Competency Expiry Due message for the competency ordered highest (on the **Competencies** tab of the Access Zone) is displayed on the reader.
  - If there are no Competency Expiry Due messages, only Competency Missing or Competency Expired messages, the message for the competency ordered highest (on the **Competencies** tab of the Access Zone) is displayed on the reader.

10. Click the **Notifications** tab to enable email and/or SMS warning notifications for competency expiries.



11. Select the **Enable competency expiry notification** checkbox.

12. Configure as appropriate.

Field	Description
Notification warning period	Defines when Cardholders are sent warning notifications. It is the amount of time until a Cardholder's competency is set to expire when the Cardholder will be sent a notification. For example, if a Notification warning period is set to 2 Weeks, a Cardholder will be warned (via email and/or SMS depending on Cardholder Personal Data) of their competency expiry two weeks before the Competency is set to expire. **Note:** Cardholders must have an Email PDF configured to receive email notifications, and a Mobile PDF configured to receive SMS notifications.
Roles to Cc for individual warning notifications	The Roles that will be carbon copied (Cc'd) in the email warning notifications that are sent to Cardholders. Remote Roles can also be added here.
Send summary to cardholder's role if within	Defines when a Cardholder's Roles are sent summaries of upcoming Cardholder competency expiries. It is the time period before a Cardholder's competency expires, within which, upcoming expiry summaries will be sent to Roles at the same times as all Notification warning period times. Summaries will be sent via email, not SMS. 'Roles' in this instance refers to all Roles in the **Cardholder's Relationships** grid in the **Relationships** tab of the Cardholder. For example, if set to Always, a Cardholder's Roles will be sent summaries of their upcoming expiries at all Notification warning periods. If set to 2 Weeks, a Cardholder's Roles will be sent summaries of their upcoming expiries at Notification warning periods of two weeks or shorter. **Notes:** • The time period options that appear in this list are purely reflective of the periods you set in the **Notification warning period** grid. • Roles are only sent summaries if **Competency Expiry Warnings** is selected in the Role's **Notifications** tab.

For a better understanding of these fields, see ***Configuration scenarios*** (next).

13. Right-click inside the **Notification warning period** grid and select **Insert...**
    A warning period is created.
14. Set the period of warning for this notification. From the drop-down list below the **Notification warning period** grid, select the unit of time. Then, using the  buttons or manually, enter the amount of your selected unit of time (days, weeks, months) you want to set the warning period for.
15. Select the Roles to be carbon copied (Cc'd) in the notifications for this warning period. From the Roles window (**Manage > Roles**), drag and drop the Roles that you want to be Cc'd in individual warning notifications, into the **Roles to Cc for individual warning notification** grid.
16. For all additional Notification warning periods you wish to configure, repeat steps 13-15.
17. From the **Send summary to cardholder's role if within** drop-down list, select when you wish Roles to be sent summaries of upcoming Cardholder expiries.
18. The content of the email notifications can be customised. If you wish to customise the email notifications, refer to ***Notifications*** (on page 35-1).
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.

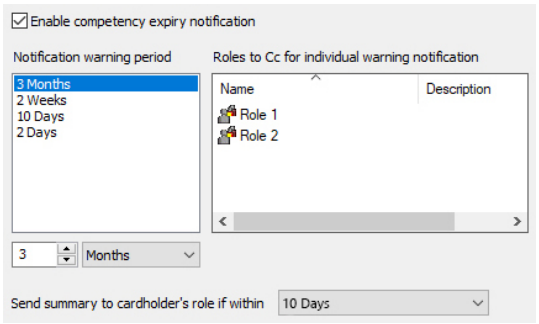
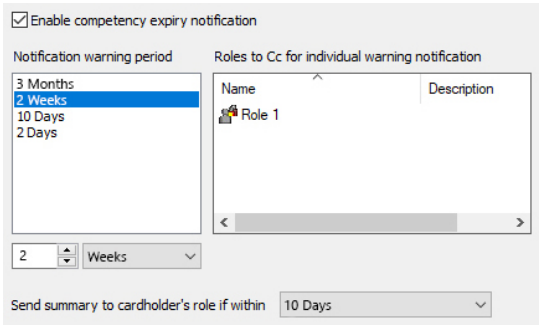
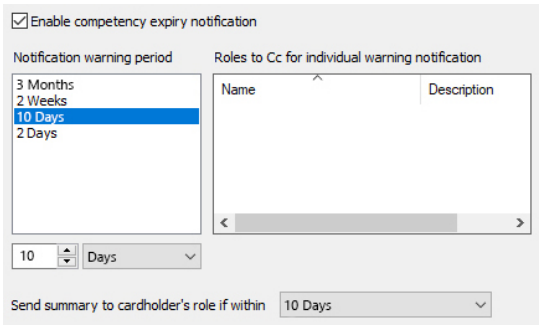
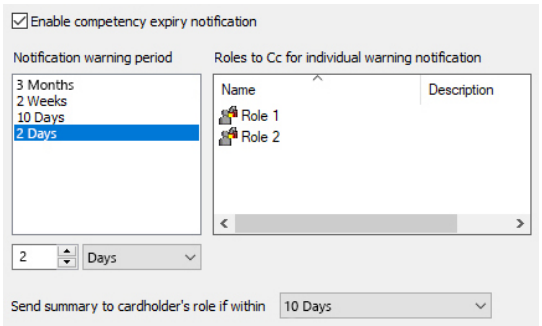
Result

A competency has been created.

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

Configuration scenarios

This topic provides further explanation of the fields on the **Notifications** tab of Competency properties.

Warning period	Screenshot of configuration	Result
3 Months		At 3 Months before expiry the Cardholder is notified. The Roles, 'Role 1' and 'Role 2', are Cc'd in the Notification. The Cardholder's Roles are not sent summaries because **Send summary to cardholder's role if within** is set to 10 Days, and the notification is being sent at 3 Months (which is not within 10 Days).
2 Weeks		At 2 Weeks before expiry the Cardholder is notified. The Role, 'Role 1' is Cc'd in the Notification. The Cardholder's Roles are not sent summaries because **Send summary to cardholder's role if within** is set to 10 Days, and the notification is being sent at 2 Weeks (which is not within 10 Days).
10 Days		At 10 Days before expiry the Cardholder is notified. No Roles are Cc'd in the Notification. The Cardholder's Roles are sent summaries because **Send summary to cardholder's role if within** is set to 10 Days, and the notification is being sent at 10 Days.
2 Days		At 2 Days before expiry the Cardholder is notified. The Roles, 'Role 1' and 'Role 2', are Cc'd in the Notification. The Cardholder's Roles are sent summaries because **Send summary to cardholder's role if within** is set to 10 Days, and the notification is being sent at 2 Days (which is within 10 Days).

Assigning Competencies to cardholders

Introduction

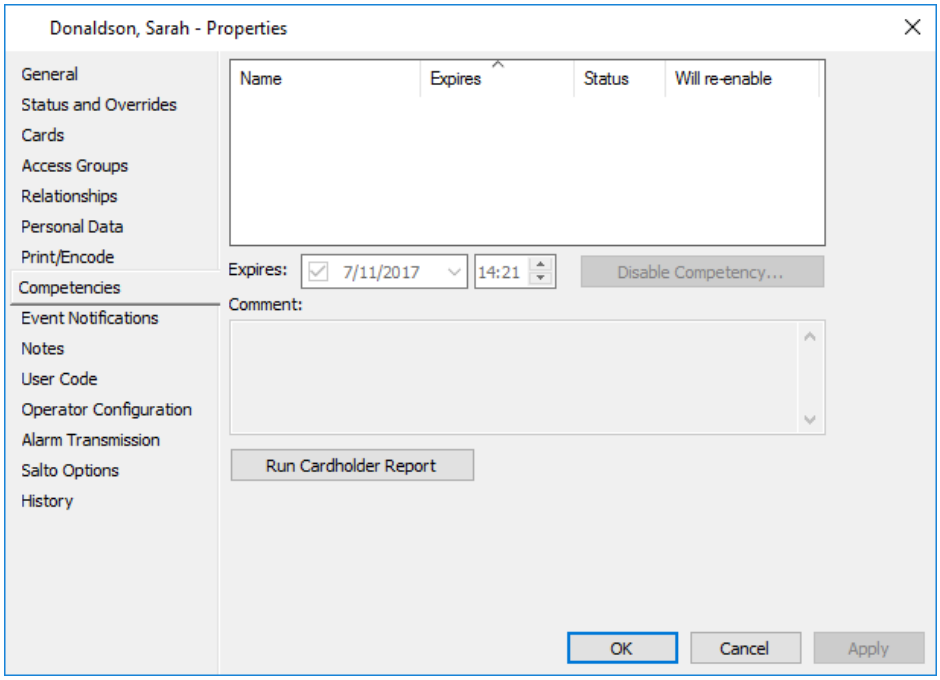
This procedure describes how to assign competencies to cardholders.

Note:

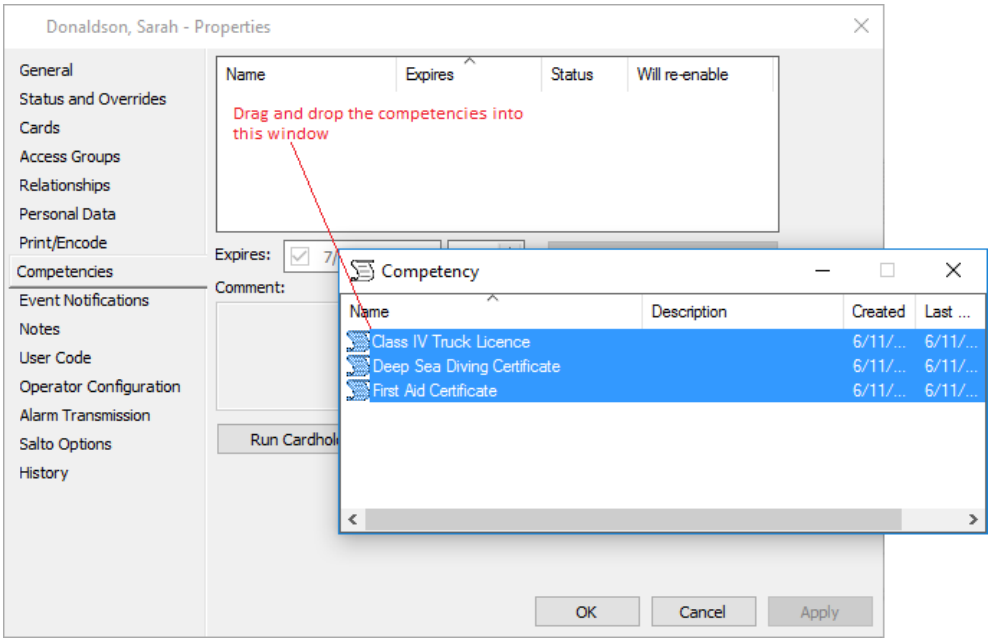
The operator privilege required to update cardholder competencies may need to be different to "Edit Cardholder" as it may involve different staff, (e.g. HR) that provide this information. Operators with the "Edit Cardholder" privilege can alter the expiry times and enable/disable competencies, however they cannot add/remove competencies from a Cardholder. In order to do this they require the "View Site" privilege. This may be required when cardholder competencies are sourced from an external system via an external interface, (e.g. from an HR system).

Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. **Right click** on the required cardholder, and select **Properties**.
3. Click the **Competencies** tab.



4. Click **Configure** from the menu bar, then **Competencies**.
   The **Competency** List Window opens.
5. Select those competency(s) you want to assign to the cardholder.
   Drag and drop them into the **Competencies** tab.



While the competencies are sorted in alphabetical order on the **Competency** List Window, when they are dragged into the upper grid on the **Competencies** tab, they are sorted according to expiry, with the competencies that are expired at the top (in red text), followed by those that will expire the soonest. If a competency is within the competency "warning period", then it will be in yellow text. A competency that is disabled will be greyed out in the competency grid.



Note: The specific shade of colour will change depending on the system colours, so with dark system text it would be a darker shade of red or yellow, and with light system text it would be a lighter shade.

6. Close the **Competency** List Window.
7. You can set the expiry date, add comments to, remove or disable a competency.

If you want to...	then select the competency and...
set an expiry date for a competency	use the **Expires** date and time control to set when the competency is due to expire.
disable a competency	click the **Disable Competency...** button. The **Re-enable Competency** dialog displays, and the **Disable Competency...** button is replaced with the **Re-enable Competency** button. If the competency is not to be re-enabled at any time, click the **Manually** radio button. However,

If you want to...	then select the competency and...
	if you want the competency to re-enable at a later date, use either the **In** control to specify the length of time until it will be re-enabled, or the **On** date and time control to set when it will be re-enabled. **Note:** When a disabled competency is selected, it can be re-enabled by clicking the **Re-enable Competency** button.
add a comment to a competency	enter your free-form text comments in the Comment grid. (Maximum = 2500 characters) **Note:** This information can be used as a historical record of changes.
remove a competency	**right click** and select **Remove from List**.

8. If you want to run a Detailed Cardholder report based on the Cardholder being edited, click the **Run Cardholder Report** button.
   The Cardholder Report Wizard automatically advances to the **Report Generation Progress** page and the report starts running. Once the report has been generated, you can close and discard the report, or use the **Back** button in the report wizard to reconfigure or save the report.
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

A competency(s) has been assigned to a cardholder.

Adding Competencies to Access Zones

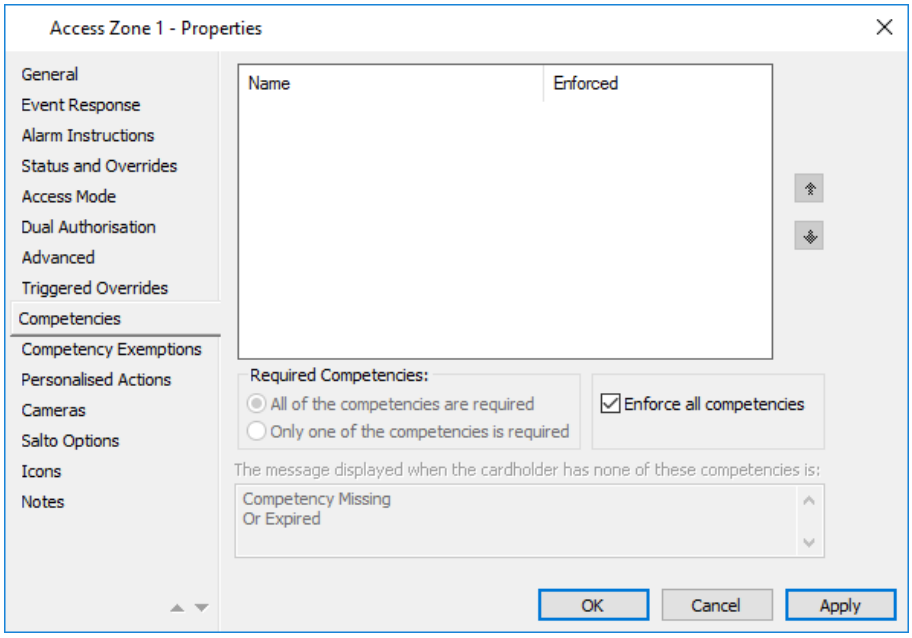
Introduction

This procedure describes how to configure an Access Zone so that cardholders attempting to enter that zone are required to have competencies.
Notes:

- Adding Competencies to an Access Zone requires Command Centre to update the Competency details of all cardholders who have access to that zone. This can result in a delay before the Competency is in effect for all cardholders. The length of this delay will depend on the number of cardholders who have access to that zone, (e.g. 1000 cardholders may take several minutes to update). Therefore, the following process is recommended when changing larger numbers of cardholders to minimise the delay experienced:
  Note: This process is probably best performed at night when there is less activity on site and less chance of disruption.
  1. Create the Competency.
  2. Initiate a Bulk Change for the necessary Cardholders with the new Competency.
     Result: All relevant cards will be updated, although there are no changes since Competencies have not been linked to the Access Zone yet.
  3. Add the Competency to the Access Zone, but leave it as "Not Enforced".
     Result: All relevant cards will be updated onto the Controller, and the Cardholders will still get access granted.
  4. "Enforce" the Competency on the Access Zone.
     Result: Only the Access Zone's configuration is sent to the Controller.
- An Access Group can be made "competency-exempt" for a specified Access Zone, which means that cardholders belonging to that Access Group will not be subject to ANY competency checks in order to enter that Access Zone, (e.g. escorted visitors).

Procedure

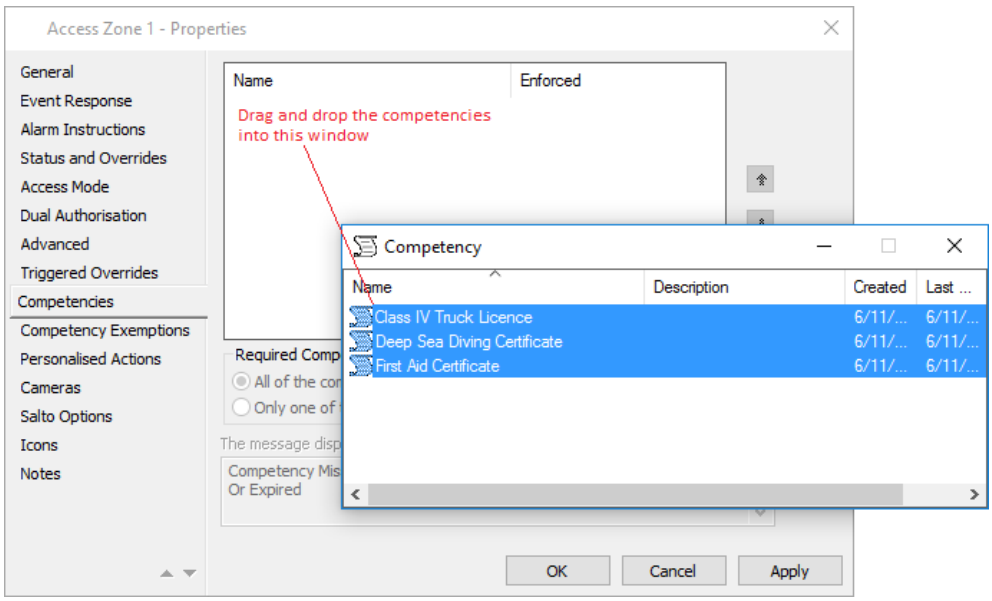
1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. **Right click** on the required Access Zone, and select **Properties**.
3. Click the **Competencies** tab.



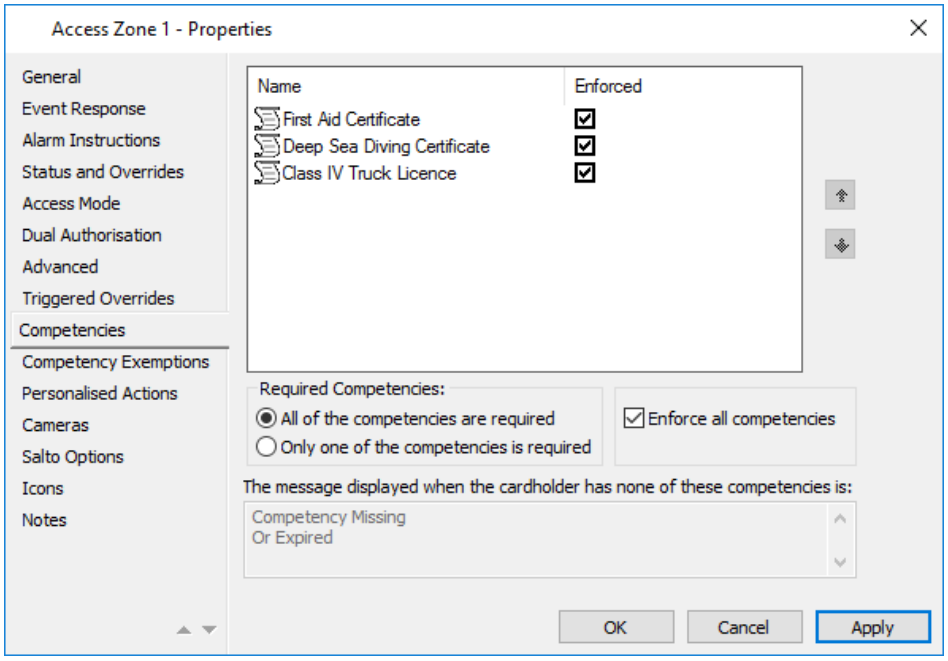
If this screen has not already had any competencies added to it, the **Required Competencies** section and the message text box below it are disabled. The **Required Competencies** section becomes enabled once a minimum of two competencies are added to the grid.

4. Click **Configure** from the menu bar, then **Competencies**.
   The **Competency** List Window opens.

5. Select those competency(s) you want to apply to this Access Zone. Drag and drop them into the grid on the **Competencies** tab.



6. Close the **Competency** List Window.
   Note: In the following example, the **Required Competencies** section has been enabled as a result of there being at least two competencies added to the grid.



By default, the **All of the competencies are required** radio button is selected, and all competencies are enforced, which means that anyone wanting access to the zone will be denied access if they do not have these competencies.

7. Click the **Only one of the competencies is required** radio button if you require this option rather than all competencies being required.
   The message text box below it becomes enabled, allowing you to alter the message that will display at any 'Message display device' that is required to show these messages, (i.e. HBUS Terminal or a secondary display via the Gallagher Controller API).
   Note: The message that displays is limited depending on the type of reader, as follows:
   - Gallagher HBUS Terminals = 2000 characters (one byte characters or Latin characters). Four lines of text are displayed. A user can access the remaining text by pressing the 'More' function key on the HBUS Terminal, then scrolling the message.
   - Secondary devices via the Gallagher Controller API can display the complete message entered.
8. Check/uncheck the **Enforced** checkbox for individual competencies as required, or alternatively use the **Enforce all competencies** checkbox if you want ALL the competencies to be enforced/not enforced.
   Note: If you chose the **Only one of the competencies is required** option, then either ALL of the competencies need to be enforced, or none of the competencies are to be enforced. If you try to apply your changes with individual competencies enforced/not enforced, the following error message will display:

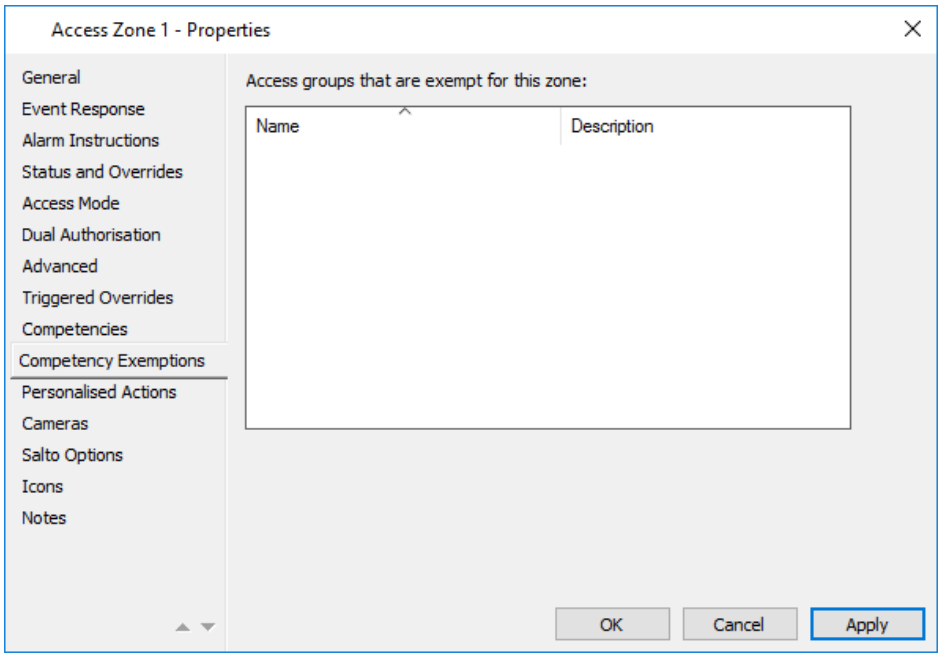
"If any competency is required to enter a zone then either all of the competencies must be enforced, or all of the competencies must be not enforced."

If...	then anyone wanting access to the zone will...
checked	be denied access if they do not have that competency, unless they are exempt, (i.e. they belong to an Access Group listed as exempt on the **Competency Exemptions** tab).
unchecked	not be denied access. However appropriate warnings and events are generated.

Note: The arrows to the side of the grid can be used to change the order of the competencies, (i.e. Select the competency you want to move and click either the up or down arrow to move the competency. This generates an event that indicates *"Changed: The order of competencies has changed"* on the **Details** tab of the Event properties window).
The order determines which competency warning will be displayed if several of the competencies are missing or expired. However, no matter what order competencies are prioritised in, if there is more than one competency due to expire, an "expiry due" notification will display for the expiry that is due to expire first.

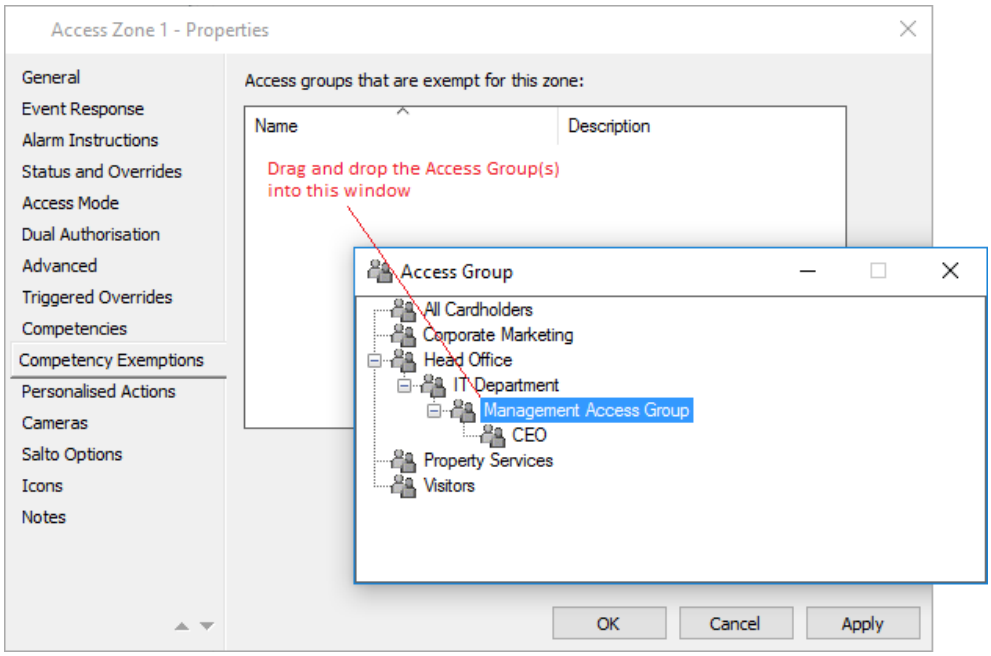
Additionally, competency expired messages for **Enforced** competencies take precedence over "expiry due" notifications.

9. Click the **Competency Exemptions** tab.



10. Click **Manage** from the menu bar, then **Access Groups**.
The **Access Group** List Window opens.

11. Select those Access Group(s) you want to be exempt for this Access Zone, (i.e. the members of the Access Group will have the ability to enter the Access Zone even if they do not have the required competencies).
    Drag and drop them into the grid on the **Competency Exemptions** tab.



12. Close the **Access Group** List Window.

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 competency(s) has been added to an Access Zone.

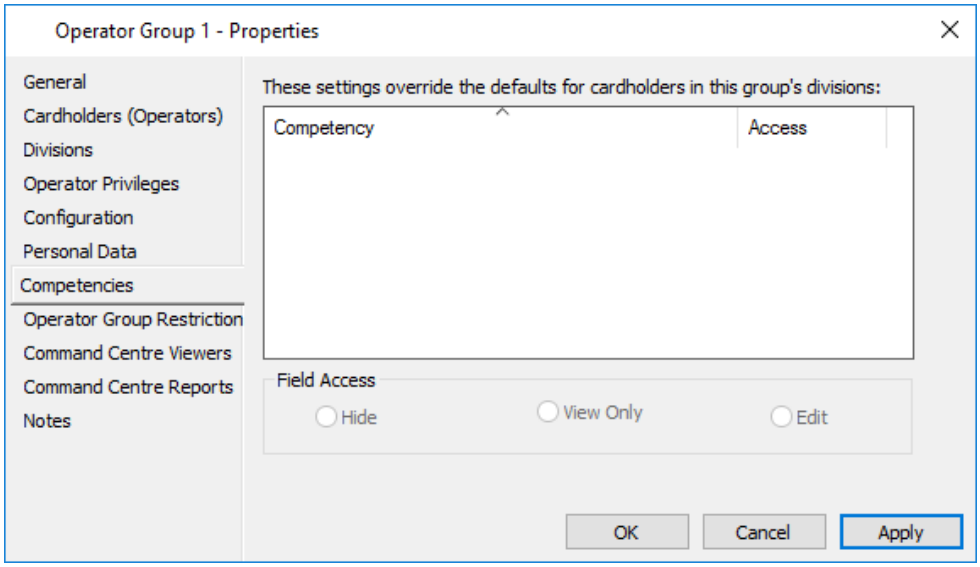
Overriding Operator Group Competencies

Introduction

This procedure describes how to override the default access of a competency for the operators in an Operator Group.

Procedure

1. Click **Manage** from the menu bar, then **Operator Groups**.
   The **Operator Group** List Window opens (in grid view).
2. **Right click** on the required Operator Group, and select **Properties**.
3. Click the **Competencies** tab.



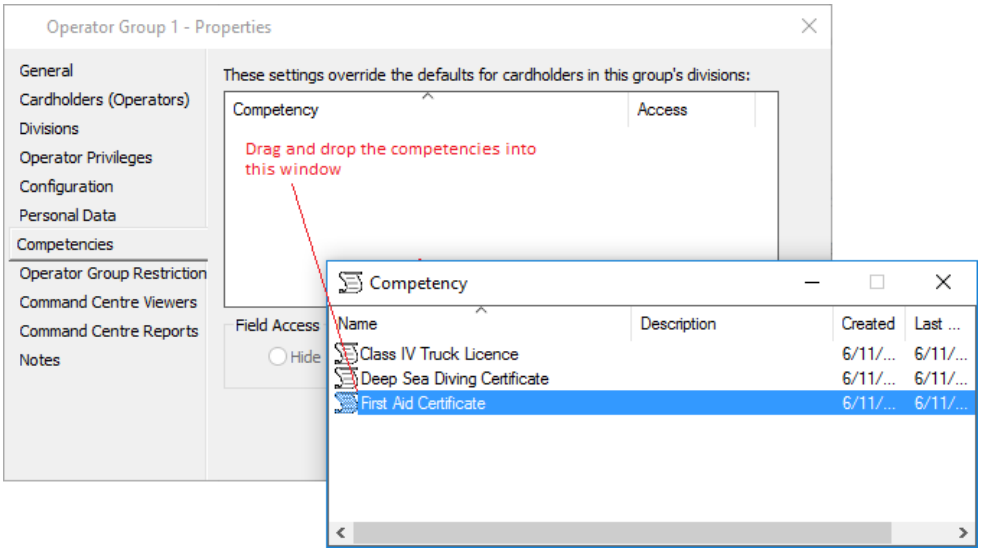
By default, this tab will not be populated with any competencies. Instead, this Operator Group will get the privileges for competencies that are assigned at the competency level. If you want to override the default privilege to something else, you can drag competencies onto this tab.

The level of operator privilege to view or edit cardholder information stored in a cardholder's competency is determined for individual competencies. The competency privileges only apply to cardholders in the Operator Group's Divisions (as configured on the **Divisions** tab).

The default operator privilege for each competency is determined when the properties of the competency are configured. The default operator privilege can be overridden for each competency by selecting a new option.

4. Click **Configure** from the menu bar, then **Competencies**.
   The **Competency** List Window opens.

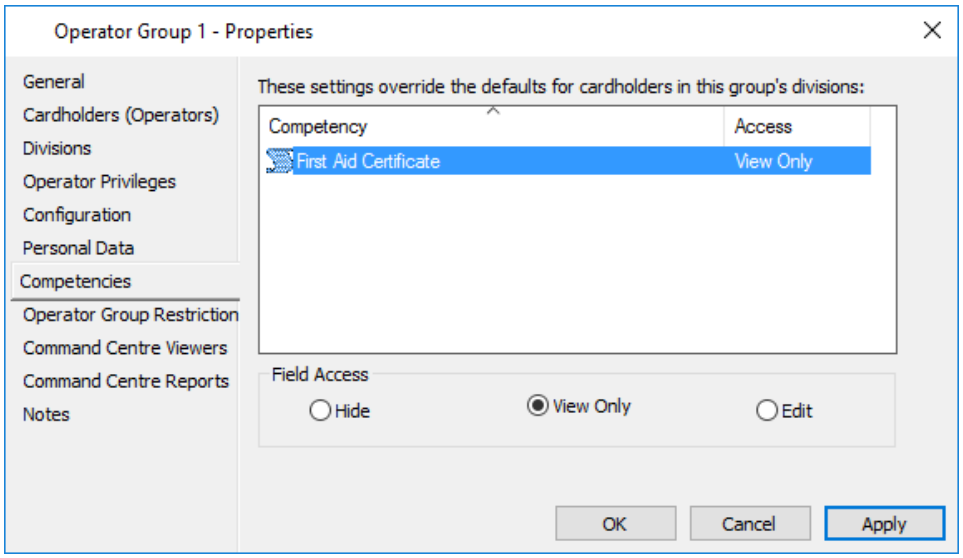
5. Select those competency(s) you want to assign a privilege to.
   Drag and drop them into the **Competencies** tab.



6. Highlight the competency you wish to determine the level of operator privilege for.
   The contents of the **Field Access** groupbox become enabled.

7. Click the radio button for the privilege you require.

Privilege	Description
Hide	Operators will not see the cardholder information recorded for this competency, for cardholders in the group's Divisions.
View Only	Operators will be able to view cardholder information for this competency, for cardholders in this group's Divisions.
Edit	Operators will be able to enter, view, change and delete cardholder information for this competency, for cardholders in this group's Divisions.



Note: To remove a competency privilege assigned to this Operator Group, **right click** on the competency and select **Remove from List**.

8. 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 default access of a competency for the operators in an Operator Group have been overridden.

Reporting on Cardholder Competencies

Introduction

This procedure describes how to run a Cardholder Report that includes Cardholder Competency details. Operators must have the "View Cardholders" and the "Edit Report Descriptions" privileges to create, save, edit and delete Cardholder Reports.

Notes:

Cardholder reports can be scheduled to run automatically at regular times (via a Macro). For further information refer to ***Automatically Generated Reports*** (on page 39-63) and ***Creating a new Macro*** (on page 20-2).

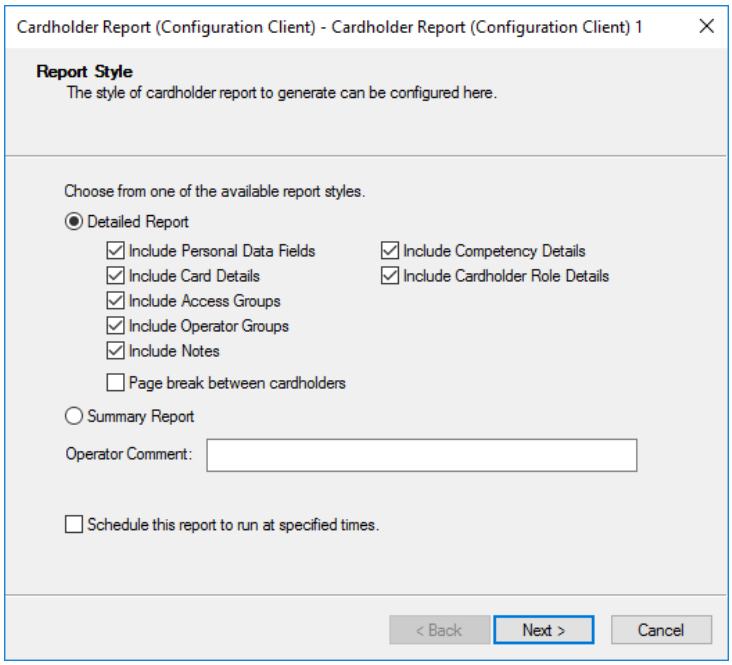
Detailed Cardholder Reports can also be run from:

- the Cardholder List Window. See ***Running a Cardholder Report from a Cardholder*** (on page 32-30) for further detail.
- the **Competencies** tab on the Cardholder properties. The competency options are selected by default using this method.
  See ***Assigning Competencies to cardholders*** (on page 52-12) for further detail.

Procedure

Click **Report** from the menu bar, then **Report Descriptions**.
The **Report Description** List Window opens (in grid view).

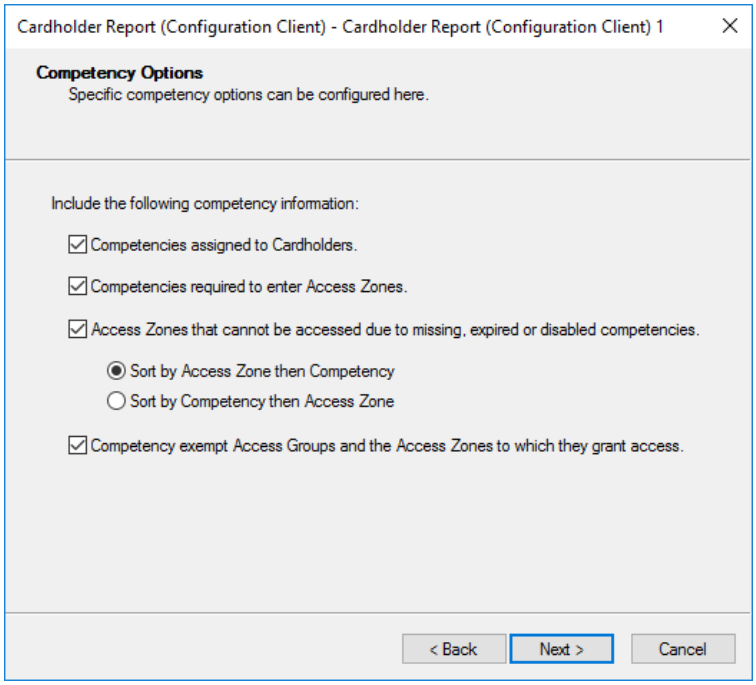
Right click and select **New...Cardholder Report**.
The "Report Style" screen of the Cardholder Report wizard displays, allowing you to select either a **Detailed** or **Summary** version of the report.



3. What style of the report do you want to run?

If...	then...
Detailed	check the **Include Competency Details** checkbox, (and any of the other checkboxes you require for the report), and click the **Next** button. Go to Step 4.
Summary	click the **Summary Report** radio button, then the **Next** button. Go to Step 6.

4. The "Competency Options" screen of the wizard displays, which allows you to specify the specific Competency information you wish to include in the report.



There are four options available, and by default they are all selected. Each option generates a separate section in the report as follows:

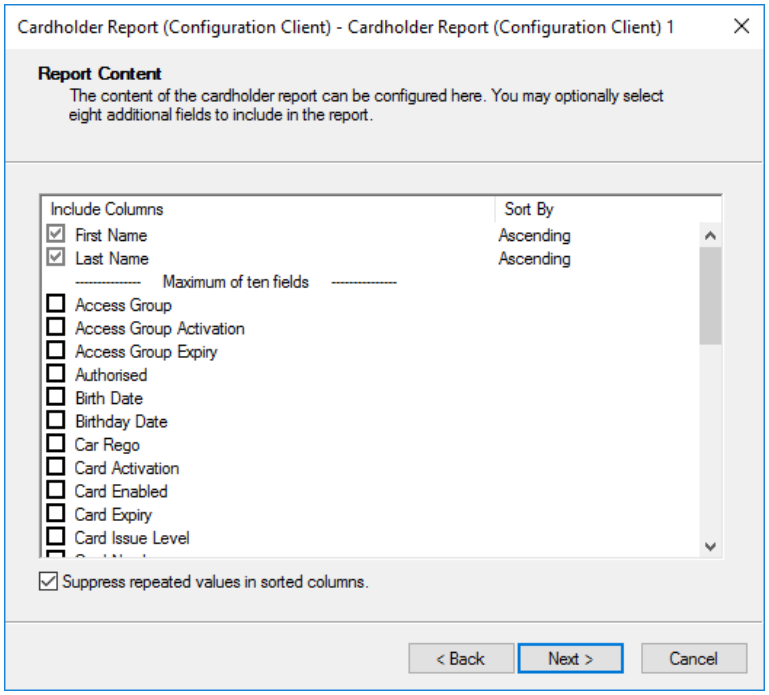
Competencies assigned to Cardholders
This option lists all competencies assigned to a Cardholder where the operator has view or edit access to the competency. This creates a table with the following columns:
a. Competency Name
b. Expiry Date
c. Notice Period (in days)
d. Expired (displays Yes = expired competencies; blank = non-expired competencies)
e. Disabled
f. Will Re-enable
g. Comment

Competencies required to enter Access Zones
This option lists competencies required to access each Access Zone that a Cardholder can otherwise access based on their Access Group memberships. This creates a table with the following columns:
a. Access Zone
b. Competency Name
Active Access Group memberships are determined based on the time the report is generated. Competencies are excluded where the operator does not have view or edit access. Each Access Zone with one or more Competencies that the operator cannot view includes the entry '{Privilege Restricted Competencies}'.

Access Zones that cannot be accessed due to...
This option lists Access Zones that can be accessed at the time the report is generated, based on Access Group memberships, but cannot be accessed based on held Competencies. This creates a table with the following columns:
a. Access Zone
b. Competency Name (only those that are preventing access)
c. Reason, (i.e. Missing, Expired or Disabled)
Competencies are excluded where the operator does not have view or edit access. Each Access Zone with one or more Competencies that the operator cannot view includes the entry '{Privilege Restricted Competencies}'. This table can be sorted by Access Zone and then Competency Name, or vice versa.

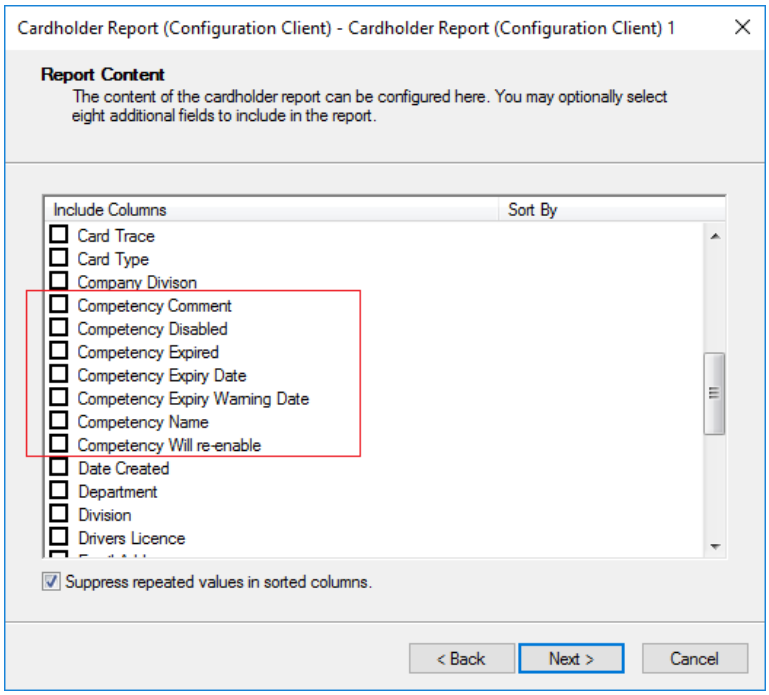
Competency exempt Access Groups
This option lists all Competency Exempt Access Groups to which a Cardholder belongs, and the Access Zones to which they provide access. This creates a table with the following columns:
a. Access Group
b. Access Zone (one or more per Access Group)
c. Schedule Access
The Schedule Access column displays 'No Access' when the Cardholder's Access Group memberships do not provide access to the Access Zone at the time the report is generated.

5. Check the option(s) you require, and click the **Next** button.
   Go to Step 13.
6. The "Report Content" screen of the wizard displays.

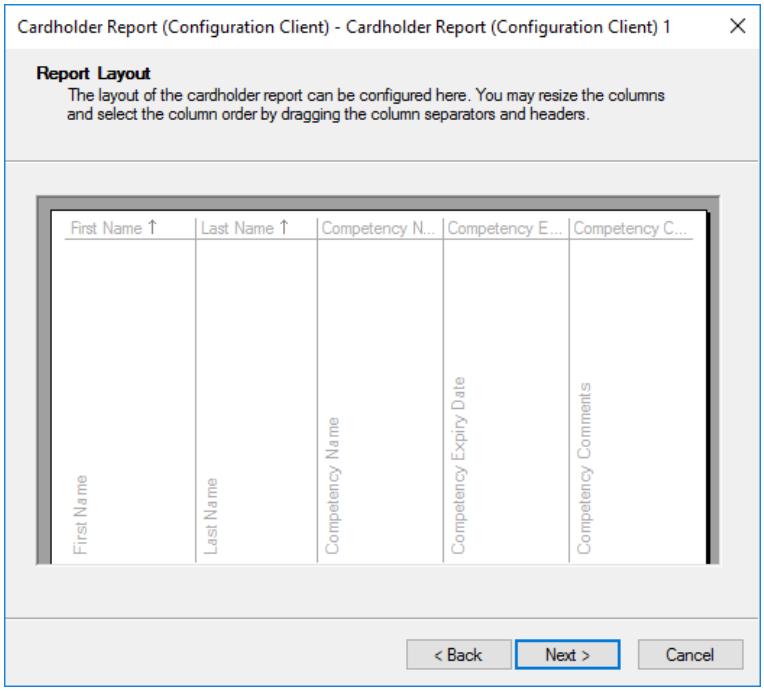


The **Summary Report** always includes the Cardholder's first and last names, but this screen allows you to select up to eight additional Cardholder fields (by marking them with a tick), from the list provided.

7. Scroll down the list to the Competency fields.



8. Select the Competency fields you want to include in the report, and click the **Next** button.
   The "Report Layout" screen of the wizard displays.



This page allows the operator to configure the layout of the report.

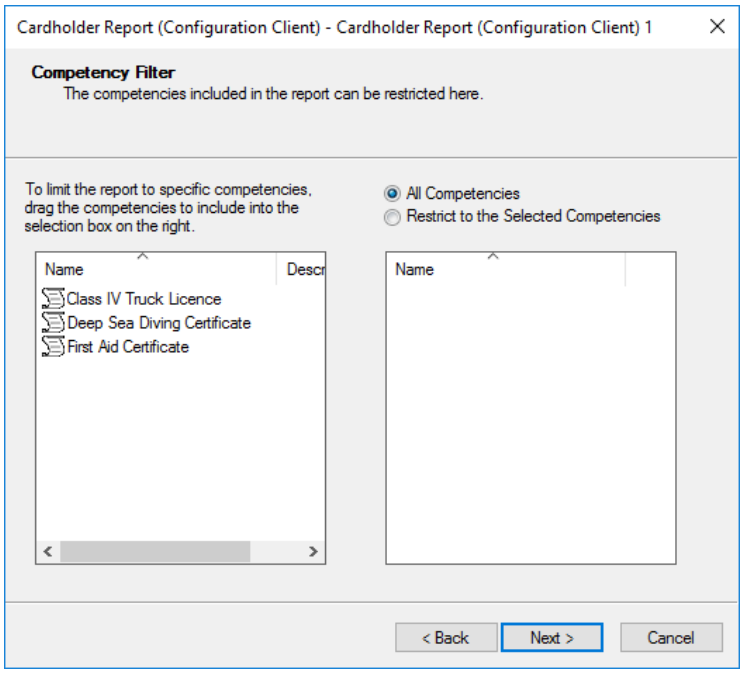
You can determine the position of the columns horizontally across the page, as follows:

a. Move the mouse pointer to the column header you want to reposition. The mouse pointer changes to a hand symbol.
b. Click and hold down the mouse button. The hand changes indicating it is grabbing the header.
c. Move the hand (and hence the column header) to the desired new position.
d. Release the mouse button.

You can also resize the width of the columns, as follows:

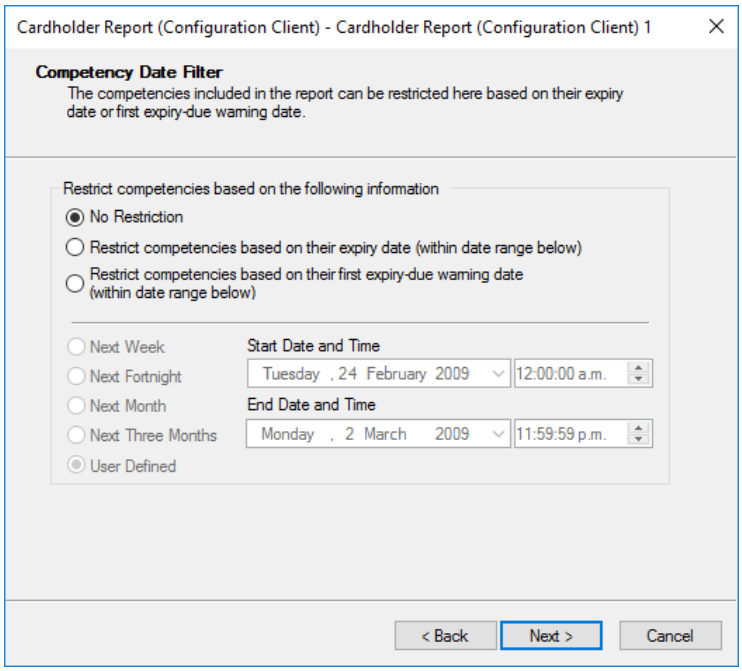
a. Move the mouse pointer to a column separator.
b. When the mouse pointer changes to a double-ended arrow ↔, drag the column separator in the required direction to achieve the desired column width.

9. Click the **Next** button.
   The "Competency Filter" screen of the wizard displays.



This screen provides a list of Competencies that an operator may include in the report. Competencies shown here are restricted to those under the Division of the operator.

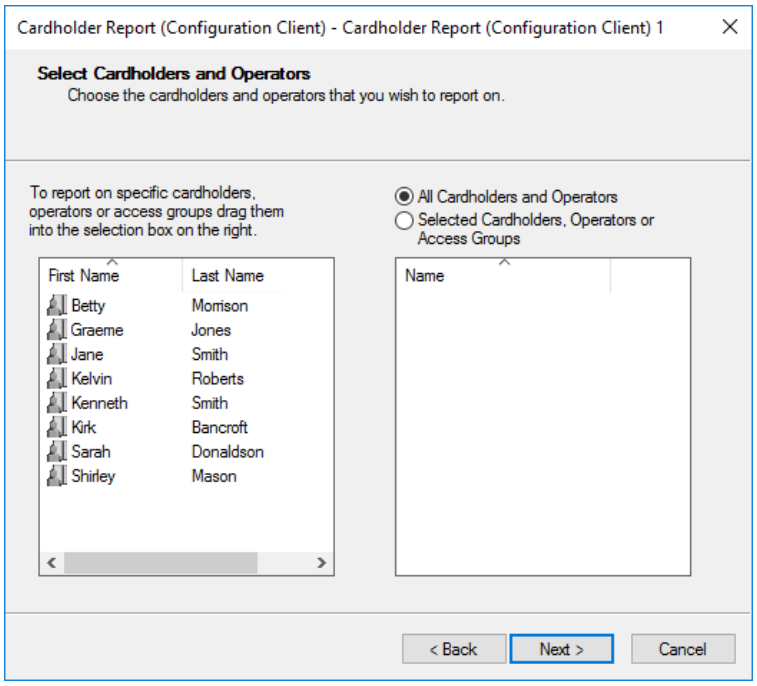
10. Select either **All Competencies**, or drag and drop those that you want included in the report from the left to the right-hand grid.
11. Click the **Next** button.
    The "Competency Date Filter" screen of the wizard displays.



This screen allows you to restrict the report to Competencies that have an expiry date or a first expiry-due warning date within an operator specified date range.

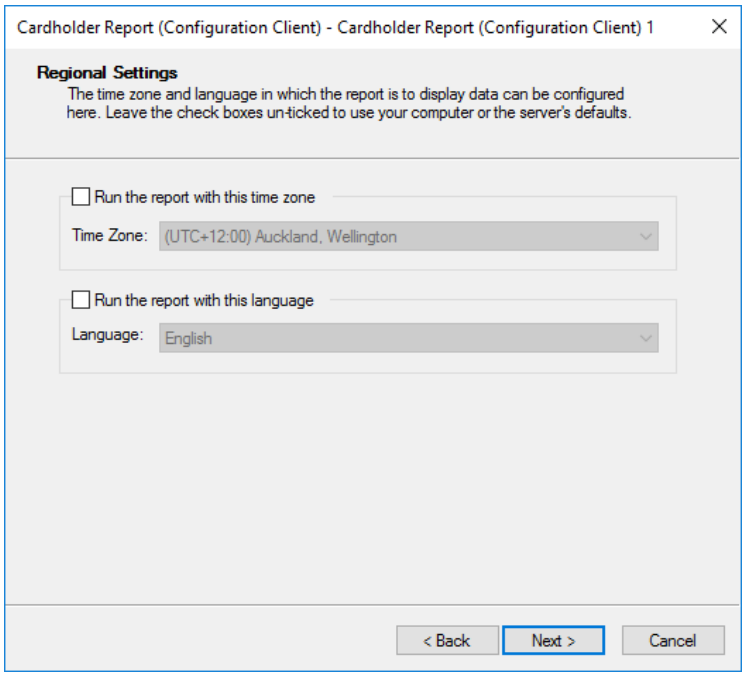
Note: By default, the "No Filter" option is selected. By leaving this selected, no restriction will be applied.

12. Make the selections you require, and click the **Next** button.
13. The "Select Cardholders and Operators" screen of the wizard displays.



This screen provides a list of Cardholders that may be included in the report. Cardholders shown here are restricted to those under the Division of the operator.

14. Select either **All Cardholders and Operators**, or drag and drop those that you want included in the report from the left to the right-hand grid.
    Note: Alternatively, you can open the Access Group List Window and drag and drop those Access Groups you require onto this screen.
15. Click the **Next** button.
    The "Regional Settings" screen of the wizard displays.



This page allows a time zone and/or language to be selected for the report. These options are specifically provided to support the Cardholder Report, (i.e. when the report is run via a macro on the server). Selection of a time zone is optional, as it is only required for Command Centre sites that span time zones. Selection of a language is also optional as it is only required for sites that have multiple languages.

If no time zone is selected, the report uses the time zone of the Command Centre server, only if the report was initiated from a macro which was triggered by an Action Plan, or a macro that was run from its schedule. In all other cases, the report uses the time zone on the workstation of the operator who has run the report, or the time zone on the workstation of the operator who ran the macro that triggered the report.

If a time zone is selected, when the report is run, all dates and times within the report will display in the selected time zone. Any dates and times configured within the report are assumed to be within the selected time zone (rather than the time zone on the configuring operator's workstation).

16. Click the **Next** button.
    The "Report Generation and Saving" screen of the wizard displays, which is the same for all report types, and provides the same options. Refer to ***Report Generation and Saving*** in the *Creating a new report* procedure (on page 39-3) for further detail.

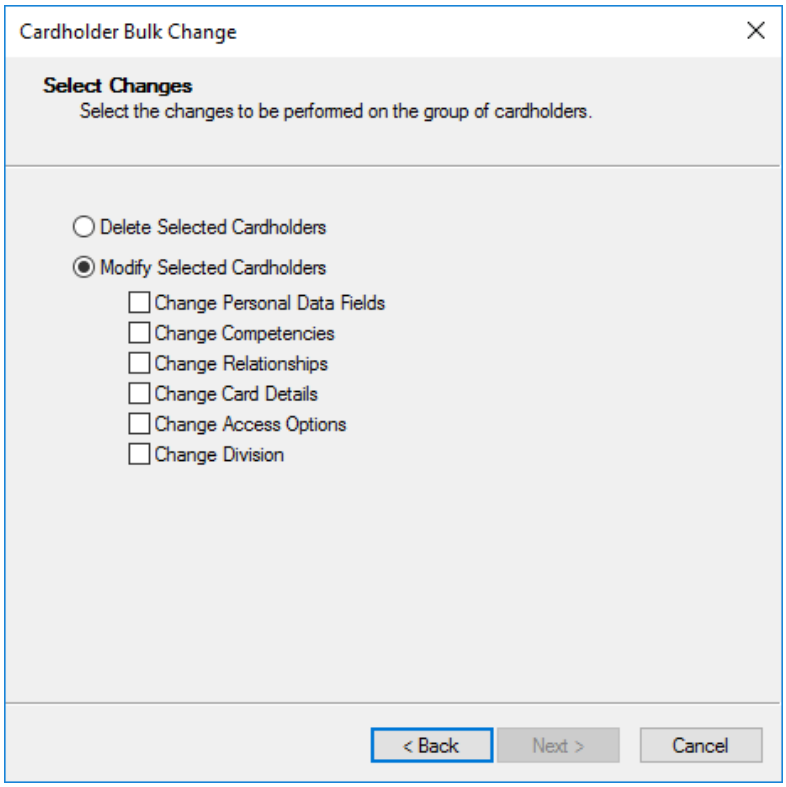
Competency Bulk Changes

Introduction

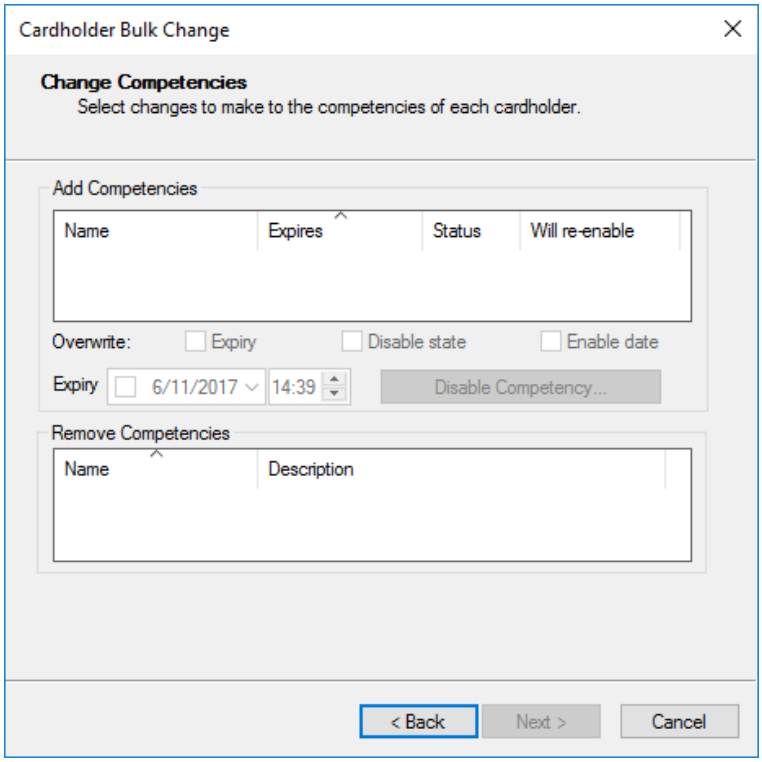
This procedure describes how to initiate a bulk change of cardholder competencies in Command Centre. To perform this procedure operator's need both the "Bulk Change" and "Edit Cardholders" operator privileges. In addition, operator's need sufficient divisional and other privileges to carry out each individual change listed within a bulk change.

Procedure

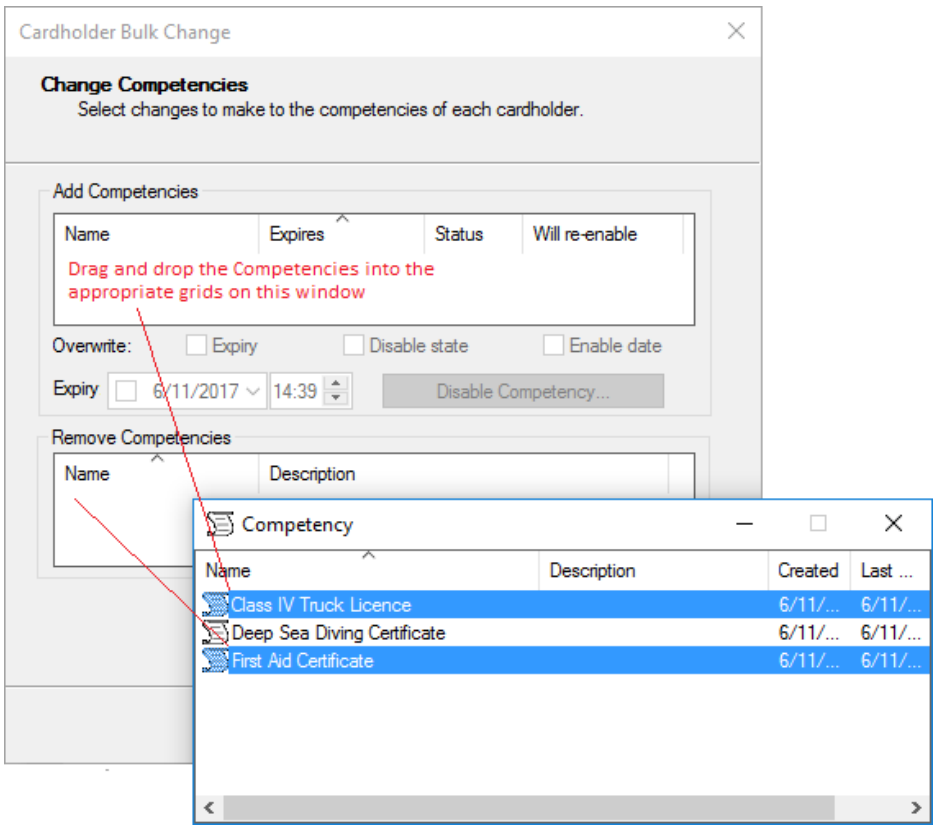
1. Perform Steps 1 - 4 of the ***Initiating a new Cardholder Bulk Change*** procedure (on page 38-3) and then go to Step 2 of this procedure.
2. Click the **Next** button.
   The "Select Changes" screen of the Cardholder Bulk Changes Wizard displays.



3. Click the **Modify Selected Cardholders** radio button, and tick the **Change Competencies** checkbox.
4. Click the **Next** button.
5. The "Change Competencies" screen of the Cardholder Bulk Changes Wizard displays.
   This screen allows you to select changes to make the cardholder competencies.



6. Click **Configure** from the menu bar, then **Competencies**.
   The **Competency** List Window opens.
   Select the Competencies that need adding to and/or removing from the cardholders, and drag and drop them into the appropriate grids on this screen of the Wizard, then close the **Competency** List Window.



7. In the "Add Competencies" section of this screen, each checkbox next to **Overwrite** indicates whether the values shown in the grid will override the appropriate field in the relevant cardholder competencies. If the **Expiry**, **Disable state** or **Enable date** are changed, the relevant checkbox is automatically checked.

   Note: For cardholders that do not have the competency, what the competency values are set to for those cardholders will show in the "Add competencies" grid.

8. If you want to disable a competency, select it and click the **Disable Competency...** button.
   The **Re-enable Competency** dialog displays, and the **Disable Competency...** button is replaced with the **Re-enable Competency** button. If the competency is not to be re-enabled at any time, click the **Never** radio button. However, if you want the competency to re-enable at a later date, use either the **In** control to specify the length of time until it will be re-enabled, or the **On** date and time control to set when it will be re-enabled.

   Note: When a disabled competency is selected, it can be re-enabled by clicking the **Re-enable Competency** button.

9. Click the **Next** button.

10. Return to the ***Initiating a new Cardholder Bulk Change*** procedure (on page 38-3) and perform Steps 28 - 31 to complete the bulk change.

Chapter 53: Guard Tours

Guard Tours, which is a licensable feature, is a sequence of checkpoints that a guard must visit in the designated order.

In a multi-server system:

- All Guard Tour specific functionality is limited to the local server only.
- Any alarms resulting from a Guard Tour will be provided to the multi-server environment.

Licensing

Guard Tours functionality is a licensable feature. The license file must contain the following option:

```
[Features]
Guard Tours=1
```

Select the item below that you require further detail on:

- ***Creating a new Guard Tour*** (on page 53-2)
- ***Running a Guard Tour*** (on page 53-6)
- ***Creating a Guard Tour Report*** (on page 53-10)

Creating a new Guard Tour

Introduction

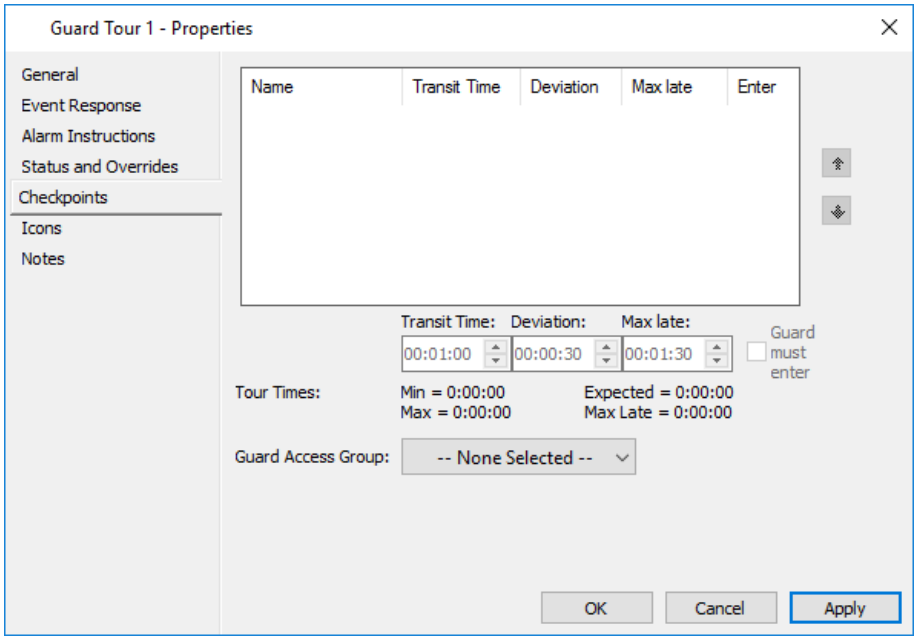
This procedure describes how to create a Guard Tour.

Operator Privileges

To...	you require the...
• view the details of the guard tour, (e.g. the checkpoints on the tour, their sequence and the timing that the guard must adhere to if they are not to trigger alarms) • view the priority assigned to each type of Guard Tour alarm and to see which guards are allocated specific Guard Tours	"View Guard Tours" privilege in the appropriate division.
• create, edit and delete the details of a Guard Tour, including the checkpoints on the tour, their sequence and the timing that the guard must adhere to if they are not to trigger alarms • assign the priority for each type of Guard Tour alarm and to allocate guards to specific Guard Tours	"Edit Guard Tours" privilege in the appropriate division.

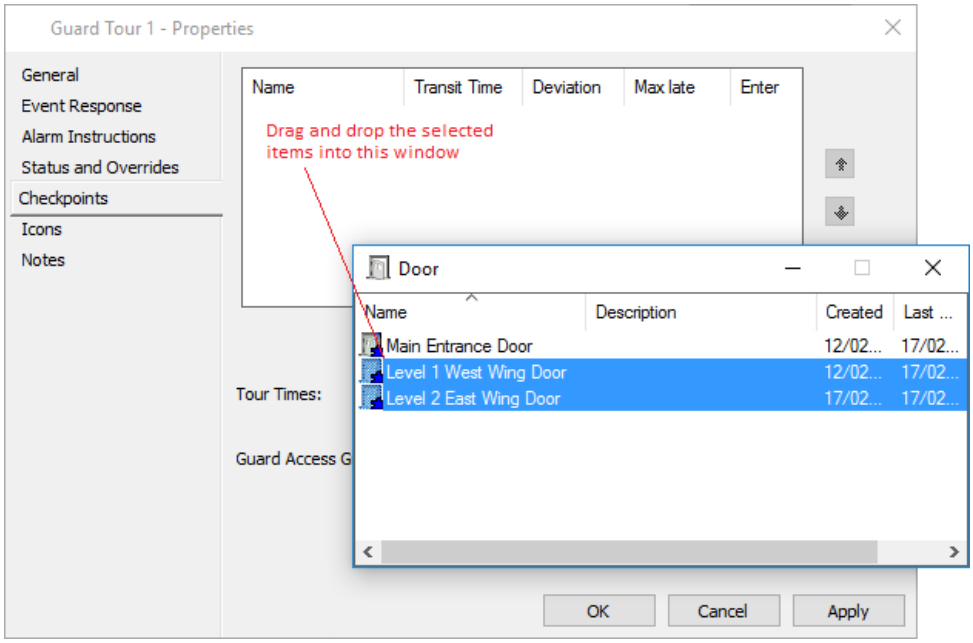
Procedure

1. Click **Configure** from the menu bar, then **Guard Tours**. The **Guard Tour** List Window opens (in grid view).
2. **Right click** and select **New...Guard Tour**.
   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 **Checkpoints** tab.



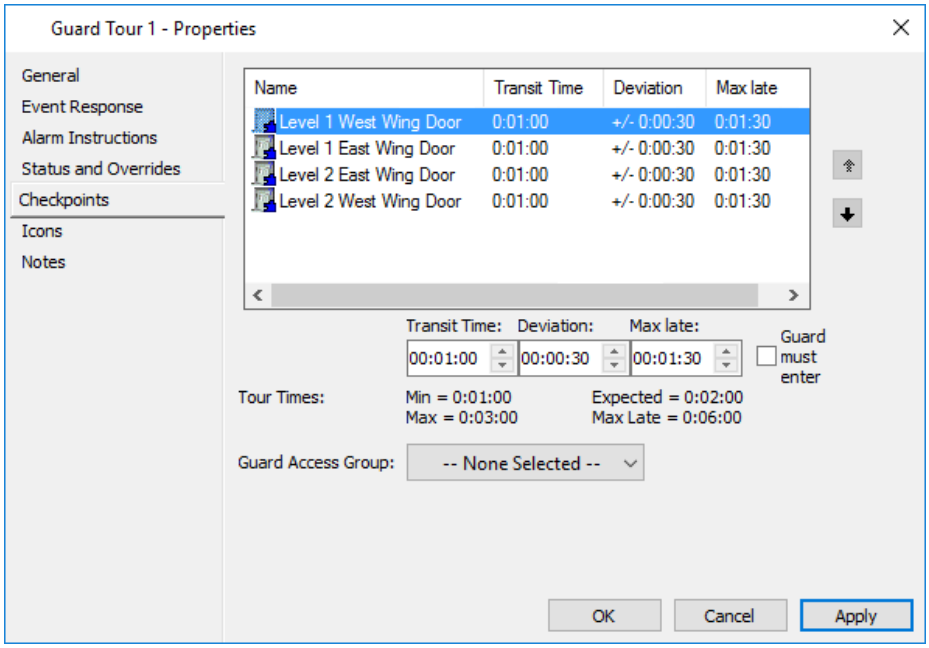
Doors, Inputs, Outputs, Logic Blocks, Aperio Doors and External System Items can be added to a Guard Tour as checkpoints. Note that each item needs to create an event in order for the Guard Tour to continue, (e.g. In the case of an input, an Alarm Zone will need to be assigned to the input with an Action Plan that logs an event when it triggers).

7. Open the List Window that contains the item required as a checkpoint in this Guard Tour.
   For example, open the **Door** List Window.
8. Select the required item(s).
   Drag and drop them into the **Checkpoints** tab.



9. Repeat Steps 7 and 8 for all items to be included as checkpoints.
10. Sort your selection of checkpoints by clicking on one and using the arrow

buttons to the right of the grid to move it.
The order you define here will be the order in which a guard must visit the checkpoints.



11. Highlight a checkpoint in the grid, and configure the timing parameters for it as follows:

Field	Description
Transit Time	The period of time (in hours, minutes and seconds), it should take a guard to move from the last checkpoint to this checkpoint. (Default = 00:01:00. Allowable range = 00:00:01 to 23:59:59)
Deviation	The maximum allowable deviation (in hours, minutes and seconds). (Default = 00:00:30. Allowable range = 00:00:01 to 23:59:59)
Max late	Maximum late time, in hours, minutes and seconds. (Default = 00:01:30. Allowable range = 00:00:00 to 23:59:59)

12. If a guard is required to enter the Access Zone related to the checkpoint, check the **Guard must enter** checkbox.
13. Repeat Steps 11 and 12 for each checkpoint.

14. Select the Access Group that your guards belong to from the **Guard Access Group** drop-down list.
    Note: Any cardholder in the selected Access Group can be assigned to the Guard Tour. For this reason, it may be helpful to create an Access Group specifically for guards. That way, when a Guard Tour is run, the Access Group acts as a filter and only guards will appear in the **Guard** drop-down list.
15. Click the **Icons** tab if you want to change the Icon Set for this Guard Tour. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
16. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Guard Tour.
    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 Guard Tour. 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.

Result

A new Guard Tour is configured.

Hints

Editing and Deleting Guard Tours
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Guard Tours.
Note: The system will not allow the deletion of a Guard Tour when it:
- is currently running,
- appears on a Site Plan, or
- is used in a Macro

Additionally, the Access Group, or a checkpoint assigned to a Guard Tour cannot be deleted without the tour being deleted, or the item first being removed from the tour.

Copy and paste
An alternative to the drag and drop method is to use the copy and paste method.

Running a Guard Tour

Introduction

A previously configured Guard Tour can be selected by an appropriately privileged operator, assigned to a guard and started at any checkpoint in the tour.

This procedure describes how operators with the "Manage Guard Tours" privilege can start, stop and restart a Guard Tour.
Notes:

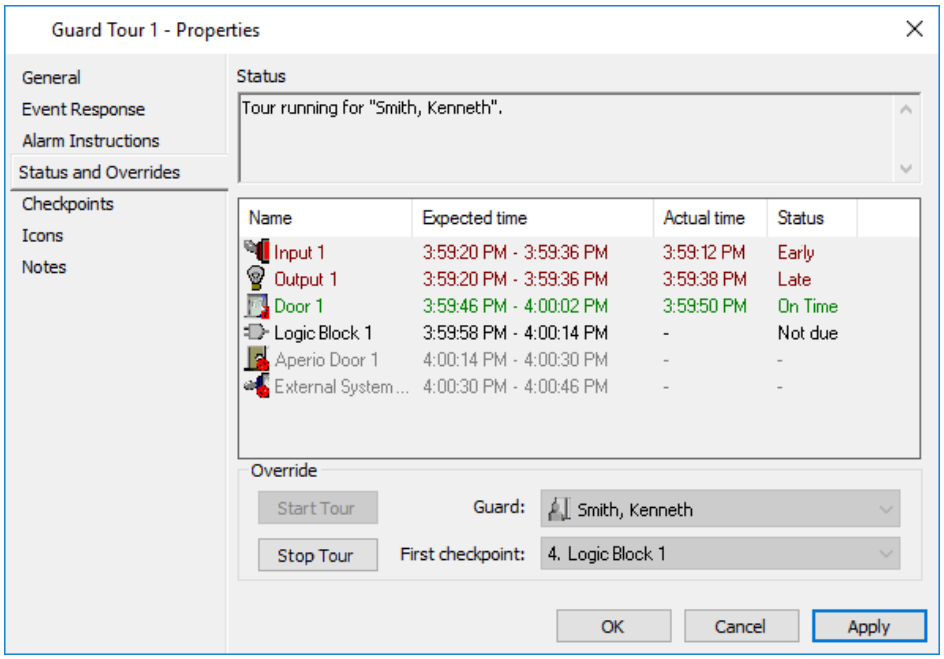
- The "Manage Guard Tours" privilege also includes the "View Guard Tours" privilege, which allows operators to view the details of a Guard Tour.
- A Macro item can be used to trigger Guard Tours actions, (e.g. a macro can be used to start more than one Guard Tour item at once, or stop them at once). See Creating a new Macro for further detail.

Procedure

Starting a Guard Tour

1. Click **Monitor** from the menu bar, then **Guard Tours**.
   The **Guard Tour** List Window opens (in grid view).
2. **Right click** on the Guard Tour you want to run, and select **Start Tour...** from the drop-down menu.
   The **Status and Overrides** tab of the Guard Tour properties displays, with the Status *"Tour not running"*.
3. Select the guard that is responsible for performing the tour from the **Guard** drop-down list.
   The **Start Tour** button becomes enabled.
   Notes:
   - The **Guard** drop-down list is populated with all cardholders viewable to the operator and belonging to the Access Group assigned to the tour on the **Checkpoints** tab.
   - If the guard you select is already allocated to another Guard Tour, they will not be able to be allocated to this tour whilst the original tour is in progress.
4. Select the checkpoint you want the tour to start at from the **First checkpoint** drop-down list.
   Note: The **First checkpoint** drop-down list is populated with all the checkpoints for the tour in order. It is updated to the current checkpoint each time a checkpoint is reached during the tour, and is reset back to the first checkpoint upon the tour completing. Thus if the tour is halted for some reason, an operator can simply click the **Start Tour** button to resume the tour from the checkpoint it was last up to.

5. Click the **Start Tour** button.



The Status changes to *"Tour running for [Guard name]"*, and all the checkpoints on the tour display in sequence, with updates occurring dynamically as each checkpoint is reached, including the due and when appropriate overdue status of the next checkpoint. The appropriate update to the Status column occurs as follows:

Status column	Description
-	For checkpoints that are after the current checkpoint.
Not due	For the current checkpoint when the expected minus deviation time has not been reached yet.
Due	For the current checkpoint when the current time is between the expected time plus or minus the deviation time, (i.e. in the time range specified in the **Expected time** column).
Overdue	For the current checkpoint when the expected plus deviation time has been exceeded.
Halted	When the tour was aborted at this checkpoint. The tour was either: - manually stopped, - the guard did not arrive, or - the guard arrived at the wrong checkpoint.
Early	When the guard arrived early to this checkpoint.
On Time	When the guard arrived on time to this checkpoint, (i.e. in the time range specified in the **Expected time** column).
Late	When the guard arrived late to this checkpoint.

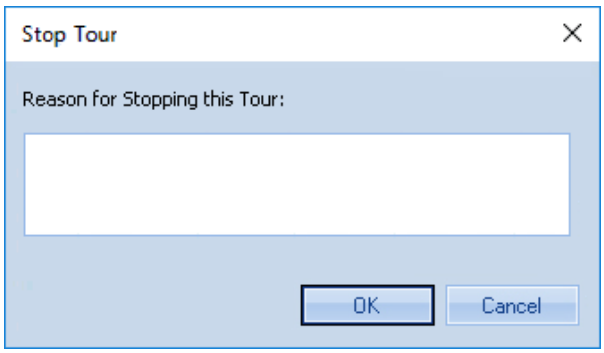
Stopping a Guard Tour

Perform the following steps to manually stop a Guard Tour that is "In Progress" from a workstation:
Note: As well as an operator being able to stop ("Halt") a tour, they can also be stopped due to an alarm.

1. Do you already have the Guard Tour properties open on the **Status and Overrides** tab?

If...	then...
yes	go to Step 2.
no	**a)** From the **Guard Tour** List Window, **right click** on the Guard Tour you want to run. **b)** Select **Stop Tour...** from the drop-down menu. The **Status and Overrides** tab of the Guard Tour properties displays, with the Status *"Tour running for [Guard name]".*

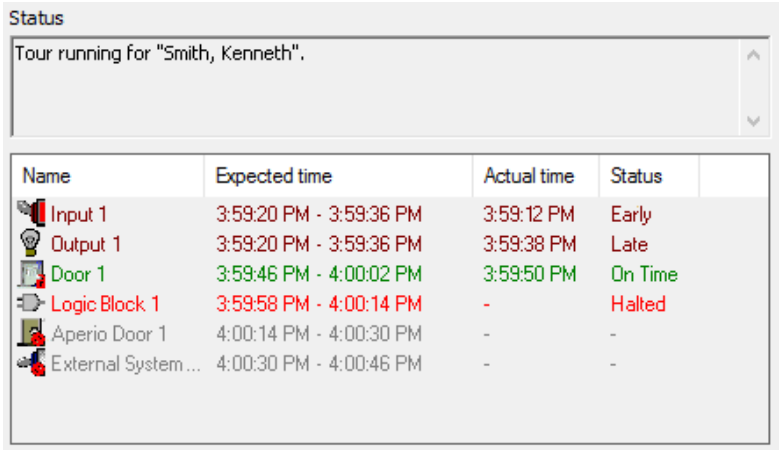
2. Click the **Stop Tour** button.
A "Stop Tour" dialog displays.



3. Do you want to enter a reason for stopping the tour?

If...	then...
no	click the **OK** button.
yes	enter the reason (up to 200 characters) and click the **OK** button. This message will be logged as part of the event generated to record your action.

The Status changes to *"Tour Halted"* and the "current" checkpoint changes to red text.



Restarting a Guard Tour

Perform the following steps to restart a Guard Tour in the "Halted" state:
Note: It can be restarted from the "current" checkpoint, (i.e. the one that has the "Halted" state), or from any other checkpoint including the first checkpoint.

1. Do you already have the Guard Tour properties open on the **Status and Overrides** tab?

If...	then...
yes	go to Step 2.
no	**a)** From the **Guard Tour** List Window, **right click** on the Guard Tour you want to restart. **b)** Select **Start Tour...** from the drop-down menu. The **Status and Overrides** tab of the Guard Tour properties displays, with the Status *"Tour Halted".*

2. Select any checkpoint as the "First checkpoint" to restart the tour, from the **First checkpoint** drop-down list.
3. Click the **Start Tour** button.
The Status changes back to *"Tour running for [Guard name]"*, and updates start occurring again for all the checkpoints on the tour as they are reached.

Creating a Guard Tour Report

Introduction

The Guard Tour Report is a tool for reporting events and alarms that occur during each initiated Guard Tour. It shows:

- the time the guard reached each checkpoint,
- times taken between check points,
- any anomalies, (e.g. early or late arrival at a checkpoint, and arriving at a checkpoint out of sequence), and
- alarm acknowledgement and processing of alarms relevant to each Guard Tour.

This procedure describes how to create a Guard Tour Report.
Notes:

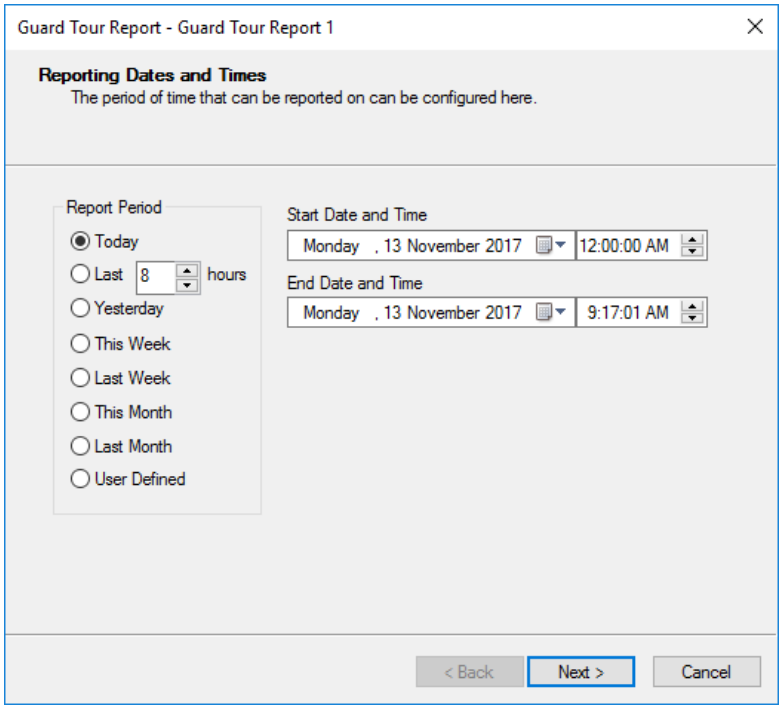
- A Guard Tour Report can be scheduled to run automatically at regular times (via a Macro). For further information refer to Automatically Generated Reports and Creating a new Macro.
- In a multi-server environment, for any given server where event aggregation is enabled, an operator can run a Guard Tour Report which incorporates events from remote guard tours. The Guard Tour Report can be filtered by remote guard tours.

Site Configuration Report

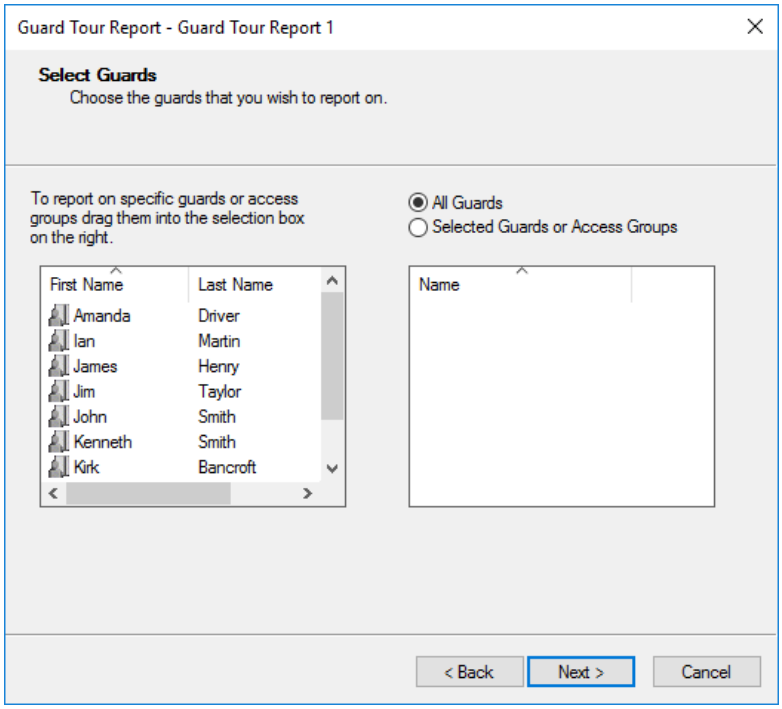
A Guard Tour Site Configuration Report can be run to provide a printed list of checkpoints for a security guard to follow on a specific tour route and indicate expected times. The report can be run in a way that eliminates all other site configuration report data, and displays only the relevant Guard Tour details. For further detail see Site Configuration Report.

Procedure

1. Click **Reports** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
2. **Right click** and select **New...Guard Tour Report**.
   The **Reporting Dates and Times** page of the Guard Tour Report wizard displays.

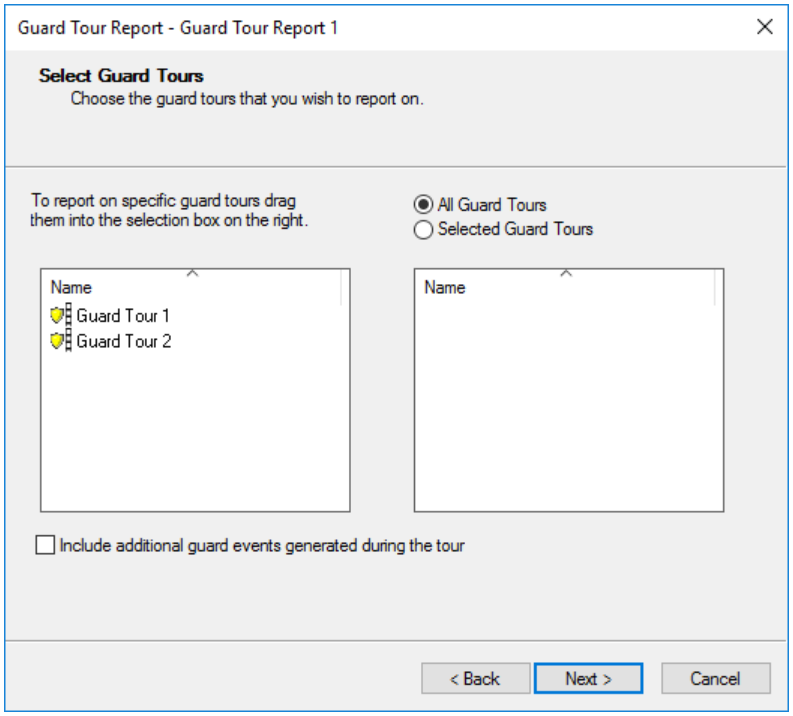


3. This page allows you to enter a start and end time for the report. Pre-defined periods are provided for simplicity, or custom start and end times can be entered.
4. Configure the period required for the report, and click the **Next** button. The **Select guards** page displays.

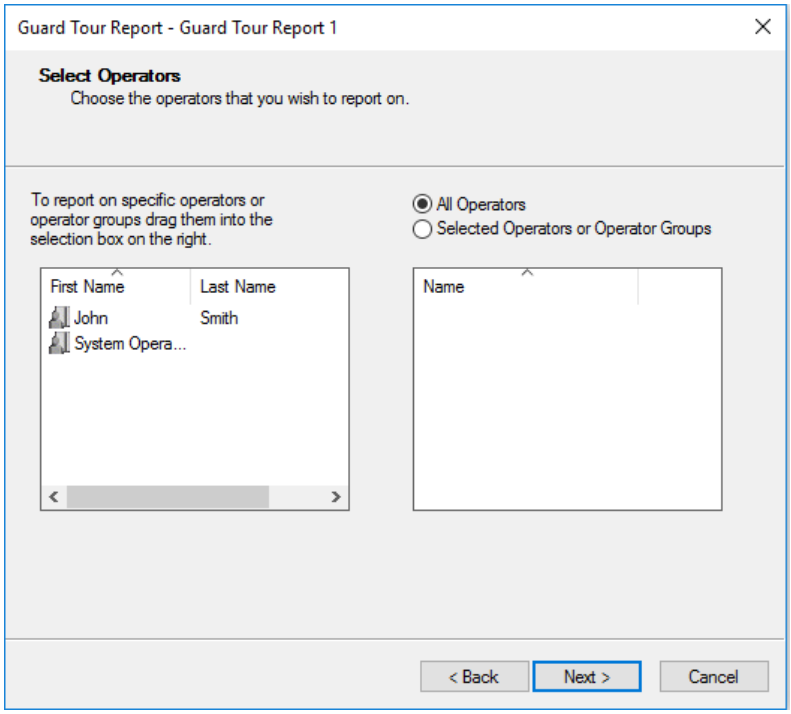


This page provides a list of Cardholders (Guards) that may be included in the report. Cardholders shown here are restricted to those under the Division of the operator. The report will filter on the Cardholder (Guard) that performs the tour. All or multiple cardholders can be selected.

5. Select the Cardholders (Guards) you want to include.
   Notes:
   - The Find Tool may be used to locate guards, which can then be dragged and dropped onto this page. Alternatively, you can open the **Access Group** List Window and drag and drop those Access Groups you require onto this page.
   - Should you wish to delete a Cardholder (Guard) or Access Group from your list on the right, **right click** on the item and click **Remove from List**.
6. Click the **Next** button.
   The **Select Guard Tours** page displays.



   This page provides a list of all the Guard Tours that may be included in the report. Guard Tours shown here are restricted to those under the Division of the operator. All or multiple Guard Tours can be selected.
   Note: In a multi-server environment, for any given remote server with event aggregation enabled, remote Guard Tours can be selected.
7. Select the Guard Tours you want to include.
8. If you want any events or alarms that the guard generates that are not related to the Guard Tour's checkpoints to be included in the report, check the **Include additional guard events generated during the tour** checkbox. When such events are reported on, they will be clearly separated and labelled "Additional guard events during tour".
9. Click the **Next** button.
   The **Select Operators** page displays.



10. This page provides a list of operators that initiate tours and may be included in the report. Operators shown here are restricted to those under the Division of the operator running the report.
    All or multiple operators can be selected. The report will be filtered by Guard Tours started by the selected operators.
11. Select the Operators you want to include, and click the **Next** button.
    The **Report Generation and Saving** page displays. This wizard page is the same for all report types, and provides the same options. Refer to ***Report Generation and Saving*** in the *Creating a new report* procedure (on page 39-3) for further detail.

Chapter 54: Enterprise Data Interface

Introduction

Enterprise Data Interface provides the ability to import cardholder data or booking data (timetable data) into Command Centre. Data can be imported from either a source file or a database.

A Cardholder Interface can be configured in Enterprise Data Interface to add, update or remove cardholders in Command Centre.

A Booking Interface can be configured in Enterprise Data Interface to update bookable resources configured in Command Centre.

Note: The Booking Interface option will only be available if your site has the "Bookable Resources" licensable feature installed also.

In order to configure an interface, source data fields must be mapped to Gallagher Command Centre fields. Once configured, an interface can be run manually (at any time), run according to a schedule or run in sequence.

Licensing

Enterprise Data Interface is a licensed feature of Gallagher Command Centre. The following table details the licensing structure:

License entry	is required when...
`EnterpriseDataInterface=1`	importing cardholders from a file.
`ScheduleEnterpriseDataInterface=1`	scheduling an interface or adding an interface to an execution sequence.
`EDI-CardholderDatabase=1`	importing cardholders from a database.
`EDI-BookingDatabase=1`	importing bookings from a database.
`EDI-BookingFile=1`	importing bookings from a file.

Supported Databases

Enterprise Data Interface supports importing data from the following databases:

- Oracle Database Express Edition 19c

  Note: If you want to use the Oracle Database feature you will need to perform the following procedure, otherwise Command Centre will fail to connect to the Oracle Database using EDI:

  1. Navigate to `C:\Program Files (x86)\Gallagher\Command Centre\Bin`.
  2. Back up **Oracle.ManagedDataAccess.dll** into another folder in the filesystem.
  3. Stop Command Centre services.
  4. Copy **Oracle.ManagedDataAccess.dll** (v4.122.19.1) into `C:\Program Files (x86)\Gallagher\Command Centre\Bin`, overwriting the existing file.
  5. Start Command Centre services.

  Try entering the server name as SERVER/SERVICE.

  If the data point is named DATA and the server is Orastage, in EDI the server would be listed as Orastage/DATA, and if they are using a custom port, (e.g. 4443), then the server would be Orastage:4443/DATA.
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2014

Configuring operators

Operator Privileges

Assign the appropriate privileges to Gallagher Command Centre operators.

Privilege	is required to...
"Edit Enterprise Data Interfaces"	view, add, edit, save, delete, enable, disable, find or manually run interfaces. This privilege should be assigned to the root division of the operator group, this operator is in. An operator with this privilege can view all PDFs (including hidden and view only), Card Types, Access Groups, Competencies and Relationships in the Edit Mappings window.
"Run Enterprise Data Interfaces"	view, find or manually run interfaces.

Notes:

- An operator with the "View Site" privilege is unable to view interfaces.
- An operator with the "Advanced User" privilege can edit and manually run interfaces.

"Run as Operator" Privileges

When an interface is run, it is run under an operator's name. This operator is referred to as the "Run as Operator". All actions performed by the interface are logged under this operator's name.

It is recommended that you create a "Run as Operator" whose sole purpose is to run all interfaces. This operator will need to be assigned the appropriate privileges in order to perform the actions specified by each interface.

Privilege	is required to...
"Create Cardholders" and "Edit Cardholders"	create and/or change cardholders
"Edit Cardholder Notes"	create and/or change a cardholder's notes
"Delete Cardholders"	delete cardholders
"Modify Access Control"	set cardholder access groups
"View Site"	view competencies

Configuring an interface

Introduction

The following process is recommended so you can complete each procedure in the correct order when configuring an interface for your site.

Configuration Process

This list can be used as a checklist to ensure you have configured all the necessary components for an interface.

✓	Procedure
☐	Generate source data
☐	Configure Gallagher Command Centre to receive source data
☐	Configure an interface: • Create the interface • Schedule or sequence an interface (if appropriate) • Define the source data location • Define the source data format • Set the "Run as Operator" • Map source fields to Gallagher Command Centre fields
☐	Enable the interface

Generating source data

Introduction

The source data for a Cardholder Interface should contain the cardholder records you wish to add, update or remove in Command Centre. The source data for a Booking Interface should contain the bookings for the bookable resources in Command Centre.

The source data must originate from either a source file, (e.g. CSV file) or a database (Oracle or Microsoft SQL Server).

Enterprise Data Interface folders

When importing data into Command Centre you will need to create the appropriate folders, as detailed in the following topics. It is recommended that you create one set of folders for the Cardholder Interfaces and another set of folders for the Booking Interfaces.
Note: In new installs of the Command Centre service account ("Network Service"), modify access permission must be granted to the Source, Image, Completed and Failed folders. This also applies to updates from versions prior to vEL7.70 where "Network Service" has been selected on install.

Importing data from a source file
If the source file is located on the local Command Centre server PC, you will need to create the following folders on the local Command Centre server PC.

If the source file is located on a remote PC, you will need to create the following folders on the remote PC. The remote PC must be setup and made available to the Command Centre server PC.

The interface will "pick-up" and process the source file from the source folder directory.
Notes:

- It is recommended you name the folders as shown below.
- It is recommended that your company limits access to these folders, only allowing certain people or services access to the folder locations.
- The image folder is not required for a Booking Interface.

Folder Name	Description
Source	This is where the interface will retrieve the source file from.
Completed	This is where the processed source file will be moved to, regardless of success.

Folder Name	Description
Failed (optional)	The unsuccessfully imported cardholder records will be copied to a new file and placed in this folder. If this folder does not exist, the failed file will be placed in the completed folder.
Image (optional)	This is where the interface will retrieve the cardholder images from. The successfully imported images will be moved to the completed folder. Images that have failed to be imported or are not specified in the source file will remain in this folder. It is recommended that you supply only the images that require importing to this folder, not images that have already been imported. This will show you what was not processed by Enterprise Data Interface. If you are not importing images, this folder is not required.

Importing from a database

If the source data is located in a database, you will need to create the following folders on the local Command Centre server PC.

Note: The image folder is not required for a Booking Interface.

Folder Name	Description
Log	The import log file will be saved to this directory.
Image (optional)	This is where the interface will retrieve the cardholder images from. The successfully imported images will be moved to the processed folder. The processed folder resides in the image folder directory. If not already present, the processed folder is automatically created when the interface is run. Images that have failed to be imported or are not specified in the source data will remain in this folder. It is recommended that you supply only the images that require importing to this folder, not images that have already been imported. This will show you what was not processed by Enterprise Data Interface. If you are not importing images, this folder is not required.

Importing cardholder images

Introduction

Cardholder images can be imported into Gallagher Command Centre via the Cardholder Interface only. A cardholder's image could be a photograph or scanned signature, etc.

Process

Enterprise Data Interface imports cardholder images by matching the image name in the source field with the image name in the image folder. If a match is successful the image is imported.

When importing from a source file, the imported images are moved from the image folder to the completed folder. When moved to the completed folder, if the image already exists, it will be overwritten.

When importing from a database, the imported images are moved from the image folder to the processed folder. The processed folder resides in the image folder directory. If not already present, the processed folder is automatically created when the interface is run.

If the source field specifies an image and the image is not in the image folder, the cardholder will be updated, but not the image. An alarm is raised to show that the interface "processed with failures". The alarm details will show the import statistics, (e.g. 5 images failed to load). The log file will specify the image name that cannot be found.

Notes:

- You will need to ensure the image name defined in the source field includes the file name extension.
- If you wish to update a cardholder's image, (e.g. supply a new image), you will need to supply the new image to the image folder. It is recommended that you supply only new images to this folder, not all cardholder images. This will save modifying cardholders unnecessarily.
- When an image is imported it may be re-sized to the dimensions specified by the image Personal Data Field. The default dimensions for the image Personal Data Field are: Width=160 pixels, Height=240 pixels.
- The same image cannot be added to all cardholders, unless a new copy is renamed for each cardholder.
- If a cardholder image is imported into Command Centre. A cardholder modified event is raised in Command Centre. This event is raised, even if the image imported was the same image as previously assigned to the cardholder.

Configuring Gallagher Command Centre to receive source data

Introduction

Before you begin configuring an interface, you will need to ensure fields in Gallagher Command Centre have been created and configured to receive the source data.

When importing cardholder data into Command Centre, you may need to create the following Command Centre fields:

- Personal Data Fields
- Access Groups
- Cards
- Competencies, or
- Roles

When importing bookings into Command Centre, you will need to create the appropriate bookable resources. Refer to *Creating a Bookable Resource Item* (in the "Bookable Resources" feature release note).

Remote items in a multi-server environment can be mapped to Enterprise Data Interface. For ease of management, all items in a multi-server site should have a unique name to prevent confusion as to which card type, access group or competency is involved.

Note: When importing a cardholder's personal data, the data will be imported but may not show until the cardholder is added to the Access Group containing the Personal Data Field.

Examples

- If you are importing a cardholder's license plate number.
  Ensure a 'License Plate' Personal Data Field has been configured in Gallagher Command Centre.
- If you are importing a cardholder's access privileges.
  Ensure an Access Group has been configured in Gallagher Command Centre that enables the cardholder to access the appropriate areas while on-site.
- If you are importing a booking. Ensure a bookable resource has been configured in Command Centre.

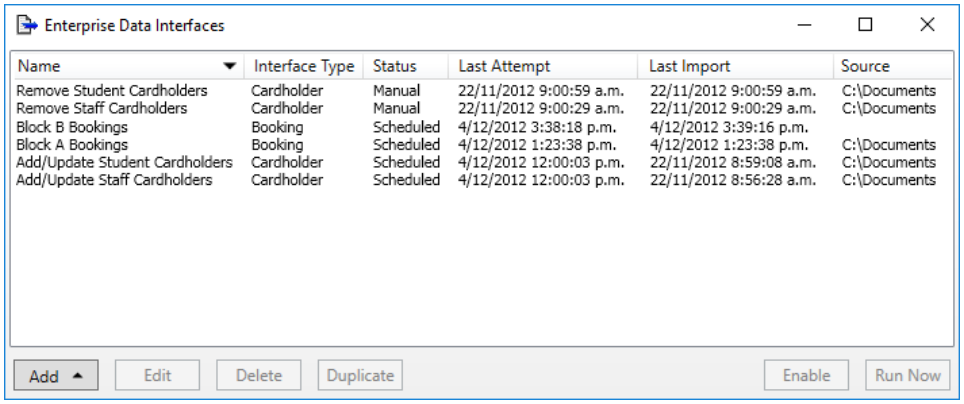
Creating an interface

Introduction

This procedure describes how to create an interface.

Procedure

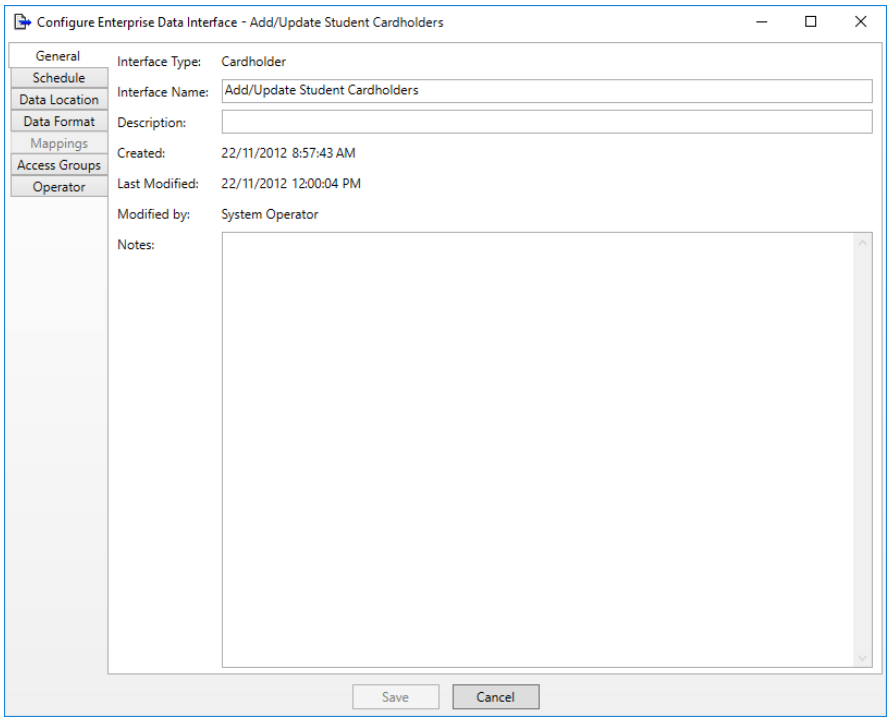
1. Click **Manage** from the menu bar.
2. Click **Enterprise Data Interface**.
   The Enterprise Data Interfaces list window opens.



   This window lists the interfaces created for your site.
3. Click the **Add** button.
4. Select the appropriate interface type, (i.e. either Cardholder Interface or Booking Interface).

   A Cardholder Interface can be configured to add, update or remove cardholders in Command Centre. A Booking Interface can be configured to update bookings within bookable resources configured in Command Centre.
   Note: The Booking Interface option will only be available if your site has the "Bookable Resources" licensable feature installed also.

   The Configure Enterprise Data Interface window opens.



By default the **General** tab displays. This tab displays the interface type, creation date, last modified date and the operator who last modified the interface.

5. Type in a **Name** (limited to 60 characters) for the interface and a logical **Description** (limited to 200 characters).
6. Type in **Notes** you want to record about the interface (limited to 2,500 characters).
7. To save the interface, click the **Save** button.
   If this interface requires further configuration a window displays detailing the further configuration required.
   - Click **Yes** if you wish to continue saving. The interface is added to the Enterprise Data Interfaces list window and its status is set to 'Incomplete'.
   - Click **No** if you wish to continue configuring the interface.
8. To configure the interface, refer to the following topics:
   - ***Scheduling an interface*** (on page 54-14)
   - ***Adding an interface to a sequence*** (on page 54-17)
   - ***Defining the source data location*** (on page 54-20)
   - ***Defining the source data format*** (on page 54-29)
   - ***Setting a "Run as Operator"*** (on page 54-35)
   - ***Mapping cardholder data to Gallagher Command Centre fields*** (on page 54-36) OR
     Mapping booking data to Gallagher Command Centre fields (on page 54-62)

Interface status

The status of an interface is displayed in the Status column on the Enterprise Data Interfaces list window.

This table provides an explanation for each interface status.

Interface status	Explanation
Incomplete	The status of an interface that requires further configuration.
Manual	The status of an interface that has been enabled but not scheduled or sequenced.
Scheduled	The status of an interface that has been enabled for import via a schedule.
Sequenced	The status of an interface that has been enabled for import via a sequence.
Disabled	The status of an interface that is disabled. A disabled interface cannot import any information.
Running	The status of an interface that is currently running.
Stopping	The status of an interface that is currently stopping.
Schedule-Expired	The status of an interface that has been enabled for import via a schedule, but the schedule has expired.
Not licensed	The status of an interface that is no longer licensed.

Editing an interface

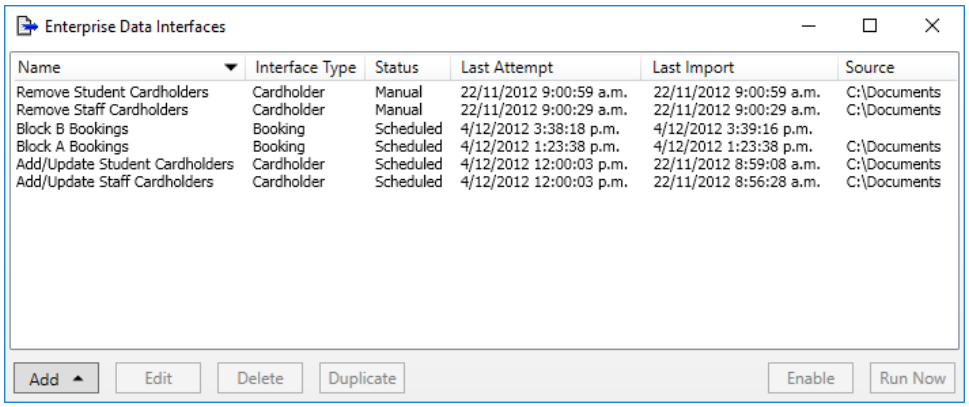
Introduction

This procedure describes how to edit an interface.

Procedure

1. Click **Manage** from the menu bar.
2. Click **Enterprise Data Interface**.

   The Enterprise Data Interfaces list window opens.



   This window lists the interfaces created for your site.

3. Select the interface you wish to edit and click the **Edit** button.

   The Configure Enterprise Data Interface window opens.

4. Edit the interface as required.

   Note: If an interface is running, the edits will be applied to the next import.

Deleting an interface

Introduction

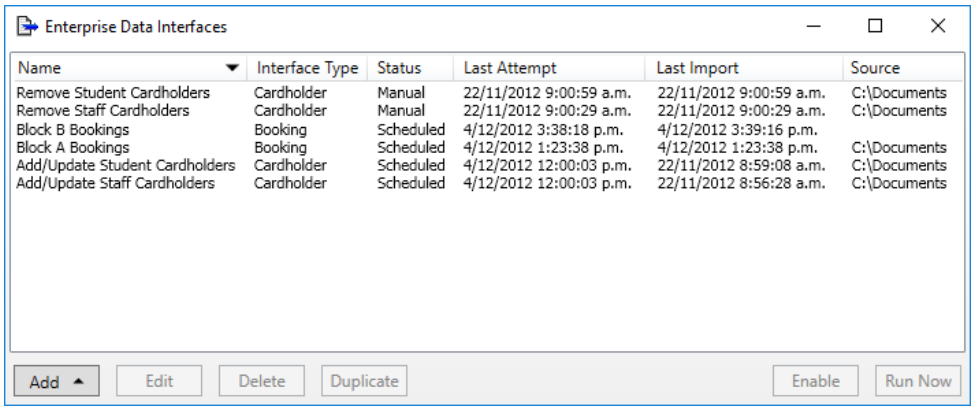
This procedure describes how to delete an interface.

Note: Deleting a running interface, will not stop it from running. The interface will finish the import operation and won't be controllable from the list window. It is recommended that you disable the interface first.

Procedure

1. Click **Manage** from the menu bar.
2. Click **Enterprise Data Interface**.

   The Enterprise Data Interfaces list window opens.



   This window lists the interfaces created for your site.

3. Select the interface you wish to delete and click the **Delete** button. A confirmation dialog window opens.
4. Click **Yes** to delete the interface. The interface is deleted and removed from the Enterprise Data Interface list window.

Duplicating an interface

Introduction

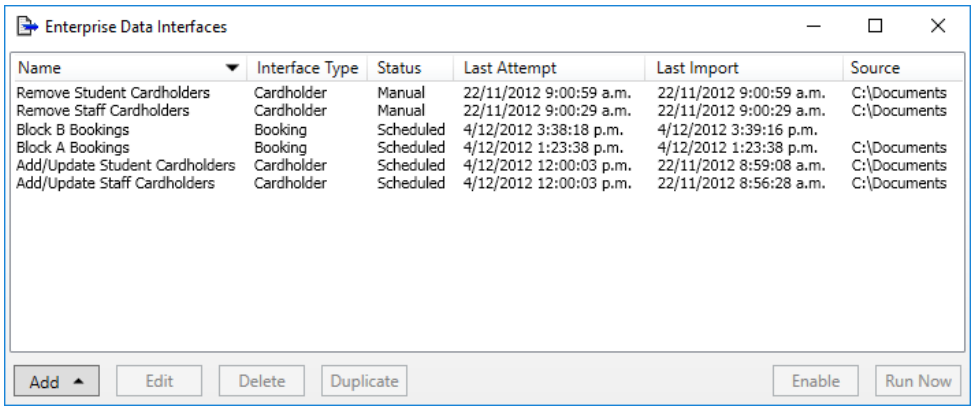
This procedure describes how to duplicate an interface.

When an interface is duplicated, an exact copy of the interface is created under a new name.

Procedure

1. Click **Manage** from the menu bar.
2. Click **Enterprise Data Interface**.

   The Enterprise Data Interfaces list window opens.

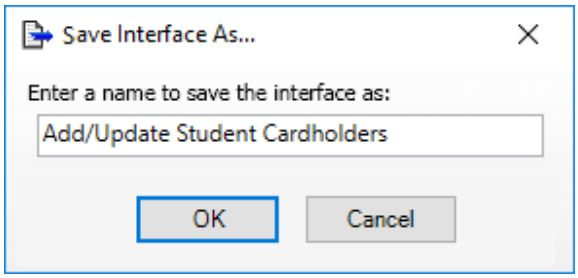


   This window lists the interfaces created for your site.

3. Select the interface you wish to duplicate and click the **Duplicate** button.

   The Configure Enterprise Data Interface window opens.

4. Click the **Save As ...** button. The Save Interface As ... window displays.



5. Enter a name for the interface. This name must be unique.
6. Click the **OK** button. The interface is saved and added to the Enterprise Data Interface list window. The interface status is set to "Disabled".

Scheduling an interface

Introduction

Note: Functionality specific to scheduling an interface is only available if your site is licensed to schedule interfaces.

When an interface has been scheduled and enabled, it will run according to the schedule without operator intervention.

You can schedule an interface to run once a day, or run on a regular basis, (e.g. every hour). This will ensure Gallagher Command Centre is regularly updated with the latest data.

If you configure your third party application to provide the source file on a regular basis, you can then schedule an interface to "pick-up" and import the source file when it is provided.

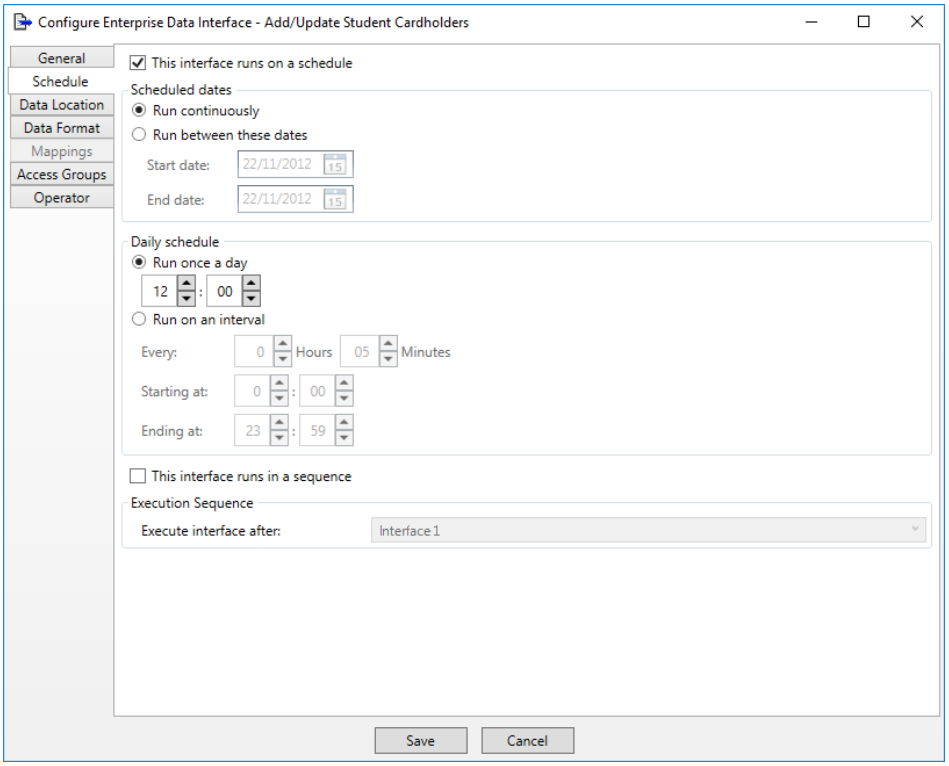
Notes:

- Only the first interface in a sequence can be scheduled. All other interfaces added to a sequence cannot be scheduled.
- If you configure your third party application to provide the source file on a regular basis, you can then schedule an interface to "pick-up" and import the source file when it is provided.
- If an interface is scheduled to run and there is no source file, the interface will not run until the next scheduled time.
- When scheduling an interface to run on an interval, the hours and minutes specify how often Gallagher Command Centre checks for a file to import, or connects to the database server.
- If an interface is scheduled to run and the interface is unable to connect to the database server, the interface will not run until the next scheduled time.
- If an interface is scheduled to run from a database, the interface will process the records as present in the database, at that time.
- If you are running a large import operation, it is recommended you schedule the import to run at a time when Gallagher Command Centre is at its least active, (e.g. late at night, during a weekend or during a public holiday).
- Scheduled interfaces are single threaded, meaning the interface will run one import operation after another via the schedule. You will need to ensure you configure your schedule to give the previous import enough time to complete, before the next import is scheduled to run. If the scheduled interface is at the start of a sequence, you will need to ensure you configure your schedule to give all interfaces in the sequence enough time to complete, before the next import is scheduled to run.

- If an interface has been scheduled to run on an interval and you have not specified a start and end date, the interface will continue to run according to the schedule until it is disabled.

Procedure

1. Click the **Schedule** tab.
   This tab displays the schedule configured for this interface.



   Note: If your site is not licensed to schedule interfaces this tab will be grayed out.

2. Check the **This integration runs on a schedule** checkbox.
   Note: If the interface forms part of a sequence a confirmation dialog window opens.

3. If you wish to run the import once a day:

   a) Select **Run continuously**.

   b) Select **Run once a day** and enter the time of day you require the import to run.

4. If you wish to run the import once a day, between specific dates:

   a) Select **Run between theses dates**.

   b) Select the **Start date** and **End date** you require the import to be run between. The End date must be greater than or equal to the Start date.

   c) Select **Run once a day** and enter the time of day you require the import to run.

5. If you wish to run the import more than once a day:
   a) Select **Run continuously**.
   b) Select **Run on an interval**.
   c) Enter the **interval**, (e.g. run every 2 hours and 30 minutes).
   d) Enter the **Starting at** time. Importing will start at this time each day.
   e) Enter the **Ending at** time. Importing will end at this time each day.
6. If you wish to run the import more than once a day, between specific dates:
   a) Select **Run between these dates**.
   b) Select the **Start date** and **End date** you require the import to be run between. The End date must be greater than or equal to the Start date.
   c) Select **Run on an interval**.
   d) Enter the **interva**l, (e.g. run every 2 hours and 30 minutes).
   e) Enter the **Starting at** time. Importing will start at this time each day.
   f) Enter the **Ending at** time. Importing will end at this time each day.

Adding an interface to a sequence

Introduction

Note: Functionality specific to adding an interface to a sequence is only available if your site is licensed to schedule interfaces.

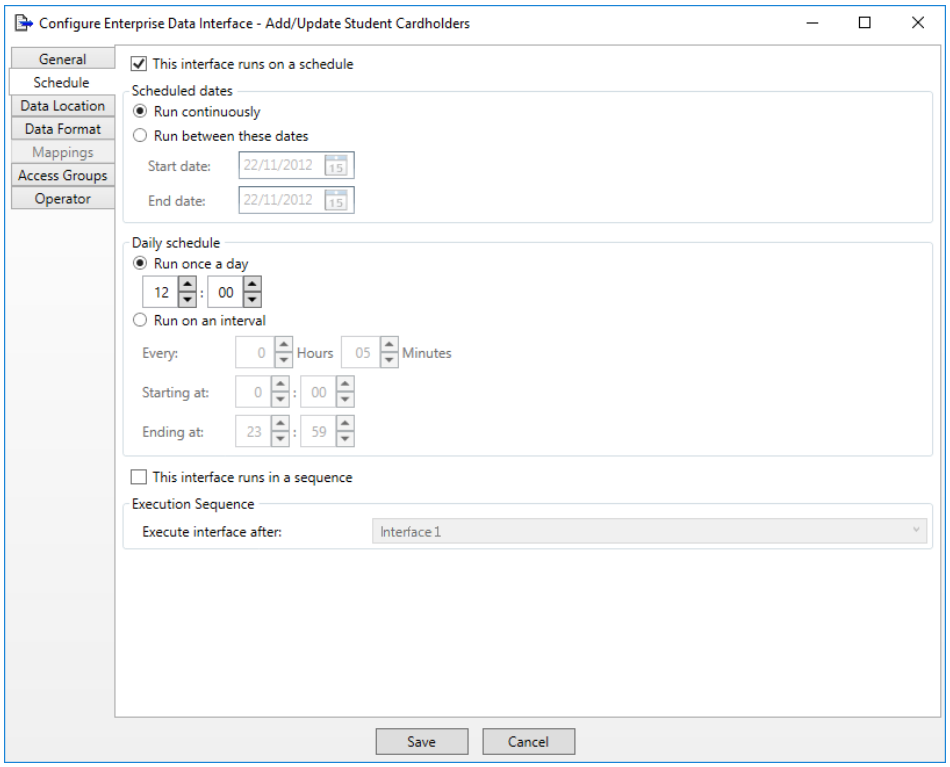
When an interface has been added to an execution sequence and enabled, it will run according to the sequence without operator intervention.

Notes:

- An interface added to a sequence will run immediately after the completion of the previous interface in the sequence. If the previous interface failed to run, the next interface in the sequence will not be run, and so on.
- If an interface located midway in a sequence is run, the next interface in the sequence will run immediately after the completion of the previous interface in the sequence, and so on.
- When importing data from a source file, you will need to configure your third party application to provide the source file, in order for the sequenced interface to "pick-up" and import the source file. If an interface is sequenced to run and there is no source file, the interface will not run.
- When importing data from a database, if the interface is sequenced to run and the interface is unable to connect to the database server, the interface will not run.
- If an interface is sequenced to run from a database, the interface will process the records as present in the database, at that time.

Procedure

1. Click the **Schedule** tab.
   This tab displays the schedule configured for this interface.



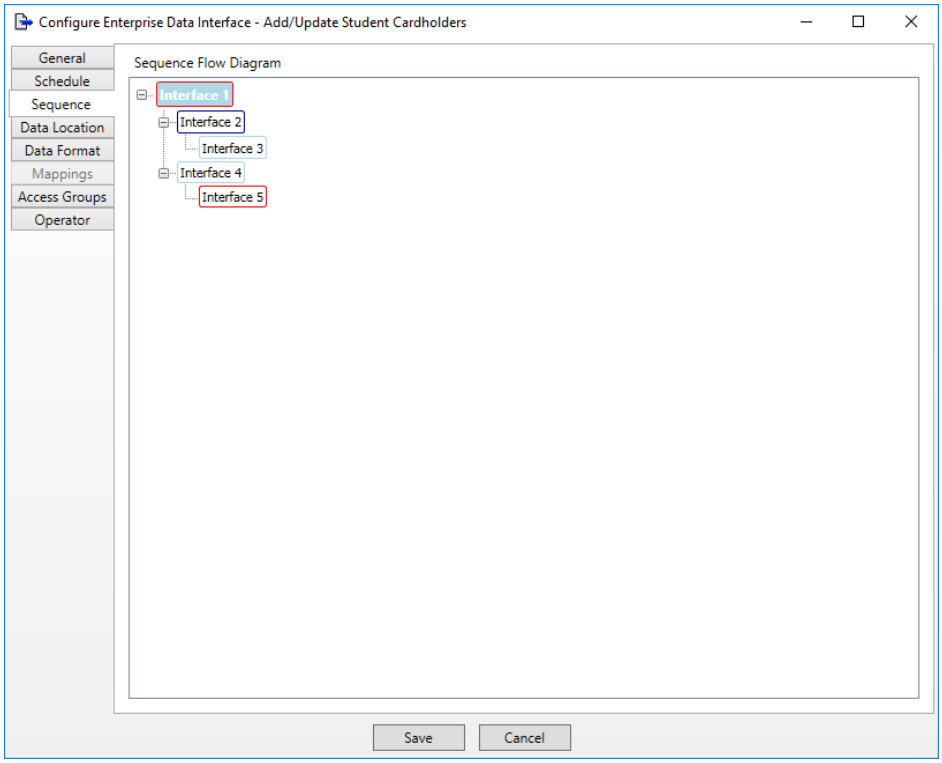
Note: If your site is not licensed to schedule interfaces this tab will be grayed out.

2. Check the **This integration runs in a sequence** checkbox.
   The Sequence tab displays below the Schedule tab.

   Note: This checkbox is disabled if the interface is the first interface in a sequence and all other interfaces belong to this sequence, (i.e. you cannot configure a sequence that is a continuous loop).

3. Select the interface that this interface will run after from the **Execute interface after** drop-down list.

4. To view the interfaces added to this sequence, click the **Sequence** tab.
   This diagram displays the flow structure of the sequence.



This table provides an explanation for each interface colour.

Interface colour	Explanation
Blue fill	The first interface in the sequence. This interface "kicks-off" the sequence.
Black outline	The current interface. The interface that is open.
Red outline	Represents an interface whose status is Incomplete, Disabled, Schedule-Expired or Not licensed.
Blue outline	Represents an interface whose status is Sequenced.

Defining the source data location

Introduction

This procedure describes how to define the source data location.

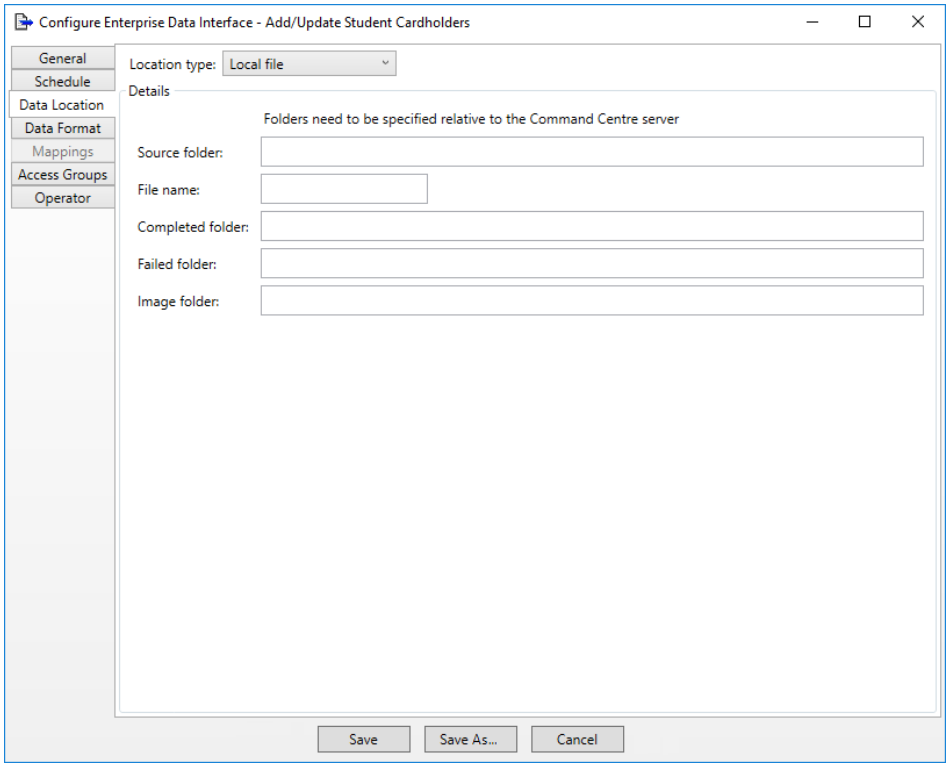
If the source file (containing the source data) is located on the Command Centre server PC, all folders must be located on the Command Centre server PC and not a network drive.

If the source file (containing the source data) is located on a network drive, you will need to specify the Windows logon used to access the drive. It is recommended that the Windows logon specified is an account created specifically for the purpose of automated data transfers, and is not a standard user account where the password may get changed, or may have more privileges on the network than required.

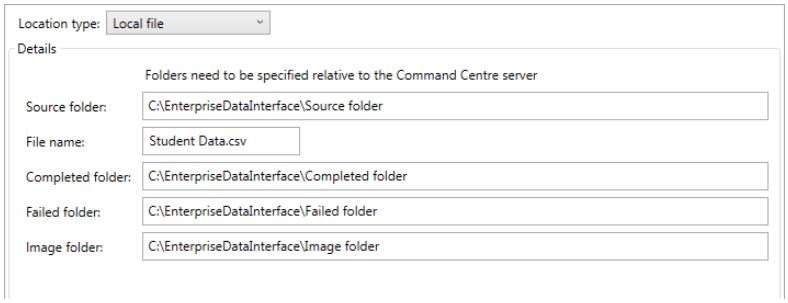
If the source data is located in a database, you will need to specify the IP address of the database PC and the logon used to access the database.

Procedure

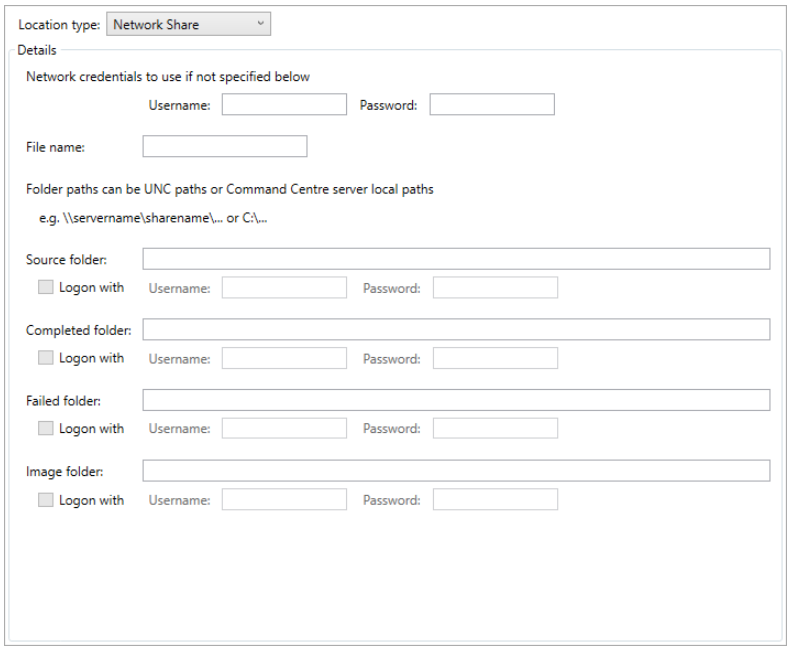
1. Click the **Data Location** tab.



2. Where is the source data located?

If...	then...
locally on Gallagher Command Centre server PC,	**a)** Ensure **Local file** is selected in the **Location type** drop-down list. **b)** Enter the source folder path into the **Source folder** field. **c)** Enter the source file name into the **File name** field. **Note:** If you don't know the source file name, or you want to import more than one source file, you can use wildcard characters, refer to ***Wildcard characters*** (on page 54-24). **d)** Enter the completed folder path into the **Completed folder** field. **e)** Enter the failed folder path into the **Failed folder** field, if required. **f)** If you are importing cardholder images, enter the image folder path into the **Image folder** field. 
on other network location(s),	**a)** Select **Network Share** from the **Location type** drop-down list. The "Details" section of this screen allows you to specify either a single network logon or different network logons for each of the folders if required. Windows networking only allows for one username at a time to connect to a Windows file server from within a Windows session. Subsequent connections to the same server with different usernames are refused with Windows system error 1219: The credentials supplied conflict with an existing set of credentials. For this reason, EDI will refuse to connect to the same share with different usernames.

If...	then...



b) Complete the fields as appropriate, (e.g. you may have a single user, multiple users, one network location or multiple network locations).
The following ***Examples*** (on page 54-25) help explain how to setup this screen depending on your situation.

Notes:

- A common logon can be used for some or all of the folders, (e.g. if one logon is used for all network locations, only the **Username** and **Password** fields at the top of the screen need completing).
- If the same **Username** is used for two folder locations, and the second folder location has an incorrect **Password**, the job may still complete if EDI only needs one network connection to reach both locations. If the first location is later changed, the incorrect password may be exposed when EDI uses the credentials of the second folder location to connect to the second location.

in a database,

a) Select **Database** from the **Location type** drop-down list.

b) Select the database type from the **Database Type** drop-down list.

c) Enter the database server name or IP address into the **Server** field (maximum 64 characters).

d) Enter the user name, used to connect to the database into the **Username** field (maximum 64 characters). This field is case sensitive.

If...	then...

e) Enter the user password into the **Password** field (maximum 64 characters). This field is case sensitive.

f) If required, select the **Test Connection** button. This can be used to validate the connection details entered.

g) If you have selected Microsoft SQL Server as the database type, select the database from the **Database Name** drop-down list.

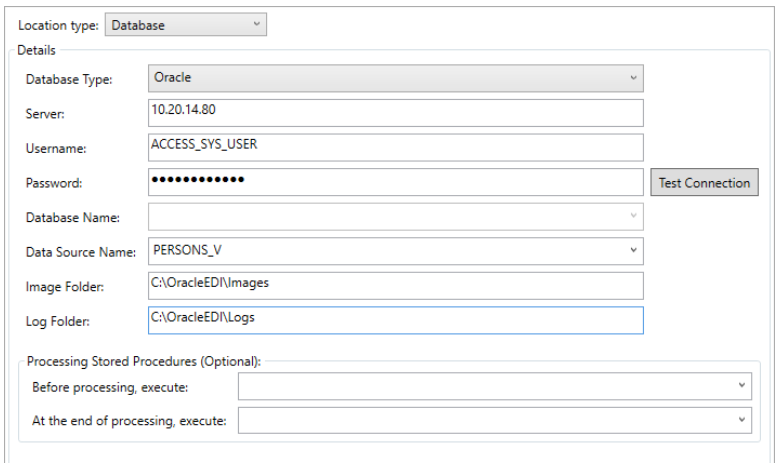
h) Select a table/view from the database that will be used as the main source for data importing, from the **Data Source Name** drop-down list.

Note: This drop-down lists the tables followed by the views that the user can view.

i) If you are importing cardholder images, enter the image folder path (local pathway) into the **Image Folder** field.

j) Enter the log folder path (local pathway) into the **Log Folder** field, if required.

k) Optionally, you can execute a stored procedure before the processing of records begins or at the end of processing records. The drop-down lists will display all selectable stored procedures that the logging user has privileges for.



Wildcard characters

Introduction

You can use wildcard characters in the source file name, if required. Wildcard characters can be used if you don't know the source file name, (e.g. the file name is a date and time stamp) or, if you want to import more than one source file.

Fields that accept wildcard characters expect a .NET regular expression, with the following exceptions:

- **?** is treated as **.** (matches any single character)
- ***** is treated as **.*** (matches any one or multiple characters)
- **.** is treated as **\.** (an escaped full stop/period)

Warning: While **.** characters are automatically escaped, (i.e. '.' is interpreted as '\.'), parentheses and square brackets characters are not. So, if you use a parenthesis or bracket character in the field, you must escape it with a backslash in front unless you are using the parenthesis/bracket as part of .NET regular expression syntax. For example, to match the name 'Doc (v1.0)', you must enter 'Doc \(v1.0\)'.

Use case

For example, in a source file name field, wildcard characters can be used if you don't know the exact source file name, (e.g. the file name is a date and time stamp), or if you want to import more than one source file (e.g. multiple files with slightly different names).

Definition

Wildcard characters are:

Character	Definition
?	Represents any alphanumeric character in the position it occupies. This wildcard character can appear at the beginning of a filename, middle of a filename, or at the end of a filename.
*	Represents zero, one, or multiple alphanumeric characters in the position it occupies. This wildcard character can appear at the beginning of a filename, in the middle of a filename, or at the end of a filename. **Note:** If only '*' is used as the file name, all files within the source folder will be imported.

Examples

Wildcard examples are:

Filename	Function
achieve?.csv	Matches any twelve-character filename such as *achieved.csv* or *achiever.csv*. Does not match *achieve.csv* or *achievement.csv*
e*t*.csv	Matches any filename such as *event.csv*, *elective.csv, electronics.csv* or *electronics1018.csv*
Data \(*\).csv	Matches any filename starting with Data, followed by something in parentheses, followed by *.csv*, such as *Data (v1.0).csv* or *Data (ABC).csv* **Note:** Parentheses characters must be escaped with a backslash in front, i.e. **\(** and **\)**.
eng*.csv	Matches any filename such as *english.csv*, *engineers.csv, engineering.csv*. or *eng1018.csv*
.	Matches any filename with any file extension.

Examples

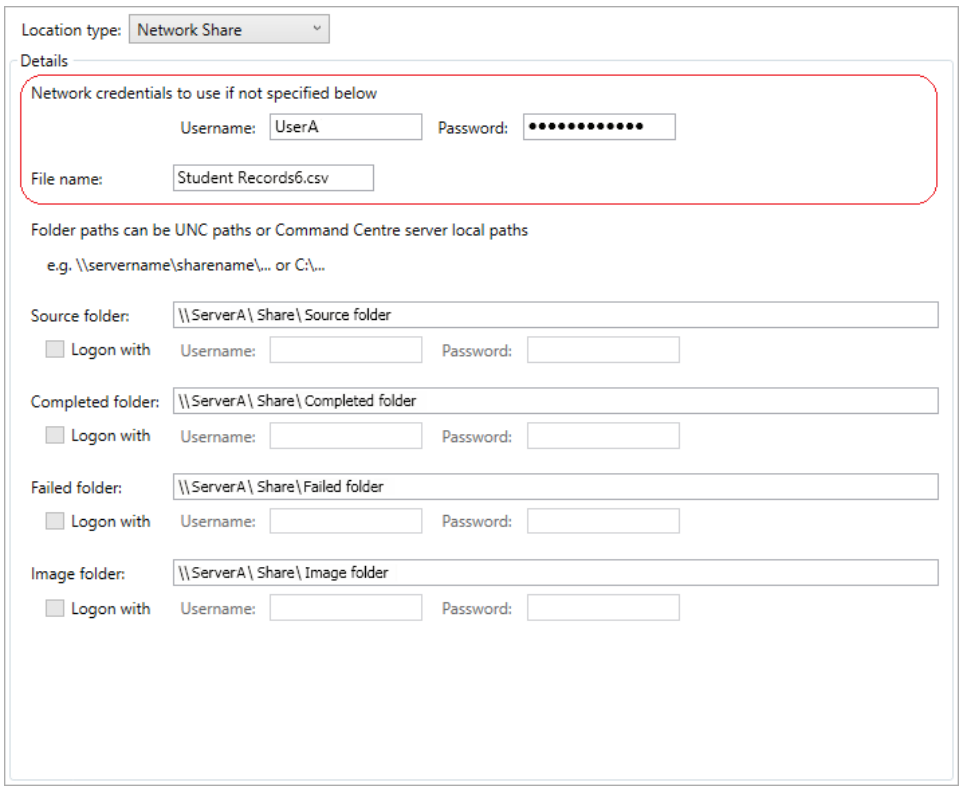
The following examples help explain how to setup the "Details" section of the **Data Location** screen depending on you situation, when you select **Network Share** as the location type.

- ***Example 1: Single user, same network location for all folders*** (on page 54-25)
- ***Example 2: Single user, different network locations for folders*** (on page 54-26)
- ***Example 3: Different users, different network locations for folders*** (on page 54-27)

Example 1: Single user, same network location for all folders

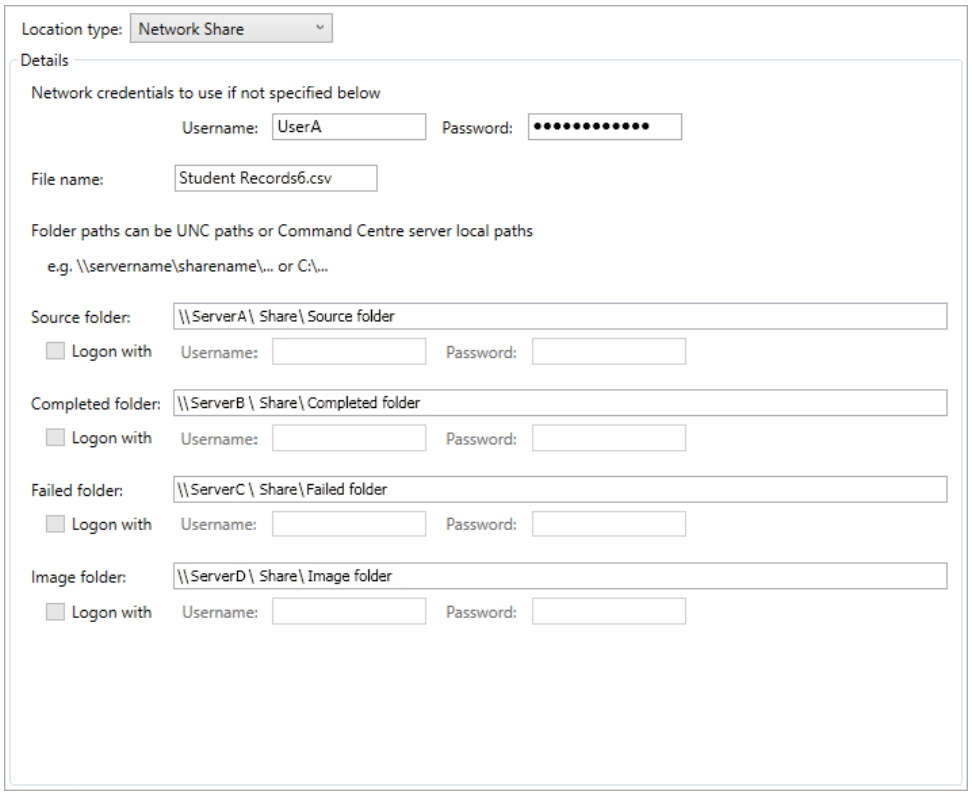
1. Enter details in the three fields in the top part of the screen, (i.e. the **Username** and **Password** of the user, and the source file name into the **File name** field).
   No other fields need completing as all the folders are on the same network location.

   Note: If you don't know the source file name, or you want to import more than one source file, you can use wildcard characters. Refer to ***Wildcard characters*** (on page 54-24).



Example 2: Single user, different network locations for folders

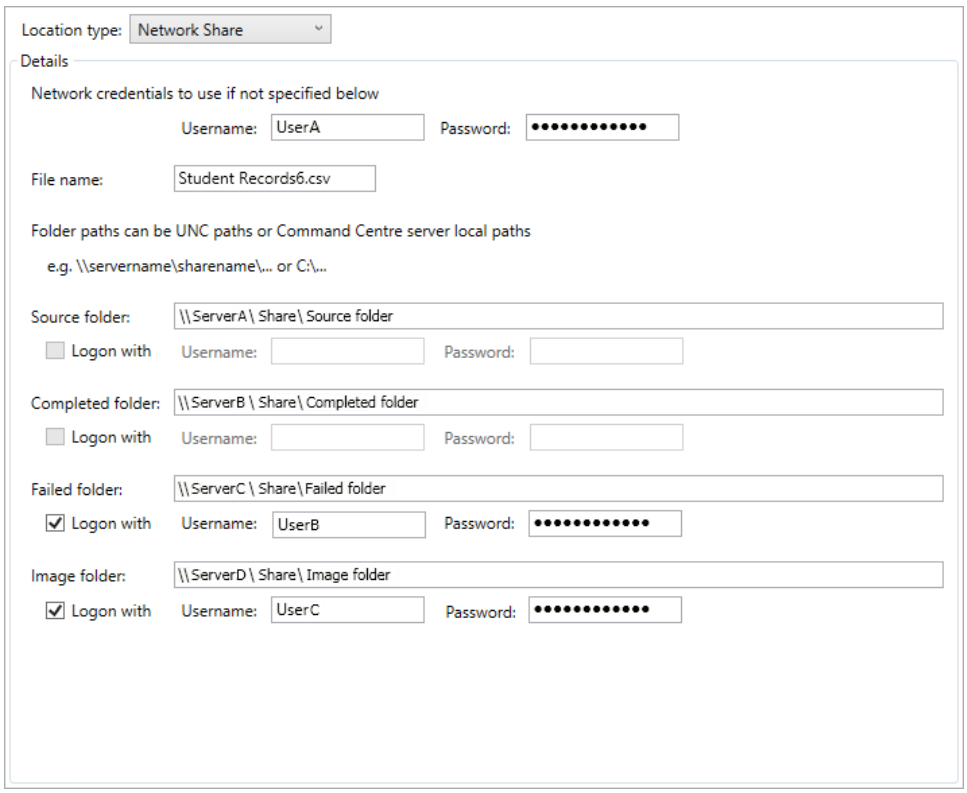
1. Enter details in the three fields in the top part of the screen, (i.e. the **Username** and **Password** of the user, and the source file name into the **File name** field).
2. Enter the individual folder paths into the **Source folder**, **Completed folder**, **Failed folder** and **Image folder** fields.



Note: As a valid folder path is entered into each of these fields, the **Logon with** checkbox directly below it becomes enabled. These can be ignored as the **Username** and **Password** of the single user has already been entered.

Example 3: Different users, different network locations for folders

Scenario 1:
In this scenario:
- User A will access the Source folder and the Completed folder
- User B will access the Failed folder
- User C will access the Image folder

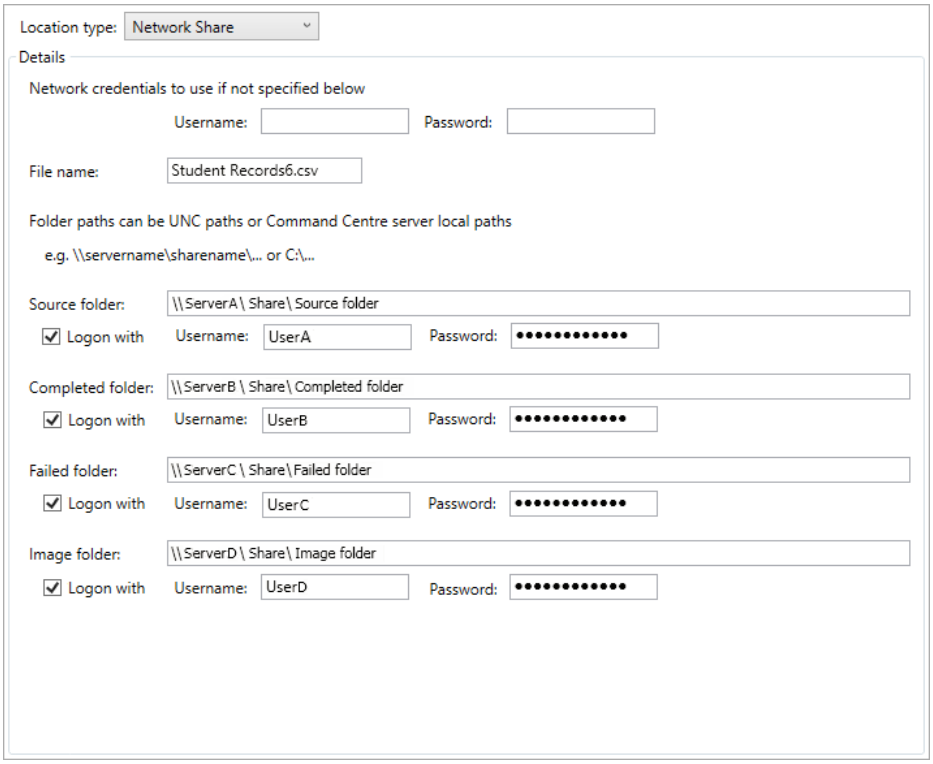


1. Enter User A's **Username** and **Password** into the fields in the top part of the screen.
   Note: Alternatively, these fields can be left blank, and User A's **Username** and **Password** can be entered into the appropriate fields directly below the **Source folder** and **Completed folder** fields.
2. Enter the source file name into the **File name** field.
3. Enter the folder paths into the **Source folder** and **Completed folder** fields. As a valid folder path is entered into each of these fields, the **Logon with** checkbox directly below it becomes enabled. These can be ignored as User A's **Username** and **Password** have already been entered in the top part of the screen.
4. Enter the failed folder path in the **Failed folder** field.
5. Check the **Logon with** checkbox directly below the **Failed folder** field, and enter User B's **Username** and **Password**.
6. Enter the image folder path in the **Image folder** field.
7. Check the **Logon with** checkbox directly below the **Image folder** field, and enter User C's **Username** and **Password**.

Scenario 2:

In this scenario:

- User A will access the **Source folder**
- User B will access the **Completed folder**
- User C will access the **Failed folder**
- User D will access the **Image folder**



1. Enter the source file name into the **File name** field.
2. Enter the source folder path in the **Source folder** field.
3. Check the **Logon with** checkbox directly below the **Source folder** field, and enter User A's **Username** and **Password**.
4. Enter the completed folder path into the **Completed folder** field.
5. Check the **Logon with** checkbox directly below the **Completed folder** field, and enter User B's **Username** and **Password**.
6. Enter the failed folder path in the **Failed folder** field.
7. Check the **Logon with** checkbox directly below the **Failed folder** field, and enter User C's **Username** and **Password**.
8. Enter the image folder path in the **Image folder** field.
9. Check the **Logon with** checkbox directly below the **Image folder** field, and enter User D's **Username** and **Password**.

Defining the source data format

Introduction

This procedure describes how to define the data format of your expected source data.

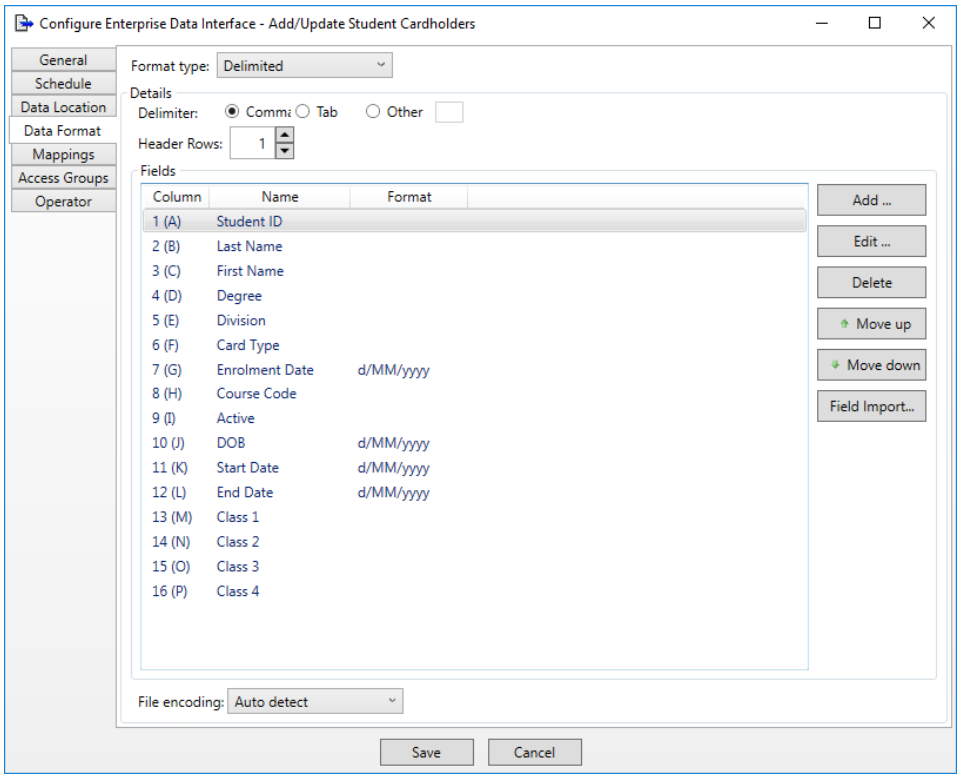
Procedure

Importing from a source file

It is important that you define all the field names in your source file. You can select which fields to import at a later stage. You can either import the field names directly from the header row of your source file, or you can enter the field names manually.

Note: The order of the fields configured on the Data Format tab, must match the order of the fields in the source file.

1. Click the **Data Format** tab.



2. Click the **Format type** drop-down list and select the format type of your source file, either **Delimited** or **Fixed Width**.

   Note: The Fixed Width field limit is 1-255.

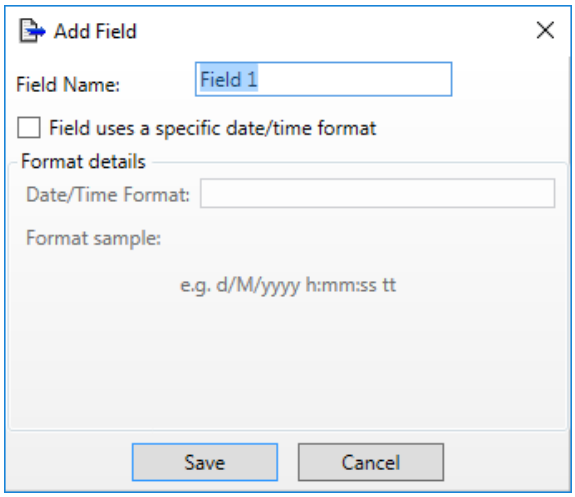
3. If you have selected delimited, define the delimiter used:

If...	then...
comma	ensure the **Comma** radio button is selected. This button is selected by default.
tab	select the **Tab** radio button.
other	select the **Other** radio button and enter the delimiter used into the field opposite.

4. Enter the number of header rows contained in your source file. The interface will import only the rows below the header rows.
5. To import field names from a file:
   a) Click the **Field Import** button. The 'Import fields from file' window displays.
   b) Navigate to the file you wish to use, select the file and click the **Open** button.

   - If the Header Rows field is populated with either "0" or "1" the first row of this file will be imported as field names.
   - If the Header Rows field is populated, for example with "10" the tenth row of this file will be imported as the field names.

   Note: If you are using a file other than the source file to import field names, ensure the fields are the same as the source file fields that will be used.
6. To manually add a field name, click the **Add** button.
   The Add Field window displays.



   a) Enter the field name into the **Field Name** field.
   Notes:

   - The field name entered is arbitrary. This field is referenced by the column identifier displayed to the left of the field name.
   - If this field is a Fixed Width field, enter the field width (maximum 255 characters).

b) If this field uses a date and/or time format, check the "Field uses a specific date/time format" check-box and enter the date and/or time format used by this field.

The components of the date/time format are; **dd** is a two digit day, **MM** is a two digit month, **yyyy** is a four digit year, **hh** is the number of hours in 12 hour form, **HH** is the number of hours in 24 hour form, **mm** is the number of minutes, **ss** is the number of seconds, **tt** is the am pm designator.

Notes:

- If you specify a format string that doesn't contain time (e.g. "d-MM-yyyy") and the field contains a date/time string such as "13-12-2009 23:59:59 pm", then the record will fail to import.
- If the source field only contains time values and the format string is only for times, the date will be assumed to be today.

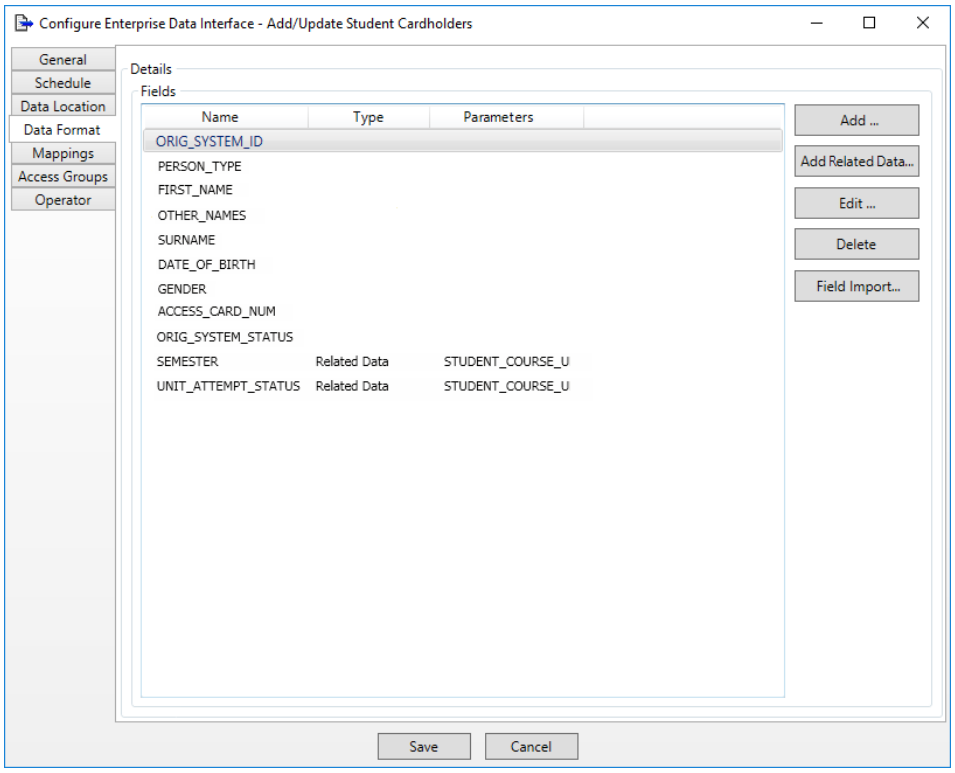
c) Click the **Save** button. This field name will be added to the Fields grid.

7. If you wish to change a field name, select the field name you wish to change then click the **Edit** button. The Edit Field window displays. Edit the field name and format details as required.
8. If you wish to delete a field name, select the field name you wish to delete then click the **Delete** button.
9. If a field name is in the wrong location, you can move the field name either up or down.
   - To move a field name up, select the field name you wish to move then click the **Move up** button.
   - To move a field name down, select the field name you wish to move then click the **Move down** button.
10. If Enterprise Data Interface cannot detect the encoding used by your source file, select either: ANSI / UTF-8, Unicode or Unicode (big endian).

Importing from a database

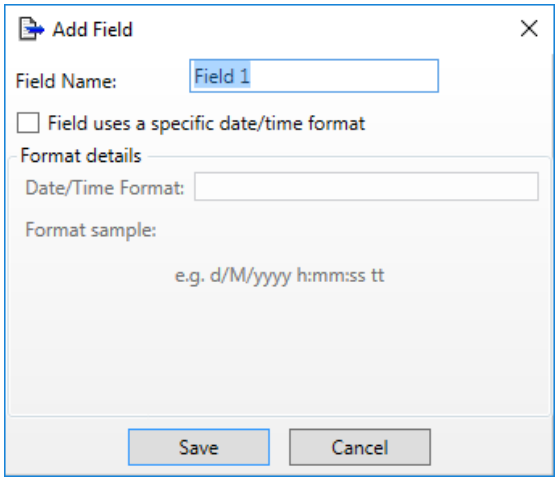
You will need to define the name of each field you want to import from the database. When importing from a database, the field is identified by the field's name and not its position.

1. Click the **Data Format** tab.



2. To import field names from a database, click the **Field Import** button. Command Centre will connect to the database and retrieve all columns from the configured **Data Source Name** (as specified on the Data Location tab).

3. To manually add a field, click the **Add** button.
The Add Field window displays.



a) Enter the field name into the **Field Name** field.
Note: The field name entered must be an exact match to the field name in the database. With an Oracle database, you can create a field name of two words with a single space in between, (e.g. First Name). Command Centre will not accept more than two words, (e.g. The First Name), or a double space, (e.g. First Name), or an apostrophe in the name, (e.g. First's Name). With a Microsoft SQL Server database, Command Centre does accept all these variations.

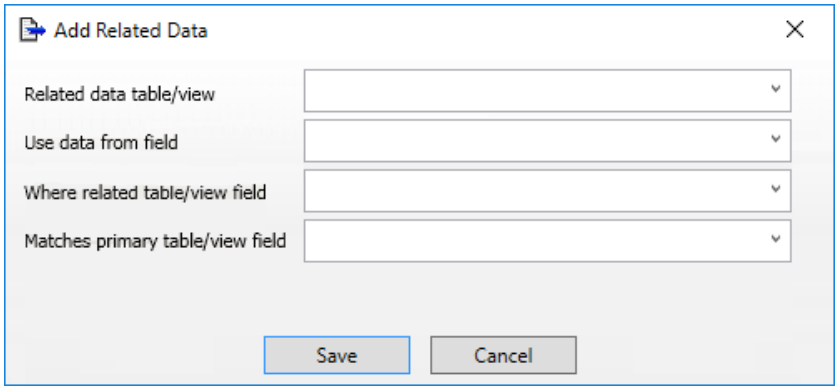
b) If this field is a text field, and contains date data of a particular format, check the "Field uses a specific date/time format" check-box and enter the date and/or time format used by this field.

The components of the date/time format are; **dd** is a two digit day, **MM** is a two digit month, **yyyy** is a four digit year, **hh** is the number of hours in 12 hour form, **HH** is the number of hours in 24 hour form, **mm** is the number of minutes, **ss** is the number of seconds, **tt** is the am pm designator.
Notes:

- If you specify a format string that doesn't contain time (e.g. "d-MM-yyyy") and the field contains a date/time string such as "13-12-2009 23:59:59 pm", then the record will fail to import.
- If the source field only contains time values and the format string is only for times, the date will be assumed to be today.

c) Click the **Save** button. This field will be added to the Fields grid.

4. If you wish to change a field, select the field you wish to change then click the **Edit** button. The Edit Field window displays. Edit the field and format details as required.
5. If you wish to delete a field, select the field you wish to delete then click the **Delete** button.
6. If you wish to add a field from a different data table/view, click the **Add Related Data** button. The Add Related Data window displays.



Note: When using a related data table, bookings cannot accept multiple source values for a record for any of the Booking fields.

7. From the **Related data table/view** drop-down list, select the data table/view that contains the field you want to add.
8. From the **Use data from field** drop-down list, select the column containing the field you want to add.
9. From the **Where related table/view field** drop-down list, select a field that will be used to identify cardholders or bookings, (e.g. unique cardholder ID or bookable resource name) in the related data table/view.

Note: This list is populated with only the fields, as determined by the related data table/view selected above.

10. From the **Matches primary table/view field** drop-down list, select a field that matches the field selected above, (e.g. unique cardholder ID or bookable resource name).

    Note: This list is populated with only the fields, as shown on the Data Format tab.

Setting a "Run as Operator"

Introduction

This procedure describes how to set a "Run as Operator" for an interface. All actions performed by the interface are logged under this operator's name.

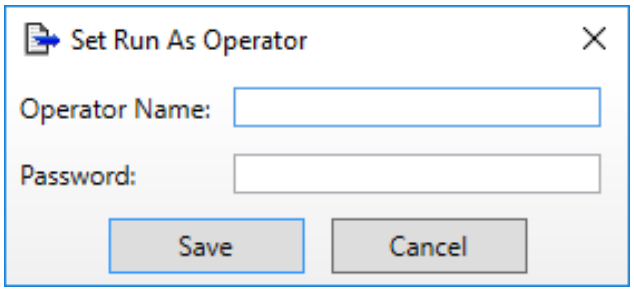
"Run as Operator" Privileges

You will need to ensure this operator has been assigned the appropriate privileges in the divisions required, in order to perform the actions specified by the interface.

Privilege	is required to...
"Edit Cardholders"	create and/or change cardholders
"Edit Cardholder Notes"	create and/or change a cardholder's notes
"Delete Cardholders"	delete cardholders
"Modify Access Control"	set cardholder access groups
"View Site"	view competencies, to add to a cardholder

Procedure

1. Click the **Mappings and Operator** tab.
2. Click **Set Operator.** The Set Run As Operator window displays.



3. Enter the operator's name into the Operator Name field.
4. Enter the operator's password into the Password field.

   Note: This password is used to verify the operator, but isn't stored in the interfaces configuration. Hence, changing the operator's password in Gallagher Command Centre does not require a reset of the "Run As Operator" details.

5. Click the **Save** button. The operator name and password will be validated before being stored.

Mapping cardholder data to Gallagher Command Centre fields

Introduction

This section of the manual describes how to map cardholder data from your source data to Gallagher Command Centre fields.

Before you can begin mapping you will need to decide the purpose of your cardholder interface. To either:

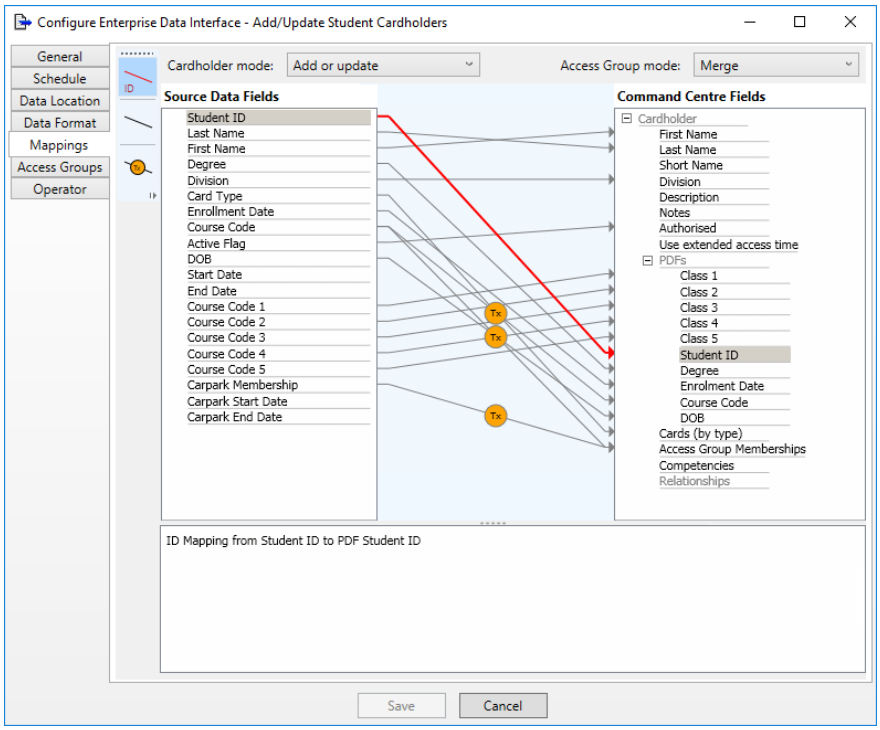
- Add or update cardholders, or
- Remove cardholders

There is one ID field used to identify the cardholder in Gallagher Command Centre, (e.g. Student ID or Employee ID). Refer to ***Creating a cardholder ID mapping*** (on page 54-38).

Adding or updating cardholders

If the purpose of your interface is to add or update cardholders, complete the following procedure:
Note: When adding cardholders, you must create a map to the Division field.

1. Click the **Mappings and Operator** tab.
2. Click **Configure**.
   This tab displays the fields you defined on the Data Format tab (these fields originate from your source data) and all Gallagher Command Centre fields that can have data imported.



3. Select **Add or update** from the Cardholder mode drop-down list.
4. If you want to retain the cardholder's pre-existing Access Groups, select **Merge** from the Access Group mode drop-down list.
5. If you want to set Access Groups to the mapped Access Groups only, select **Replace** from the Access Group mode drop-down list.
6. To continue mapping source fields to Gallagher Command Centre fields, refer to the following topics:
   - ***Creating a cardholder ID mapping*** (on page 54-38)
   - ***Creating a cardholder direct mapping*** (on page 54-39)
   - ***Creating a cardholder transformation mapping*** (on page 54-41)

Removing cardholders

If the purpose of your interface is to remove cardholders, complete the following procedure:

1. Click the **Mappings and Operator** tab.
2. Click **Configure**. The Edit Mappings window opens.
3. Select **Remove** from the Cardholder mode drop-down list.
4. Create an ID mapping. Refer to ***Creating a cardholder ID mapping*** (on page 54-38). Cardholders whose unique Personal Data Field value matches the unique source value will be removed. Other mappings can exist, but they will have no effect when removing cardholders.

Creating a cardholder ID mapping

Introduction

This procedure describes how to create a cardholder ID mapping.
An ID mapping identifies cardholders in the Gallagher Command Centre database. This mapping must be present in order to add, update or remove cardholders.

Notes:

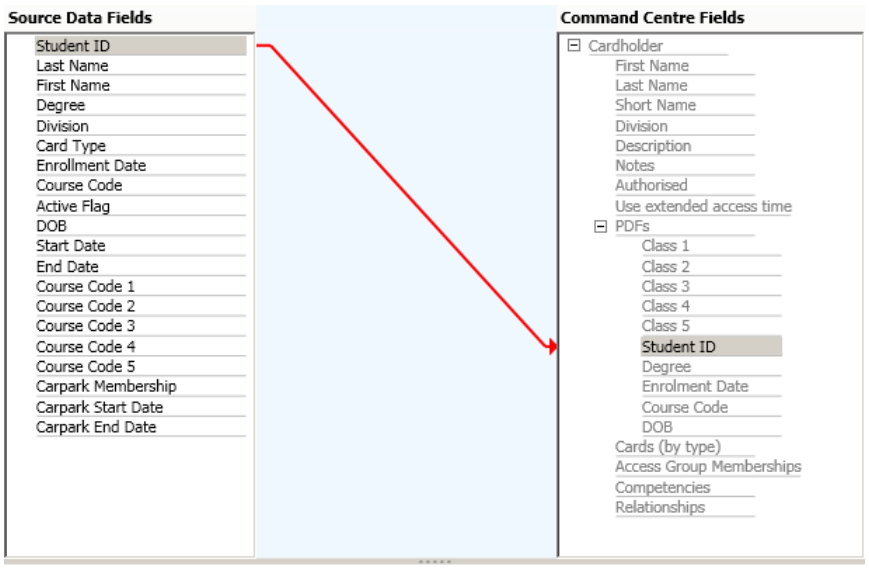
- Only one ID mapping can be set.
- The source field used as an ID mapping can also be used to map to other Gallagher Command Centre fields.
- When mapping from a database, if the source field is a related data field containing multiple values, the cardholder will not be imported.
- If the source field for an ID mapping contains a blank or null value, the cardholder record will not be imported.

Procedure

1. Select the 

tool.
2. Select the unique source field you wish to map from.
3. Hold down the mouse button and drag the cursor over the unique Command Centre field you wish to map to.

   Note: The  icon will only appear if the Gallagher Command Centre field is a unique text or numeric PDF field.
4. Release the mouse button. A red line appears between the two fields and a message appears in the window below.



ID Mapping from Student ID to PDF Student ID

Creating a cardholder direct mapping

Introduction

This procedure describes how to create a cardholder direct mapping.

A direct mapping imports the exact wording from your source field into Gallagher Command Centre. You can create direct mappings for the following Gallagher Command Centre fields:

- Cardholder fields
- Personal Data fields (including notification PDFs)
- Access Groups
- Cards
- Competencies
- Relationships

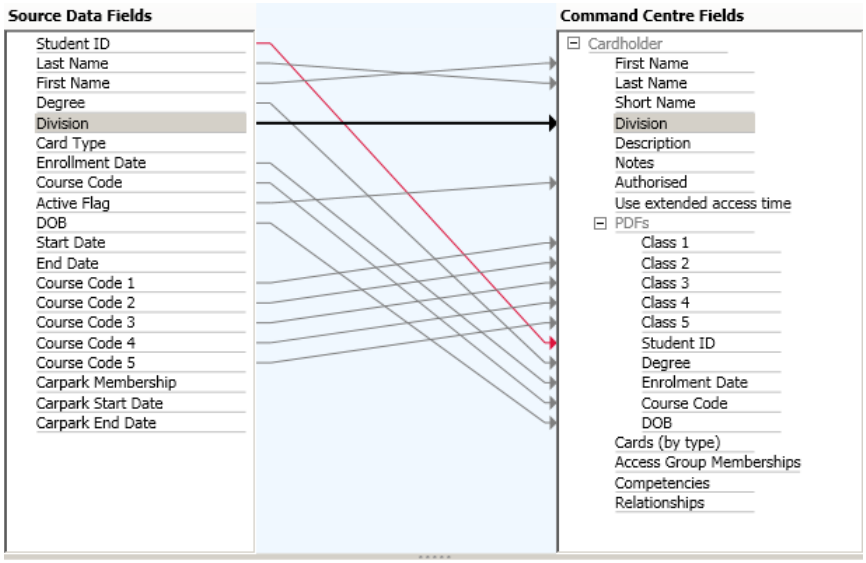
You can import (map) data from a single source field to more than one Gallagher Command Centre field.

Notes:

- If a blank or null value is mapped to the Authorised field, new cardholders will be Authorised. For existing cardholders, this value will remain unchanged.
- If regular expression validation is configured on the PDF field being mapped to, then Enterprise Data Interface will also validate data as it is imported to make sure that it matches the configured regular expression.
- When mapping from a database, if the source field is a related data field containing multiple values and the destination field can only accept a single value, then the cardholder record will not be imported.
- If the source field contains a blank or null value, refer to ***Mapping blank values*** (on page 54-57).

Procedure

1. Select the  tool.
2. Select the source field you wish to map from.
3. Hold down the mouse button and drag the cursor over the Gallagher Command Centre field you wish to map to.
4. Release the mouse button. A black line appears between the two fields and a message appears in the window below.



Mapping from Division to Cardholder Division

For direct mappings to fields such as Notification PDF fields, Access Groups, Cards, Competencies and Relationships, additional information may be supplied as part of the mapping. This information is shown in the panel below the mappings.

For relationship mappings, a role and a related cardholder ID field must also be selected for the mapping to be valid.

Notes:

- When adding cardholders, you will need to create a map to the Division field.
- If the source field contains a blank value, refer to ***Mapping blank values*** (on page 54-57).
- If a blank value is mapped to the Authorised field, new cardholders will be Authorised. For existing cardholders, this value will remain unchanged.
- If regular expression validation is configured on the PDF field being mapped to, then Enterprise Data Interface will also validate data as it is imported to make sure that it matches the configured regular expression.

Creating a cardholder transformation mapping

Introduction

This procedure describes how to create a transformation mapping.
A transformation mapping enables you to transform a source value into a Gallagher Command Centre value. When imported the source value will be changed to the configured Gallagher Command Centre value.

You can create transformation mappings for the following fields:

- Cardholder fields
- Personal Data fields (excluding notification PDFs)
- Card fields
- Access Group Membership fields
- Competency fields

Notes:

- Transformation mappings are not available to Relationship fields or notification PDFs. These fields can only be mapped to with "direct mappings".
- You can import (map) data from a single source field to more than one Gallagher Command Centre field or vice versa.
- If your source field contains blank values, it is recommended that you replace the blank values with a default value. This default value can then be transformed to a value in Gallagher Command Centre.
- Transformations to date fields will use the service account regional settings, which may be different from the users regional settings.
- Database fields are compared in their text representation. Therefore for date data types it may be necessary to define the field format for use in comparison.
- When mapping from a database, if the source field is a related data field containing multiple values and the destination field can only accept a single value, then the cardholder record will not be imported.
- If the source field contains a blank value, refer to ***Mapping blank values*** (on page 54-57).

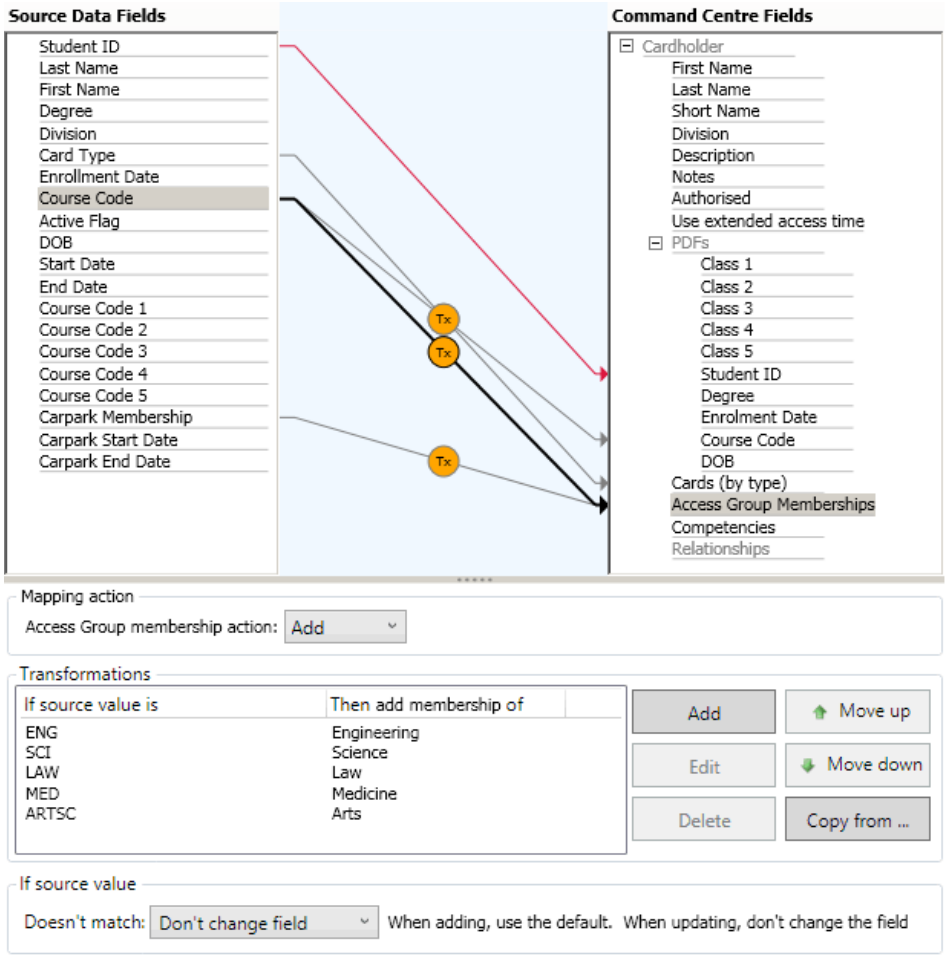
Procedure

This procedure describes how to transform a source value to a Gallagher Command Centre value.

1. Select the  tool.
2. Select the source field containing the source value you wish to transform.

3. Hold down the mouse button and drag the cursor over the Gallagher Command Centre field you wish to map to.
4. Release the mouse button. A black line and the transformation icon are shown between the two fields.

   The transformations grid displays below. This grid lists the transformations for this mapping.



5. To Add a transformation, refer to one of the following topics:
   - ***Adding a Cardholder field transformation*** (on page 54-44)
   - ***Adding a Personal Data Field transformation*** (on page 54-45)
   - ***Adding a Card transformation*** (on page 54-47)
   - ***Adding an Access Group transformation*** (on page 54-51)
   - ***Adding a Competency transformation*** (on page 54-54)
6. To edit a transformation, select the transformation you wish to edit then click the **Edit** button. The Edit Transformation window displays. Edit the transformation as required.
7. To delete a transformation, select the transformation you wish to delete then click the **Delete** button.

8. To move a transformation up, select the transformation you wish to move then click the **Move up** button.
9. To move a transformation down, select the transformation you wish to move then click the **Move down** button.
10. To copy a set of transformations refer to ***Copying transformations*** (on page 54-59).

    Notes:

    - Transformations are performed in the order specified by the transformations grid.
    - The first transformation that matches will be performed only. Any later matches are ignored.
    - You can use the wildcard character "*" as a transformation to catch all remaining values within the source field. This transformation should be listed last in the grid. It is recommended that this transformation is mapped to a default value.
    - If the source value doesn't match a transformation, refer to ***Mapping a value that doesn't match a transformation*** (on page 54-58).

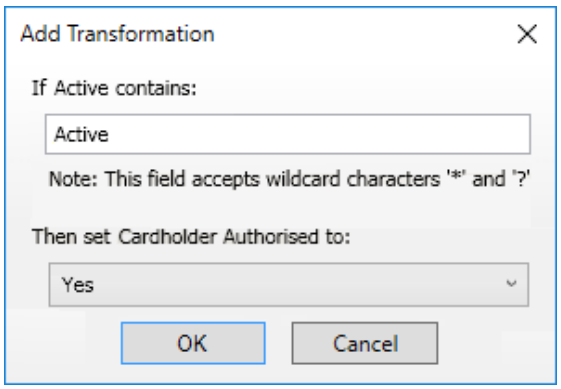
Adding a cardholder field transformation

Introduction

When a source value is transformed, it can be used to assign a cardholder value.

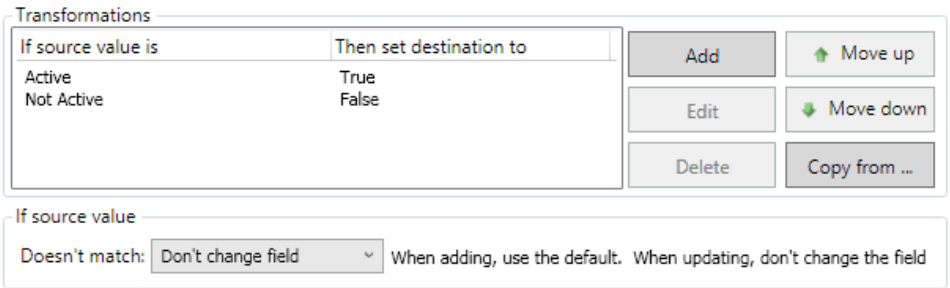
Procedure

1. Create a transformation mapping to the Gallagher Command Centre Cardholder field you wish to map to.
2. Click the **Add** button to add a transformation. The Add Transformation window displays.



Note: The appearance of this window may vary, depending on the destination Cardholder field.

3. In the upper field, enter the source value you wish to transform.
Note: This field accepts wildcard characters. Refer to ***Wildcard characters*** (on page 54-24).
4. In the lower field, enter or select the Cardholder value you wish to set when this source value is transformed.
5. Click the **OK** button. Your transformation is added to the Transformations grid.
6. Repeat as necessary, to add additional transformations.



Note: If the source value doesn't match a transformation, refer to ***Mapping a value that doesn't match a transformation*** (on page 54-58).

Adding a Personal Data Field transformation

Introduction

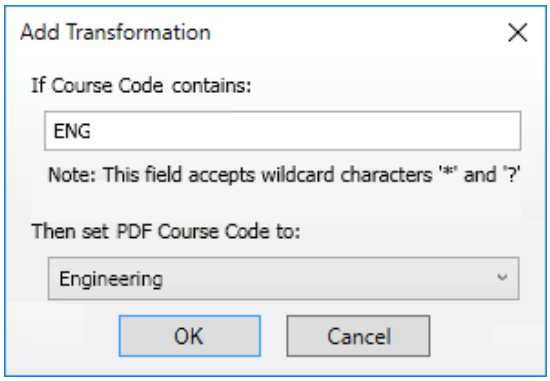
When a source value is transformed, it can be used to assign a Personal Data Field value to cardholders.

You will need to ensure your transformed source value matches the Personal Data field data type.

Notification PDF fields (email and mobile PDF types) cannot be mapped using transformations. Use direct mappings instead.

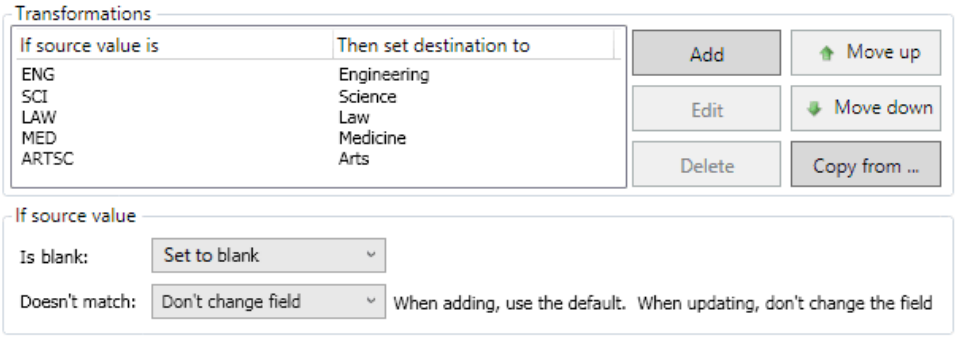
Procedure

1. Create a transformation mapping to the Gallagher Command Centre Personal Data Field you wish to map to.
2. Click the **Add** button to add a transformation. The Add Transformation window displays.



Note: The appearance of this window may vary, depending on the data type of your selected Personal Data Field.

3. In the upper field, enter the source value you wish to transform.
Note: This field accepts wildcard characters. Refer to ***Wildcard characters*** (on page 54-24).
4. In the lower field, enter or select the Personal Data Field value you wish to set when this source value is transformed.
5. Click the **OK** button. Your transformation is added to the Transformations grid.
6. Repeat as necessary, to add additional transformations.



Notes:

- If the source field contains a blank value, refer to ***Mapping blank values*** (on page 54-57).
- If the source value doesn't match a transformation, refer to ***Mapping a value that doesn't match a transformation*** (on page 54-58).

Adding a Card transformation

Introduction

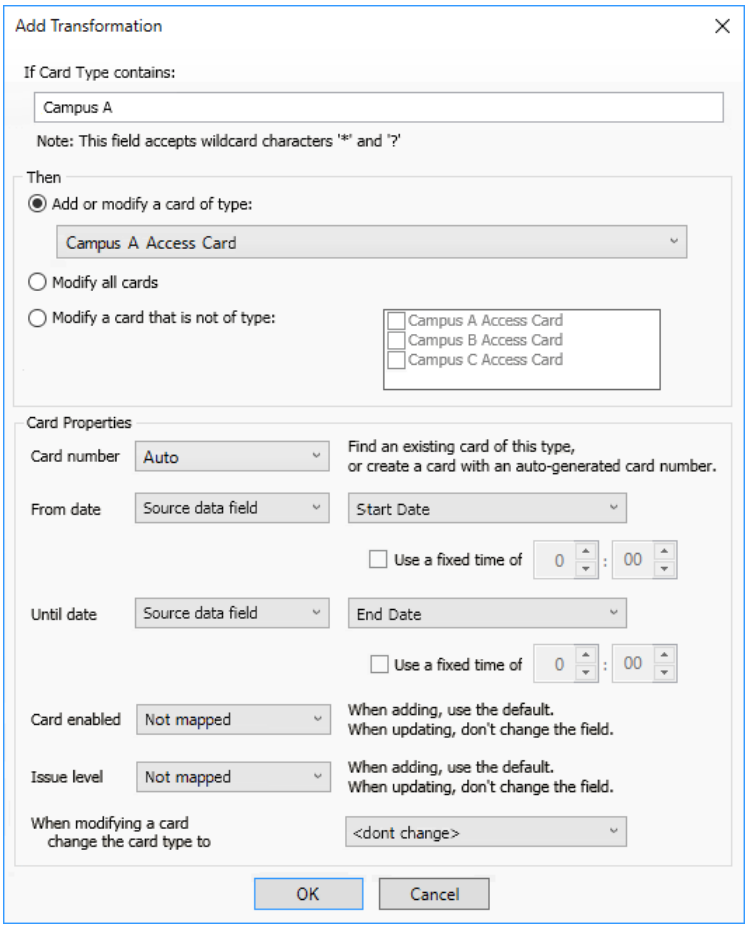
When a source value is transformed, it can be used to assign a card and define the card's properties.

A Card transformation can be used to modify the properties of a particular card type or the properties of all card types assigned to a cardholder.

Alternatively, a Card transformation can be used to change a cardholder's card type. When the cardholder is imported, the cardholder's card type will be changed to that of the card type specified.

Procedure

1. Create a transformation mapping to the Gallagher Command Centre Cards field.
2. Click the **Add** button to add a transformation. The Add Transformation window displays.



3. In the upper field, enter the source value that identifies the card type you wish to add or update.
   Note: This field accepts wildcard characters. Refer to ***Wildcard characters*** (on page 54-24).

4. To assign or modify a single card of this type, ensure the **Add or modify a card of type** radio button is selected.
5. Select the card type you want to assign or modify from the drop down list. The properties of this card will be modified as per the properties below.
    - This card type will be assigned to, or modified for, all values that match the transformation in the source data.
    - If a card of this type has already been assigned, its properties will be updated.

    Note: If you select a GovPass card type additional **Visitor Contractor** fields appear in the Card Properties section (under the **Card enabled** fields). To set the Visitor Contractor, select either:

    - **Not mapped.** When added, the Visitor Contractor will be set to the default, (i.e. Visitor / Contractor = No, Owned by Site = Yes). When updating the card, this value will remain unchanged.
    - **Fixed value.** Select either "Visitor / Contractor" or "Full Rights".

If set to…	the settings on the Cardholder Cards tile in Command Centre Client will be…
Visitor / Contractor	Visitor / Contractor = Yes, Owned by Site = Yes
Full Rights	Visitor / Contractor = No, Owned by Site = Yes

    - **Source data field.** Select the appropriate source data field value.

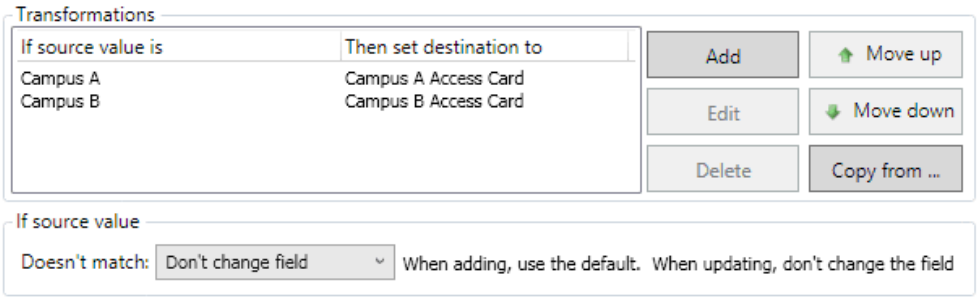
If value is…	the settings on the Cardholder Cards tile in Command Centre Client will be…
Either 1 or True	Visitor / Contractor = Yes, Owned by Site = Yes
Either 0 or False	Visitor / Contractor = No, Owned by Site = Yes

6. To modify all cards of any type assigned to cardholders, select the **Modify all cards** radio button. The properties of all existing cards on the cardholder will be modified as per the properties below.
7. To modify a card type (excluding specific card types), select the **Modify a card that is not of type** radio button, then select the card types that will not be modified.
8. To set the card number, select either:
    - **Auto**. When added, a card number will be automatically generated. When updating the card, the card number will remain unchanged. Only one card of this type should exist on the cardholder, when specifying "Auto". Otherwise the card number must be supplied in the source file.
    - **Source data field**. Select the source field to retrieve the card numbers from.
        - If the source field contains a blank value, the cardholder record will fail to import.
        - If the source field contains a non card number value, (text, negative number or out of range) the cardholder record will fail to import.

9. To set the card enabled From date and card enabled Until date, click the From or Until date drop down arrow and select either:
   - **Not mapped**. When added, the date and time will be set to the default card type date and time. If a date and time has already been set, this value will remain unchanged.
   - **Fixed date**. Enter a date and time. The Until date and time must be greater than or equal to the From date and time.
   - **Source data field**. Select a source field to retrieve the date and time from.

     If you wish to specify a fixed From time or fixed Until time, check the "Use a fixed time of" check-box and enter a time. This time will override the time specified by the source field.
     - If the source field contains a date but not a time and the "Use a fixed time of" check box is unchecked, the time will be set at 0:00 hours on the From date and 0:00 hours on the Until date.
     - If the source field contains a time but not a date, then today's date will be used.
     - If the source field contains a non date value, the cardholder record will fail to import.
     - If the Until date and time is less than the From date and time, the cardholder record will fail to import.
     - If the source field contains a blank value, the From or Until date and time will not be set.
10. To enable or disable the card, select either:
    - **Not mapped**. When added, the card will be enabled. When updating the card, this value will remain unchanged.
    - **Fixed value**. Select either "Card Enabled" or "Card Disabled".
    - **Source data field**. Select a source field to retrieve the enabled or disabled value from. Boolean characters will be used to determine if the card is enabled or disabled.
      Refer to ***Mapping Boolean values*** (on page 54-60).
11. To set the card issue level, select either:
    - **Not mapped**. When added, the issue level will be set to the card type default. When updating the card, this value will remain unchanged.
    - **Fixed value**. Enter an issue level for the card (0-15).
    - **Source data field**. Select the source field to retrieve the issue level value from.
      - If the source field contains a non issue level value, the cardholder record will fail to import.

12. To set the card type, select a card type from the drop-down list.
    Notes:
    - The "Edit Enterprise Data Interfaces" operator privilege enables an operator to view all card types in the drop-down list.
    - Only card types with the same Region Code and Facility Code can be changed.
    - The card transformation has to match one card on the cardholder. If a cardholder has multiple cards of one type, then the record will fail.
    - A card type cannot be added and changed using a single transformation.
13. Click the **OK** button. Your transformation is added to the Transformations grid.
14. Repeat as necessary, to add additional transformations.



Note:

- If the source value doesn't match a transformation, refer to ***Mapping a value that doesn't match a transformation*** (on page 54-58).
- When mapping from a database, if the source field is a related data field containing multiple values, then each value will be processed in turn.

Adding an Access Group transformation

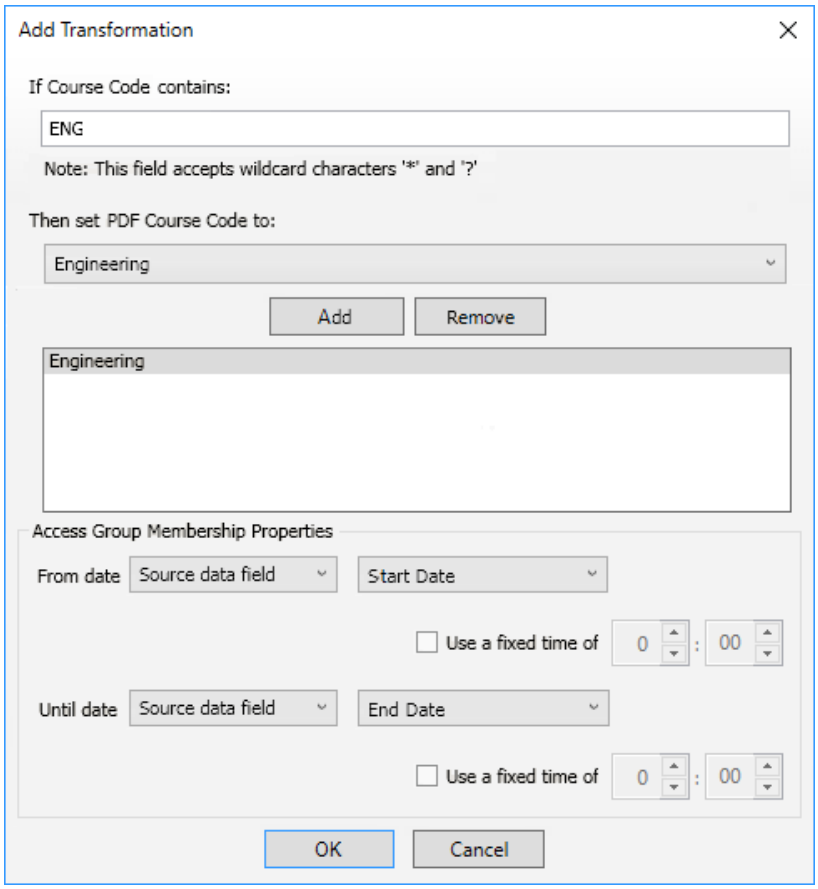
Introduction

When a source value is transformed, it can be used to change a cardholder's Access Group membership, either permanently or temporarily.
The source value will specify which Access Groups to add cardholders to, or which Access Groups to remove cardholders from.
Notes:

- The Access Groups you can map to are limited to the Access Groups present in Gallagher Command Centre.
- If an Access Group has a Required Personal Data Field assigned and a value has not been entered for the Required Personal Data Field, the cardholder will not be added to the Access Group until a value is entered.
- If the "Run As Operator" does not have both the "Modify Access Control" and "Edit Cardholder" privileges assigned for the Division the cardholder's Access Groups are in, then the cardholder record will fail to be imported.
- If a cardholder is added temporarily to an Access Group and the Temporary Access Group value and mapping remains, then each time the cardholder is imported another Temporary Access instance will be added (to the Cardholder's Access Groups tab).
- If an Access Group has been configured with a default "From" or "Until" date, the cardholder will receive these dates when added to the Access Group, if no other dates have been specified by the cardholder.

Procedure

1. Create a transformation mapping to the Gallagher Command Centre Access Group Memberships field.
2. To add cardholder memberships, select **Add** from the Access Group membership action drop down list.
3. To remove cardholder memberships, select **Remove** from the Access Group membership action drop down list.
4. Click the **Add** button to add a transformation. The Add Transformation window displays.



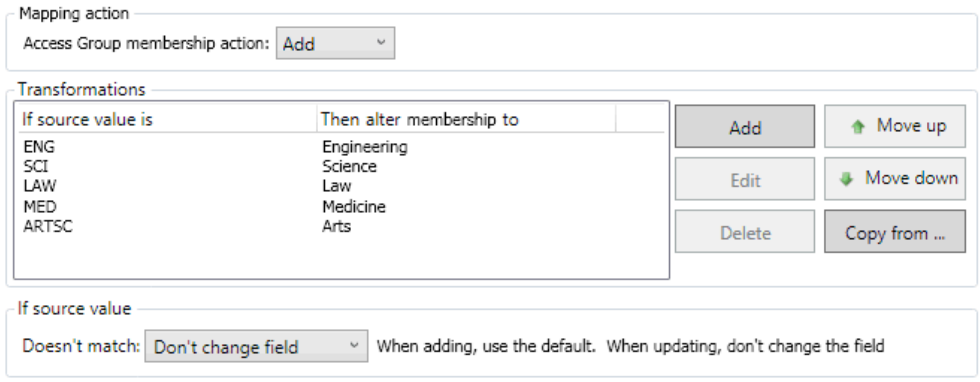
5. In the upper field, enter the source value you wish to transform.
   Note: This field accepts wildcard characters. Refer to ***Wildcard characters*** (on page 54-24).
6. Select the Access Group whose membership you want to change and click the **Add** button.
7. To add additional Access Groups, repeat the above step.

   Cardholders will either be added to the Access Groups listed in the grid, or removed from the Access Groups listed in the grid.
8. To remove an Access Group from the grid, select the appropriate Access Group in the grid and click the **Remove** button.
9. To set a From date and time and Until date and time for all Access Groups listed in the grid, click the From or Until date drop down arrow and select either:
   - **Not mapped**. When added, the date and time will be set to the default Access Group Membership date and time. If a date and time has already been set, this value will remain unchanged.
   - **Fixed date**. Enter a date and time. The Until date and time must be greater than or equal to the From date and time.
   - **Source data field**. Select a source field to retrieve the date and time from.

If you wish to specify a fixed From time or fixed Until time, check the "Use a fixed time of" check-box and enter a time. This time will override the time specified by the source field.

- If the source field contains a date but not a time and the "Use a fixed time of" check box is unchecked, the time will be set at 0:00 hours on the From date and 0:00 hours on the Until date.
- If the source field contains a time but not a date, then today's date will be used.
- If the source field contains a non date value, the cardholder record will fail to import.
- If the Until date and time is less than the From date and time, the cardholder record will fail to import.
- If the source field contains a blank value, the From or Until date and time will not be set.

10. Click the **OK** button. Your transformation is added to the Transformations grid.
11. Repeat as necessary, to add additional transformations.



Notes:

- If the source value doesn't match a transformation, refer to ***Mapping a value that doesn't match a transformation*** (on page 54-58).
- When mapping from a database, if the source field is a related data field containing multiple values, then each value will be processed in turn.

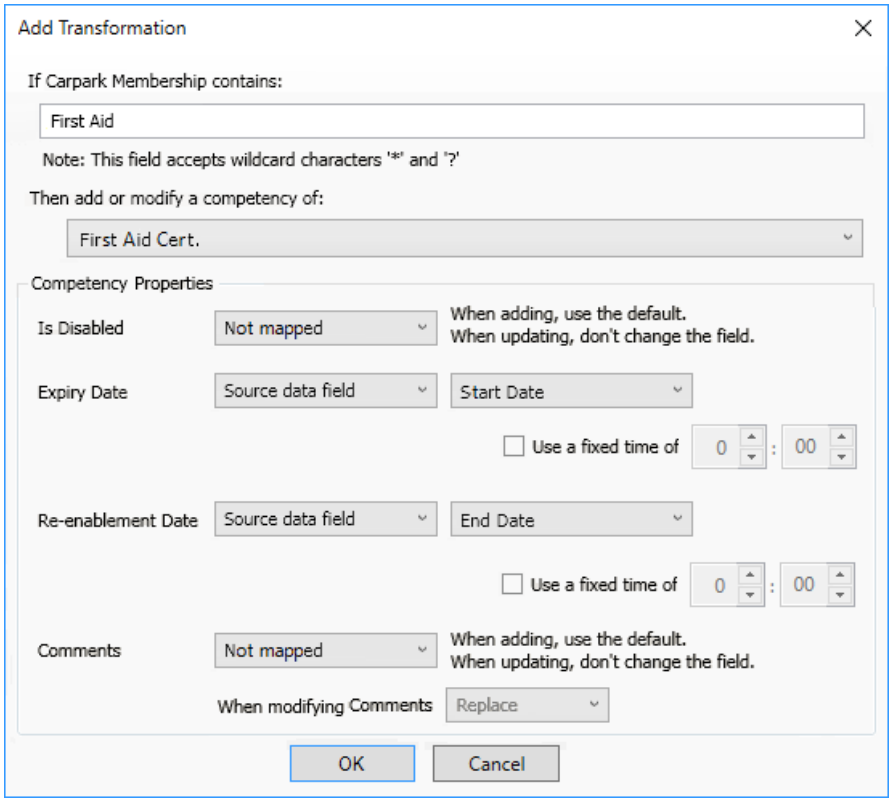
Adding a Competency transformation

Introduction

When a source value is transformed, it can be used to add, update or remove a competency from a cardholder.

Procedure

1. Create a transformation mapping to the Gallagher Command Centre Competencies field.
2. Click the **Add** button to add a transformation. The Add Transformation window displays.



3. In the upper field, enter the source value you wish to transform.
   Note: This field accepts wildcard characters. Refer to ***Wildcard characters*** (on page 54-24).
4. Select the competency you want to assign to cardholders, from the drop down list.
5. To enable or disable the competency, select either:
   - **Not mapped**. When added, the competency will be enabled. When updated, this value will remain unchanged.
   - **Fixed value**. Select either Disabled or Enabled. Disabled will disable the competency until the specified Re-enablement Date. Enabled will activate the competency until the specified Expiry Date.

- **Source data field**. Select a source field to retrieve the enabled or disabled value from. Boolean characters will be used to determine if the competency is enabled or disabled. A positive value will disable the competency. Refer to ***Mapping Boolean values*** (on page 54-60).

6. To set an expiry date and time for the competency, select either:
   - **Not mapped**. When added, the competency default expiry date and time will be used. When updated, this value will remain unchanged.
   - **Fixed value**. Enter a date and time.
   - **Source data field**. Select a source field to retrieve the date and time from.

     If you wish to specify a fixed expiry time, check the "Use a fixed time of" check-box and enter a time. This time will override the time specified by the source field.

     - If the source field contains a date but not a time and the "Use a fixed time of" check box is unchecked, the competency will expire at a time of 0:00 hours on the defined date.
     - If the source field contains a time but not a date, then today's date will be used.
     - If the source field contains a non date value, the cardholder record will fail to import.
     - If the source field contains a blank value, a transformation mapping will clear the competency's expiry date and time. Note that this is the opposite behaviour from a direct mapping.
7. To re-enable the competency at a specified date and time, select either:
   - **Not mapped**. When added, the competency will remain disabled. When updated, this value will remain unchanged.
   - **Fixed value**. Enter a date and time.
   - **Source data field**. Select a source field to retrieve the date and time from.

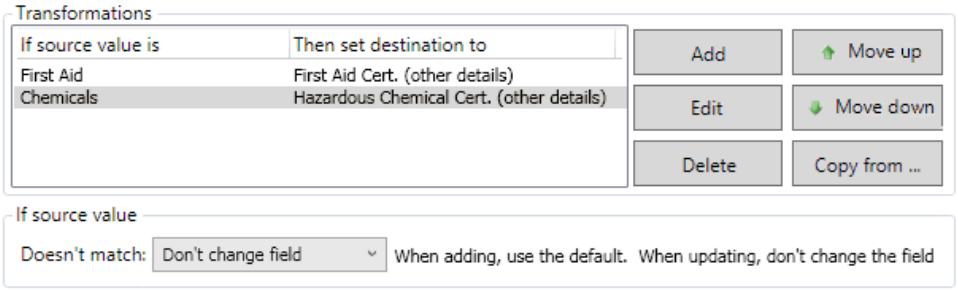
     If you wish to specify a fixed re-enablement time, check the "Use a fixed time of" check-box and enter a time. This time will override the time specified by the source field.

     - If the source field contains a date but not a time and the "Use a fixed time of" check box is unchecked, the competency will re-enable at a time of 0:00 hours on the defined date.
     - If the source field contains a time but not a date, then today's date will be used.
     - If the source field contains a non date value, the cardholder record will fail to import.

- If the source field contains a blank value, the re-enablement date and time will not be set.

8. To add a comment to the competency, select either:
   - **Not mapped**. When added, a comment will not be added. When updated, the comment will remain unchanged.
   - **Fixed value**. Enter your free-form text comment (limited to 1500 characters).
   - **Source data field**. Select a source field to retrieve the comment from.
     - If the source field contains a blank value, the comment field will be set to blank.
9. To replace the existing comment, select **Replace** from the drop down list.
10. To append the comment, select **Append** from the drop down list.

    If the new text when added, exceeds the maximum size for the comment field, text will be removed from the beginning.
11. Click the **OK** button. Your transformation is added to the Transformations grid.
12. Repeat as necessary, to add additional transformations.



Notes:

- If the source value doesn't match a transformation, refer to ***Mapping a value that doesn't match a transformation*** (on page 54-58).
- If you have mapped more than one source field to a competency (not recommended), then the last mapping listed in the Edit Mappings window will be used to add/update the competency for the cardholder.
- When mapping from a database, if the source field is a related data field containing multiple values, then each value will be processed in turn.

Mapping blank values

Introduction

When setting a direct or transformation mapping, you will need to define what will happen if the source value is blank.

Notes:

- For a Cardholder Interface, if a blank value is present in an ID mapping, the cardholder will not be added, updated or removed.
- For a Booking Interface, if a blank value is present in an ID mapping, the bookable resource for the bookings to be imported into will not be found, and therefore the bookings will not be added, changed or removed.
- When mapping from a database, null or an empty string is regarded as a blank value.
- When importing a null or blank value for a Booking field, the booking import will fail. The exception to this rule is the Booking Name field. A blank value can be imported for the Booking Name field. The default value for the Booking Name field is blank.
- For direct mappings of Cards, Access Groups and Competency fields, if the source data is blank it acts as an "ignore mapping", (e.g. it won't add an Access Group or remove any existing Access Groups).

If a source value is blank you can choose to either:



- **Set to blank**
  The field will be set to blank. Any existing value is removed.
- **Don't perform mapping**
  When updating a cardholder, the existing value remains unchanged.

  When adding a cardholder, the Gallagher Command Centre default will be used, if a default has not been specified the field will be set to blank.

  For the fields 'Authorised' and 'Use extended access time' the Gallagher Command Centre defaults will be used. Authorised=True, Use extended access time=False.

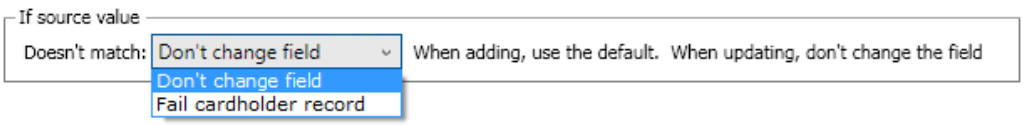
Mapping a value that doesn't match a transformation

Introduction

When setting a transformation mapping, you will need to define what will happen if a source value doesn't match a transformation.

Note: If you have used a wildcard character to catch all values within a source field, selecting one of the below options has no effect.

If the source value doesn't match a transformation, you can choose to either:



- **Don't change field**
  When adding a cardholder, the Gallagher Command Centre default will be used, if a default has not been specified the field will be set to blank.

  When updating a cardholder, the existing value remains unchanged.

  When importing a source value that doesn't match a transformation for a booking field, the default value will be used.
- **Set to source value**
  This option effectively does a direct mapping. It matches the name of the data coming from the data source file to an Command Centre item name in Command Centre, and adds it with the default values on the Command Centre item.
- **Fail data record**
  The record will fail to import.

  Use this to indicate that all possible values have been specified. If the source field contains a value that is not listed as a transformation, then the record is in error.

Copying transformations

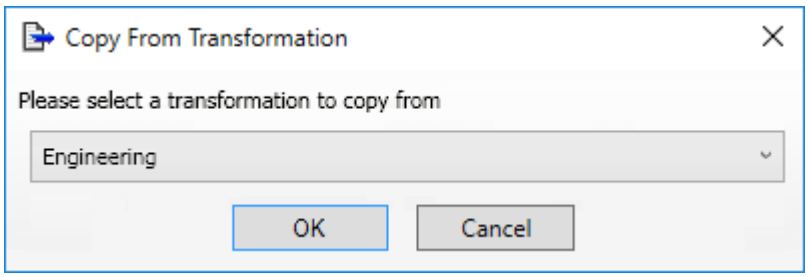
Introduction

You can copy a set of transformations to another transformation mapping. You can then edit the transformations, if required.

Transformations must be copied from the same Gallagher Command Centre field type, (e.g. a set of Personal Data Field transformations, can only be copied from another Personal Data Field transformation mapping).

Procedure

1. Select the map you wish to copy transformations into.
2. Click the **Copy from...** button.
   The Copy From Transformation window displays.



3. Click the drop-down arrow and select the map you wish to copy transformations from.
4. Click the **OK** button. The transformations are displayed in the Transformations grid.

   Note: If this transformation map already contains one or more transformations, a dialog box displays. Click **Yes** to clear the existing transformations. Click **No** to retain the existing transformations. The copied transformations will be added to the Transformations grid.

Mapping Boolean values

Gallagher Command Centre Boolean fields are:

- Authorised
- Use extended access time
- Card Enabled, and
- Competency Is Disabled

When mapping to a Boolean field, you will need to use the values defined below:

Positive value	Negative value
YES	NO
TRUE	FALSE
Y	N
T	F
1	0
ENABLE	DISABLE
ENABLED	DISABLED
E	D

Notes:

- If the source value is not one of these values, the cardholder record will fail to import, (i.e. results in a formatting error).
- When importing from a database, if the source field type is numeric, use either "1" or "0". Other Boolean values should not be used.
- Alternatively, for "Authorised" and "Use extended access time" consider using a transformation mapping.

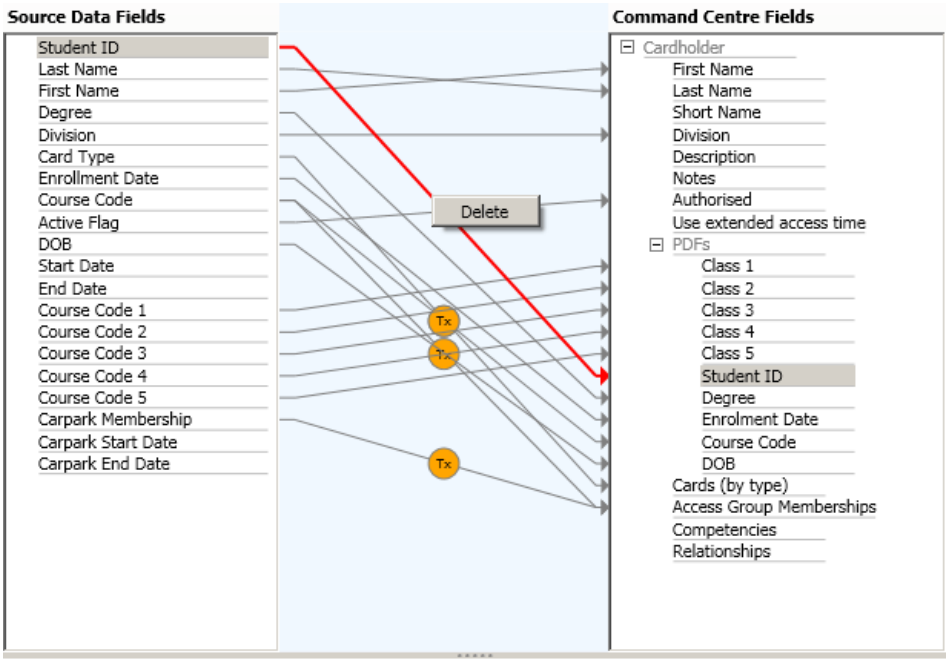
Removing a mapping

Introduction

This procedure describes how to remove a mapping from the Edit Mappings window.

Procedure

1. Open the Edit Mappings window.
2. Right click the mapping you wish to remove.
   The Delete button displays.



ID Mapping from Student ID to PDF Student ID

3. Select **Delete**. The mapping is removed from the interface.

   Note: Alternatively, select the mapping you wish to delete then press the delete key on your keyboard. The mapping is removed from the interface.

Mapping booking data to Gallagher Command Centre fields

Introduction

This section of the manual describes how to map fields from your source data to Gallagher Command Centre fields.

Replace processing mode

Replace processing mode assumes all bookings have been provided from the third party system. At processing time the booking record for a bookable resource will be:

- removed if the booking no longer exists;
- added if the booking never existed;
- changed if the booking reference is provided and the booking has been changed;
- remain if the booking details are the same

Notes:

- As mentioned above, all booking data must be provided from the third party system. If the third party system provides booking data for the latest bookings only, the existing bookings will be removed.
- A booking for a bookable resource may occur at the same time or overlap another booking for the same bookable resource. This behaviour is by design, and allows for more flexibility in the booking system.

Command Centre fields

The following table describes the Command Centre bookable resource fields.

Field	Data Type	Description
Name	String. Maximum 110 alpha-numeric characters.	The bookable resource name. This field must be mapped. This field requires an ID mapping. The value mapped cannot be blank.
Booking Reference	String. Maximum 255 alpha-numeric characters.	The unique booking ID provided by the third party system. If mapped, the value cannot be blank.
Booking Name	String. Maximum 255 alpha-numeric characters.	The display name given to the booking. Used in status messages, events and alarms in Command Centre. If mapped, the value can be blank.

Field	Data Type	Description
Start Date	Date/Time	The start date of the booking. This field must be mapped.
End Date	Date/Time	The end date of the booking. If mapped, the value cannot be blank.
Start Time	Date/Time	The start time of the booking. This field must be mapped.
End Time	Date/Time	The end time of the booking. This field must be mapped.
Interval Type	Interval Type	Can be used if the source data doesn't specify a booking end date. Enables you to specify re-occurring bookings, (i.e. One Off, Daily, Weekly or Monthly). Use either the Interval Count or the Occurrence Pattern field to specify the repeat instances. Defaults to "One Off" if not specified.
Interval Count	Numeric. Maximum 32767 numeric characters.	The number of re-occurring instances for the booking. Defaults to "1" if not specified.
Occurrence Pattern	String that must only contain the characters "1" or "0". Maximum 64 characters.	The number of re-occurring instances for the booking. Where "1" is a booking instance. Maximum 64 characters.

Notes:

- If the booking end date is specified, and the booking spans more than one day, the booking will run until the end date and time is reached.
- Repeat bookings, (i.e. bookings using an Interval Type of daily, weekly, or monthly and an Interval Count/Occurrence Pattern mapping) cannot be configured to span midnight.
- The dates and times for a booking must be synchronized with the Command Centre server PC time zone.
- If the date for a monthly re-occurring booking falls on a day that does not exist in the calendar, (e.g. 31st of February), then the booking will occur on the last day of that month, (e.g. 28th February).

- If a Booking Reference has been provided, then the last record processed containing the Booking Reference will be imported. All other booking instances containing the Booking Reference will not be imported. However, the same Booking Reference can be used by two bookings on different bookable resources.

Procedure

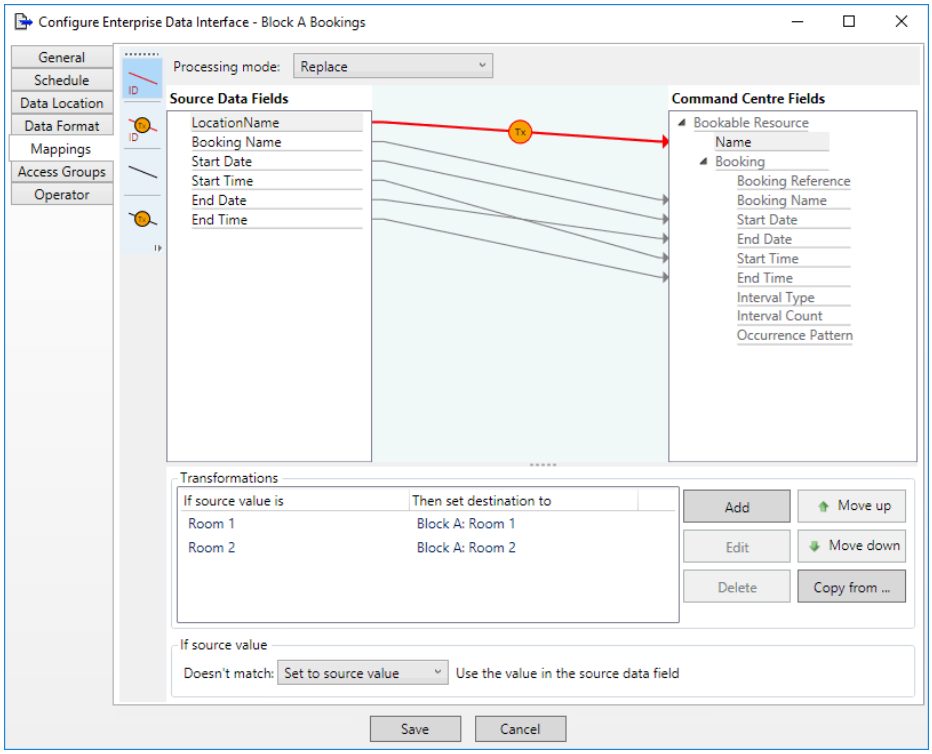
To map fields from your source data to Command Centre fields, complete the following procedure:

1. Click the **Mappings and Operator** tab.
2. Click **Configure**. The Edit Mappings window opens.
   This window displays the fields you defined on the Data Format tab (these fields originate from your source file) and all Gallagher Command Centre fields that can have data imported.
3. Select **Add or update** from the Cardholder mode drop-down list.
4. If you want to retain the cardholder's pre-existing Access Groups, select **Merge** from the Access Group mode drop-down list.
5. If you want to set Access Groups to the mapped Access Groups only, select **Replace** from the Access Group mode drop-down list.
6. To continue mapping source fields to Gallagher Command Centre fields, refer to the following topics:
   - ***Creating an ID mapping*** (on page 54-38)
   - ***Creating a direct mapping*** (on page 54-39)
   - ***Creating a transformation mapping*** (on page 54-41)

Removing cardholders

If the purpose of your interface is to remove cardholders, complete the following procedure:

1. Click the **Mappings and Operator** tab.
2. Click **Configure**. The Edit Mappings window opens.



This window displays the fields you defined on the **Data Format** tab (these fields originate from your source data) and all Command Centre fields that can have data imported.

3. To continue mapping source fields to the Command Centre fields, refer to the following topics:

   - ***Creating a booking ID mapping*** (on page 54-66)
   - ***Creating a booking ID transformation mapping*** (on page 54-67)
   - ***Creating a booking direct mapping*** (on page 54-70)
   - ***Creating a booking transformation mapping*** (on page 54-71)

Creating a booking ID mapping

Introduction

This procedure describes how to create a booking ID mapping.

An ID mapping identifies the bookable resources in Command Centre. An ID mapping must be present in order to add, update or remove bookings.
Notes:

- Only one ID mapping can be set.
- The ID mapping must be set to the Command Centre Bookable Resource Name field.
- The source field used as an ID mapping can also be used to map to other Command Centre fields.
- When mapping from a database, the source field used as an ID mapping must contain a single value.
- If the source field used as an ID mapping contains a blank or null value, the bookings will not be imported.

Procedure

1. Select the 

tool.
2. Select the source field you wish to map from.
3. Hold down the mouse button and drag the cursor over the Command Centre Bookable Resource Name field.

   Note: The  icon will only appear for the Command Centre Bookable Resource Name field.
4. Release the mouse button. A red line appears between the two fields and a message appears in the window below.



ID Mapping from Location to Name

Creating a booking ID transformation mapping

Introduction

This procedure describes how to create a booking ID transformation mapping.

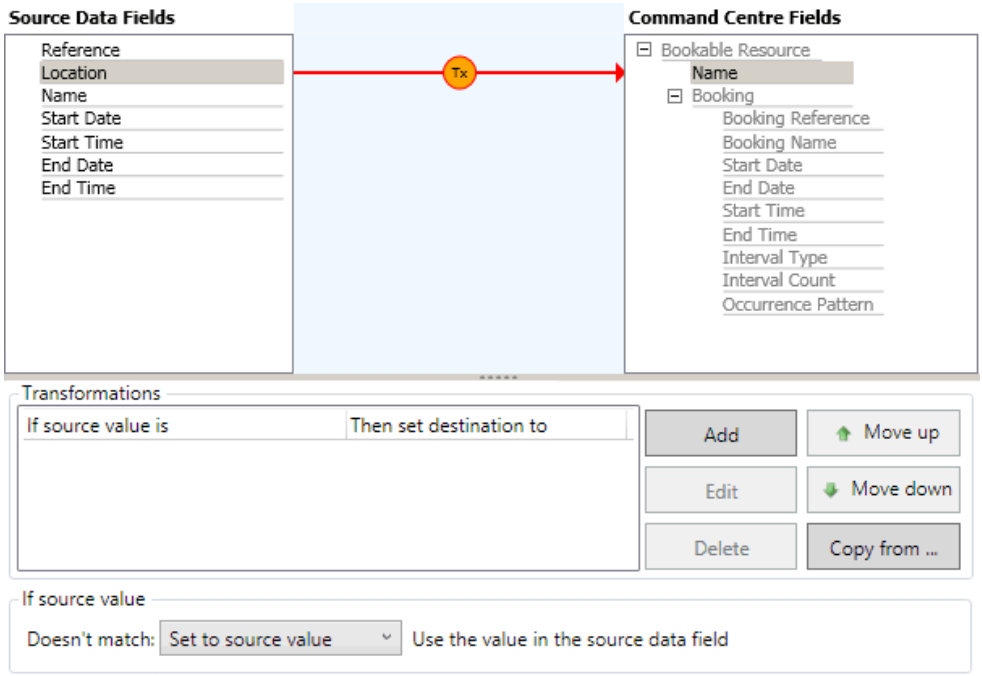
An ID transformation mapping enables you to transform a source value into a Bookable Resource Name.
When an import is run, the bookings for the source value will be applied to the selected bookable resource.
Notes:

- Only one ID mapping can be set.
- The ID mapping must be set to the Command Centre Bookable Resource Name field.
- The source field used as an ID mapping can also be used to map to other Command Centre fields.
- When mapping from a database, the source field used as an ID mapping must contain a single value.
- If the source field used as an ID mapping contains a blank or null value, the bookings will not be imported.

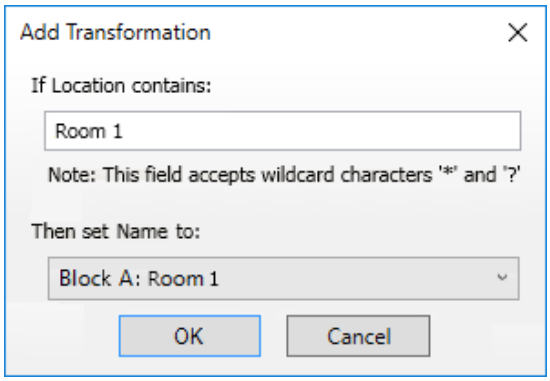
Procedure

1. Select the  tool.
2. Select the source field containing the source value you wish to transform.
3. Hold down the mouse button and drag the cursor over the Command Centre Bookable Resource Name field.

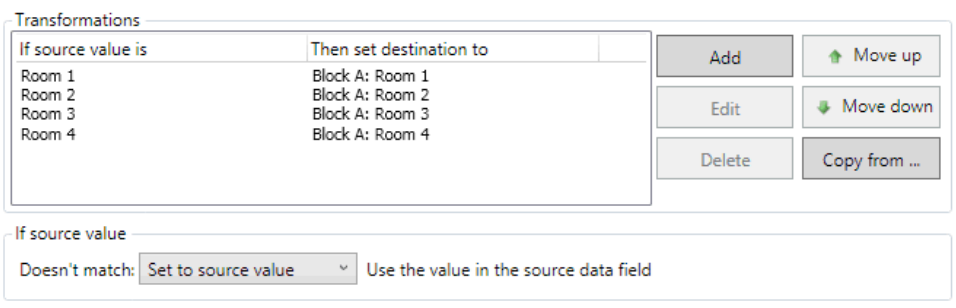
   Note: The  icon will only appear for the Command Centre Bookable Resource Name field.
4. Release the mouse button. A red line and the transformation icon are shown between the two fields.
   The transformations grid displays below. This grid lists the transformations for this mapping.



5. Click the **Add** button to add a transformation. The Add Transformation window displays.



6. In the upper field, enter the source value you wish to transform.
   Note: This field accepts wildcard characters. Refer to ***Wildcard characters*** (on page 54-24).
7. In the lower field select the Bookable Resource Name you wish to set when this source value is transformed.
8. Click the **OK** button. Your transformation is added to the Transformations grid.
9. Repeat as necessary, to add additional transformations.



10. To edit a transformation, select the transformation you wish to edit then click the **Edit** button. The Edit Transformation window displays. Edit the transformation as required.
11. To delete a transformation, select the transformation you wish to delete then click the **Delete** button.
12. To move a transformation up, select the transformation you wish to move then click the **Move up** button.
13. To move a transformation down, select the transformation you wish to move then click the **Move down** button.

Notes:

- Transformations are performed in the order specified by the transformations grid. The first transformation that matches will be performed only. Any later matches are ignored.
- You can use the wildcard character "*" as a transformation to catch all remaining values within the source field. This transformation should be listed last in the grid. It is recommended that this transformation is mapped to a default value. If the date and time of one booking coincides with that of another booking, the booking that is processed later will be imported.
- If the source value doesn't match a transformation, refer to ***Mapping a value that doesn't match a transformation*** (on page 54-58).

Creating a booking direct mapping

Introduction

This procedure describes how to create a booking direct mapping. A direct mapping imports the exact data from your source field into Command Centre. You can create direct mappings for the following Command Centre Booking fields:

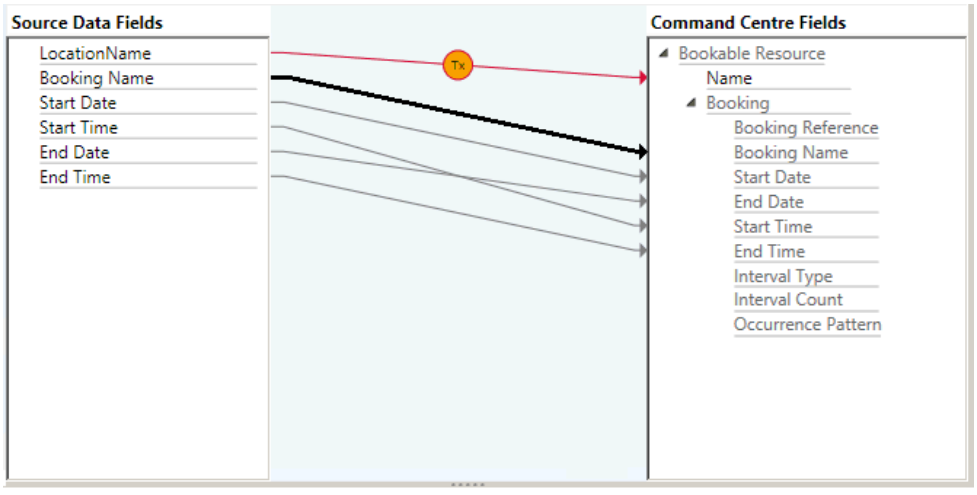
- Booking Name
- Start Date
- End Date
- Start Time
- End Time
- Interval Count
- Occurrence Pattern
- Interval Type
- Booking Reference

Notes:

- You can import (map) data from a single source field to more than one Booking field.
- When mapping from a database, the source field used as a direct mapping must contain a single value.
- If the Booking Reference is used, then all updates are applied to that booking and are not new bookings.

Procedure

1. Select the  tool.
2. Select the source field you wish to map from.
3. Hold down the mouse button and drag the cursor over the Command Centre field you wish to map to.
4. Release the mouse button. A black line appears between the two fields and a message appears in the window below.



Mapping from Booking Name to Booking Name

Creating a booking transformation mapping

Introduction

This procedure describes how to create a booking transformation mapping.

A transformation mapping enables you to transform a source value into a Command Centre value.
When imported the source value will be changed to the configured Command Centre value.

You can create transformation mappings for the following Command Centre Booking fields:

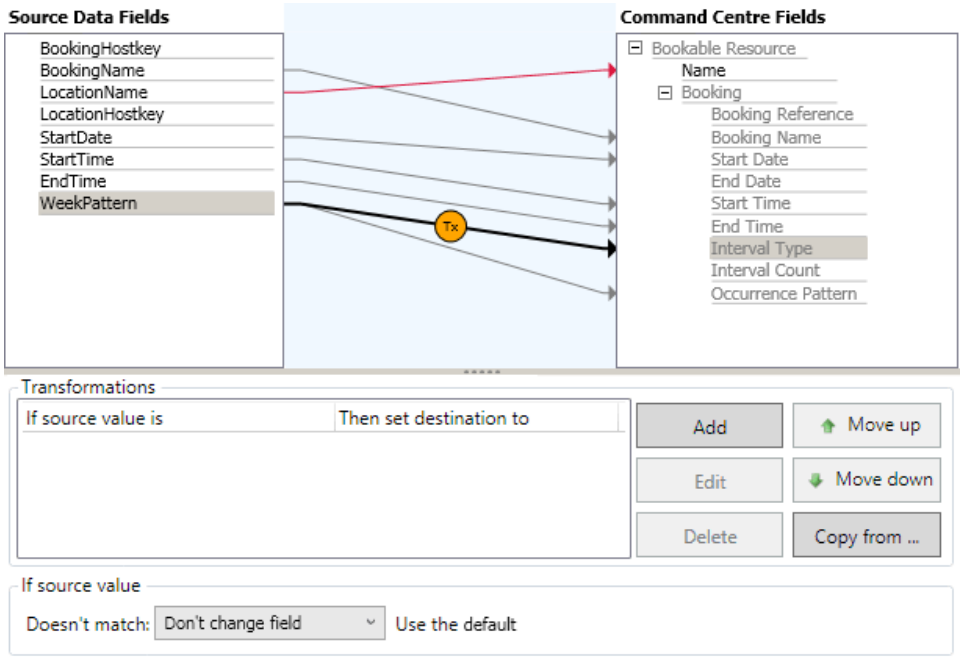
- Booking Name
- Interval Type
- Interval Count
- Occurrence Pattern

Notes:

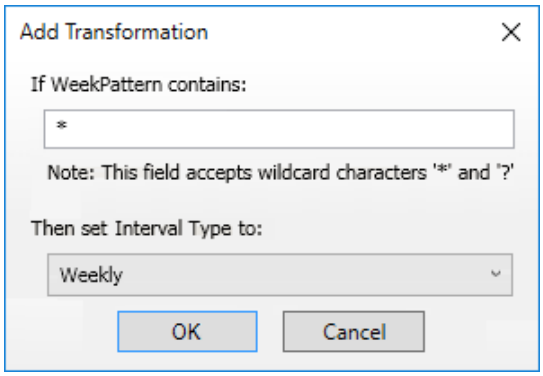
- You can import (map) data from a single source field to more than one Command Centre field.
- If your source field contains blank values, it is recommended that you create a transformation that maps blank values to a default Command Centre value.
- When mapping from a database, the source field used as a transformation mapping must contain a single value.

Procedure

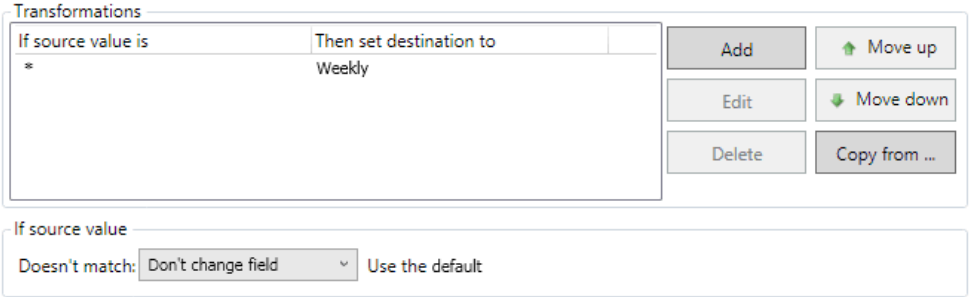
1. Select the  tool.
2. Select the source field containing the source value you wish to transform.
3. Hold down the mouse button and drag the cursor over the Command Centre field you wish to map to.
4. Release the mouse button. A black line and the transformation icon are shown between the two fields.
   The transformations grid displays below. This grid lists the transformations for this mapping.



5. Click the **Add** button to add a transformation. The Add Transformation window displays.



6. In the upper field, enter the source value you wish to transform.
   Note: This field accepts wildcard characters. Refer to ***Wildcard characters*** (on page 54-24).
7. In the lower field, enter or select the booking value you wish to set when this source value is transformed.
8. Click the **OK** button. Your transformation is added to the Transformations grid.
9. Repeat as necessary, to add additional transformations.



10. To edit a transformation, select the transformation you wish to edit then click the **Edit** button. The Edit Transformation window displays. Edit the transformation as required.
11. To delete a transformation, select the transformation you wish to delete then click the **Delete** button.
12. To move a transformation up, select the transformation you wish to move then click the **Move up** button.
13. To move a transformation down, select the transformation you wish to move then click the **Move down** button.

Notes:

- Transformations are performed in the order specified by the transformations grid. The first transformation that matches will be performed only. Any later matches are ignored.
- You can use the wildcard character "*" as a transformation to catch all remaining values within the source field. This transformation should be listed last in the grid. It is recommended that this transformation is mapped to a default value.
- If the source value doesn't match a transformation, refer to ***Mapping a value that doesn't match a transformation*** (on page 54-58).

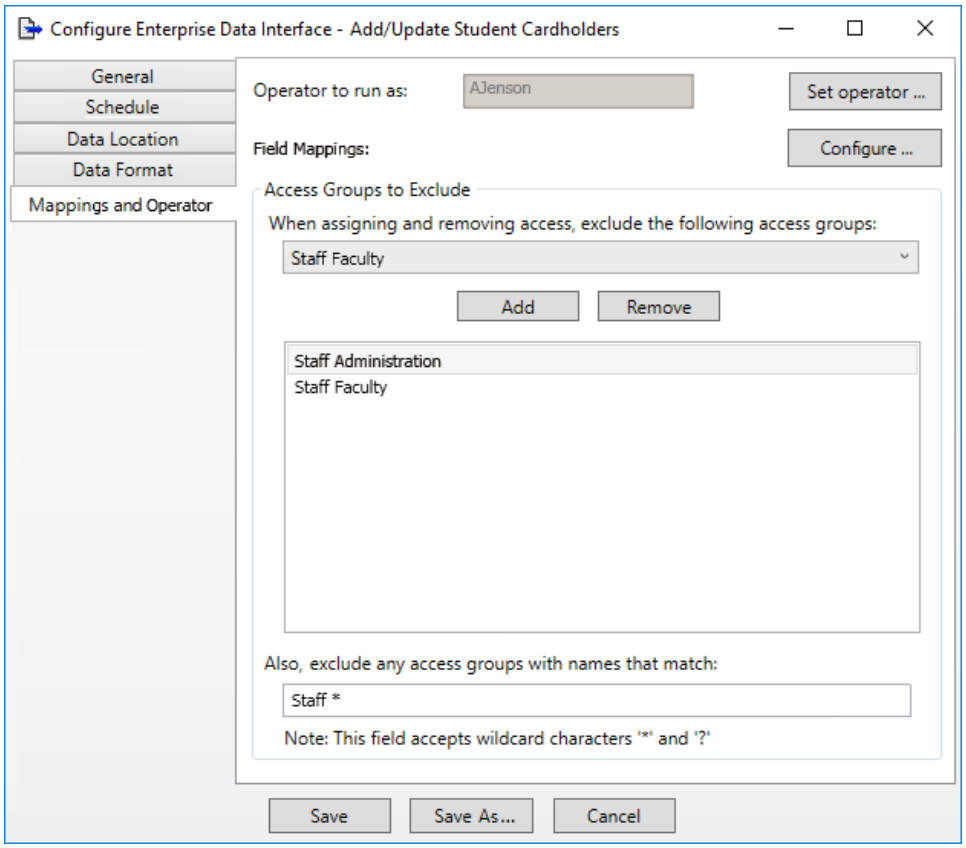
Excluding Access Groups

Introduction

This procedure describes how to exclude specific Access Groups when assigning and removing access.

Procedure

1. Click the **Mappings and Operator** tab.



2. Select the Access Group you want to exclude when processing a cardholder's access from the **Access Groups to Exclude** drop-down list.
3. Click the **Add** button. The Access Group is added to the exclusion list below.
4. To remove an Access Group from the grid, click the **Remove** button.
5. You can type the name of an Access Group to exclude in the field below. This field accepts wildcard characters. By using wildcard characters you can specify multiple Access Groups to exclude. Refer to ***Wildcard characters*** (on page 54-24).

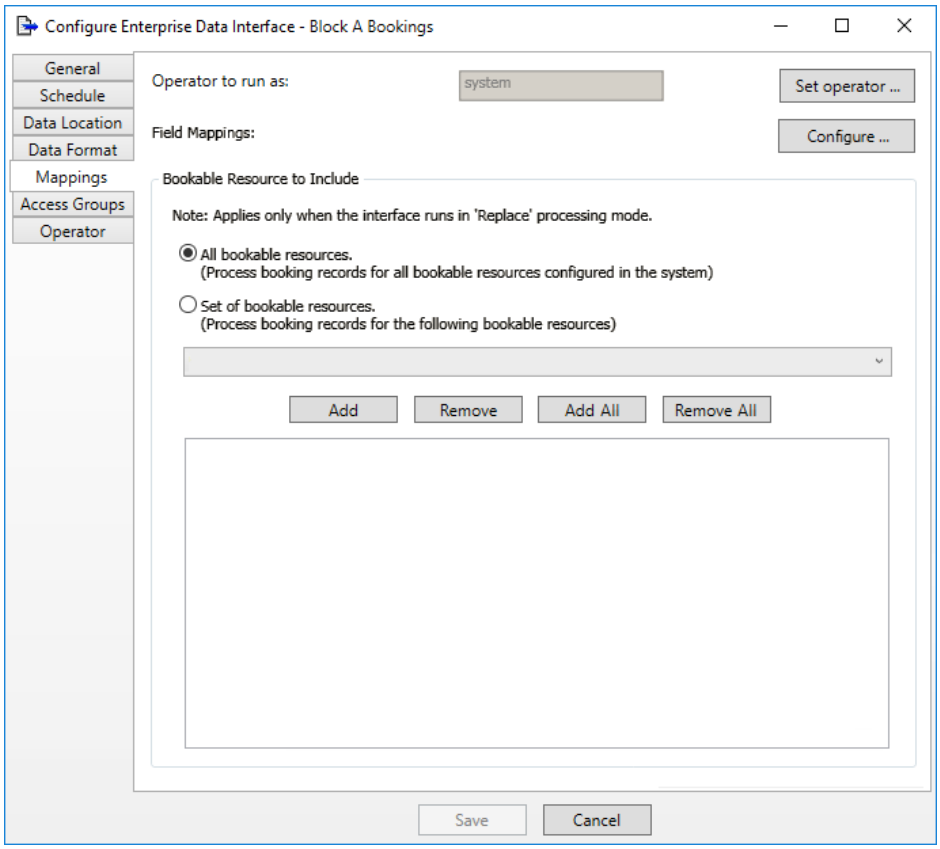
Including Bookable Resources

Introduction

This procedure describes how to process booking records for specific bookable resources only.

Procedure

1. Click the **Mappings and Operator** tab.



2. Select the **Set of bookable resources** radio button.
3. From the drop-down list select the bookable resource to include.
   Note: Only the bookable resources that the Booking Interface intends to maintain the bookings of should be included. If other bookable resources (that are not maintained by this booking data) are included, the bookings for these bookable resources will be removed.

   Alternatively, to include all bookable resources, click the **Add All** button.
4. Click the **Add** button. The bookable resource will be added to the inclusion grid below. Booking records will only be processed for the bookable resources listed in the inclusion grid.
5. To remove a bookable resource from the grid, click the **Remove** button.

   Alternatively, to remove all bookable resources listed in the grid, click the **Remove All** button.

Enabling an interface

Introduction

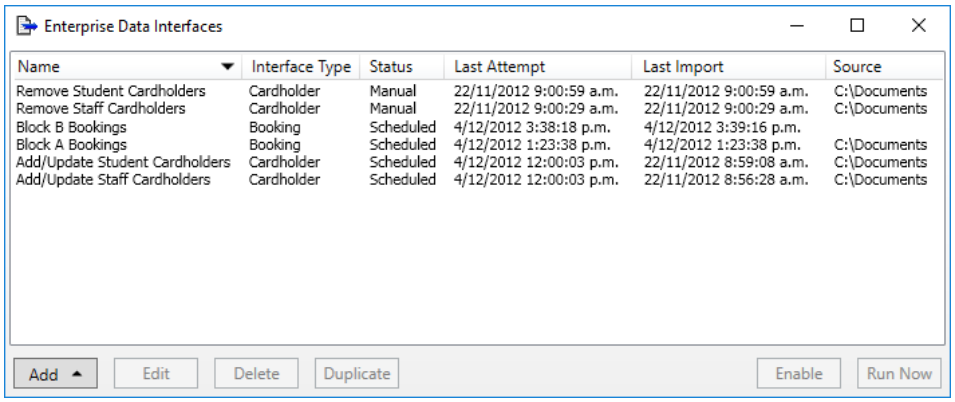
This procedure describes how to enable an interface. Interfaces when created are disabled by default.

If the interface has been configured to run on a schedule or added to a sequence, it will not run until such time as it has been enabled.

If an interface has been configured to run manually, it cannot be run until such time as it has been enabled.

Procedure

1. Click **Manage** from the menu bar.
2. Click **Enterprise Data Interface**.
   The Enterprise Data Interfaces list window opens.



3. Select the interface you wish to enable/disable.
4. To enable the interface, click the **Enable** button.
   The interface is enabled and the status is changed to "Manual", "Scheduled" or "Sequenced".
   The **Run Now** button is enabled.
5. To disable the interface, click the **Disable** button.
   The interface is disabled and the status is changed to "Disabled".
   The **Run Now** button is disabled.

Manually running an interface

Introduction

You can manually run an interface at any time. In order to run an interface the interface must first be enabled.

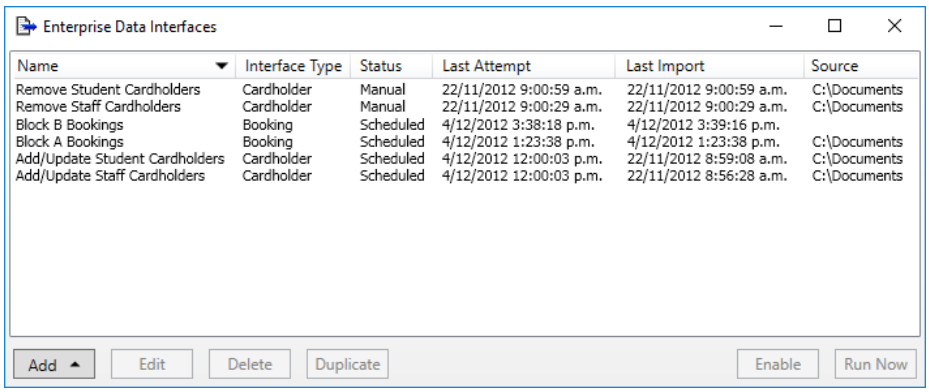
If an interface has been scheduled to run, but is unable to run because another scheduled interface is still running, you can use this feature to run the interface immediately.

Notes:

- When an interface is run, it will be run under the "Run as Operator" name.
- If an interface is running, it won't run again until it has completed running.
- If you manually run a scheduled or sequenced interface, it will still run according to its schedule or sequence.
- If you manually run an interface that forms part of a sequence, a dialog window displays allowing you to run all interfaces (from this point on) in the sequence, or only this interface.
- If an interface has been scheduled to run once a day, it can be manually run more than once in a day.

Procedure

1. Click **Manage** from the menu bar.
2. Click **Enterprise Data Interface**.
   The Enterprise Data Interfaces list window opens.



3. Select the Enterprise Data Interface you wish to run.
4. Click the **Run Now** button.

Stopping an interface

Introduction

Only an interface that is currently running can be stopped.

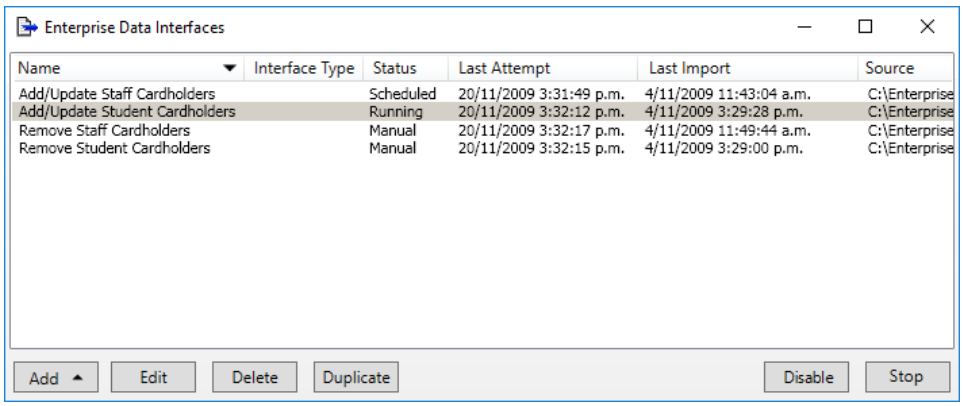
When an interface is stopped an event is generated. This event shows when the interface was stopped and by whom.

Notes:

- If a manually run interface with multiple import files is stopped, the other files will not be processed.
- If a scheduled interface with multiple import files is stopped, the next file will be processed at the next scheduled time, unless the interface is disabled. If an interface that belongs to a sequence, with multiple files is stopped, the next interface in the sequence will not run, until such time as the previously sequenced interface has completed.
- When an interface is stopped the source file will be moved to the completed folder. Failed and un-processed cardholder records will be copied to a new file and placed in the failed folder. The log file details all un-processed cardholder records.

Procedure

1. Click **Manage** from the menu bar.
2. Click **Enterprise Data Interface**.
   The Enterprise Data Interfaces list window opens.



3. Select the Enterprise Data Interface you wish to stop.
4. Click the **Stop** button.

The log file

Introduction

The log file can be used for troubleshooting purposes. The log file details the date and time the import started and completed.

The log file also lists all records that failed to be imported and provides a reason as to why each record failed.

When importing data from the source file, the log file is located in the completed folder directory and is named after the source file followed by the date and time of processing, (e.g. Student Data_20091103_114732.log).

When importing data from a database, the log file is located in the log folder directory and is named after the Data Source Name followed by the date and time of processing, (e.g. PERSONS_V_20121103_114732.log).

Rows shown in the log file

Each row in the log file displays the following data:

Row	Displays...
First	• the date and time the import started • names the file imported
Middle	• the date and time the record was processed • the record processed • a reason as to why the record failed
Last	• the date and time the import completed • provides a summary of the import

Example

The following example shows a log file where the "Run as Operator" did not have sufficient privileges to import all cardholder records:

```
Reason = Operator doesn't have sufficient privilege to see access group to add to cardholder.
Reason = Operator doesn't have sufficient privilege to competency 'Competency 3'
Reason = Operator doesn't have sufficient privilege to competency 'Competency Root Division'
Reason = Operator doesn't have sufficient privilege to see access group to add to cardholder.
Reason = The operator does not have sufficient privilege to view card type 'Card Type A11111 - Division 3'
Reason = The operator does not have sufficient privilege to view card type 'Card Type (out of Division)'
Reason = The operator doesn't have sufficient privilege to division 'Division 3'
Reason = The operator doesn't have sufficient privilege to division 'Root Division'
Reason = The operator does not have sufficient privilege to view card type 'Card Type (out of Division)'
```

The failed file

A failed file is generated when importing data from a source file only. This file is generated when one or more records fail to be imported. This file contains a copy of all records that failed to be imported.

The failed file file is located in the failed folder directory and is named after the source file followed by 'failed' and the date and time of processing, (e.g. Student Data_failed_20091103_114732.csv).

If required, you can correct the reasons for failure (as specified in the log file) then import the failed file.

Note: The failed file does not contain header rows. If you choose to import the failed file, it is recommended that you add the required header rows to the failed file. Alternatively, you can adjust the configuration of the interface (Header Rows field) before importing the failed file.

Cardholder Interface configuration example

Introduction

The following is a fictional example, showing how a source file containing student details will be imported into Gallagher Command Centre.

Example

The following table shows how source fields have been mapped to Gallagher Command Centre fields.

Source Field	Description/Comments	Command Centre Field	Description/Comments
Student ID	Unique ID number	Student ID	Maps to a unique PDF
Last Name		Last Name	
First Name		First Name	
Degree		Degree	PDF
Division	Student	Division	Maps to Student division
Card Type		Cards	Maps to a card type
Enrolment Date		Enrolment Date	PDF
Course Code		Course Code, Access Group Memberships	Maps to a PDF and the Access Group Memberships field
Active	This is a boolean value in the source file that indicates if the student is currently active	Authorised	If the boolean value is positive the cardholder is Authorised in <Brand>
DOB		DOB	PDF
Start Date			Card From date
End Date			Card Until date
Class 1		Class 1	PDF
Class 2		Class 2	PDF
Class 3		Class 3	PDF
Class 4		Class 4	PDF
Class 5		Class 5	PDF
Carpark Membership	Identifies if the student has access to the carpark	Access Group Memberships	Carpark Access Group
Carpark Start Date			Carpark Access Group From date
Carpark End Date			Carpark Access Group Until date

Access Group Memberships
Course codes will be used to define a student's Access Groups, (i.e. the areas a student can access while on-site).

The following table shows the course codes present in the source file and what Access Groups they will be mapped to.

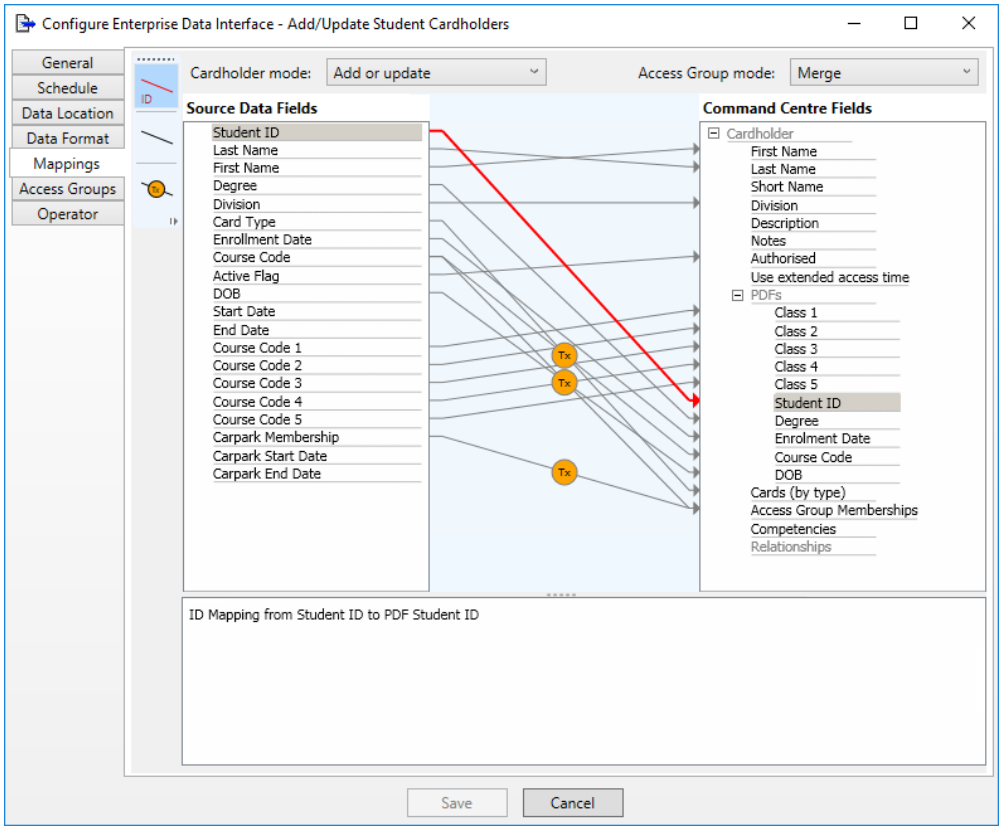
Course Code	Access Group
ENG	Engineering
SCI	Science
LAW	Law
MED	Medicine
ARTSC	Arts

If a student has a Carpark Membership value, the student will be placed in the Carpark Access Group, (i.e. the student will have access to the carpark).

The Carpark Start and Finish dates will be used to define the period of access the student has to the carpark.

Cards

The Card Type value will be used to define a student's card type. The Start and Finish dates will be used to define the card's enablement period.



Booking Interface configuration examples

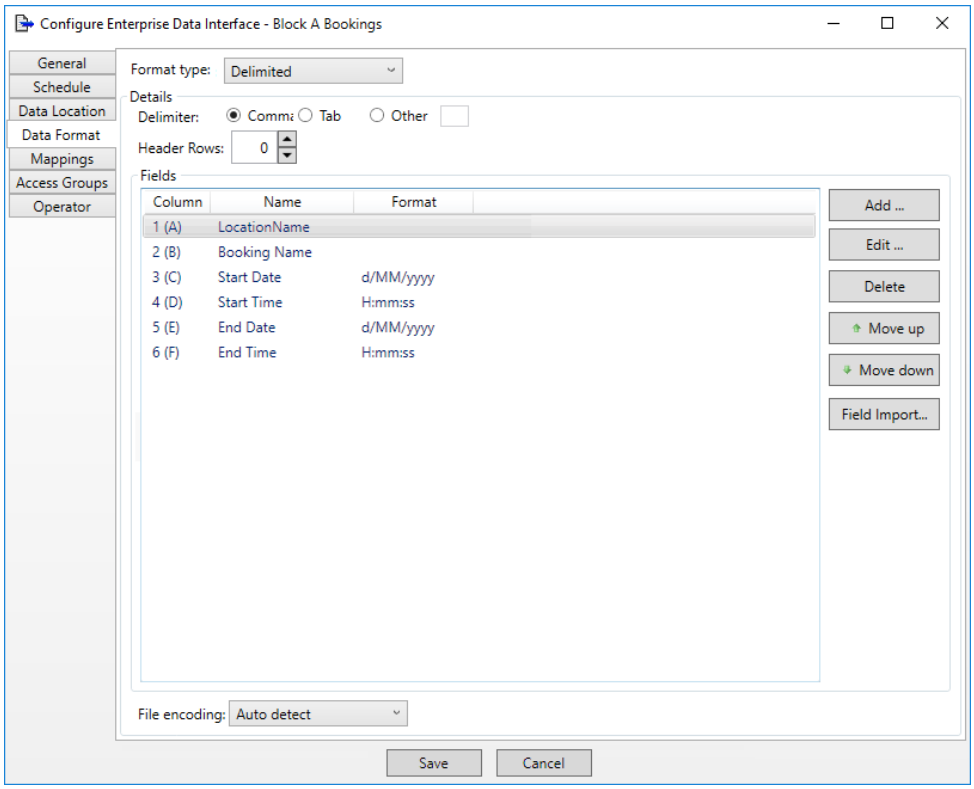
Importing bookings from a source file

The following is a fictional example, showing how a source file, (e.g. CSV file) containing booking data will be imported into Command Centre.

The source file contains the following fields:

Reference	Location	Name	Start Date	Start Time	End Date	End Time
B1	Room 1	Room 1 Booking	03/12/2012	08:30:00	03/12/2012	09:30:00
B2	Room 2	Room 2 Booking	03/12/2012	08:30:00	03/12/2012	09:30:00
B3	Room 1	Room 1 Booking	04/12/2012	08:30:00	04/12/2012	09:30:00
B4	Room 1	Room 1 Booking	05/12/2012	08:30:00	05/12/2012	09:30:00

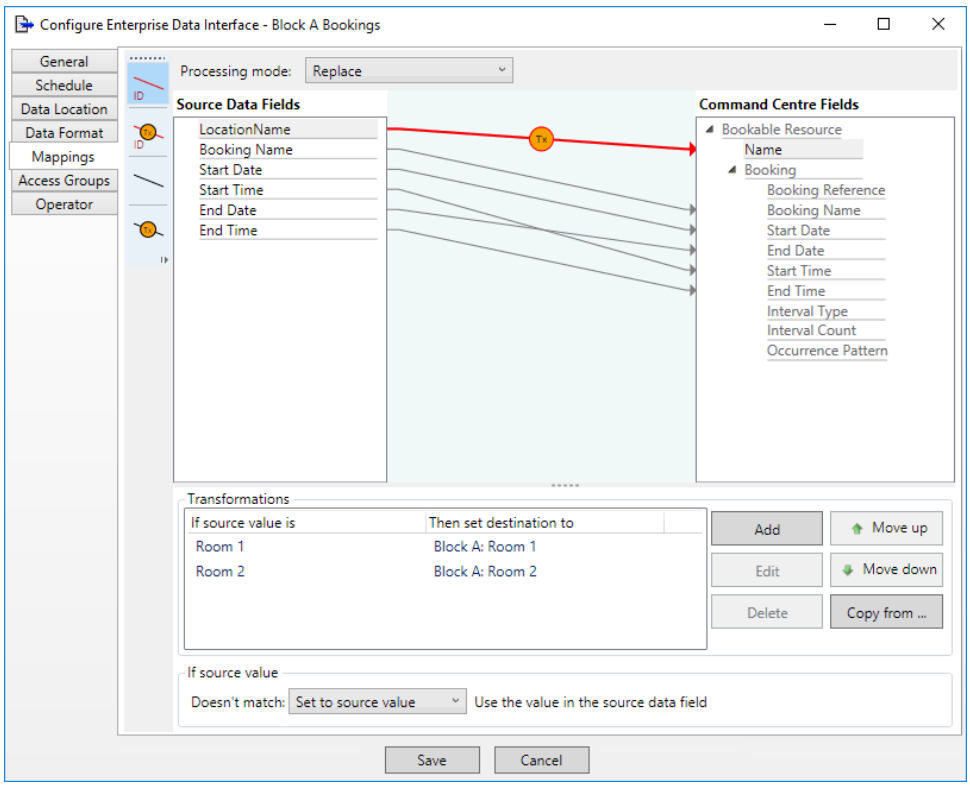
The data format for this Booking Interface is configured as shown:



Notes:

- The source file format type is "Delimited". The delimiter used is "Comma". A header row of "1" has been entered.
- The date format is "day/month/year". The time format is "24 hour".
- You can import the field names directly from the source file. To do so, click the **Field Import** button, then select the source file.

The mappings for this Booking Interface are configured as shown:



Note: An ID transformation mapping from "Room 1" to the "Block A: Room 1" bookable resource item has been created. An ID transformation mapping from "Room 2" to the "Block A: Room 2" bookable resource item has also been created.

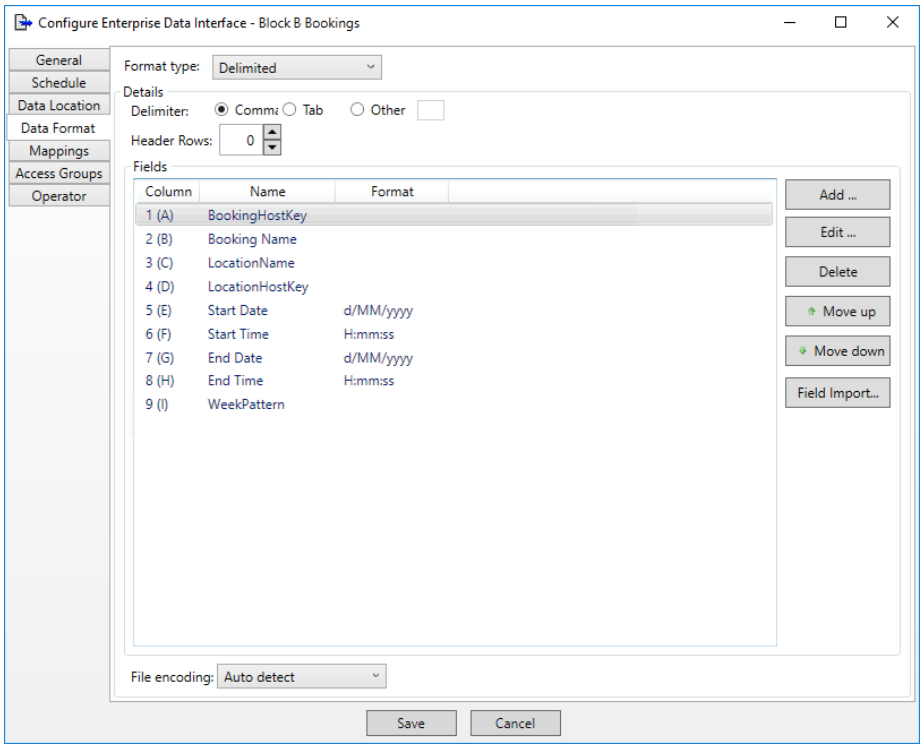
Importing bookings from a Microsoft SQL database

The following is a fictional example, showing how booking data provided from the timetabling/booking system Syllabus Plus will be imported into Command Centre. The data provided specifies re-occurring bookings.

The source table contains the following fields:

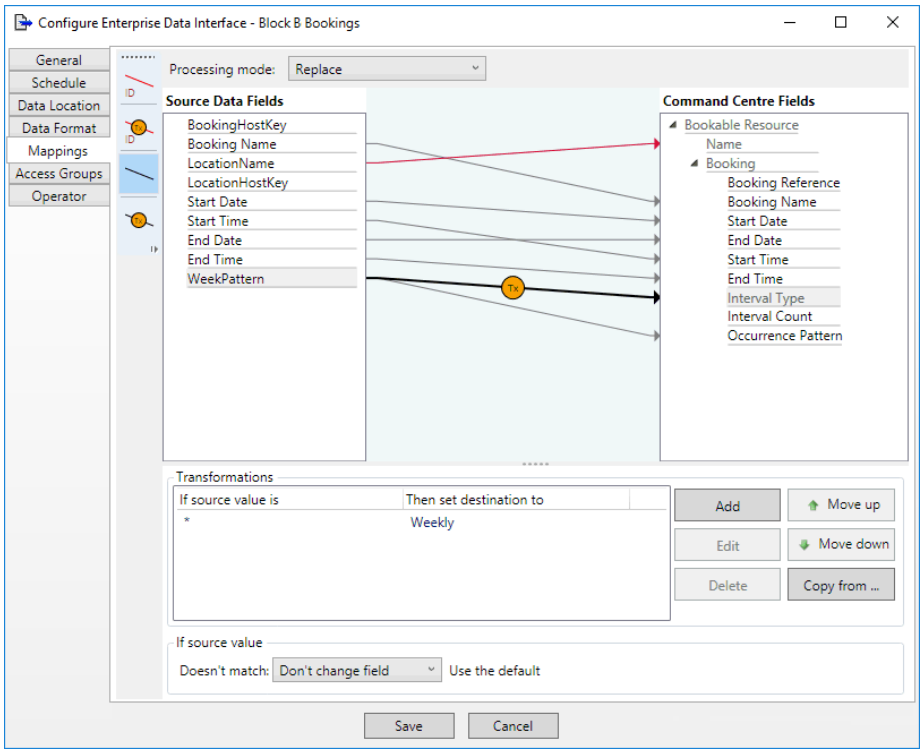
BookingHostKey	BookingName	LocationName	LocationHostKey	StartDate	StartTime	EndTime	WeekPattern
Business Studies/T/01	Business Studies/T/01	Tutorial Room 3	Room3	2012-01-06 00:00:00.000	1900-01-01 15:00:00.000	1900-01-01 16:30:00.000	111111011111011111
Business Studies/T/02	Business Studies/T/02	Tutorial Room 3	Room3	2012-01-02 00:00:00.000	1900-01-01 10:00:00.000	1900-01-01 11:00:00.000	111111011111011111
Business Studies/T/03	Business Studies/T/03	Tutorial Room 3	Room3	2012-01-04 00:00:00.000	1900-01-01 12:00:00.000	1900-01-01 13:00:00.000	111111011111011111
Business Studies/T/04	Business Studies/T/04	Tutorial Room 3	Room3	2012-01-06 00:00:00.000	1900-01-01 10:00:00.000	1900-01-01 11:00:00.000	111111011111011111

The data format for this Booking Interface is configured as shown:



Note: You can import the field names directly from the source table. To do so, click the **Field Import** button.

The mappings for this Booking Interface are configured as shown:



For the Syllabus Plus data, the Interval Type has been configured as a wildcard transformation mapping to "Weekly". The Booking Name source field has been used as the Booking Name.

Note: If the Booking Reference is used, then all updates are applied to that booking, and are not new bookings.

Troubleshooting

The following table provides solutions to problems you may encounter when using Enterprise Data Interface:

Problem	Solutions
When importing from a source file the import did not run	• Check the source folder to see if the source file is present. • The source file name has been incorrectly entered on the Data Location tab, (e.g. the file extension has not been entered).
Unable to convert value. The value could not be imported, as it is not of the correct format	• The source field has not been defined correctly on the Data Format tab, (e.g. the date format has been defined as dd/MM/yyyy but the date in the source file is d/MM/yyyy). Define the date format as d/MM/yyyy. Dates with a double day digit will still be imported. • The header row has been processed.
Enterprise Data Interface has been upgraded and the Gallagher Command Centre Services will not start after restoring a backup	The sequence for restoring a backup is: • Restore your Enterprise Data Interface backup. • Exit Gallagher and stop the Gallagher Command Centre Services. • Uninstall Enterprise Data Interface. • Reinstall Enterprise Data Interface (same or later version). • Restart the Gallagher Command Centre Services.
The interface has been scheduled to run on an interval and the "Ending at" time is the same time as it is scheduled to run	Check the Gallagher Command Centre Event Viewer to see if the interface has run.
A cardholder does not have the expected mapped value	This may occur if you have mapped more than one source field to the cardholder field (this is not recommended). The last mapping made in the Edit Mappings window is used to add/update the cardholder field.

Problem	Solutions
Operator doesn't have sufficient privilege	The operator must be assigned the appropriate privileges in the required divisions to perform the actions specified by the import.
When importing from a database the import does not run	Ensure the Windows Firewall on the database server allows incoming connections from the Command Centre server.
When importing bookings (for a Bookable Resource), and a booking is not imported, but the log states that the booking was successfully imported	Ensure that each booking record that is imported using the Booking Reference field uses a unique value. If a unique value is not used, the last booking record containing the Booking Reference will be the one that remains at the end of the import processing. All other booking records containing the same Booking Reference in the data set will not be imported.

Chapter 55: Perimeter Sensors

Introduction

The following sensors can be connected to Command Centre and configured as hardware items, for the purpose of perimeter intrusion detection - Z10 Tension Sensors, D21 Disturbance Sensors and D10 Tautwire Sensors.

Notes:

- Z10 Tension Sensors, D21 Disturbance Sensors and D10 Tautwire Sensors can be connected to the Controller 6000 and 7000.
- A maximum of 64 Z10 sensors can be connected to a Controller 6000 and 7000; either all off the same HBUS port, or spread over two.
- The Z10 Tension Sensor measures wire tension and signals an alarm when the wire tension exceeds the predetermined attack alarm threshold. Because the sensor measures wire tension, it can also signal an alarm when the wire tension exceeds predetermined maintenance alarm thresholds.

Licensing

The use of sensors with Command Centre is a licensable feature. The total number of sensors is governed by the license, as follows:

```
[Limits]
Z10 Tension Sensors=<nn> OR Disturbance Sensors=<nn>
```

where <nn> is the number of sensors your site is allowed.

Operator Privileges

Operator Privilege	is required to...
"View Site"	view Z10 Tension Sensor Groups, D21 Disturbance Sensors and D10 Tautwire Sensors
"Edit Site"	view and edit Z10 Tension Sensor Groups, D21 Disturbance Sensors and D10 Tautwire Sensors
"Maintenance Override"	override Z10 Tension Sensor Groups, D21 Disturbance Sensors and D10 Tautwire Sensors

This chapter covers the following topics:

- ***Configuring a Z10 Tension Sensor Group*** (on page 55-3)
- ***Fence Configuration example*** (on page 55-8)
- ***Performing a Maintenance Mode Override*** (on page 55-9)
- ***Performing a Walk Test Mode Override*** (on page 55-12)
- ***Tension Overload*** (on page 55-14)
- ***Configuring a Z20 Disturbance Sensor*** (on page 55-15)
- ***Configuring a D10 Tautwire Sensor*** (on page 55-18)
- ***Assigning Z20 and D10 sensors to a Controller 6000*** (on page 55-20)
- ***Performing a 'Log Tuning Data' override on a Z20 Disturbance Sensor*** (on page 55-22)

Configuring a Z10 Tension Sensor Group

Introduction

This procedure describes how to configure a Z10 Tension Sensor Group.

Sensors must be grouped by fence, (e.g. North Fence Sensor Group). By grouping sensors you can logically identify the sensors belonging to a specific fence. This allows for easier monitoring and maintenance of individual fences on your site.

Notes:

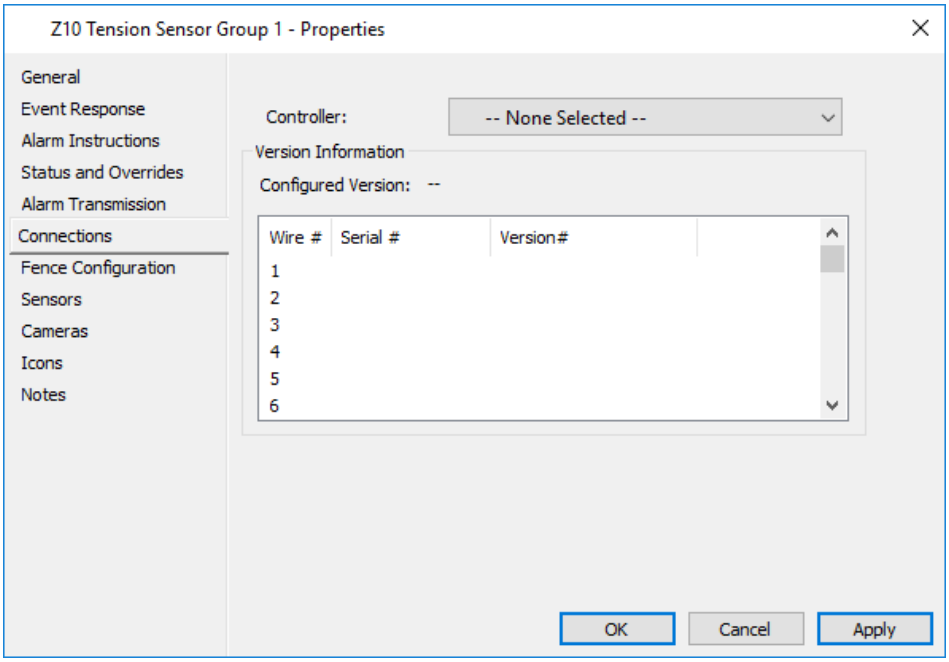
- Multiple sensor groups can belong to one fence.
- A maximum of 64 Z10 sensors can be connected to a Controller 6000 and 7000; either all off the same HBUS port, or spread over two.
- A maximum of 55 sensors can be assigned to a sensor group.
- The sensors belonging to a sensor group cannot span multiple Controllers.
- The maximum constant tension rating for a sensor is 60 kg.
- The maximum tension rating for a sensor is 200 kg.
- To change the measurement units, (e.g. metric to imperial) select the **Measurement Units** tab in the **Server Properties**.

Before you begin

Ensure all sensors for this group are connected to the same Controller. Once connected, the sensors will appear as un-configured devices on the **HBUS Devices** tab in the Controller's properties.

Procedure

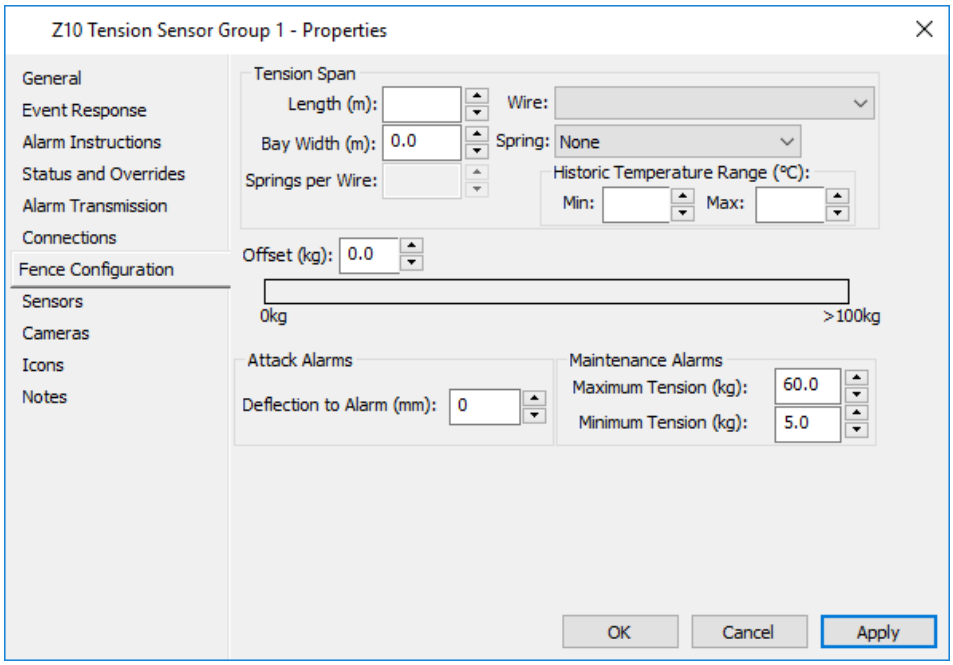
1. Click **Configure** from the menu bar, then **Z10 Tension Sensor Groups**.
   The **Z10 Tension Sensor Group** List Window opens.
2. **Right click** and select **New...Z10 Tension Sensor Group.**
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail 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.



7. Select the appropriate Controller from the drop-down list, (i.e. the Controller that the sensors in this group are connected to).

   Note: Once the sensor group has been configured, and the **Apply** button clicked, the version of sensor code stored on the selected Controller displays in the **Configured Version** field. This version of code will be automatically downloaded to all sensors belonging to this group. The Serial number and Version of code for each sensor belonging to this group is then displayed.

8. Click the **Fence Configuration** tab.
   This tab allows you to define the configuration of your fence.



9. Configure the fields as required:

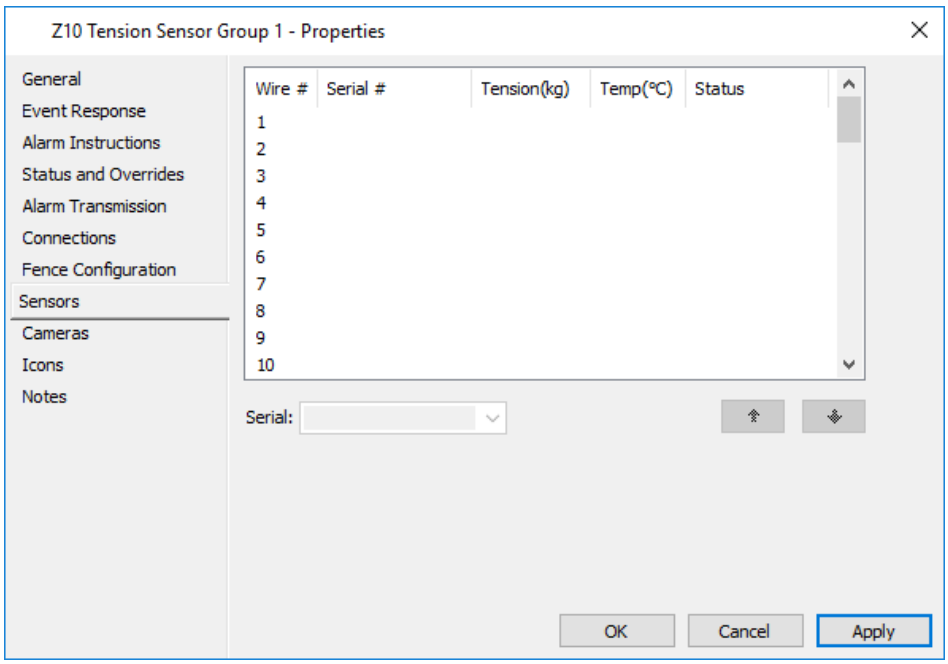
Field	Description
Length	This value indicates the length of the fence. This value will alter the attack alarm threshold. (Default = 0.0 meters. Range = 0.0 meters to 304.5 meters)
Bay Width	This value indicates the length of each bay (space between intermediate posts). If you have bays of varying lengths, this value should be set to that of the largest bay. This value will alter the attack alarm threshold. (Default = 0.0 meters. Range = 0.0 meters to 30.4 meters)
Springs per Wire	This value indicates the number of springs per wire. You will need to specify the spring type used to enable this field. This value will alter the attack alarm threshold. (Default = 0 springs. Range = 0 springs to 9 springs)
Wire	Select the wire type used. This value will alter the attack alarm threshold.
Spring	Select the spring type used. This value will alter the attack alarm threshold.
Historic Temperature Range	These values indicate the minimum and maximum temperatures the fence may be subjected to. These values will alter the tension range. (Range -100 ºC to +100 ºC)
Offset	Specify the shift (offset) in tension range. (Range = 0 kg to 60 kg)
Attack Alarms	When this value (wire movement) is exceeded an attack alarm is raised in Command Centre. Most likely you will receive an alarm before this value is exceeded.
Maintenance Alarms	These values indicate the maximum and minimum wire tension that must be exceeded before a maintenance alarm is raised in Command Centre. **Notes:** • You will need to ensure you have configured the Maintenance Alarm limits to accommodate fluctuations in temperature and tension. If the Maintenance Alarm limits are tightly bound to the target tension range, then a high occurrence of maintenance alarms may occur. On the other hand, by having Maintenance Alarm limits set wider than the target tension range, there is a risk of wires requiring tensioning, being overlooked.

Field	Description
	• For a maintenance alarm to be raised, the condition must exist for more than 30 seconds. A hysteresis of 1 kg applies.

When configuring the tension span, you will be warned if:

- The tension range exceeds the sensor tension rating. The maximum constant tension rating for the sensor is 60 kg.
- The tension range exceeds the wire yield point. This may cause stretching for the wire selected.
- The attack deflection could raise the tension over 200 kg. The maximum tension rating for the sensor is 200 kg.

10. Click the **Sensors** tab.



11. Open the properties of the Controller that the sensors are connected to, and click the **HBUS Devices** tab.

    The sensors connected to this Controller are displayed.

12. Select the appropriate sensors for this group, and drag and drop them into the grid.
    Notes:

    - If required, you can add sensors to this group, by selecting a sensor from the **Serial** drop-down list. This drop-down lists all sensors assigned to the selected Controller, that have not been assigned to a group.
    - Once the sensors have been assigned to this group, and the **Apply** button clicked, the Tension, Temperature, and Status for each sensor belonging to this group displays in the grid.

13. Assign each sensor to the appropriate wire, by using the **up** and **down** arrow buttons below the grid.
14. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this sensor group.
    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 sensor group.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
16. Click the **Custom Fields** tab if you want to add and assign a custom field value to this sensor group.
    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 sensor group.
    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.

Result

A Z10 Tension Sensor Group has been configured.

When first configured a Maintenance Mode override will be in effect. This is represented by the icon overlay (yellow screw driver). Once the final tensioning has taken place, you will need to cancel the Maintenance Mode override. The sensor group will then be functioning normally. For details regarding the operation of the Maintenance Mode override, refer to the topic ***Performing a Maintenance Mode Override*** (on page 55-9).

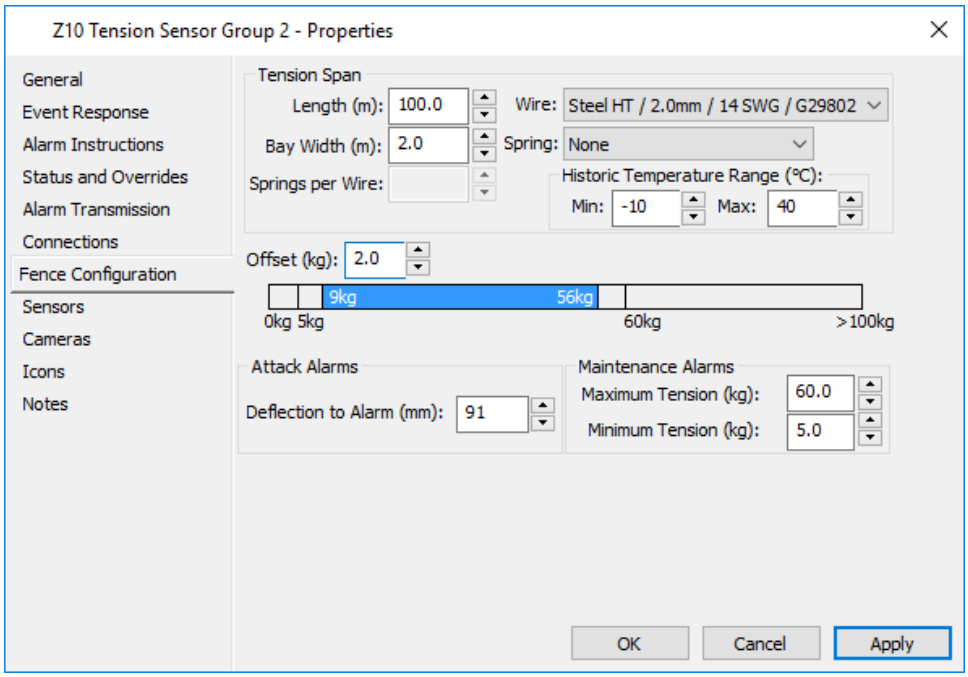
Note: A Site Configuration Report can be generated for a Z10 Tension Sensor Group. This report displays the parameters configured for the group and lists the sensors assigned to the group.

Fence Configuration example

Introduction

The following example shows the fence configuration for a Z10 Tension Sensor Group. The Tension Span fields (Length, Bay Width, Springs per Wire, Wire, Spring, and Historic Temperature Range) determine the wire tension range for this fence.

Example



Tension Range Bar

The following table describes the information shown in the tension range bar.

Information	Explanation
Tension range	9 kg to 56 kg (shown in blue). This is the tension range based on the values entered in the Tension Span fields.
Acceptable tension range	5 kg to 60 kg. The tension range must be within this range.
Offset	This is the shift in fence tension range. In the example above an offset of 2 kg has been entered.
Ideal tension	In this example the ideal tension for each wire is 27.2 kg (at 28.4 ºC). Wires should be tensioned to this value. **Note:** The sensors assigned to this item must be connected and online in order to view the ideal tension.

Performing a Maintenance Mode Override

Introduction

This procedure describes how to perform a Maintenance Mode override for a Z10 Tension Sensor Group.

When a sensor group is placed into Maintenance Mode all tension related alarms (attack and maintenance) are suppressed.

Maintenance Mode can be used when tensioning during installation, re-tensioning, or performing maintenance on the fence. To help tension the wires, each sensor is equipped with a tension status LED. This LED provides a visual indication of the current wire tension, based on the fence configuration.

When in Maintenance Mode only, the sensor's LED will display one of the following flash patterns:

LED	Wire Tension Status
1 Flash per second (Green)	The wire tension is within target tension range.
1 Flash per second (Red)	The wire is over tensioned.
1 Flash per second (Blue)	The wire is under tensioned.

LED	Diagnostic Status
3 Flash per second (Red)	No communications with the Controller.
2 Flash per second (Red)	Communications with the Controller, but sensor is not configured.
1 Flash per second (Green, Red or Blue)	Fully configured and functioning normally. The sensor's LED displays the current wire tension status.

LED	Tension Overload Status
3 Flash for 3 seconds (Green), then 3 Flash for 3 seconds (Red, Blue then Green)	The wire tension is within target tension range. The sensor has reported a tension overload event.
3 Flash for 3 seconds (Red), then 3 Flash for 3 seconds (Red, Blue then Green)	The wire is over tensioned. The sensor has reported a tension overload event.
3 Flash for 3 seconds (Blue), then 3 Flash for 3 seconds (Red, Blue then Green)	The wire is under tensioned. The sensor has reported a tension overload event.

Notes:

- A Maintenance Mode override is retained during a power or communications failure. If the override mode is changed during this time, the sensor group will follow the new override mode as soon as communications are restored.
- Shunting a sensor group takes precedence over a Maintenance Mode override. When a sensor group is shunted, all tension related alarms (attack and maintenance) are suppressed. All sensor LED activity ceases. However, each sensor will continue to report tension and temperature.

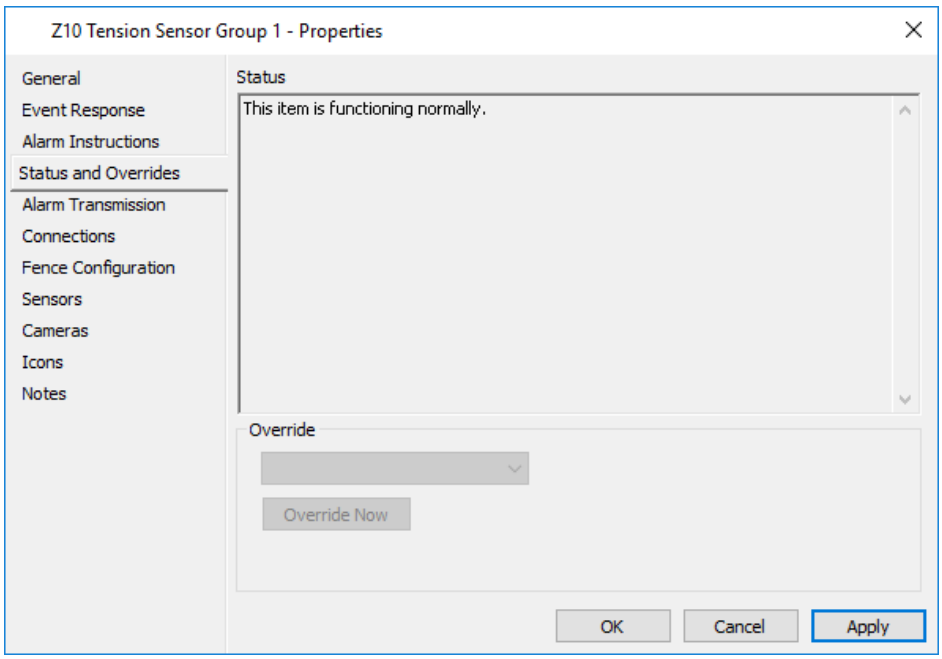
Before you begin

Before you begin this procedure:

- Ensure you have configured a sensor group. Refer to the topic ***Configuring a Z10 Tension Sensor Group*** (on page 55-3).
- Ensure the operator has been assigned the "Maintenance Override" operator privilege.

Procedure

1. Click **Configure** from the menu bar, then **Z10 Tension Sensor Group**. The **Z10 Tension Sensor Group** List Window opens.
2. **Right click** the appropriate Z10 Tension Sensor Group, and click **Override...** from the drop-down menu.
   The **Status and Overrides** tab on the Properties window for the item displays.



3. Click within the Override field and select **Maintenance Mode** 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 Z10 Tension Sensor Group is now in Maintenance Mode:

- The Z10 Tension Sensor Group icon now displays a yellow screw driver, indicating the sensor group is in Maintenance Mode.
- All tension related alarms (attack and maintenance) for this group are suppressed. Voltage and offline alarms will still be generated.
- LED activity commences for all sensors within this group.
- A Maintenance Mode alarm is raised in Command Centre. For example, *[Z10 Tension Sensor Group Name] - Maintenance Mode override in effect*. This alarm remains active, until the Maintenance Mode override is cancelled.

Performing a Walk Test Mode Override

Introduction

This procedure describes how to perform a Walk Test Mode override for a Z10 Tension Sensor Group.

When a sensor group is placed into Walk Test Mode the sensor's LED will turn solid green. If the sensor has reported a tension overload event, the sensor's LED will display the tension overload status. When an alarm condition is detected, the sensor's LED will change to red, and remain red until the alarm condition is removed.

Walk Test Mode can be used to provide visual evidence that an alarm can be generated by the sensor.

When such an event occurs, a Walk Test Mode Attack alarm is raised in Command Centre. For example, [*Z10 Tension Sensor Group Name*] wire [*Number*] detected an attack. This alarm allows an operator to generate an Activity Report detailing all alarms raised.

Notes:

- A Walk Test Mode override is retained during a power or communications failure. If the override mode is changed during this time, the sensor group will follow the new override mode as soon as communications are restored.
- Shunting a sensor group takes precedence over a Walk Test Mode override. When a sensor group is shunted, all tension related alarms (attack and maintenance) are suppressed. All sensor LED activity ceases. However, each sensor will continue to report tension and temperature.

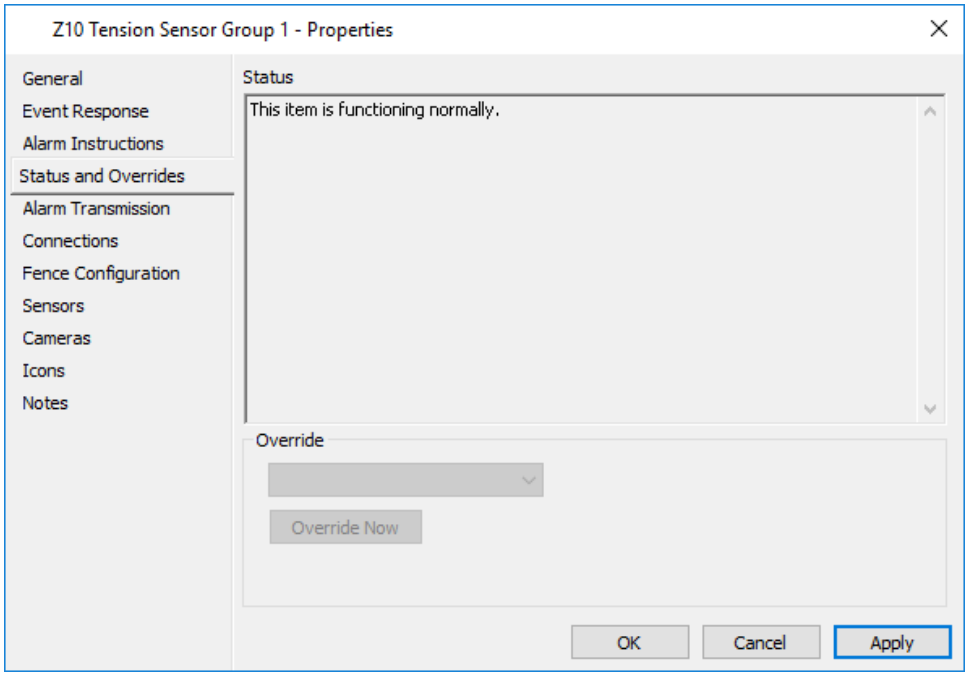
Before you begin

Before you begin this procedure:

- Ensure you have configured a sensor group. Refer to the topic ***Configuring a Z10 Tension Sensor Group*** (on page 55-3).
- Ensure the operator has been assigned the "Maintenance Override" operator privilege.

Procedure

1. Click **Configure** from the menu bar, then **Z10 Tension Sensor Group**. The **Z10 Tension Sensor Group** List Window opens.
2. **Right click** the appropriate Z10 Tension Sensor Group, and click **Override...** from the drop-down menu.
   The **Status and Overrides** tab on the Properties window for the item displays.



3. Click within the Override field and select **Walk Test Mode** 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 Z10 Tension Sensor Group is now in Walk Test Mode:

- The Z10 Tension Sensor Group icon now displays a yellow screw driver, indicating the sensor group is in Walk Test Mode.
- The Event Group Walk Test Mode Attack will be used to report attack alarms for this sensor group.
- LED activity commences for all sensors within this group.
- A Walk Test Mode alarm is raised in Command Centre. For example, *[Z10 Tension Sensor Group Name] - Walk Test Mode override in effect*. This alarm remains active, until the Walk Test Mode override is cancelled.

Tension Overload

Introduction

The maximum tension rating for a Z10 sensor is 200 kg.

If the sensor reports a tension rating exceeding 200 kg, the load cell within the sensor may have incurred damage and should be replaced.

When such an event occurs, a Sensor Abnormal alarm is raised in Command Centre. For example, [*Z10 Tension Sensor Group Name*] wire [*Number*] tension overload. This alarm remains active, until the sensor is replaced.

Visual identification

To visually identify a sensor that has reported a tension overload, you will need to perform a Maintenance Mode override, or Walk Test Mode override for the sensor group. Refer to the topics ***Performing a Maintenance Mode Override*** (on page 55-9), or ***Performing a Walk Test Mode Override*** (on page 55-12) for details.

When a sensor has reported a tension overload event, the sensor's LED will display one of the following flash patterns:

LED	Tension Overload Status
3 Flash for 3 seconds (Green), then 3 Flash for 3 seconds (Red, Blue then Green)	The wire tension is within target tension range. The sensor has reported a tension overload event.
3 Flash for 3 seconds (Red), then 3 Flash for 3 seconds (Red, Blue then Green)	The wire is over tensioned. The sensor has reported a tension overload event.
3 Flash for 3 seconds (Blue), then 3 Flash for 3 seconds (Red, Blue then Green)	The wire is under tensioned. The sensor has reported a tension overload event.

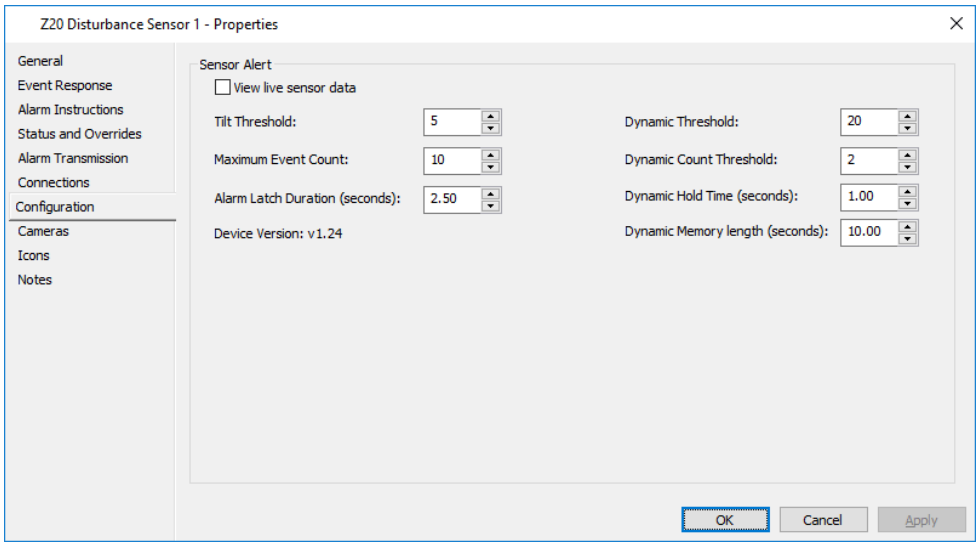
Configuring a Z20 Disturbance Sensor

Introduction

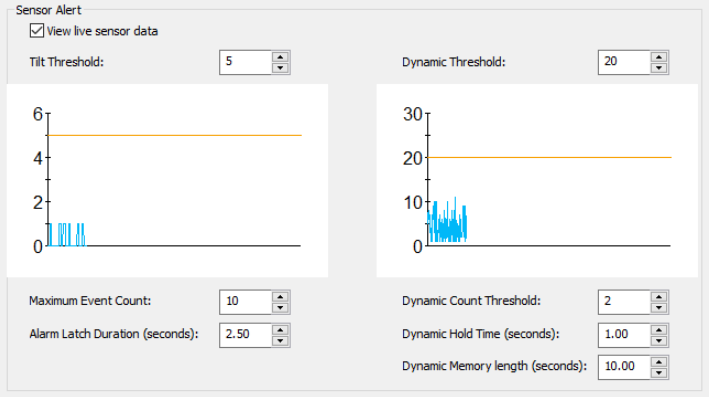
This procedure describes how to configure a Z20 Disturbance Sensor.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Sensor Devices** > **Z20 Disturbance Sensor**.
   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 fields **Connected to** and **Device number** will only be populated once you assign the sensor to a Controller.
7. Click the **Configuration** tab.



8. Configure the fields as required:

Field	Description
View live sensor data	When checked, **Tilt Threshold** and **Dynamic Threshold** graphs display, showing actual values generated by each sensor over the last two minutes. The **Y** axis represents the threshold and the yellow line indicates the actual setting. The **X** axis is time - 120 seconds.  The data in the **Tilt Threshold** and **Dynamic Threshold** fields will display dynamically. This makes it possible to see changing values when the page is open. Data will continue to be updated and displayed until the tab is closed. **Note:** When checked, the Dynamic and Tilt values are displayed and updated on the **Status and Overrides** tab also.
Tilt Threshold	This number determines the rate that the device can be tilted, (i.e. its orientation changed) before it generates an alarm event. (Default = 50. Range = 1 to 1000)
Dynamic Threshold	This number determines the degree of disturbance energy the device can sense before it registers a dynamic disturbance. (Default = 300. Range = 1 to 5000)
Maximum Event Count	This is the maximum number of dynamic events that can be stored. (Default = 10. Range = 1 to 100)
Alarm Latch Duration	This number determines how long an alarm condition is maintained after an alarm condition is reached. (Default = 2.5 seconds. Range = 0.01 seconds to 600.00 seconds, i.e. 10 minutes)

Field	Description
Dynamic Count Threshold	This is the number of recurring disturbances that are treated as a single alarm event if they occur within a preset period (Dynamic Hold Time). (Default = 2. Range = 1 to 100)
Dynamic Hold Time	This is the period within which recurring disturbances (as set by the Dynamic Count Threshold) are treated as a single alarm event. (Default = 1 second. Range = 0.01 seconds to 600.00 seconds, i.e. 10 minutes)
Dynamic Memory length	This value indicates how long the device will remember a dynamic disturbance. (Default = 10 seconds. Range = 0.01 seconds to 600.00 seconds, i.e. 10 minutes) **Note:** The Dynamic Memory length must be equal to or greater than the Dynamic Hold Time, multiplied by the Dynamic Count Threshold.

9. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Disturbance Sensor.
   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 Disturbance Sensor.
    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 Disturbance Sensor.
    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 Disturbance Sensor.
    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 new Z20 Disturbance Sensor has been configured.

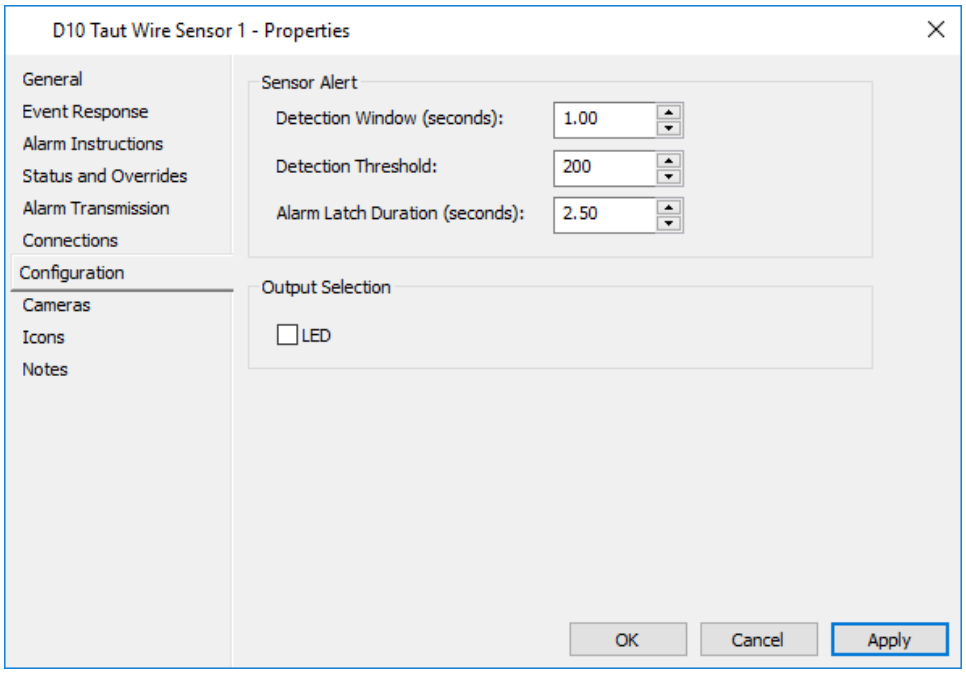
Configuring a D10 Tautwire Sensor

Introduction

This procedure describes how to configure a D10 Tautwire Sensor.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Sensor Devices** > **D10 Tautwire Sensor**. 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 fields **Connected to** and **Device number** will only be populated once you assign the sensor to a Controller.
7. Click the **Configuration** tab.



8. Configure the fields as required:

Field	Description
Detection Window	This value indicates the least amount of time that the Detection Threshold must be exceeded by in order to indicate an alarm. (Default = 1 second. Range = 0.01 seconds to 60.00 seconds, i.e. 1 minute)
Detection Threshold	This value is the threshold that the processed value must exceed for a certain duration in order to indicate an alarm. (Default = 200. Range = 1 to 1000)
Alarm Latch Duration	This number determines how long an alarm condition is maintained after alarm condition is reached. (Default = 2.5 seconds. Range = 0.01 seconds to 600.00 seconds, i.e. 10 minutes)

9. If required, check the **Output Selection LED** checkbox.
   When checked the device provides a visual indicator if the device is in alarm.
10. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Tautwire Sensor.
    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 Tautwire Sensor.
    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 Tautwire Sensor.
    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 Tautwire Sensor.
    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.

Result

A new D10 Tautwire Sensor has been configured.

Assigning Z20 and D10 sensors to a Controller 6000

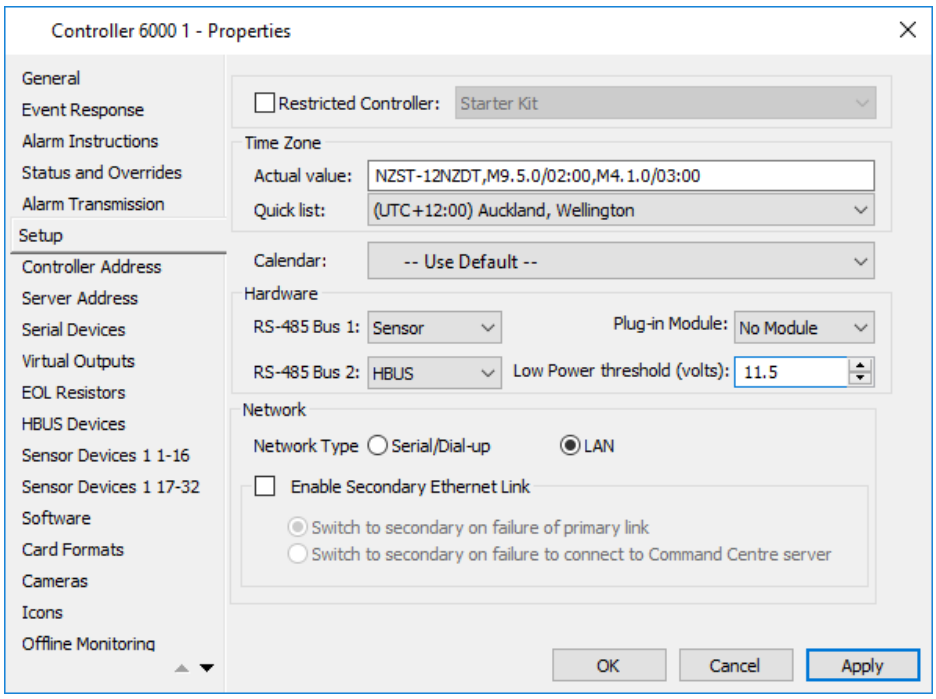
Introduction

This procedure describes how to assign either a Z20 Disturbance Sensor or a D10 Tautwire Sensor to a Controller 6000.

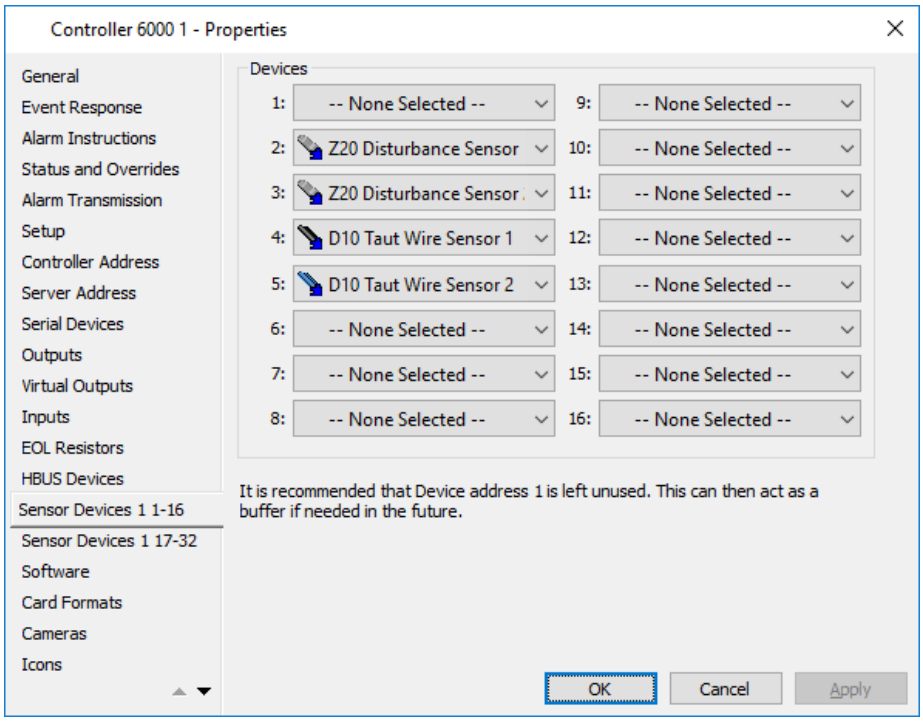
Note: A maximum of 32 (Z20 and D10) sensors can be connected per BUS to a Controller 6000, (i.e. a total of 64 Z20 and D10 sensors can be connected per Controller 6000).

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Double click** on the Controller 6000 you want to assign the sensor device to. By default the **General** tab displays.
3. Click the **Setup** tab.



4. Select "Sensor" from the **Bus 1** drop-down list.
   The tabs **Sensor Devices 1 1-16** and **Sensor Devices 1 17-32** appear, allowing you to now add up to 32 Sensor Devices to the Bus 1 port of this Controller.
   Note: If you want to assign Sensor Devices to **Bus 2**, configure the Bus 2 port as above. The tabs **Sensor Devices 2 1-16** and **Sensor Devices 2 17-32** will appear.
5. Click the **Sensor Devices 1 1-16** tab.



6. Assign the sensor to the appropriate device address by selecting it from the relevant drop-down list. The device address in Command Centre should be the same as the address configured for the sensor.
   Notes:
   - Two sensors with the same address must not be connected to the same BUS. They can however be connected to different BUSes.
   - We recommend you do not use Device 1 address, so it can act as a buffer if needed in the future.
     Sometimes when sensors go offline their address resets to 1. If this happens, performing a "Re-assign from Address 1" override (via the **Status and Overrides** tab of the sensors properties) will re-address the sensor correctly.

     Misaddressed Z20 Disturbance Sensors can be corrected by performing a 'Reset Z20 address to 1' override, which will re-address the sensor to 1.
     Important: A 'Reset Z20 address to 1' override should only be performed on one device on a bus at a time, otherwise all devices will go offline.
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

A sensor device has been assigned to the Controller 6000.
Notes:

- The address of the sensor now appears on **Connections** tab of the sensor's property pages.
- The sensor's version number now appears at the bottom of the sensor's **Configuration** property page, (e.g. Device Version: v0.22).

Performing a 'Log Tuning Data' Override on a Z20 Disturbance Sensor

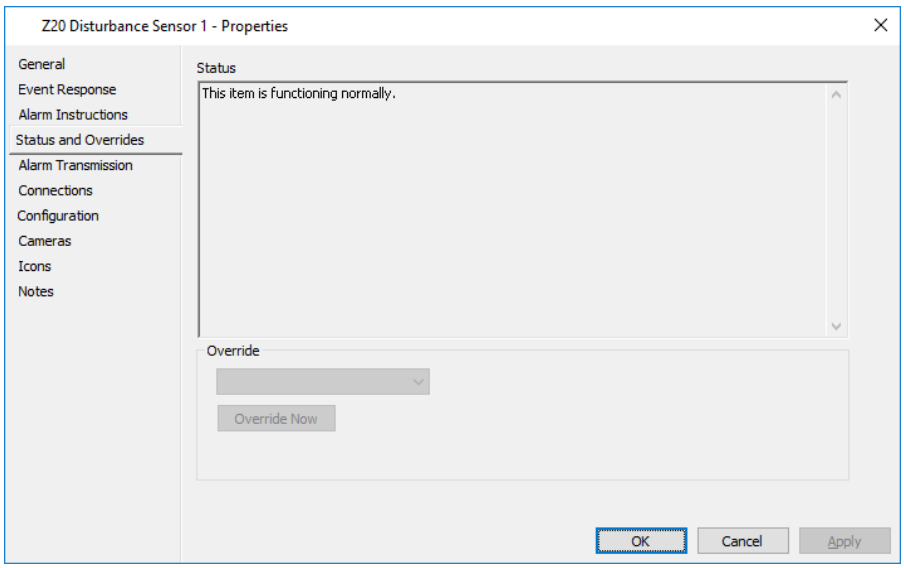
Introduction

Log Tuning Data mode on a Z20 Disturbance Sensor is used for maintenance checks and fault finding. During Log Tuning Data mode, Command Centre monitors and records the Dynamic Threshold value of a Z20 Disturbance Sensor.

This procedure describes how to perform a 'Log Tuning Data (48 hours)' override on a Z20 Disturbance Sensor.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** the appropriate Z20 Disturbance Sensor, and click **Override...** from the drop-down menu.
   The **Status and Overrides** tab on the Properties window for the item displays.



3. Click within the Override field and select **Log Tuning Data (48 hours)** from the drop-down.
4. Click the **Override Now** button.
   From this screen you can see the status change from 'Normal' to 'Logging Data' as a result of the override.
5. Click the **OK** button.
   This override will last for up to 48 hours or until it is cancelled.

   Sensors that are overridden this way will raise an alarm that stays active until the override is cancelled or it times out.

   Note: A report can be run from Command Centre Client, (i.e. not Configuration Client) that displays the data recorded over the 48 hours.

Chapter 56: PIV Card Support

The Federal Information Processing Standard Publication 201 (FIPS201) is a United States federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors.

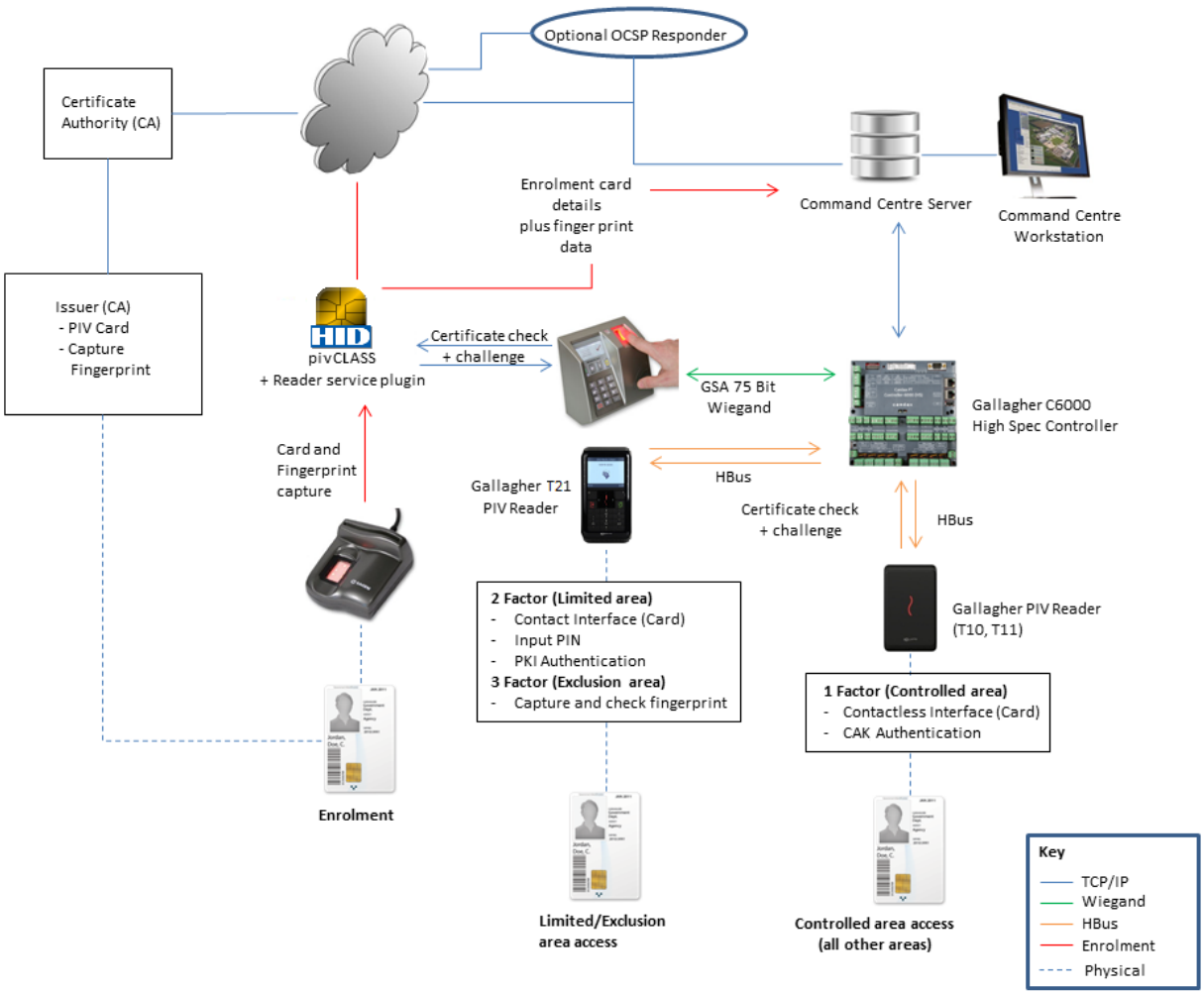
U.S. federal departments and agencies must use accredited issuers to issue PIV cards containing identity credentials for federal employees and contractors. Issued cards are enrolled into Gallagher Command Centre either using the registration process in Command Centre Client or via the pivCLASS Workstation software. Biometric and PIN validation occurs at this enrolment point.

Licensing

PIV Card functionality is a licensable feature. The license file must contain the following option:

```
[Features]
PIV=1
```

FIPS201 Topology



Enabling Windows FIPS mode

1. From the **Start** menu, click **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Local Policies** > **Security Options**.
2. Scroll down and double-click on **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing**.
3. Click the **Enabled** radio button, and then the **OK** button.

Note: The Command Centre Notifications feature is not supported in Windows FIPS 201 mode. Therefore, sites wishing to use the Windows FIPS 201 mode setting should not enable the email or SMS Notifications feature settings in Command Centre.

Select the item below that you require further detail on:

- ***Installing the necessary applications/tools for a pivCLASS Workstation*** (on page 56-3)
- ***Editing the PIV Card Type*** (on page 56-7)
- ***Configuring a PIV Card Reader*** (on page 56-19)
- ***Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Readers*** (on page 56-21)
- ***Supporting custom OCSP URLs for PIV certificate validation*** (on page 56-30)
- ***Enrolling PIV and PIV-I cards using a pivCLASS Workstation*** (on page 56-32)
- ***PIV cards in Command Centre*** (on page 56-33)

Installing the necessary applications/tools for a pivCLASS Workstation

Introduction

PIV cards can be enrolled for FIPS201 using either:

- **Command Centre Client** (the preferred method)
  Refer to the "PIV Cardholder Registration Process" in the *Gallagher Command Centre Client User Guide* for detailed instructions for this method

  OR

- **a pivCLASS Workstation** (covered in this topic)
  The following applications/tools all need to be installed before PIV cards can be enrolled for FIPS201 using a pivCLASS Workstation:
  - **pivCLASS PACS Plug-in for Command Centre** (to be installed on the Gallagher Command Centre Server)
  - **pivCLASS Workstation** (to be installed on the workstation - either server or remote)
  - **Gallagher Command Centre Import/Export Service**
  - **CCFT Data Manager** (configure only as this is installed with the Import/Export Service)
    Note: The pivCLASS PACS Plug-in must be restarted whenever a change is made to CCFT Data Manager.

pivCLASS Workstation captures the PIV data when PIV cards are enrolled, and the pivCLASS PACS Plug-in passes them to Gallagher Command Centre using the Gallagher Command Centre Import/Export Service.

Note: If your site is using supported Morpho (Sagem) contact card PIV encoders, you will need to install (or upgrade) their drivers to version MorphoSmart_USB_Driver_3_59_1_3, located in the Morpho Utilities.zip file of the Command Centre installation files.

Pre-requisites in Command Centre

Before proceeding with this procedure, ensure the following pre-requisites have been configured in Command Centre:

- Add a "CardholderId" text unique PDF which holds the FASC-N.
- Add a "Photo" PDF.
- If needed, create a default Access Group for PIV cardholders to be assigned on enrolment.
- Add the two PDFs created above to the default PIV Access Group.
- Add the "CardholderId" PDF as the Third-Party ID on the **Import** tab of the Server Properties.
- Create an operator for pivCLASS to use for enrolment, and give them the "Edit Cardholder", "Edit Cardholder Notes" and "Modify Access Control" privileges.

Procedure

Use the following procedure to install and configure all the applications/tools required for enrolling PIV cards for FIPS201.
Note: All User Manuals referred to in this procedure are located in the **'PIV Solution'** directory of the Gallagher Command Centre installation files.

Installing pivCLASS PACS Plug-in

1. Run the **pivCLASSPACSServiceCommandCentre-1.2.xxx.0.msi** file, located in the **'PIV Solution'** directory of the Gallagher Command Centre installation files.
   The Welcome screen of the pivCLASS PACS Service plug-in wizard displays.
2. Work your way through the wizard. When you reach the 'Completion' screen, click the **Finish** button.
   Refer to the "Installing the PACS Service" topic in Chapter 3 of the *PACS Service User Manual* for a detailed procedure.
   The pivCLASS PACS Plug-in is installed.
   Note: It installs to the default location **'C:\Program Files\HID Global\pivCLASS PACS Service'**, or another location if you opted to change it on the 'Destination Folder' screen of the wizard. A pivCLASS PACS Plug-in desktop shortcut may also have been selected during the install.
3. Configure the pivCLASS PACS Plug-in, by completing the "Configuring the PACS Database Parameters" procedure on page 16 of the *Command Centre Plugin User Manual*.
   Notes:
   - Use the default user name and password, "admin" and "password" on the Login screen.
   - Use the operator already created (as a prerequisite above) for **Username** and **Password**.
   - The **Server name** can be "localhost" if Command Centre is installed on the same server.
   - Both **Test** buttons need to be clicked to enable the **Accept** button.
   - The "Database Connection Parameters" section can be ignored.
   - Browse the Product path and select the correct path for your installation of Command Centre.
4. In the XML template file, change the Access Groups section to reflect the default PIV Access Group chosen/created (as part of the Prerequisites above), as follows:
   a) Open the **template.xml** file, usually located in **'C:\Program Files (x86)\HID Global\pivCLASS PACS Service\templates'** in a text editor.
   b) Scroll down to the Access Groups item:

```
<item>
  <card>Access Group 1</card>
  <pacs>AccessGroup.1</pacs>
</item>
```

c) Modify the " <card>Access Group 1</card>" section to reflect the name of the Access Group you want the cardholders assigned when they are enrolled.

d) Save the modified **template.xml** file.

Installing pivCLASS Workstation

5. Run the **pivCLASSWorkstation-1.2.xxx.0.msi** file, located in the **`'PIV Solution'`** directory of the Gallagher Command Centre installation files. The Welcome screen of the pivCLASS Workstation Setup wizard displays.
6. Work your way through the wizard. Once you reach the 'Completion' screen, click the **Finish** button.
   Refer to the "Installation" topic in Chapter 5 of the *pivCLASS Registration Workstation Use Manual* for a detailed procedure.
   pivCLASS Workstation is installed.
7. Login to pivCLASS Workstation and license it.
   Refer to "Chapter 5-13: Logging In and Licensing pivCLASS" of the *pivCLASS Registration Workstation Use Manual* for a detailed procedure.
   Notes:
   - Once the software is deployed at the customer site, the technician must send the system ID to ordersamer@hidglobal.com.
     Once pivCLASS receive this information, they will return a licensing key with licensing to match what was purchased via the GGL purchase order.
   - Use the default user name and password, "admin" and "password" on the Login screen.
8. Configure pivCLASS Workstation as appropriate.
   Refer to "Chapter 6: Configuring pivCLASS" of the *pivCLASS Registration Workstation Use Manual* for a detailed procedure.
9. Complete the "Client Authentication" section on pages 40 - 42 of the *pivCLASS Registration Workstation Use Manual*, to add the pivCLASS Workstation client to the pivCLASS PACS Plug-in.
10. Complete the installation and configuration of your selected Smart Card Reader that will be used for enrolment of cardholders via pivCLASS. Refer to the "Peripheral Setup" section in Chapter 4 of the *pivCLASS Registration Workstation Use Manual* for a detailed procedure.

Installing the Gallagher Command Centre Import/Export Service

11. Install the Gallagher Command Centre Import/Export Service on the same PC as pivCLASS PACS Plug-in.
    Refer to the "Installing the Service" topic in the *Gallagher Command Centre Import/Export Utility User Guide* (**Import_User Guide.chm**) for a detailed procedure. This document is located in the **`'Utilities\import export'`** directory of the Gallagher Command Centre installation files.

Editing the PIV Card Type

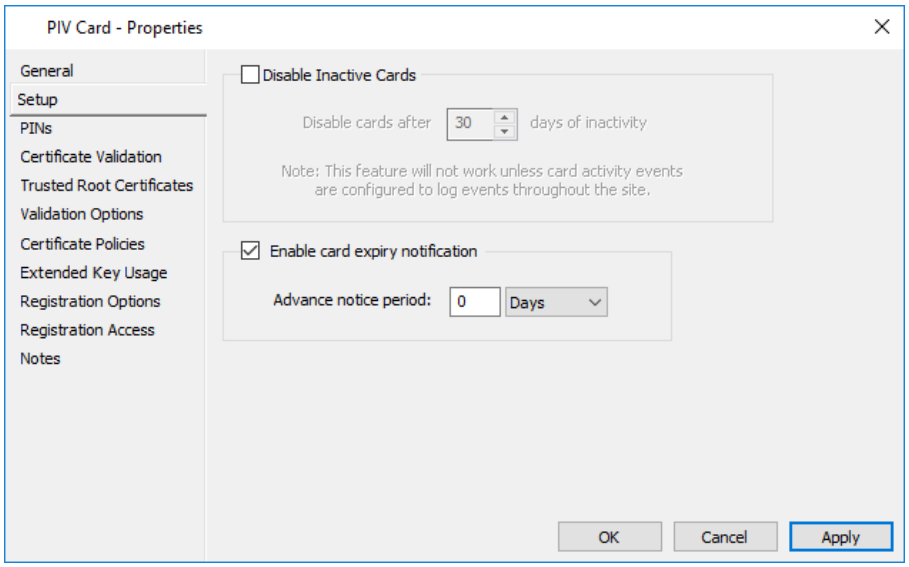
Introduction

When a site is licensed for Personal Identity Verification (PIV), a PIV card type is available by default in the Card Type List Window. The PIV card type is a special card type for the exclusive use of PIV and PIV-I cards, and is not creatable, (i.e. only one PIV card type record will exist, and cannot be deleted, copied or created manually).

Operators require the "Configure Site" privilege in the appropriate division to be able to edit the PIV Card Type.
Note: The "View Site" privilege in the appropriate division will allow an operator to view (but not edit) the PIV Card Type.

Procedure

1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens (in grid view), with the "PIV Card" appearing by default.
2. **Right click** on the "PIV Card" and select **Properties**.
   By default the **General** tab displays.
3. Edit the **Description** and the **Division** that the PIV card type exists in if required.
   Note: The **Name** is non-editable, and therefore disabled.
4. Click the **Setup** tab.



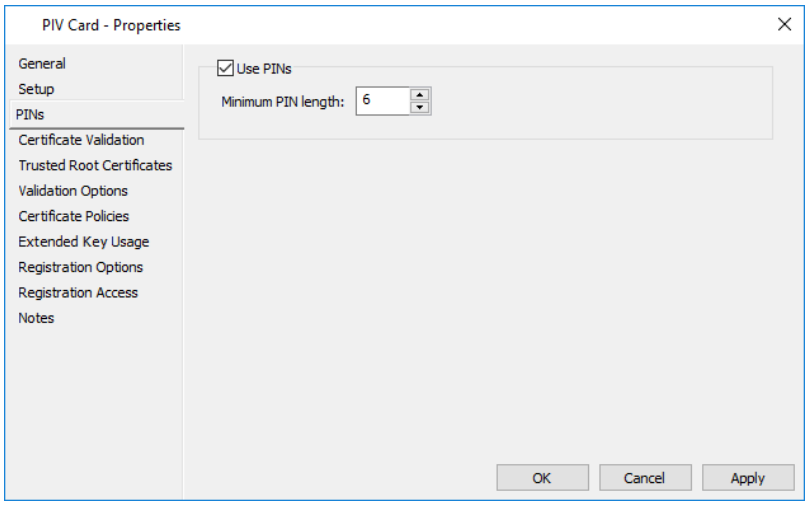
5. Do you wish to enable the Inactive Card Expiry feature?
   Note: All cards of a particular type shall share a common inactivity timeout if enabled.

If...	then...
yes	check the **Disable Inactive Cards** checkbox. Go to Step 6.
no	leave the **Disable Inactive Cards** checkbox unchecked. Go to Step 7.

6. Enter a figure to represent the number of days of inactivity that will disable a card. **Notes:**
   - When this feature is first enabled the default timeout = 30 days. The range is 1 - 999 days.
   - If you set a card type to disable after 1 day of inactivity, these cards will become disabled 24 hours to the second after the **Apply** button is clicked, (e.g. card type set on 27/11/2011 at 16:10:15; if not used these cards become disabled on 28/11/2011 at 16:10:15).
   - Cardholders will be expired regardless of activity if card activity events are not configured to log events throughout the site (see Event Defaults for further detail).
7. The **Enable card expiry notification** section of this screen allows you to configure warning notifications of pending card expiry to be sent when the specified period is reached, for all cards regardless of status.
   Do you want to enable card expiry notification?

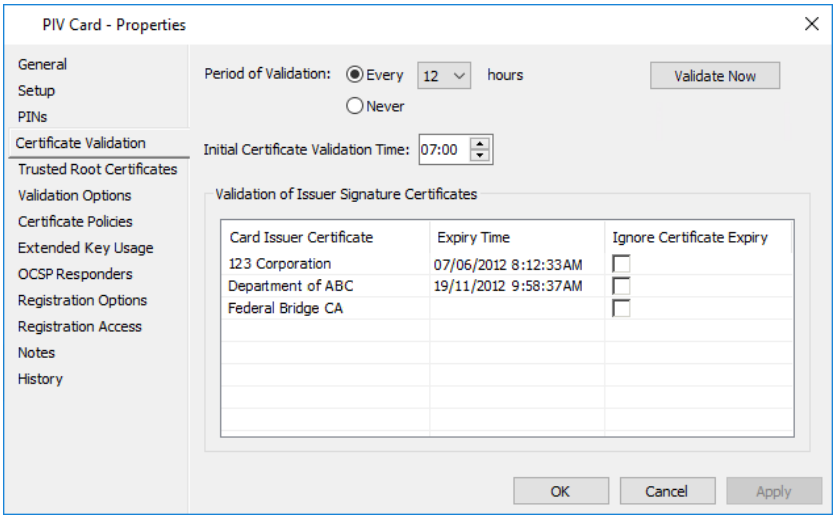
If...	then...
no	uncheck the **Enable card expiry notification** checkbox, and leave the **Advance notice period** as 0 Days.
yes	**a)** Ensure the **Enable card expiry notification** checkbox remains checked. **b)** Set the Advance notice period to the value that is required to represent the number of days, weeks, months or years prior to card expiry to initiate the warning notification.

8. Click the **PINs** tab.



9. If you want to use PINs, check the **Use PINs** checkbox and set the **Minimum PIN length**. (Default = 6 digits. Range = 4 - 8 digits) **Notes:**
   - If you do not choose to **Use PINs**, the **Assign PIN** button on the Cardholder Cards tile in Command Centre Client will be disabled.
   - The maximum PIN length is **8** digits. There is no mechanism to reduce the maximum size. Hence if a site sets minimum at 4, the user can enter PIN length anywhere from 4 to **8** digits.
   - The system prevents PINs with 3 consecutive or 3 repeating numbers from being either manually entered or automatically generated.

10. Click the **Certificate Validation** tab.



11. The **Period of Validation** can either be specified in hours, it can occur immediately, or it can be turned off.

If you want to...	**then...**
change the period of validation,	**a)** Click the **every** radio button. **b)** Select the appropriate number from the **hours** drop-down for the period between validation occurrences. (Default = 12 hours. Range = 1, 2, 3, 4, 6, 8, 12, 24 hours) **c)** Go to Step 12.
Validate immediately,	**a)** Click the **Validate Now** button. **Note:** Validations cannot be run concurrently. If one is already running the message *"A validation is already in progress"* will display. **b)** Go to Step12.
turn validation off,	**c)** Click the **Never** radio button. The **Initial Certificate Validation Time** is disabled. **d)** Go to Step 13. **IMPORTANT:** Clicking the **Never** radio button turns off all validation, not just for cards subsequently enrolled. It does not reinstate disabled cards from a previous validation where they have failed.

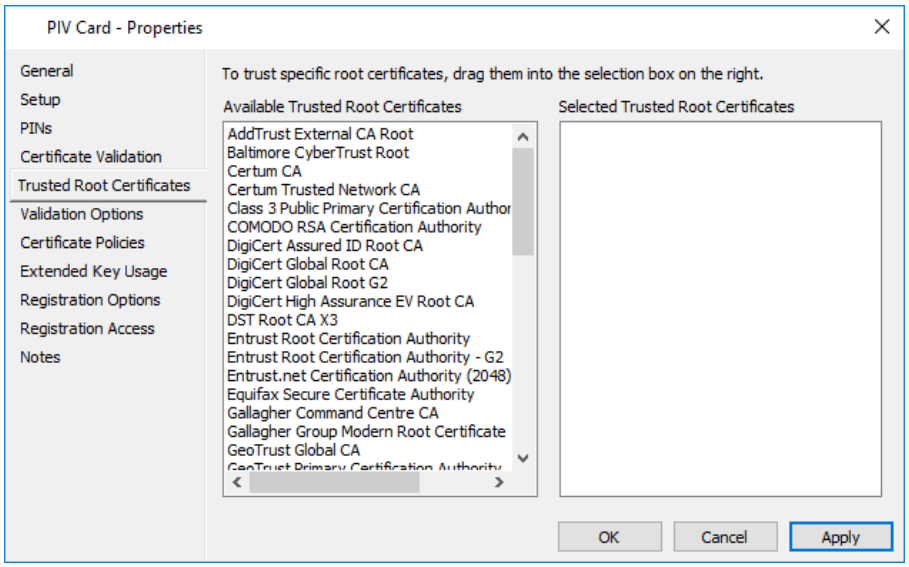
Notes:

- If certificate validation is still occurring at the time of the next validation scheduled start time, the next validation will be skipped, and an event is raised indicating that a validation cycle has been skipped.
- If the Command Centre service is restarted after the cards are enrolled but before any validation has occurred, (i.e. validation has NOT been turned off), automatic validation on enrolment will never occur.
- When the validation process results in Command Centre recognising that a PIV card's PIV, CAK or Issuer Signature certificate is invalid, the following occurs:

- the card cannot be used to gain access,
- an Alarm is raised, and
- the card is marked with the status **Revoked**, **Expired** or **Not Trusted**.

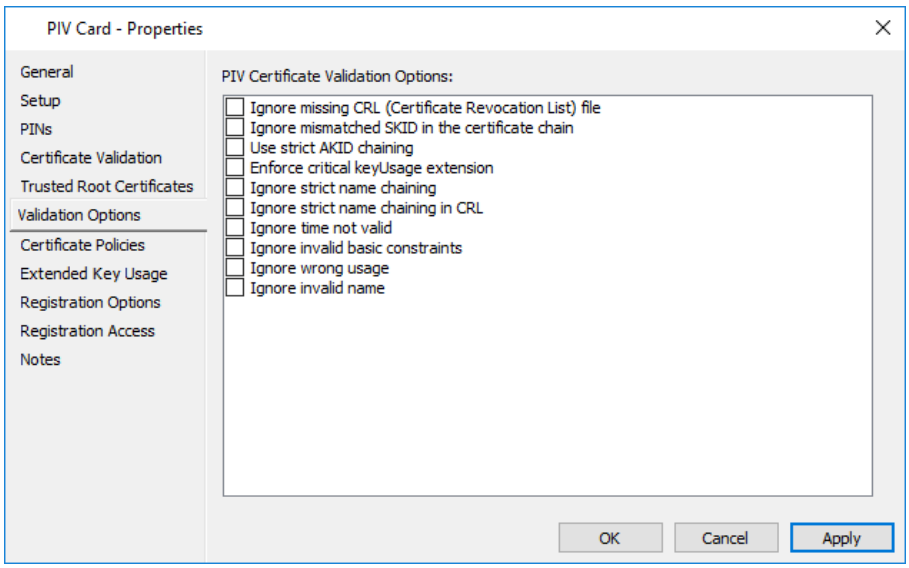
Note: Cards with a status of **Revoked** or **Expired** must be re-enrolled. If a root certificate is added to the Windows Certificate Store and the Selected Trusted Root Certificates listbox relating to a card with a status of **Not Trusted**, the card will become **Active** and can be used after the next successful validation.

12. When Command Centre is licensed for PIV the first credential/path validation check will occur at the next occurrence of the **Initial Certificate Validation Time**. The default for this control is 07:00 (7am).
    Notes:
    - When the **Initial Certificate Validation Time** is changed, the validation will start at the next occurrence of that daily time, and subsequent validation will begin based on the period.
    - For the validation checks via internet you need to run the Command Centre service as a user who has access to the internet. This may also require some configuration by your IT Department.
13. The **Validation of Issuer Signature Certificates** section on this tab provides a list of certificate issuers with an option to exclude/ignore validation of expired Issuer Signature certificates when the card has not expired. By default all checkboxes are enabled and deselected, so that when a card is not expired, all Issuer's Issuer Signature certificates are validated regardless of the expiry status of the certificate.
    Note: Use this feature in the event that PIV Card Issuers have issued cards that expire after the expiry of certificates higher in the certificate chain, if you do not wish such cards to be considered revoked.
14. Check the **Ignore Certificate Expiry** checkbox for Card Issuer(s), as required.
    Note: When the **Ignore Certificate Expiry** checkbox is checked for a particular Card Issuer, if a card has not expired but that Issuer's Issuer Signature certificate has expired, the validation will not run for that certificate.
15. Click the **Trusted Root Certificates** tab.



This tab allows you to explicitly add Trusted Root Certificates that exist in the server's certificate store.
The 'Available Trusted Root Certificates' grid is populated with all Trusted Root Certification Authority certificates available to the server in the Windows certificate store.

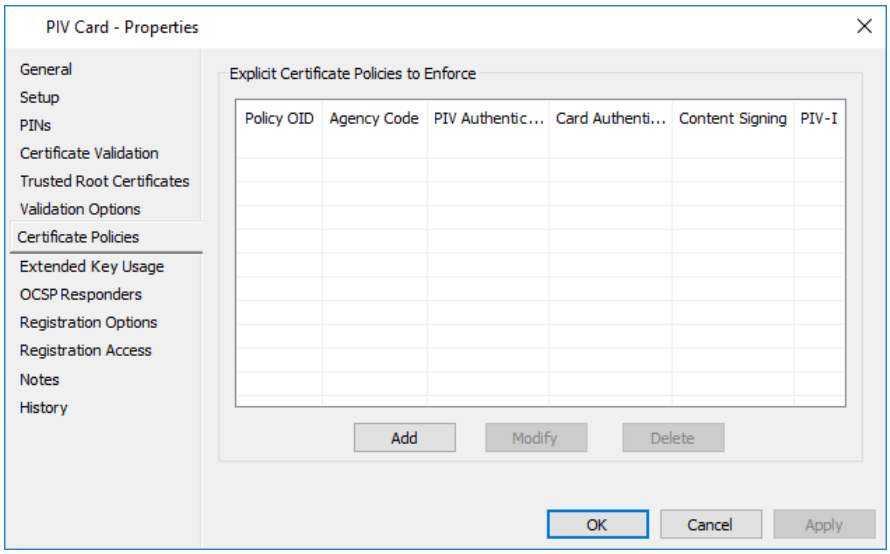
16. Drag any of the certificates you require from the 'Available Trusted Root Certificates' grid across to the 'Selected Trusted Root Certificates' grid.
Notes:
    - If a required certificate does not appear in the 'Available Trusted Root Certificates' grid, see ***Setup Certificate Manager*** (on page 56-17) for instructions on how to import it into the list.
    - When a certificate is added to the 'Selected Trusted Root Certificates' grid, the certificate is removed from the 'Available Trusted Root Certificates' grid. When a certificate is removed from the 'Selected Trusted Root Certificates' grid (via a right click and selecting **Remove from List**), the certificate reappears in the 'Available Trusted Root Certificates' grid.
    - When a PIV card is presented at a reader it must have its Trusted Root Certificate explicitly selected before access can be granted. If not, a 'Certificate Not Trusted' event will be raised.
17. Click the **Validation Options** tab.



This tab provides options to ignore validation faults that can make a card unusable due to certificate errors. The options are as follows:

			Outcome				
Checkbox	**Type of fault**	**Checked (Y/N)**	Fault is ignored	Card remain in normal (Active) status	Card flagged as "card certificate error" status during validation	Card flagged as "certificate status unknown"	Card can still be used for access
Ignore missing CRL (Certificate Revocation List) file	Missing CRL file fault	N	✗	✗	✓	✗	✗
		Y	✓	✗	✗	✓	✓
Ignore mismatched SKID in the certificate chain	Mismatched SKID fault	N	✗	✗	✓	✗	✗
		Y	✓	✓	✗	✗	✓
Use strict AKID chaining	Mismatched AKID fault	N	✓	✓	✗	✗	✓
		Y	✗	✗	✓	✗	✗
Enforce critical keyUsage extension	Non-critical keyUsage extension fault	N	✓	✓	✗	✗	✓
		Y	✗	✗	✓	✗	✗
Ignore strict name chaining	Mismatched issuer common name fault in the certificate	N	✗	✗	✓	✗	✗
		Y	✓	✓	✗	✗	✓
Ignore strict name chaining in CRL	Mismatched issuer common name fault in the CRL	N	✗	✗	✓	✗	✗
		Y	✓	✓	✗	✗	✓
Ignore time not valid	Invalid certificate notAfter or notBefore time	N	✗	✗	✗ Card flagged as “card certificate time invalid” status during validation	✗ Card flagged as “card certificate time invalid” status during validation	✗
		Y	✓	✓	✗	✗	✓
Ignore invalid basic constraints	CA certificate(s) has invalid or missing basic constraints	N	✗	✗		✗	✗
		Y	✓	✓	✗	✗	✓
Ignore wrong usage	Invalid keyUsage extension for CA certificate	N	✗	✗	✓	✗	✗
		Y	✓	✓	✗	✗	✓
Ignore invalid name	Invalid certificate subject name	N	✗	✗	✓	✗	✗
		Y	✓	✓	✗	✗	✓

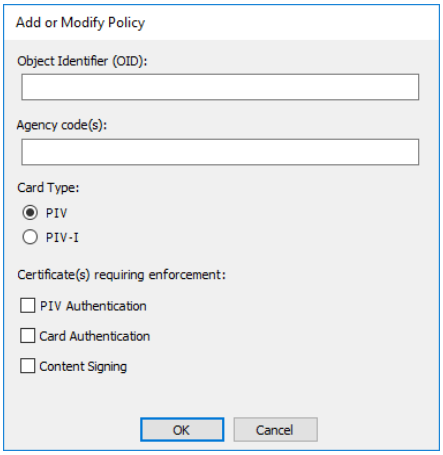
18. If required, check the appropriate checkbox(es) for any faults that are to be ignored.
19. Click the **Certificate Policies** tab.



This tab allows you to add certificate policies (represented by their corresponding Object Identifiers (OIDs)), to cards issued by a particular agency/agencies, which will be explicitly enforced during periodical certificate validation.

20. Do you want to add Policy OIDs to this PIV Card Type?

If...	then...
no	go to Step 21.
yes	**a)** Click the **Add** button. An Add or Modify Policy dialog displays.



b) Enter the **Object Identifier (OID)** and **Agency code(s)** in the appropriate fields.

c) Click the appropriate radio button to indicate if the policy is to be applied to PIV or PIV-I cards.

d) Select at least one type of certificate that requires enforcing, by checking the appropriate checkbox(es).

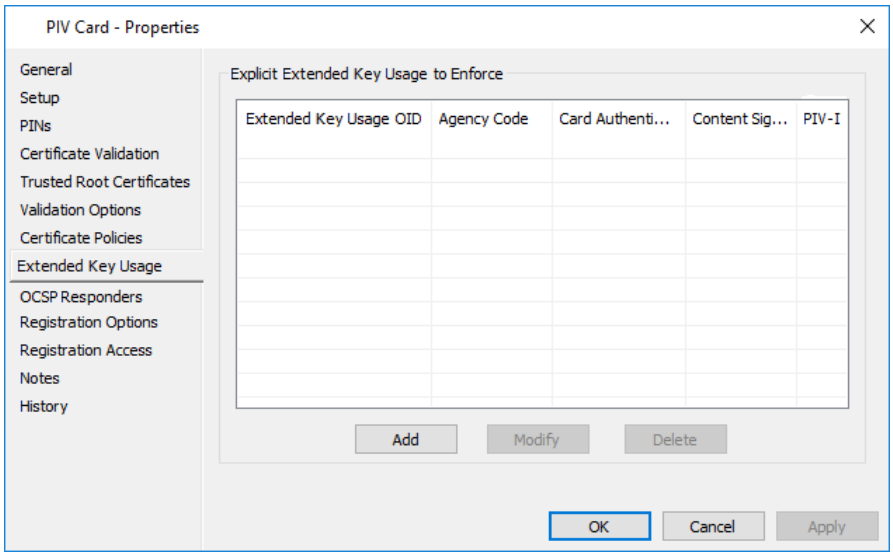
e) Click the **OK** button. The Add or Modify Policy dialog closes.

Notes:

- The PIV-I column in the grid will display 'Yes' for Policy OIDs that are to be applied to PIV-I cards or 'No' for those to be applied to PIV cards.

If...	then...
	• The **Modify** button allows existing Policy OIDs to be modified, and the **Delete** button allows them to be deleted. As soon as the **Apply** button is clicked, the system will automatically attempt to validate the certificates. • If an error is found during validation an alarm is generated. The **Details** tab of the alarm properties describes the cause of the validation error.

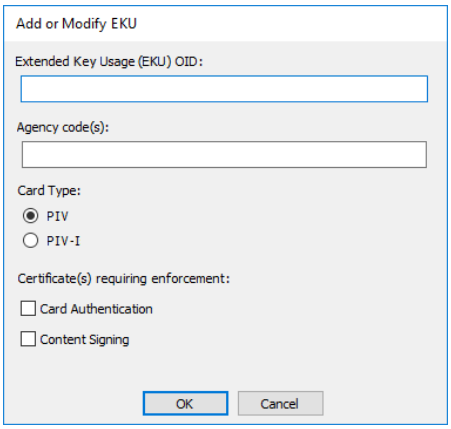
21. Click the **Extended Key Usage** tab.



This tab is optional and allows the Operator to select which Extended Key Usages (EKUs) they want to enforce.

22. Do you want to add an EKU?

If...	then...
no	go to Step 23.
yes	**a)** Click the **Add** button. An Add or Modify EKU dialog displays.

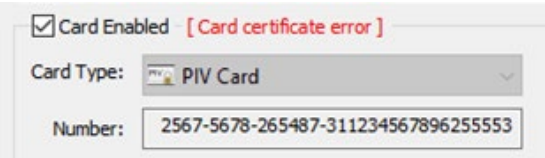


b) Enter the **Extended Key Usage (EKU) OID** (13 digits in the format *n.nn.nnn.n.nnn.n.n.n*) and **Agency code(s)** (4 digits) in the appropriate fields.
Note: If the Extended EKU OID applies to multiple Agency codes, separate the codes with a semi-colon.

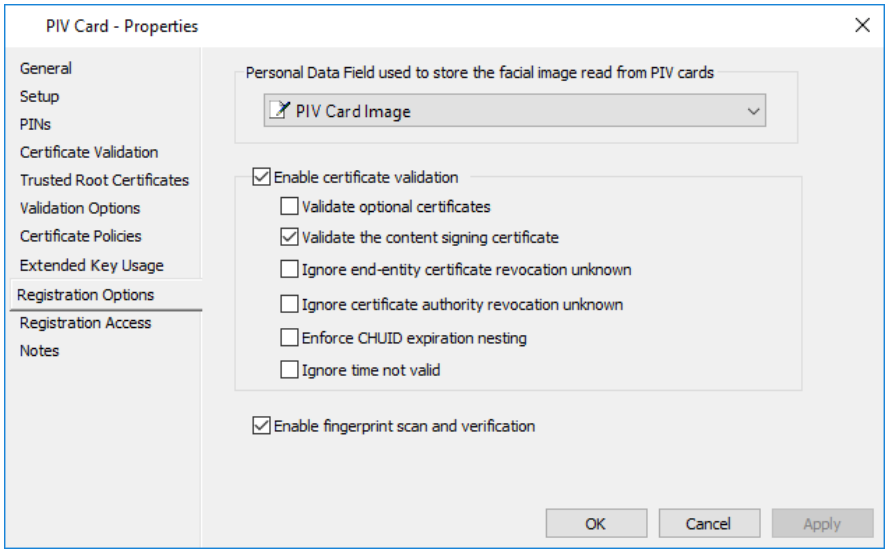
If...	then...
	c) Click the appropriate radio button to indicate if the policy is to be applied to PIV or PIV-I cards. **d)** Select at least one type of certificate that requires enforcing, by checking the appropriate checkbox(es). **e)** Click the **OK** button. The Add or Modify EKU dialog closes.

Notes:

- The PIV-I column in the grid will display 'Yes' for EKU OIDs that are to be applied to PIV-I cards or 'No' for those to be applied to PIV cards.
- The **Modify** button allows existing Policy EKUs to be modified, and the **Delete** button allows them to be deleted. As soon as the **Apply** button is clicked, the system will automatically attempt to validate the certificates.
- If an error is found during validation an alarm is generated. The **Details** tab of the alarm properties describes the cause of the certificate validation error, and the Cardholder's properties (on the **Cards** tab) displays as error:



23. Click the **Registration Options** tab.



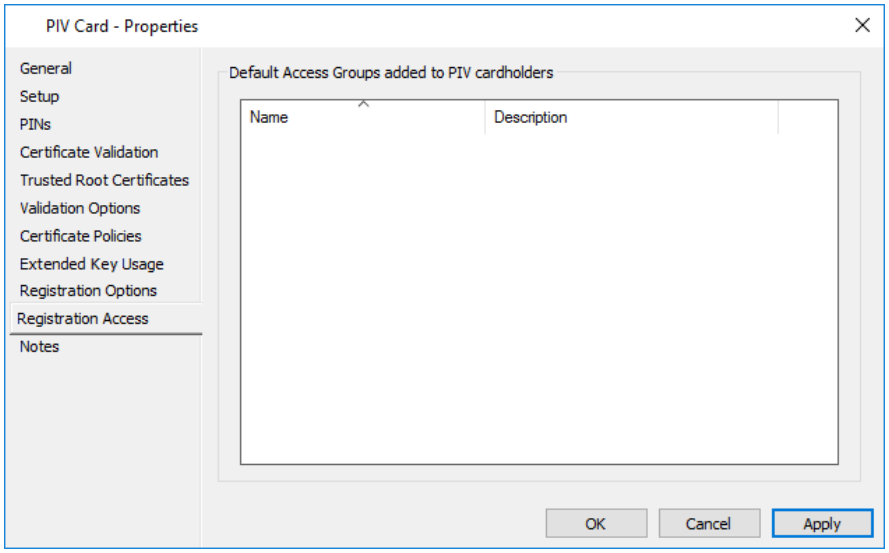
This tab provides a number of options that can be configured for PIV Cardholder registration.

24. If you want to register PIV Cardholders, configure as required:
    a) Select the Image PDF from the drop-down list, which will be used to store the facial image read from PIV cards.
    b) If you want to enable certificate validation at the time of card registration, ensure the **Enable certificate validation** checkbox is ticked, and any other checkboxes in that section to further refine the controls.

c) If you want fingerprint verification to be part of the PIV Cardholder registration process, ensure the **Enable Fingerprint can and verification** checkbox is ticked.
IMPORTANT: If you do NOT want to enrol fingerprints you have to untick this checkbox.

Note: PIV Cardholder Registration is done in the Command Centre Client. Refer to the ***PIV Cardholder Registration Process*** (on page 3-175) in the *Gallagher Command Centre Client User Guide* for the complete process.

25. Click the **Registration Access** tab.



This tab allows you to add default Access Groups to be assigned to PIV Cardholders during registration.

26. Add default Access Groups (if required), as follows:
    a) Click **Manage** from the menu bar, then **Access Groups**.
    The **Access Group** List Window opens.
    b) Drag and drop the required Access Groups into the **Registration Access** tab.
    c) Close the **Access Group** List Window.

    Note: If an Access Group contains a 'Required' PDF that does not have a default value, then the cardholder registration will fail with the error message:
    "Failed to save Cardholder changes.
    The cardholder failed to save due to an empty required Personal Data Field".

    Population of a default value or removal of the 'required' PDF from Access Groups that are added to PIV cardholders during registration is recommended.

27. Click the **Notes** tab if you want to add a note(s) about the PIV Card Type. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
28. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Setup Certificate Manager

Introduction

If a required certificate does not appear in the 'Available Trusted Root Certificates' list (on the **Trusted Root Certificates** tab of the PIV Card Type properties), this procedure can be used to import the certificate into the list.

You will need to have available or download the required Root Certificate to be able to complete this procedure.

Procedure

1. From the **Start** menu, click **Run…**
2. Type in **MMC** and click **OK**.
   The MMC Console window displays.
3. Select **File** from the menu bar, then **Add/Remove Snap-in…**
   The Add or Remove Snap-ins dialog displays.
4. Select **Certificates** in the 'Available snap-ins' grid on the left, and click the **Add** button.
   A Certificates snap-in screen displays.
5. Click the **Computer account** radio button, then click the **Next** button.
   The Select Computer screen displays.
6. Click the **Finish** button.
7. Click the **OK** button.
   The Add or Remove Snap-ins dialog closes.
8. Select **File** again from the menu bar, then **Save As…**
9. Choose a name, then save in your Administrative Tools programs directory.
   The local machine certificate store should now be visible in tree view in the left grid.
10. Click on the local machine certificate store in the left grid.
11. Right-click on **Trusted Root Certification Authorities**, then select **All Tasks** > **Import…**
    The Certificate Import Wizard displays.
12. Click the **Next** button.
13. Click the **Browse** button and navigate to the location of the Trusted Root Certificate.
    Note: You may need to change the "File Type" for the certificate to appear.
14. Select the certificate and click the **Open** button.
15. Click the **Next** button.

16. Select the **Place all certificates in the following store** option, and click the **Next** button.
17. Click the **Finish** button.
    The import completes.
18. Select **File** again from the menu bar, then **Exit**.
    The certificate should now be visible in the 'Available Trusted Root Certificates' grid on the **Trusted Root Certificates** tab of the PIV Card Type properties.
    Note: You may need to **right click** > **Refresh List** for the grid to update.

Configuring a PIV Card Reader

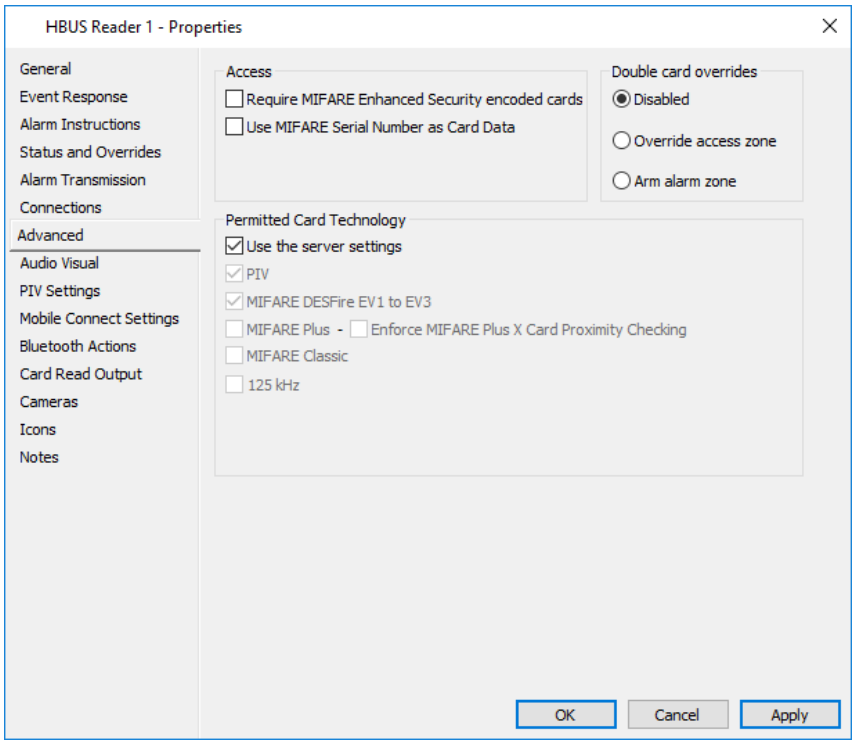
Introduction

The PIV reader is distributed as a new 'part', separated from standard readers. This procedure describes how to configure a PIV card reader in Command Centre. Operators require the "Edit Site" privilege in the appropriate division to be able to create, edit and delete PIV Card Readers.

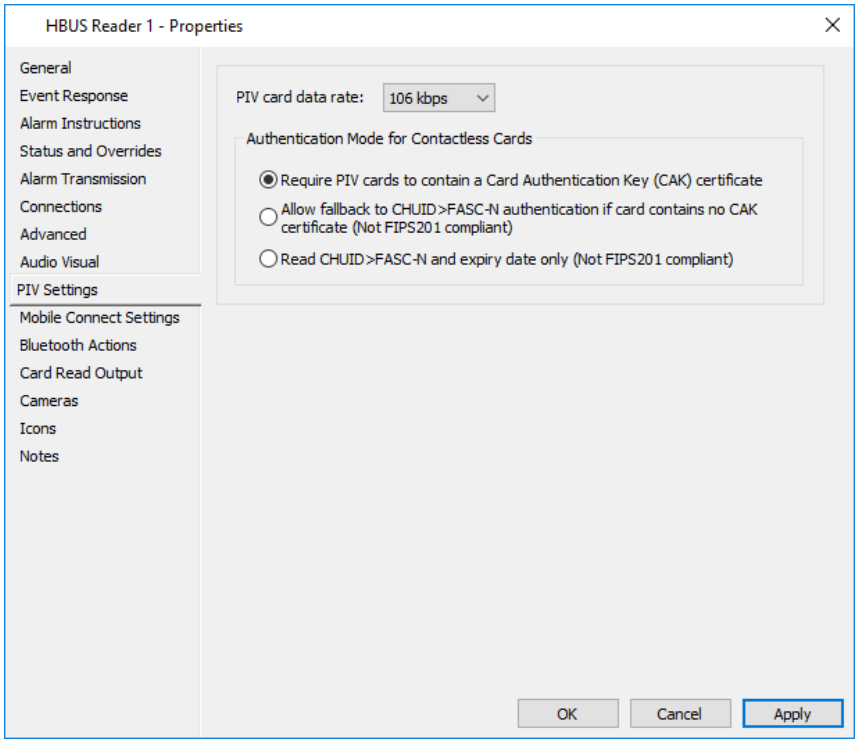
Note: The "View Site" privilege in the appropriate division will allow an operator to view (but not edit) PIV Card Readers.

Procedure

1. Complete the reader configuration as per the procedure for ***Creating Readers*** (on page 21-40), and then go to Step 2 of this procedure.
   Note: If configuring an HBUS PIV Terminal, refer to the procedure Configuring an HBUS Terminal. If configuring an HBUS PIV Contact Card Reader, refer to the procedure ***Configuring an HBUS Contact Card Reader*** (on page 21-88).
2. If you want to restrict the reader to reading PIV cards only, click the **Advanced** tab and deselect all **Permitted Card Technology** checkboxes, except the PIV or PIV Contactless checkbox.
   Notes:
   - For the HBUS Contact Card Reader to accept both contact and contactless PIV cards, check the **PIV Contactless** checkbox in the Permitted Card Technology section.
   - You will only be able to do this if you have the "Configure Site" operator privilege as well as the "Edit Site" privilege.



3. Click the **PIV Settings** tab.



4. Change the **PIV card data rate** if necessary by selecting another rate from the drop-down list. The PIV reader supports card data rates of 106 (the default), 212, 424 and 848 kbps.

   Note: If a card cannot support the selected rate, then the highest supported rate will be used.

5. Select the appropriate Authentication Mode by clicking the relevant radio button. By default, **Require PIV cards to contain a Card Authentication Key (CAK) certificate** is selected.
   Notes:

   - Only one authentication mode can be selected.
   - PIV Authentication mode is only valid when using PIV Contactless cards.
   - Regardless of the PIV Authentication mode selected, when the card is inserted at a High Sec T21 Reader, it always looks for CAK and then for PIV key when CAK is absent.
   - When Cards don't have CAK certificate, the cardholder will be prompted to insert the card at a High Sec T21 Reader and prompted to enter PIV PIN to validate the PIV Certificate.
   - The **Allow fallback to CHUID>FASC-N authentication if card contains no CAK certificate (Not FIPS201 compliant)** option allows a reader to fallback to the CHUID> FASC-N when the PIV Card does not contain a CAK certificate, but this is not FIPS201 compliant.

Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Readers

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.

The Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Reader provides three factor authentication, (i.e. Card, PIN and Fingerprint), if required.

OSDP Veridt Stealth PIV Readers should only be assigned to Gallagher PIV Controller 6000s. We recommend only using one Veridt Reader per RS-485 Bus.

Functionality not supported

The following functionality is NOT supported on OSDP Veridt Stealth PIV Readers:

- PIN to PACS
- PIN is User Code
- Code only code
- Duress
- PIN's mode when the reader is on an Elevator Car.
  Note: If the Access zone is in "Secure - No PIN" mode, but Veridt Reader access mode mapping is Two Factor, a PIN will be requested for access.
- Double card overrides will work on the Veridt Reader using proximity PIV cards. Not supported with PINs mode or when card inserted.

Known Issues

- Veridt Readers will reset and generate a "not responding" alarm when a PIN is not entered or just the **#** key is entered for the second consecutive time after inserting the card.
- When a non-BIO Veridt Reader is configured as Three Factor, it will respond with "Access Denied" after entering the PIN, and a Fingerprint Mismatch event will be generated in Command Centre.
- When power cycling a Veridt Reader on Address 1, the baud rate will change to 9600.
- Changing Address will set the baud rate to the default of 9600.
- Veridt Readers may restart when PIV Contactless cards are presented immediately at the end of every access transaction.

Select the item below that you require further detail on:

- ***Configuring an OSDP Veridt Stealth PIV Reader*** (on page 56-22)
- ***Assigning an OSDP Veridt Stealth PIV Reader to a Gallagher PIV Controller 6000*** (on page 56-27)

Configuring an OSDP Veridt Stealth PIV Reader

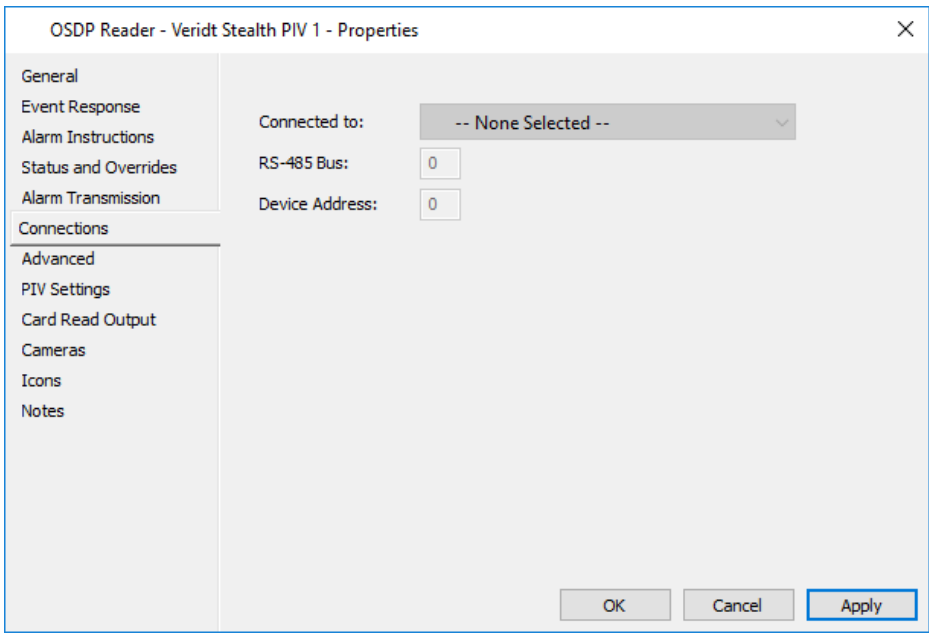
Introduction

This procedure describes how to configure an Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Reader in Gallagher Command Centre.

Operators require the "Edit Site" privilege in the appropriate division to be able to create, edit and delete OSDP Veridt Stealth PIV Readers.
Note: The "View Site" privilege in the appropriate division will allow an operator to view (but not edit) OSDP Veridt Stealth PIV Readers.

Procedure

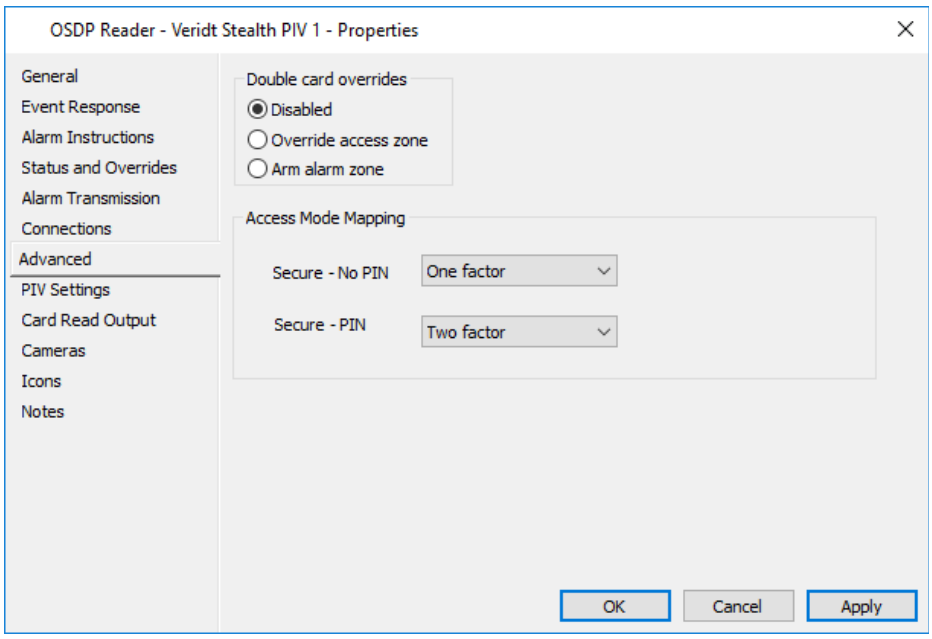
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...OSDP Devices** > **OSDP Reader - Veridt Stealth PIV.**
   By default the **General** tab displays.
3. Complete the fields as required.
   For further 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 reader to a PIV Controller 6000. See

Assigning an OSDP Veridt Stealth PIV Reader to a Gallagher PIV Controller 6000 (on page 56-27) for further detail.

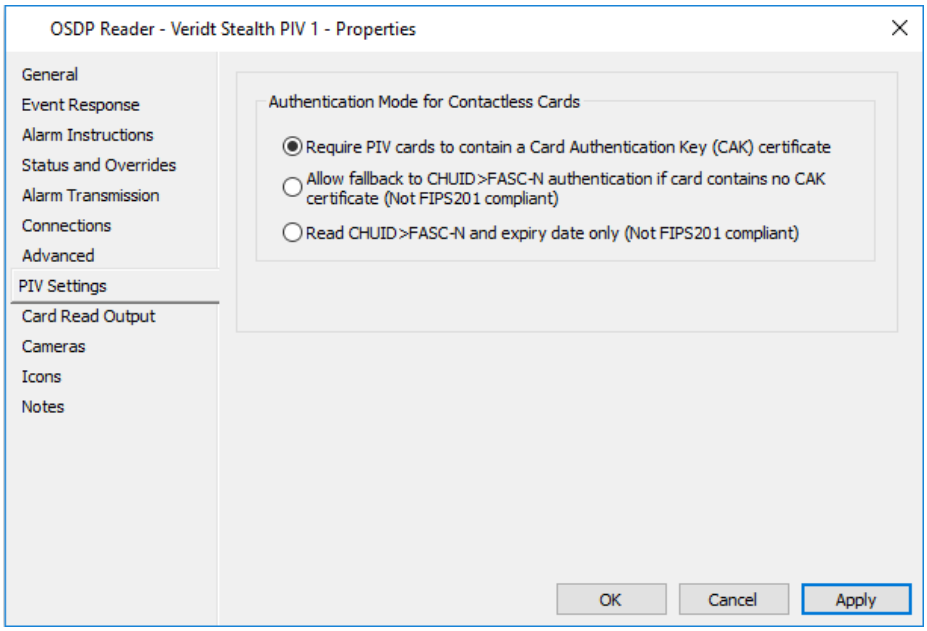
7. Click the **Advanced** tab.



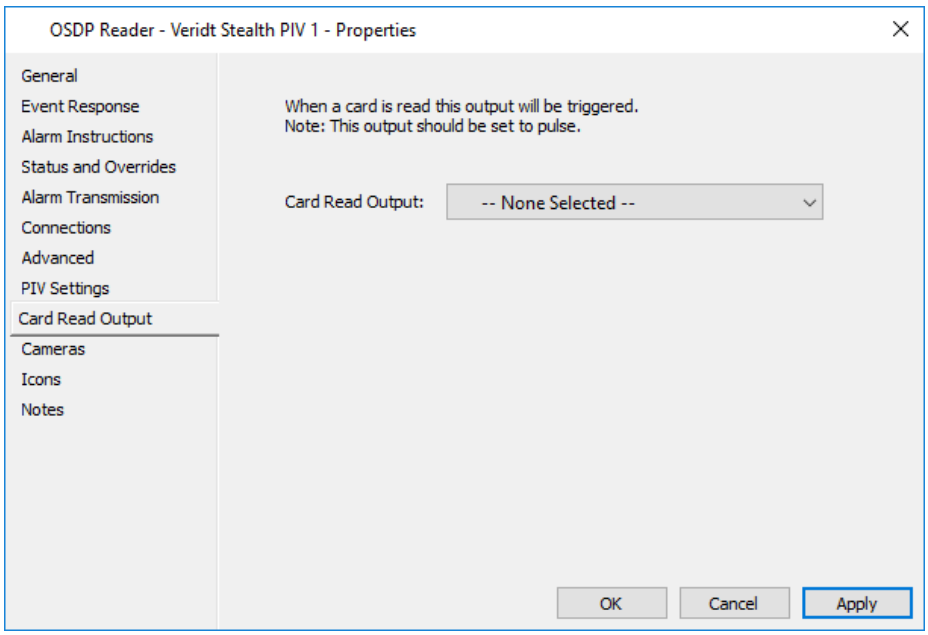
8. If you want the double-card override feature to be available, click either the **Override access zone** or the **Arm alarm zone** radio button, depending on whether you want the double-card override to override the state of the Access Zone or arm the Alarm Zone associated with the Access Zone.
Note: It will only work with proximity cards. Contact will not work.
9. Configure the access mode mapping for the reader as appropriate.

Field	Description
Secure - No PIN	There are two options available from the drop-down, (i.e. One factor or Two factor). Default = One factor
Secure - PIN	There are two options available from the drop-down, (i.e. Two factor or Three factor). Default = Two factor

10. Click the **PIV Settings** tab.



11. Select the appropriate Authentication Mode by clicking the relevant radio button. By default, **Require PIV cards to contain a Card Authentication Key (CAK) certificate** is selected.
    Notes:
    - The authentication mode applies to PIV contactless cards only.
    - Only one authentication mode can be selected.
    - The **Allow fallback to CHUID>FASC-N authentication if card contains no CAK certificate (Not FIPS201 compliant)** option allows a reader to fallback to the CHUID> FASC-N when the PIV Card does not contain a CAK certificate, but this is not FIPS201 compliant.
12. Click the **Card Read Output** tab.



13. 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:

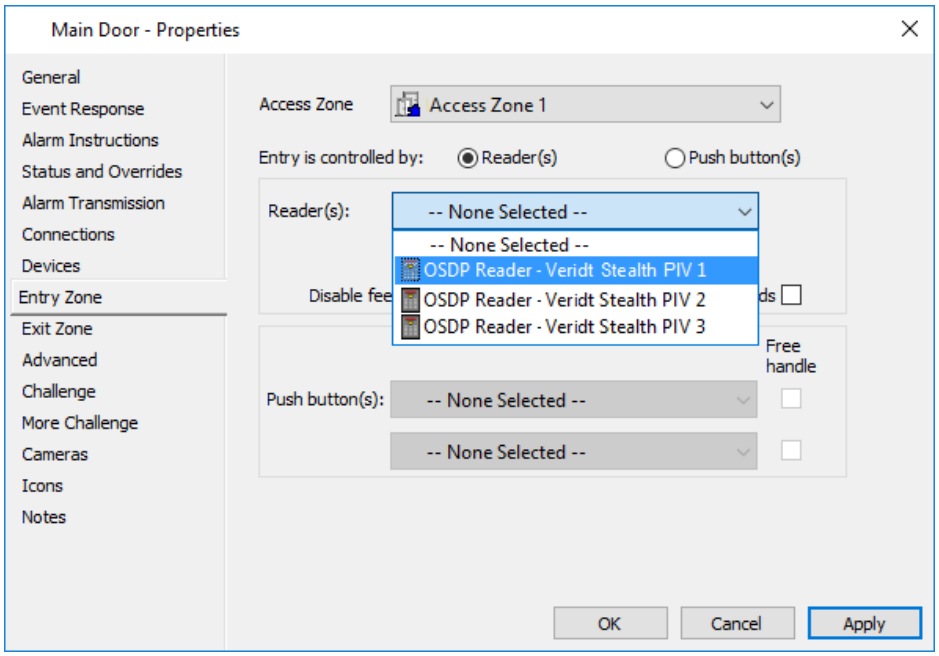
- Badging a card at this reader will switch on the associated relay. The relay will then be immediately switched off unless the relay output is configured to pulse, in which case the relay will stay on for the pulse time and then be switched off. The card format does not have to be correct, nor does 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.

14. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this HBUS Contact Card Reader.
    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 HBUS Contact Card Reader.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
16. Click the **Custom Fields** tab if you want to add and assign a custom field value to this reader.
    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 HBUS Contact Card Reader.
    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 the Reader

Once the configuration work is complete, you need to assign the Reader to a Gallagher PIV Controller 6000 and a Door.

19. Assign this reader to a PIV Controller 6000. See ***Assigning an OSDP Veridt Stealth PIV Reader to a Gallagher PIV Controller 6000*** (on page 56-27) for further detail.
20. From the Door List Window, highlight the door you want to assign this reader to.
21. **Right click** and select **Properties**.
22. Click the **Entry Zone** or **Exit Zone** tab as appropriate.
23. Assign the reader to the appropriate Reader Address by selecting it from the relevant **Reader(s)** drop-down list.



23. If the reader is set to dual authentication/escort+visitor or double card override, click the **Advanced** tab and increase the **Second card (for two-card entry) must be swiped within** value above 30 seconds.
24. 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 Veridt Stealth PIV Reader has been configured.
Notes:

- The Veridt Readers capacity displays on the **Status and Overrides** tab. For example, the status message below indicates that the reader supports Biometrics.

  Normal.The reader has Contact Card support. The reader has Biometric support.

- An OSDP HID Reader or non-Veridt Reader assigned to the Veridt Reader FT Item will have the status message *"The OSDP device is not a Veridt Reader"* (on the **Status and Overrides** tab), or it could go offline.

Assigning an OSDP Veridt Stealth PIV Reader to a PIV Controller 6000

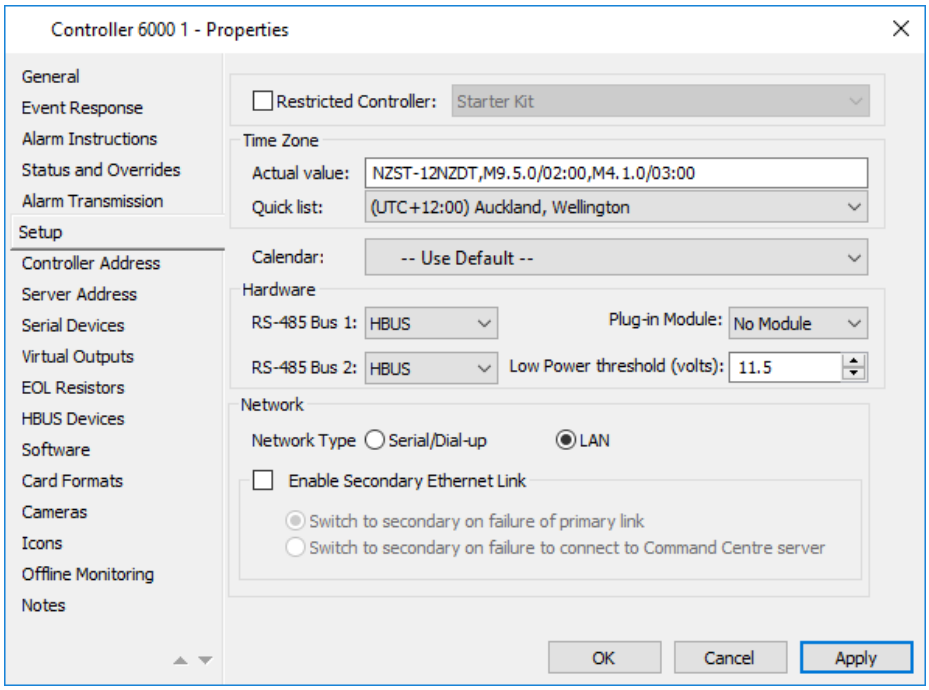
Introduction

This procedure describes how to assign an Open Supervised Device Protocol (OSDP) Veridt Stealth PIV Reader to a Gallagher PIV Controller 6000.

Note: When a Verdit Reader is connected to a non-PIV Controller and a PIV card is presented, a *"PIV Controller required for this transaction type"* event is generated in Command Centre.

Procedure

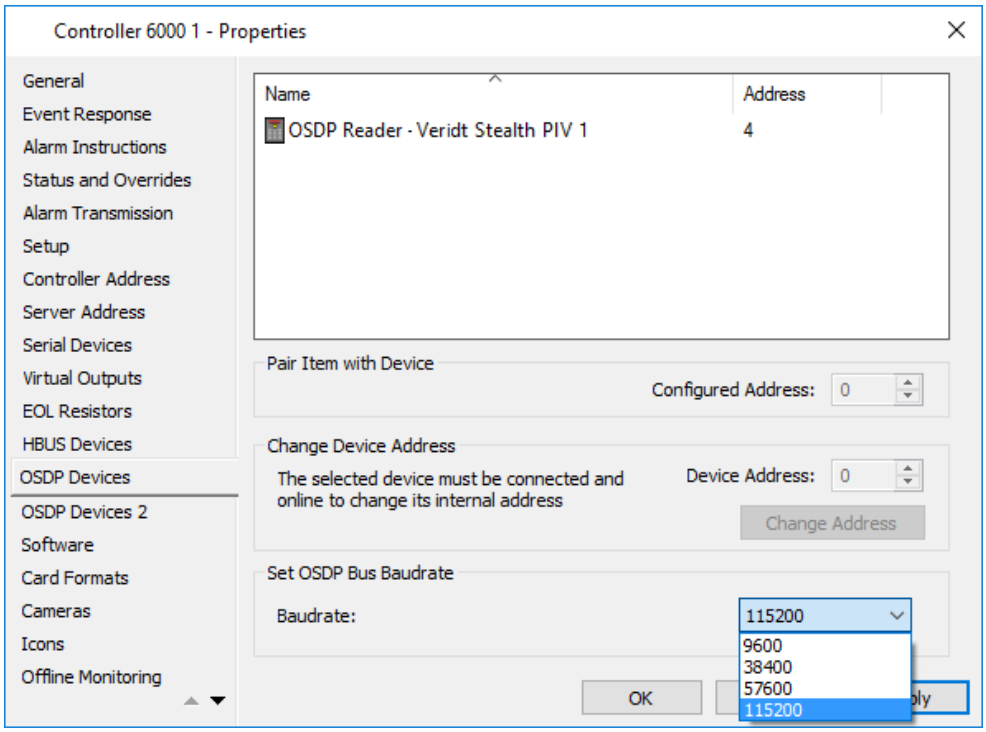
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Controller 6000 you want to assign the new OSDP Veridt Stealth PIV Reader to.
3. **Right click** and select **Properties.**
   By default the **General** tab displays.
4. Click the **Setup** tab.



In the Hardware section of this screen, select the '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 to the Bus port on this Controller.

Note: The recommendation is to use just one OSDP Reader per Bus port.

5. Click the **OSDP Devices** tab.
6. From the **Hardware** List Window, select the OSDP Veridt Stealth PIV Reader(s) attached to this Bus. Drag and drop each reader into the grid on the **OSDP Devices** tab.



7. 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)
8. 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)
   Notes:
   - Address 1 can be used, but it will reset the baudrate when power cycled. Therefore, we specify not to use Address 1.
   - The Change Device Address controls will be disabled if the selected device's status is offline, unknown or unconfigured.
9. 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. When reader baudrate is different to Controller OSDP baudrate, the reader will remain offline.

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 Veridt Stealth PIV Reader has been created and it has been assigned to a Gallagher PIV Controller 6000. As a result, the following occurs:

- the OSDP Veridt Stealth PIV Reader will display within the Hardware List Window.
- on the **Connections** tab of the OSDP Veridt Stealth PIV Reader, the Gallagher PIV Controller 6000 name will appear in the **Connected to** field.

Supporting custom OCSP URLs for PIV certificate validation

Introduction

This procedure describes how to support custom OCSP URLs for PIV certificate validation. This may be useful in the following scenarios:

- Specify OCSP download locations for certificates issued without an OCSP URL in the authority information access.
  If an organisation has previously deployed many certificates that did not include an OCSP URL, they can designate an OCSP download location instead of re-configuring the CA and reissuing all affected certificates.
- Override existing OCSP URLs in the authority information access with new locations.
  If an organisation has deployed internal OCSP URLs in their certificates and now wishes to use the certificates on the external network, the authority information access OCSP URLs must be updated with externally available URLs. Like specifying OCSP download locations for certificates without an OCSP URL, you can designate an externally available URL by using Group Policy or the Certificate Management Console.
- Use internal OCSP responder when firewall policies prevent network retrieval for revocation checking.
  Some networks do not enable connectivity to external networks. If a certificate was issued by an external provider, the lack of connectivity to external networks will prevent successful revocation checking. The clients can be redirected to an internally accessible OCSP URL for certificates issued by the external provider. Again, Group Policy or the Certificate Management Console can be used to designate the internally accessible URL for OCSP revocation checking.

Procedure

The procedure below describes designating custom OCSP URLs on a Windows Server 2008 operating system:

1. Log on to a Domain Controller running Windows Server 2008 (or a computer running Windows Server 2008 with the Group Policy Management feature enabled) with a user account that can edit the certificate properties.
2. From the **Start** menu, click **Administrative Tools** > **Group Policy Management Editor**.
3. In the Console tree, expand **Forest:ForestName**, then expand **Domains**, and click **Domain**.
4. In the **Details** pane, right-click on **Default Domain Policy** and click **Edit**.
   Note: You can choose to implement the OCSP responder settings in any GPO.
5. In the **Group Policy Management Editor**, in the console tree, expand

Default Domain Policy, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings** and then expand **Public Key Policies**.

If you are adding a...	then...
Root CA certificate,	right-click **Trusted Root Certification Authorities**, and then click **Import**.
subordinate CA certificate,	right-click **Intermediate Certification Authorities**, and then click **Import**.

6. In the Certificate Import Wizard, click the **Next** button.
7. On the 'File to Import' page, in the **File name** field, type the full path of the new root or subordinate CA certificate, and then click the **Next** button.
8. On the 'Certificate Store' page, click the **Next** button.
9. On the 'Completing the Certificate Import Wizard' page, click the **Finish** button.
10. In the **Certificate Import Wizard** message box, click the **OK** button.
11. In the **Details** pane, right-click the newly imported certificate, and then click **Properties**. The CAName Properties dialog displays.
12. Click the **OCSP** tab, and define the appropriate options.
    You can either: 1) Disable CRLs, or 2) Add a custom OCSP responder URL.
13. Click the **OK** button after adding your custom OCSP URLs.
14. Close the **Group Policy Management Editor**, and then close the **Group Policy Management console**.

Notes

- Designating custom OCSP URLs is per Certificate Authority (CA) based. This means you need to get the CA certificate and import it into the Windows Intermediate Certificate Authorities store. This won't be a problem in most cases because the CA certificate should be publicly available (either from the issuer or through the URL specified in the AIA extension of a PIV card certificate).
- If the custom OCSP responder goes offline, CryptoAPI will use the OCSP URL of the AIA extension for revocation checking. If there is no OCSP URL in the AIA extension or the OCSP responder is also offline, CryptoAPI will fallback to use the CRL URL of the CRL Distribution Points (CDP) extension.

References

- Managing OCSP Settings with Group Policy. The link: ***http://technet.microsoft.com/en-us/library/ee619786(v=ws.10).aspx***
- Support for Independent OCSP Signer and Custom OCSP URLs. The link: ***http://technet.microsoft.com/en-us/library/ee619784(v=ws.10).aspx***

Enrolling PIV and PIV-I cards using a pivCLASS Workstation

Introduction

PIV and PIV-I cards can be enrolled into Command Centre via either:

- **Command Centre Client** (the preferred method)
  Refer to the ***PIV Cardholder Registration Process*** (on page 3-175) in the *Gallagher Command Centre Client User Guide* for details of this method

  OR

- **a pivCLASS Workstation** (covered in this topic)

  pivCLASS provides cardholder and card data to Command Centre via the XML import. This data is required to be held in Command Centre to facilitate credential authentication.

  Note: In a multi-server system, enrolment of a PIV Cardholder (and associated PIV Card) need only occur at one server. All PIV cardholder details (including card details) will be replicated to all servers in a multi-server environment.

Before you begin

Before you begin enrolling PIV and PIV-I cards ensure:

- the pivCLASS PACS Plug-in has been installed on the Command Centre Server.
  See ***Installing pivCLASS PACS Plug-in*** (on page 56-4) for the procedure.
- pivCLASS Workstation has been installed on the workstation (either server or remote).
  See ***Installing pivCLASS Workstation*** (on page 56-5) for the procedure.

Procedure

1. Enrol this card in the pivCLASS Workstation.
   Refer to "Chapter 7: Identity Verification" of the *pivCLASS Registration Workstation Use Manual* (**pivCLASS_Registration_Workstation_User_Manual.pdf** provided with the Gallagher Command Centre installation files), for a detailed procedure.
   The cardholder is registered with pivCLASS and also created in Command Centre.
   Additional credential and path validation is run from Command Centre upon import to ensure the validity of PIV card certificates. Any revoked, expired or not trusted cards are disabled and events/alarms are generated.
2. Configure the cardholders access.
   Note: If a cardholder is enrolled for a PIV card it will appear as 'read-only' on the **Cards** tab of their properties (in Configuration Client), or on the 'Cardholder Cards Tile' (in Command Centre Client). All fields will be pre-populated.

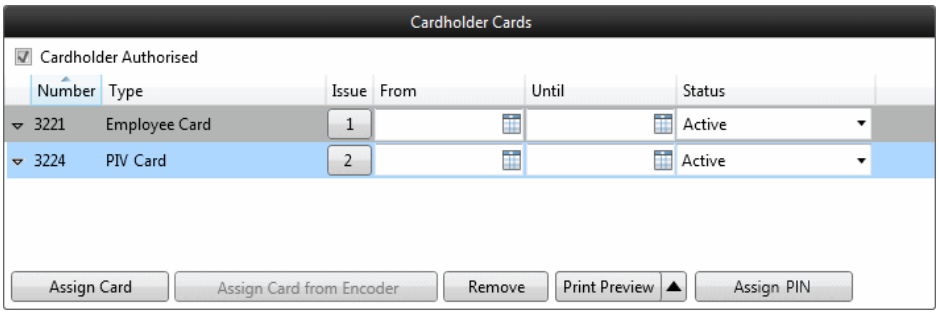
PIV cards in Command Centre

There are a number of differences between PIV cards and other card types, and how they appear in either of the Command Centre clients, (i.e. Configuration Client and Command Centre Client).

When PIV card types appear on the 'Cardholder Cards Tile' in Command Centre Client, or on the **Cards** tab of a Cardholders properties in Configuration Client, it is important to be aware of the following differences with other card types:

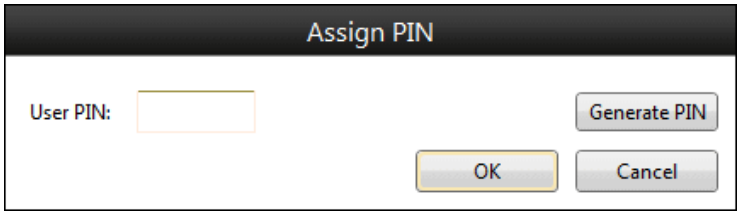
- The **Issue** Level is "read-only" for PIV cards.
- Activation (**From**) and Expiry (**Until**) Dates/Times are not enabled, as they are read directly from the PIV card itself during enrolment and registration.
  Note: The **Until** Time is Midnight UTC and will show as the local workstation time, (i.e. New Zealand will be 12:00).
- When assigning a card to a cardholder, the PIV Card Type does not appear in the **Card Type** drop-down list, as PIV cards cannot be manually assigned.
- None of the encoding options are enabled for PIV cards.
- When the Validation server is unable to be contacted, the cardholder card status shows as 'Certificate status unknown', (i.e. in the **Status** column in the Command Centre Client, or to the right of the **Card Enabled** checkbox in the Configuration Client). PIV cards with this status remain in an 'active' state and can still be used to gain access where appropriate.
- In Command Centre Client, the **Last Validation Time** column only appears if a cardholder has at least one PIV card, and will be populated with the last successful time that the active PIV card certificates have been validated.
- In Command Centre Client, a random or user generated PIN number can be securely hashed and stored in the database for each PIV card record.
  Note: The PIV card will not be read at the time of setting the PIN.

  For any selected PIV card that an operator has the privilege to edit, and has been configured to 'Use PINs' (in Configuration Client), the Cardholder Cards tile will display an enabled **Assign PIN** button to launch the Assign PIN window.
  Note: When the operator only has the privilege to view the card, the **Assign PIN** button will be disabled.



Assigning PINs

1. Click the **Assign PIN** button.
   The Assign PIN pop-up displays.



2. Either:
   - Manually type a PIN number into the first **User PIN** field, and then confirm it by repeating it in the second **User PIN** field, OR
   - Click the **Generate PIN** button to automatically generate a random PIN.
     Note: Generated PINs will only display while the Assign PIN window is open. Once closed, there will be no way of re-viewing the PIN number since the PIN itself is not stored. Generated PINs will be of length equal to the minimum PIN length set against the PIV Card type.

   Note: The system prevents PINs with 3 consecutive or 3 repeating numbers from being either manually entered or automatically generated.
3. Click the **OK** button.
   The Assign PIN pop-up closes.
4. Click the **Save** button.

Searching for PIV cards in Command Centre Client

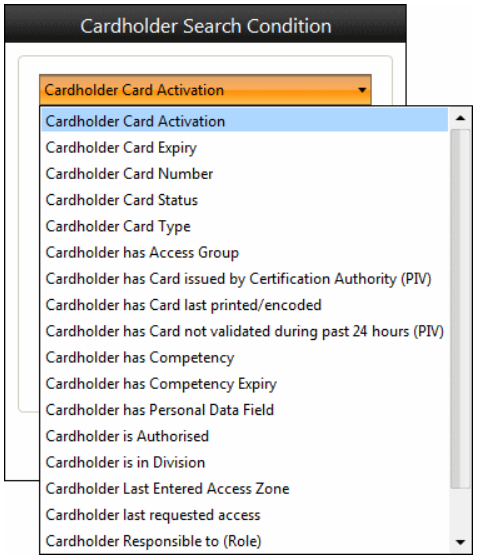
Simple Searching

When performing a simple search for a PIV card, by card number, the numbers entered in the **Search** field must match the Federal Agency Smart Credential Number (FASC-N) PIV card format, including the dashes, (i.e. 4-4-6 digits. With the first 4 digits being the Agency code, the next four digits the System code and the last six digits the Credential number).
For example, if there was a PIV card number 1234-5678-987654, and 123456* was entered in the **Search** field, the card would not be found. However, if 1234-56* was entered, it would appear in the search results.

Advanced Searching

When performing an advanced search for PIV cards, there are a number of conditions available to help define your search. When you click the **Insert Condition** button on the 'Advanced Search Rule Definition' pop-up, the following options are available:

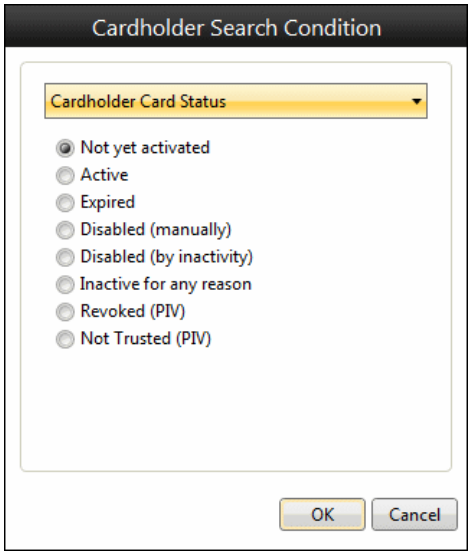
- From the Condition Type drop-down list you can select either **Cardholder has Card issued by Certification Authority (PIV)** or **Cardholder has Card not validated during past 24 hours (PIV)**.



The **Cardholder has Card issued by Certification Authority (PIV)** option can:
- find all cardholders that have PIV cards issued by a particular Certification Authority.
- combine with a revoked search to find all revoked cards for a particular Certification Authority.
- combine with other search filter criteria to find a subset of cards issued by a particular Certification Authority.

The **Cardholder has Card not validated during past 24 hours (PIV)** option returns cardholder records that have PIV cards that have failed to have all certificates validated in the past 24 hours, due to an inability of Command Centre to contact the Validation Authority.
Note: Newly created cardholder records will not be returned until a minimum 24 hours after enrolment.

- By selecting the Condition Type "Cardholder Card Status" from the drop-down list, you can search for PIV cards of either a **Revoked** or **Not Trusted** status.



Chapter 57: Active Directory Single Sign-on

Introduction

Active Directory Single Sign-on is a licensable feature, i.e. your licence file must contain the option:

```
[Features]
ADSingleSignOn=1
```

Single Sign-on refers to the ability to use a Windows User Name and Password for logging onto one or more applications. Command Centre supports the ability for the system to automatically log an operator onto Command Centre using their Windows logon and password, when it is launched.

Note: If Single Sign-on doesn't work after enabling the SSO, it is most probably an issue within the registration of SPN. If manual registration does not work, (i.e. the commands do not work accordingly to register the SPN), the following link to the Gallagher Security Hub describes the minimum required privilege an account requires to register SPN:
(**Note:** An account is required to access the Security Hub, so register if needed.)
https://resources.security.gallagher.com/Site_Troubleshooting/Active_Directory_Integration/Active_Directory_Single_Sign-On/Active_Directory_Single_Sign-On_-_Troubleshooting

Another link which may be useful describes the Delegating Authority to modify SPNs:
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731241(v=ws.11)

Benefits of an Active Directory integration

- A reduction in the number of user names and passwords people have to remember.
- It allows sites to take advantage of Windows logon management for the purpose of logging onto Command Centre. Windows allows for the specification of more complex rules for passwords (than is currently available for Command Centre) and to require a combination of authentication methods including biometrics.
- The ability to prevent people from logging on to other applications by disabling their account in a central place, (i.e. Active Directory).
- The following Gallagher clients and applications can be logged onto using a Windows account:
  - Command Centre Client (automatic logon using the logged-on Windows account)
  - Configuration Client (automatic logon using the logged-on Windows account)

- Visitor Management Kiosk
- Command Centre Mobile (manually enter a Windows username and password)
- Web Client (manually enter a Windows username and password

This chapter covers the following topics:

- ***Configuring Single Sign-on and Automatic logon*** (on page 57-2)
- ***Linking operators to their Active Directory account*** (on page 57-3)

Configuring Single Sign-on and Automatic logon

The following configuration is required in order for an operator to be logged on automatically using their Active Directory user name and password:

- The server connected to the workstation they are launching the application from has to be enabled for Active Directory Single Sign-on. Refer to Operator Defaults for the procedure.
- The operator's Cardholder record needs to be configured with their Windows logon.
  Refer to ***Linking operators to their Active Directory account*** (on page 57-3) for the procedure.

Notes:

- Where the server, workstation and Windows user are in different domains, trust relationships need to be established between these domains in order for single sign-on to work. The trust relationship type must be Forest, not External. This is the responsibility of the company's IS department.
- There is an issue if the Command Centre service has been changed to logon using a different account from the default of local system. Technical Document 13778 has details on this procedure. This is available by logging into the Gallagher Security support site and navigating to **Technical Documents**. Alternatively, you can contact Gallagher Technical Support for assistance.

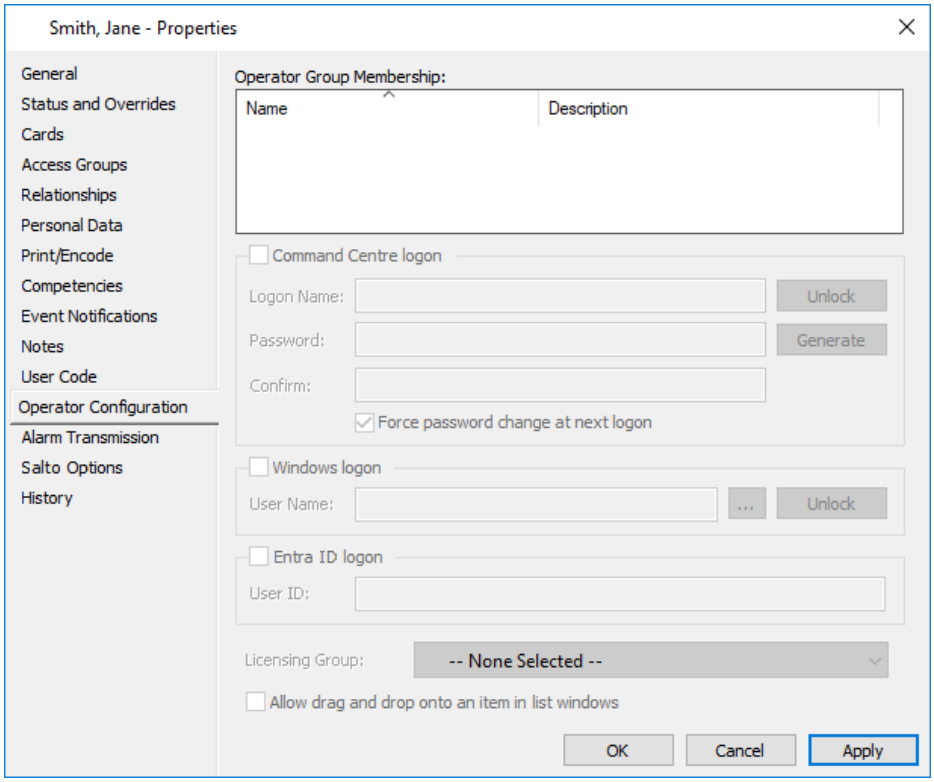
Linking operators to their Active Directory account

Introduction

In order for an operator to log onto the system using single sign-on (using their Active Directory user name and password), their Cardholder records need to be configured with their Windows logon.
See Active Directory Single Sign-on for further detail about this feature.

Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the Cardholder you want to configure their Windows logon for.
3. Right click and select **Properties**.
4. Click the **Operator Configuration** tab.

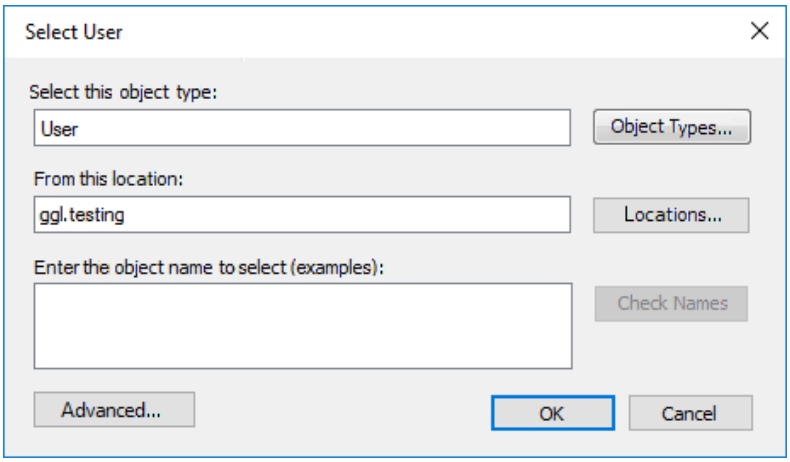


Note: If the server to which the workstation connects is enabled for Active Directory Single Sign-on, this tab will display as shown (when the cardholder is not in an Operator Group).

If the Cardholder was an Operator BEFORE the server was enabled for Active Directory Single Sign-on they will already have a Command Centre logon, so the **Command Centre Logon** checkbox will be checked and their logon name will appear in the **Logon Name** field.

If the Cardholder is made an Operator (by assigning them Operator Groups) AFTER the server is enabled for Active Directory Single Sign-on, the **Command Centre Logon** checkbox will be enabled but unchecked, and the **Logon Name** field will be blank and disabled.

5. Check the **Windows Logon** checkbox.
   The **User Name** field and Browse ... button become enabled.
6. If the **User Name** field is empty, it needs to be populated with the domain name, (e.g. "Gallagher.Local").
   Do this by either:
   - typing the user name or pasting it into the **User Name** field, or
   - clicking the ... button to browse to the Active Directory for a Windows user name.
     The Select User dialog displays:



   Note: Choosing the user name by browsing will overwrite any content in the **User Name** field.
7. Click the **Object Types** button to select the appropriate object type.
8. Click the **Locations** button to select the domain.
9. Click the **OK** button.
   The Select User dialog closes.
10. If the Cardholder is not already an Operator, (i.e. the Operator Group grid is blank), open the **Operator Group** List Window and drag and drop the required Operator Groups into the grid.
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.

Chapter 58: Austco Intercoms

Austco Intercoms is a licensable feature, i.e. your license file must contain the following options:

```
[Features]
AustcoIntercom=1
[Limits]
Austco Intercom Systems=n
Austco Intercom=nn
```

The Austco Intercom System item (located in the **External Systems** List Window) allows the Austco Intercom System to be integrated with Gallagher Command Centre.

At the time your site installed Command Centre, the 'Intercom Server' option should have been checked under the Server components. If it was not, you will need to re-install Command Centre (remembering to check the 'Intercom Server' option), before using the Intercom Systems feature.

The integration between the two systems provides support for:

- Notifying a Command Centre operator when a call request is received.
- Answering an intercom call from a Command Centre workstation.
- Making an intercom call from a Command Centre workstation.
- Managing a queue of waiting calls from a Command Centre workstation.
- Allowing an operator to open a Command Centre door in response to an intercom call.
- Logging events and alarms from the Austco Intercom System into the Command Centre activity log.
- Monitoring the status of an intercom.

Notes:

- The integration between the two systems does not allow for recording an intercom call, or integrating an intercom's general purpose I/O into Command Centre.
- The time settings on the server and workstations must be synchronised. Any time difference between the server and workstation will result in the amount of time difference to be added or subtracted from the displayed "Seconds Remaining" in the Austco Intercom Viewer.
- Do not generate alarms from intercom call events.

Austco components

This integration is intended for use with Austco sites where their ACM configuration file has been modified by Austco to include sending ACMIP messages to an external device, such as "(_1_1 CONNECT _AC-H1-1), and (_1_1 DISCONNECT _AC-H1-1)". Please contact Austco to ask for the modifications needed for use with Command Centre. You will then be required to transfer new node files to your Austco nodes. Without these modifications, this integration will not work correctly.

Note: The message-interface SYMBOL is hard coded in the Gallagher system as "_ED-1". This may cause problems when a site is installing an Austco intercom system, (i.e. the intercom service may not start, and the Austco intercom may not connect to Command Centre if the Austco server is not left in it's default SYMBOL configuration).

This integration has been tested using the following Austco software and hardware:

Software	Hardware
ACM-CS v3.1-b7	2 x CI-CC Austco Intercom
FSS Kernel ACM-CS v4.5.7-b2	1 x CI-8A Austco Intercom Controller
ACM v0.7	1 x CI-3210 Staff Station
Site Configuration v4.0.20.1	
Site Management Console v 2.4.11	

Austco Intercom icons

The Austco Intercom icon (which can appear on the Status Viewer and Site Plans) has three states, as follows:

When an intercom is...	then the icon is in the...
idle,	 Normal Operation state, and on a Site Plan the line/area colour is Black.
ringing,	 Call ringing state, and on a Site Plan the line/area colour is Red.
connected on a call,	 Call connected state, and on a Site Plan the line/area colour is Green.

Configuring Austco Intercoms

To configure Austco Intercoms, perform the following procedures in the Configuration Client:

- ***Configuring an Austco Intercom System*** (on page 58-3)
- ***Configuring an Austco Intercom Item*** (on page 58-4)
- ***Assigning an Austco Console to a Workstation*** (on page 58-5)
- ***Locating an Austco Symbol*** (on page 58-6)

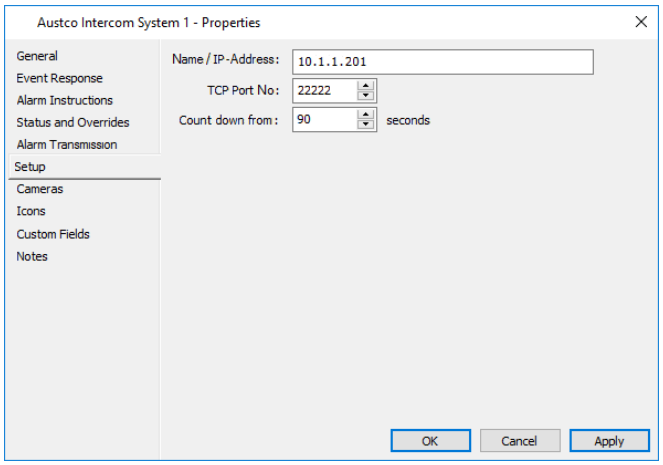
Configuring an Austco Intercom System

Introduction

This procedure describes how to configure an Austco Intercom System.

Procedure

1. Click **Configure** from the menu bar, then **External Systems**.
2. Right click and select **New...Austco Intercom System**.
3. Type in the Name, Description and select the Division.
4. Click the **Event Response** tab and assign a primary Alarm Zone for all events.
5. Click the **Setup** tab.



6. Enter the Austco Intercom server PC's IP Address in the **Name/IP Address** field. This field is limited to 255 alpha-numeric characters.
7. Enter the Austco Intercom server PC's TCP Port Number in the **TCP Port No.** field. This field must be between 1 - 65535.
8. Enter the count down time period (in seconds) in the **Count down from** field. This is the period of time whereby an operator is required to select the **Connect** button.

   This field must be between 1 - 600. Default is 90 seconds.
   Note: A value of zero means an unanswered call will not timeout.
9. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Intercom System. 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 Austco Intercom System. For further details 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 Intercom System. 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 Austco Intercom System. For further details 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.

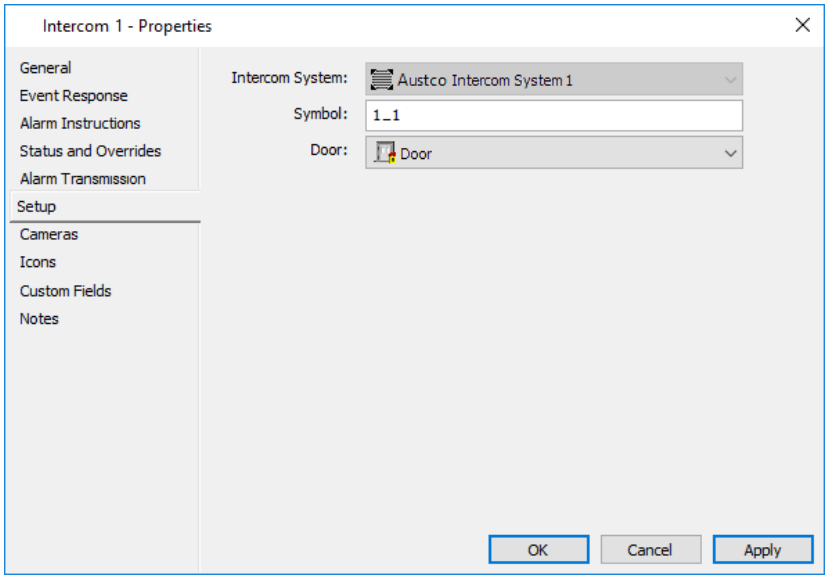
Configuring an Austco Intercom Item

Introduction

This procedure describes how to configure an Austco Intercom Item.

Procedure

1. Click **Configure** from the menu bar, then **External Systems**.
2. Right click and select **New...Austco Intercom**.
3. Type in the Name, Description and select the Division.
4. Click the **Setup** tab.



5. Select the Intercom System from the **Intercom System** drop-down list.
6. Enter the intercom symbol as shown in the Austco Site Configuration application into the **Symbol** field. See ***Locating an Austco Symbol*** (on page 58-6) for further detail. Maximum of 64 characters.

   Note: The intercom symbol is checked for uniqueness within the same Intercom System.
7. Select the appropriate Door from the **Door** drop-down list. This should be the door corresponding to this intercom.
8. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Intercom Item. For further details see ***Cameras tab*** (on page 3-24).
9. Click the **Icons** tab if you want to change the Icon Set for this Austco Intercom Item. 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 Austco Intercom Item. 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 Austco Intercom Item. For further details see ***Notes*** (on page 6-85).
12. 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 Austco Console to a Workstation

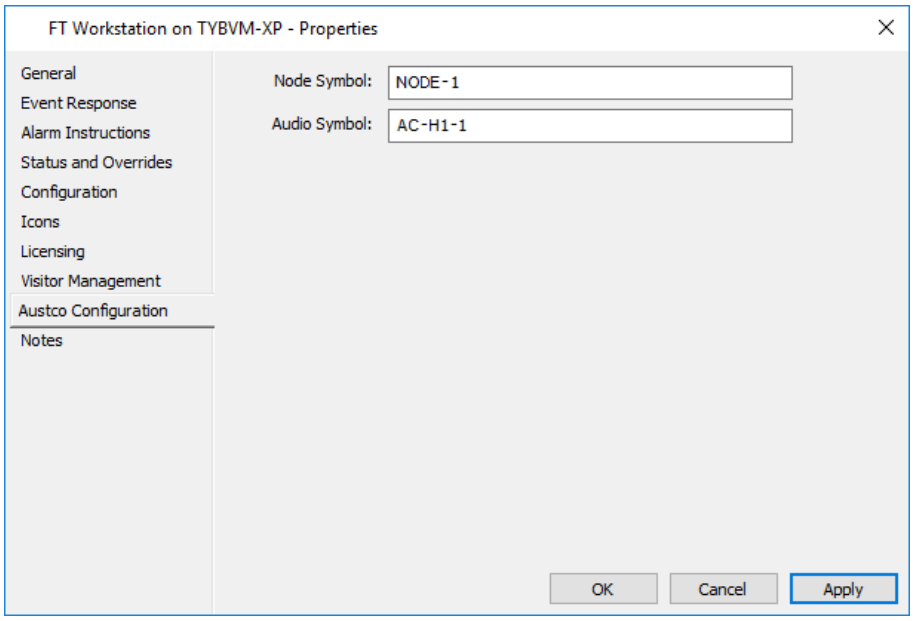
Introduction

The Austco Console must be located near the Command Centre workstation. If an operator responds to an intercom call event via the workstation, the call event will be removed from all other operator workstations.

Perform the following procedure to assign an Austco Console to a Command Centre workstation.

Procedure

1. Click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens.
2. Open the workstation you want to assign the Austco Console to.
3. Click the **Austco Configuration** tab.



4. Enter the Austco Console Node Symbol in the **Node Symbol** field. See ***Locating an Austco Symbol*** (on page 58-6) for further detail. (Maximum of 64 characters.)
   Note: The **Node Symbol** is case sensitive.
5. Enter the Austco Console Audio Symbol in the **Audio Symbol** field. See ***Locating an Austco Symbol*** (on page 58-6) for further detail. (Maximum of 64 characters.)
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.

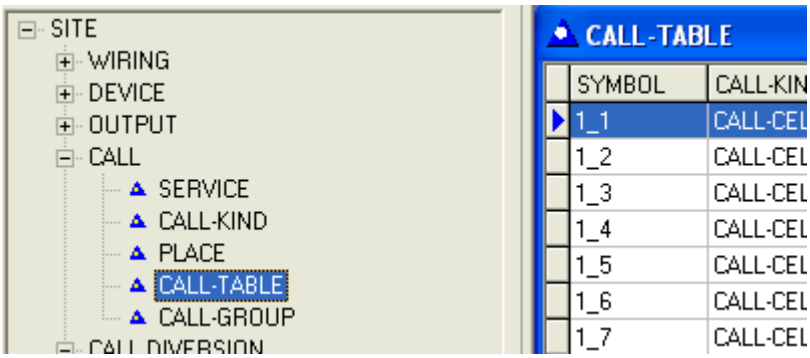
Locating an Austco Symbol

Introduction

This topic describes how to locate a Symbol (item identifier) in the Austco Site Configuration application.
Note: The linking between Node Symbols and Audio Symbols should be configured by an Austco Installer.

Procedure

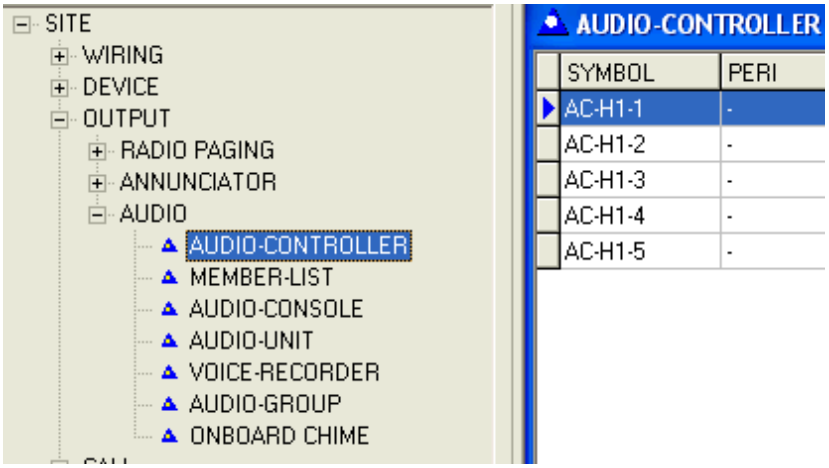
1. Open the Austco Site Configuration application.
2. Open your Site Configuration.
3. In the Navigation Panel, located on the left hand side, select **SITE** > **CALL** > **CALL-TABLE**.
   The CALL_TABLE table displays. This table lists the **Symbol** configured against the Austco Intercom Item in Command Centre.



4. In the Navigation Panel, select **SITE** > **WIRING** > **NODE**.
   The NODE table displays. This table lists the **Node Symbol** configured against the Workstation item in Command Centre.



5. In the Navigation Panel, select **SITE** > **OUTPUT** > **AUDIO** > **AUDIO-CONTROLLER**.
   The AUDIO-CONTROLLER table displays. This table lists the **Audio Symbol** configured against the Workstation item in Command Centre.


SITE
WIRING
DEVICE
OUTPUT
RADIO PAGING
ANNUNCIATOR
AUDIO
AUDIO-CONTROLLER
MEMBER-LIST
AUDIO-CONSOLE
AUDIO-UNIT
VOICE-RECORDER
AUDIO-GROUP
ONBOARD CHIME
AUDIO-CONTROLLER
SYMBOL
PERI
AC-H1-1
AC-H1-2
AC-H1-3
AC-H1-4
AC-H1-5

Chapter 59: Jacques Intercoms

Jacques Intercoms is a licensable feature, i.e. your license file must contain the following option:

```
[Features]
JacquesIntercom=1
```

The Intercom System item (located in the **External Systems** List Window) allows the Jacques IP Intercom System to be integrated with Gallagher Command Centre.

At the time your site installed Command Centre, the 'Intercom Server' option should have been checked under the Server components. If it was not, you will need to re-install Command Centre (remembering to check the 'Intercom Server' option), before using the Intercom Systems feature.

The integration between the two systems provides support for:

- Notifying a Command Centre operator when a call request is received.
- Answering an Intercom call on a Jacques Intercom connected to a Gallagher Command Centre workstation.
- Making an Intercom call from a Gallagher Command Centre workstation connected to a Jacques Intercom.
- Placing a call on hold from a Gallagher Command Centre workstation.
- Forwarding an Intercom call to another Intercom from a Gallagher Command Centre workstation.
- Monitor (listen to) an intercom from a Gallagher Command Centre workstation (only available in Command Centre Client).
- Managing a queue of waiting calls from a Gallagher Command Centre workstation.
- Allowing an operator to open a Gallagher Command Centre door in response to an Intercom call.
- Temporarily placing a workstation into "remote mode".
- Logging events and alarms from the Intercom System into the Gallagher Command Centre activity log.
- Monitoring the status of an Intercom.

Notes:

- The integration between the two systems does not allow for recording an Intercom call, or integrating an Intercom's general purpose I/O into Gallagher Command Centre.
- This interface is supported, and has been tested on version 4.64 of the Jacques Intercom software server.
- HLI-VRX is the correct type to use for the Workstation.

Jacques Intercom Icons

The Jacques Intercom icon (which can appear on the Status Viewer and Site Plans) has four states, as follows:

When an intercom is...	then the icon is in the...
idle,	 Normal Operation state, and on a Site Plan the line/area colour is Black.
ringing,	 Call ringing state, and on a Site Plan the line/area colour is Red.
connected on a call,	 Call connected state, and on a Site Plan the line/area colour is Green.
connected for monitoring,	 Monitoring connected state, and on a Site Plan the line/area colour is Blue.
on hold,	 On Hold state, and on a Site Plan the line/area colour is Orange.

Configuring the Jacques Intercom feature in the Configuration Client

To configure the Jacques Intercom feature, perform the following procedures in the Configuration Client:

- ***Configuring a Jacques Intercom System*** (on page 59-3)
- ***Configuring a Jacques Intercom*** (on page 59-5)
- ***Opening the Intercom window*** (on page 59-7)
- ***Placing a call*** (on page 59-10)
- ***Answering a call*** (on page 59-11)

Configuring a Jacques Intercom System

Introduction

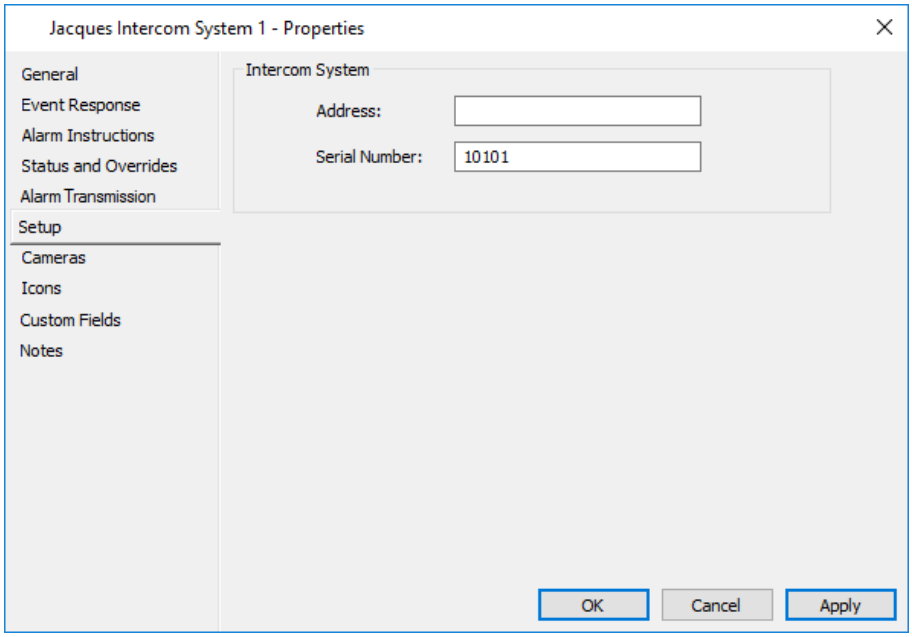
This topic describes how to configure a Jacques Intercom System in Command Centre, allowing the Jacques IP Intercom System to be integrated with Command Centre.

Notes:

- Only one Jacques IP Intercom System can be configured in Command Centre.
- Operators require the "Edit Site" operator privilege to be able to add, modify and delete the Jacques Intercom System.

Procedure

1. Click **Configure** from the menu bar, then **External Systems**.
   The External Systems List Window opens (in tree view).
2. Right click and select **New...Jacques Intercom 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 **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 **Setup** tab.



7. Enter the IP Address in the **Address** field.
   This will be the IP address that workstations use to make the initial connection to the Intercom server.
8. Enter the unique **Serial Number** issued to your site by Jacques.
   Range = 0 to 2147483647

   This Serial Number is usually the **uvalue** of tag '10101' in the **tag_device** table in the Jacques database, located at:
   Jacques > Webcfg > MySQL > Databases > siteconfigDB > tag_device

   If you are unsure, Gallagher recommends asking Jacques for your site's unique serial number.
9. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Intercom System.
   For further details see ***Cameras tab*** (on page 3-24).
10. Click the **Icons** tab if you want to change the Icon Set for the Intercom System.
    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 the Intercom System.
    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 the Intercom System.
    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

The Jacques Intercom System has been created and displays at the root level of the External Systems window, with no children.

To check that the Jacques Intercom System is online, check that it, (e.g. **tag** '10101') displays with a **curstate** of 'online' in the **device_state** table, located at: Jacques > Webcfg > MySQL > Databases > stateDB > device state

Hint

Editing and Deleting Jacques Intercom Systems
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Jacques Intercom Systems.
Notes about deleting the Jacques Intercom System:

- The Jacques Intercom System will only allow deletion if it does not have any children, (i.e. no Jacques Intercoms referencing it).
- If an item is on a Site Plan you will not be able to delete it until it is removed from the Site Plan.

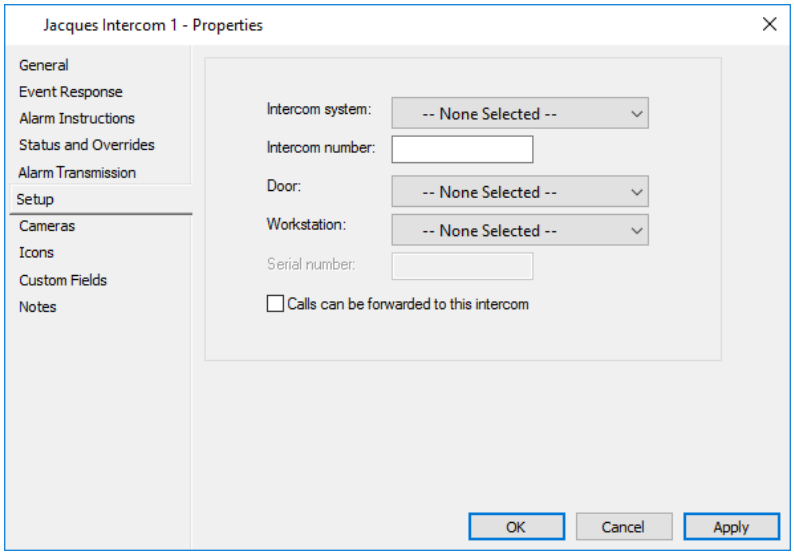
Configuring a Jacques Intercom Item

Introduction

This topic describes how to configure a Jacques Intercom in Command Centre.
Notes: Operators require the "Edit Site" operator privilege to be able to add, modify and delete a Jacques Intercom.

Procedure

1. Click **Configure** from the menu bar, then **External Systems**.
   The External Systems List Window opens (in tree view).
2. Right click and select **New...Jacques Intercom**.
   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. If you do not want to receive tamper alert alarms, click the **Status and Overrides** tab, and check the **Disable Tamper** checkbox.
7. Click the **Setup** tab.



8. Complete the fields on this tab as required.

Field	Description
Intercom system	This specifies which Intercom System this Intercom belongs to.
Intercom number	This is the number that uniquely identifies the Intercom to the Intercom server. Each Intercom belonging to an Intercom System must have a different Intercom number. This number must match the **tag** number of an intercom in the Jacque's database's **tag_device** table, located at: Jacques > Webcfg > MySQL > Databases > siteconfigDB > tag_device

Field	Description
	If this field is left blank or is incorrect it will not be possible to call the Intercom from a Command Centre workstation and Command Centre will not be able to resolve the name and description of the Intercom when a call arrives.
Door	This is the door that can optionally be opened by an operator answering a call from the Intercom. **Note:** A door can be associated with any number of Intercoms.
Workstation	This is the Command Centre workstation the Intercom is associated with. This field should be empty if the Intercom is not associated with a workstation. If assigning a workstation, the 'Calls can be forwarded to this intercom' checkbox is automatically switched on. **Note:** A workstation can only be associated with one Intercom.
Serial number	This number is a string that the Command Centre workstation uses to identify itself to the Intercom server. Only Intercoms connected to workstations need to have a serial number. This serial number must match the **uvalue** of an intercom in the Jacques database's **tag_device** table, located at: Jacques > Webcfg > MySQL > Databases > siteconfigDB > tag_device This field allows 63 alpha/numeric characters. **Note:** This field will remain greyed out if no workstation is selected.
Calls can be forwarded to this intercom	If this checkbox is ticked, this Intercom will be available for selection when forwarding a call.

9. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Intercom. 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 Intercom. 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 the Intercom.
    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 the Intercom.
    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

The new Jacques Intercom has been created and displays as a child of the Jacques Intercom System in the **External Systems** List Window.
To check that a Jacques Intercom is online in the Jacques system, check that the device displays with a **curstate** of 'online' in the **device_state** table, located at:
Jacques > Webcfg > MySQL > Databases > stateDB > device state

Opening the Intercom window

Introduction

Most of the interaction with the Intercom System is through the Intercom window. To utilise the Intercom window you need to have the "Use Intercom" operator privilege.

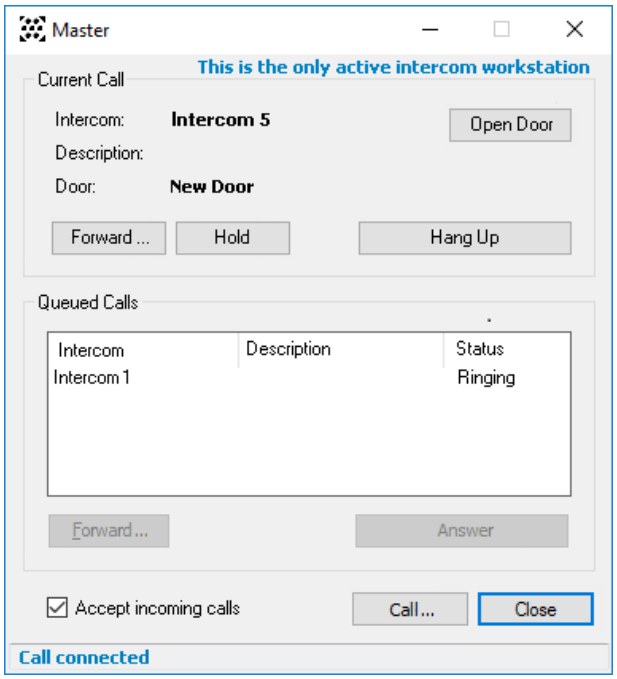
Note: The Intercom window will not show until you have set up an Intercom with a workstation, and then logged off and on again on the configured workstation.

Procedure

1. Click **Monitor** form the menu bar.
2. Click **Intercom Window**.

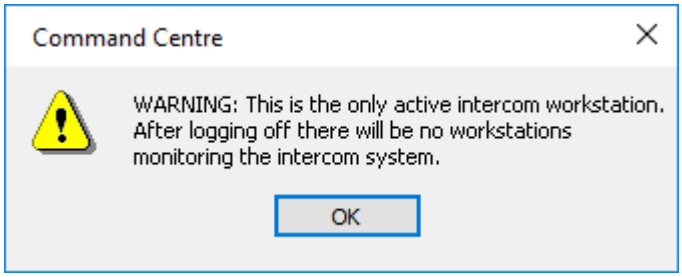
Result

The Intercom window displays for the Intercom that has a workstation assigned to it.



If this is the only workstation running, a message displays directly under the title bar indicating that this is the only active Intercom window. This text flashes between blue and red for 5 seconds, then it remains on the window (in blue) until another workstation comes active.

Should you attempt to shutdown or log off the workstation while this state is active, the following warning message will display:



Current call section

This section of this window contains information about the current call and buttons which operate on the current call. The current call is either the call that is in progress or the first unanswered call if there are no calls in progress.

Field / Button	Description
Intercom	This field displays the name of the Intercom at the other end of the current call.
Description	This field displays the description of the Intercom at the other end of the current call.
Door	This field displays the name of the door associated with the Intercom at the other end of the current call.
Open Door	This button allows you to open the door associated with an Intercom.
Forward ...	This button allows you to forward a call to another Intercom.
Hold	This button places the current call on hold. It is enabled when a call is in progress.
Hang Up	This button disconnects the current call. It is enabled when a call is in progress.

Queued calls section

This section of the window contains a list of queued calls (including the current call which appears at the top of the list), and buttons which operate on queued calls. Note that these buttons apply to the call that is selected in the list, which may not be the current call.

When there are no calls in progress the only options available are to call another Intercom (via the **Call** button) and to set the workstation to remote mode (via the **Accept incoming calls** checkbox).

Button / Checkbox	Description
Forward ...	This button allows you to forward a call to another Intercom.

Button / Checkbox	Description
Answer	This button allows you to answer a selected call only located in the "Queued calls" section. **Note:** Alternatively, double-clicking on a call in the queue enables you to auto-answer it (providing there is no current call or the server is connected, etc.)
Call...	This button allows you to place a call to another Intercom. This option is always available unless the workstation is in remote mode.
Close	This button allows you to close the Intercom window.
Accept incoming calls	This checkbox allows you to put the workstation into remote mode. This option is always available.

Placing a call

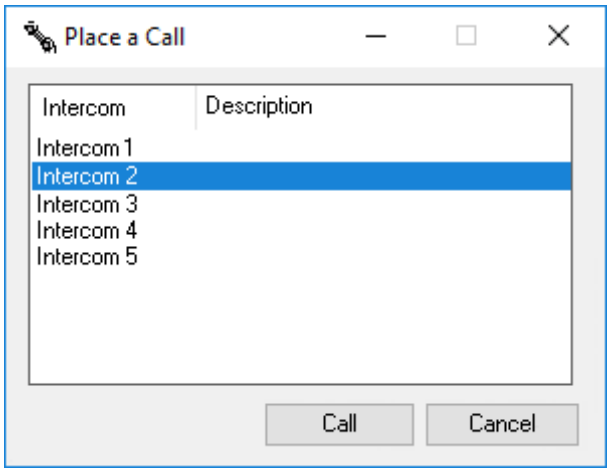
Introduction

An operator can place a call from the Intercom window.
Notes:

- It is also possible to place a call by locating the Intercom on a Site Plan, the Find Tool or from the Intercom Systems list window. Once you locate and highlight the Intercom using any of these methods, right click on it and select **Call**. This starts the call and displays the Intercom window.
- If the call does not open the Intercom window then log off and on again.

Procedure

1. Open the **Intercom** window. ***How?*** (see "***Opening the Intercom window***" on page 59-7)
2. Click the **Call** button.
   The **Place Call** window displays with a list of possible call destinations. The list includes all the Intercoms in the operator's division that belong to the same Intercom System item as the workstation's Intercom.



3. Highlight the Intercom you wish to call and click the **Call** button.

Result

You are returned to the **Intercom** window. The workstation calls the Intercom and the call appears in the "Current call" section.

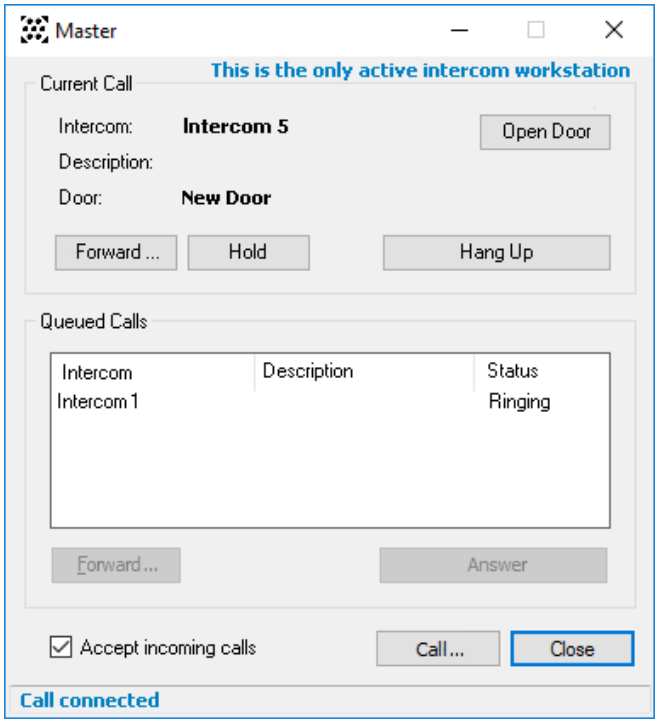
You can now forward, hold, record, open a door or hang up a call.

Answering a call

Introduction

When a workstation receives a call request, the Intercom window pops up if it is not already visible.
Note: This window does not provide an audio prompt when a call arrives.

The Intercom window displays information about the incoming call in the "Queued call" section, (i.e. the name and description of the corresponding Intercom item and its status).



If a call arrives while the operator is handling another call, the new call is added to the end of the call queue.

Procedure

1. Highlight the call.
2. Click the **Answer** button in the "Queued calls" section of the window.
3. Once you have answered a call it moves to the "Current call" section and out of the queued grid. You can now:
   - place the call on hold
   - open the door associated with the Intercom
   - forward a call
   - end a call

   Take the appropriate action as required:

Placing a call on hold

Once you have answered a call, you have the option to place the call on hold at any time.

1. Click the **Hold** button.
   The status of the call changes to "On hold" and the call is moved to the "Queued calls" section.

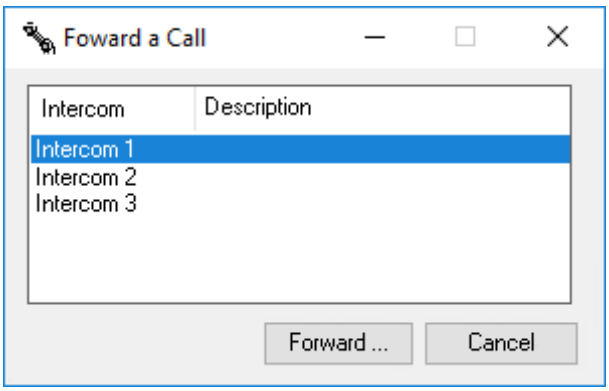
Opening the door associated with an Intercom

1. Click the **Open Door** button.
   The door that is associated with the Intercom opens.
   Notes:
   - If no door is associated the **Open Door** button is disabled.
   - You need the "Door Override" operator privilege to perform this function.

Forwarding a call

A current call or any queued call can be forwarded to another Intercom.

1. From the **Intercom** window, select the call you wish to forward to another Intercom.
2. Click the **Forward** button.
   The **Forward Call** window displays with a list of all the Intercoms in the operator's division that have the "Calls can be forwarded to the intercom" option enabled and belong to the same Intercom System item as the Intercom that initiated the call.



3. Highlight the Intercom you wish to forward the call to, and click the **Forward** button.
   The call is forwarded to the Intercom selected.

Ending a call

Once you have answered a call, you have the option to end the call at any time.

1. Click the **Hang up** button.
   The call is disconnected.

Chapter 60: Commend Intercoms

Commend Intercoms is a licensable feature, so your license file must contain the following option:

```
[Limits]
Commend Intercom Systems=1
Commend Intercom=x
```
(where **x** is the number of intercoms required)

```
[Features]
CommendIntercom=1
```

The Commend Intercom System item (located in the External Systems List Window) allows the Commend Intercom System to be integrated with Gallagher Command Centre.

The integration between the two systems provides support for:

- Notifying a Command Centre operator when a call request is received.
- Answering an intercom call from a Command Centre workstation.
- Making an intercom call from a Command Centre workstation.
- Placing a call on hold from a Command Centre workstation.
- Forwarding an Intercom call to another Intercom from a Gallagher Command Centre workstation.
- Managing a queue of waiting calls from a Gallagher Command Centre workstation.
- Allowing an operator to open a Command Centre door in response to an intercom call.
- Logging events and alarms from the Commend Intercom System into the Command Centre activity log.
- Monitoring the status of an intercom.

Notes:

- The integration between the two systems does not allow for recording an intercom call, or integrating an intercom's general purpose I/O into Command Centre.
- The time settings on the server and workstations must be synchronised. Any time difference between the server and workstation will result in the amount of time difference to be added or subtracted from the displayed "Seconds Remaining" in the Commend Intercom Viewer.
- Do not generate alarms from intercom call events.
- This integration does not support video intercom calls.

Commend Components

This integration has been tested using the following Commend software and hardware:

Software	Commend Native Hardware
Commend Server: VirtuoSIS (GE300 and GE800 are compatible) Minimum firmware version PRO800 5.0	• Master: EE900A and Commend Intercom Client • Cell station: 100094-3 • Door station: 100094-2 **Note:** Commend advises that all IoIP (Intercom over IP) devices produced by Commend should function with this integration. For further information please contact Commend. **Third Party SIP Hardware** • SIP Server: Grandstream • SIP Video Phone: T-CCS-SIP-MS1-W • SIP Video Door Intercom: T-CCS-SIP-DSV1 **Note:** Commend advises that not all SIP intercoms will function with this integration. Gallagher recommends that you contact Commend to understand if your intercoms are compatible.

Commend Intercom icons

The Commend Intercom icon (which can appear on the Status Viewer and Site Plans) has seven states, as follows:

When an intercom is...	the icon is in the...
idle,	 and on a Site Plan/Area the colour is black.
ringing in,	 and on a Site Plan/Area the colour is red.
ringing out,	 and on a Site Plan/Area the colour is orange.
connected (on a call),	 and on a Site Plan/Area the colour is green.
paused (on hold),	 and on a Site Plan/Area the colour is yellow.
forwarding,	 and on a Site Plan/Area the colour is purple.
busy,	 and on a Site Plan/Area the colour is blue.

The Commend Intercom system icon (which can appear on the Status Viewer and Site Plans) is . It only has one state.

Configuring Commend Intercoms

To configure Commend Intercoms, perform the following procedures in the Command Centre Configuration Client:

Configuring a Commend Intercom System (on page 60-4)

Configuring a Commend Intercom Item (on page 60-6)

Assigning a Commend Console to a Workstation (on page 60-8)

Using Commend Intercoms (on page 60-9)

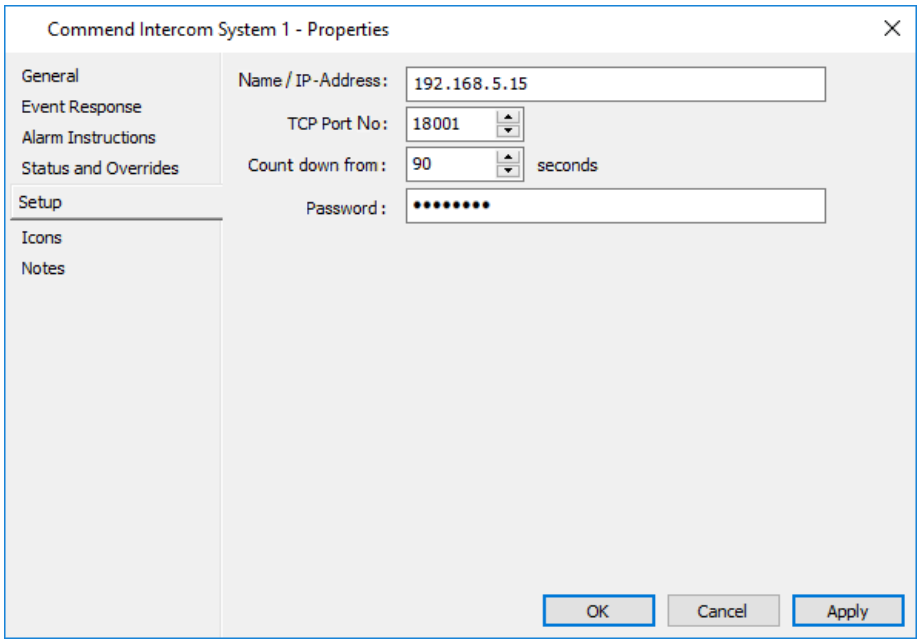
Configuring a Commend Intercom System

Introduction

This procedure describes how to configure a Commend Intercom System. Only one Commend Intercom System can be installed per Command Centre Server.

Procedure

1. Click **Configure** from the menu bar, then **External Systems**.
   The External Systems List Window opens (in tree view).
2. Right click and select **New...Commend Intercom System**.
   By default the **General** tab displays.
3. Type in the Name and select the Division. The **Description** field is populated and updated automatically from the Commend Intercom server.
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 **Setup** tab.



6. Enter the Commend Intercom ICX interface's PC's IP Address in the **Name/IP-Address** field.
   This field is limited to 255 alpha-numeric characters. The IP Address will be provided by your Commend Intercom installer.
7. Enter the Commend Intercom ICX interface's Local Port Number in the **TCP Port No.** field.
   This field must be between 1 and 65535. The Port Number will be provided by your Commend Intercom installer.

8. Enter the count down time period (in seconds) in the **Count down from** field.
   This is the period of time whereby an operator is required to select the **Answer** button, and must be between 0 and 600. Default is 90 seconds.
   Note: A value of zero means an unanswered call will not timeout.
9. Enter a password into the **Password** field if you have been provided one from your Commend Intercom installer. Otherwise, leave blank.
10. Click the **Icons** tab if you want to change the Icon Set for the Intercom System.
    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 the Intercom System.
    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 the Intercom System.
    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

The Commend Intercom System has been created and displays at the root level of the External Systems window, with no children.

Configuring a Commend Intercom Item

Introduction

This procedure describes how to configure a Commend Intercom Item. The maximum number of Intercoms you can install per Commend Intercom System is defined in your licence file:

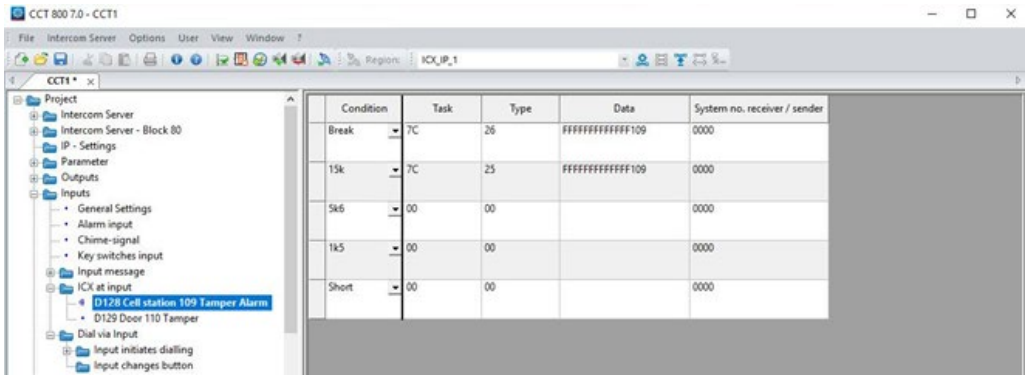
```
[Limits]
Commend Intercom=x
```
(where **x** is the number of intercoms required)

Monitor Tamper Alarm (optional)

If you want to monitor the intercom's tamper alarm, your Commend technician will need to configure this in the Commend software before configuring the intercom item. This is optional.

Complete the following fields as appropriate in the Commend software:

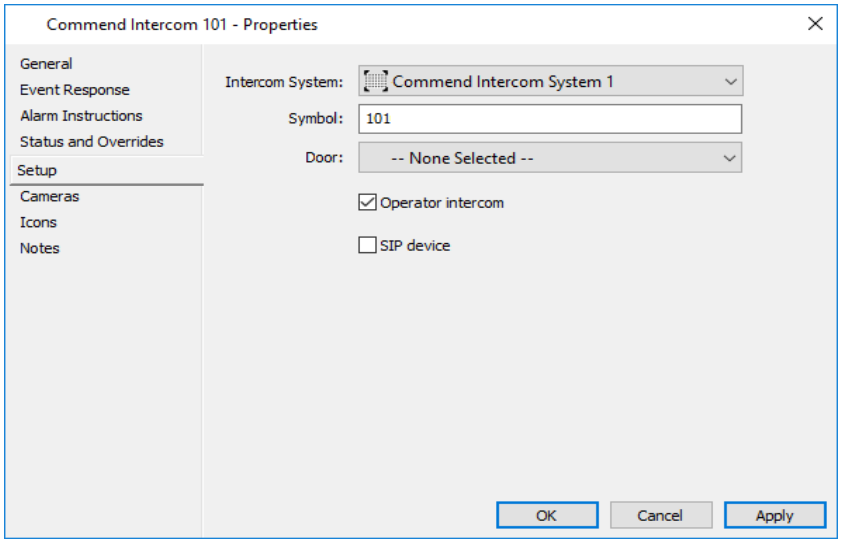
Field	Input
Condition	Select Break for idle status, or 15k for tamper status.
Task	7C
Type	Select 26 for idle status, or 25 for tamper status.
Data	Type the intercom or station number, with leading Fs so there is a total of 16 characters.



Procedure

1. Click **Configure** from the menu bar, then **External Systems**.
   The External Systems List Window opens (in tree view).
2. Right click the Commend Intercom System you have already created and select **New...Commend Intercom**.
   By default the **General** tab displays.

3. Type in the Name and select the Division. The **Description** field is populated and updated automatically from the Commend Intercom server.
4. Click the **Setup** tab.



5. Select the Intercom System from the **Intercom System** drop-down list.
6. Enter the intercom symbol as shown in the Commend Site Configuration application into the **Symbol** field. Maximum of 16 digits. Notes:
   - The intercom symbol will be provided by your Commend Intercom installer.
   - The intercom symbol is checked for uniqueness within the same Intercom System.
7. If required, select the Door that corresponds to this intercom from the **Door** drop-down list.
8. Tick the **Operator intercom** checkbox if the intercom is the control desk/ operator intercom which will be assigned to a workstation.
9. Tick the **SIP device** checkbox if the Intercom is an SIP device (your Commend Intercom installer can advise if this is the case).
10. Click the **Icons** tab if you want to change the Icon Set for the Intercom Item. For further details see ***Icons*** (on page 6-80).
11. Click the **Custom Fields** tab if you want to add and assign a custom field value to the Intercom Item. 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 the Intercom Item. 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

The new Commend Intercom has been created and displays as a child of the Commend Intercom System in the **External Systems** List Window.

Assigning a Commend Console to a Workstation

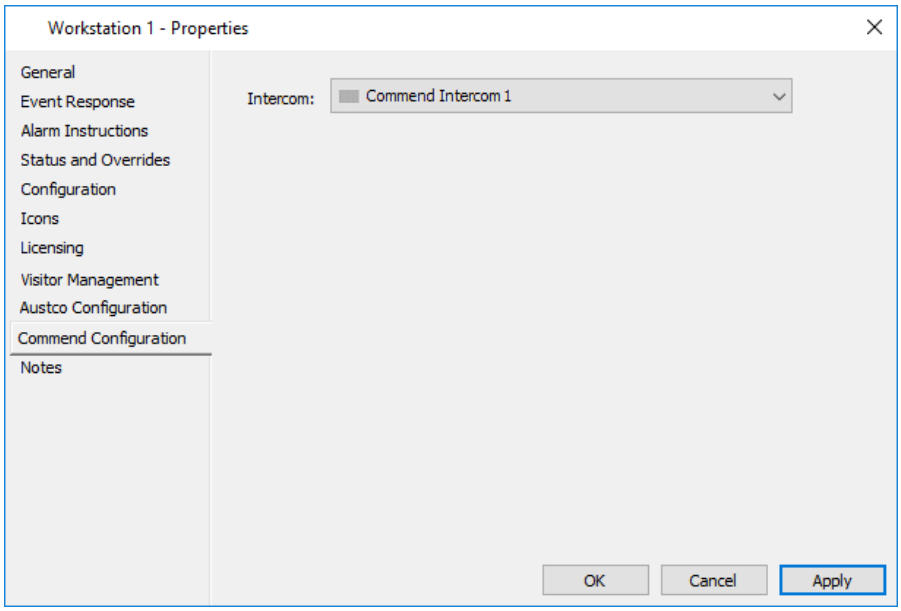
Introduction

The Commend Console must be located near the Command Centre workstation. If an operator responds to an intercom call event via the workstation, the call event will be removed from all other operator workstations.

Perform the following procedure to assign a Commend Console to a Command Centre workstation.

Procedure

1. Click **Configure** from the menu bar, then **Services & Workstations**. The Services & Workstations List Window opens.
2. Open the workstation you want to assign the Commend Console to.
3. Click the **Commend Configuration** tab.



4. Select the Commend Intercom that you want to assign to the workstation.
   Notes:
   - Only master intercoms can be associated with a workstation.
   - A master intercom can only be associated with one workstation.
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.

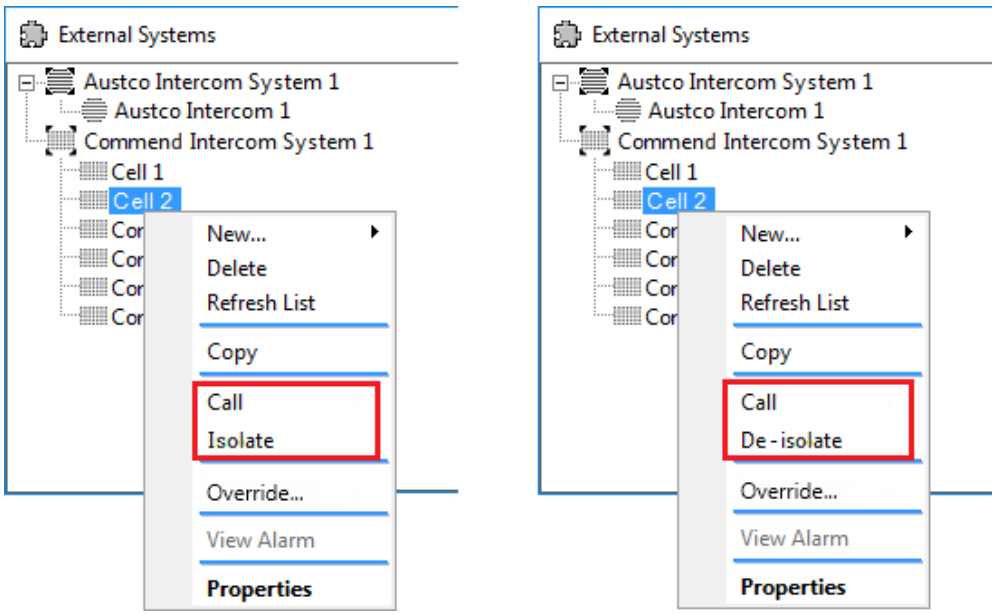
Result

A Commend Console has been assigned to a Command Centre workstation.

Using Commend Intercoms

You can *Call* and *Isolate/De-isolate* Intercoms from the Configuration Client. See the ***Configuring a Commend Intercom System*** (on page 60-4) topic for instructions on setting up the Commend Intercom System.

1. Click **Configure** from the menu bar, then **External Systems**.
   The External Systems List Window opens.
2. Right click the Commend Intercom System you want to call, isolate or deisolate.
   A context menu displays.
3. Click the action you want to complete.



4. The action is applied.

Commend Isolate Function

The Commend Intercom's 'Isolate' function is an override option. It allows an operator to disable a specified intercom until the operator chooses to de-isolate it.

Note: Some intercoms cannot be isolated, (e.g. master and SIP intercoms).

Chapter 61: Class 5 End-of-Line Module (ELM)

Introduction

The Gallagher 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 has three binary inputs and one output intended for monitoring and reporting sensor state from a position physically close to the sensor location. The three binary inputs are intended for connecting to the sensor's alarm, tamper, and trouble outputs. The output can be used to enable the sensor's test LED during pre-arm or Alarm Zone testing modes. The ELM transmits the state of these contacts to the Gallagher PIV C6000HS Controller, over an encrypted communications link.

Note: The Class 5 ELM only works with a Gallagher PIV C6000HS Controller.

Licensing

Creation of Class 5 ELM items in Gallagher Command Centre requires the following option in the license file:

```
[Features]
Class5=1
```

There are no licensing limits for the number of Class 5 ELM items that can be created.

Integration with FT items

Class 5 ELMs can be assigned to any Command Centre item that an Input can be assigned to, (i.e. Access Zones, Alarm Zones, Interlock Groups, Guard Tours, Site Plans, Hardware, Doors, Elevator Cars and Logic Blocks). Basically, they can be used instead of an Input, (i.e. a Class 5 ELM can be dragged and dropped anywhere an Input can).

As the Class 5 ELM has many states, not just open and close, each item may require the non-open close states to be filtered out.

Select the item below that you require further detail on:

- ***Configuring a Class 5 ELM*** (on page 61-2)
- ***Configuring Class 5 ELMs for Test Modes*** (on page 61-7)
- ***Performing Overrides for Class 5 ELMs*** (on page 61-9)

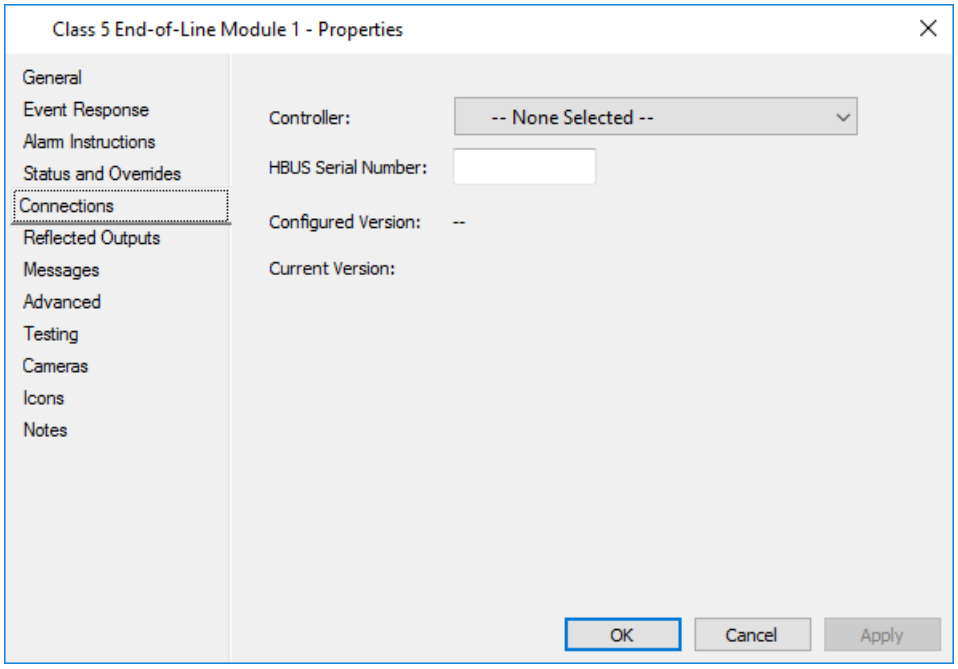
Configuring a Class 5 ELM

Introduction

This procedure describes how to configure a Class 5 ELM in Command Centre.

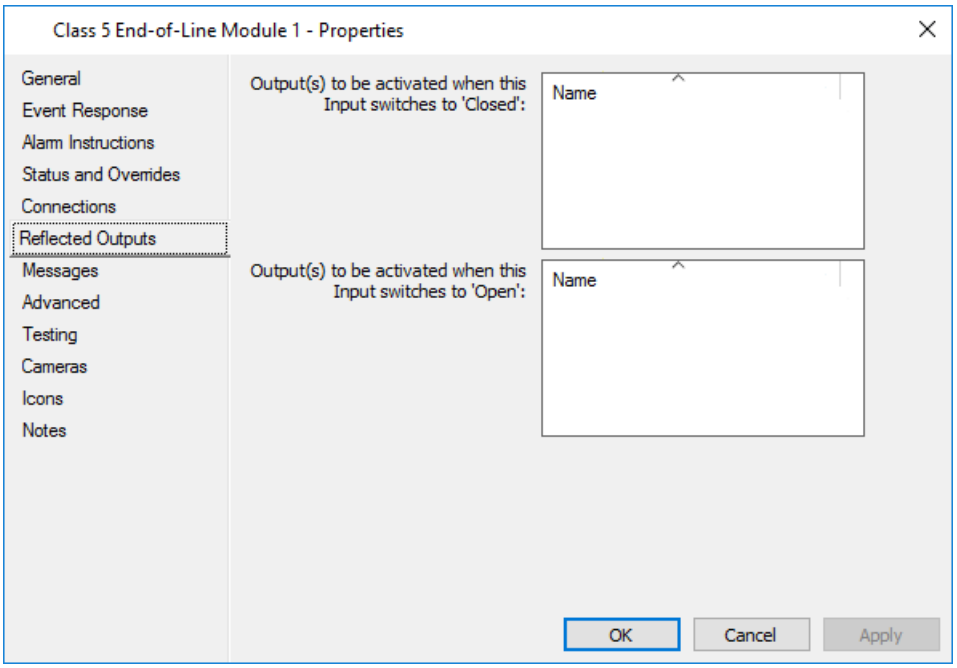
Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...HBUS Devices**.
3. Select **Class 5 End-of-Line Module**.
   By default the **General** tab displays.
4. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
5. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
6. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
7. Click the **Connections** tab.



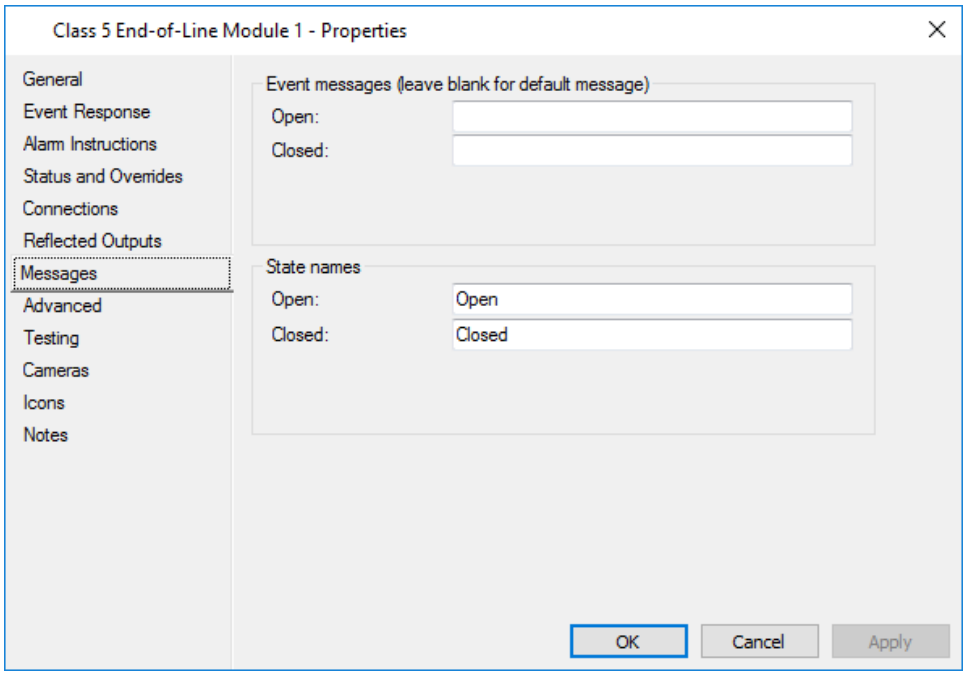
8. Select the Controller 6000 you want to assign this ELM to, from the **Controller** drop-down list.
   Note: When an HBUS device is added to a Controller 6000, it will appear on the **HBUS Devices** tab of the Controller. In this case, the **Controller** field will be pre-populated with that Controller name.

9. If not already present, enter the HBUS serial number (10-character hexadecimal string) into the **HBUS Serial Number** field.
   Note: The HBUS serial number is optional, however the ELM will be considered as not properly configured unless one is entered.
10. If you click the **Apply** button, software version numbers display.
    The **Configured Version** is the version of the device software in the configured Controller 6000 FTS file, (i.e. not the version of the Controller 6000 software). The Current Version is the version of software as last reported by the ELM itself.
11. Click the **Reflected Outputs** tab.

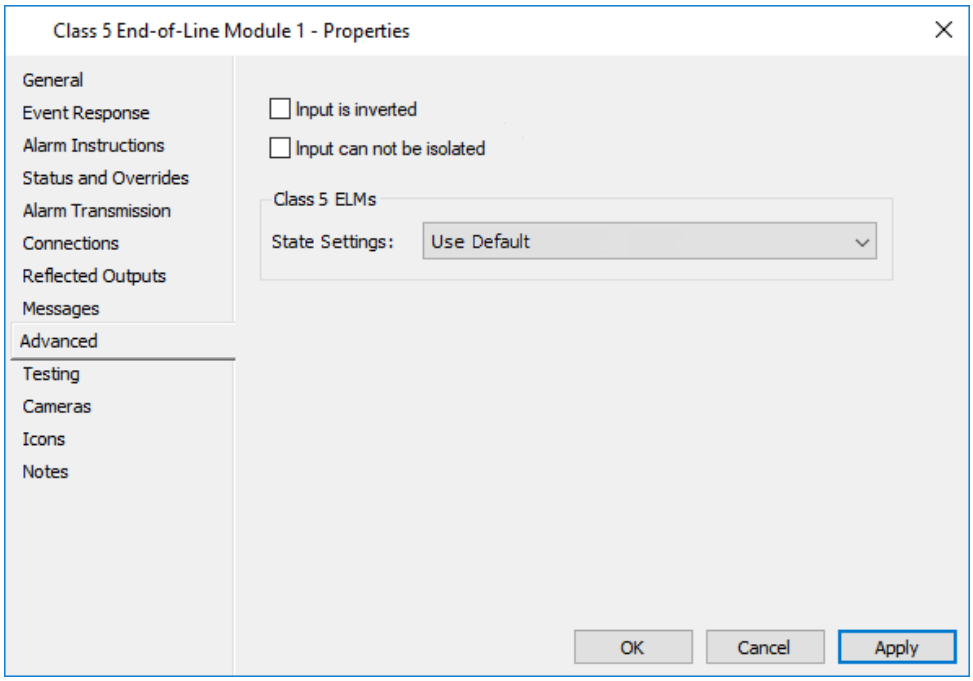


12. Drag and drop the appropriate Output(s) into the two grids.
    The top grid lists the Output(s) that reflect the closed state of the Input, and the bottom grid lists the Output(s) that reflect the opposite state of the Input.

    Note: The Output will only be reflected to the Alarm Input on the ELM.
13. Click the **Messages** tab.



14. Enter the state and event names (if different from the site-wide default), that will display in Command Centre when this ELM is activated and deactivated.
15. Click the **Advanced** tab.



16. Tick the checkboxes as required.

Checkbox	Description
Input is inverted	If checked, the state of the Input is reversed, (i.e. the system considers the Input 'open' when it is closed, and 'closed' when it is open).
Input cannot be isolated	If checked, the Input will not be ignored when an Alarm Zone is armed with the ‘Isolate’ option.

17. Select the required state for this Class 5 ELM from the **State Settings** drop-down list. The options are:

Option	Description
Use Default	This is the default setting. Selecting this option means that the global state setting (as configured on the **Advanced** tab of the Server Properties) will apply.
Trouble Output = Masked State	This setting indicates the Masked state.
Trouble + Alarm Outputs = Masked State; Trouble Output = Fault State	Selecting this option means that trouble and alarm means Masked, and trouble alone indicates Fault. If this state is selected, ensure that a fault state is not raised accidentally (via the Trouble input). • If the Trouble and Alarm inputs are opened together, one will always appear to open briefly before the other: ▪ If the Alarm input opens first, an Alarm state (Input Open) is raised just before the Masked state is raised. ▪ If the Trouble input opens first and the Alarm input is opened within 2 seconds, only a Masked state is raised. ▪ If the Trouble input opens first and the Alarm input is opened after 2 seconds, a Fault state is raised and then a Masked state is raised. • If the Alarm input is opened on its own, the Alarm state will immediately initiate. • If the Trouble input is opened on its own, the Fault state will initiate after 2 seconds. If both the Trouble and Alarm inputs are open and the ELM is in Masked state, closing the inputs will have this effect: • If the Trouble input is closed first, an Alarm (Input Open) state is reported, and then an Input Closed state once the Alarm input closes. • If the Alarm input is closed first and the Trouble input is closed within 2 seconds, only an Input Closed state is reported. • If the Alarm input is closed first and the Trouble input is closed after 2 seconds, only an Input Closed state is reported and then a Fault state is raised.

18. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Class 5 ELM.
    For further details see ***Cameras tab*** (on page 3-24).
19. Click the **Icons** tab if you want to change the Icon Set for this Class 5 ELM.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
    Note: There are separate states for the Class 5 ELM, (i.e. Closed, Open, Unknown, Masked, Tamper and Offline). The Tamper state will override any other states.
20. Click the **Custom Fields** tab if you want to add and assign a custom field value to the Class 5 ELM.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
21. Click the **Notes** tab if you want to add a note(s) about the Class 5 ELM.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
22. 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.

Configuring Class 5 ELMs for Test Modes

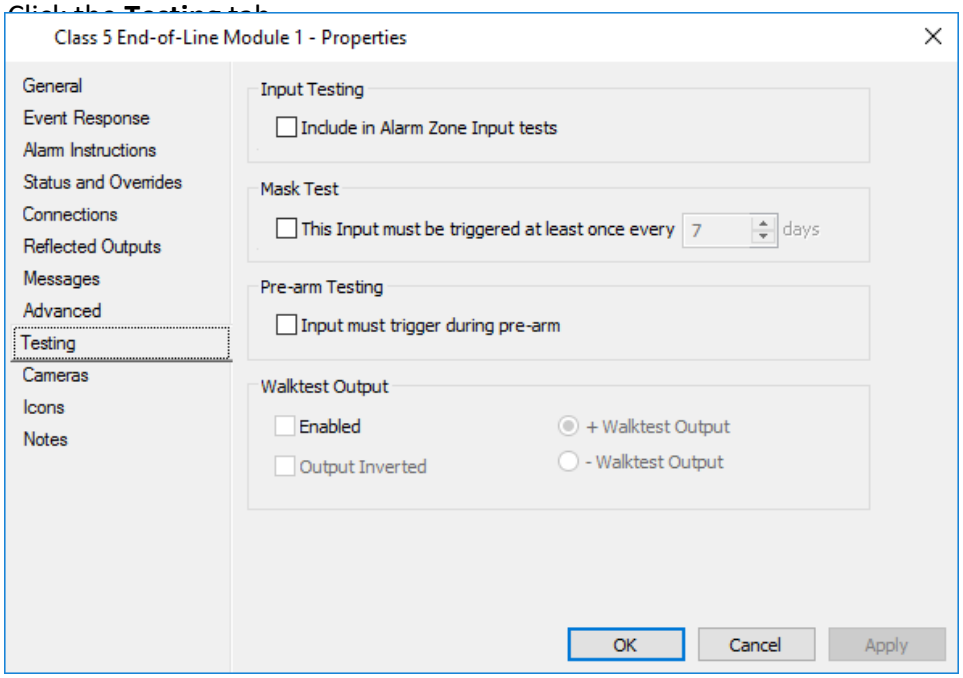
Introduction

This procedure describes how to configure each Class 5 ELM that requires testing.

Note: The normal state of all Class 5 ELMs should be 'closed'. If an ELM is 'open' you will need to reverse the state of the ELM, by checking the 'Input is inverted' checkbox on the **Advanced** property page for the ELM.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** on the appropriate Class 5 ELM and select **Properties**.
3. Click the **Event Response** tab.
4. If the ELM requires a visual indication that it is working, (e.g. a light turns on when the input is activated) assign an Action Plan to the Open/Off Event Group.
   This Action Plan will need to trigger the light when the ELM changes state.
5. Assign a primary Alarm Zone for all events from the drop-down list.
6. Click the **Testing** tab.



7. If the ELM requires periodic or manual testing, check the **Include in Alarm Zone Input tests** checkbox.
   The ELM will be included in all periodic and manual tests.

8. If the ELM requires mask testing, check the **This Input must be triggered at least once every X days** checkbox and enter the number of days the ELM must be activated within.
   (Default = 7 days. Configurable from 1 to 30 days.)
9. If the ELM is a seismic detector, check the **Input must trigger during pre-arm** checkbox.
10. Enable the **Walktest Output** if required, by checking the **Enabled** checkbox and configuring as appropriate.

Checkbox/Button	Description
Output Inverted	When selected, the output operation is inverted, (i.e. it will be on and when operated will turn off).
+ Walktest Output	If selected, the output will be 'On High'.
- Walktest Output	If selected, the output will be 'On Low'.

Notes:

- The Walktest Output has three settings, as follows:

  Off: High impedence between output terminals.

  On High: Output driven to +13V - this will be the on state if ELM has **+ Walktest Output** selected.

  On Low: Output driven to GND - this will be the on state if ELM has **- Walktest Output** selected.

- **Interaction with Input Testing and Pre-Arm testing**

  IF 'Include in Alarm Zone Inputs tests' is selected for this ELM and the Walktest Output is configured, the Walktest Output will operate (as configured) when Test Mode is selected for the Alarm Zone from the T20 or tested during disarming.

  IF 'Input must trigger during pre-arm' is selected and the Walktest Output is configured, the Walktest Output will operate (as configured) during the Pre-Arm.

  IF 'Include in Alarm Zone Inputs tests' AND 'Input must trigger during pre-arm' are selected, the Walktest Output will operate (as configured).

- **Interaction with Mask Test**
  There is no requirement to interact with the Mask Testing (this is generally long term testing) and for security purposes the Walktest LED should be disabled on a day to day basis and only turned on when required.

11. Click the **OK** button to exit and save your changes.
12. Repeat this procedure for each ELM that requires testing.

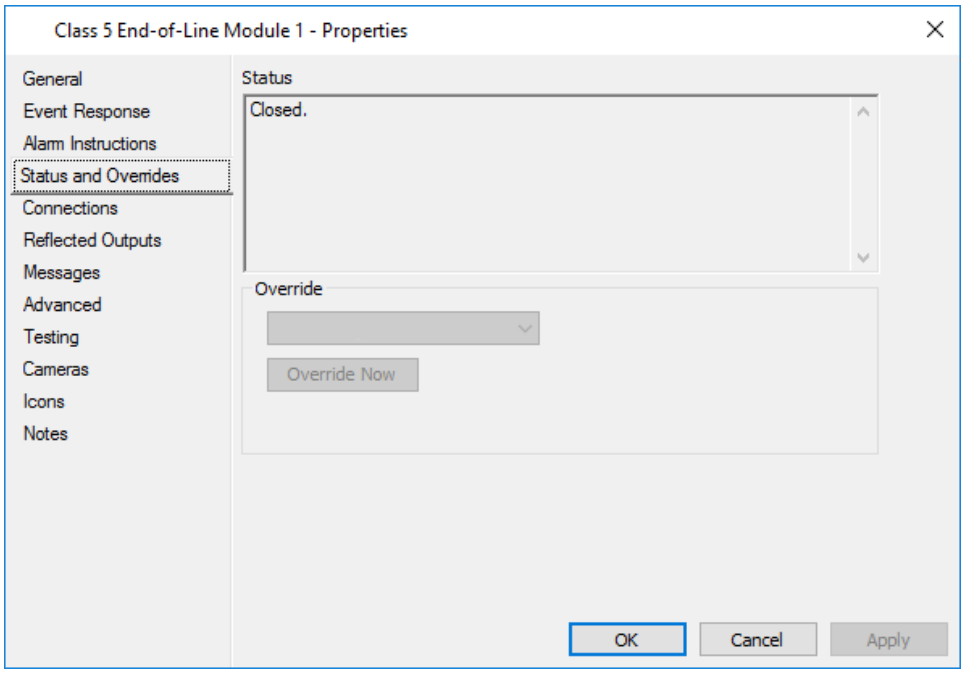
Performing Overrides for Class 5 ELMs

Introduction

This procedure describes how to temporarily override the status of a Class 5 ELM.
Note: A Class 5 ELM cannot be isolated if the **Input can not be isolated** option is selected on the **Advanced** tab of its property pages.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** on the Class 5 ELM you want to override, and click **Override…**from the drop-down menu.
   The **Status and Overrides** tab on the properties window for the ELM displays.



3. Click within the **Override** field and select the appropriate status from the drop-down list.

Status	Description
Reset	This performs a software reset on the ELM.
Shunt	This stops communication with the ELM and will remain this way until you "Unshunt".
Unshunt	This starts polling of the ELM.

Status	Description
Isolate	Will isolate the ELM, so that the Alarm Zone can be armed. Alarms from the ELM will no longer be raised.
De-isolate	The ELM is no longer isolated.

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

Note: The Class 5 ELM presents a single status to the system by combing the states of the ELM's three inputs as follows:

ELM Status	Alarm Input	Masked Input	Tamper Input
Closed	Closed	Closed	Closed
Open	Open	Closed	Closed
Masked	Any	Open	Closed
Tamper	Any	Any	Open
The Device is not responding	Unknown	Unknown	Unknown
Controller Offline	Unknown	Unknown	Unknown

Chapter 62: Locker Management Solution

Introduction

The 'Locker Management Solution' is used to manage Cardholders access to Lockers. You can configure Lockers to enable Cardholders to self-assign Lockers, or the operator can manually assign Lockers to Cardholders via the Locker Viewer, Cardholder Viewer or Bulk Changes. You can configure Lockers so that they are automatically quarantined for a specified period upon the expiry of their Cardholder assignments, or the operator can manually quarantine Lockers at any time. While quarantined, Lockers cannot be assigned to Cardholders, and can only be opened by privileged Access Groups. Using the Locker Viewer, an operator can view all current assignments he is privileged to.

This feature enables you to (in either the Command Centre or Configuration Client):

- manage individual and group access to Lockers
- configure Lockers for self-assignments and/or manual assignments
- configure Lockers for automatic quarantining and/or manual quarantining
- notify the Cardholder when a Locker has been assigned or removed (via existing Command Centre Notifications framework), see ***Enabling Event/Alarm Notifications for a Cardholder*** (on page 35-9)
- report on Locker activity (access events plus alarms such as Locker Forced Open and Locker Open Too Long)
- report on Cardholders including current Locker assignments
- view status, and override Lockers
- manage remote site Lockers. See **Multi-server** section below.

Notes:

- The recommended lockers limit is 256 lockers per Controller 6000 or 7000, with 16 x High Density IO boards and 2 to 4 readers. This limit is derived from the Controller 6000 or 7000 Input/Output hardware limit.
- if an Alarm Zone is assigned to an HBUS Terminal (via Alarm Zones tab), then that HBUS Terminal cannot be allocated to a Locker Bank.

Licensing

The 'Locker Management Solution' is a licensable feature, i.e. your license file must contain the following options:

```
[Features]
Lockers=1

[Limits]
Lockers=n
```

[n] indicates the number of Lockers that can be created

Operator Privileges

An Operator requires the appropriate Locker privileges to perform Locker tasks. The privileges only apply within the Divisions assigned to that Operator Group.

Operator Privilege	is required to...
"Edit Lockers"	create, edit and delete Lockers and Locker Banks.
"Manage Locker Assignments"	assign (allocate), modify and/or remove Lockers from Cardholders. It does not include View Cardholder privilege however; View Cardholder privilege is not required to see existing Locker assignments in Locker Viewer.
"Override"	manually quarantine Lockers ('Quarantine Locker' override), and cancel the active override on a Locker ('Cancel Override'). Performing 'Cancel Override' on a quarantined Locker will take it out of quarantine.
"Override - Open Locker"	open Lockers and unallocated Lockers ('Open Locker' override).
"View Lockers and Assignments"	view Lockers, Locker Banks and Locker assignments.

Notes:

- Edit Site does not include Edit Lockers therefore, you cannot create, edit or delete Lockers or Locker Banks.
- View Site cannot view Lockers or Locker Banks.

Multi-server

The following Command Centre multi-server functionalities can be achieved from a remote server:

- override Lockers (Open Locker)
- override Locker Banks (Unlock Unallocated Lockers)
- view Lockers
- assign and/or remove Lockers

Considerations

- Cardholders can continue to self-allocate and use Lockers while the Command Centre server is down. The Command Centre server will be updated once it is back online.
- When the Controller and the Command Centre server reconnect, there is a conflict between an attempted operator allocation (that occurred while the Controller was offline) and a self-allocation. The self-allocation takes precedence and the attempted Operator allocation will be ignored.

- While the Controller is offline, Locker Configuration and operator modification of Locker assignments will be ignored by the Command Centre. For example, a Cardholder assignment is about to expire in 3 minutes. The connection between server and controller is lost, and the operator modifies the Locker Configuration to extend the Cardholder assignment. After 4 minutes, the connection is re-established. However, the change to the Cardholder assignment has not occurred, and the Locker has been removed from the Cardholder. Therefore, configuring, assigning, or removing Lockers while the Controller is offline are not recommended.
- While the Controller is offline and a Cardholder self-assigns a Locker, if the allocated Locker is being accessed for the first time, the T-20 reader grants access, but it does not display the Locker name.
- If a Locker Bank and a Locker reader are connected to different Controllers, and a Cardholder presents a credential to the reader, the reader will time out after 20 seconds and the Cardholder will be denied access.

Bulk Configuration Tool

The Bulk Configuration Tool can be used to create and configure a large number of Lockers and Locker Banks. Refer to the *Bulk Configuration Tool* page on the Gallagher Security Hub for further detail: https://resources.security.gallagher.com/Install,_Upgrade_and_Tools/Tools_and_Utilities/Bulk_Configuration_Tool

Note: An account is required to access the Security Hub, so register if needed.

Configuration

To configure Locker Management, perform the following procedures:

Configuring a Locker Bank (on page 62-4)

Locker Bank Status and Overrides (on page 62-16)

Configuring a Locker (on page 62-17)

Locker Status and Overrides (on page 62-19)

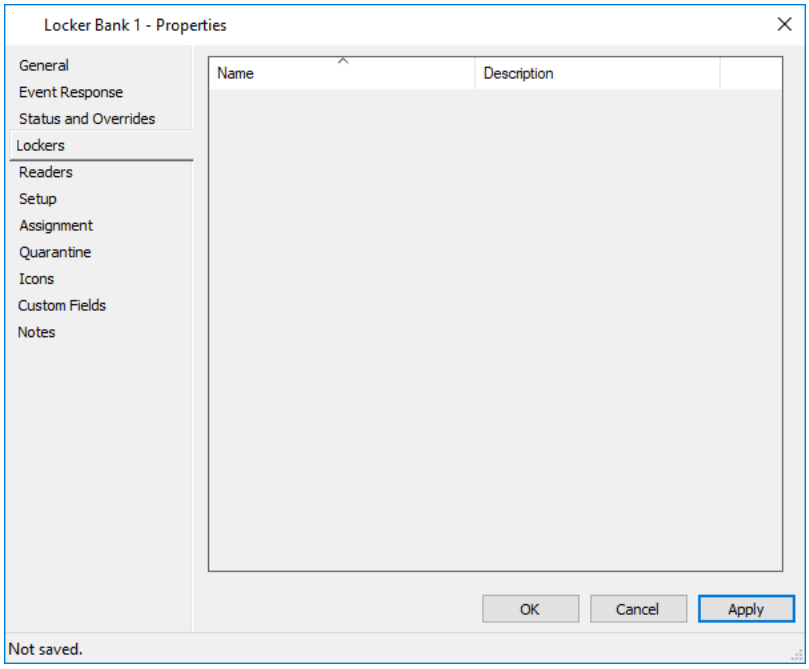
Configuring a Locker Bank

If you need to configure a large number of Lockers, you can use the Bulk Configuration Tool. Refer to the *Bulk Configuration Tool* page on the Gallagher Security Hub for further detail:
https://resources.security.gallagher.com/Install,_Upgrade_and_Tools/Tools_and_Utilities/Bulk_Configuration_Tool

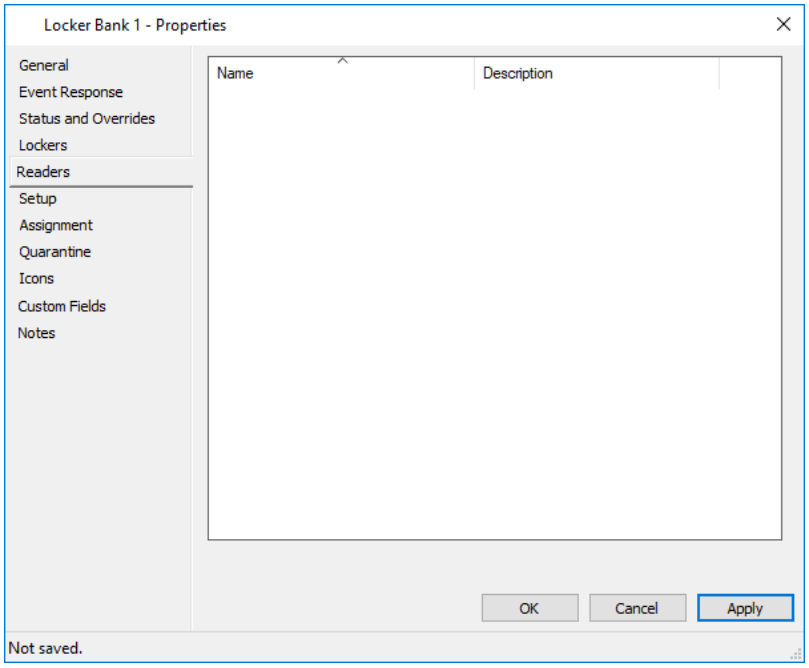
Note: An account is required to access the Security Hub, so register if needed.

Perform the following procedure to configure a Locker Bank:

1. From the Gallagher Configuration Client main window, click **Configure** > **Lockers.**
2. Right-click and select **New...Locker Bank.**
   The Locker Bank Properties window opens to the **General** tab by default.
3. Complete the fields as required.
   For further details 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).
   Note: If you receive an *"Unable to save configuration as an Alarm Zone is required"* message, assign a primary Alarm Zone to the Locker Bank and try again.
5. Click the **Alarm Instructions** tab, and configure as required.
   For further details see ***Alarm Instructions tab*** (on page 3-22).
6. Click the **Lockers** tab.



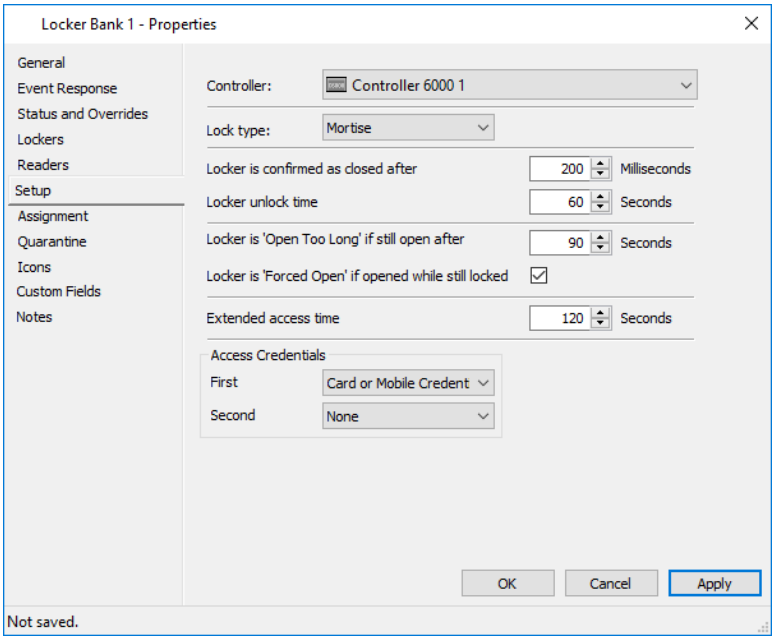
   This tab displays names and descriptions of lockers assigned to the Locker Bank.
7. Click the **Readers** tab.



8. Add the appropriate reader(s) to the Locker Bank using drag and drop.
   Locker Management Solution has been tested with the following readers:
   - T-Series Readers (T20,T12,T11,T10) - using HBUS or connected to 4R and 8R modules
   - HID multiCLASS SE® RPK40 (921PTPTEK00385) - using OSDP
   - HID iCLASS RPK40 (6136AKN000000) - using HBUS I/O 4-in 2-Out Door Module - Wiegand

   Note: Biometric readers connected to 4R and 8R are not supported in this version.

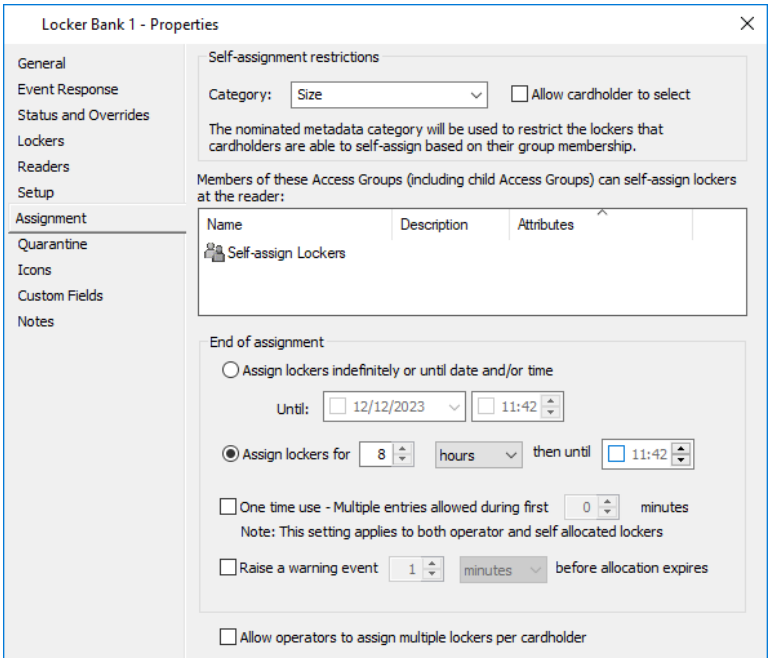
   Notes:
   - A reader cannot be assigned to more than one Locker Bank.
   - If this Locker Bank uses quarantining, only the T20 Reader is supported, as a screen is required to manage quarantined Lockers at the reader.
   - It is not possible to assign an HBUS Terminal with Alarm Zones to a Locker Bank.
9. Are you using a Third Party/OSDP Reader on this Locker Bank?
   If **no**, go to the **Setup** tab (Step 10).
   If **yes**, note the following:
   With the Lockers licence, the **HBUS Terminal Display** tab of a Third Party/OSDP Reader is enabled. On this tab, you can assign an HBUS Terminal to a Third Party/OSDP Reader, so feedback from the Third Party/OSDP Reader is displayed on the screen of the HBUS Terminal. This overcomes the issue of Third Party/OSDP Readers not being able to display feedback.
   To do this, perform the procedure described in ***Assigning an HBUS Terminal to a Third Party/OSDP Reader*** (on page 62-13).
10. Click the **Setup** tab.



11. Select a controller from the **Controller** drop-down list.
12. Select a lock from the **Lock type** drop-down list.
    By default, Mortise is selected.
13. Configure the Locker timeouts as required.

Option	This setting...
Locker is confirmed as closed after	is to stop Locker door bounce causing a forced door alarm. (Valid range is 0 - 500 milliseconds. Default = 200 milliseconds)
Locker unlock time	determines the maximum time the Unlock relay is energised. (Valid range is 1 - 86400 seconds. Default = 60 seconds)
Locker is 'Open Too Long' if still open after	determines when a Locker door Open Too Long alarm is generated. (Valid range is 5- 9999 seconds. Default = 90 seconds)
Locker is 'Forced Open' if opened while still locked	when checked, causes a Forced Locker alarm to be generated if the open sensor detects the Locker door is opened.
Extended access time	determines an alternate unlock time, allowing the Locker 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 = 120 seconds)
Access Credentails	Specify the first and second **Access Credentials** required to access the locker bank. The default first access credential required is "Card". The default second access credential required is "None". **Note:** If "User Code" is exclusively selected, a Mobile Credential cannot be used to open a locker. Mobile connect uses Passcode or Fingerprint (or Face ID) for second factor authentication.

14. Click the **Assignment** tab.

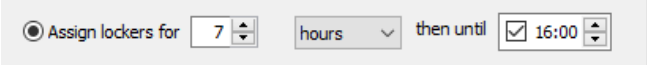


15. Enter the appropriate access group(s) allowed to self-assign Lockers.
    Drag and drop the access group(s) into the grid.

    If you want a cardholder to be able to self-assign a locker with attributes, go to Step 20.

16. Configure 'End of assignment' as required.
    See ***Locker Bank Configuration (Scenarios)*** (on page 62-14) for details.

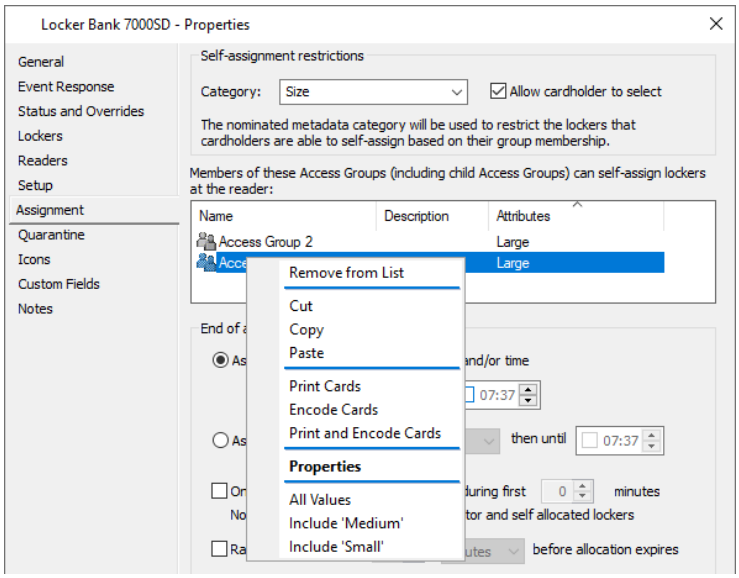
To...	then
Assign Lockers with explicit until date and/ or time	**a)** Click the **Assign Lockers with explicit until date and/or time** radio button. The Until date and time fields activate. **b)** Select the **Until** date checkbox. **c)** Click the date drop-down button, then select an explicit end of assignment date. **d)** Do you need to configure an explicit end of assignment time? If **no**, then go step 17. If **yes**, select the **Until** time checkbox, then enter the specified time. **Notes:** • If you do not configure the 'Until' date or, time or the 'One time use - Multiple entries allowed during first N minutes', then Locker assignments will be permanent. • When the configured 'Until' date expires, Cardholders will be unable to self-assign Lockers. • If you only configure the 'Until' time (i.e. the Until date checkbox is deselected), the Cardholder will have access to that Locker until the next occurrence of the configured time.

To...	then
Assign Lockers for (fixed period)	**a)** Click the **Assign Lockers for** radio button. **b)** Enter a numeric value for **the Assign Lockers for**, then from the drop-down list select an option (minutes, hours, days, weeks or months). **c)** Do you want to configure a specific end of assignment time? If **no**, then go step 15. If **yes**, select the **then until** time checkbox, then enter the specified time. **Note:** The 'then until' time will always overlap to the next occurrence time if the initial 'Assign Lockers for' period has not ended before the 'then until' time. E.g. If the Locker Bank is configured as:  • If the Cardholder badges at 09:02, the 7 hours assignment will not end before 16:00. Therefore, the Cardholder will have access to the Locker until the next occurrence of 16:00 hours. • If the Cardholder badges at 08:02, the 7 hours of the assignment will finish at 15:02, but the Cardholder will continue to have access to the Locker until 16:00.
Raise a warning event before allocation expires	Select the Raise warning checkbox. Set the raise warning event period to the value that is required to represent the number of minutes, hours, days, weeks or months before the allocation expires to raise a warning event. When the configured period is reached, the following event raised: *"[Locker name] of [Locker Bank] is due to expire for [Cardholder] at [YYY-MM-DD] [HH:MM]."* Using this event (Event Group: Cardholder Locker Expiry Warning), you can set up a Notification Filter to alert Cardholders in advance of their imminent allocation expires. For more, see ***Creating a Notification Filter*** (on page 35-5). **Notes:** • If **One time use** checkbox is selected, then the Raise warning event option is disabled. • The warning event is raised for self-assigned Lockers, and Operator allocated Lockers that have an Allocated Until date.

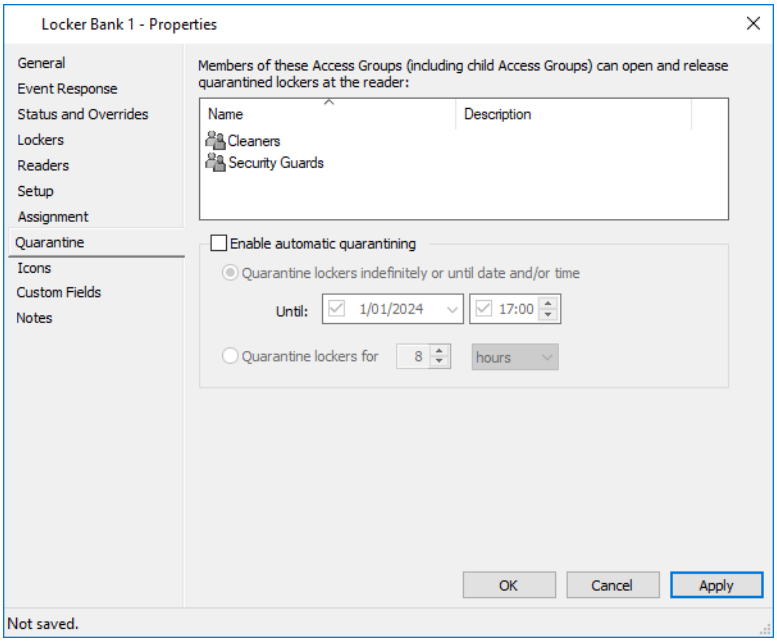
17. You can configure the 'One time use - Multiple entries allowed during first N minutes' in conjunction with both the above options. The cardholder can use the Locker as many times as required during this period.
However, once this period is over and the Cardholder badges, the Locker will open (to allow the Cardholder to remove his/her items from the Locker), then the Locker will be unallocated from the Cardholder despite the remaining assignments period.

Do you want to configure 'One time use - Multiple entries allowed during first N minutes'?
If **no**, then go step 19.
If **yes**, select the **One time use - Multiple entries allowed during first N minutes** checkbox.

18. Enter the number of minutes during which the Cardholder is allowed multiple entries (this is limited to 999 minutes).
    Note: If the 'One time use - Multiple entries allowed during first' is selected and has a value of '0' minutes, Lockers will be unallocated from Cardholders after:
    - the first badge, if the Locker was manually assigned, OR
    - the second badge (first badge to self-assign, second badge to remove), if the Locker was self-assigned.
19. Do you want to allow the operators to assign multiple lockers to a Cardholder?
    If **no**, go to step 20.
    If **yes**, select the **Allow operators to assign multiple lockers per cardholder** checkbox.
20. If you want a cardholder to be able to assign Custom Fields Attributes:
    Note: You need to create Custom Fields first.
    a) Click on the ▼ of the **Category** field and select a Category.
    b) Check the **Allow cardholder to select** checkbox.
    A cardholder who is a member of the Access Group will be able to self-select only a locker that has the Attribute in the Attribute column.
    Note: If you do not check the checkbox, the next available locker will be auto-assigned to the cardholder.
    c) Right-click the Access Group.
    The context menu will give you a list of the attributes that can be added (from the list created on the **Custom Fields** tab of one or more Lockers).
    d) Add the attribute and continue until you have selected all the attributes you want. Additional attributes are added by selecting Include '[Value Name]', (e.g. Include 'Medium').
    If you do not add an attribute the default is 'All Values'. This means the same as selecting each available type individually.



21. Click the **Quarantine** tab.



About quarantine: Putting a Locker into the 'quarantined' status restricts it to only be opened and released from quarantine by members of the Access Group(s) you assign to this tab, as well as privileged Command Centre operators. This tab allows you to set Lockers to automatically be quarantined when their Cardholder allocations expire. Lockers cannot be allocated to Cardholders while quarantined. This may be used, for example, so only cleaners may access used Lockers, and then release them from quarantine so they can be allocated again.

22. From the Access Group list window, select the Access Group(s) who will be allowed to open this Locker Bank's quarantined Lockers and release Lockers from quarantine (cancel quarantine) at the Locker Bank's T20 Terminal. Then, drag and drop (or copy and paste) the Access Group(s) into the grid on the **Quarantine** tab.

    About opening and releasing quarantined Lockers: Members of the Access Group(s) added here will be able to:
    - open quarantined Lockers via the Locker Bank's T20 Terminal, and
    - release Lockers from quarantine (cancel quarantine) via the Locker Bank's T20 Terminal.

    This is different from the 'Open' and 'Cancel Override' overrides, which are performed by privileged Command Centre operators. When a member of these Access Groups badges their credential at the Locker Bank's T20 Terminal, they will be able to view the Locker Bank's quarantined Lockers, and select a specific quarantined Locker to open it or release it from quarantine. If they are a member of an Access Group added to the **Assignment** tab, they also have the option of assigning themselves a Locker.

23. If you want this Locker Bank's Lockers to be quarantined automatically when their Cardholder assignment ends (as per the 'End of assignment' configuration on the **Assignment** tab), select the **Enable Automatic Quarantining** checkbox.

Note: Lockers are not automatically quarantined when their Cardholder assignment is manually removed.

24. Did you select **Enable Automatic Quarantining**?
    If **yes**, go to Step 25.
    If **no**, go to Step 26.
25. Configure automatic quaratining as required.

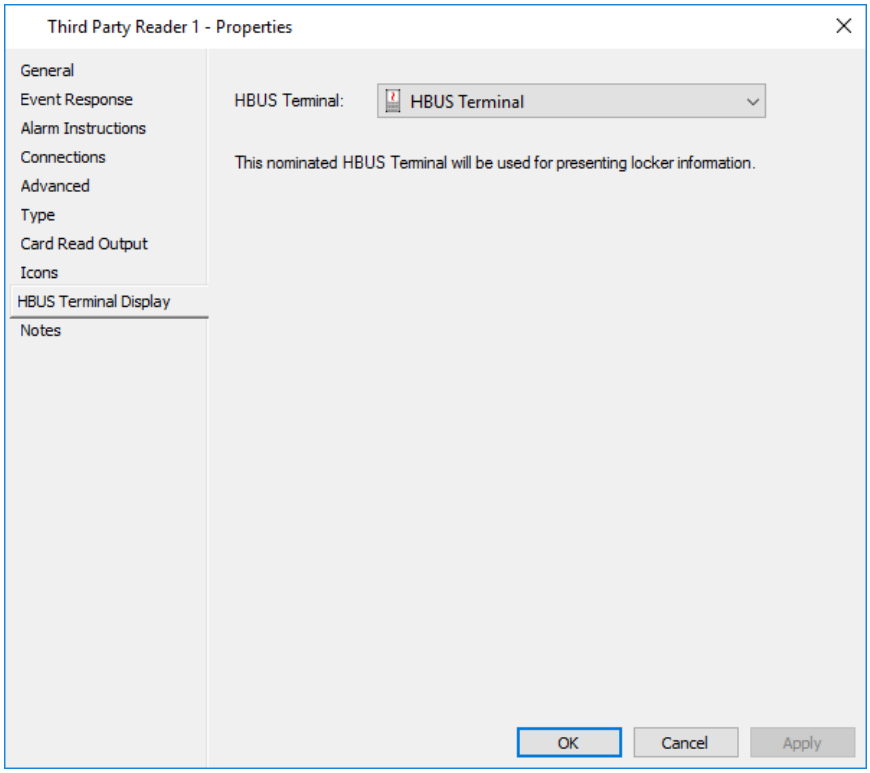
To…	then…
Automatically quarantine Lockers indefinitely (i.e. forever until something cancels the quarantine	1. Click the **Quarantine Lockers indefinitely or until date and/or time** radio button. The 'Until' date and time fields activate. 2. Do *not* select the date or time checkboxes. With no date or time set, Lockers are quarantined indefinitely. For a Locker to come out of quarantine with this configuration, an operator will need to manually perform a 'Cancel Override' action on the Locker, or a Macro would need to run with a 'Cancel Override' action for the Locker.
Automatically quarantine Lockers until a specific date and/or time	1. Click the **Quarantine Lockers indefinitely or until date and/or time** radio button. The 'Until' date and time fields activate. 2. Do you want to configure a specific end of quarantine date? If **no**, go Step 5. Lockers will end quarantine at the next occurrence of the specified time regardless of the current date. If **yes**, select the date check box, then enter the specified date. **Notes:** • If you only configure the 'Until' date (i.e. the time check box is unchecked), the Locker will be quarantined until 11:59 p.m. on the specified date (i.e. at the end of that day). • Once the specified date has passed (in real time), the selected date is automatically updated to today's date each day past that date. The date cannot ever be in the past. However, the selected time is unaffected by this behaviour. This means if the date auto-matically rolls over to today's date and the unaffected specified time is currently in the past (e.g. it has been set to 9:00) when a Locker is automatically quarantined (e.g. at 10:00), then the Locker will be immediately taken out of quarantine because the datetime is in the past. Ensure you maintain the selected date and time so unexpected scenarios like this do not occur.

To…	then…
	3. Do you want to configure an explicit end of quarantine time? If **no**, go Step 7. Lockers will end quarantine at 11:59 p.m. on the specified date. If **yes**, select the time check box, then enter the specified time. **Note:** If you only configure the 'Until' time (i.e. the date check box is unchecked), the Locker will be quarantined until the next occurrence of the configured time, whether that is today or the next day. **Notes:** • If you select **Quarantine Lockers until date and/or time** but do not select either the date *or* time check boxes, then Lockers are quarantined indefinitely. • When the configured 'Until' date and/or time is reached, the Lockers are set to 'Free'.
Automatically quarantine Lockers for a fixed period	1. Click the **Quarantine Lockers for** radio button. 2. Enter a numeric value in the **Quarantine Lockers for** field, then select a unit option from the drop-down list (minutes, hours, days, weeks, or months).

26. Click the **Icons** tab if you want to change the Icon Set for this Locker Bank.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
27. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Locker Bank.
    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 Locker Bank.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
29. Click **OK** to exit and save your changes.
    Click **Apply** to save your changes and stay in this window.
    Click **Cancel** to exit without saving your changes.

Assigning an HBUS Terminal to a Third Party/OSDP Reader

1. Open the Properties window of the required Third Party/OSDP Reader, and click the **HBUS Terminal Display** tab.



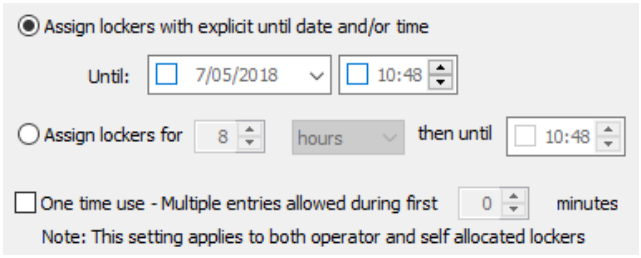
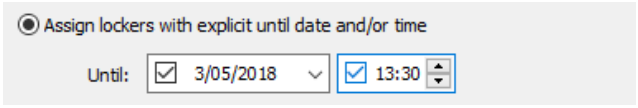
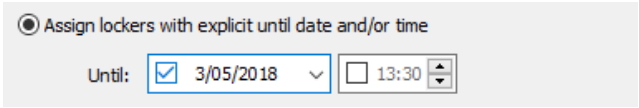
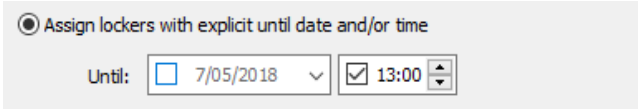
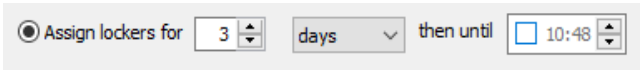
2. From the **HBUS Terminal** drop-down list, select the HBUS Terminal that is to display feedback from this Third Party/OSDP Reader.
3. Click **OK** to exit and save your changes.
4. To use this Third Party/OSDP Reader and HBUS Terminal for a Locker Bank, add both the Third Party/OSDP Reader and the HBUS Terminal to the **Readers** tab of the Locker Bank (refer to step 7 earlier in this topic).

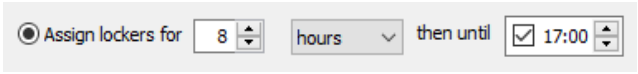
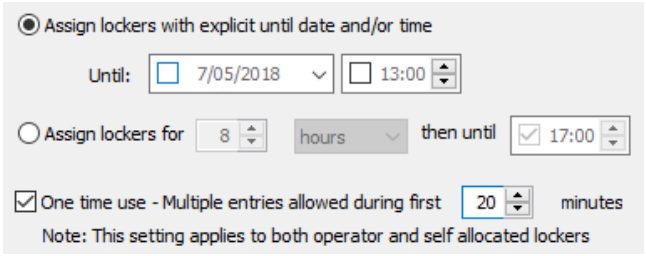
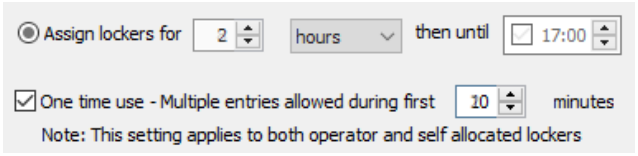
Result

- The Third Party/OSDP Reader can be used for reading third-party cards.
- The HBUS Terminal will display the Locker that the Cardholder has been assigned and when the Locker assignment will expire on its screen.

Note: The **First** option for the Locker Bank's **Access Credentials** must be set to **Card**, the **Second** option must be set to **None** (refer to step 12 later in this topic). Neither the Third Party/OSDP Reader or the HBUS Terminal will ever prompt for PIN/User Code.

Configuring a Locker Bank (Scenarios)

Scenario	Configuration / Explanation
Assign Lockers permanently (without an until date/time)	 The 'Until' date and time checkboxes are deselected. The 'One time use - Multiple entries allowed during first' checkbox is deselected.
Assign Lockers to end at a future explicit date and time	 Locker assignments will end at the configured date and time (i.e. on 3/05/2018 at 13:30).
Assign Lockers to end at a future explicit date	 Locker assignments will end at 23:59 on that explicit date (i.e. on 3/05/2018 at 23:59).
Assign Lockers to end at the next occurrence of an explicit time	 Locker is assigned until the next occurrence of the explicit time. Depending on the time of allocation, an assignment could be only for a few minutes or almost an entire day. E.g. If a Cardholder badges: • at 12:56 to assign a Locker, the Locker will be assigned for only a few minutes. • at 13:01 to assign a Locker, the Locker will be assigned for almost an entire day.
Assign Lockers to end in a specific number of minutes, hours, days, weeks or months	 In this example, the Locker is assigned for 3 days.

Scenario	Configuration / Explanation
Assign Lockers to end in a specific number of hours or days etc. and then at the next occurrence of an explicit time	 Locker is assigned for the configured period (i.e. 8 hours) plus the time until the next occurrence of the configured time (i.e. 17:00). Depending on the time of the allocation, the assignment period can vary. **E.g.** The first Cardholder is assigned a Locker at 08:58. This Cardholder's assignment will be for 8 hours and 2 minutes. The second Cardholder is assigned a Locker at 09:02. This Cardholder's assignment will be for 31 hours and 58 minutes. This is because the first assignment period (i.e. 8 hours) wasn't finished before the first occurrence of 17:00, therefore the assignment was extended till next occurrence of the 17:00.
Assign Lockers for one-time use - Multiple entries allowed during first xxx minutes	 Locker is assigned permanently however, once the one time use minutes have lapsed (i.e. after 20 minutes), and the Cardholder badges, the Locker opens (to allow the Cardholder to remove items) then it is removed from the Cardholder. **Note:** During the one time use period, the Cardholder can badge as many times as required without losing the Locker.
Assign Lockers for a certain period (i.e. 2 hours) but only for one-time use - Multiple entries allowed during first xxx minutes	 Locker is assigned for a maximum of 2 hours with 10 minutes of multiple entry time (the Cardholder can badge to use the Locker as often as required in the first 10 minutes). However, once this period is over, and the Cardholder badges, the Locker opens (to allow the Cardholder to remove items) then the Locker is removed from the Cardholder. Otherwise, the assignment will end after 2 hours.

Locker Bank Status and Overrides

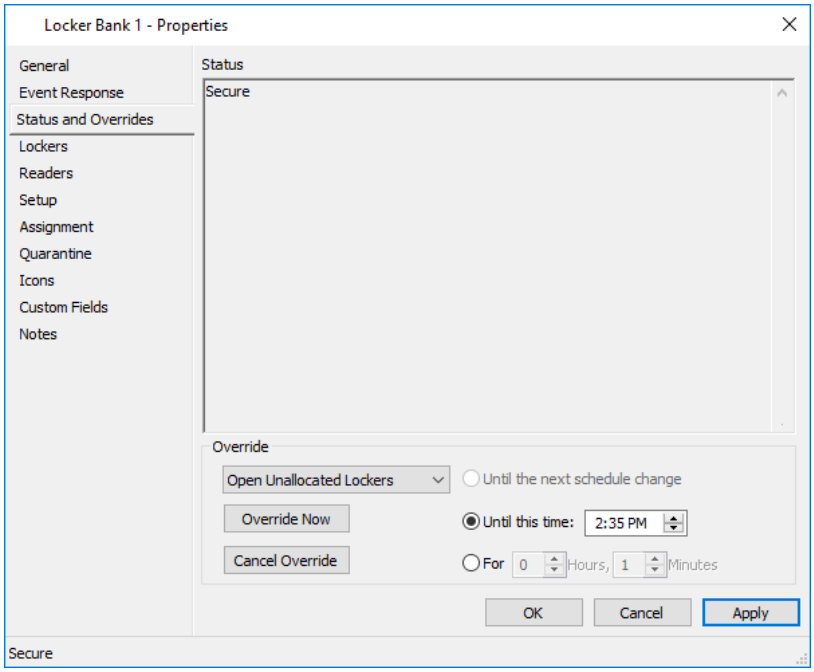
An Operator can perform the following overrides at the Locker bank level:

- Open Unallocated Lockers - Unlocks all unassigned Lockers (including quarantined Lockers)
- Cancel Override - Cancels the Unlock Unallocated Lockers override

Procedure

To override a Locker Bank, perform the following procedure:

1. From the Configuration Client menu, click **Configure** > **Lockers**.
   The Locker List Window displays.
2. Double-click on the appropriate Locker Bank.
   By default the **General** tab displays.
3. Click the **Status and Overrides** tab.



4. Select 'Open Unallocated Lockers' from the **Override** drop-down list. This includes quarantined Lockers.
5. 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, minutes and/or AM/PM.
6. Click the **Override Now** button.
7. Click **OK**.

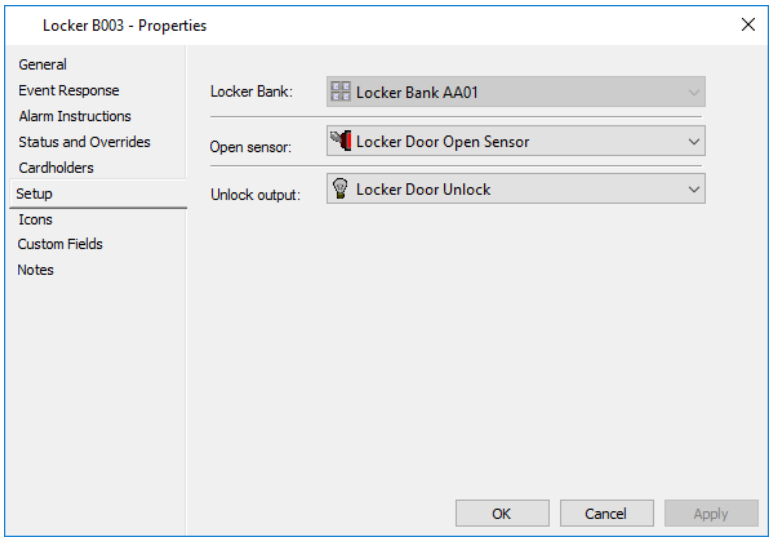
Configuring a Locker

If you need to configure a large number of Lockers, you can use the Bulk Configuration Tool. Refer to the *Bulk Configuration Tool* page on the Gallagher Security Hub for further detail:
https://resources.security.gallagher.com/Install,_Upgrade_and_Tools/Tools_and_Utilities/Bulk_Configuration_Tool

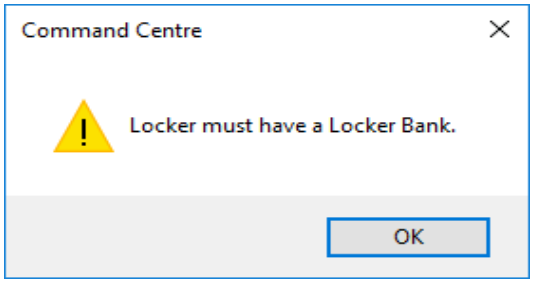
Note: An account is required to access the Security Hub, so register if needed.

Perform the following procedure to configure a Locker.

1. From the Gallagher Configuration Client main window, click **Configure** > **Lockers**.
2. Right-click and select **New...Locker.**
   The Locker Properties window opens to the **General** tab by default.
3. Complete the fields as required.
   For further details 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).
   Notes:
   - The Locker Bank Alarm Zone is assigned to the Locker automatically when creating a new Locker.
   - If you receive an *"Unable to save configuration as an Alarm Zone is required"* message, assign a primary Alarm Zone to the Locker and try again.
5. Click the **Alarm Instructions** tab, and configure as required.
   For further details see ***Alarm Instructions tab*** (on page 3-22).
   Notes:
   - The **Status and Overrides** tab shows the Locker status. Once the Locker is fully configured, you can override it by selecting Open Locker from the Override drop-down list.
   - The **Cardholders** tab is read-only, and it shows the current assignments.
6. Click the **Setup** tab.



7. Select a locker bank from the **Locker Bank** drop-down list.
   Note: You must select a Locker bank for a Locker. Otherwise, the *'Locker must have a Locker Bank'* error displays.



8. Select a sensor from the **Open sensor** drop-down list.
   Note: The Locker cannot verify if the assigned I/O is unique.
9. Select an output from the **Unlock output** drop-down list.
   Note: The Locker cannot verify if the assigned I/O is unique.
10. Click the **Icons** tab if you want to change the Icon Set for this Locker.
    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 Locker.
    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 Locker.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
13. Click **OK** to exit and save your changes.
    Click **Apply** to save your changes and stay in this window.
    Click **Cancel** to exit without saving your changes.

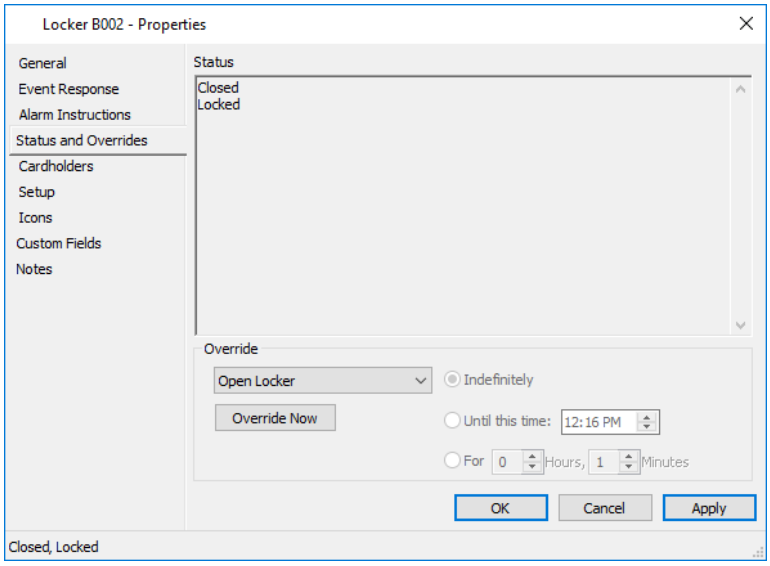
Locker Status and Overrides

Several overrides are available for Lockers on the 'Status and Overrides' tab.

Procedure

To override a Locker, perform the following procedure:

1. From the Gallagher Configuration Client menu, click **Configure** > **Lockers**. The Locker List Window displays.
2. Double-click on the appropriate Locker. By default the **General** tab displays.
3. Click the **Status and Overrides** tab.



4. Select the required override:

Override	Description
Open Locker	Unlocks the Locker so someone may access it.
Quarantine Locker	Puts the Locker into quarantined state. To be quarantined, a Locker must not be assigned to any Cardholder. When the Locker is quarantined, only Cardholders in an Access Group assigned to the Locker Bank's 'Quarantine' tab are able to open it via the Locker Bank's T20 Terminal. **Notes:** • If a 'Quarantine Locker' override is sent to the Locker while its Controller is offline, and a Cardholder also assigns that Locker to themself while the Controller is offline, the quarantine is canceled and the assignment remains when the Controller comes online. • If this Locker's Locker Bank item was last configured/ modified before the quarantine feature was added (i.e. in Command Centre 9.00 or earlier), you must right-click the Locker Bank item (in the Lockers list window) and select 'Push Configuration' in order for the 'Quarantine Locker' override to work.

5. Click the **Override Now** button.
6. Click **OK**.

Cancel an override

To cancel the active override, click the **Cancel Override** button on the 'Status and Overrides' tab.

Chapter 63: REST API

Introduction

The Gallagher Command Centre REST API defines a set of HTTP functions that allow developers to:

- create and monitor events
- manage Cardholders
- view the status of Command Centre items
- override Command Centre items.

Why use a REST API?

- A REST API uses HTTP to obtain data from different systems. It is independent of the language used by each system, hence it promotes longevity and evolution of both systems.
- A REST API provides superior integration performance. Sites can quickly and cost-effectively integrate third-party systems with Command Centre.

REST API features

The Command Centre REST API has the following features:

REST API feature	Requires the following licence string…
Events and Alarms	`RESTEvents=1`
Cardholders	`RESTCardholders=1`
Status	`RESTStatus=1`
Overrides	`RESTOverride=1`
Inbound Events	`RESTCreateEvents=1`

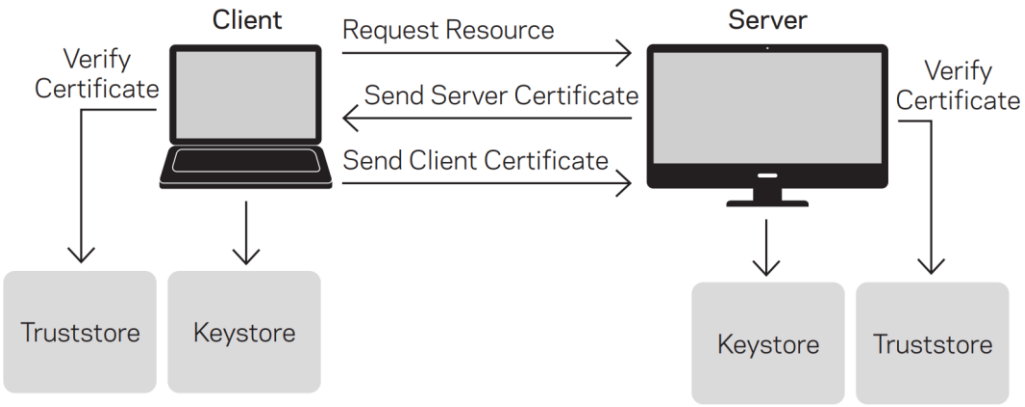
For further detail refer to:
https://products.security.gallagher.com/security/nz/en_NZ/products/software/interfaces/c/system_interfaces

REST API Security Features

Gallagher REST APIs provide the following security features:

- Privacy assured by HTTPS.
- Server authentication optionally assured with your site's own certificate.
- Client authentication assured with an API key, an optional client certificate, and optional IP filtering.
- Integration's visibility of data is restricted by Division and Operator Privileges.
- REST API call logging which provides the IP address of the computer that made the call, and the Certificate Common Name (CN) that made the call.

The following diagram illustrates REST API client/server authentication:



Configuration

Before using any Command Centre REST API feature, you need to perform the following procedures on the Configuration Client:

- ***Web Services*** (on page 6-32)
- ***Creating a REST API Client Item*** (on page 28-9)

Developer documentation

For detailed information on how to use the Gallagher Command Centre REST API, refer to the developer documentation and sample code stored at: https://gallaghersecurity.github.io/

Chapter 64: UK GovPass Card Support

Introduction

Command Centre supports UK GovPass cards. They are DESfire EV2 and are supplied with six key sets so that they can be rolled if required. The ability to roll the keys is in case one of the keys in use were to be discovered. Keys required for reading cards are loaded using a configuration card. Each configuration card also supplies the key used to read the next configuration card used to roll keys.

Note: If your site uses the Visitor Management application, from v9.00 the GovPass Card Type can be used as a Visitor Card Type. GovPass cards including Visitor/Contractor cards can be assigned to a visitor and once unassigned/ removed from the system those cards can be re-used on future visitors. Also, visitors with own GovPass card (belonging to a different department) can also be used to assign for the duration of their visit.

Licensing

UK GovPass card functionality is a licensable feature. The license file must contain the following option:

```
[Features]
UKGovPass=1
```

This chapter covers the following topics:

- ***Enrolling a UK GovPass configuration card*** (on page 64-2)
- ***Rolling configuration on a UK GovPass card*** (on page 64-5)
- ***Configuring and printing UK GovPass card layouts*** (on page 64-6)
- ***UK GovPass cards in Command Centre*** (on page 64-7)

Enrolling a UK GovPass configuration card

Introduction

A UK GovPass Card Type needs to be configured in the Configuration Client to be able to assign GovPass cards to Cardholders.

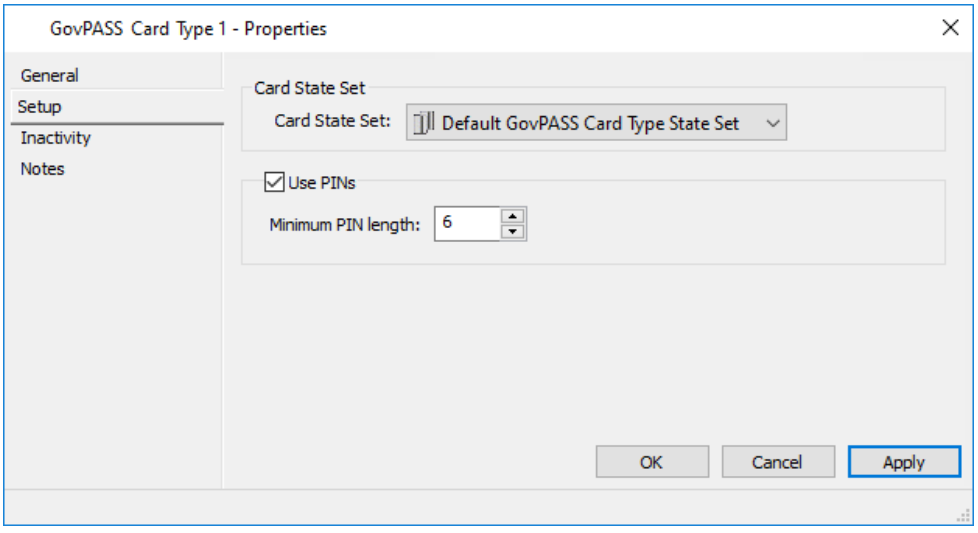
Notes:

- There is no limit to the number GovPass card flows and card types a site can have.
- The "Manage Keys" operator privilege is required to read the configuration card.
- The configuration data includes the keys that are required to validate the next configuration card if the site keys ever need to be rolled.
- GovPass Check is a service that maintains a record of every GovPass card's validity and enrolment history. If a site requires this service, the Command Centre service can connect to the GovPass Check service using the GovPass REST API, once the "Online Validation" section has been configured on the **Standards** tab (**GovPass** sub-tab) of the Server Properties.

Configuration

To configure a GovPass Card Type, perform the following procedure in Gallagher Configuration Client:

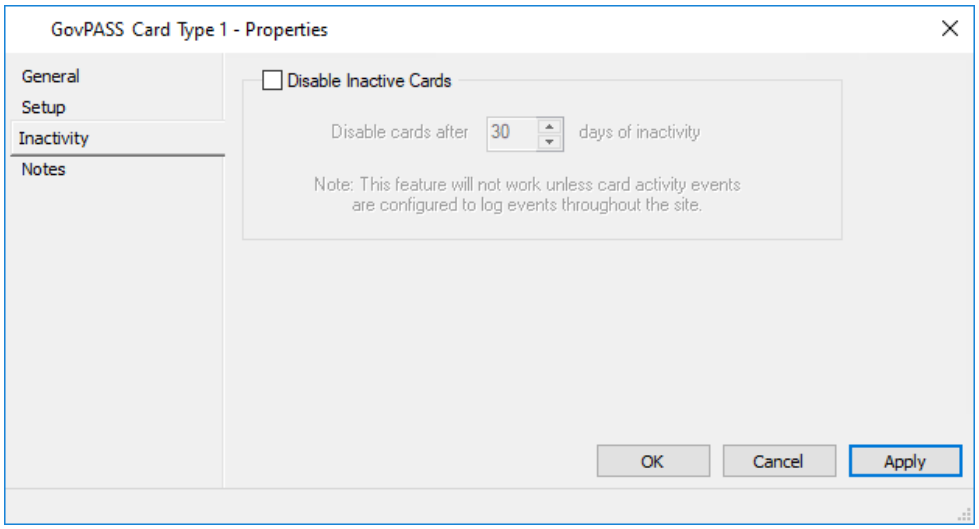
1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. **Right click** and select **New...GovPass Card Type**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Setup** tab.



5. Select the appropriate **Card State Set** (if only one exists it will default) to be associated with this GovPass card type, from the drop-down box.

Note: Once the Card State Set is assigned to the GovPass Card Type and saved, it cannot be changed.

6. If you want to use PINs, check the **Use PINs** checkbox and set the **Minimum PIN length**. (Default = 6 digits. Range = 4 - 8 digits)
   Notes:
   - If you do not choose to **Use PINs**, the **Assign PIN** button on the Cardholder Cards tile in Command Centre Client will be disabled.
   - The maximum PIN length is **8** digits. There is no mechanism to reduce the maximum size. Hence if a site sets minimum at 6, the user can enter PIN length anywhere from 6 to **8** digits.
7. Click the **Inactivity** tab.



8. Do you wish to enable the Inactive Card Expiry feature?
   Notes:
   - All cards of a particular type shall share a common inactivity timeout if enabled.
   - Cards that become disabled due to inactivity trigger an update of the card Enrolment State to 'Suspended' in the GovPass Check service.

If…	**then…**
yes	check the **Disable Inactive Cards** checkbox. Go to Step 9.
no	leave the **Disable Inactive Cards** checkbox unchecked. Go to Step 10.

9. Enter a figure to represent the number of days of inactivity that will disable a card.
   Notes:
   - When this feature is first enabled the default timeout = 30 days. The range is 1-999 days.
   - If you set a card type to disable after 1 day of inactivity, these cards will become disabled 24 hours to the second after the **Apply** button is clicked, (e.g. card type set on 27/01/2022 at 16:10:15; if not used these cards become disabled on 28/01/2022 at 16:10:15).

- 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.)

10. Click the **Notes** tab if you want to add a note(s) about the UK GovPass Card Type.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
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.

Result

A UK GovPass Card Type has been created.

Note: Once the configuration is saved it cannot be edited.

Rolling configuration on a UK GovPass card

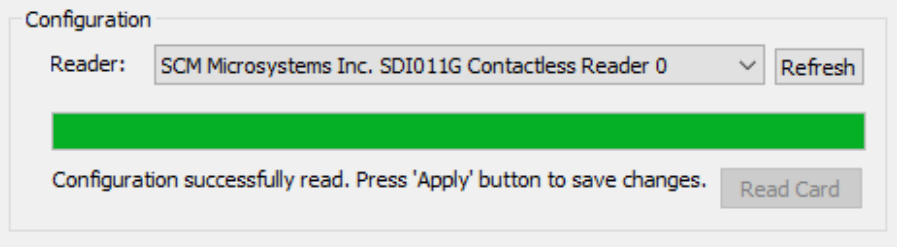
Introduction

If GovPass keys have been compromised they can be rolled by creating a new configuration card which is then reimported to Command Centre.
Note: Configuration on GovPass cards can be rolled a maximum of six times. After that, all cards would need reissuing.

This procedure describes how to update/modify the Configuration Key on a GovPass Card Type.

Configuration

1. Click **File** from the menu bar, then **Server Properties**. The Command Centre Server Properties List Window opens.
2. Click the **Standards** tab.
3. Click the **GovPass** sub-tab.
4. Present the correct card at the reader and click the **Read Card** button



Result

The system successfully reads the new configuration data, and once the **Apply** button is clicked the configuration is sent to the Controller(s).

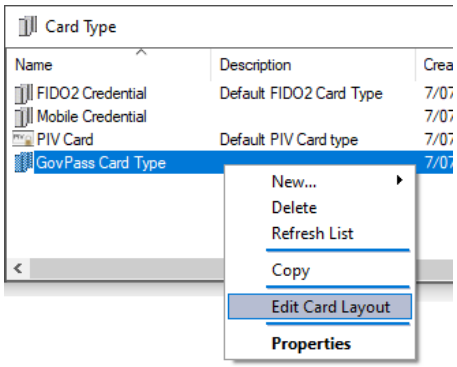
Important: The user must apply the changes.

Configuring and printing UK GovPass card layouts

An operator with the correct privileges can configure and/or print card layouts for GovPass cards.

Operator Privilege	is required to...
"Configure Site"	edit the GovPass card layout.
"Print/Preview & Encode Card"	print GovPass cards. **Note:** Card encoding is not supported for GovPass cards.
"Allow Re-Printing and Re-Encoding"	be able to re-print GovPass cards. **Note:** If you do not have this privilege and you attempt to re-print a GovPass card, the following warning message displays: *"The selected card details have already been printed."*

1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. **Right click** on the GovPass card, and select **Edit Card Layout**.



   The **Card Editor** window displays.
3. There are three objects you can add to the GovPass card layout, (i.e. Text, Image and Barcode).
   Go to the procedure that you require further detail on:
   - ***Adding Text*** (on page 47-20)
   - ***Adding an Image*** (on page 47-22)
   - ***Adding a Barcode*** (on page 47-24)
4. Click the **OK** button.
   The Card Editor window closes.
5. Print the GovPass card for cardholders as required, referring to ***Printing/ Encoding Cards*** (on page 47-55) for the procedure.

When a GovPass card is printed, an event is generated in the Event Viewer window. The event details:

- the card type and the card number
- who printed the card
- which cardholder had a card printed, and
- the reason for printing the card, if this has been configured

UK GovPass cards in Command Centre

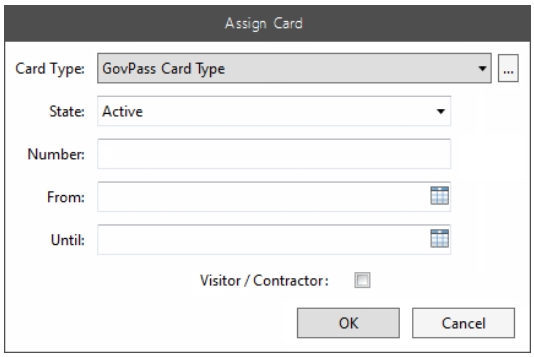
Introduction

After the GovPass Card Type has been configured in Configuration Client, GovPass cards can be assigned to a Cardholder in the Command Centre Client for the purpose of access control at T Series Readers.
Note: GovPass Cards can only be assigned to Cardholders from Command Centre Client, (i.e. not from Configuration Client).

Enrolling GovPass cards

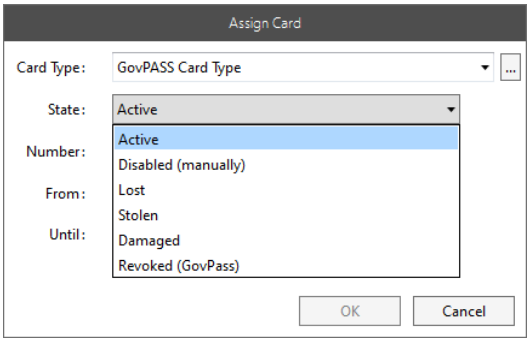
To assign and activate a Cardholder GovPass card, perform the following procedure in Gallagher Command Centre Client:

1. From the Cardholder Viewer, locate the Cardholder you want to assign a GovPass card to.
2. On the Cardholder Cards tile, click the **Assign Card** button.
3. From the **Card Type** drop-down list select the GovPass Card Type.



Once the GovPass Card Type is selected a **Visitor/Contractor** checkbox appears, allowing you to specify whether or not it is a visitor or contractor card.

4. The **State** indicates the status of the GovPass Card Type.
Select the appropriate **State** from the drop-down list.



The following table describes the available states.

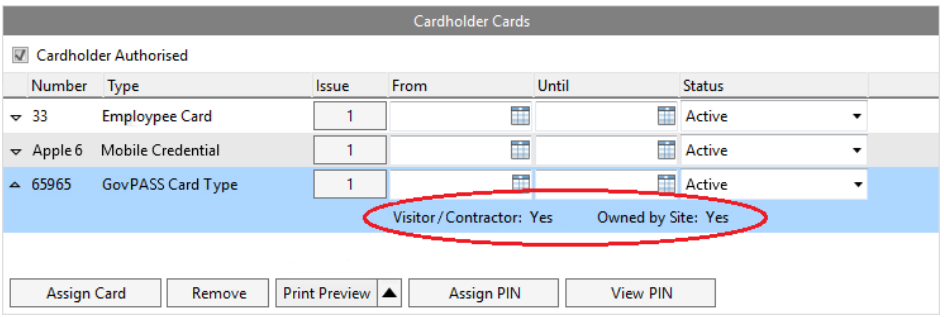
State	Description
Produced *	A GovPass card that has been encoded but not issued to a site. This should not occur at live sites, and will trigger an alarm.

State	Description
Active	An active GovPass card that can be enrolled at other locations.
Issued	A GovPass card that has been issued to a site but not yet enrolled for the first time.
BuildingOnly	This is reserved for GovPass cards allocated for use as 'Visitor' or 'Contractor' passes that should not be used for access to any other building. Cards enrolled with this state will trigger an alarm if not owned by the requesting building.
Lost *	The GovPass card has been reported as 'Lost' by its Issuing Building, and an alarm will be triggered.
Revoked *	When a GovPass card has been returned to the pass office or taken away from a user.
Expired *	Where the validity date of a GovPass card has expired, (i.e. the holder's clearance or contract has expired/ended).
Inactive *	This state is reserved for future use where a pass has been disabled. It will trigger an alarm.

* When a GovPass card is enrolled with a bad state, (i.e. *Produced*, *Lost*, *Revoked*, *Expired* or *Inactive*), the card will fail enrolment. An alarm will generate and the following error message will display:

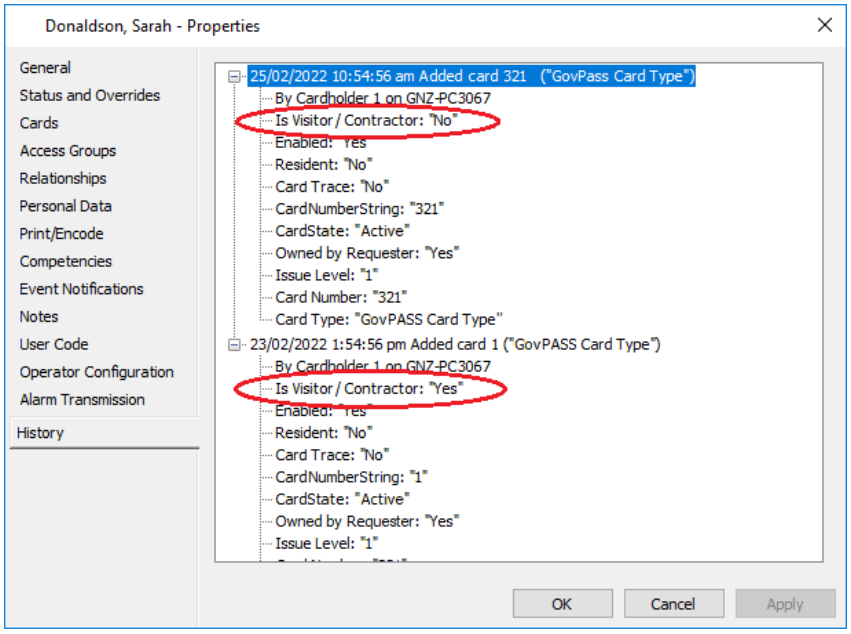


5. Configure the **Number**, **From** and **Until** fields as appropriate.
6. If required, check the **Visitor/Contractor** checkbox to prevent the card from being enrolled at other sites.
   Note: Cards of this type won't be enabled on other servers.
7. Click the **OK** button.
   Note: Once **OK** has been clicked, the **Visitor/Contractor** setting cannot be modified.
   If valid, the **Assign Card** pop-up will close and the card will appear in the grid in the Cardholder Cards tile.
8. To display site information for the GovPass Card Type, click on the arrowhead to the left of GovPass Card Type.



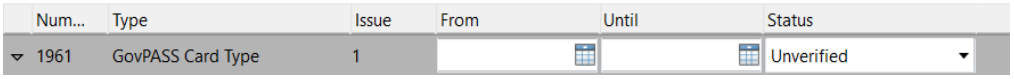
In the above example, "Visitor/Contractor" = Yes because the **Visitor/Contractor** checkbox was checked during enrolment, and "Owned by Site" = Yes the site that enrolled this card was identified as the owner of the card by the GovPass API.

9. Click the **Save** button.
   Note: The **History** tab of a cardholder's properties (in Configuration Client) will also show what has been set during enrolment.



Offline enrolment

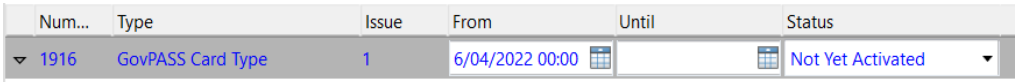
It is possible to enrol GovPass cards when GovPass Check service is offline to Command Centre. In this situation the card is activated and its status in Command Centre is updated to 'Unverified'. Also, an alarm is raised for this unverified credential enrolment.



Card Activation and Expiry

'From' date and card activation

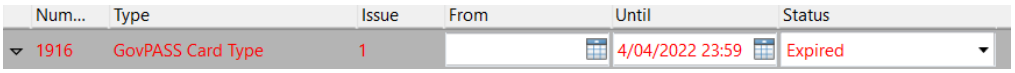
When the From date is set to a future date, the Command Centre Status changes to 'Not Yet Activated', but there will be no change to the card status or the enrolment status on the GovPass REST API.



When the system date passes the From date, the GovPass card Status becomes 'Active' in Command Centre, and the card status on the API updates to 'Active' and the enrolment status to 'Enrolled'. Also, an update enrolment status is sent to the API from the remote servers to 'Enrolled' state.

'Until' date and card expiry

When the Until date is set to expire in the future, the Command Centre Status will still be 'Active'. There will be no card status and enrolment status update on the GovPass REST API.

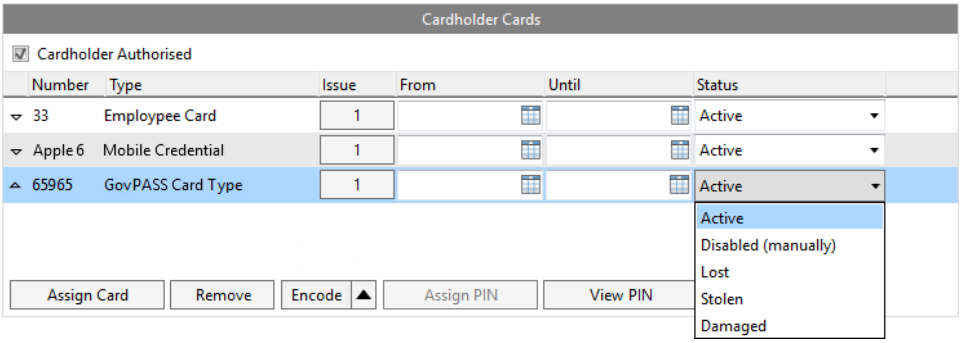


When the system date passes the Until date, the card Status updates to 'Expired' in Command Centre and there is no change to the card status on the API, but the enrolment status updates to 'Suspended'. Also, an update enrolment status is sent to the API from the remote servers to 'Suspended' state.

Updating the card state

The state of an enrolled GovPass card can be changed manually in the Cardholder Cards tile, as follows:

1. Click in the **Status** field of the GovPass card.
   A drop-down list of the available states displays.

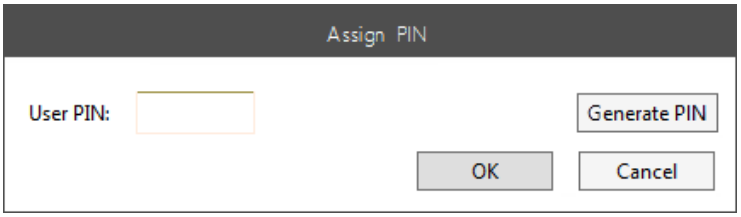


2. Select the required Card State from the drop-down list.
   The Status changes.
3. Click the **Save** button.

Assigning PINs

If the GovPass Card Type was configured to use PINs (in the Configuration Client), the **Assign PIN** button will be enabled.

1. Click the **Assign PIN** button.
   The Assign PIN pop-up displays.

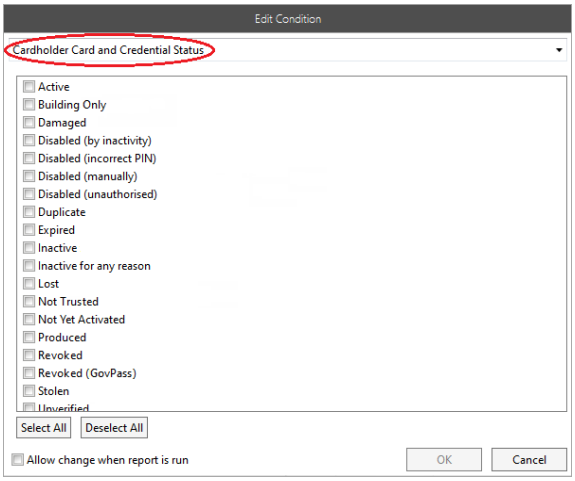


2. Either:
   - Manually type a PIN number into the first **User PIN** field, and then confirm it by repeating it in the second **User PIN** field, OR
   - Click the **Generate PIN** button to automatically generate a random PIN. **Note:** Generated PINs will only display while the Assign PIN window is open. Once closed, there will be no way of re-viewing the PIN number since the PIN itself is not stored. Generated PINs will be of length equal to the minimum PIN length set against the GovPass Card type.

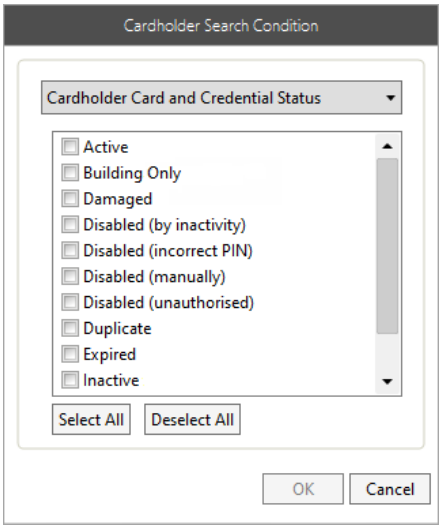
3. Click the **OK** button.
   The Assign PIN pop-up closes.
4. Click the **Save** button.

'Cardholder Card and Credential Status' Report Filter

Report Filter Conditions are configured when a report is created. When 'Cardholder Card and Credential Status' is selected as the **Condition Type** for a Cardholder or Activity Report filter, there are five additional states available in the list for sites licensed for GovPass. They are: 'Building Only', 'Inactive', 'Produced', 'Revoked (GovPass)' and 'Unverified'.



Note: These five additional states also appear when doing an "advanced search" for Cardholders in the Cardholder Viewer, (i.e. when setting the conditions to define the search on the Cardholder Search Condition pop-up and selecting 'Cardholder Card and Credential Status' as the **Condition Type**.



Chapter 65: Prepay Car Parking

Introduction

The Prepay Car Parking feature enables Command Centre to manage prepay Cardholder access to paid car parks. Benefits of the Prepay Car Parking feature are:

- One access card can be used for both building access and car park access, eliminating the need for multiple access cards.
- Caps a prepay Cardholder's car parking charge to one charge per defined period of time.
  A Cardholder can enter and exit the car park multiple times during the defined period of time.
- Provides full traceability of Cardholder car park entry and exit access.
- The Cardholder is charged based on their car park entry and exit events. The Cardholder must have parked a car for long enough to be considered for charging.

Licensing

Prepay Car Parking functionality is a licensable feature. The license file must contain the following option:

```
[Limits]
Prepay Car Parks=n
```

(where `n` is the number of Car Parks that can be created)

Notes:

- The number of Prepay Car Park Groups that can be created is not limited by the number of Car Parks that can be created.
- This feature is NOT supported in a Command Centre multi-server environment.

Operator Privileges

Privilege	is required to…
"View Car Parks and Sections"	view and find Prepay Car Park Group and Car Park items.
"Edit Car Parks and Sections"	view, find, create, edit, save and delete Prepay Car Park Group and Car Park items

Note: An operator with the "View Site" privilege is unable to view Prepay Car Park Group and Car Park items. An operator with the "Advanced User" privilege can view, find, create, edit, save and delete Prepay Car Park Group and Car Park items.

This chapter covers the following topics:

- ***Understanding the Prepay Car Parking feature*** (on page 65-3)
- ***Configuration examples*** (on page 65-4)
- ***Configuring the Prepay Car Parking feature*** (on page 65-5)
- ***Configuring a low credit warning signal*** (on page 65-14)

Understanding the Prepay Car Parking feature

How does Prepay work?

One of the following prepay options can be used:

Fixed periodic payment

A Cardholder pays a fixed amount of money for a defined period of time, (e.g. an amount is deducted from a Cardholder's salary/wage per month). The Command Centre operator then activates the Cardholder's Car Parking Competency for the defined period of time. The Cardholder can then access the paid car parks during the defined period of time.

Prepay

A Cardholder purchases car parking credits, (e.g. number of 'parks' allowed). The Command Centre operator then activates the Cardholder's Car Parking Competency and updates the Cardholder's limited credit amount. The Cardholder can then access the paid car parks, until their credit runs out.

When is the Cardholder charged?

A Cardholder is charged if:

- The Cardholder has the required Car Parking Competency, and
- The Cardholder has limited credit on the Car Parking Competency, and
- The Cardholder's car has stayed in the managed car parks for more than the free parking duration, and
- When the Cardholder exits the managed car parks, the Cardholder is found not having been charged within the previous 'charged parking duration' period.

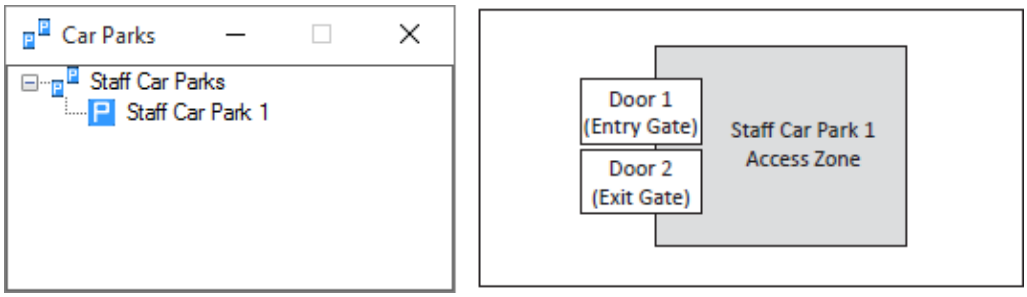
Limitations

- One Car Park can belong to one Car Park Group only. This restriction is not suitable for managing shared prepay car parks that may serve multiple tenant companies, where each company is charged differently.
  A car parking credit is a whole unit only. If cash value is to be used as credit, the value should be entered in the unit of cents.
- As long as a prepay Cardholder has the active car parking credit Competency, the Cardholder is allowed access to paid car parks even when the Cardholder does not have the minimum required car parking credit.
- For long stays, (e.g. one month), the Cardholder's Competency credit is deducted only once (the 'Credit to deduct' value) when the Cardholder exits the car park. The credit deduction event details, include a warning, indicating the stay time has been longer than the charged parking duration.

Understanding the Prepay Car Parking feature

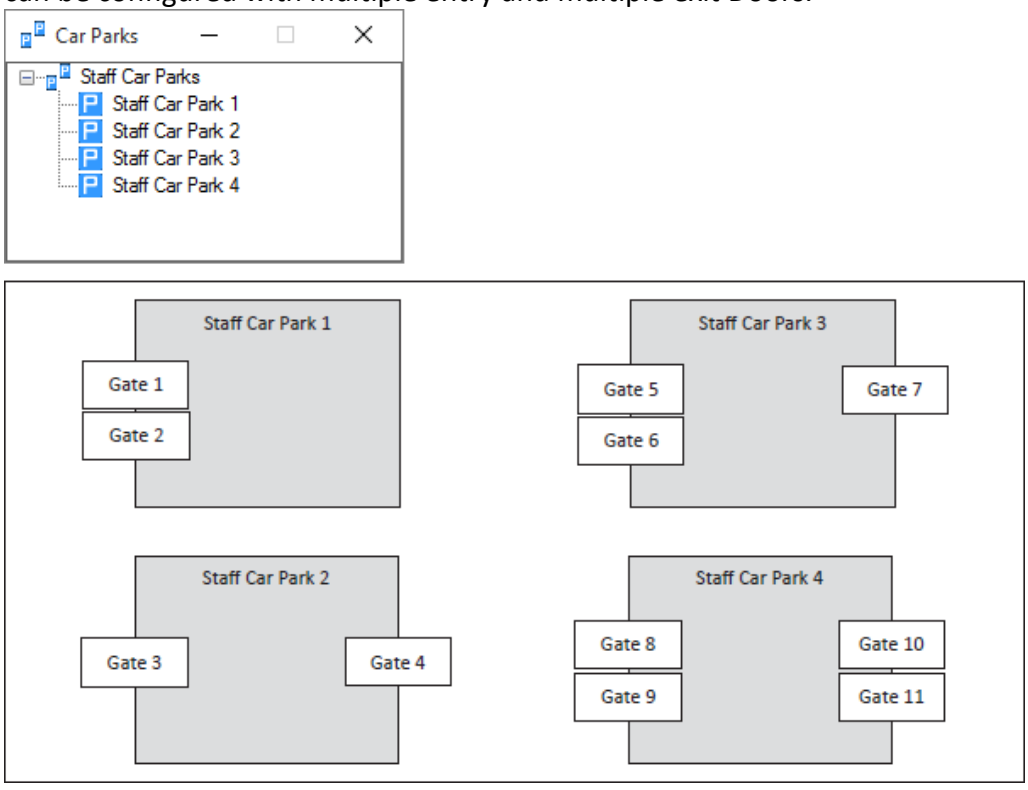
Single Car Park

The site configuration below shows one Car Park. This Car Park has been configured with one entry Door and one exit Door.
The configuration instructions in this release note document how to configure the site configuration, as shown below.



Multiple Car Parks

The site configuration below shows four Car Parks. If required, each Car Park can be configured with multiple entry and multiple exit Doors.



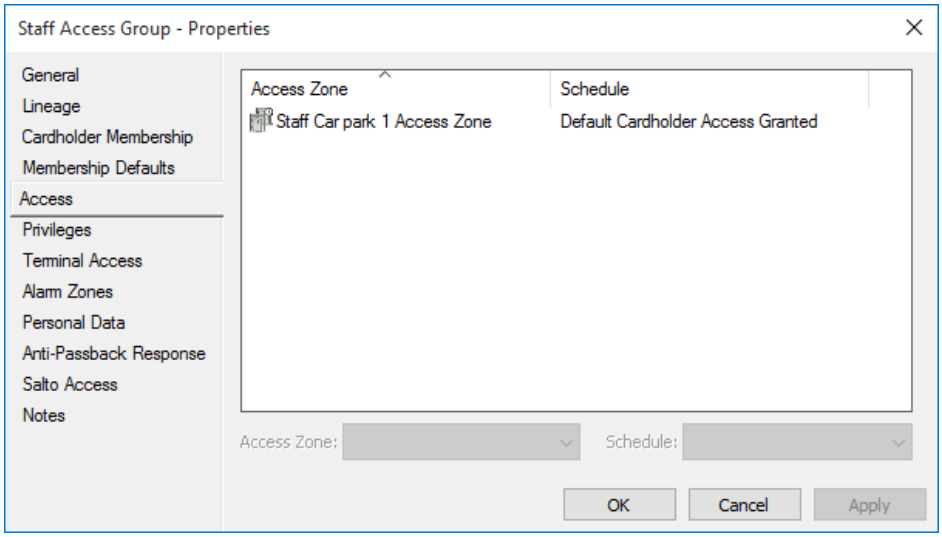
Note: In this configuration, the charging rate is the same regardless of which Car Park a Cardholder chooses to park.

Configuring the Prepay Car Parking feature

To configure the 'Prepay Car Parking' feature, perform the following procedures in Gallagher Configuration Client:

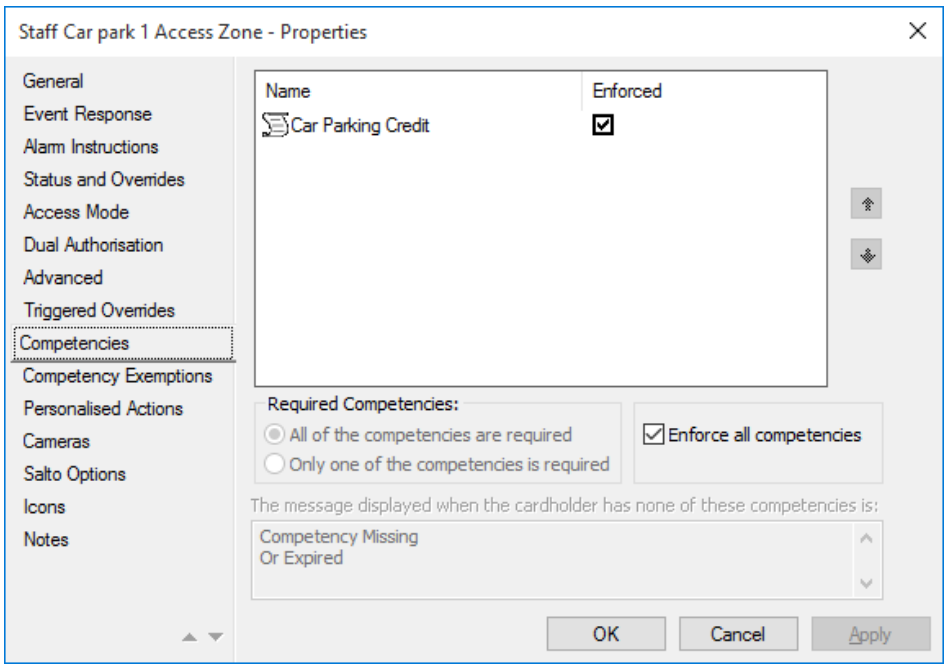
Configuring an Access Zone

1. Create the 'Staff Car Park 1 Access Zone'.
   Refer to the topic Adding a new Access Zone (on page 10-3) for the procedure.
2. Assign the 'Staff Car Park 1 Access Zone' to the Access Groups, for all Cardholders requiring access to this zone.
   Ensure the Schedule assigned allows access to this zone at all times.



Configuring a Competency

1. Create the 'Car Parking Credit' Competency.
   Refer to the topic Configuring Competencies (on page 52-5) for the procedure.
2. Assign the 'Car Parking Credit' Competency to the 'Staff Car Park 1 Access Zone'.
3. Enforce the 'Car Parking Credit' Competency. Cardholders will require the 'Car Parking Credit' Competency in order to access this zone.



Configuring Readers

1. Create the 'Door 1 Entry Reader'. A Cardholder is required to badge at the entry reader before entering the Car Park.
   Refer to the topic ***Creating Readers*** (on page 21-40) for the procedure.
2. Create the 'Door 2 Exit Reader'. A Cardholder is required to badge at the exit reader before exiting the Car Park.
   Note: Multiple entry and exit points can be configured for a single Car Park.

Configuring Doors

This topic describes how to configure an entry Door and exit Door for the Car Park. The entry Door will report entry events and the exit Door will report exit events.
Once assigned to a Car Park, these Doors will provide full traceability of Cardholder access in and out of the Car Park.
Notes:

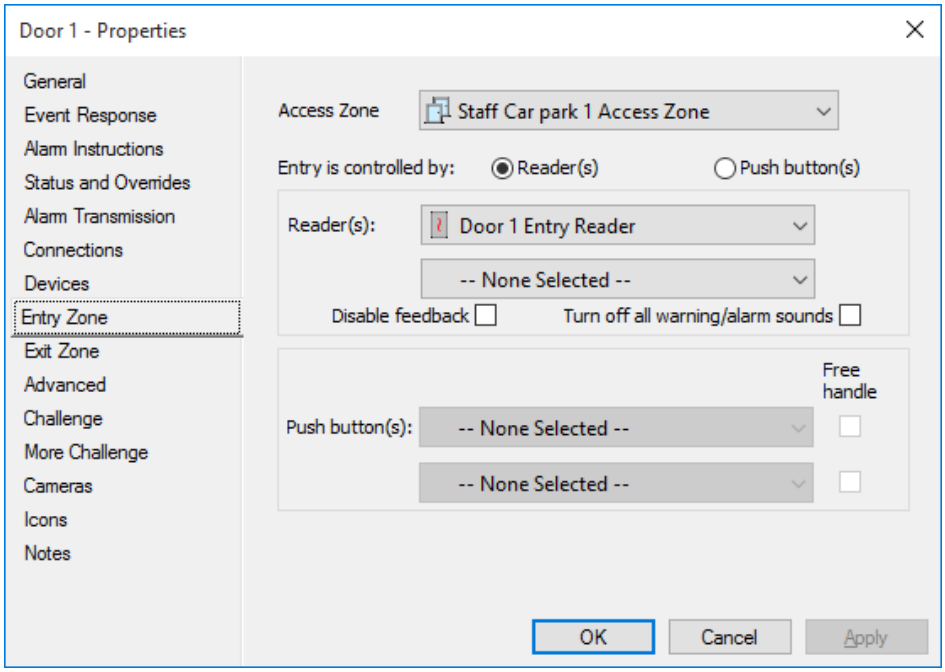
- A Door is required at each access point to operate the barrier arm.
- If required, a special Door (i.e. VIP Entrance) can be configured that allows access for specific Cardholders only. Create the Door. Assign a separate Access Zone as the entry zone for the Door. Allow only specific Cardholders access to this zone.

Configuring the entry Door

To configure the entry Door, perform the following procedure:

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

3. Type in the **Name**, **Description** and select the **Division**.
4. Click the **Event Response** tab, and assign a primary Alarm Zone for all events.
5. Click the **Connections** tab, and select the Controller that will host this Door.
   Note: Select the Controller with the majority of Door hardware assigned to it. It is preferable to have all Door hardware on the same Controller.
6. Click the **Devices** tab, and assign the appropriate Inputs and Outputs for the Door.
   For a description of each of the devices that can be assigned to the Door, refer to the topic ***Creating Doors*** (on page 22-2).
7. Click the **Entry Zone** tab.

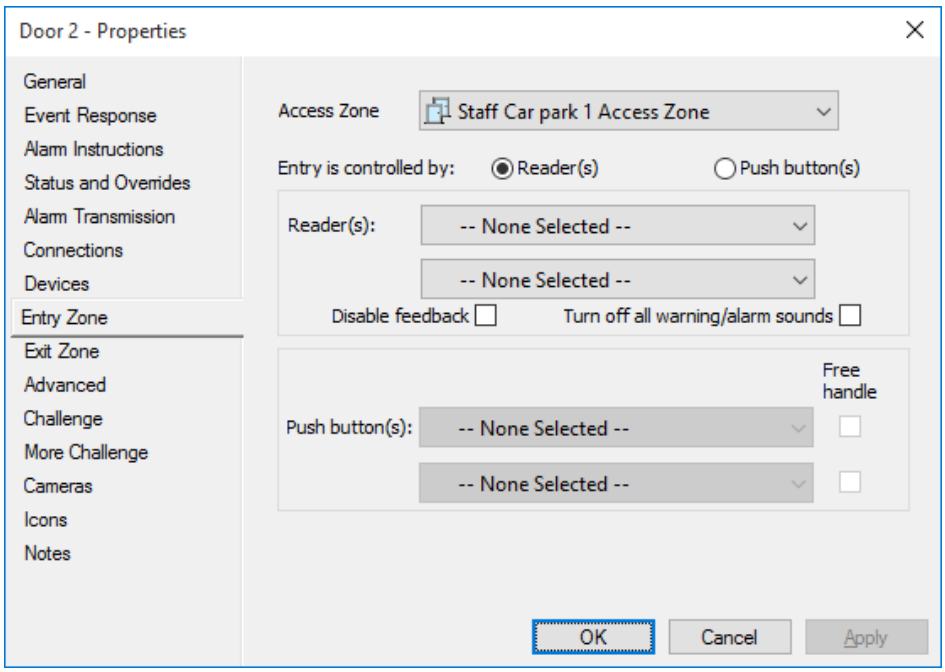


8. Select the the 'Staff Car Park 1 Access Zone' from the **Access Zone** drop-down list.
   Cardholders will enter into this Access Zone.
9. Select the **Reader(s)** radio button, to ensure entry is controlled by a reader.
10. Select the 'Door 1 Entry Reader' from the **Reader(s)** drop-down list.
    Entry will be controlled by this reader.
11. Click the **Icons** tab, and select the Standard Barrier Arm Icons Icon Set.
12. Click **OK** to exit and save your changes.
    Click **Apply** to save your changes and stay in this window.
    Click **Cancel** to exit without saving your changes.

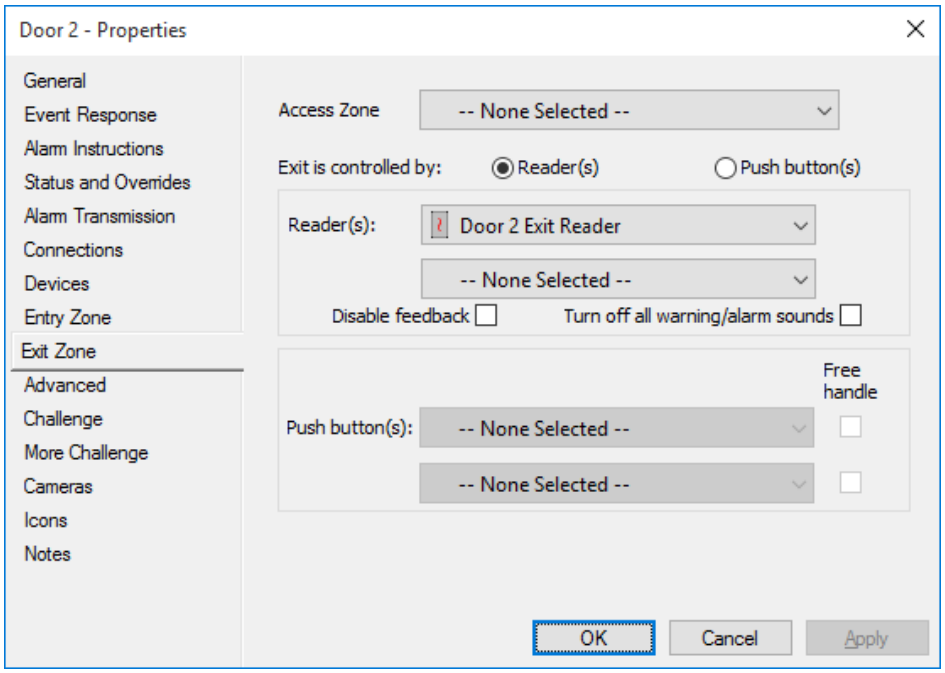
Configuring the exit Door

To configure the exit Door, perform the following procedure:

1. Repeat Steps 1-6 of the procedure above.
2. Click the **Entry Zone** tab and select the 'Staff Car Park 1 Access Zone' from the **Access Zone** drop-down list.



3. Click the **Exit Zone** tab and assign the 'Door 2 Exit Reader' as the exit reader for the Door, by selecting it from the **Reader(s)** drop-down list.

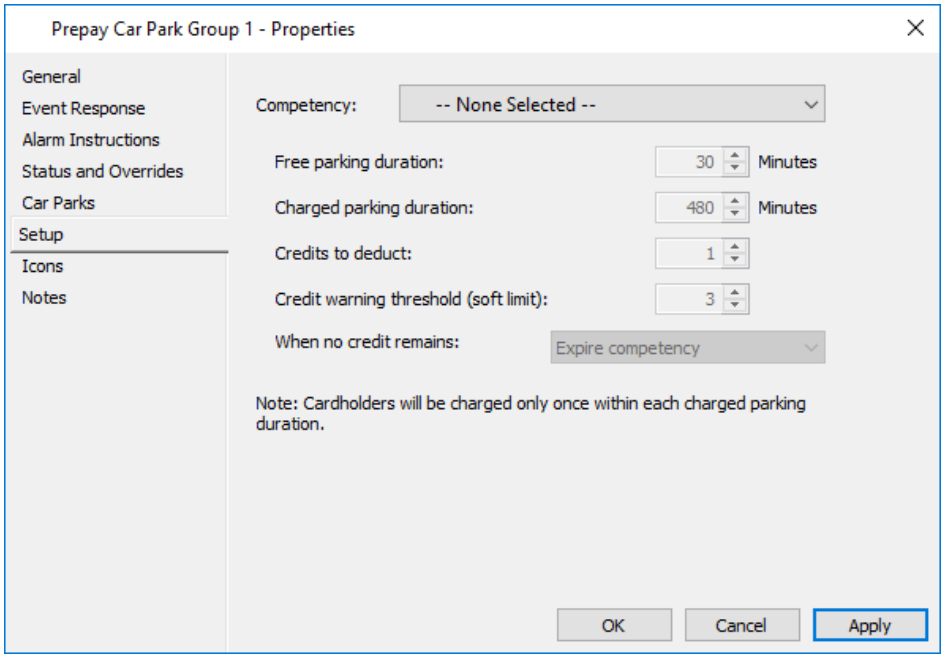


Note: An Exit Zone Access Zone is not required.

Configuring a Prepay Car Park Group

To configure a Prepay Car Park Group, perform the following procedure in Gallagher Configuration Client:

1. From the Gallagher Configuration Client main window, click **Configure** > **Car Parks.**
   The Car Parks List Window displays.
2. Right-click and select **New...Prepay Car Park Group.**
   The Prepay Car Park Group Properties window opens to the **General** tab by default.
3. Complete the fields as required. For further details see General tab (on page 3-18).
4. Click the **Setup** tab.



5. Select the 'Car Parking Credit' Competency, from the **Competency** drop-down list.
   If a Competency is not selected, then credit deduction does not apply to this group.
6. Enter the Free parking duration. (Default = 30 minutes. Maximum = 99 minutes)
   If the duration between the time a car enters a Car Park and the time the car exits the same Car Park is no longer than the free parking duration, the Cardholder is not charged.
   For example, if a Cardholder enters a Car Park but cannot find a car park slot, the Cardholder can exit the Car Park immediately without being charged.
7. Enter the **Charged parking duration**. (Default = 480 minutes [8 hours]. Maximum = 9999 minutes)

This is the period of time a Cardholder will be charged x credits.
Notes:

- A Cardholder may enter and exit the Car Parks belonging to the same group freely within this duration without being charged multiple times.
- If a Cardholder exceeds the charged parking duration time, the Cardholder will be charged again.

8. Enter the **Credits to deduct**. (Default = 1 credit. Maximum = 9999 credits)

   This is the credit to deduct after the free parking duration time has passed since the car entered any of the Car Parks belonging to the group.
   Note: If the Command Centre Services are offline, Cardholders may not be immediately charged (credit deducted upon exit event) for car parking. The Cardholder will be charged when the services are restored.

9. Enter the **Credit warning threshold (soft limit)**. (Default = 3 credits. Maximum = 9999 credits)

   Each time a Cardholder is granted access to a Car Park, if the Cardholder's credit is at or below this threshold, a visual signal can be turned on to warn the Cardholder that their credit is low.

10. Select the action to take after a Cardholder runs out of credit, from the **When no credit remains** drop-down list. When a Cardholder's credit reaches zero the selected action occurs.
    Selectable actions are:

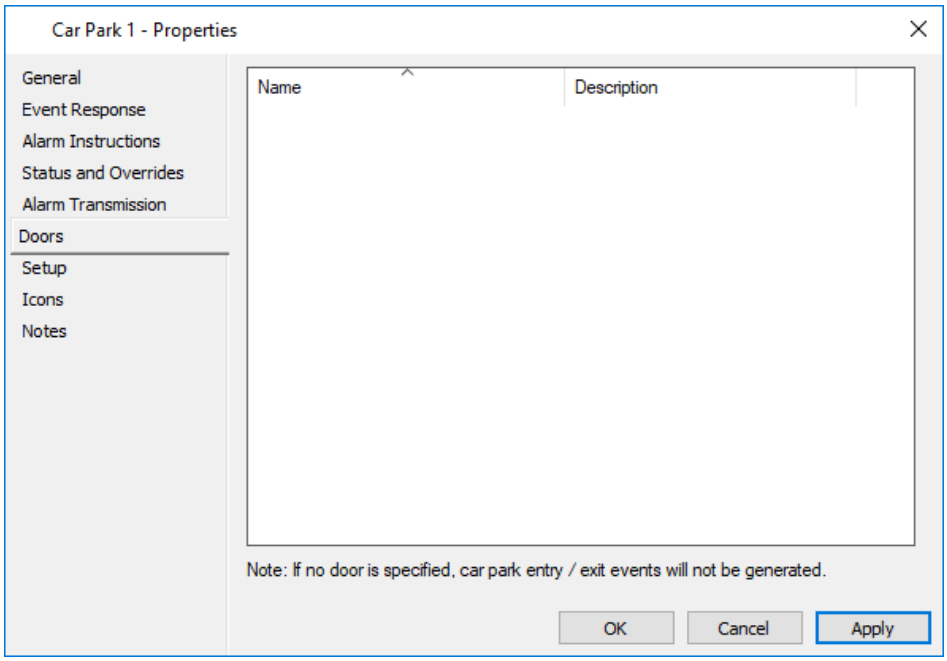
    - **No action**
      It is strongly recommended that you select this action if the 'Staff Car Park 1 Access Zone' enforces the 'Car Parking Credit' Competency. Otherwise, cars may queue behind a Cardholder who has been denied access.
    - **Expire competency**
      The Competency expiry date and time will be set to the date and time of when the Cardholder exits a Car Park Group, and credit was deducted, and the credit reaches zero.
    - **Disable competency**
      The Competency will be disabled. The expiry date and time for the Competency will remain, as previously configured. Hence if the Competency is re-enabled, the expiry date and time may still be valid.

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

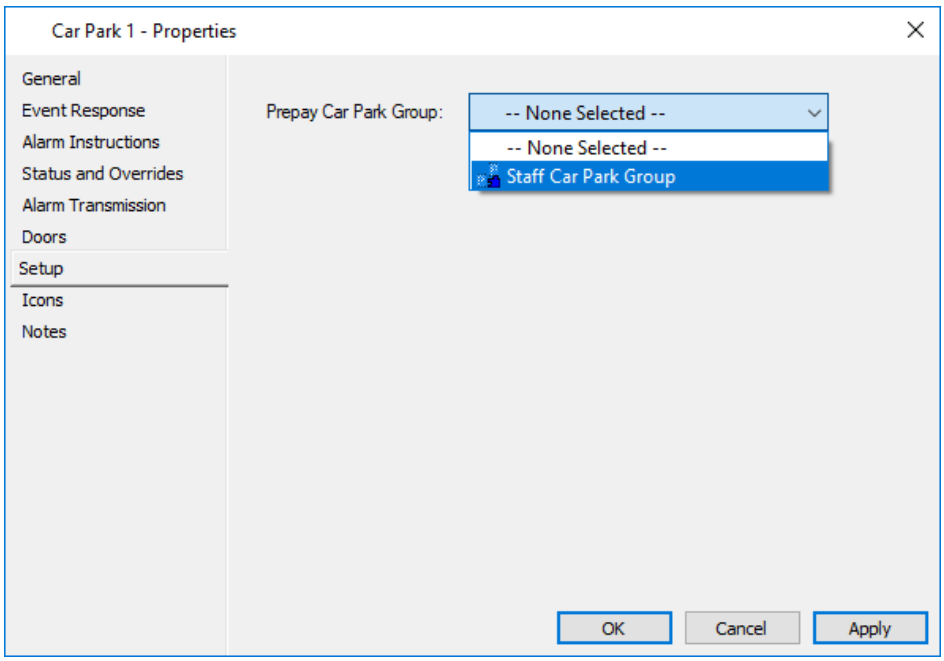
Configuring a Car Park

To configure a Car Park, perform the following procedure in Gallagher Configuration Client:

1. From the Gallagher Configuration Client main window, click **Configure** > **Car Parks.**
   The Car Parks List Window displays.
2. Right-click and select **New...Car Park.**
   The Car Park Properties window opens to the **General** tab by default.
3. Complete the fields as required. For further details 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 **Doors** tab.



6. Drag and drop the Doors that will be used as entry and exit points for this Car Park into the grid.
   Notes:
   - Each Door can be assigned to only one Car Park.
   - If no Doors are assigned to this Car Park, no Car Park entry or exit events will be reported.
   - An entry access granted event at one of the Doors listed in the grid, indicates the Cardholder is in the Car Park. An exit event at one of the Doors listed in the grid, indicates the Cardholder is no longer in the Car Park.
7. Click the **Setup** tab.

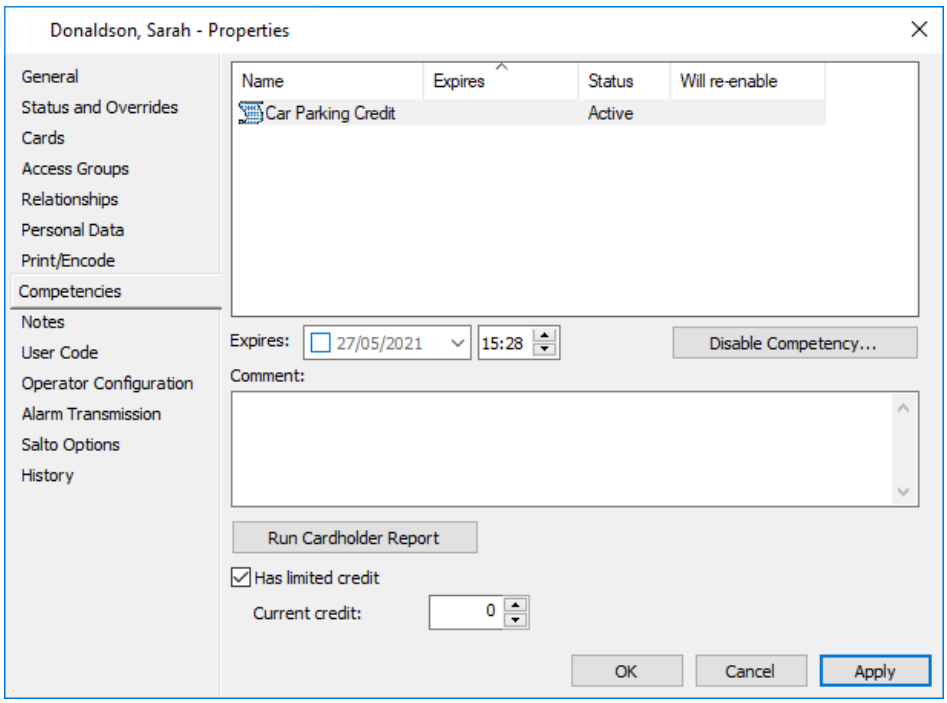


8. Select the Car Park Group you want to assign this Car Park to, from the **Prepay Car Park Group** drop-down list.
   Notes:
   - A Car Park that does not have a Prepay Car Park Group assigned does not belong to any Car Park Group, thus it does not have the credit deduction related functionality provided by the Car Park Group.
   - A Car Park that does not have a Car Park Group assigned will not log any entry or exit events.
9. Click **OK** to exit and save your changes.
   Click **Apply** to save your changes and stay in this window.
   Click **Cancel** to exit without saving your changes.

Configuring Cardholder Access

To configure Cardholder access for Prepay Car Parks, perform the following procedure in Gallagher Configuration Client:

1. From the Gallagher Configuration Client main window, click **Manage** > **Cardholders.**
   The Cardholder List Window displays.
2. Right-click on the required Cardholder and select **Properties.**
3. Click the **Competencies** tab.



Note: In order to view the current credit for the Cardholder, ensure you select the 'Car Parking Credit' Competency.

4. Assign the 'Car Parking Credit' Competency to the Cardholder. Ensure the Competency status is set to 'Active'.
5. To configure limited credit for this Competency, check the **Has limited credit** checkbox.
6. Enter the Cardholder's credit into the **Current credit** field.
   Notes:
   - Operator changes to a Cardholder's car parking credit is logged by Command Centre operator events. Thus a Cardholder's car parking credit change history can be retrieved from Command Centre when required.
   - The current credit may be a negative value, indicating the Cardholder is in debt.
7. Click **OK** to exit and save your changes.
   Click **Apply** to save your changes and stay in this window.
   Click **Cancel** to exit without saving your changes.

Configuring a low credit warning signal

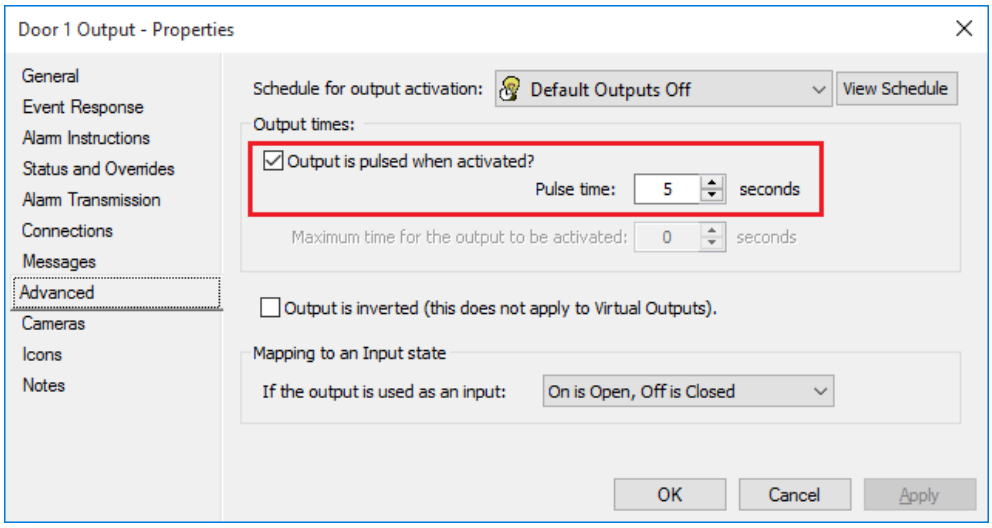
After a prepay Cardholder is granted entry access to a Car Park that requires car parking credit, if the Cardholder's car parking credit is at or below the configured threshold, a warning event is generated.
This warning event can be used to activate a visual warning signal, (e.g. a red light located near the entry reader to the car park) to warn the Cardholder of their low credit status.
Note: The warning signal does not decrease the Cardholder's car parking credit.

Using the Notifications feature of Command Centre

In addition to a warning signal, you can configure the Notifications feature of Command Centre to send a text message and / or email (when the warning event is generated) to the car park manager.
Refer to ***Notifications*** (on page 6-48) for details about this feature.
To configure a warning signal, perform the following procedures in the Configuration Client:

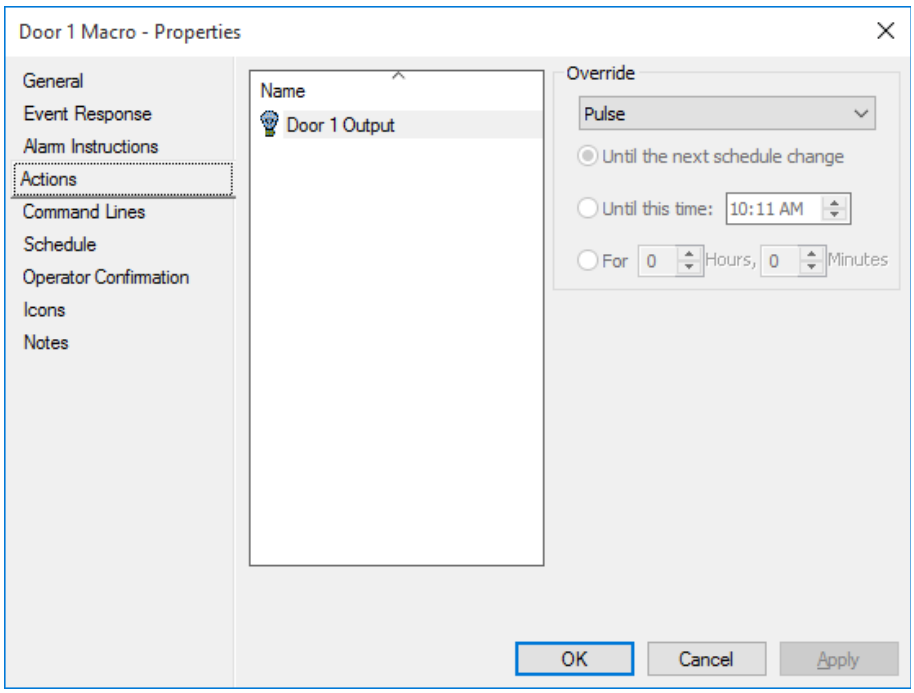
Creating an Output

Create the Output (warning signal) that will activate after a prepay Cardholder is granted entry access to a Car Park that requires car parking credit, if the Cardholder's car parking credit is at or below the configured threshold.
You will need to ensure the Output is set to 'Pulse' when activated.



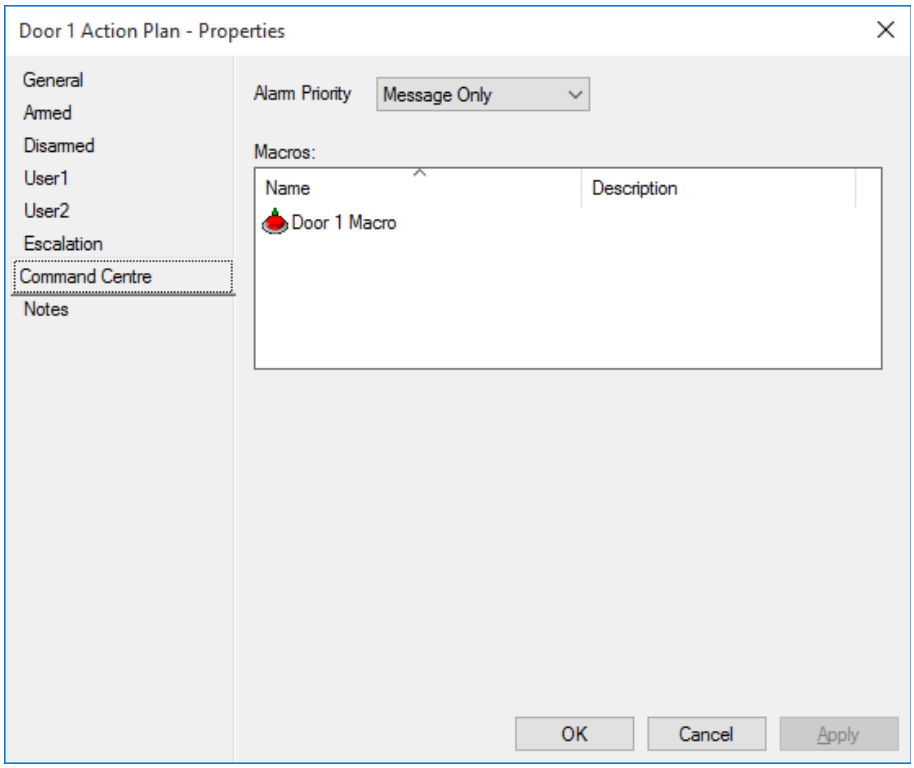
Creating a Macro

1. Create the Macro that will trigger the Output to activate.
2. Click the **Actions** tab.
3. Drag and drop the Output into the **Name** grid.
4. Select the Output in the **Name** grid and select Pulse from the **Override** drop-down list.



Creating an Action Plan

1. Create an Action Plan to trigger the Output.
2. Click the **Command Centre** tab.
3. Specify the priority of events or alarms generated, from the **Alarm Priority** drop-down list.
   When an event occurs the response will be of this priority.
4. Drag and drop the Macro to be triggered, into the **Macros** grid.

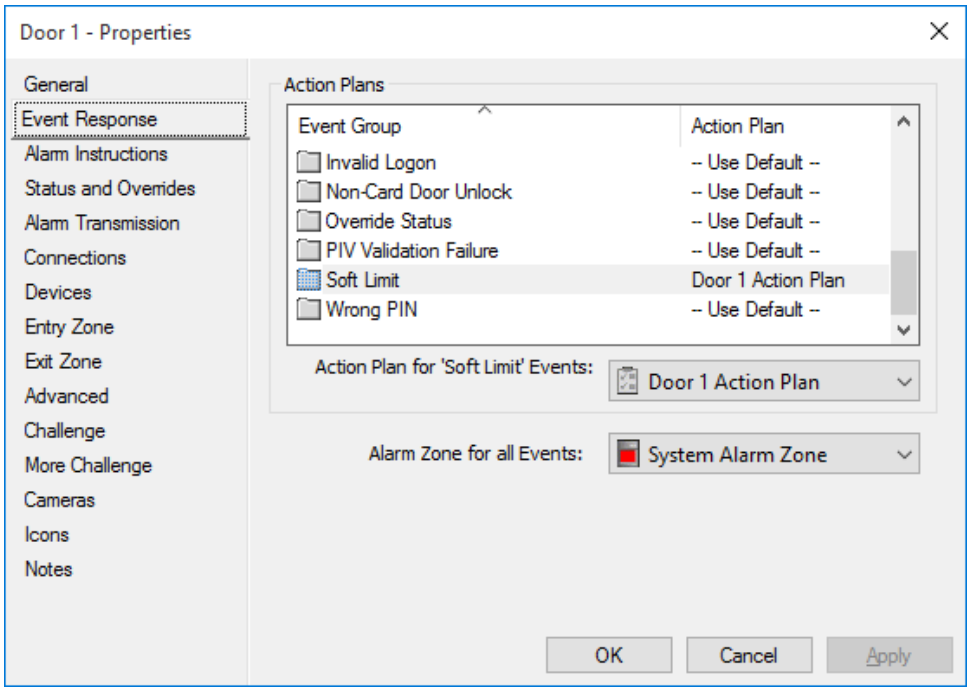


Assigning the Action Plan to a Door

Assign the Action Plan to the 'Soft Limit' Event Group on the entry Door to the Car Park.

When a 'Soft Limit' event occurs at the Door, the Output for this Door will be activated via the Action Plan and Marco.

Note: If required you can assign an Alarm Instruction to the 'Soft Limit' Event Group. *For example*, the Alarm Instruction may instruct the operator to warn the Cardholder of their low credit status.



Chapter 66: Tag Tracking

Introduction

The Tag Tracking feature ais intended for tracking the location of participating Cardholders. Tag Tracking has not been designed for anti-theft functionality, or for scenarios where the tag holder may attempt to obscure their location.

The Tag Tracking feature allows you to assign iBeacon and Eddystone Bluetooth™ 'tracking tags' to Cardholders. A Cardholder's Bluetooth™ tracking tag can be read by Gallagher T-Series Bluetooth™-capable Readers to update the Cardholder's location when they pass near a Reader. Command Centre Tracking Tag Types (like Card Types) are required for you to assign new tracking tags to Cardholders. Tracking tags can only be assigned to Cardholders in the Command Centre Client.

Warning: Gallagher recommends you do **not** use tracking tags for physical access into secure areas because tags can be easily copied, and the communication from tags to Readers is not encrypted, authenticated, or guaranteed.

Licensing

Tag Tracking is a licensable feature. You must purchase the following licence to configure tracking tags in Gallagher Command Centre:

```
[Limits]
TrackingTags=X
```

Where `X` is the maximum number of tracking tags that can be assigned across your Command Centre system. Once the maximum has been reached, no more tracking tags can be assigned until one or more are removed.

Considerations

Item	Consideration
Access Control	Gallagher recommends you do **not** use tracking tags for access control or for any security purposes.
Surrounding environment	Environments with metal obstructions or high amounts of Bluetooth™ noise can impact how efficiently tracking tag advertisements are received by Readers.
Reader positioning	Readers must be positioned far enough apart that a tag is read by the correct reader, (i.e. the reader that will update the Cardholder's location to the zone they are entering).
Access Decisions	When a Cardholder's tracking tag is read at a Reader, an access decision is made and the Cardholder's location is updated.

Item	Consideration
Supported Access Modes	Tracking tags require the Access Mode of the entry zone to be 'Secure - No PIN', 'Code or Card - No PIN', or 'Free - No PIN'. PIN and Dual Auth Access Modes are not supported. In 'Secure - No PIN' and 'Code or Card - No PIN' modes, a Cardholder's location is only updated if access is granted. In 'Free - No PIN' mode, an access granted decision is not required for the Cardholder's location to be updated; Access Group membership, Competencies, and tracking tag status are ignored.
Unlocking Doors with tracking tags	If using tracking tags to unlock physical doors (not recommended), note that: • Cardholders may unlock Doors from a considerable distance without realising. • A Door may be unlocked by one of a group of Cardholders, and it is not clear to the group which one of them was granted access. • If a Cardholder unlocks a Door but does not enter before the Door re-locks, the Cardholder needs to move outside the range of the Door's Readers before they can unlock it again. Or, the Cardholder can unlock the Door with a different credential (e.g. a card).
Enabling/ disabling tracking tags for Doors	You can disable a Reader from letting tracking tags unlock a Door - while still tracking their location - by not assigning an 'Unlock output' to the Reader's Door. However, this will disable all credential types (e.g. cards, Mobile Credentials) from unlocking that Door. You cannot disable tracking tags from unlocking a Door while allowing other credential types to unlock that Door.

Card Expiry

The 'card expiry' feature allows the life of a tracking tag to be specified by defining a 'From' time and date as well as an 'Until' time and date. Tracking tags with these defined are therefore enabled between those two points in time. When that time has passed, they are expired due to 'Scheduled Card Expiry'.

The 'Inactive Card Expiry' feature provides an additional way that tracking tag expiry can be defined. Inactive Card Expiry enables the automatic disabling of tracking tags, invoked after a period of tracking tag inactivity, within a Command Centre controlled site. The period of inactivity is configured on the Tracking Tag Type item.

Select the item below that you require further detail on:

- ***Configuring the Tag Tracking feature*** (on page 66-3)
- ***Setting up Tracking Tag Types*** (on page 66-8)

Note: Tracking tags can only be assigned to Cardholders in Gallagher Command Centre Client. Refer to the topic *"Tag Tracking tags in Command Centre"* in the Gallagher Command Centre Online Help.

Configuring the Tag Tracking feature

Introduction

This procedure covers what you need to configure for the Tag Tracking feature.
Note: The 'Configure Site' operator privilege is required to perform this procedure.

Configuration

To set up your site for Tag Tracking, perform the following procedures in Gallagher Configuration Client:

Configuring Card Technology settings

To enable…	See procedure…
individual Gallagher T-Series Readers (i.e. only some Readers) to read tracking tags,	*"Enabling tracking tags per Reader"*
Gallagher T-Series Readers to read tracking tags by default for your whole site (not recommended),	*"Enabling tracking tags for your whole site"*

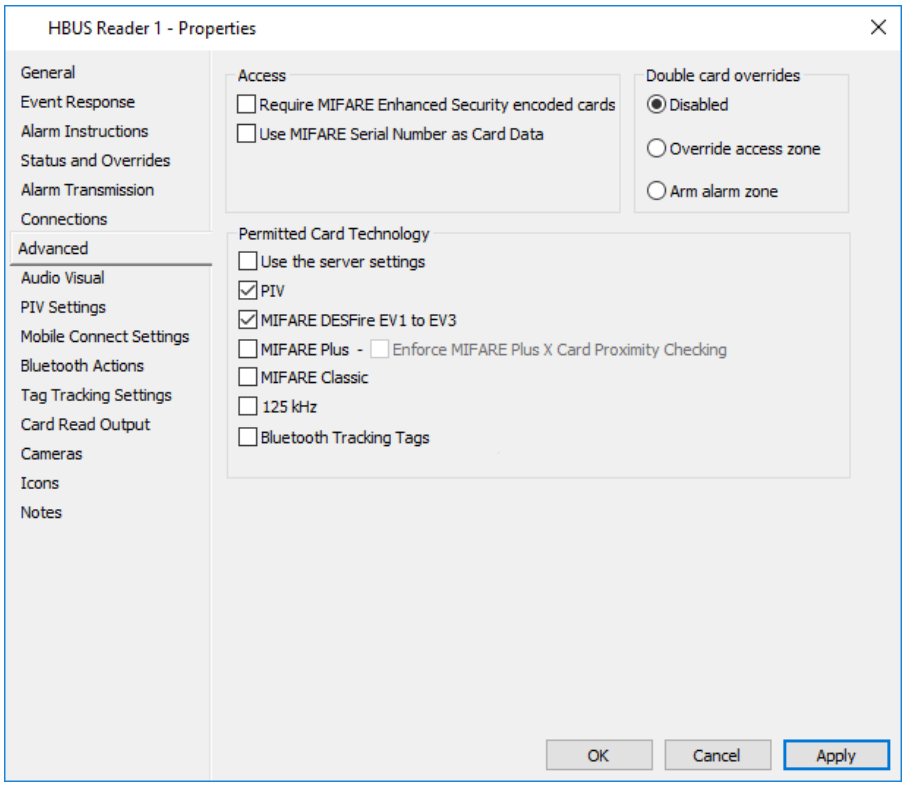
Enabling tracking tags per Reader

To enable individual Gallagher T-Series Readers (i.e. only some Readers) to read tracking tags, perform the following procedure:

a) Click **Configure** from the menu bar, then **Hardware**.
The Hardware List window opens.

b) Open the properties of the Gallagher T-Series Reader(s) that you wish to enable to read tracking tags.

c) Click the **Advanced** tab.



d) If the **Use the server settings** checkbox is checked, the Reader will use the configuration as specified on the Server Properties. See *"Enabling tracking tags for your whole site"* below to set the card technology server settings.

e) To configure permitted card technology specific to this Reader, deselect the **Use the server settings** checkbox and select the **Bluetooth Tracking Tags** checkbox.

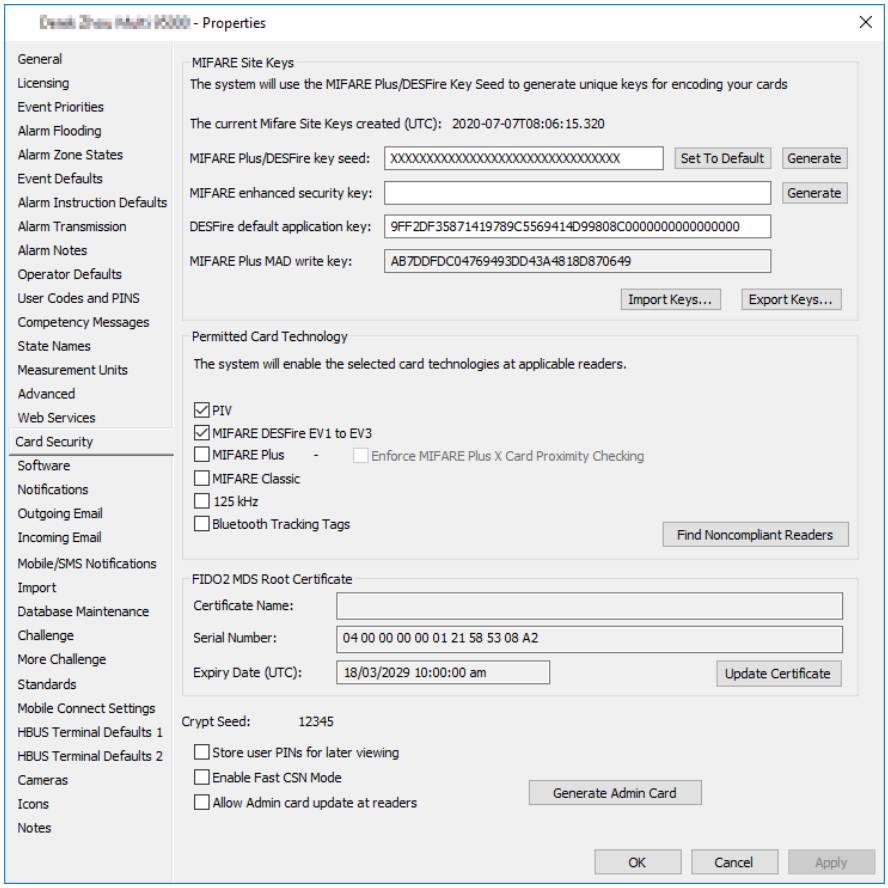
f) Click **OK** to close and save your changes.

Enabling tracking tags for your whole site

To enable Gallagher T-Series Readers to read tracking tags by default for your whole site (not recommended), perform the following procedure:

a) Click **File** from the menu bar, then **Server Properties**.
The **Server Properties** window opens.

b) Click the **Card Security** tab.



c) In the 'Permitted Card Technology' section of this screen, select the **Bluetooth Tracking Tags** checkbox.

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

Configuring Reader settings

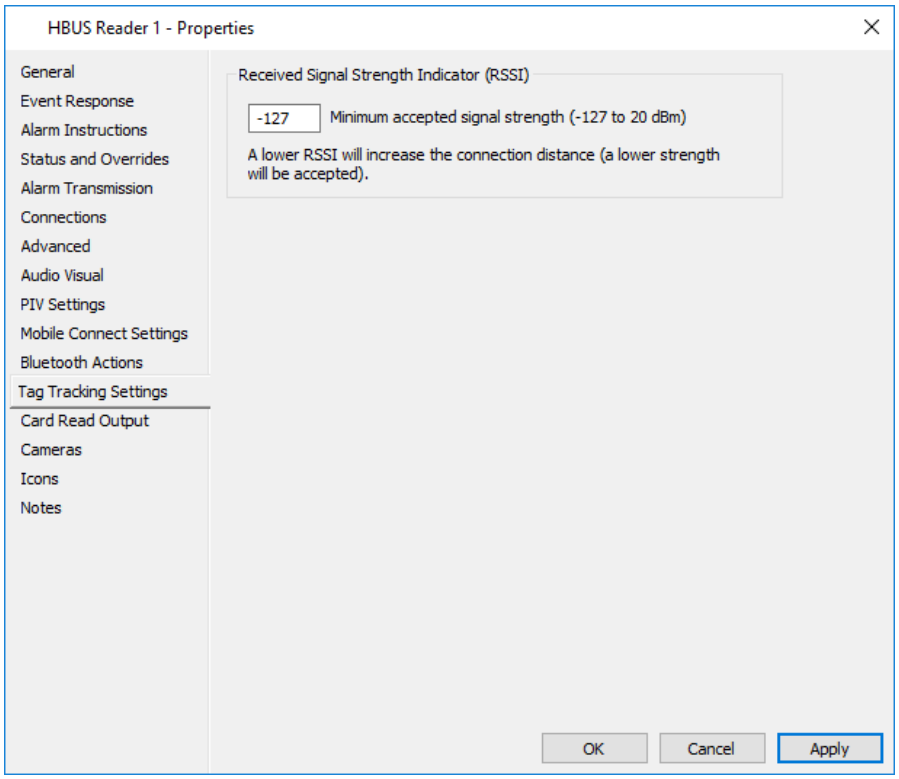
The Minimum accepted signal strength

The 'Minimum accepted signal strength' provides an approximate control for the distance from the Reader within which a tracking tag will be read. A lower minimum accepted signal strength allows the Reader to read tracking tags that are farther away.

a) Click **Configure** from the menu bar, then **Hardware**.
The Hardware List window opens.

b) Right-click the Gallagher T-Series Readers for which you want to set the 'Minimum accepted signal strength', and select **Properties**.

c) Click the **Tag Tracking Settings** tab.



d) In the **Minimum accepted signal strength** field, enter the minimum signal strength (in dBm) that this Reader will require for it to read a tracking tag. Received signal strengths less than this value will be ignored.

Recommendation: To give the Reader the best chance of receiving advertisements from a tag that passes it, Gallagher recommends leaving the 'Minimum accepted signal strength' as the default value (-127). This will best counter the factors that can impact the received signal strength, including:

- Transmission strength configured within the tag
- Tag low battery
- Objects that may alter the radio path loss between the tag and the reader
- Atmospheric conditions

e) Click **OK** to close and save your changes.
Click **Cancel** to close without saving your changes.
Click **Apply** to save your changes and stay in this window.

Configuring Door settings

The Minimum out-of-range time

A Door's 'Minimum out-of-range time' is the time for which a tracking tag's advertisements must not be received by the Door before the tag can be again considered for an access decision at that Door.

- When a tag comes within range of a Reader, an access decision is made.

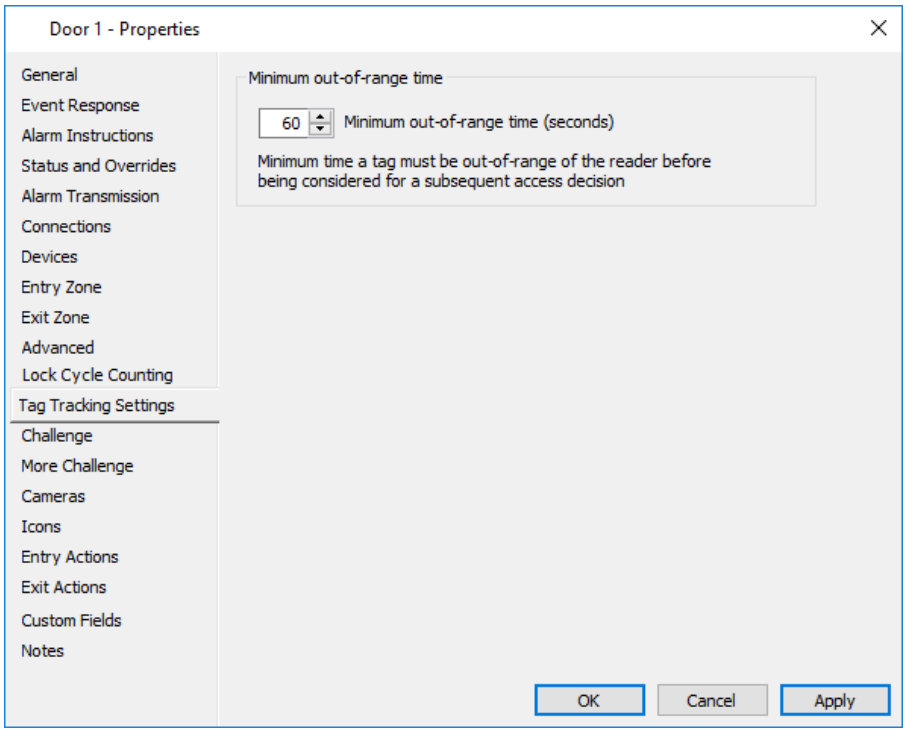
- When a tag comes within range of a Reader, an access decision is made.
- While the tag remains in range of the Reader, no further access decisions are made.
- Once the tag goes out of range of the Reader, the Minimum out-of-range time must pass before it can come back within range and be treated as another access attempt.
- If the tag comes back within range before the Minimum out-of-range time has passed, it is not considered as another access attempt, and the timer is reset.

Warning: Gallagher recommends leaving the Minimum out-of-range time as the default value. Lowering the value may cause excess access decisions to be made due to intermittently received tag advertisements.

a) Click **Configure** from the menu bar, then **Doors**.
The Door List window opens.

b) Right-click the Doors for which you want to set the 'Minimum out-of-range time', and select **Properties**.

c) Click the **Tag Tracking Settings** tab.



d) In the **Minimum out-of-range time** field, enter the time (in seconds) that a tracking tag must be out of range of the Door's Readers for before it is considered for another access decision.

e) Click **OK** to close and save your changes.
Click **Cancel** to close without saving your changes.
Click **Apply** to save your changes and stay in this window.

Setting up Tracking Tag Types

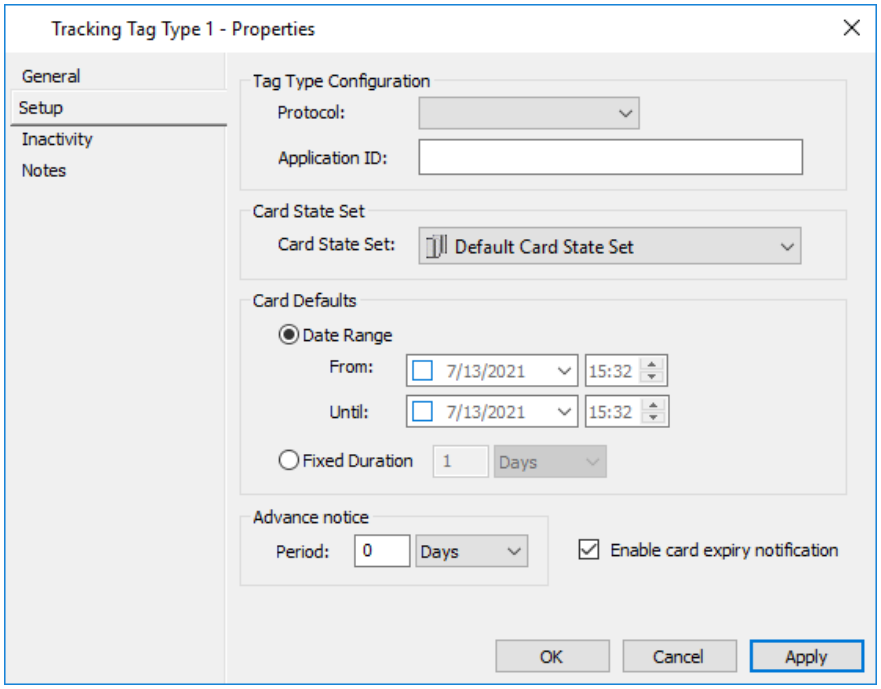
Introduction

This procedure covers how to set up a new Tracking Tag Type.
Note: The 'Configure Site' operator privilege is required to perform this procedure.

Configuration

To set up a Tracking Tag 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 (in grid view).
2. **Right-click** and select **New...** > **Tracking Tag Type**.
   The **General** tab displays.
3. Complete the fields as required.
   For further details, see ***General tab*** (on page 3-18).
4. Click the **Setup** tab.



5. Select the protocol your tracking tags use from the **Protocol** drop-down list.
   Note: Once the Protocol is set for the Tracking Tag Type and saved, it cannot be changed.
6. Enter the appropriate identifier:

If you selected...	then...
iBeacon,	enter the universally unique identifier (UUID) of your tracking tags into the **UUID** field. The UUID must be 32 hexadecimal characters.

If you selected…	then…
Eddystone UID,	enter Namespace ID (NSID) of your tracking tags into the **NSID** field. The NSID must be 20 hexadecimal characters.

7. From the **Card State Set** drop-down list, select the appropriate Card State Set to be associated with this Tracking Tag Type. If only one exists, it will default.
   Note: Once the Card State Set is assigned to the Tracking Tag Type and saved, it cannot be changed.
8. In the **Card Defaults** section, you can configure tracking tags of this Tracking Tag Type to be activated by default for either a specific Date Range or a Fixed Duration.
   Click the appropriate radio button:

If you select…	then…
Date range,	set the date and time that tracking tags of this type will activate and expire in the **From** and **Until** fields. **Notes:** ▪ If you do not enter a date in the **From** field, when a tracking tag of this type is registered to a Cardholder and the tracking tag is enabled, activation will be immediate. ▪ If you do not enter a date in the **Until** field, the tracking tag will not expire.
Fixed Duration,	set the duration by selecting an option from the drop-down list, (i.e. Minutes, Hours, Days, Weeks, Months or Years) and entering the appropriate number, (e.g. 2 Weeks). **Note:** When **Fixed Duration** is selected, the expiry date for a tracking tag will be set to the current date when the tracking tag is assigned *plus* the fixed duration value (e.g. assigned on 01/05/2021 + fixed duration of 2 weeks = expire by default on 15/05/2021).

9. The **Advance notice** section of this screen allows you to configure warning notifications of upcoming tracking tag expiries to be sent to Cardholders when the configured expiry period is nearly reached. Notifications will be sent for all tracking tags regardless of status.
10. Do you want to enable card expiry notification?

If…	then…
yes,	Set the **Period** to the number of days, weeks, months or years before tracking tag expiry to send a warning notification. Select the unit of time (e.g. Days) from the drop-down list. Ensure the **Enable card expiry notification** check box is checked.

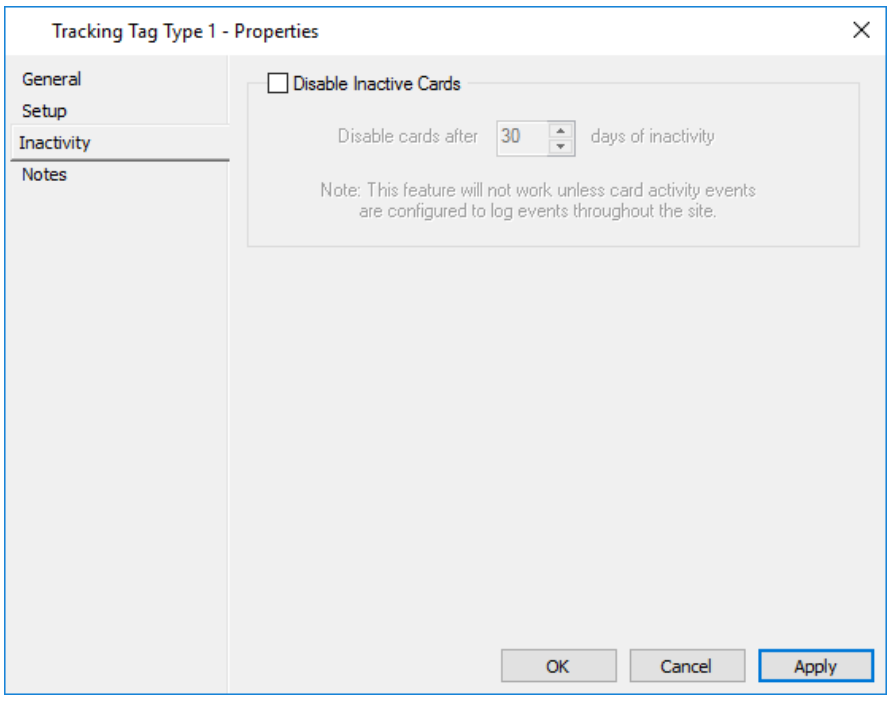
If…	then…
no,	leave the **Period** as 0 days, and deselect the **Enable card expiry notification** checkbox.

Inactive Card Expiry
A tracking tag whose Tracking Tag Type has the Inactive Card Expiry feature enabled is disabled if that tracking tag makes no successful access events for the duration of the inactivity period. Examples of a successful access event are "Door Access Granted" or "Card Exit Granted".

Some tracking tag authorisation features take precedence over Inactive Card Expiry, as follows:

- If a Cardholder is de-authorised, (i.e the **Cardholder Authorised** check box is unchecked on the **Cards** tab), then all of the Cardholder's credentials (cards, tracking tags, etc.) are disabled, irrespective of the 'Inactivity' status.
- If a tracking tag is disabled, (i.e the **Card State** is set to anything but 'Active' on the **Cards** tab), then that tracking tag is disabled irrespective of the 'Inactivity' status.
- If a tracking tag is expired according to the configured **From**/**Until** activation period on the **Cards** tab, then the tracking tag is expired irrespective of the 'Inactivity' status.

11. Click the **Inactivity** tab.



12. Do you wish to enable the Inactive Card Expiry feature?
Note: All tracking tags of this Tracking Tag Type will share a common inactivity timeout if enabled.

If…	then…
yes,	Select the **Disable Inactive Cards** checkbox. Go to Step 13.
no,	Leave the **Disable Inactive Cards** checkbox unchecked. Go to Step 14.

13. Enter the number of days of inactivity that will disable a tracking tag.
    For example: if set to '30', if a tracking tag is not used at any Reader for 30 days, it is disabled.
    Notes:
    - When this feature is first enabled, the default timeout is 30 days. The range is 1-999 days.
    - If tracking tag activity events are not configured to log events, tracking tags will be expired after the configured inactivity period regardless of activity (refer to ***Event Defaults*** on page 6- 12 for further detail).
14. Click the **Icons** tab if you want to change the Icon Set for this Tracking Tag Type.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
15. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Tracking Tag Type.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
16. Click the **Notes** tab if you want to add a note(s) about this Tracking Tag Type.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
17. Click **OK** to close and save your changes.
    Click **Cancel** to close without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Chapter 67: SIP Integration

Introduction

The Gallagher SIP Integration allows Command Centre operators to configure and use SIP devices within Command Centre Client. The integration currently supports SIP intercom devices.

Intercoms

The Gallagher SIP Integration supports SIP Intercom devices. The integration only allows calls to be placed and accepted from Gallagher Command Centre Client (not Configuration Client). The SIP Integration supports video intercoms, with the current limitation of only supporting 720p resolution video. The SIP Integration currently does not support encryption or isolating SIP Intercoms.

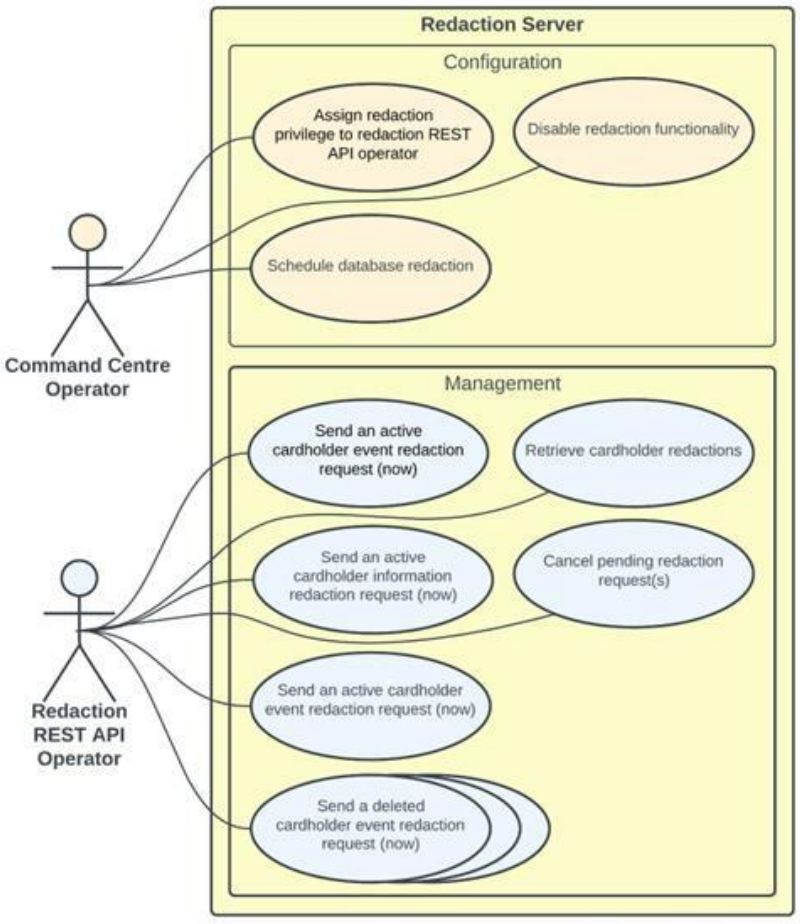
For further further detail refer to the document **"Release Note SIP Integration.pdf"** located in the 'Utilities' directory of the Command Centre installation media.

Chapter 68: PII Redaction

Introduction

The The Redaction functionality enables the removal of cardholder personal identifiable information (PII) from Command Centre system to protect client data in European countries and the UK. This feature is provided to users as a set of REST API calls in Command Centre.

In vEL8.80, automatic redactions are configured in Configuration Client, but manual redactions are available only via the REST API. You will need to use a tool like Postman to get this feature to work for manual redactions.
Note: Archive and operator events cannot be redacted in this version.



There are two types of redaction, as follows:

Cardholder Event Redaction:

- Redacts an optional specified “before” time non-operator events on the cardholder. This includes movement events, as well as the operator events that the cardholder is a changed target.

- This can be scheduled to future.
- There can be multiple pending event redactions on one cardholder.
- Includes Command Centre generated events.

Cardholder Information Redaction:

- Delete the cardholder (remove pdfs, cards, relationships, e.g. where the cardholder is assigned to an Access Group or an Operator Group)
- This can be scheduled to future.
- There is only one pending cardholder redaction on the same cardholder. Last added/updated cardholder redaction marks old pending same cardholder redactions to cancelled.

Licensing

Redaction functionality is a licensable feature. Your license file must contain the following options:

```
[Features]
PIIRedaction=1
```

Operator Privileges

An operator requires the appropriate privileges to perform redaction tasks. The privileges only apply within the Division assigned to that Operator Group.

Operator Privilege	is required for..
"Delete Cardholder History"	event redactions.
"Delete Cardholder History" and "Delete Cardholders"	cardholder redactions.
"Manage Redaction Settings"	changing redaction settings.

This chapter covers the following topics:

- ***Redaction Configuration in Command Centre*** (on page 68-3)
- ***Requesting a Cardholder Event Redaction*** (on page 68-6)
- ***Requesting a Cardholder Information Redaction*** (on page 68-7)
- ***Redacted Cardholders*** (on page 68-8)
- ***Redaction events*** (on page 68-10)

Redaction Configuration in Command Centre

Introduction

Before the PII Redaction functionality can be used, the following configuration is required in Command Centre Configuration Client:
- Configure the Redaction Server settings
- Connect to the REST API
- Configure Redaction REST API Operator(s)

Who is responsible

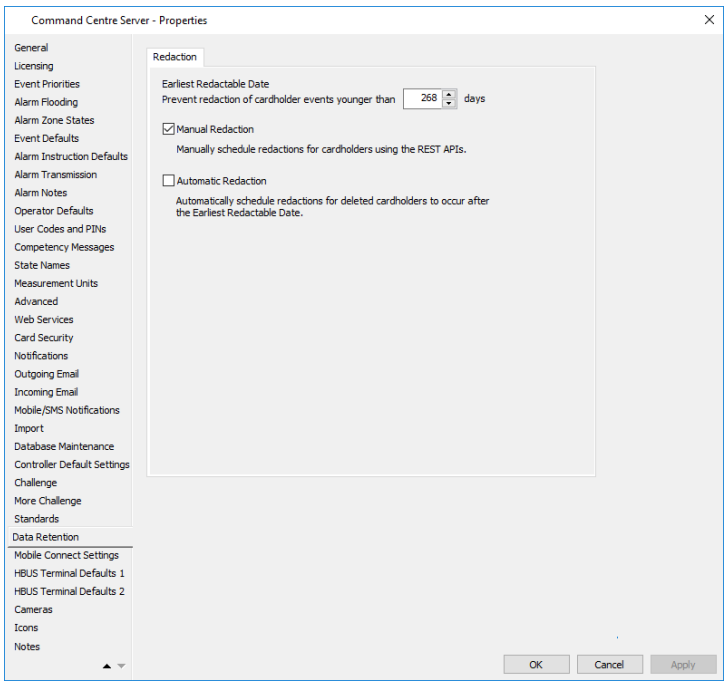
A Command Centre Operator with the "Manage Redaction Settings" operator privilege is responsible for configuring the Redaction Server and Redaction REST API operators.

Procedure

Use the following procedures to configure the Redaction functionality in Command Centre Configuration Client.

Configuring Redaction settings

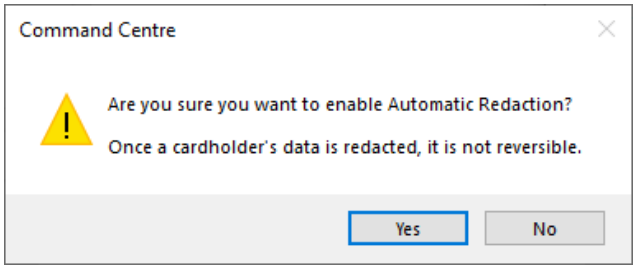
1. Click **File** on the menu bar, then **Server Properties**.
   The Command Centre Server Properties window displays.
2. Click the **Data Retention** tab.
   The **Redaction** sub-tab displays by default.



3. Tick the appropriate checkbox for the type of redaction you require, (i.e. Manual or Automatic).
   Notes:
   - The checkboxes will be disabled if you do not have the "Manage Redaction Settings" operator privilege.

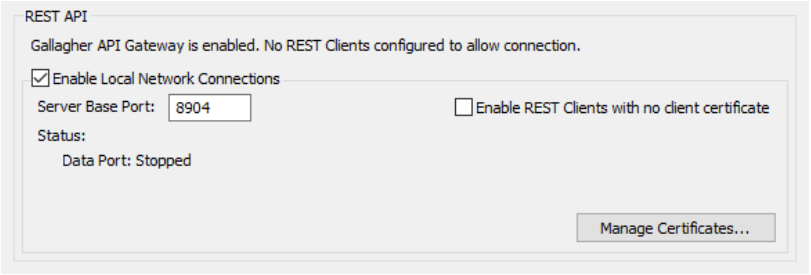
- If you do not tick one of these options, an error message will display when attempting to run a redaction from the API.
  Error: 403 Forbidden
  "message": "Redaction has not been enabled"

4. Enter the required number of days in the **Prevent redaction of cardholder event younger than** field.
   (Default = 268 days. Range = 30 - 9999 days.)
5. Click **OK** to exit and save your changes.
   Note: If you selected Automatic Redaction the following warning message displays when applied.



Connecting to REST API

1. Open the **Command Centre Server Properties** window, and click the **Web Services** tab.
2. In the 'REST API' section, tick the **Enable Local Network Connections** checkbox.

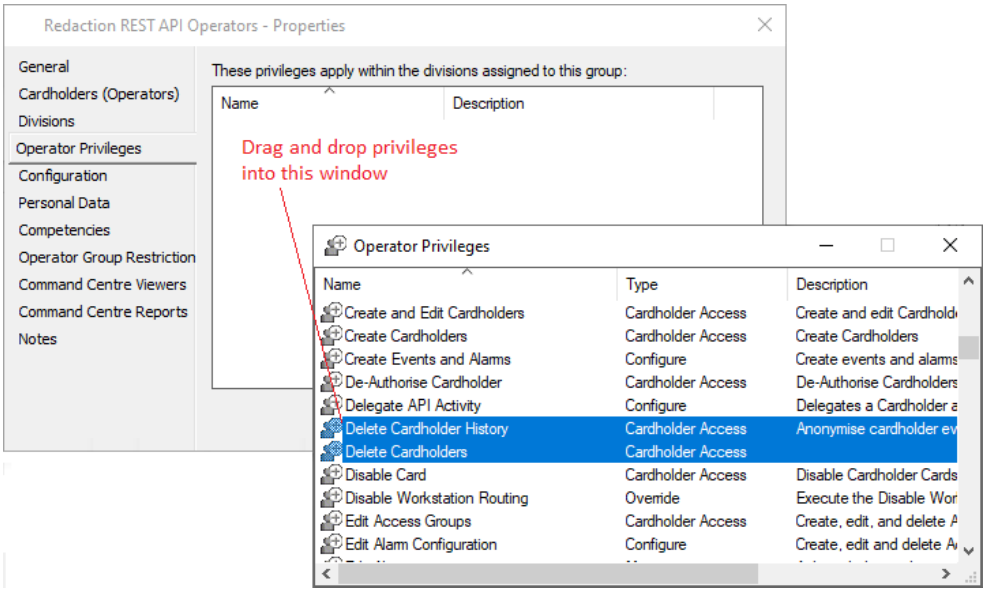


3. Click **OK** to exit and save your changes.
4. Configure a REST API Client Item.
   See ***Creating a REST API Client Item*** (on page 28-13) for the procedure.

Configuring a Redaction Operator

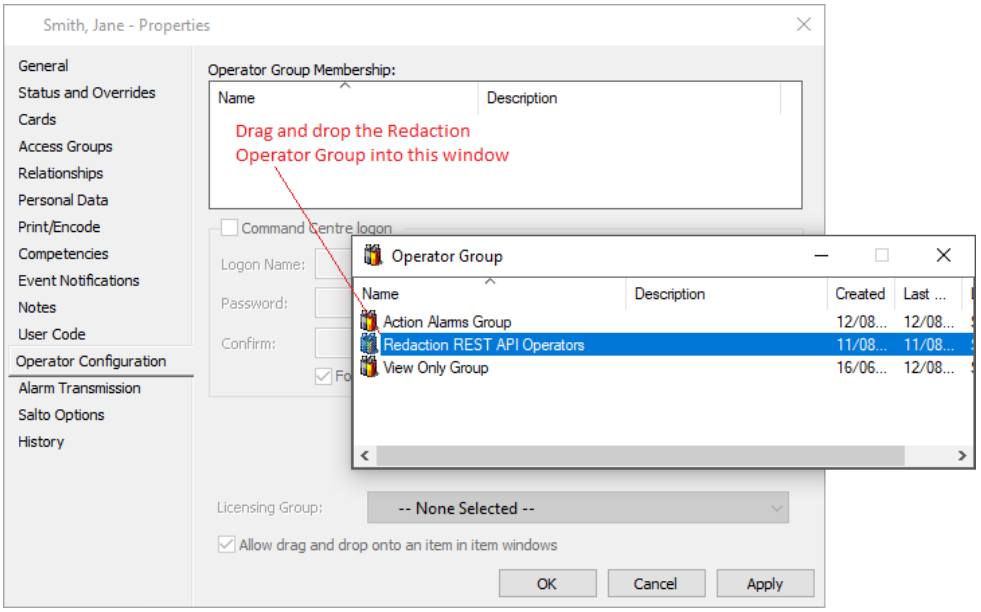
1. Create an Operator Group for Redaction REST API operators, as described in the ***Setting up Operator Groups*** procedure (on page 36-5).

   On the Operator Groups **Operator Privileges** tab, drag and drop the "Delete Cardholder History" and "Delete Cardholders" privileges from the Operator Privileges List Window.



2. Add the required cardholders to the Redaction Operator Group, as described in the ***Configuring Operators*** procedure (on page 36-14).

   On the Cardholders **Operator Configuration** tab, drag and drop the Redaction Operator Group from the Operator Groups List Window.



Requesting a Cardholder Event Redaction

Introduction

This procedure describes how to send an active Cardholder Event Redaction request.

Who is responsible

A Redaction REST API operator with the "Delete Cardholder History" operator privilege is responsible for requesting a Cardholder Event Redaction.

Procedure

With the Cardholder ID, send a Cardholder Event Redaction request.

Result

The request is received by the Cardholder API. If the request is successful, the following occurs:

- You receive a successful redaction request response.
- A 'Cardholder Event Redaction Requested' event is generated from the API call.
- Events relating to the Cardholder are redacted from the system at the scheduled time.
- A 'Cardholder Event Redaction Completed' event is generated at the scheduled time.

Requesting a Cardholder Information Redaction

Introduction

This procedure describes how to send an active Cardholder Information Redaction request.

Who is responsible

A Redaction REST API operator with the "Delete Cardholder History" and "Delete Cardholders" operator privileges is responsible for requesting a Cardholder Information Redaction.

Procedure

With the Cardholder ID, send a Cardholder Information Redaction request.

Result

The request is received by the Cardholder API. If the request is successful, the following occurs:

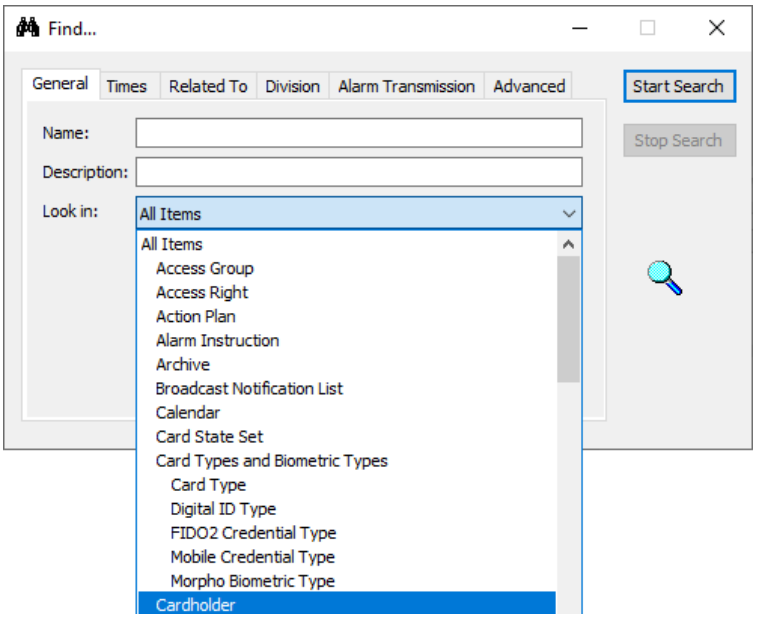
- You receive a successful redaction request response.
- A 'Cardholder Information Redaction Requested' event is generated from the API call.
- The Cardholder is redacted from the system at the scheduled time.
- A 'Cardholder Information Redaction Completed' event is generated at the scheduled time.

Redacted Cardholders

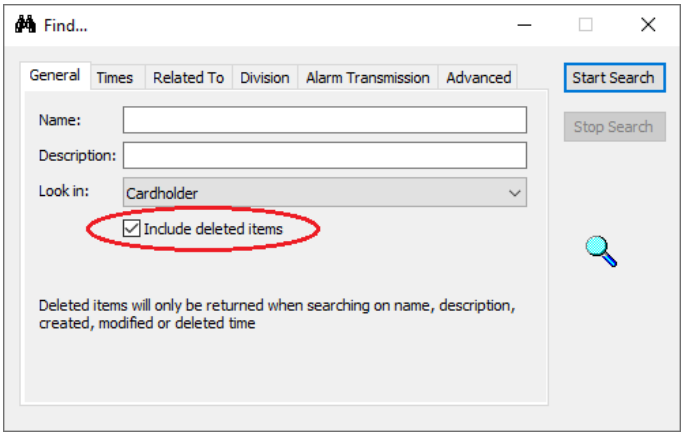
A "[redacted]" cardholder item exists in Command Centre, acting as a cardholder placeholder for all related items of the "to-anonymise" cardholder. It is "read-only" and does not appear in the Cardholder List Window (in Configuration Client) or the Cardholder Viewer (in Command Centre Client).

The only place the "[redacted]" cardholder item appears is using the Find Tool in Configuration Client, as follows:

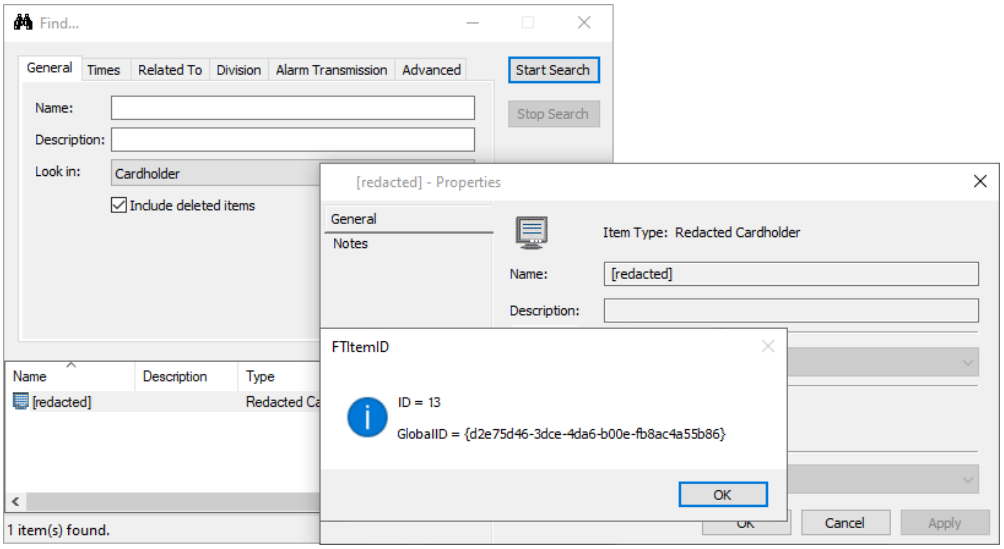
1. Click **Monitor** from the menu bar, then **Find...**
   The Find tool opens.
2. Click within the **Look in** field.
   From the displayed drop-down menu, click **Cardholder**.



3. Tick the **Include deleted items** checkbox.



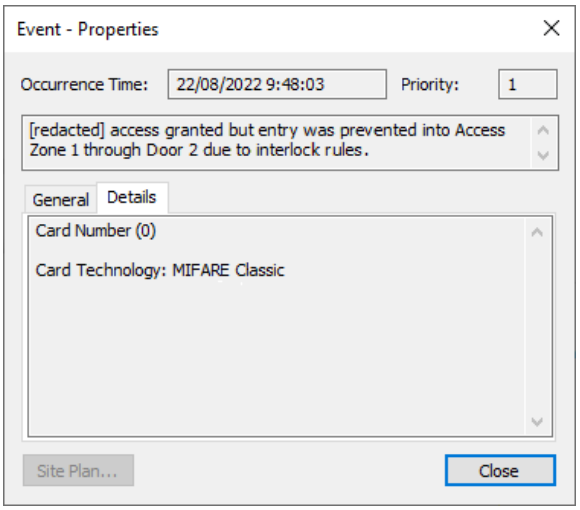
4. Click the **Start Search** button.
   The Search list window opens and displays the [redacted] cardholder item.



The [redacted] cardholder item is there for any time a redaction is done. The Cardholder ID will be replaced with this ID in the event database so that nobody can trace the events back to a Cardholder ID.

Redaction Events

In both Configuration Client and Command Centre Client, once a Cardholder has been redacted, their name will show as [redacted] in any event messages, and Card Numbers will show as (0).
For example:



If there are any details that contain personal identifiable information (PII), the entire details will be removed and will show as [redacted].
For example:



Event Reports will show the cardholder as [redacted].

Chapter 69: Apple Employee Badge

Introduction

The Apple Employee Badge solution is for specific customers only. Please contact your local Gallagher representative if you're interested in adopting this solution.

This solution allows Cardholders to add an Apple Employee Badge to Apple Wallet on their compatible iPhone and Apple Watch to request access using NFC at doors, elevators, turnstiles, and other facilities at their corporate workplaces.

Licensing

The Apple Employee Badge solution is a licensable feature. To configure this solution in Gallagher Command Centre the following license strings are required:

```
[Features]
Apple Pass=1

[Limits]
Mobile Credentials=X
```

Where 'X' is the number of mobile credentials that can be assigned to Cardholders

Features and Functionalities

Solution features and functionalities are:

- Use NFC from your iPhone or Apple Watch when requesting access at the reader.
- Use Apple Express Mode to request access without unlocking their iPhone. Apple badges are provisioned by default in Express Mode.
- Gallagher Command Centre can be configured to require second factor (2FA) at the reader. When 2FA is enforced, the user must present a second factor (Face ID, Touch ID, or Passcode) when requesting access.
- Use Apple Power Reserve Mode to request access when your iPhone needs a charge. Power Reserve provides up to five hours of access, so you can still get inside.
  Note: Power Reserve Mode only works for the user's default wallet credential, (i.e. usually the credit card).
- Cardholders can view and manage their Apple Badge on their iPhone, Apple Watch, or by logging into their iCloud account from any PC. Cardholder management functions are adding a badge, suspending a badge, resuming a badge, and removing a badge.
- Operators can view and manage Apple Badges in Command Centre. Operator management functions are suspending a badge, resuming a badge, and removing a badge.
- Supports one iPhone and one Apple Watch per Cardholder.
- Supports two factor authentication at the reader. Two factor authentication can be configured always on, or according to a schedule. When two factor authentication is enforced, the Cardholder must present a second factor (Face ID, Touch ID, or Passcode).

- Supports Cardholder First Name and Last Name updates to the Apple badge. Supports regeneration of Apple Keys, and Apple badge artwork updates.
- Provides a secure credential. The credential data is protected by the device's Secure Element (SE). The SE is a dedicated chip that is physically isolated from the main processor, specifically designed to handle sensitive transactions like those in Apple Pay.
- The Shareable Keys section (on the **Mobile Wallet** tab of the Server Properties) enables the retrieval of an Apple Read Key from Command Centre, which can then be programmed at a third-party reader, allowing Apple credentials to be read at the reader. Using Apple credentials, an employee can authenticate at all readers onsite.

Prerequisites

Solution prerequisites are:

- The Gallagher Command Centre system must be version 9.10 MR3 (or later).
- The Command Centre server must be connected to the Gallagher Cloud and Gallagher API Gateway. Refer to ***Connecting to the Cloud*** (on page 28-7) for further details.
- Command Centre Customer Experience Improvement Program (CEIP) must be enabled.
- The site must be using supported Gallagher Multi-Tech readers.
- The Gallagher Mobile Connect app (or SDK) must be installed on the Cardholder's iPhone.
- The Cardholder's iPhone must be iPhone 8 or later running iOS 16 or later.
- The Cardholder's Apple Watch must be Watch Series 5 or later running watchOS 10 or later.
- The Cardholder must have an active iCloud account (Apple ID).

Limitations

- It is recommended that Apple Employee Badge be assigned to permanent employees not visitors, as is the purpose of the badge. The Apple Employee Badge is not removed when a visitor is marked offsite, however the visitor is removed from all Access Group assignments when marked offsite, meaning the visitor will be unable to gain access. It is recommended that a separate Mobile Credential Type be created for visitors, that doesn't allow provisioning of the Apple Employee Badge Type.
- 2FA is not supported by Apple Employee Badge when the Gallagher reader is assigned to an Elevator Car.

This chapter covers the following configuration steps:

1. Configure Apple Keys (on page 69-3)

2. Configure Mobile Wallet Readers (on page 69-5)

3. Configure the Apple Employee Badge Type (on page 69-7)

4. Enable In-app Apple Employee Badge Provisioning (on page 69-9)

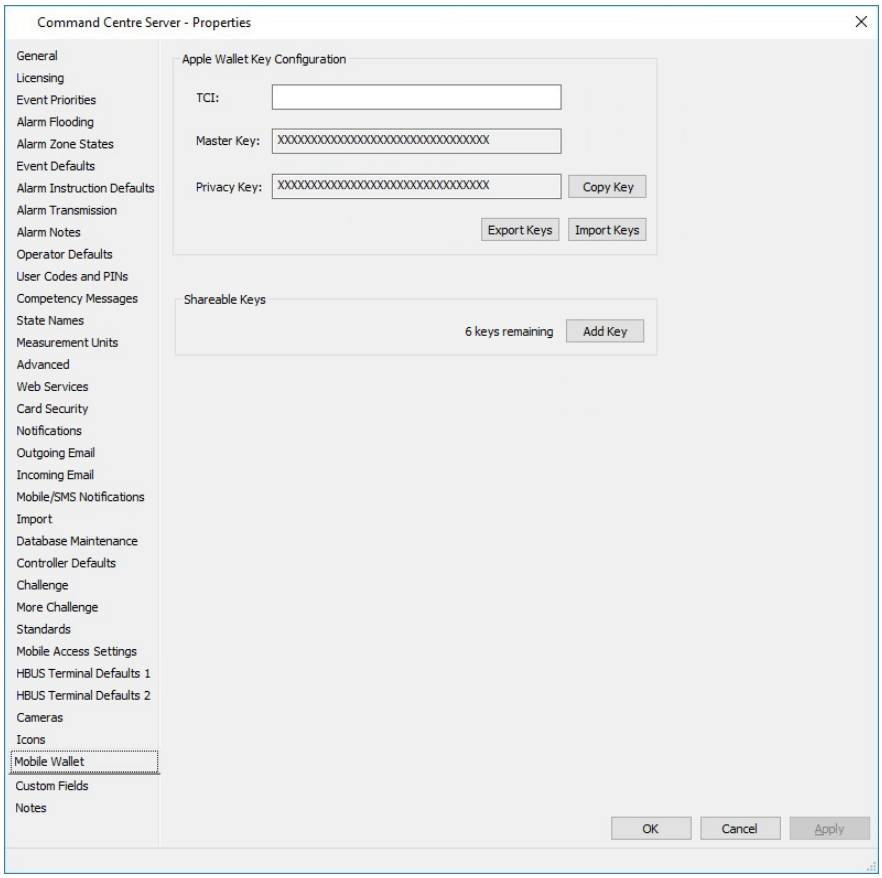
5. Manage Apple Employee Badges (on page 69-11)

6. Report Apple Employee Badge Assignments (on page 69-14)

1. Configure Apple Keys

This procedure describes how to configure the site TCI and Apple keys, as follows:

1. Click **File** on the menu bar, then **Server Properties**.
   The Command Centre Server Properties window displays.
2. Click the **Mobile Wallet** tab.

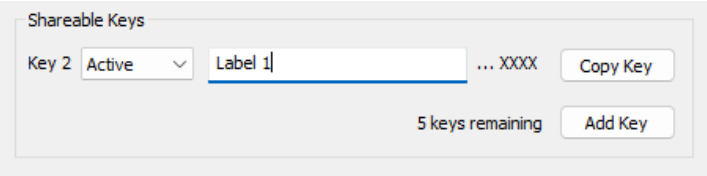


3. Enter your Apple Terminal Capabilities Identifier (TCI) in the **TCI** field. A TCI will be provided to you as part of the Apple Employee Badge onboarding process. The TCI is unique to this system. Gallagher readers will advertise a singular TCI. The TCI is linked to the Apple Employee Badge during provisioning to support Auto-Presentment and Express Mode features on the reader.
4. The **Master Key** and **Privacy Key** fields, each with a random 32-character hexadecimal string will be automatically generated when the TCI has been saved. The Master Key is your system's unique diversified MIFARE DESFire master key allowing the Apple Employee Badge to be read at Gallagher readers onsite. The Privacy Key is your system's unique diversified MIFARE DESFire long-term privacy key used to retrieve the credential identifier (card number) from the device (phone or watch).

5. The **Shareable Keys** section enables the retrieval of an Apple Read Key from Command Centre, which can then be programmed at a third-party reader, allowing Apple credentials to be read at the reader. Using Apple credentials, an employee can authenticate at all readers onsite.
   Notes:
   - Six Shareable Apple Read Keys can be retrieved.
   - Operators require the "Manage Keys" operator privilege to retrieve an Apple Read Key from Command Centre.
   - To program a supported third-party reader you require the following:
     - Apple TCI,
     - Privacy Key,
     - Read Key, and
     - Key Number

   Configure Shareable Key(s) as follows:

   a) Click the **Add Key** button.

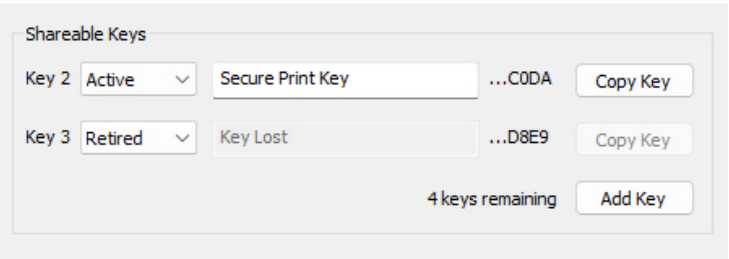


   b) Select the appropriate key state from the drop-down list to allow key usage to be tracked.

State	Description
Active	The Key has been assigned and can be used at a third-party reader.
Retired	The key should not be assigned. When a key is 'Retired', the **Copy Key** button and the field for entering a label are disabled, but the label previously entered still displays. **Note:** Although the key has been retired and shouldn't be used, it doesn't get revoked from the credential.

   c) Enter an appropriate label, (e.g. Secure Print Key).
   Note: The key can be recognised by the last four characters that display.

   d) Repeat Steps a) to c) for additional keys.



6. Click the **OK** button.

2. Configure Mobile Wallet Readers

Only Gallagher Multi-Tech readers, with the NXP chip that supports reading wallet credentials can be used. Readers manufactured from 2019 onwards have the required NXP chip.

From Command Centre v8.90 readers report their device attributes. The FT Support Tool can be used to report all readers that are wallet capable, their assigned door(s), and controller. The FT Support Tool is included with the Command Centre installation software in the `'Utilities\FT Support Tool'` directory.

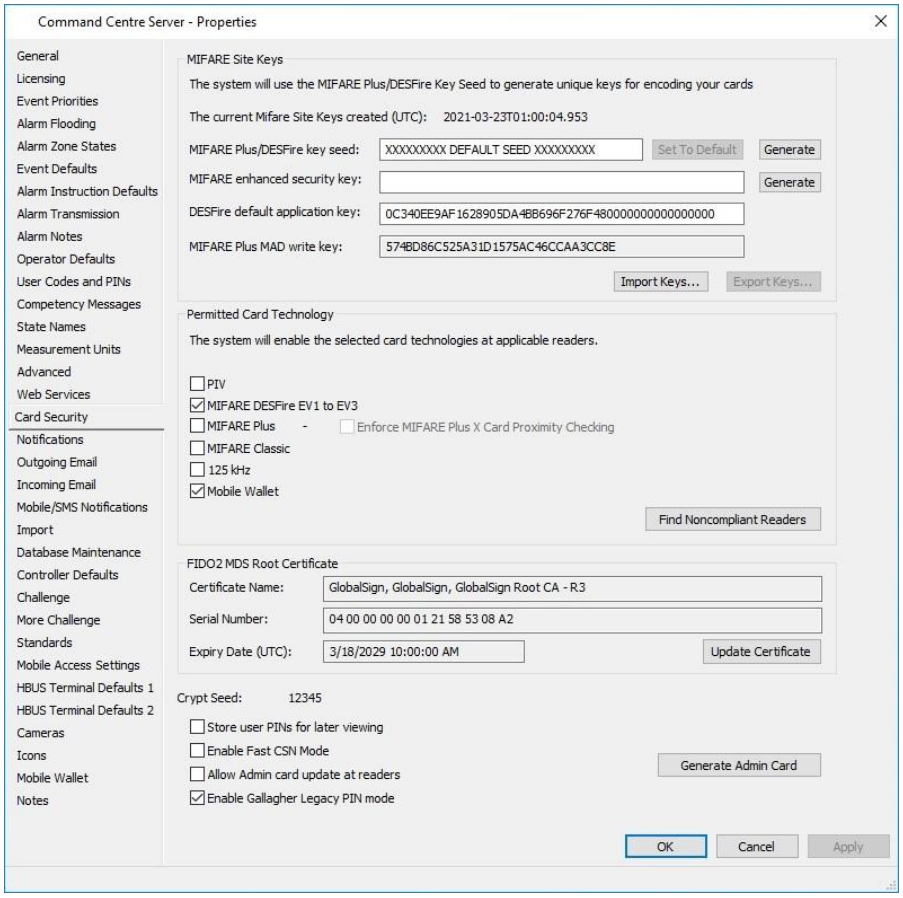
From Command Centre v9.10 CEIP reports the number of readers that are wallet capable.

CEIP Metric	Description
hardware.usage hardware.readers.count	This metric reports the total number of readers configured.
hardware.usage hardware.readers.mobileWalletCapable.count	This metric reports the total number of readers configured that are wallet capable.
hardware.usage hardware.readers.mobileWalletEnabled.count	This metric reports the total number of readers that have been configured to read wallet credentials, (i.e. the **Mobile Wallet** checkbox is ticked in the reader's properties).

Note: High Sec Multi-Tech readers are not supported.

Readers can be configured individually (via the **Advanced** tab of the Reader Properties) or site-wide from the Server Properties.
This procedure describes how to configure all readers to read a wallet credential, as follows:

1. Click **File** from the menu bar, then **Server Properties**.
   The Command Centre Server Properties window opens.
2. Click the **Card Security** tab.
3. In the **Permitted Card Technology** section, tick the **Mobile Wallet** checkbox.
   Note: The T30 Keypad and T20 Terminal software will change, reducing the NFC read range for mobile wallets to less than 11cm, ensuring a valid access request is being made at the reader.



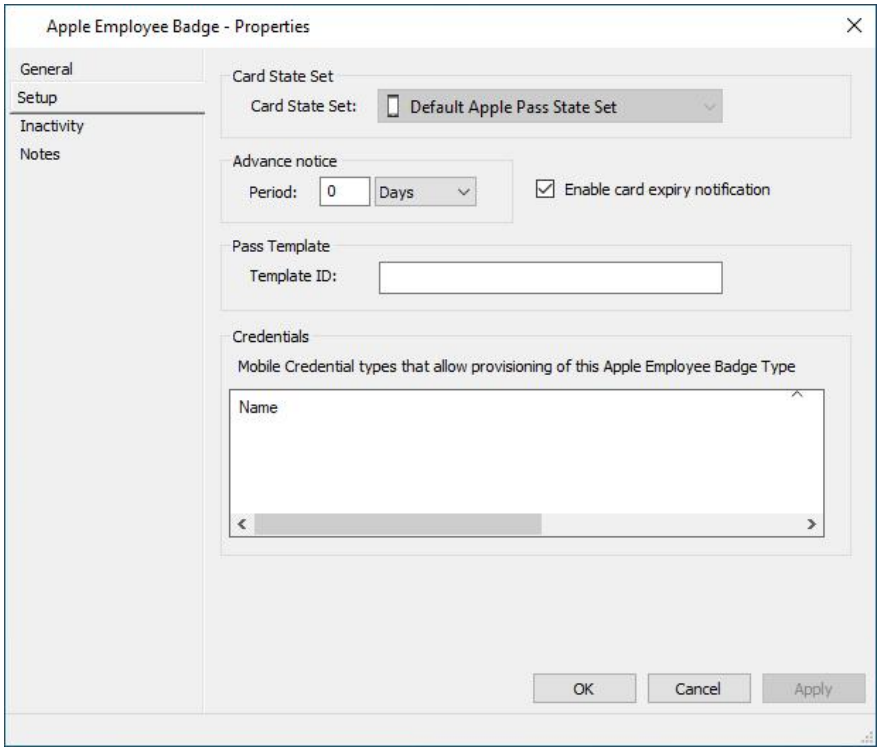
4. Click the **OK** button.
   Notes:

   - A Reader Bulk Change can be performed to change the card technologies accepted at readers and Find tool results can be dragged onto the Reader Bulk Change wizard. See ***Initiating a new Reader Bulk Change*** (on page 38-34) for further detail.
   - On the **Mobile Access Settings** tab of the Server Properties, the option **Second factor always required for mobile**, enforces second factor at all readers when reading an Apple Employee Badge. Passcode, Touch ID, or Face ID will be required at the iPhone. Passcode will be required at the Apple Watch. Note: This functionality is not supported when the reader is assigned to an Elevator Car.

3. Configure the Apple Employee Badge Type

This procedure describes how to configure an Apple Employee Badge Type, a follows.
Note: Only one Apple Employee Badge Type can be configured within the system.

1. Click **Configure** from the menu bar, then **Card Types**.
   The Card Type List Window opens
2. **Right click** and select **New...New Apple Employee Badge Type**.
   By default the **General** tab displays.
3. Type in an appropriate **Name** (limited to 60 characters) for the Apple Employee Badge Type.
4. Click the **Setup** tab.



   The Default Apple Employee Badge State Set is displayed in the **Card State Set** field.
5. The **Advance notice** section of this screen allows you to configure a warning notification (email or SMS) for pending Apple Employee Badge expiry.
   This notification will be sent when the specified period is reached.
   To configure outgoing notifications from Command Centre, refer to ***Outgoing Email*** (on page 6-50) or ***Mobile/SMS Notifications*** (on page 6-54) for further detail.
6. Select the mobile credential that will allow in-app provisioning of the Apple Employee Badge. Cardholders assigned this mobile credential will see the **Add to Apple Wallet** button in the Mobile Connect app.

This mechanism provides the following functions:

- The ability for an operator to stagger the rollout of Apple Employee Badges to select Cardholders. Meaning a site can create a new mobile credential that allows the provisioning of the Apple Employee Badge and assign to specific Cardholders only.
- The ability to display the **Add to Apple Wallet** button in the Mobile Connect app for specific Cardholders only, (i.e. a separate mobile credential that does not allow the provisioning of the Apple Employee Badge Type should be used for visitors and contractors).
- The ability to display the **Add to Apple Wallet** button in the Mobile Connect app, without needing to re-provision mobile credentials to Cardholders.

7. Enter a **Template ID**.
   The Template ID is 36-character (hyphenated) GUID, that maps the Apple Employee Badge to a specific artwork bundle in the Apple cloud. Your Template ID will be provided to you as part of the Apple Employee Badge onboarding process.
8. Click OK to save the Apple Employee Badge Type.

4. Enable In-app Apple Employee Badge Provisioning

The Apple Employee Badge Type is linked to a mobile credential (refer to the section above). Assignment of a mobile credential is required to authenticate the Cardholder, and to enable download of the Mobile Connect app used to provision an Apple Employee Badge into the Wallet app.

Important: When the Cardholder provisions an Apple Employee Badge into the Wallet app, the organisation will be charged a fee.

Procedure

This procedure describes how to enable in-app Apple Employee Badge provisioning, as follows:

1. Assign the Cardholder a mobile credential that enables in-app provisioning of the Apple Employee Badge.
   For details on how to assign a mobile credential refer to the topic *"Assigning a Card, Credential, or Digital ID"* in the Command Centre Online Help.
   Notes:
   - If the mobile credential has any of the following states, the Cardholder will be unable to add an Apple Employee Badge to their Wallet app.:
     - Expired,
     - Disabled (manually),
     - Lost,
     - Stolen,
     - Damaged,
     - Disabled (unauthorized),
     - Invitation Expired,
     - Waiting for Registration, or
     - a custom card state
   - If the Cardholder is not authorised, meaning the mobile credential state is Disabled (unauthorized), the Cardholder will be unable to add an Apple Employee Badge to their Wallet app.
2. The Cardholder receives the mobile credential email invitation and downloads the Mobile Connect app.
   Note: The **Add to Apple Wallet** button will **not** show at this point, as the Cardholder hasn't been authenticated.
3. The Cardholder navigates back to the email invite and selects the **Accept Credential** button.
   The Cardholder may be required to enter a 6-digit confirmation code sent via SMS to verify their device.
4. The Cardholder will be required to specify the second factor to be used (Face ID, Touch ID, or Passcode). This must be entered at the phone when the reader requests a second factor using Bluetooth.
   Note: The second factor is optional if the invitation is created with the REST API.

5. The Cardholder selects the **Add to Apple Wallet** button.
6. The Cardholder must agree to the Terms and Conditions. These terms describe how the Cardholder's organisation, as the Apple Employee Badge provider ("Participating Provider") will use certain personal information to enable the Cardholder's usage of Apple Wallet with Command Centre.
7. The Cardholder selects the **Done** button.

Result

The Apple Employee Badge will display within the Wallet app. The Apple Employee Badge is provisioned in Express Mode, meaning the device needn't be unlocked, or the Wallet app open to request access at the reader.

To view the information on the rear of the Apple Employee Badge, select the Information Icon, top right of the badge. The rear of the badge displays. To remove the badge, scroll down and select **Remove Badge**.

To use the Apple Employee Badge, present the phone or watch at the reader.
Note: If the Mobile Connect app is open in the foreground, Apple Employee Badge will not be used to communicate with the reader, Bluetooth® will be used instead.

5. Manage Apple Employee Badges

An operator can change the state of an Apple Employee Badge in Command Centre.

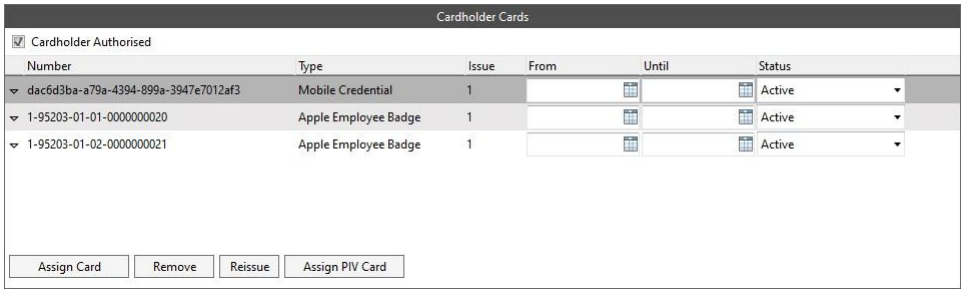
An Apple Employee Badge provisioned to the phone and watch will appear as two independent credentials in Command Centre. Each credential can be managed independently of the other, by the operator or the Cardholder. Each credential will have a unique 21-character card number, as known as the credential identifier.

Credential Identifier

V-UUUUUU-II-DD-CCCCCCCCCC

V = Version
U = Unique Site Identifier
I = Issue Level
D = Device Type (where 01 is iPhone and 02 is Apple Watch)
C = Card Number

Note: When mapping the credential identifier to a third-party system, (e.g. print system) it is recommended, the whole card number be passed.



Cardholder Apple Employee Badge states

The credential can be placed into the following states by the Cardholder:

State	Description
Suspended by user	When the Cardholder places their device into Lost Mode, their Apple Employee Badge will transition into the 'Suspended by user' state in Command Centre. **Note:** An operator belonging to an Operator Group with the privilege 'Override Card Status' can change the 'Suspended by user' state. The operator may want to change the state to 'Disabled (manually)', meaning when the phone exits Lost Mode (Cardholder authenticates at their phone), the credential won't return to its previous 'Active' state. If the phone does not have internet connectivity when Lost Mode is exited, the credential will remain active in the wallet but will be disabled in Command Centre and cannot be used to request access.

State	Description
	If an operator changes the 'Suspended by user' state to 'Active', the state change is queued in the Apple Cloud and will not take effect until the Cardholder exits Lost Mode (Cardholder authenticates at their phone). This is the same behaviour as the credit card – the card cannot be used when the phone is in Lost Mode.
Active	When the Cardholder adds their Apple Employee Badge to the Wallet app, it is added in the 'Default' state, set on the Card State Set. By default, the 'Default' state is 'Active' but this can be changed. If the 'Default' state is changed to 'Disabled (manually)' badges are added in a 'Disabled' state. If the Cardholder finds their device after placing in Lost Mode (Cardholder authenticates at their device), their badge will resume, (i.e. change from 'Suspended by user' to 'Active'). **Note:** If the Cardholder removes the credential from their Wallet, the credential is removed in Command Centre.
Removed by user	The Cardholder can remove their Apple Employee Badge from the Wallet app on each device, or by logging onto iCloud and removing from there.

Admin Apple Employee Badge states

The credential can be placed into the following states by the Command Centre operator:

State	Description
Not yet Active	The Apple Employee Badge 'From' date us in the future. The Apple Employee Badge displays the following message in the Wallet app.: *"This badge cannot be used. Gallagher has suspended use of this badge"*
Active	The Apple Employee Badge is active. The Apple Employee Badge displays as usable in the Wallet app.
Expired	The Apple Employee Badge 'Until' date is in the past. The Apple Employee Badge displays the following message in the Wallet app: *"This badge cannot be used. Gallagher has suspended use of this badge"*
Disabled (manually)	The Apple Employee Badge has been disabled by the operator. The Apple Employee Badge displays the following message in the Wallet app: *"This badge cannot be used. Gallagher has suspended use of this badge"*

State	Description
Custom	All custom card states are inactive card states. The Apple Employee Badge displays the following message in the Wallet app: *"This badge cannot be used. Gallagher has suspended use of this badge"*

Notes:

- By default, Apple Employee Badges are provisioned into the Wallet app in an active state. For example, if the operator disables an Apple Employee Badge, then the Cardholder removes the badge from the Wallet app, then adds it back, the badge will be added in an active state. If the operator doesn't want the Cardholder to provision an Apple Employee Badge, they must de-authorise the Cardholder, or assign the Cardholder a mobile credential that doesn't allow the provisioning of an Apple Employee Badge.
- If the operator unauthorizes the Cardholder, all badges assigned to the Cardholder will display as "Suspended" in the Wallet app.
- If a Cardholder suspends their Apple Employee Badge, (i.e. places their device into Lost Mode), then an operator with the "Override Card Status" privilege activates the Cardholder's badge, the Cardholder must first unlock their device, before it can be used at the reader.
- Cardholder **First Name** and **Last Name** is stored in the Gallagher Cloud. If a Cardholder record is deleted or redacted, the Cardholder's **First Name** and **Last Name** (used to provision the badges) are purged from the Gallagher Cloud.

Account Binding

The Gallagher Apple Employee Badge solution employs strong account binding and a badge device transfer limit to prevent fraudulent use of Apple badges.

As a result, a cardholder cannot transfer their provisioned Apple badge to a different iCloud account. Additionally, a device migration limit is enforced to prevent badge duplication across devices (phone or watch). Only one device transfer limit can occur within a 90-day period. This limit is enforced after the first transfer, meaning a user can provision a badge to their device, migrate to another device, then the 90-day period is enforced.

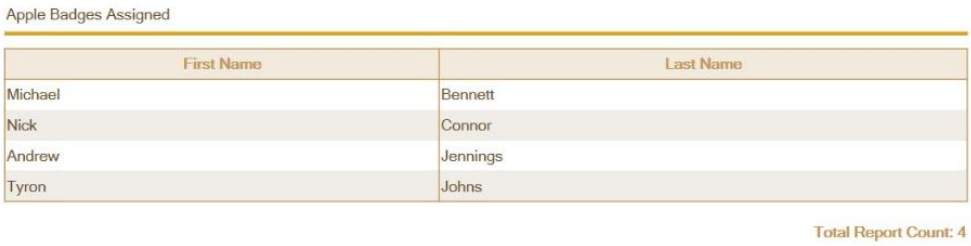
For further detail refer to the ***Removing Apple Account Binding*** procedure (under *Using Command Centre* > *Working with Viewers* > *Cardholder Viewer*) in the Command Centre Client user guide.

6. Report Apple Employee Badge Assignments

A Cardholder Report can be configured to return all Cardholders assigned an Apple badge.

Create a new Cardholder Report. Name it something useful, (e.g. Apple Badges Assigned). Use the 'Cardholder Card Type' filter and select the 'Apple Employee Badge Type'. Configure the Report Layout to use the **First Name** and **Last Name** columns. Tick 'Display total report count' to view the total number of cardholders assigned the Apple Employee Badge Type.

Note: The report cannot return a Cardholder record that no longer exists. If a deleted Cardholder provisioned an Apple badge, this information will be absent from the report. It is therefore possible the Apple invoice (reporting the number of Apple badge activations for the site) will differ from the total number of cardholders assigned an Apple badge, shown in this report.



Apple Badges Assigned

First Name	Last Name
Michael	Bennett
Nick	Connor
Andrew	Jennings
Tyron	Johns

Total Report Count: 4

Chapter 70: Shifts

Introduction

The licensed Shifts feature introduces a new 'Shift' item to Gallagher Command Centre, which must be configured in Gallagher Configuration Client. Shift items can be configured with the shift's start date, days on shift, days off shift (break days), daily hours of the shift, and optionally an end date. The Access Groups that work this shift can then be assigned to the Shift item. This allows for two main functions:

Shifts in Time Reports
The Time Report and Time Report - Overview allow Shifts to be used. In these reports, specific Shifts can be applied to the Report Date and Time filter, so that the report only includes events for Cardholders who were assigned to one (or more) of those Shifts within the Report Period. Additionally, when Shifts are used in the Report Date and Time filter, rather than setting 'Daily Time Ranges' to mark the earliest and latest assumed entry and exit times, Shift items are used. Where a Cardholder is missing an entry or exit event within the specified Report Period, the Start time or End time of their Shift can be used to assume the missing entry or exit time.

The Report Layout can also be configured to include the 'Shift' column, to display the Shift(s) the Cardholder was working during the time between each entry and exit event.

Note: A report row's 'Shift' column only displays a Shift if the Cardholder was actively in an Access Group associated with a Shift at the times that the entry or exit events occurred. This also applies to the past movement time for historical manual access events; it is not relevant in the report whether the Cardholder is associated with a Shift at the time an operator manually creates an event.

Regulated Zones - Shift management
Regulated Zones is a separately licensable feature of Command Centre. It introduces a 'Shift management' rule that raises an alarm when a Cardholder enters a zone early for their shift, fails to enter on time, or fails to exit on time. Previously configured using Personal Data Fields to specify shift details, this feature has been enhanced to allow Shift items to be used instead, with a similar but more intuitive configuration, and an expanded result.

Licensing

Shifts items are a licensable feature. You must purchase the following licence to configure Shifts in Gallagher Command Centre:

```
[Features]
Shifts=1
```

Configuration

This chapter covers the following configuration steps:

Configuring a Shift (on page 70-3)

Purging Shift history (on page 70-6)

Reports
Shifts are only applicable to the reports 'Time Report' and 'Time Report - Overview' in Gallagher Command Centre Client (not Configuration Client). Refer to the *"Creating Reports"* chapter and the *"Quick Tips for configuring the 'Report Date and Time' filter"* topic in the Gallagher Command Centre Help.

Regulated Zones
Regulated Zones is a separate licensable feature. Refer to the document *"Release Note Regulated Zones (v9.11).pdf"* (or later version) for information about using Shifts with Regulated Zones.

Configuring a Shift

Introduction

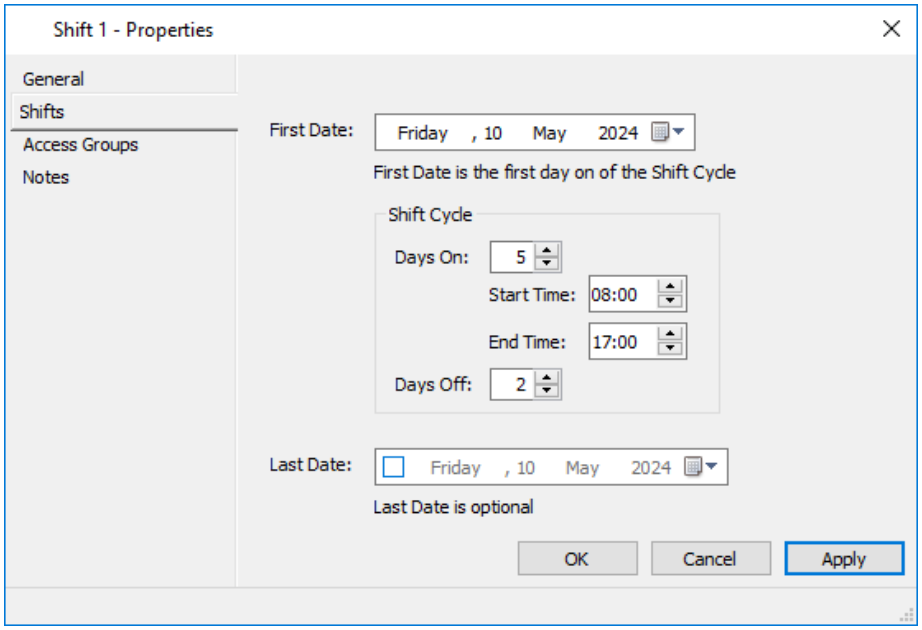
This procedure covers how to set up a new Shift. A Shift item can be configured for each shift that is worked on site, with details such as their on days and off days, and start and end times. Assigning the applicable Access Groups to the Shift allows for the Shift to be used to report on the Cardholders in those groups.

Note: The 'Edit Site' operator privilege is required to perform this procedure.

Configuration

To create a Shift, perform the following procedure in Gallagher Configuration Client:

1. Click **Configure** from the menu bar, then **Shifts**.
   The **Shift** List Window opens (in grid view).
2. **Right-click** and select **New...** > **Shift**.
   The **General** tab displays.
3. Complete the fields as required.
   For further details, see ***General tab*** (on page 3-18).
4. Click the **Shifts** tab.

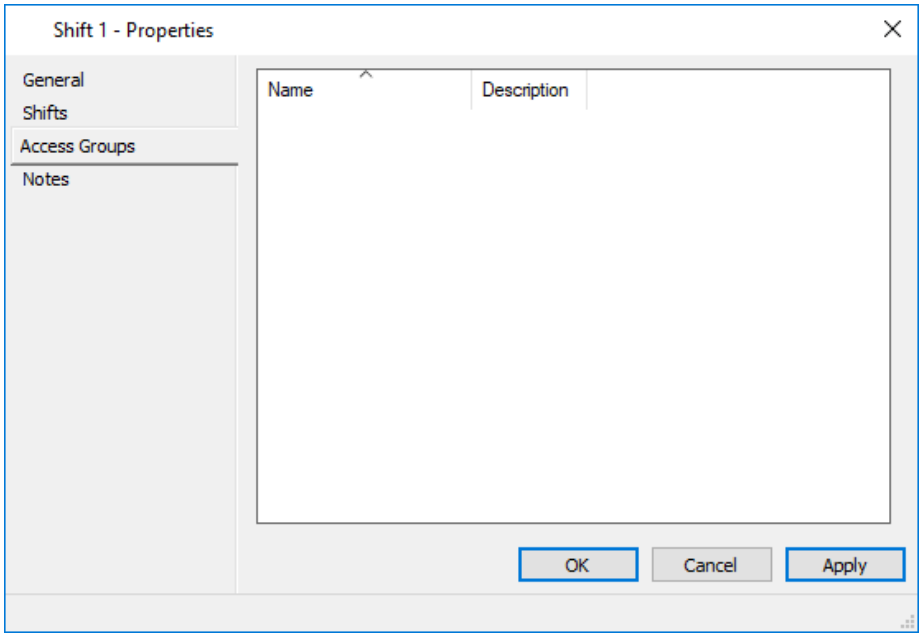


5. In the **First Date** field, click the drop-down and select the date of the first 'Day On' day (working day). This could be in the past or future.

   If this shift has already begun in reality (i.e. staff are already working this shift), select the first 'Day On' of the *current* shift cycle. For example, if today is January 4th, and the most recent 'Day Off' (break day) was January 1st, and January 2nd was therefore the first 'Day On' of the current shift cycle, set 'First Date' to January 2nd.

If this shift has not begun yet, select the first 'Day On' (working day) that will be worked by workers of this shift. The Shift will not be valid until the start of this day.

6. In the **Days On** field, enter the number of working days in the shift. This is the number of consecutive days that staff work between their break days.
7. In the **Start Time** field, enter the time of day that the shift starts on each of the 'Days On'.
8. In the **End Time** field, enter the time of day that the shift ends on each of the 'Days On'.
9. In the **Days Off** field, enter the number of break days in the shift. This is the number of consecutive days that staff stop working for, after the last 'Day On' of the shift cycle and before the first 'Day On' of the next shift cycle.
10. In the **Last Date** field, optionally click the drop-down and select the last day that this Shift is valid for. This date must not be earlier than the 'First Date'. This date does not need to line up with the shift cycle. After this date, this Shift will not apply to any Cardholders. Therefore, after this date:
    - if selected in a Time Report's or Time Report - Overview's 'Report Date and Time' filter, the Shift will have no effect on the Report, and,
    - if using the licensed Regulated Zones feature, Shift management Regulated Zone Rules using this Shift will no longer activate/disable the Competency or raise any alarms in accordance with this Shift. For example, a Shift management rule will not raise an early arrival alarm for a Cardholder whose shift is invalid, since there is no longer a valid definition of 'early'.
11. Click the **Access Groups** tab.



12. Drag and drop all Access Groups that work this Shift to the grid on the Access Groups tab.

    Each Cardholder in these Access Groups will have this Shift applied to them, so their access events will appear in a Time Report or Time Report -

Overview with this Shift applied to the 'Report Date and Time' filter, and they can be managed by a Regulated Zones Shift management rule with this Shift assigned.

Once an Access Group is added to a Shift, the Shift will display in a read-only list on the Access Group's 'Shifts' tab.

13. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Shift item.
    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 Shift Type.
    For further details regarding the **Notes** tab, see Notes (on page 6-85).
14. Click **OK** to close and save your changes.
    Click **Cancel** to close without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Purging Shift history

Introduction

The Command Centre database keeps historical records of:

- Shift items that have been deleted,
- The previous configurations of Shift items that have had configuration on their 'Shifts' tab changed, and
- Associations between Cardholders and Shifts that have since been removed (i.e. it keeps a memory of when a Cardholder was assigned to a Shift, even after the Cardholder is un-assigned).

This is so that Time Reports and Time Report - Overviews can report on Shift information for dates in the past, even after the Shifts have been un-assigned from Cardholders, re-configured, or deleted. Since this takes up space in the Command Centre database, you can optionally configure Command Centre to purge this historical information after a certain number of days since the Shift was unassigned or deleted. You may, for example, decide that you will never wish to report on Shifts that were worked more than 1 year ago, so you configure the system to purge Shift information that has been 'historical' for more than 365 days.

- After the configured number of days have passed since a Shift item was deleted, it is purged so that it can no longer appear in Time Reports or Time Report - Overviews that report on the period during which the Shift existed.
- After the configured number of days have passed since a Cardholder was un-assigned from a Shift, the Cardholder-Shift association is purged so that the Cardholder can no longer be reported as having worked that Shift in Time Reports or Time Report - Overviews that report on the period during which the Cardholder was assigned that Shift.

The automated purge (if enabled) runs daily. The ability to purge Shift history is only available at system level, therefore where the system is used by multiple companies, it will not be possible for them to purge Shift history according to different "number of days" settings.

You can configure the parameters for when Shift history gets purged from the system via the **Database Maintenance** tab in the Server Properties. See ***Database Maintenance*** (on page 6-57) for details.

Notes:

- The "purge process" can be disabled.
- In a multi-server system, Shifts are not replicated, so the purge needs to be run on *each* server using Shifts.

Operation

Only historical Shift items or Cardholder-Shift associations get deleted. The following do **not** get deleted as part of the purge:

- Cardholder records (active or historical)
- Active (non-deleted) Shift items
- Active Cardholder-Shift associations
- Events

An event is logged when the purge starts and another when the purge completes.

If the purge process encounters a Shift history which cannot be deleted, it will skip that history and continue deleting the others. A message will be logged to the log file showing any available information on why the Shift history failed to delete, and the "purge process" will try to delete the history again during its next run (i.e. the next day).

Chapter 71: CipherToken Card Support

Introduction

Command Centre supports CipherToken cards. They are DESfire EV2 and are supplied with six key sets so that they can be rolled if required. The ability to roll the keys is in case one of the keys in use were to be discovered. Keys required for reading cards are loaded using a configuration card. Each configuration card also supplies the key used to read the next configuration card used to roll keys.

Licensing

CipherToken card functionality is a licensable feature. The license file must contain the following option:

```
[Features]
CipherToken=1
```

This chapter covers the following topics:

- ***Enrolling a CipherToken configuration card*** (on page 71-2)
- ***Rolling configuration on a CipherToken card*** (on page 71-5)
- ***Configuring and printing CipherToken card layouts*** (on page 71-6)
- ***CipherToken cards in Command Centre*** (on page 71-7)

Enrolling a CipherToken configuration card

Introduction

A CipherToken Card Type needs to be configured in the Configuration Client to be able to assign CipherToken cards to Cardholders.

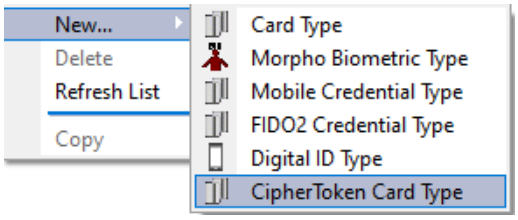
Notes:

- There is no limit to the number CipherToken card flows and card types a site can have.
- The "Manage Keys" operator privilege is required to read the configuration card.
- The configuration data includes the keys that are required to validate the next configuration card if the site keys ever need to be rolled.

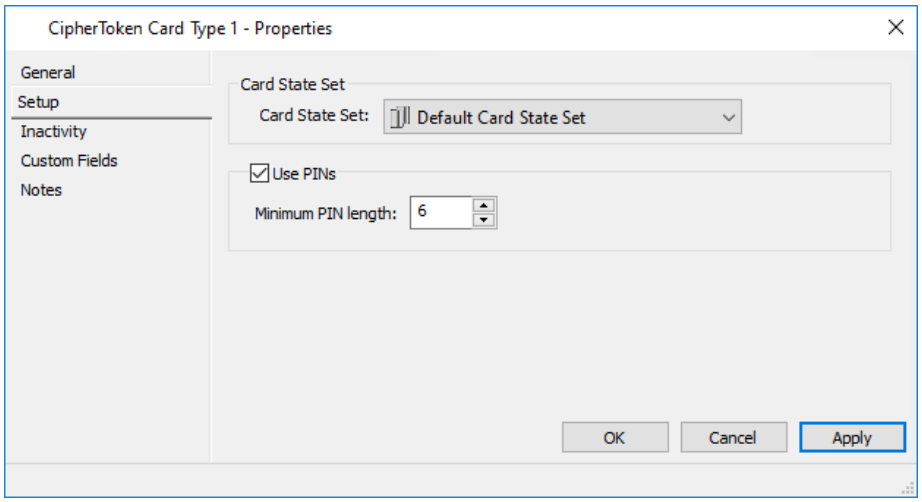
Configuration

To configure a CipherToken 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...CipherToken Card Type**.



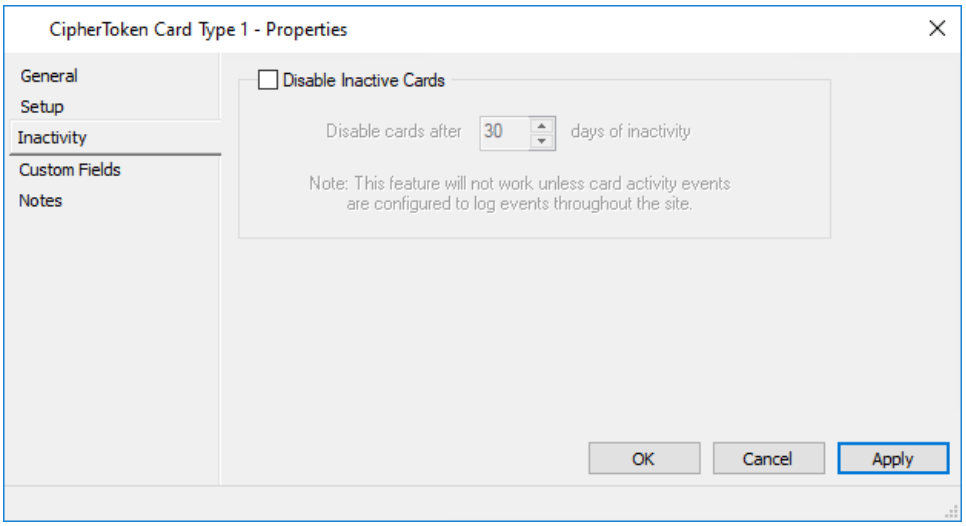
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Setup** tab.



5. Select the appropriate **Card State Set** (if only one exists it will default) to be associated with this CipherToken card type, from the drop-down box.

Note: Once the Card State Set is assigned to the CipherToken Card Type and saved, it cannot be changed.

6. If you want to use PINs, check the **Use PINs** checkbox and set the **Minimum PIN length**. (Default = 6 digits. Range = 4 - 8 digits)
   Notes:
   - If you do not choose to **Use PINs**, the **Assign PIN** button on the Cardholder Cards tile in Command Centre Client will be disabled.
   - The maximum PIN length is **8** digits. There is no mechanism to reduce the maximum size. Hence if a site sets minimum at 6, the user can enter PIN length anywhere from 6 to **8** digits.
7. Click the **Inactivity** tab.



8. Do you wish to enable the Inactive Card Expiry feature?
   Note: All cards of a particular type shall share a common inactivity timeout if enabled.

If...	**then...**
yes	check the **Disable Inactive Cards** checkbox. Go to Step 9.
no	leave the **Disable Inactive Cards** checkbox unchecked. Go to Step 10.

9. Enter a figure to represent the number of days of inactivity that will disable a card.
   Notes:
   - When this feature is first enabled the default timeout = 30 days. The range is 1-999 days.
   - If you set a card type to disable after 1 day of inactivity, these cards will become disabled 24 hours to the second after the **Apply** button is clicked, (e.g. card type set on 27/01/2022 at 16:10:15; if not used these cards become disabled on 28/01/2022 at 16:10:15).
   - 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.)

10. Click the **Custom Fields** tab if you want to add and assign a custom field value to the CipherToken Card Type.
    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 the CipherToken Card Type.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
12. 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 CipherToken Card Type has been created.

Note: Once the configuration is saved it cannot be edited.

Rolling configuration on a CipherToken card

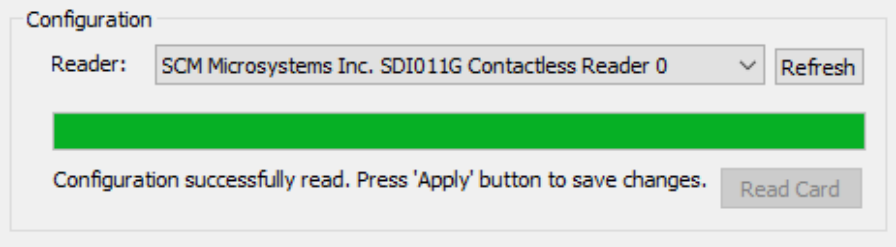
Introduction

If CipherToken keys have been compromised they can be rolled by creating a new configuration card which is then reimported to Command Centre.
Note: Configuration on CipherToken cards can be rolled a maximum of six times. After that, all cards would need reissuing.

This procedure describes how to update/modify the Configuration Key on a CipherToken Card Type.

Configuration

1. Click **File** from the menu bar, then **Server Properties**.
   The Command Centre Server Properties List Window opens.
2. Click the **Standards** tab.
3. Click the **CipherToken** sub-tab.
4. Present the correct card at the reader and click the **Read Card** button.



Result

The system successfully reads the new configuration data, and once the **Apply** button is clicked the configuration is sent to the Controller(s).

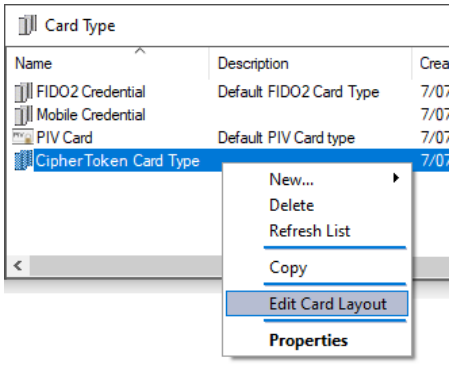
Important: The user must apply the changes.

Configuring and printing CipherToken card layouts

An operator with the correct privileges can configure and/or print card layouts for CipherToken cards.

Operator Privilege	is required to…
"Configure Site"	edit the CipherToken card layout.
"Print/Preview & Encode Card"	print CipherToken cards. **Note:** Card encoding is not supported for CipherToken cards.
"Allow Re-Printing and Re-Encoding"	be able to re-print CipherToken cards. **Note:** If you do not have this privilege and you attempt to re- print a CipherToken card, the following warning message displays: *"The selected card details have already been printed."*

1. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens.
2. **Right click** on the CipherToken card, and select **Edit Card Layout**.



   The **Card Editor** window displays.
3. There are three objects you can add to the CipherToken card layout, (i.e. Text, Image and Barcode).
   Go to the procedure that you require further detail on:
   - ***Adding Text*** (on page 47-20)
   - ***Adding an Image*** (on page 47-22)
   - ***Adding a Barcode*** (on page 47-24)
4. Click the **OK** button.
   The Card Editor window closes.
5. Print the CipherToken card for cardholders as required, referring to ***Printing/Encoding Cards*** (on page 47-55) for the procedure.

When a CipherToken card is printed, an event is generated in the Event Viewer window. The event details:

- the card type and the card number
- who printed the card
- which cardholder had a card printed, and
- the reason for printing the card, if this has been configured

CipherToken cards in Command Centre

Introduction

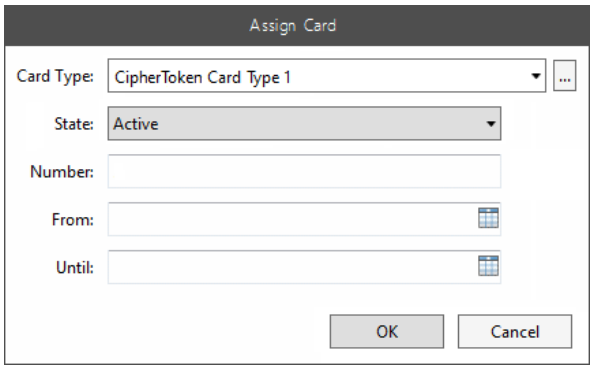
After the CipherToken Card Type has been configured in Configuration Client, CipherToken cards can be assigned to a Cardholder in the Command Centre Client for the purpose of access control at T Series Readers.

Note: CipherToken Cards can only be assigned to Cardholders from Command Centre Client, (i.e. not from Configuration Client).

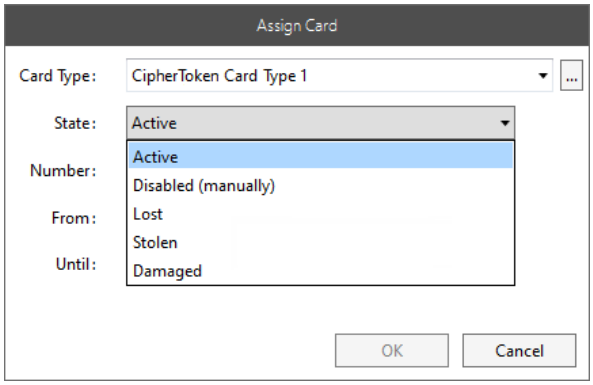
Enrolling CipherToken cards

To assign and activate a Cardholder CipherToken card, perform the following procedure in Gallagher Command Centre Client:

1. From the Cardholder Viewer, locate the Cardholder you want to assign a CipherToken card to.
2. On the Cardholder Cards tile, click the **Assign Card** button.
3. From the **Card Type** drop-down list select the CipherToken Card Type.



4. The **State** indicates the status of the CipherToken Card Type. Select the appropriate **State** from the drop-down list.

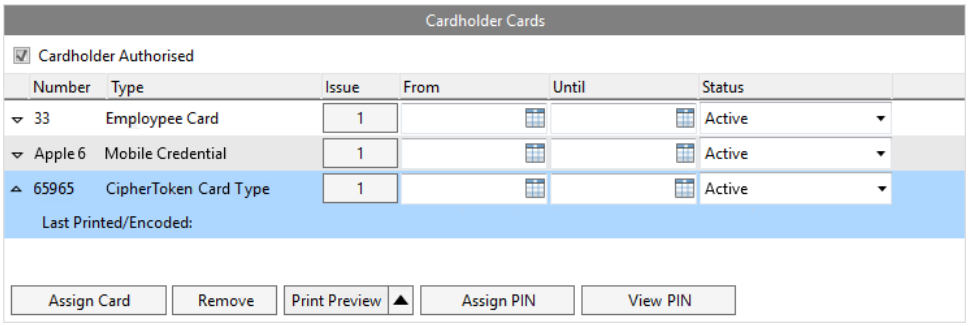


The following table describes the available states.

5. Configure the **Number**, **From** and **Until** fields as appropriate.
6. Click the **OK** button.

   If valid, the **Assign Card** pop-up will close and the card will appear in the grid in the Cardholder Cards tile.

7. To display site information for the CipherToken Card Type, click on the arrowhead to the left of CipherToken Card Type.

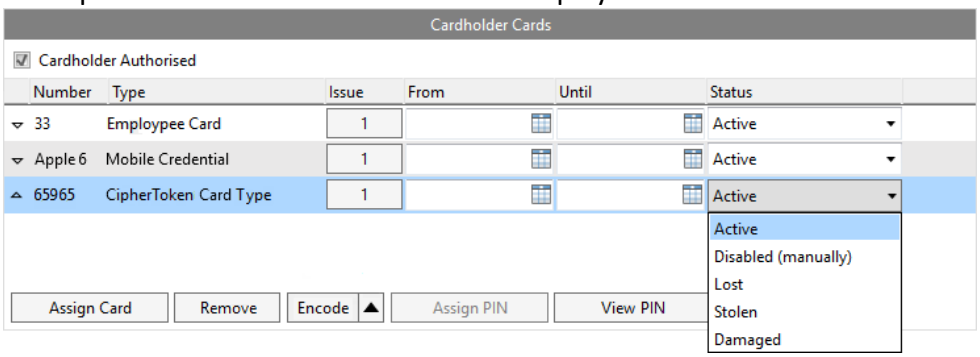


8. Click the **Save** button.
   Note: The **History** tab of a cardholder's properties (in Configuration Client) will also show what has been set during enrolment.

Updating the card state

The state of an enrolled CipherToken card can be changed manually in the Cardholder Cards tile, as follows:

1. Click in the **Status** field of the CipherToken card.
   A drop-down list of the available states displays.

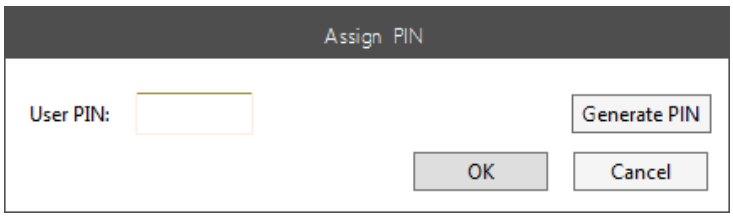


2. Select the required Card State from the drop-down list.
   The Status changes.
3. Click the **Save** button.

Assigning PINs

If the CipherToken Card Type was configured to use PINs (in the Configuration Client), the **Assign PIN** button will be enabled.

1. Click the **Assign PIN** button.
   The Assign PIN pop-up displays.



2. Either:
   - Manually type a PIN number into the first **User PIN** field, and then confirm it by repeating it in the second **User PIN** field, OR
   - Click the **Generate PIN** button to automatically generate a random PIN. **Note:** Generated PINs will only display while the Assign PIN window is open. Once closed, there will be no way of re-viewing the PIN number since the PIN itself is not stored. Generated PINs will be of length equal to the minimum PIN length set against the CipherToken Card type.
3. Click the **OK** button.
   The Assign PIN pop-up closes.
4. Click the **Save** button.

Chapter 72: Entra ID Single Sign-on

Introduction

Entra ID Single Sign-on is a licensable feature, i.e. your licence file must contain the option:

```
[Features]
EntraIDSingleSignOn=1
```

OR

```
[Features]
EntraIDSync=1
```

Single Sign-on refers to the ability to use an Entra ID credential for logging onto one or more applications. Command Centre supports the ability for the system to automatically log an operator onto Command Centre Client using their Entra ID credential, when it is launched. Configuration Client does not support logon using Entra ID Single Sign-on.

Benefits of an Entra ID integration

- A reduction in the number of usernames and passwords people have to remember.
- It allows sites to take advantage of Entra ID logon management for the purpose of logging onto Command Centre. Entra ID allows for the specification of more complex rules for passwords (than is currently available for Command Centre), and can require a combination of authentication methods including biometrics.
- The ability to prevent people from logging on to other applications by disabling their account in a central place (i.e. Entra ID).
- Entra ID credentials can be synced to Command Centre operator accounts using the separately licensed Entra ID Sync feature, reducing manual operator configuration. The Entra ID Sync license also includes the Entra ID Single Sign-on license. For details about this feature, contact the Gallagher Support Team.

Considerations

- **Supported clients:** Entra ID Single Sign-on can only be used for logging onto the Command Centre Client and Visitor Management Kiosk (not Configuration Client). Operators must continue to log onto Configuration Client via Command Centre Client or using other authentication methods.
- **Registry configuration:** The site's Entra ID tenant details must be manually entered in the registry on the Command Centre server.
- **Single tenant:** A Command Centre server can only connect to one app registration of one Entra ID tenant.
- **Multi-server:** If your site is using multi-server, all servers must be licensed for Entra ID Single Sign-on and connect to the same Entra ID tenant and app registration.

- **Windows accounts:** When an operator logs onto Command Centre using Entra ID Single Sign-on, their Entra ID account details are cached to the Windows account they are using, so they do not need to enter their Entra ID account details every time they log onto Command Centre. This means multiple operators with different Entra ID accounts cannot use Entra ID Single Sign-on using the same Windows account. To remove the cached Entra ID account from a Windows account, log onto the machine as the Windows account and delete the following file:

  %LocalAppData%\Gallagher\Command Centre\SSOToken.cache
- **Proxy:** Gallagher suggests that Entra ID Single Sign-on will work using a proxy if:
  - the proxy is configured at the machine level (e.g. via Group Policy) so that services running as Network Service or Computer Account inherit proxy settings, or
  - a dedicated Service Account with the correct user-level proxy settings is used to run the Command Centre service.

  Note: The Command Centre Cloud's proxy is not used for this.

This chapter covers the following topics:

- ***Configuring Entra ID Single Sign-on and Automatic logon*** (on page 72-3)
- ***Entra ID admin center configuration*** (on page 72-4)
- ***Linking operators to their Entra ID account*** (on page 72-5)
- ***Migrating from Active Directory Single Sign-on*** (on page 72-7)

Configuring Entra ID Single Sign-on and Automatic logon

The following configuration is required for an operator to be logged onto Command Centre Client automatically using their Entra ID credential:

- An Entra ID app registration must be configured in Entra ID admin center, and Entra ID details must be configured on the Command Centre server.
  Refer to ***Entra ID admin center configuration*** (on page 72-4) for the procedure.
- The server connected to the workstation from which they are launching the application must be enabled for Entra ID Single Sign-on.
  Refer to ***Operator Defaults*** (on page 6-19) for the procedure.
- The operator's Cardholder record needs to be configured with their Entra ID 'User Principal Name'.
  Refer to ***Linking operators to their Entra ID account*** (on page 72-5) for the procedure.

Entra ID admin center configuration

Introduction

Before Entra ID Single Sign-on can be used with Command Centre Client, an app registration must be correctly configured in Entra ID admin center. Then, Entra ID details must be configured in the Command Centre server's registry. To complete this procedure, you must have access to Entra ID admin center.

Entra ID admin center configuration

1. In Entra ID admin center, add a new app registration.
2. In the registration's **Authentication**, add a platform for Mobile and desktop applications.
3. In the platform, add the following as a custom redirect URI, replacing `[client_id]` with the **Application (client) ID** shown in the app registration's Overview:
   `ms-appx-web://microsoft.aad.brokerplugin/[client_id]`
4. In the registration's **API permissions**, add the following permissions: **offline_access, openid** and **profile**.

Command Centre server configuration

1. On the Command Centre server, open the Registry Editor from the Start menu.
2. Navigate to the following registry key:
   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Gallagher\Command Centre
3. Add the following String values (**right-click** > **String Value**):

String Value name	Value data
OidcAppId	The **Application (client) ID** of the app registration you created in the previous procedure.
OidcTenantId	The **Tenant ID** of your Entra ID tenant.
OidcAuthority	The following URL, replacing `[TenantId]` with your Tenant ID: `https://login.microsoftonline.com/[TenantId]/v2.0/.well-known/openid-configuration`

4. Restart the Gallagher Command Centre Services for these registry values to take effect.

Linking operators to their Entra ID account

Introduction

In order for an operator to log onto Command Centre Client using Entra ID single sign-on (using their Entra ID credential), their Cardholder record needs to be configured with their Entra ID User ID (User Principal Name).

See ***Entra ID Single Sign-on*** (on page 72-1) for further detail about this feature.

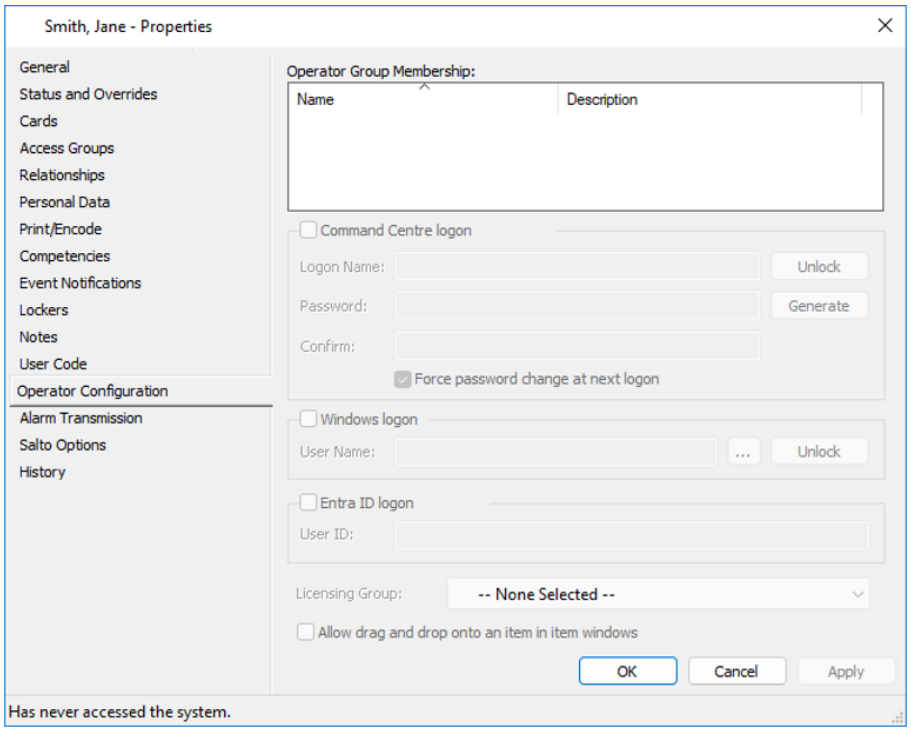
Automating this process

The 'User Principal Name' (and other details) of each Entra ID user can be synced to their Command Centre operator using the separately licensed Entra ID Sync feature. This removes the need for each operator to have their User Principal Name manually typed or pasted into Command Centre. For details about this feature, contact the Gallagher Support Team.

Procedure

To manually assign an Entra ID user's User Principal Name to their Command Centre operator, perform the following procedure:

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
2. Locate and highlight the Cardholder whose User ID you want to assign.
3. Right click and select **Properties**.
4. Click the **Operator Configuration** tab.



Note: If the server to which the workstation connects is enabled for Entra ID Single Sign-on, this tab will display as shown (when the Cardholder is not in an Operator Group).

If the Cardholder was an Operator *before* the server was enabled for Entra ID Single Sign-on, they will already have a Command Centre logon, so the **Command Centre Logon** checkbox will be checked and their logon name will appear in the **Logon Name** field.

If the Cardholder is made an Operator (by assigning them Operator Groups) after the server is enabled for Entra ID Single Sign-on, the **Command Centre Logon** checkbox will be enabled but unchecked, and the **Logon Name** field will be blank and disabled.

5. If the Cardholder is not already an Operator, (i.e. the 'Operator Group Membership' grid is blank), open the **Operator Group** List Window and drag and drop the required Operator Groups into the grid.
6. Check the **Entra ID Logon** checkbox.
   The **User ID** field becomes enabled.
7. In the **User ID** field, type or paste the operator's Entra ID 'User Principal Name'. This can be found in the overview of the user's details in Entra ID admin center.
8. 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.

Migrating from Active Directory Single Sign-on

Introduction

This topic is intended for sites that are already using the Active Directory Single Sign-on feature for Command Centre and want to begin using Entra ID Single Sign-on.

Option 1: Use both Active Directory Single Sign-on and Entra ID Single Sign-on

Active Directory Single Sign-on and Entra ID Single Sign-on can both be used simultaneously. A single operator can even be set up to use both authentication methods, (i.e. Windows logon and Entra ID logon). By default, Command Centre logs an operator on using the last logon method used. If you want to use Entra ID Single Sign-on and continue using Active Directory Single Sign-on, just follow the process outlined in ***Configuring Entra ID Single Sign-on and Automatic logon*** (on page 72-3).

Option 2: Use only Entra ID Single Sign-on

If you want to use only Entra ID Single Sign-on and *not* Active Directory Single Sign-on:

1. Follow the process outlined in ***Configuring Entra ID Single Sign-on and Automatic logon*** (on page 72-3).
   Assign **User IDs** (User Principal Names) to a few operators.
2. For these few operators, disable the **Windows logon** in each operator's properties, to prevent them logging on with Active Directory Single Sign-on.
3. Test that these operators can log into Command Centre Client using Entra ID Single Sign-on.
4. Once you have verified Entra ID Single Sign-on is working, disable Active Directory Single Sign-on in the Server Properties to disable it for all operators. Refer to ***Operator Defaults*** (on page 6-19) for the procedure. You do not need to remove the Windows logons from each operator; they will not be usable once Active Directory Single Sign-on is disabled.