Gallagher Command Centre

Configuration Client User Guide

Volume 1

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 21-46
Linking devices to Controllers 21-48
Creating Inputs and Outputs 21-50
Linking Inputs and Outputs to devices 21-56
Creating Readers 21-57
Configuring HBUS Devices 21-65
Configuring an HBUS Keypad Reader 21-68
Configuring HBUS Terminals 21-74
Configuring an HBUS Contact Card Reader 21-109
Configuring an HBUS I/O Interface 21-127
Configuring an HBUS QuickSwitch Board 21-132
Chapter 22: Doors 22-1
Creating Doors 22-2
Configuring extended access time for a Door 22-11
Interlocking Doors 22-13
Challenge 22-19
Action on Access 22-31
Chapter 23: Elevator Cars 23-1
Low Level Interface Elevator Cars 23-2
High Level Interface Elevator Cars 23-7

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

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

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

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

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

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

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

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

Table of Contents - Volume 2

Part 3: Site Management

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

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

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

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

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

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

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

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

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

Part 4: Site Monitoring

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

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

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

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

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

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

Table of Contents - Volume 3

Part 5: Licensable Features

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter 63: REST API 63-1

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

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

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

Chapter 67: SIP Integration 67-1

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

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

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

Table of Contents - Volume 4

Part 6: Integrated Systems

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

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

Chapter 75: Nedap Readers 75-1

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

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

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

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

Chapter 80: QR Code Readers 80-1

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

Chapter 82: HALO Smart Sensor Integration 82-1

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

Glossary of Terms G-1

Index I-1

Part 1: Introduction to Command Centre

This part of the User Guide includes the following chapters:

- **Chapter 1: Introduction to Command Centre**
- **Chapter 2: Getting Started**
  This chapter provides procedures for basic operations you will perform regularly when using Command Centre
- **Chapter 3: Knowing your way around**
  This chapter provides details to help you navigate around the Command Centre environment.
- **Chapter 4: Utilities**
  This chapter details a number of additional utilities available with the Command Centre.

Chapter 1: Introduction

Command Centre System

Command Centre is a comprehensive access control, alarm monitoring and security management system designed to satisfy the most stringent security requirements.

Control of the Command Centre system is via intelligent 32 bit field devices called Gallagher Controllers. These devices link to a central computer called the Command Centre Server.

Command Centre Server

The Command Centre Server runs on a personal computer (PC) under any of the following Microsoft operating systems:
- Windows Server 2025,
- Windows Server 2022,
- Windows 11 Pro/Enterprise,
- Windows Server 2019

Note: Windows 10 Pro N and 11 Pro N are NOT supported operating systems.

The Command Centre Server is a background application which drives Command Centre Workstations.

The use of a USB mouse for the Server is highly recommended. This is because USB devices support hot swapping, whereas Ps2 devices require a shutdown and restart of the Server in the event of a mouse failure.

Command Centre Workstations

The Command Centre Workstation is the user interface to the Command Centre system. Command Centre consists of two clients, (i.e. Gallagher Configuration Client and Gallagher Command Centre Client).

Workstations are connected to the Command Centre Server via the network. Through the workstations, operators can monitor, modify and manage the entire system, or selected parts of it, depending upon their allocated privileges.

Note: Microsoft Windows allows the size of text and other items to be changed via **Control Panel** > **Display**, however Command Centre does **not** support alternate icon sizes, (i.e. only the default option of 100% is supported).

Foreign Languages

While English is the default language for Command Centre, there is the ability to translate it into other languages. Languages are a licensable feature, and only dialects and languages listed in the 'Language' key in the

licence file are available to a site. All sites are by definition licensed for the fallback language, even if the fallback language is not specifically mentioned.

This manual

This manual describes the operation of the Command Centre Workstations and the actions the operators can perform in Configuration Client only. There is a separate manual available for Command Centre Client.

Command Centre database integrity recommendations

Sites have full access to the Command Centre databases. This means administrators can grant local and/or domain Windows users access to edit, manage and maintain the SQL Instance and attached Gallagher (CCFT) databases.

Customer Responsibilities
As per the Software License and Maintenance Terms and Conditions accepted upon installation of Command Centre, Gallagher will not be liable in any circumstances for the loss or corruption of data.

It is the responsibility of the customer to:

- Not modify any Data, Metadata or Schemas in the Gallagher Command Centre databases by any method other than via the Gallagher Command Centre Application.
- Not share the database instance with other services.
- Not upgrade the databases while in Availability groups.
- Implement appropriate measures to ensure adequate levels of data security.
- Manage, monitor and maintain their Gallagher Command Centre databases, this includes backups (scheduled and manual), archiving and database transaction log files.
- Accept full responsibility for any data loss or corruption associated with the unauthorized modification of data or schemas within the Gallagher system.
- Accept that if the event data is required for legal purposes, Gallagher will be unable to verify that the data has not been altered by an unauthorized method, or software outside the Gallagher Command Centre application.
- Communicate promptly and completely in response to all issues and requests for information from Gallagher.

Support Approach
Support requests resulting from the tampering, corruption, failure to maintain transaction log files or unauthorized modification of any Gallagher system Data or Schema will be at the Customers full cost where possible.

Chapter 2: Getting Started

This chapter details a number of operations you will perform regularly when using the Command Centre system.

- ***Logon*** (on page 2-2)
- ***Restricting System View*** (on page 2-9)
- ***Logoff*** (on page 2-11)
- ***Automatic Logoff*** (on page 2-12)
- ***Exit*** (on page 2-13)
- ***Help*** (on page 2-14)
- ***Operator Passwords*** (on page 2-15)
- ***Dual Monitors*** (on page 2-24)
- ***Magnetic window snapping*** (on page 2-25)
- ***Using the advanced drag and drop feature*** (on page 2-26)

Logon

Introduction

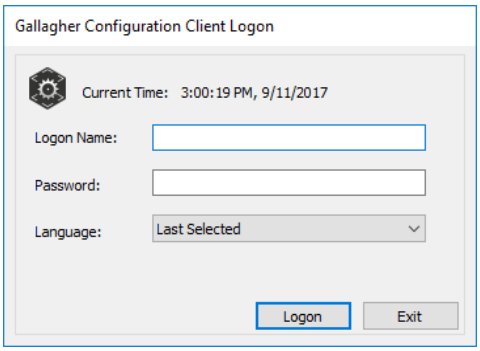
You must log on to the Configuration Client to access the system operations.

Notes:

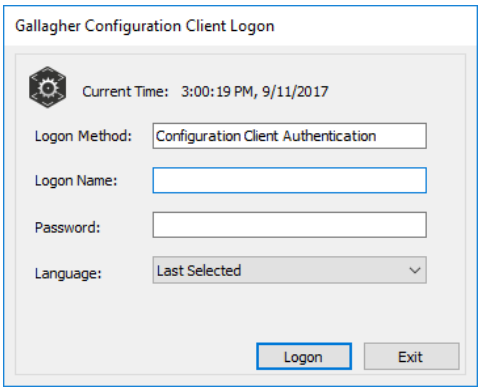
- Workstations can be on a different build to the server, but it has to be lower OR equal to the server version. When Command Centre is launched, if the version number is newer than the server, logon will fail and the message *"The client version is incompatible with the server. Startup failed!"* will display on the splash screen.
- When the Configuration Client is launched, if the server to which the workstation 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 Configuration Client. If Active Directory single sign-on is being used, ensure you have a domain account, (e.g. Windowsuser@Gallagher.Local).
- The following procedure describes the 'standard' method of logging on to the Configuration Client, (i.e. via entry of a valid operator username and password). However, it may be possible to log on and off designated Configuration Client workstations using a FIDO2 authenticator, if cardholders have FIDO2 Credentials enrolled against them. For further detail refer to ***Logon with FIDO2 Credentials*** (on page 2-7).

Procedure

1. Open the Configuration Client by either:
   - double-clicking the **Configuration Client** icon on your Desktop, OR
   - from the **Start** menu, click **All Programs** > **Gallagher** > **Configuration Client**.
2. Is your site licensed for Active Directory single sign-on?

If...	then...
no	the following logon screen displays:  Go to Step 4.
yes	if automatic logon is possible, the Configuration Client main window displays. If not, an error message informing the user of the reason logon

If...	then...
	has failed displays, followed by the logon screen next:



Note: For the system to automatically log the operator onto the Configuration Client 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 the Configuration Client.

Go to Step 3.

3. Select the appropriate Authentication Logon method from the **Logon Method** drop-down box.

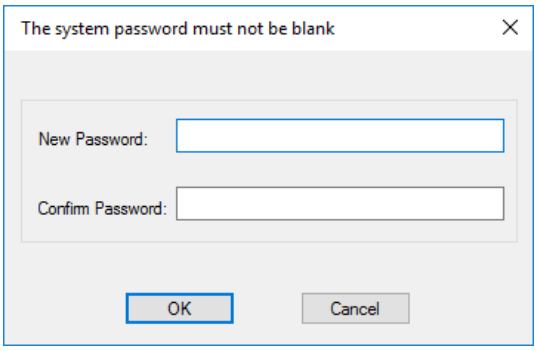
If you click...	then...
Windows Authentication,	the system will find the operator linked to the user's domain account and log onto the workstation as that operator.
Configuration Client Authentication,	this allows the operator to enter a Configuration Client Logon Name and Password. Go to Step 4.

4. Type your **Logon Name**.
   Note: When you first log on as the system operator, **system** is the default 'Logon Name', but there is no default 'Password'. For any other operator logging on, the **Logon Name** will be blank for a new install on a workstation or server that has not had an attempted logon. After that, it will be populated with last attempted Logon Name for that workstation or server.
5. Click within the **Password** field.
   (Alternatively, press the **Tab** key.)
6. Type your password.
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.

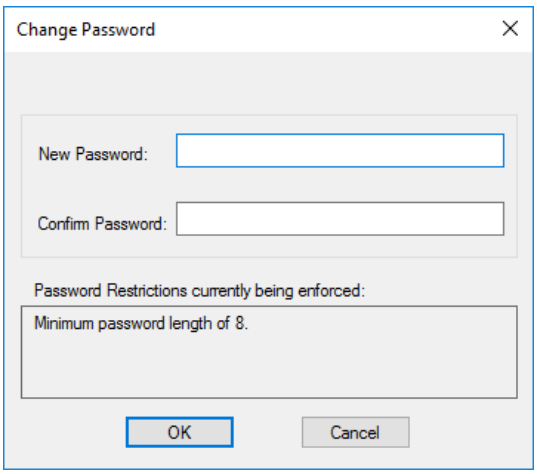
8. Click **Logon**.
   (Alternatively press the **Enter** key.)

   Notes:

   - If you do not have the "Launch Configuration Client" operator privilege, the following message appears on the logon screen:
     "You do not have the privilege to launch the configuration client. Please contact your system administrator".
   - When you log on for the first time as the system operator, the system password must not be left blank, therefore the following screen displays:



     When other operators log on for the first time the following screen will display so they can change their password from the one the system administrator provided them with:

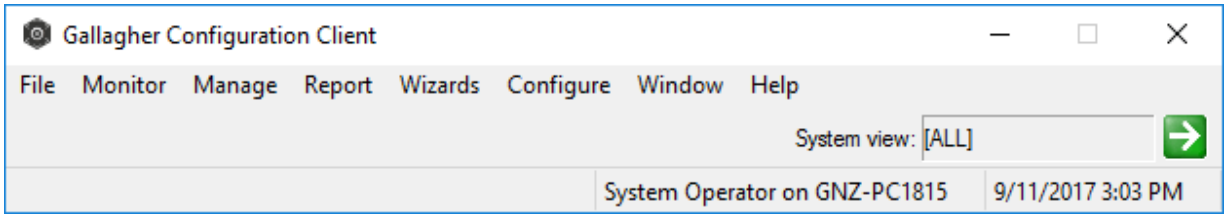


     1. Type in the **New Password**.
     2. **Confirm Password** by re-typing it.
     3. Click the **OK** button.

   - The System Operator is initially used to set up Command Centre. Once other operators have been created, the System Operator should be disabled by another operator.
     See ***Disabling the System Operator*** (on page 32-34) for further detail.

Result

- The Logon window is removed from the screen.
- The Configuration Client main window displays providing the following information:



  - Your user name
  - The current date and time
  - A **System view** drop-down box may also display, depending on whether you have the operator privilege to see it, (i.e. the "Select System View" or "Advanced User" operator privilege). If it does display, you can restrict (change) your system view. See ***Restricting System View*** (on page 2-9) for further detail.

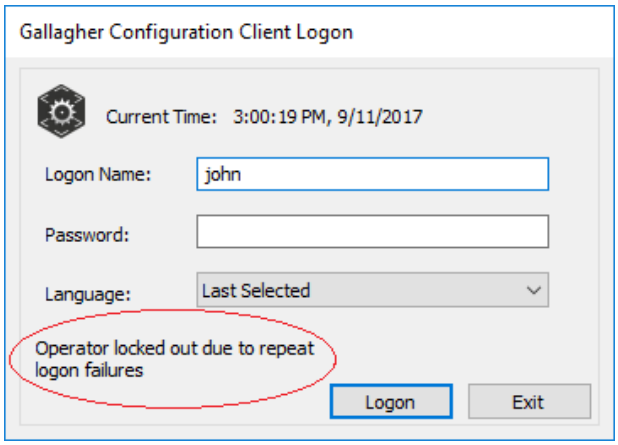
  Note: The Configuration Client main window can be resized down to 480px if required.

- A visual Activity Indicator 

may display to indicate that the Configuration Client is communicating with the server. The purpose of this indicator is to provide operators with confirmation that the Configuration Client has not ceased operation.
  The Activity Indicator can be enabled/disabled via the **Advanced** tab of the Server Properties. (See Advanced.) Once enabled, the Activity Indicator is always visible while the Configuration Client is running and responding, and can be moved anywhere on your screen by clicking on it and holding down the mouse button, then dragging it.
- You can access those menus available to you.
  Note: Depending on your operator privileges or current system view, some of the menu options shown on the screen above may not appear.
- The session will be added to the list of sessions visible in the Operator Sessions Viewer of the Configuration Client and the Operator Sessions tile in the Command Centre Client.

Hint

Failed logons
If an operators' successive logon attempts reach 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. See ***Unlocking an Operator account*** (on page 2-20) for further detail.

Note: Lockout state does not get replicated to remote servers in a multi-server environment.

Logon with FIDO2 Credentials

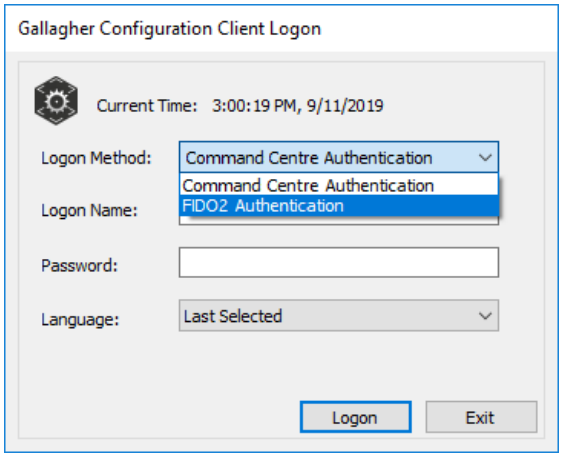
Introduction

Cardholders that have FIDO2 Credentials enrolled against them can log on or off designated Command Centre workstations with a FIDO2 authenticator.
Note: FIDO2 Credentials are only supported from Windows 10, version 1903.

Configuration of FIDO2 Credentials is performed in Command Centre Client. For further information refer to the "FIDO2 Credentials" section in the *Command Centre Client Help file.*

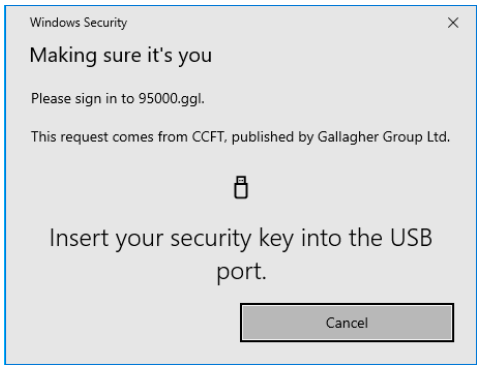
Procedure

1. Open Configuration Client by either:
   - double-clicking the **Configuration Client** icon on your Desktop, OR
   - from the **Start** menu, click **All Programs** > **Gallagher** > **Configuration Client**.
2. Select "FIDO2 Authentication" from the **Logon Method** drop-down list.

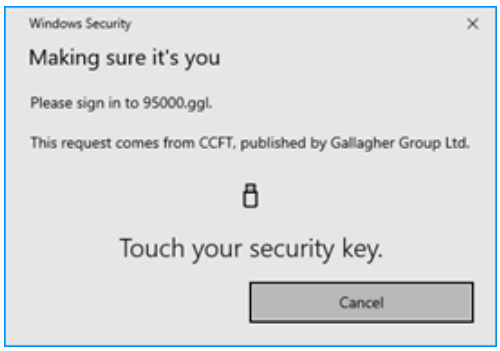


Once "FIDO2 Authentication" is selected, the Password field is disabled (greyed out).

3. Type your **Logon Name**.
4. Click the **Logon** button.
   The username is sent to the server, and Windows prompts for the FIDO2 token.



5. Insert the FIDO2 token (and biometric/PIN if applicable).
   Verification data is passed to the server, and you are prompted to 'touch' the token to verify there is someone there.



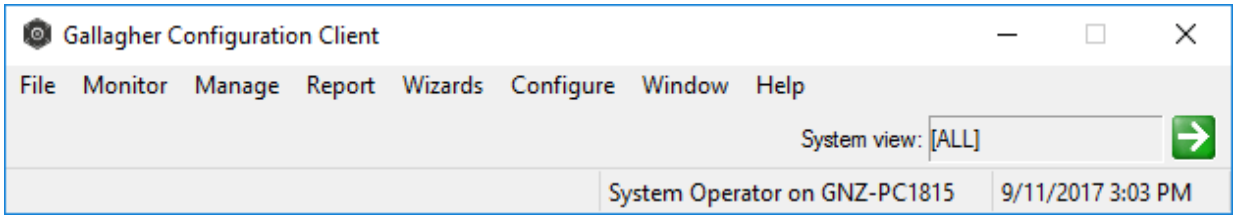
   Note: The system will time out if no action is taken within 60 seconds.

6. Does the system verify the token?
   If **yes**, you are logged into Command Centre Configuration Client.
   If **no**, a message displays indicating the reason why access is denied.

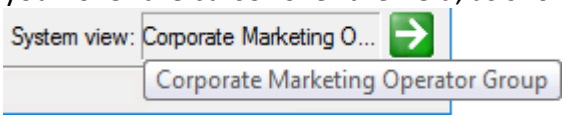
Restricting System View

Introduction

When an operator logs on to Command Centre the **System view** field (on the Command Centre main window) displays their system view selection retained from their last log off. Their system view is limited to the site items, cardholders, Personal Data Fields (PDFs) and operator privileges assigned to them from the selected Operator Groups.



The content of the **System view** field changes as follows:

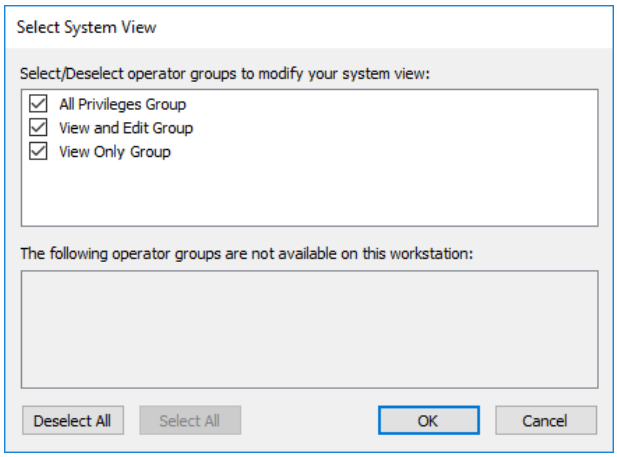
Content	Description
[ALL]	This displays if the current system view includes **all** Operator Groups available to the operator at this workstation.
[Restricted view]	This displays if the current system view includes only **some** of the operator's Operator Groups.
<Operator Group Name>	The name of the Operator Group displays if the current system view includes only **one** Operator Group. **Note:** If the name of the Operator Group is too long to fit in the **System view** field, it will appear as a "Tool Tip" when you hover the cursor over the field, as shown below: 

Note:
If an operator's system view was restricted, (i.e. did not include **all** Operator Groups) when they last logged off, the next time they log on the **Select System View** screen will display before the Command Centre main window appears. This allows an operator to confirm their system view, by either retaining the existing view or altering it.

Procedure

This procedure describes how an operator can restrict (change) their system view. For operators to be able to perform this procedure they require the "Select System View" operator privilege.

1. From the Command Centre main window, click the button beside the "System view" field.
   The **Select System View** screen displays.



The selections already made on this screen reflect your current system view, and the list of Operator Groups includes **all** Operator Groups that you belong to.

2. Select the Operator Groups that you want to include in your current system view. You can either check or uncheck individual Operator Group checkboxes, or use the buttons available.

Button	Description
Select All	Checks **all** the Operator Group checkboxes.
Deselect All	Unchecks **all** the Operator Group checkboxes. If you belong to many Operator Groups, and you want to restrict your system view to only a few of them, this is a quick method of achieving that rather than unchecking all the groups you do not want to include in your view. Click the **Deselect All** button and then re-check the groups you want. **Note:** If you leave all Operator Groups unselected the **OK** button becomes disabled, forcing you to select at least one group.
OK	Saves the settings you have chosen, and closes the **Select System View** screen.
Cancel	Cancels the changes you made and closes the **Select System View** screen.

Result

Your system view has been restricted.

Note: Changing System View in Configuration Client does not affect what an Operator can see and do in Command Centre Client, and vice versa.

Logoff

Introduction

For system security and integrity, it may be important to log off when away from the workstation.

Procedure

1. Click **File** from the menu bar.
2. From the drop-down menu, click **Logoff**.

Result

- Your user name is removed from the Command Centre main window.
- The Logon window automatically displays; waiting for the next operator to logon.

Automatic Logoff

An "automatic logoff" time can be configured so that operators are logged off 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.

Automatic Logoff

An "automatic logoff" time can be configured so that operators are logged off after a specified period of inactivity, closing all windows and discarding any unsaved changes. There are various methods of configuring this, depending on what is required:

- for the entire system via the **Operator Defaults** tab of the Command Centre Server properties.
  (see ***Operator Defaults*** on page 6-19 for further detail)
- by workstation, via the **Restrictions** tab of the Workstation properties.
  (see ***Creating a new Workstation Item*** on page 28-2 for further detail)
- by Operator Group via the **Operator Group Restriction** tab of the Operator Group properties.
  (see ***Setting up Operator Groups*** on page 36-5 for further detail)

Notes:

- Automatic logoff times specified for a workstation will override any automatic logoff time configured for the entire system via the Server Properties.
- If a task that takes a long time, (e.g. Activity Report), is being carried out at the time of "automatic logoff", this constitutes activity on the workstation. This prevents an operator from being logged off while waiting for a task to be completed by the system.
- When an operator belongs to two or more Operator Groups with differing automatic logoff restrictions, the lowest inactivity time takes precedence.
  For example:
  The automatic logoff time for Operator Group 1 is 30 minutes, and 45 minutes for Operator Group 2. Operator X belongs to both Operator Groups 1 and 2, so will be logged off after 30 minutes of inactivity.
- When a workstation logoff restriction applies as well as an operator group restriction, the lowest inactivity time takes precedence.
  For example:
  The automatic logoff time for Operator Group 1 is 30 minutes, and 10 minutes for Workstation Z (which has Operator Group 1 included in its restrictions). Operator X belongs to Operator Group 1 and is logged into Workstation Z, so will be automatically logged off after 10 minutes of inactivity.

Exit

Introduction

In one procedure, you can log off and close the Command Centre interface on your workstation.

Procedure

1. Click **File** from the menu bar.
2. From the drop-down menu, click **Exit**.

Result

This workstation's *view* of the Command Centre interface is closed.
Note however, the actual Command Centre system is still "running" on the server.

Note:
It is possible to configure Gallagher Command Centre Workstations so that operators cannot exit from them. This avoids accidental closure of the workstation, and is configured by checking the **Disable Exit from Command Centre** checkbox on the **Configuration** tab of the Workstation properties. Checking this disables:

- the **Exit** button on the **File** menu bar,
- the  button in the top right-hand corner, and
- Close <**Alt**+**F4**>

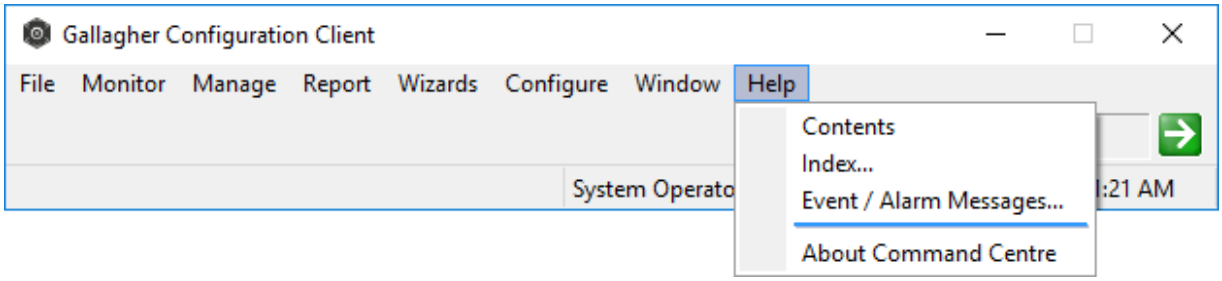
Help

Introduction

If you are unsure of a procedure, or you are learning a new feature, you can display the information on screen via the Help menu.

Procedure

1. Click **Help** from the menu bar.



2. From the displayed drop-down menu, select which **help option** to display on screen:

   Contents

   Click Contents to browse through topics by category.

   Index...

   Click Index to see a list of index entries; either type the word you are looking for, or scroll through the list.

   Event/Alarm Messages...

   Click Event / Alarm Messages to see a full list of all the messages in Command Centre. A further explanation of each message is provided along with the Event Group and Event Type it belongs to.

   About Command Centre

   This window displays:

   - the **Product Version** number of Command Centre currently running, **Note:** The Server Version number will display in brackets beside the Product Version number if it doesn't match.
   - the Command Centre license **Serial Number**,
   - a number of Copyright notices for third party components used in the Configuration Client, and
   - a clickable link to the home page of the Gallagher Security website.

   Click the **OK** button to close this window.

Operator Passwords

Operator passwords are configurable via the **Operator Defaults** tab of the Command Centre Server Properties (see ***Operator Defaults*** on page 6-19). From there, the following password restrictions can be specified:

- The minimum password length.
- Whether there must be mixed case in the password.
- If and how often the password expires.
- Whether there must be non-alphabetic characters in the password.
- How many passwords are remembered to make sure operators don't just enter the same password when they are forced to change them.

This section covers the following topics:

- ***Changing Operator Passwords*** (on page 2-16)
- ***Resetting Operator Passwords*** (on page 2-18)
- ***Unlocking an Operator account*** (on page 2-20)
- ***Preventing context specific passwords*** (on page 2-22)

Changing Operator Passwords

Introduction

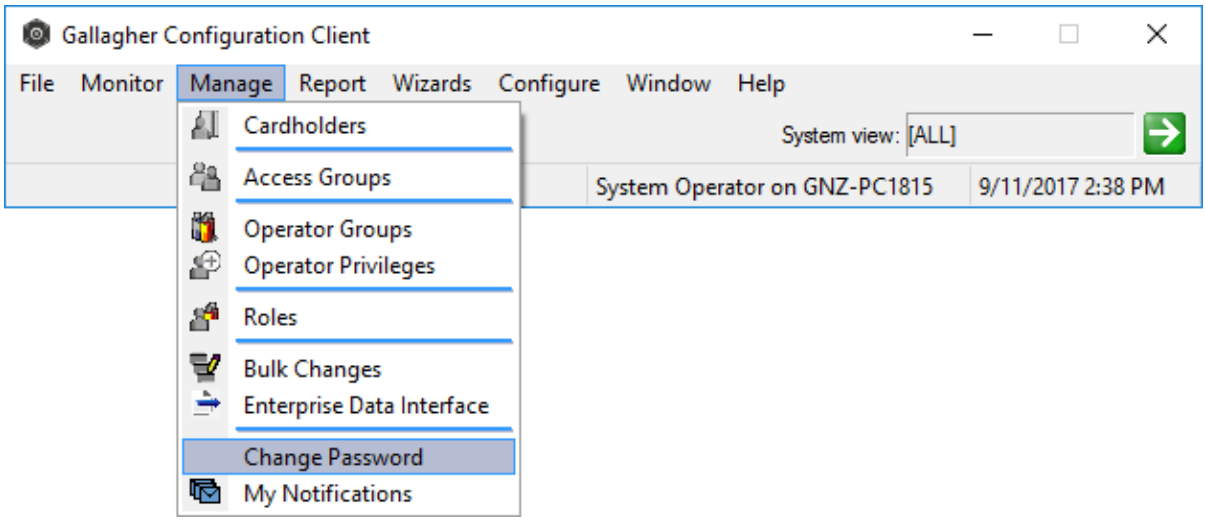
When a system administrator sets up an operator in Command Centre, they will provide the operator with a Logon Name and Password. When the operator logs on to Command Centre for the first time they need to change their password. As standard practice operators should change their password routinely, (i.e. once a month is a good duration). This helps protect the operator, should someone obtain their password without their knowledge.

This option should also be used anytime an operator suspects their password integrity has been lost.

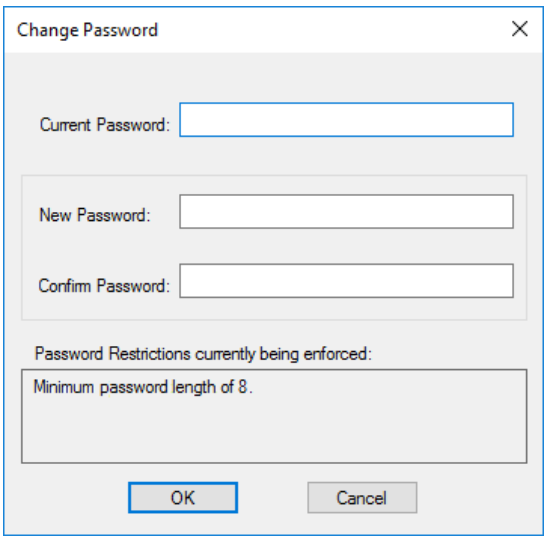
Note: To add new operators, see Adding a new Cardholder.

Procedure

1. Click **Manage** from the Menu bar.

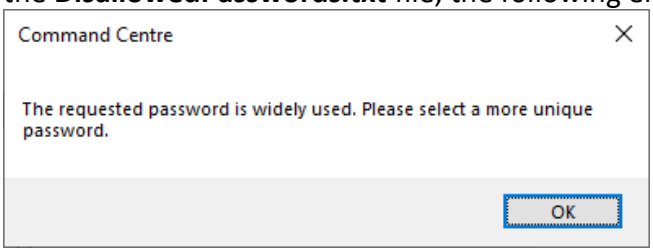


2. Click **Change Password**.

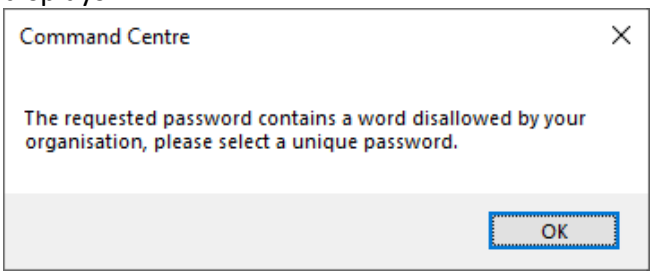


3. Type in the **Current Password**.
   Notes:
   - Make sure that your new password complies with any 'Password Policy' restrictions on this window. These restrictions have been configured on the **Operator Defaults** tab of the Command Centre Server Properties (see ***Operator Defaults*** on page 6-19).
   - For each character you enter (in all the fields on this window), an asterisk will display so that your current and new passwords are not visible.
4. Type in the **New Password**.
5. Confirm the **New Password** by re-typing it.
6. Click **OK**.
   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 further details see ***Preventing context specific passwords*** (on page 2-22).

Result

The operator's password is changed.

Resetting/Generating Operator Passwords

Introduction

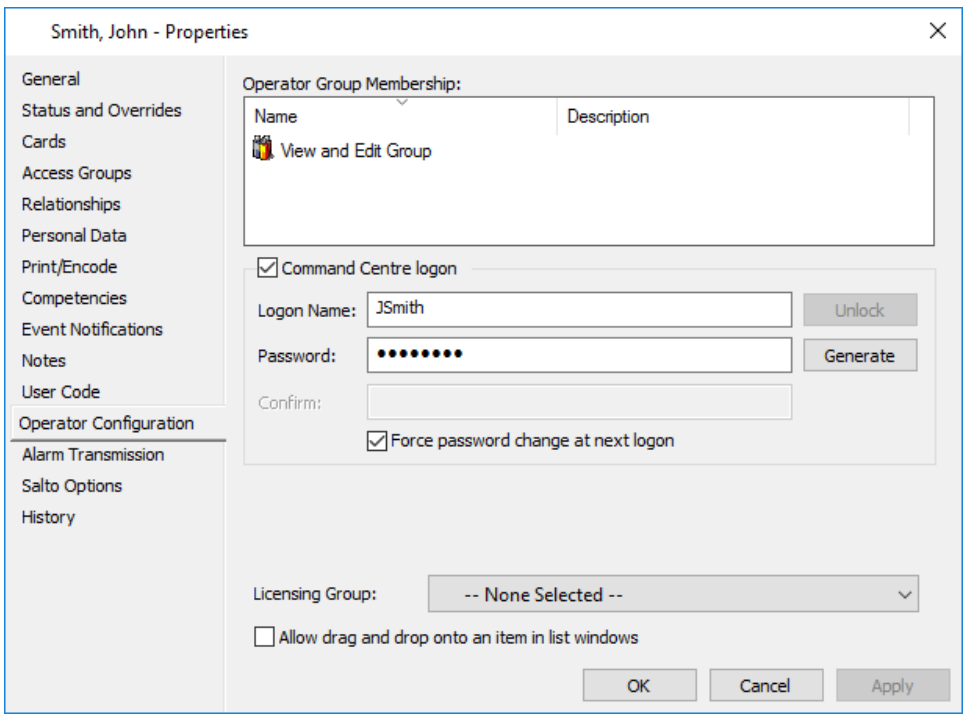
Examples of when a system administrator would need to generate/reset a password:

- An operator password may need to reset if they forget their password
- The System Administrator may want to reassign an operator login to someone else, (e.g. if they were using a generic operator name rather than specific ones), then they would generate a new password so the new person could login.

Only the System Operator, or an operator with the correct privileges, can reset passwords.

Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Highlight the operator whose password needs resetting.
3. **Right click** the mouse button.
4. From the displayed drop-down menu, select **Properties**.
   By default the **General** tab displays.
5. Click the **Operator Configuration** tab.



6. Generate a password for the operator by either:
   - manually typing a password into the **Password** field, and re-typing it in the **Confirm** field, OR
   - clicking the **Generate** button to generate a random password.
     A system generated password populates the **Password** field.
7. Check the **Force password change at next logon** checkbox.
   Note: This will already be checked if either the **EN50131 Compliance** or **SSF1014 Compliance** checkbox is checked on the **Standards** tab of the Server Properties.
8. Click the **OK** button.

Result

An operator's password has been reset/generated.
The first time the operator logs on they will be forced to change their password.

Unlocking an Operator account

Introduction

If an operators' successive logon attempts reach 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.

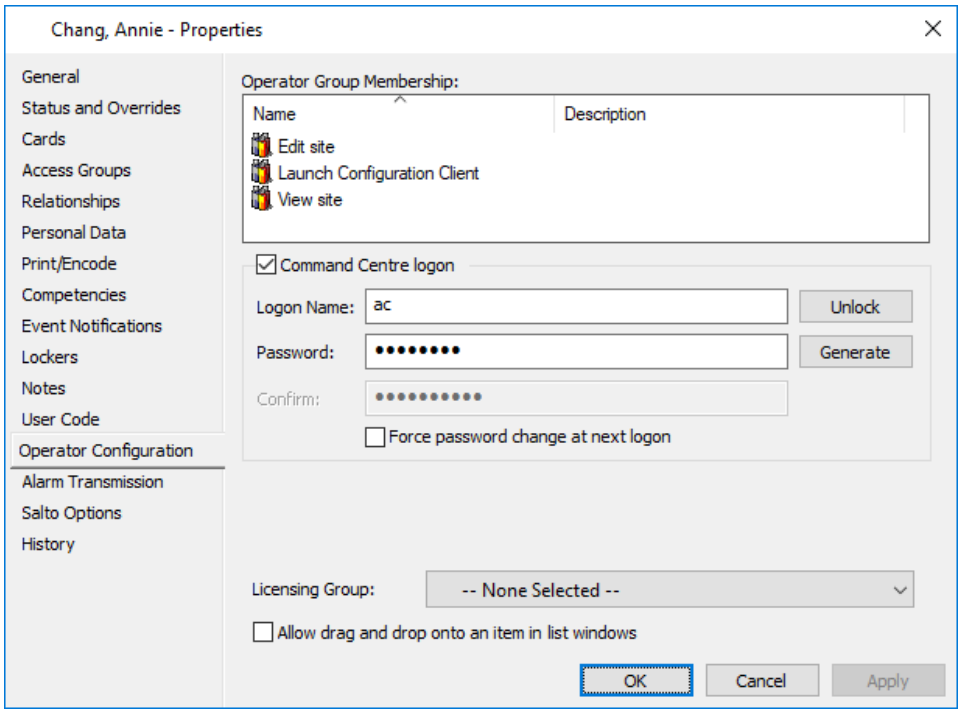
Note: Lockout state does not get replicated to remote servers in a multi-server environment.

A privileged operator (with the "Edit Operators" privilege) can clear an account lockout for an operator in the Configuration Client by either:

- selecting the **Unlock** button on the appropriate operator/cardholder record, OR
- by resetting an operator's password

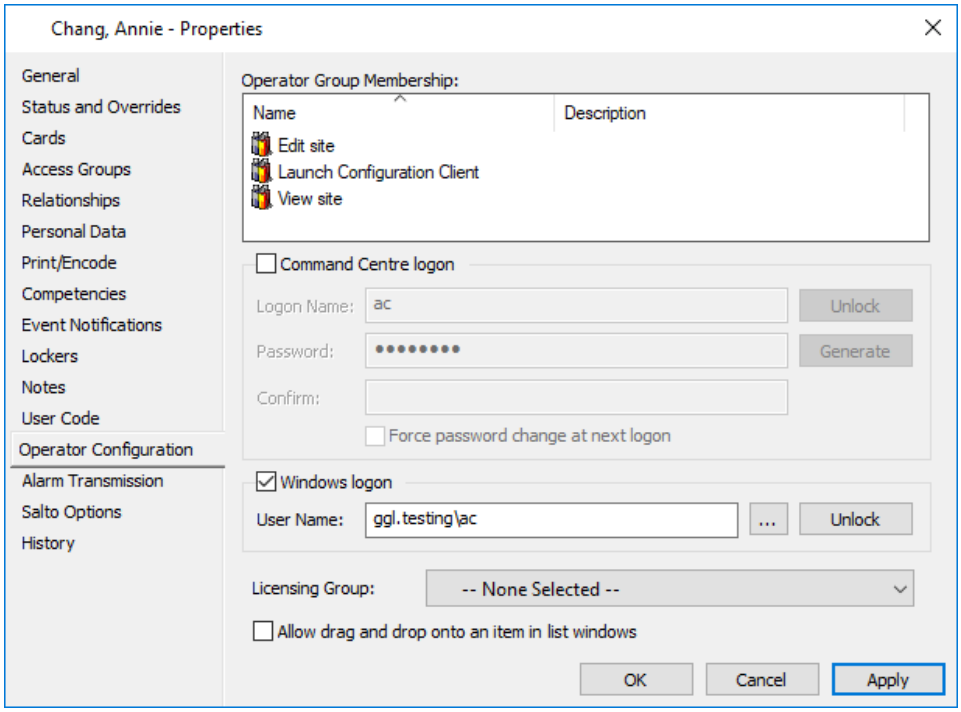
Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
2. Locate, and highlight, the operators' name.
3. **Right click** and select **Properties**.
4. Click the **Operator Configuration** tab.
   If the server to which the workstation connects is NOT enabled for Active Directory Single Sign-on, this will display as shown:



Note: The **Unlock** button is enabled, indicating that the operator account is locked out.

If the server to which the workstation connects is enabled for Active Directory Single Sign-on, this tab will display as shown:



5. Click the **Unlock** button.
   The account is unlocked and the message *"The operator account has been unlocked"* displays.

   Note: If the lockout occurs for a configured period of time, and if the operator record remains open during the process, the **Unlock** button will not disable after that time has elapsed. However, the Unlock button will disable on successful logon.

6. Notify the operator that their account has been unlocked.

Preventing context specific passwords

Introduction

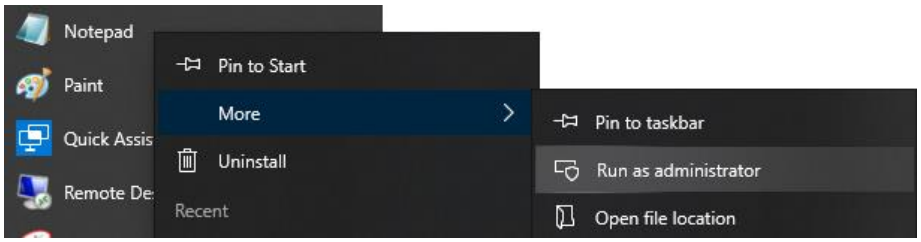
As well as configuring 'Password Policy' restrictions on the **Operator Defaults** tab of the Command Centre Server Properties, sites can also control allowed passwords through the following two files that are pre-installed with Command Centre in `C:\Program Files(x86)\Gallagher\Command Centre\Bin`:

- **DisallowedPasswords.txt** contains a list of commonly used passwords which should be avoided, therefore are not allowed
- **ContextSpecificPasswords.txt** is initially empty but can be edited to contain a list of strings that should not be included in any password, (e.g. product names, company names). The list is case insensitive.
  For example: If *gallagher* is in this list, any word containing *gallagher* will not be allowed as a password; G*allagher*, *gallagher, gallagher1!*
  Note: The maximum file size supported is 10MB.

Procedure

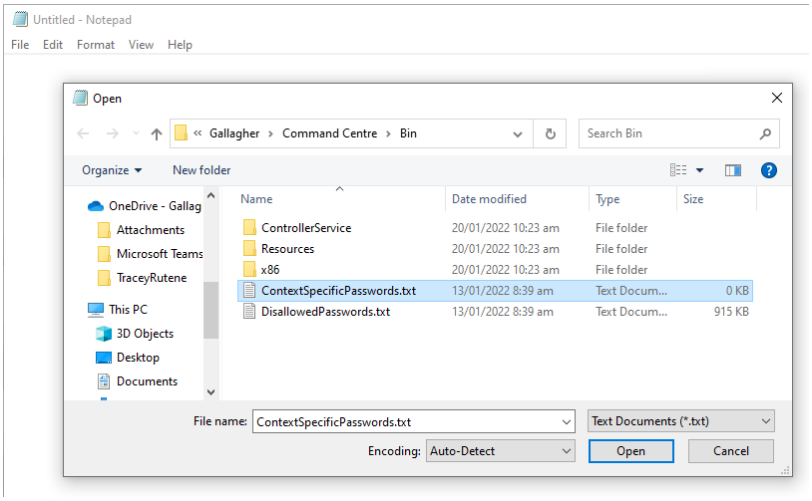
To add to the list in either the **DisallowedPasswords.txt** or **ContextSpecificPasswords.txt** file:

1. Path your way to `C:\Program Files(x86)\Gallagher\Command Centre\Bin`.
2. **Right-click** on Notepad, and select **More** > **Run as administrator**.



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

3. In Notepad, select **File** from the menu bar, then **Open…**
4. Path your way to `C:\Program Files(x86)\Gallagher\Command Centre\Bin` and select either the **DisallowedPasswords.txt** or **ContextSpecificPasswords.txt** file.



5. Click the **Open** button.
6. Make changes as necessary.
7. Select **File** from the menu bar, then **Save.**
   Note: Restarting the Command Centre service may be needed for the changes to take effect.

Dual Monitors

Introduction

Command Centre supports dual monitors. If a workstation has been set up in Windows to operate with dual monitors, Command Centre acknowledges this by allowing the operator to make use of both monitors that make up the desktop.

When a window's position is saved, and the desktop comprises of dual monitors, its position is saved relative to the entire desktop area, (i.e. not relative to a particular monitor).

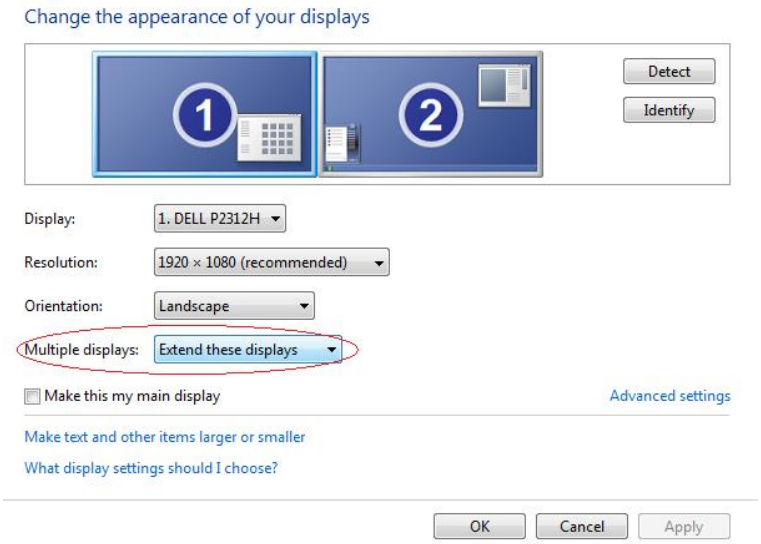
Operator preferences for the size and position of windows are saved on a "per operator" basis, (i.e. not on a "per operator/workstation" basis).

Limitations

- When using Gallagher Command Centre on a multi-monitor PC, Command Centre will expand to cover the Windows Task bar when maximized.
- When Windows taskbar is set to auto-hide, Gallagher Command Centre will not allow the task bar to peek over Command Centre and the client will need to be minimised or restored to allow visibility of the task bar.

Recommended Setup

1. From the **Control Panel**, click **Display**.
2. Click the **Change display** s**ettings** option.
   The recommended desktop setup for dual monitors has the Primary monitor on the left and the Secondary monitor on the right, as shown in the following screen shot:



3. Select "Extend these displays" from the **Multiple displays** drop-down.
4. Click the **OK** button.

Magnetic window snapping

This feature enables an operator to move and/or resize windows to align them perfectly with each other and with screen boundaries, as follows:

- Attach List Windows to the main window.
  This is achieved by dragging the List Window towards the main window and when it is close it will 'snap' into position. When the main window is moved the 'attached' List Windows will move also.
- Align List Windows to the edge of "Desktop Work Area".
  This is achieved by dragging the windows towards the edge of the "Desktop Work Area" and when it is very close it will 'snap' into position.
  Note: This includes the area on all monitors, in the case of dual monitors, excluding the task bar area.

Notes:

- If there is more than one edge it could snap to, it chooses the closest edge.
- If the alarm viewer is set to appear on occurrence it will appear over the top of other windows when an alarm occurs.
- If the alarm viewer is set to always be top, and you try to snap a window over the top, it will snap to position, but be placed below the alarm viewer, (i.e by moving the alarm viewer aside, the window will appear).
- All windows in Command Centre perform magnetic snapping, (e.g. List Windows, property pages, etc.), with the exception of the Enterprise Data Interfaces.

Hint

Temporarily turning "snapping" off
Magnetic window snapping can be temporarily turned off by holding down the <**Ctrl**> key whilst moving or resizing the window. The dragging of all windows snapped to the Main window can likewise be disabled by holding the <**Ctrl**> key at the moment at which the dragging began.

Using the advanced drag and drop feature

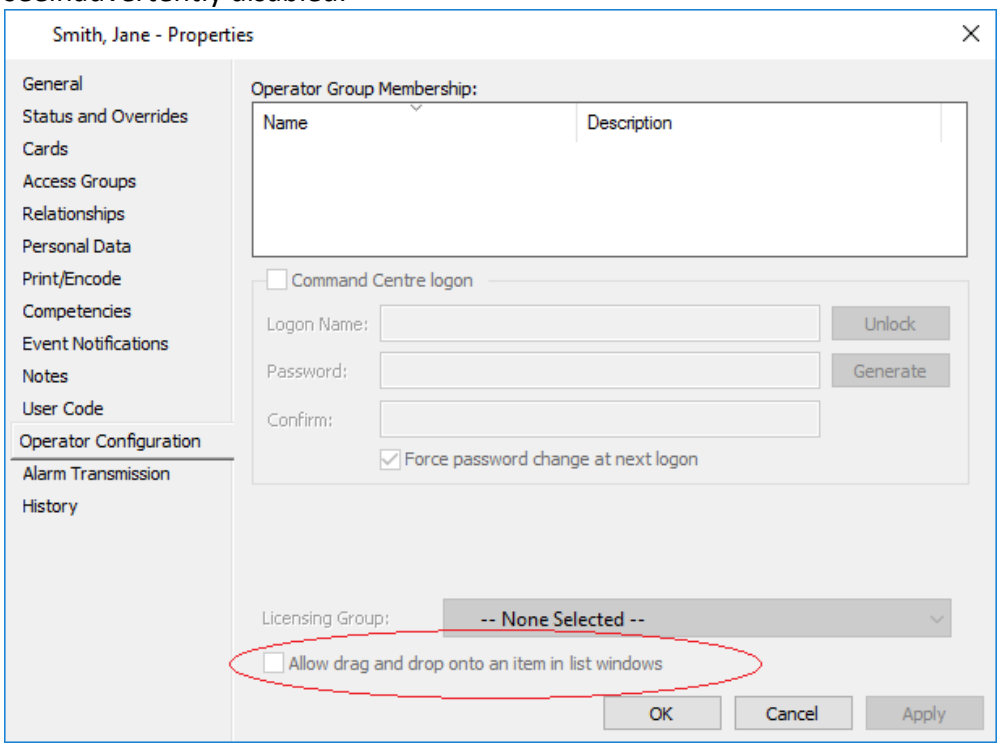
Introduction

The advanced drag and drop feature allows operators to drag and drop certain items directly from their own List Window into an item on another List Window, as follows:

- An Access Group can be dragged and dropped onto a Cardholder to put the cardholder into the Access Group.
- A Cardholder can be dragged and dropped onto an Operator Group to put the Cardholder into the Operator Group.

This procedure describes how an operator uses the advanced drag and drop feature.

Note: For operators to use this feature, there is an **Allow drag and drop onto an item in list windows** checkbox (on the **Operator Configuration** tab of the Cardholder properties). By default, this is enabled. However, if an operator experiences problems using this feature, check that it has not been Oh I seeinadvertently disabled.



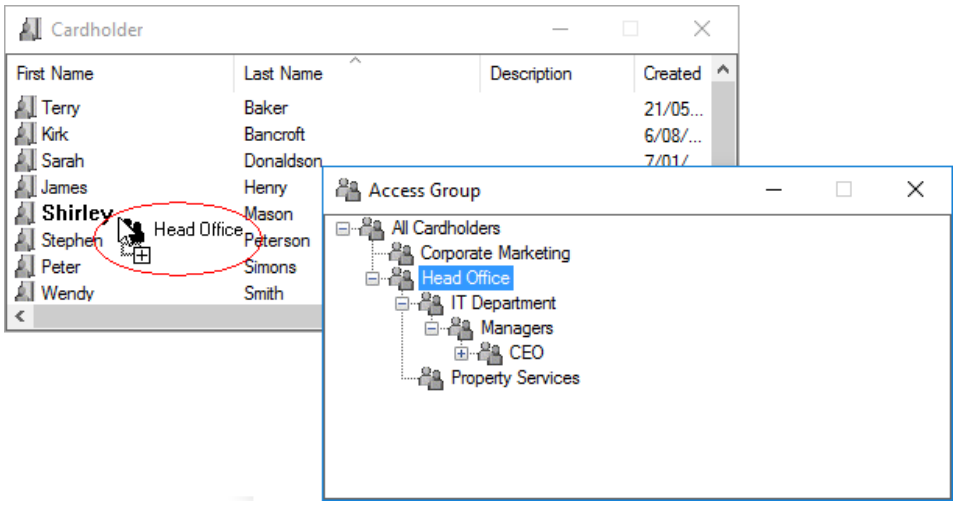
Procedure

While this procedure describes how to drag and drop an Access Group onto a Cardholder, the concept is the same for dragging and dropping a Cardholder onto an Operator Group.

1. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).

2. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
3. Select the Access Group that you want a cardholder to belong to.
4. Click and hold down the mouse button, and drag it onto the Cardholder List Window until the 'First Name' of the required Cardholder changes into a **bold** and larger font than the other names.

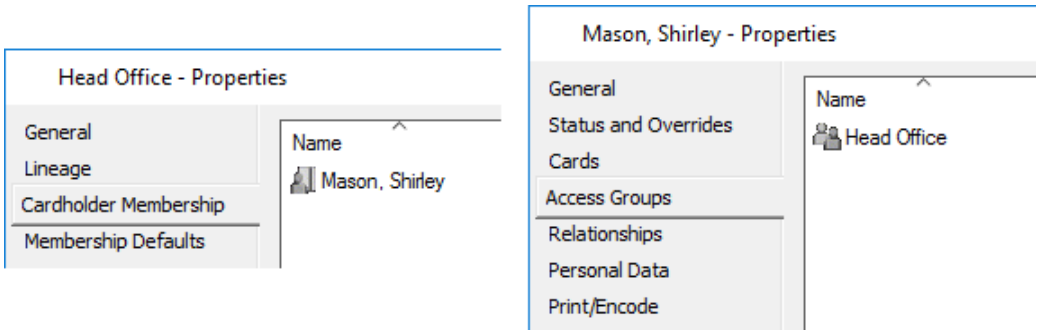
   For example:
   In the following example, the 'Head Office' Access Group is dragged across to the cardholder 'Shirley Mason'.



5. Release the mouse button.

Result

The Cardholder is now a member of the Access Group, and appears on the **Cardholder Membership** tab of the Access Group. Likewise, on the **Access Groups** tab of the Cardholder, the Access Group appears.



Note: When this procedure is used to make a Cardholder a member of an Operator Group, the results are:

- the Operator Group appears on the **Operator Configuration** tab of the Cardholder, and
- the Cardholder appears on the **Cardholders (Operators)** tab of the Operator Group.

Chapter 3: Knowing your way around

Command Centre is a comprehensive system, and this topic details a number of procedures that could make your life easier when managing and monitoring the system. If you are familiar with the Windows Operating System, you may have already encountered some of these procedures.

- ***List Windows*** (on page 3-2)
- ***Generic Properties configuration*** (on page 3-14)

List Windows

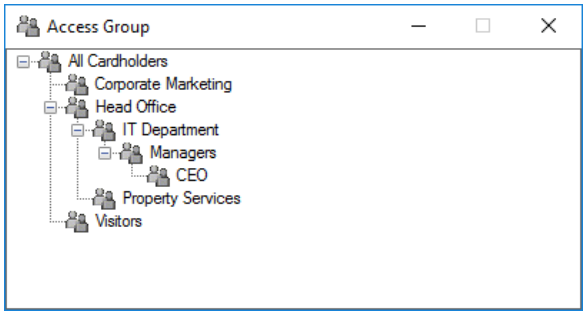
Introduction

List Windows are the starting point for managing items in your Command Centre system. From a List Window you can:

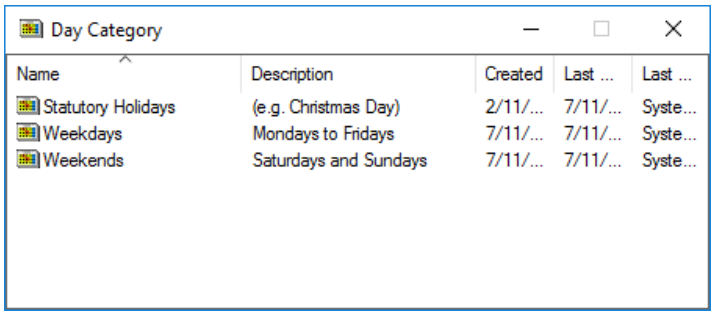
- view existing items,
- edit existing items,
- create new items, and
- delete old items

Each item within a List Window has its own Properties window, making it easier to manage the site items.

Information in List Windows displays as either a tree view or a grid view.
A tree view example is the **Access Group** List Window, as shown below. From this you can see the parent item(s) and/or any child(ren) item(s) they have.



A grid view example is the **Day Category** List Window, as shown:



Select the item below that you require further detail on:

- ***Tree view*** (on page 3-3)
- ***Grid view*** (on page 3-4), and what you can change within grid view windows
- ***Sizing windows*** (on page 3-9)
- ***Switching between windows*** (on page 3-10)
- ***Pop-up menus*** (on page 3-11)

Tree view

Information within the following Command Centre system windows displays as a tree view:
- Hardware
- Divisions
- Site Plans
- Access Groups
- Access Zones
- External Systems (licensable feature)

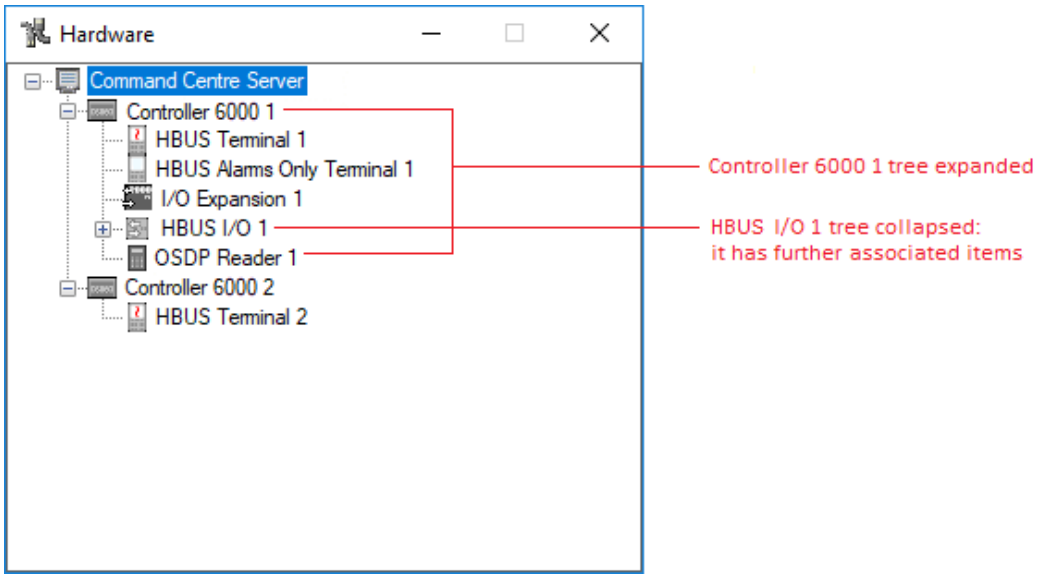
A tree view displays the information with branches representing the different levels in the hierarchy.

For example: Which devices connect to which Controllers.

The tree can be expanded - so you can see all items related or it can be collapsed - so you can only view the "top level" item. This makes it easy to see which items are associated with each other.

⊞ = Tree is collapsed - there are items "beneath".

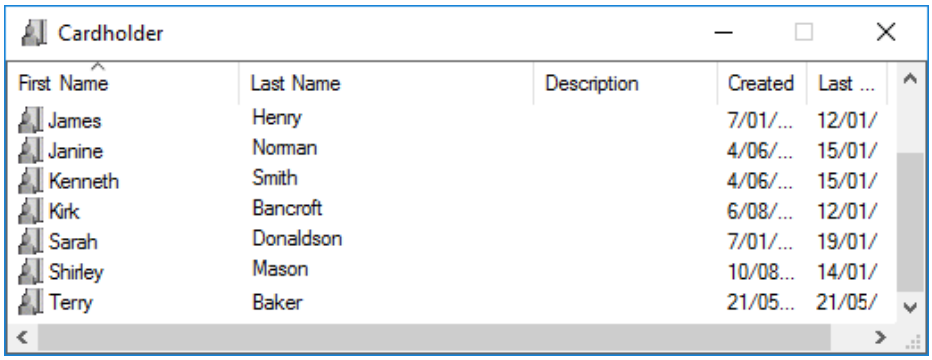
⊟ = Tree has been expanded.



Note: You cannot multi-select items in a tree view. Instead, the Find Tool can be used to search for items in a tree view as an alternative.

Grid view

Some windows display in a grid view; there is one line of information for each item in the list.



When adding or deleting items to a grid view, the window updates automatically, (i.e. items are added to the view immediately when created, and deleted items are removed immediately).

Within Grid View windows you can change various aspects of the window and you can select information from the window.

- ***Resizing the Column Headers*** (on page 3-5)
- ***Repositioning the Column Headers*** (on page 3-6)
- ***Selecting items within the displayed list*** (on page 3-7)
- ***Sorting the information*** (on page 3-8)

Resizing the Column Headers

Introduction

Within Grid view windows, you can resize the Column Headers to view more or less of the column information.

Procedure

- Manually -

1. Move the mouse pointer over the edge of the Column Header. The mouse pointer changes to a double-ended arrow ↔ indicating the directions in which you can resize the column.
2. Drag the Column Header in the required direction.

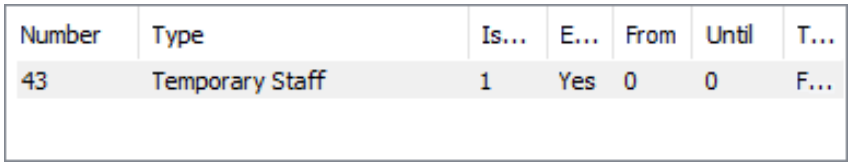
- Automatically -

1. Double click on the appropriate Column Header.
   The Command Centre system automatically resizes the column to the maximum width to suit the longest item.

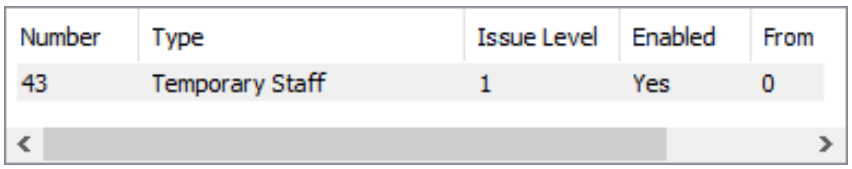
   Note: If there is no information contained with the column, the system will automatically shrink the column.

Result

Example before:



Example after:



Hint

Scroll bars automatically display when the Column Headers become too long for all information to be displayed.

Repositioning the Column Headers

Introduction

You can change (reorder) the position of the Column Headers to suit your requirements, within the Grid view windows.

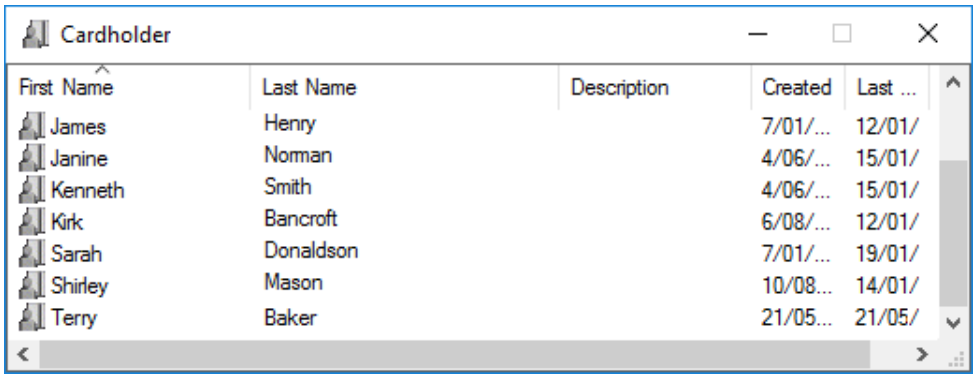
Procedure

1. Move the mouse pointer to the Column Header you want to reposition.
2. Click and hold down the mouse button.
3. Move the mouse (and hence the Column Header) to the required new position.
4. Release the mouse button.

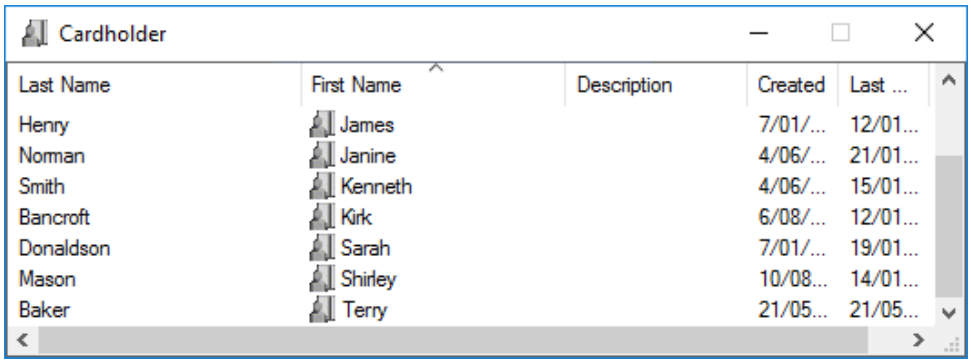
Result

The Columns are displayed in their new position.

Example before:



Example after:
The two 'Name' columns have been re-ordered.



Hint

When you close and reopen the window, the Column Header positions are remembered by the system.

Selecting items within the displayed list

Introduction

You can select individual items, or multiple items, displayed within a Grid view window.

Note: Selecting a mix of different items, (e.g. Interlock Groups have a grid that supports both doors and inputs), for adding or removing is not possible. These items would need to be selected separately.

Procedure

- Select an individual item -

1. Move the mouse pointer to the required item.
2. Click the left mouse button.

- Select a continuous range of items -

1. Click on the first item in the required range.
2. Hold down the Shift key.
3. Click on the last item in the required range.
4. Release the Shift key.

- Select several distinct items -

1. Click on the first item you require.
2. Hold down the Control key.
3. Click on each required item from the list.
4. Release the Control key.

- Locate an item -

1. To locate a particular item in a grid view, highlight an item at the top.
2. Start to type.
   The highlighted record moves to one that matches what you have typed.

Result

The items are selected. This is indicated by each selected item being "highlighted".

Hint

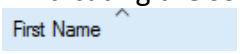
To successfully "drag" multiple selected items from one window into another window, it is important you click (and hold) on actual text of a record (not on the blank area between the text).

Sorting the information

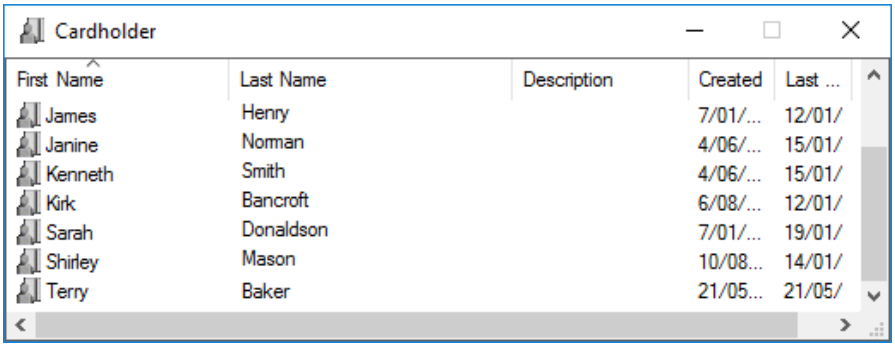
Introduction

You can sort the information displayed within Grid View windows.

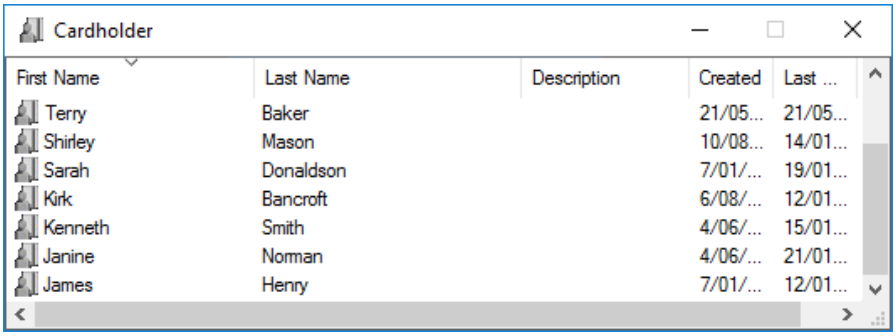
Procedure

1. Click on the Column Header corresponding to the information that you want to sort.
   The arrow indicating the sort order displays in the column header pointing upwards 

   This means that for:
   Name fields - the displayed names will be sorted alphabetically - A to Z.
   Date fields - the dates will be sorted chronologically - oldest to newest.



2. Click on the Column Header again to reverse the sorting order.
   The sort arrow now displays pointing downwards.
   This means that for:
   Name fields - the displayed names will be sorted Z to A
   Date fields - the dates will be sorted newest to oldest.



Hint

By default, only one column has a sort applied initially, (i.e. by **Name**), however Grid View windows can be sorted by up to four columns at once. Secondary, tertiary and quaternary sorting is based on the previous sort applied in each case, (e.g. the primary sort is by **Name**, which is then changed to **Description**, so **Name** becomes the secondary sort. The sort is then changed to **Type**, so **Name** becomes the tertiary sort and **Description** the secondary sort).

Sizing the windows

Introduction

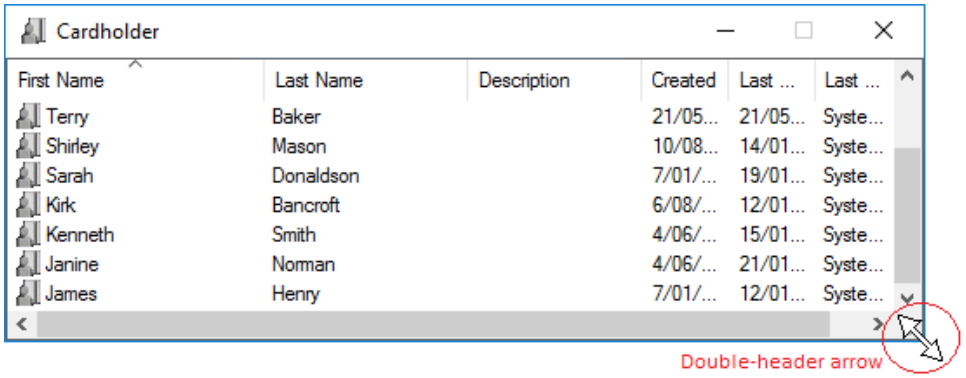
If a list window or property window is too big or too small, you can change its size.

This is particularly useful if you have more than one window open and you want to view all displayed information.

Note: Wizard windows cannot be resized.

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.

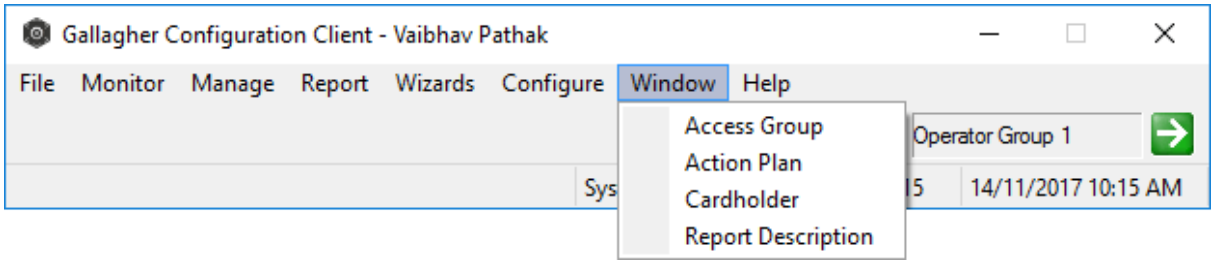
Switching between windows

Introduction

When you have multiple Command Centre windows open, it can be confusing to find the actual window you want to view. Via the Window menu, you can quickly select the window you want.

Procedure

1. Click **Window** from the menu bar.
2. From the displayed drop-down menu, select the title of the window that you want to be active.



Result

The selected window is moved to the foreground. It is now the active window.

Hints

Titles displayed
The drop-down menu list only contains those window titles that are currently open and are sorted alphabetically. For example, if you have four windows open, those four window titles will be displayed in the list.

There is a maximum of 30 windows that will display in the window drop-down menu list at once. The oldest opened window is the one that is dropped off the bottom of the list.

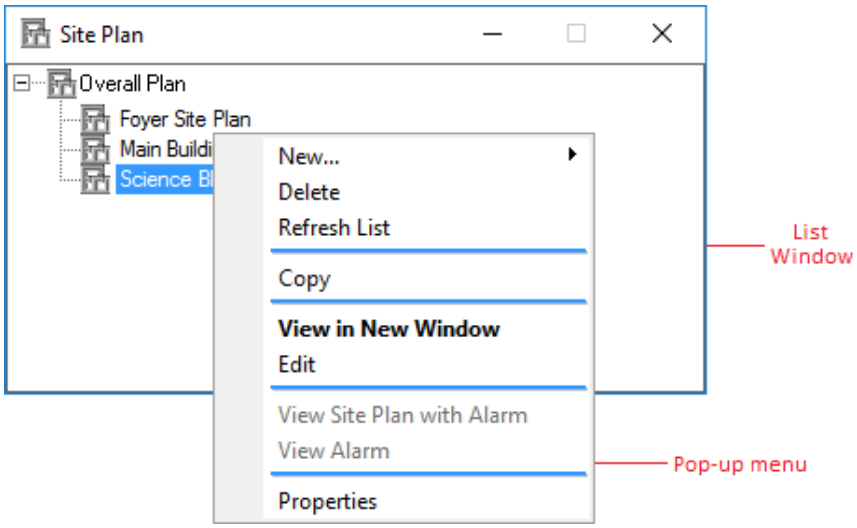
Organising your screen

- Close, (by clicking the  button in the top right corner), or minimise those windows you are not using.
- Resize the windows to suit.

Pop-up menus

Introduction

List Windows are the starting point for managing items in your Command Centre system, (i.e. creating new items, viewing existing items, editing existing items and deleting old items). A number of common menu options (via a pop-up menu) are available for items within List Windows, (e.g. the option **New** is available for all items).



Depending on the type of selected item, additional specific options display, (e.g. with a site plan selected the options **View in New Window** and **Edit** are also available).

Procedure

There are two methods of opening pop-up menu options from a List Window.

Either:

1. **Double click** on an item.
   The window that displays will depend on the item type and state. (Note: It will however be the option from the pop-up menu that is in **bold** print. In the above screen example the Site Plan would display.)
   For example:
   - A Sequence Viewer window would display for a camera if the **View** option was in bold.

Or:

1. Click on the item.
2. **Right click** the mouse button.

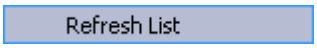
3. From the displayed pop-up menu, select the option you require:



For creating a new item.



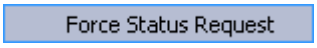
Deletes an item from the system. If the item is physically linked to another item however, you are prompted for confirmation and cannot delete it even when **Yes** is clicked. A message explaining why you cannot delete the item displays.



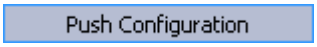
Enables an operator to update (refresh) a window to reflect any changes that may have been made.
An alternative method of refreshing is to press **F5** on your keyboard.



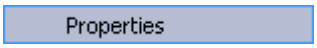
For copying and pasting. An alternative to the drag and drop method, or using shortcut keys, (i.e. <**Ctrl**+**C**> for copying, <**Ctrl**+**X**> for cutting, and <**Ctrl**+**V**> for pasting).



For double checking the status of an item if it looks incorrect, (e.g. a guard can see that a door is open but the item does not show this). The status of an item will be up-to-date after selecting this option.



This forces an update of the configuration of the site item to the Controller. This is most likely to be used for installers after an upgrade of Command Centre.



Displays the properties window for existing items.

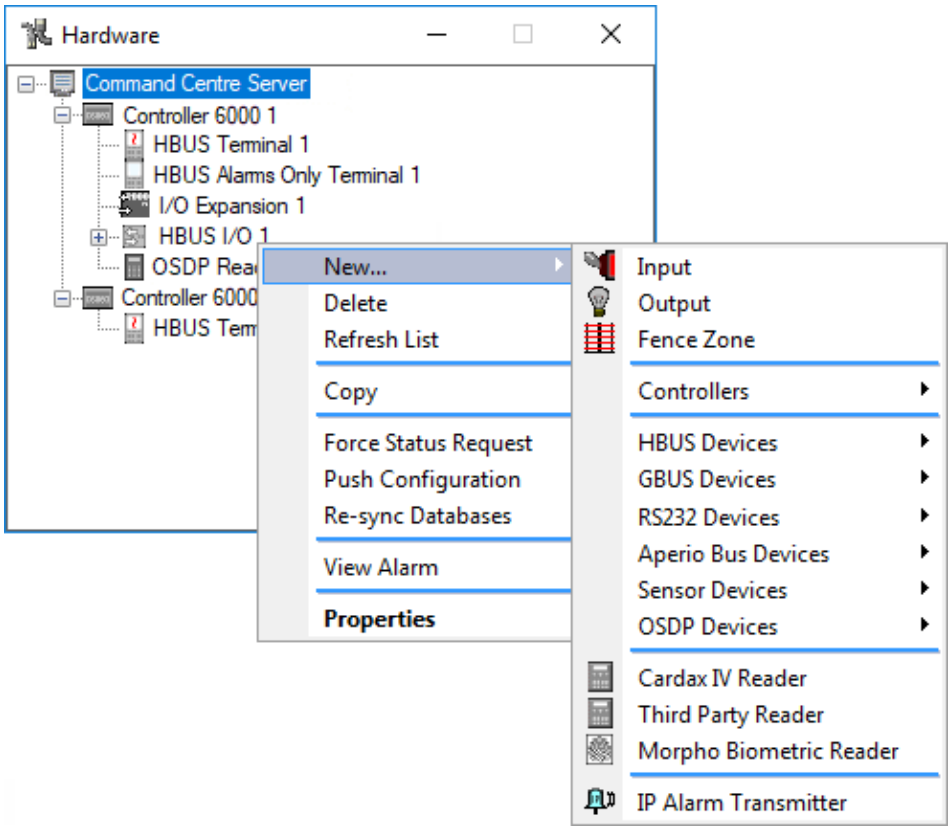
Sub-menu
When an "arrowhead" displays to the right of a displayed menu option, this indicates an associated sub-menu.



To display the sub-menu, move the mouse cursor onto the option with the arrowhead displayed.

Result

The pop-up menu applicable to the item you selected displays.
For example:



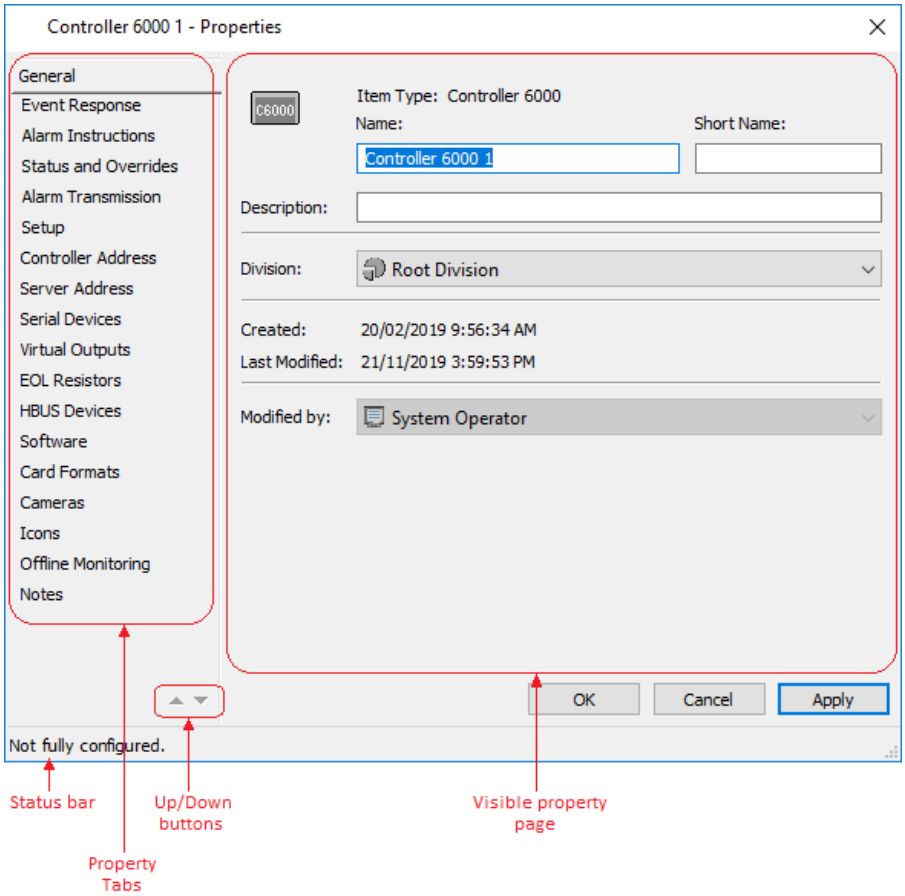
Hint

To remove the pop-up menu, simply click outside the displayed pop-up menu.

Generic Properties configuration

Most Command Centre items are maintained via a **Property window**. Property windows display a set of property tabs down the left-hand side (as shown in the sample screen shot below) for the item's supported property pages. Each property page displays some properties of the item and allows the operator to maintain these properties.

The Status bar at the bottom of a property window shows the current status of that item.



Some property pages are common to a number of Command Centre items, (e.g. all items that utilise a Property window have a **General** tab). Likewise, some of the procedures for maintaining items in Command Centre are very similar, (e.g. deleting items).

Select the item below that you require further detail on:

- ***Item icons*** (on page 3-15)
- ***Viewing item properties*** (on page 3-17)
- ***General tab*** (on page 3-18)
- ***Event Response tab*** (on page 3-20)
- ***Alarm Instructions tab*** (on page 3-22)
- ***Cameras tab*** (on page 3-24)
- ***Editing items*** (on page 3-26)
- ***Deleting items*** (on page 3-27)

Item icons

Introduction

For quick, visual identification, a small picture (icon) is associated with each item.
For example:

 = Command Centre Server icon

 = Controller icon

 = Door Closed icon

 = HBUS Terminal icon

 = Input ON icon

 = Output OFF icon

The icon changes to reflect the status of the item it is representing, by way of an overlay that is placed on top of the icon, (e.g. if a Controller goes offline, its icon will indicate this with an overlay on top of it ) . Those Gallagher devices that are linked to the offline Controller will also indicate the offline status. This is true also for the tampered state.

The overlays and their states are shown in the following table. They are ordered by importance, with the most important at the top. When two of these conditions occur, the most important one is shown.

State	Icon	Description
Offline		The device is offline. It cannot be communicated with.
Unknown		The device has not responded with it's state since the system came online.
Tampered		A device has been tampered. If the device is a *parent* device, then all it's children will also show this overlay.
Power Failure		A power condition is abnormal, possibly Battery Low, Mains Failure.
Not Configured		The item is not configured for proper operation.

State	Icon	Description
Deleted		A Rubbish Bin indicates that the item has been deleted.
Door locked		Shows that the door is closed and locked.
Door unlocked		Shows that the door is closed and unlocked.

Viewing item properties

Introduction

The procedure for viewing the properties for existing items in Command Centre is very similar for most items, as demonstrated below.

Procedure

1. Open the list window for the item you want to view.
2. Highlight the item you want to view.
3. **Right click** and select **Properties**.
   The information available about the item is grouped under each tab down the left side of the property window.
4. Click the tab(s) for information you want to view.
   Note: Some of the tabs that are common to many items in Command Centre are listed below:

   General

   Shows general details about the item, (i.e. the name, description, creation date and time, and who last modified the item's properties and when).

   Event Response

   Shows the site item events that are individually linked to Action Plans for this item.

   Alarm Instructions

   Shows the Alarm Instructions assigned to the Event Groups and Types for this item.

   Status and Overrides

   Shows the status of the item and any overrides that have been applied to it. This tab also provides operators the opportunity to override the item if they have the correct privilege. See Performing Overrides for procedure.

   Icons

   Shows what Icon Set has been assigned to this item.

   Notes

   Shows any notes that have been recorded about the item.
5. Click **Cancel**.

Result

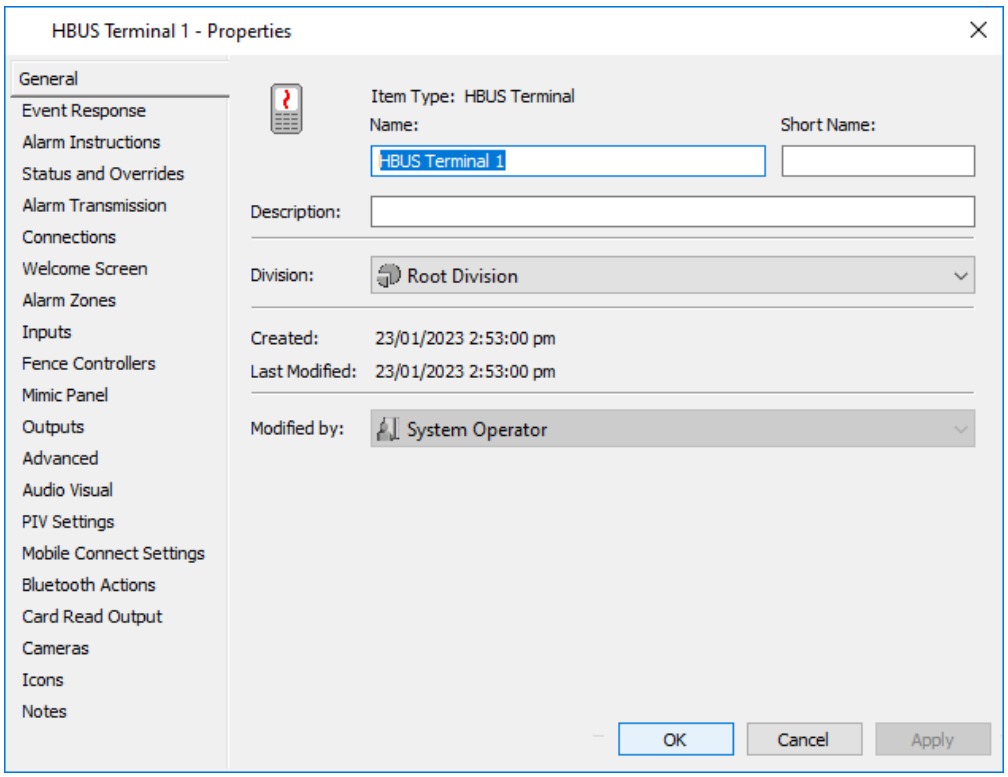
The Properties window for the item closes.
You have viewed details about the item but taken no action.

Hint

Resizing Property windows
Property windows can be resized. See ***Sizing the windows*** (on page 3-9) for further detail.

General tab

All items that utilise the Properties window to display/configure their attributes include a **General** tab, which is always the first tab in the name tabs area in the Properties window. The **General** tab displays by default when any Command Centre item is opened via the Properties option.
Note: The example screen shot below is for a HBUS Terminal, and while it will differ slightly for other items, the procedure is still the same.



1. Type in a **Name** (limited to 60 characters) for the Command Centre item and a logical **Description** (limited to 200 characters).
   Note: When an item is first created, the **Name** defaults to the item type name, plus a number on the end to ensure that there are no duplicate names, (e.g. HBUS Terminal 1). The number increments by one if an item of that type already exists with that number on the end.
2. Is there a **Short Name** field?

If...	then...
no	go to Step 3.
yes	the **Short Name** is used by the Gallagher Mobile Connect App instead of the **Name**. **Notes:** • This field is limited to 16 characters. If you do not enter a short name, the system will automatically use the first 16 characters from the **Name** field when displayed on a mobile device.

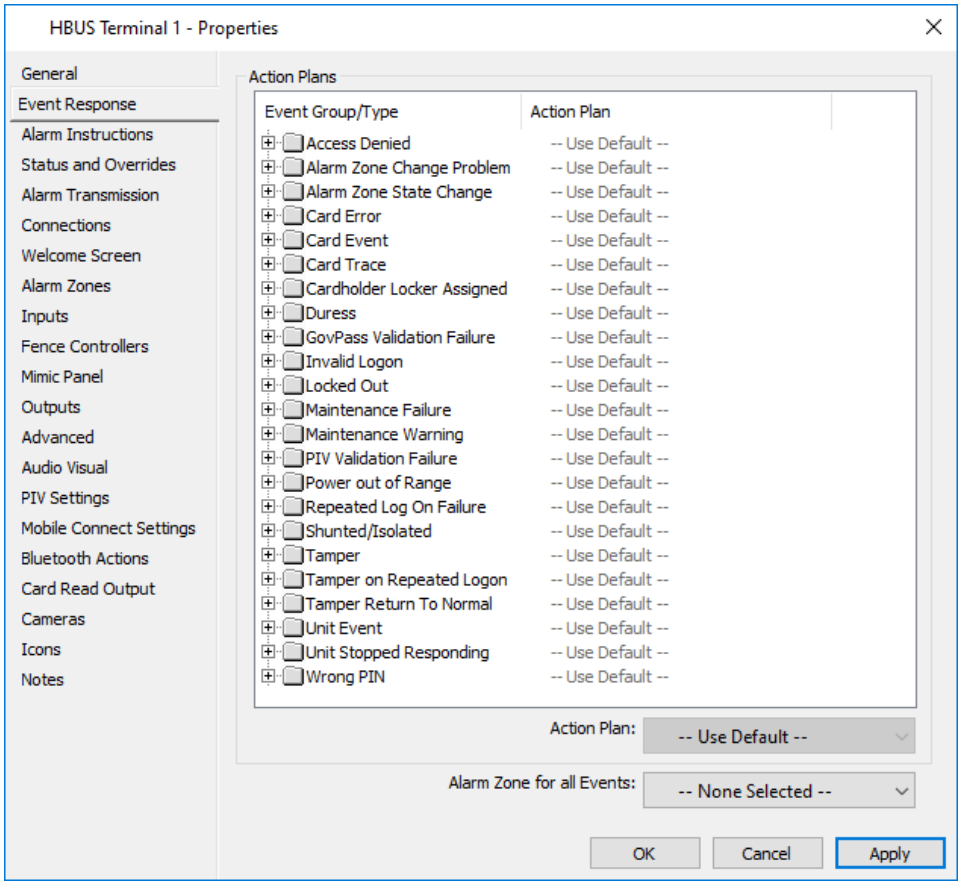
If...	then...
	In the case of Cardholder names displayed on a mobile device, the mobile device will use the first 16 characters from the **Last Name** field and then the **First Name** field, (e.g. If Cardholder Lillian Phillipson logs into the Gallagher Mobile Connect App her name will display as **Phillipson, Lill**). • The following characters should not be used in the Name or Short Name as they do not display correctly: **\ ' | ~**

3. Select the appropriate **Division** from the drop-down list.
   Notes:
   - When creating new items, the last division an operator used for creating or saving an item would normally populate the **Division** field. However, if the operator's last used division is not available, then by default the system will select the highest division that the operator has access to. If there is more than one division at the same level, then the system will select the division which was created first.
   - If you have not set up Divisions yet, you can add these to your item at a later stage.

Event Response tab

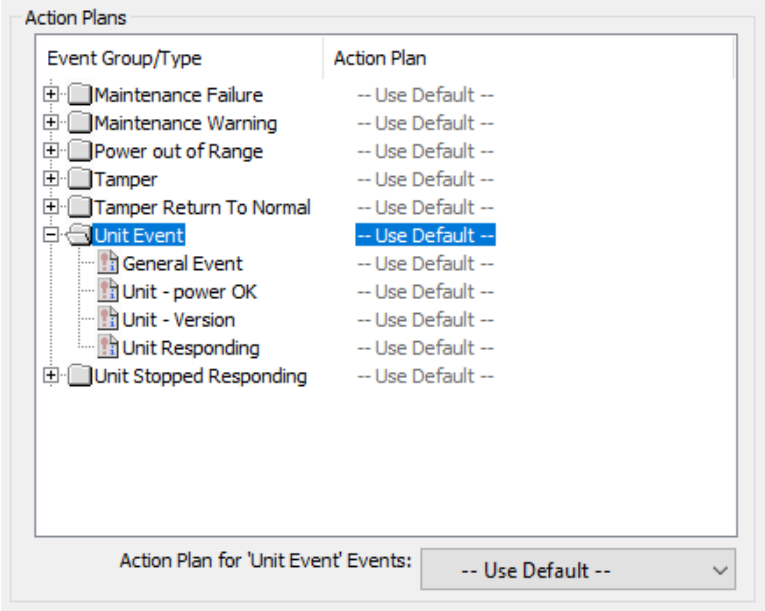
Items that support event reporting include an **Event Response** tab in their Properties window as the second tab in the name tabs area. This tab allows you to individually link site item events to Action Plans. All the Event Groups and Types available for that particular item are listed as a tree so that each individual Event Type can have a different Action Plan assigned to it. If an Action Plan is not assigned at Event Type level, the Event Group Action Plan is used.

Note: The example screen shot below is for an HBUS Terminal, and while it will differ slightly for other items, the procedure is still the same. The 'Alarm Zone for all Events' field only appears for Controller items.

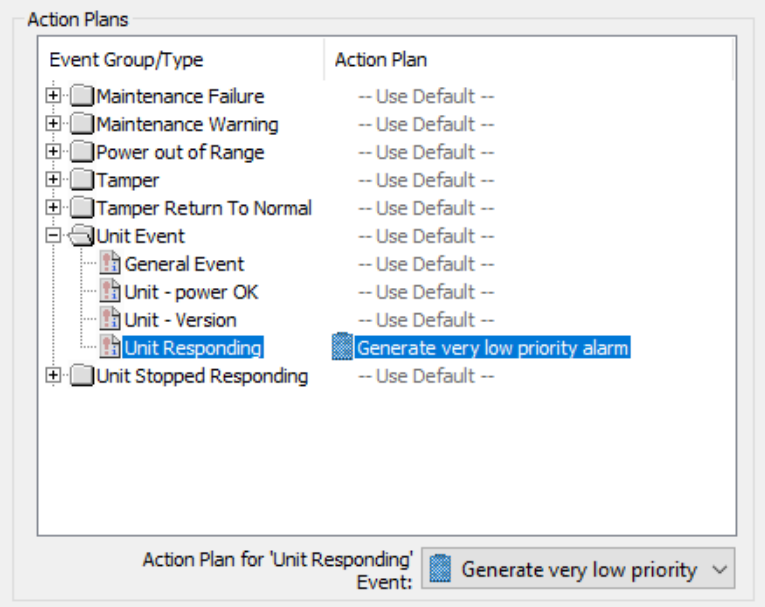


1. Highlight the Event Group/Type you want to assign an Action Plan to. The edit box is then enabled.
   - You can assign an Action Plan at an Event Group level, or at an individual Event Type. If an Action Plan is assigned to an Event Group, all Event Types in that group will default to the groups Action Plan. However, Action Plans assigned to individual Event Types override the group event.
   - It is possible to assign Action Plans to Event Types and/or Event Groups as site wide default settings. See ***Event Defaults*** (on page 6-12) for further details.

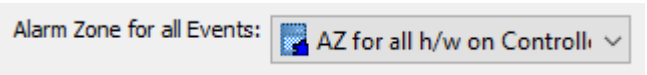
To see all the Event Types in a Group, expand the tree by clicking on the ⊞ icon.



2. Click the drop-down menu list to display the available Action Plans, and select the required plan.



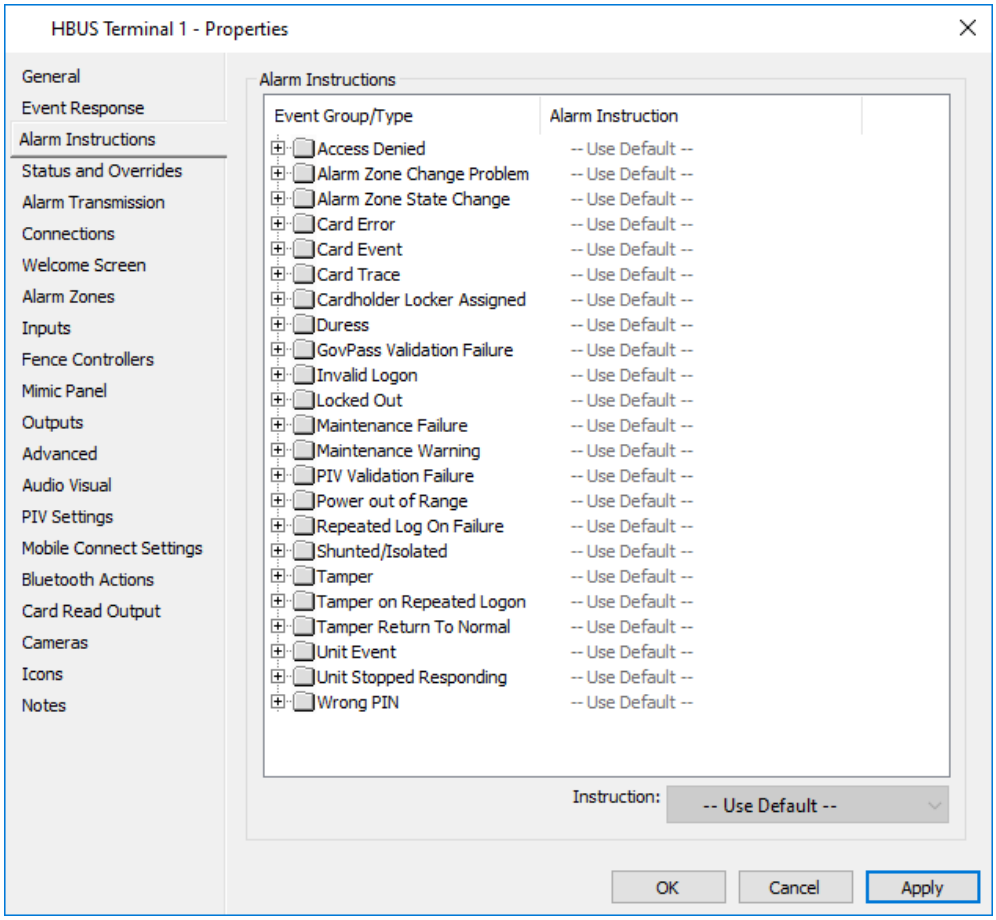
3. Repeat Steps 1 - 2 as necessary.
4. If there is an 'Alarm Zone for all Events' field, assign a primary Alarm Zone for all events from the drop-down list.



Alarm Instructions tab

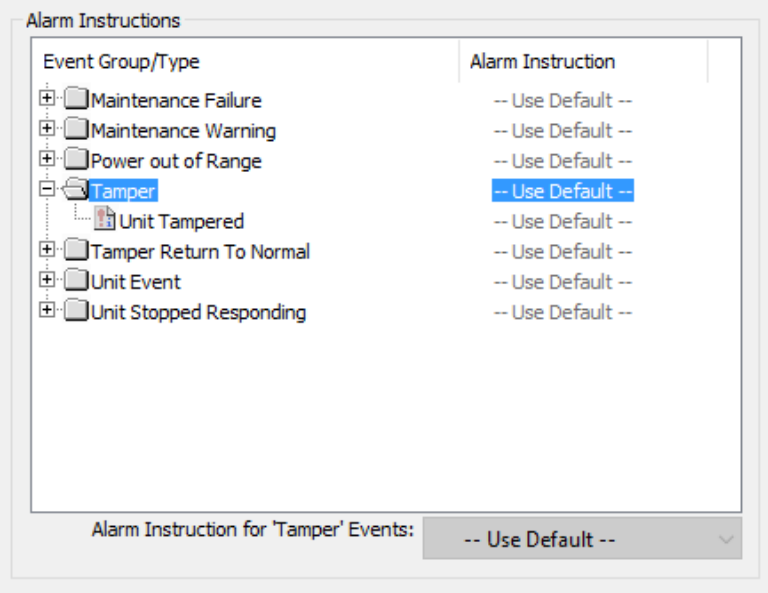
Site items that can generate alarms include an **Alarm Instructions** tab in their Properties window as the third tab in the name tabs area. This tab allows you to assign Alarm Instructions to each of the Event Types and/or their Event Group. As with the **Event Response** tab, all the Event Groups available for that particular item are listed.

Note: The example screen shot below is for an HBUS Terminal, and while it will differ slightly for other items, the procedure is still the same.

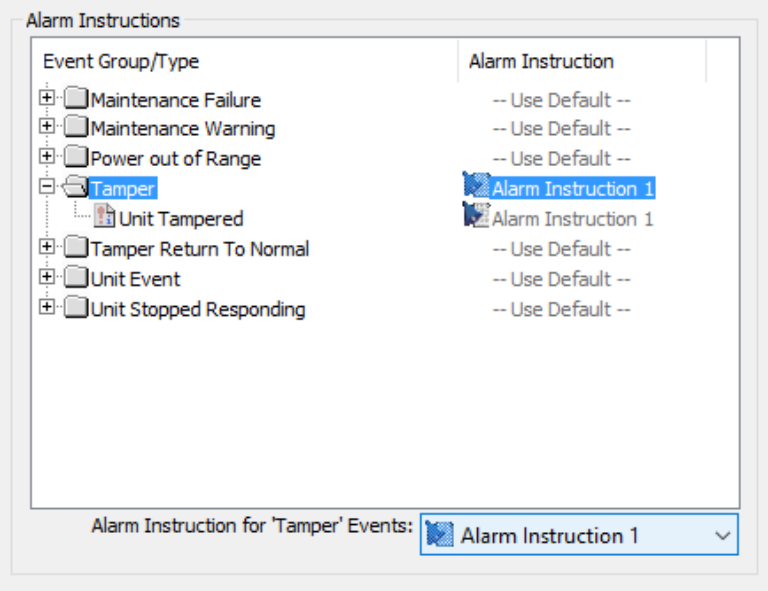


1. Highlight the Event Group/Type you want to assign an Alarm Instruction to. The edit box is then enabled.
   Notes:
   - You can assign an Alarm Instruction at an Event Group level, or at an individual Event Type. If an Alarm Instruction is assigned to an Event Group, all Event Types in that group will default to the groups Alarm Instruction. However, Alarm Instructions assigned to individual Event Types override the group event.
   - It is possible to assign Alarm Instructions to Event Types and/or Event Groups as site wide default settings. See ***Alarm Instructions Defaults*** (on page 6-13) for further details.

To see all the Event Types in a Group, expand the tree by clicking on the ⊞ icon.



2. Click the drop-down list to display the available Alarm Instructions, and select the required instruction.

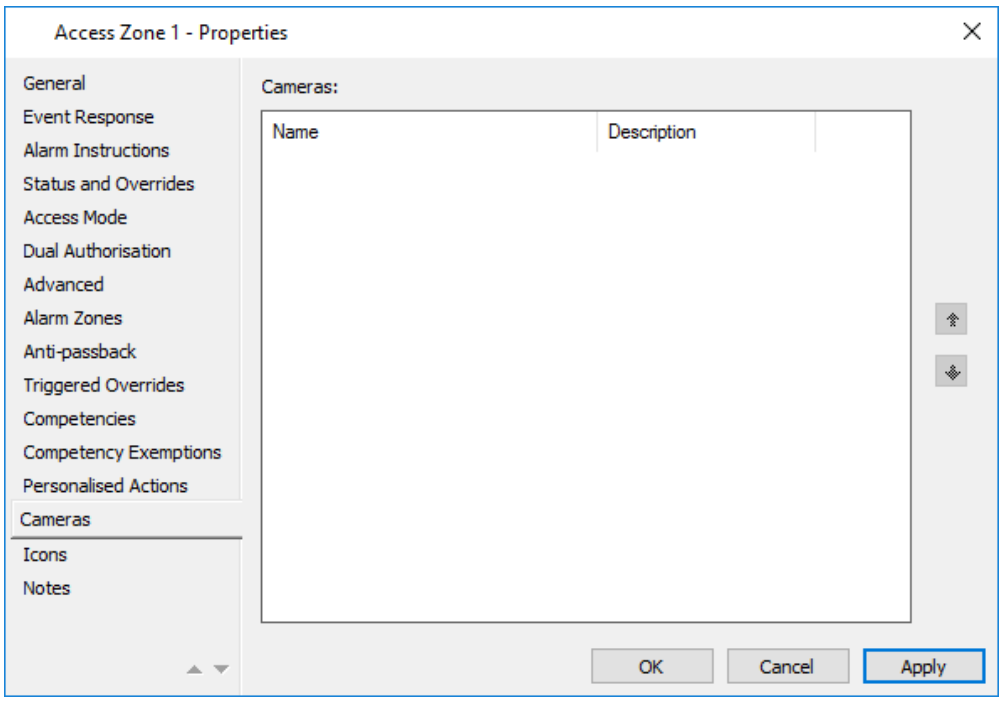


3. Repeat Steps 1 - 2 as necessary.

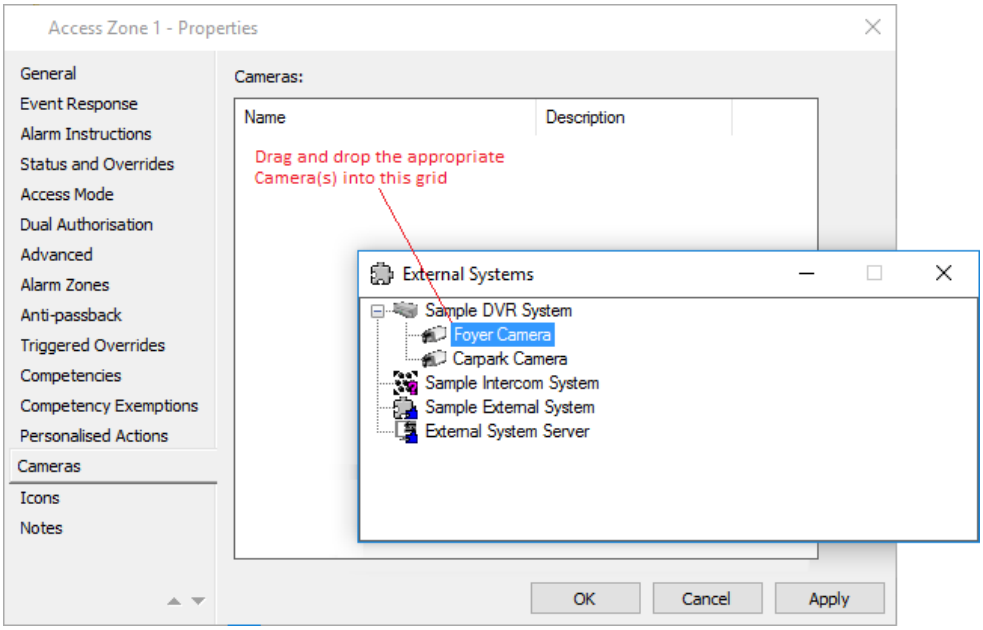
Note: If you change the assignment of alarm instructions for items already in alarm, they will not show the change of alarm instruction until the workstation is logged off and on again. Any new alarms that come in will however adopt the changes straight away.

Cameras tab

All site items include a **Cameras** tab in their Properties window. This tab allows you to assign DVR Cameras to a site item, so that when an event occurs at the item, the **Camera** tile in Command Centre Client will display footage for the camera associated with it.
Note: The procedure and example screen shot below is for an Access Zone, however the procedure is still the same for all site items.



1. Click **Configure** from the menu bar, then **External Systems**.
   The **External Systems** List Window opens.
2. Select those DVR Camera(s) appropriate for this Access Zone.
   Drag and drop them into the grid on the **Cameras** tab.
   The **Camera** tile in Command Centre Client can be configured to display live feed from one of the cameras listed in this grid.



Note: The **up** and **down** arrows to the side can be used to change the order of the DVR Cameras if required.

The order you sort the cameras here will be their “position in list” when you choose to Live feed from Event Source Camera and specify the number of the camera that the feed will be taken from in Command Centre Client.

Editing items

Introduction

The procedure for editing information about existing items in Command Centre is very similar for most items, as demonstrated by the following procedure.

Procedure

1. Open the list window for the item you want to edit.
2. Highlight the item you want to edit.
3. **Right click** the mouse button.
4. Click **Properties** and then the appropriate tab(s).
5. Edit the relevant information as required.
6. Click **OK** to exit and save your changes.
   Click **Cancel** to exit without saving your changes.
   Click **Apply** to save your changes and stay in this window.

Result

The item details are changed accordingly.

Deleting items

Introduction

The procedure for deleting items in Command Centre is very similar for most items, as demonstrated by the following procedure.

Note: The system will only allow the deletion if the item is not used. If any site item is linked to the item you want to delete, (and hence is valid in the security operation of the site), you cannot delete it, (e.g. an Insertion Tag associated with an Alarm Instruction, Site Plans linked to other Site Plans, etc.).

Procedure

1. Open the list window for the item you want to delete.
2. Highlight the item you want to delete.
3. **Right click** and select **Delete**.
   A confirmation window displays.
4. Click **Yes** to delete the item.

Result

The item disappears from the list window.

Hint

Locating linked items
If you attempt to delete an item that is linked to another item a message will display, for example:
"This item cannot be deleted, as it currently appears on a site plan."

Such messages however do not indicate which particular item it is linked to, of which there could be hundreds. Therefore a quick method of locating the item is to use the Find Tool.
See ***Example 2: Searching using Related To details*** (on page 41-8) for the procedure.

Note: "Related To" items for an Interlock Group are doors, Controller, Inputs, Outputs, Division, Icon Set, Action Plan, Alarm Zone, Alarm Instruction, Logic Block and Site Plan. A "Related To" search for an interlock item appearing in an exception pair on an Interlock Group will not return the other interlock item of the pair used in that Interlock Group. However, the search will return the Interlock Group containing the door or Input. A "Related To" search on an Output will show the item it is attached to, (e.g. door), or if it is a warning output in a group it will show the Interlock Group.

Chapter 4: Utilities

The following additional utilities are available with the Command Centre system.

DCOM Setup Utility

This utility is used to change or repair DCOM (Distributed Component Object Model) settings for Command Centre. Refer to the *DCOM Setup Utility Release Note* in the **'Utilities\DCOMSetupUtility'** directory of the Command Centre installation files for further detail.

Import/Export Utility

This provides the functionality for the import and export of Cardholder details, and the import of schedules. It allows sites to link the Command Centre system to external systems, (e.g. Human Resources databases or Student Enrolment systems), without the need to re-key Cardholder information.

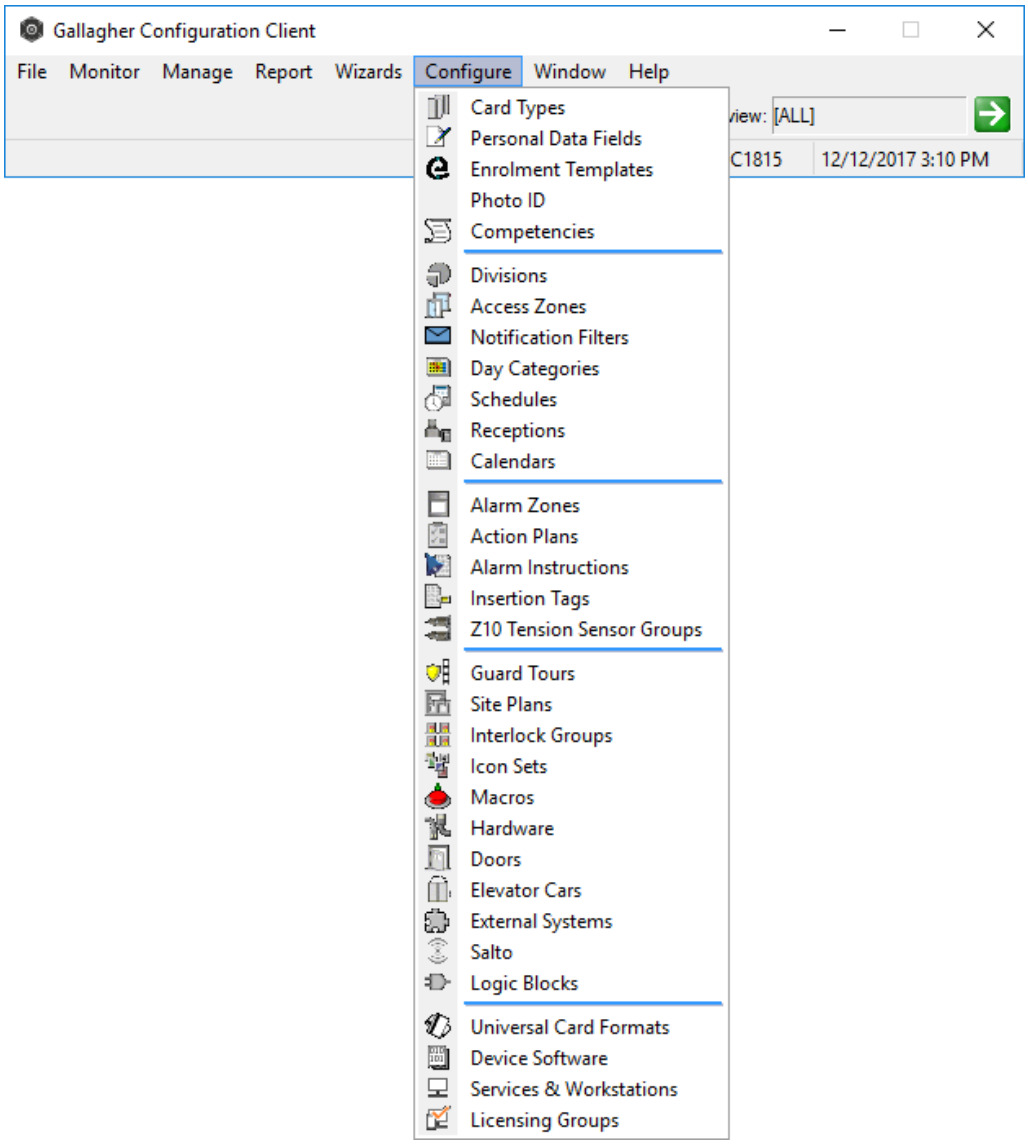
An *Import/Export Utility User Guide* (**Import_User Guide.chm**) is provided in the **'Utilities\Import Export'** directory of the Command Centre installation files, which provides instructions on how to perform Cardholder and Schedule imports.

Part 2: Site Installation

It is the role of the Installer to install and configure Command Centre software and hardware.

This part of the User Guide provides details on how to perform the functions required for installing and configuring a site.

As you will see from the screen shot below, most of the chapters included in this part reflect menu items accessible via the **Configure** option on the Configuration Client main menu bar.



The remainder of the chapters are not menu items, with the exception of Chapter 6 - Server Properties, which is accessible via the **File** option on the menu bar.

Notes:

- Depending on your operator privileges or your current system view, some menu items referred to may not be visible to you.
- Licensable features may also be included in the list of options available under **Configure**, (e.g. Card Encoding). These items will only be available if your site has them included in their license file. If you require further detail on any of these features, refer to *Part 5: Licensable Features* or *Part 6: Integrated Systems* as appropriate.

Chapter 5: Setting up your Site

This chapter details a number of procedures to set up and configure your system.

This chapter contains the following information:

- ***Recommended Site Configuration Process*** (on page 5-2)
- ***Wizards*** (on page 5-5)
  (interface to assist with configuring a system)

Recommended Site Configuration Process

Introduction

The following process should be followed to ensure that each activity is performed in the correct order when setting up your site, and therefore the relationships between the various entities in Command Centre are maintained.

This process refers to separate step-by-step procedures which are either detailed in this section, or other sections as indicated.

Before you begin

Before you get to the Command Centre installation process, it is advised that formal design work for the site has been completed, and is available to use as a configuration guide.

Process

1. Although not necessary, it is advisable to ensure that all the equipment has been physically installed on site, according to the design specification for the site, and as instructed in the "Gallagher Installation Manual" (Part No. C209100).
2. Install Command Centre.
   (See the Command Centre Release Note for a description of the options and the installation procedure.)
3. Log on to Command Centre, and set up your system password.
   (See ***Getting Started*** on page 2-1 for procedure.)
4. Set up System Divisions.
   (See ***Setting up System Divisions*** on page 9-3 for procedure.)
   Note: As an alternative to following the rest of this procedure, there are configuration wizards available. These wizards help simplify the process for configuring some basic Command Centre settings, hardware devices, doors, cards and cardholders. See ***Wizards*** (on page 5-5) for further details.
5. Rename the "Default Day Category", (e.g. Weekdays), and create one additional Day Category, (e.g. Weekends).
   (See ***Day Categories*** on page 11-1 for procedure.)
6. Create Calendar Days (See ***Calendars*** on page 13-1 for procedure).
7. Create Card Types and Facility Codes (see ***Setting up Card Types*** on page 7-2 for procedure), and create a Crypt Seed (see ***Server Properties*** on page 6-1 for procedure).
   Note: Depending on the license file the Crypt Seed may be present already.

8. Create a Cardholder, and make it part of the System Division you created in Step 4.
   (See ***Adding a new Cardholder*** on page 32-2 for procedure.)
9. Create an Operator Group with the advanced privilege and put your new Cardholder into this group.
   (See ***Operator Groups*** on page 36-1 for procedure.)
10. Log off the system and log on the new user.
    This will make all items that are created in the new division, which saves time and prevents mistakes with the operator forgetting to change the division.
11. Configure the hardware.
12. Create ***Schedules*** (see ***Schedules*** on page 12-1 for procedure).
13. Create an Alarm Zone for all the devices. Give the Alarm Zone a meaningful name like "AZ for all h/w on Controller#1".
    (See ***Alarm Zones*** on page 14-1 for procedure.)
14. Get the Controller online, i.e. ensure the Controller has an IP address (2 flashes on Red LED), and put this IP address in the **Advanced** tab of the Controller Properties screen. (See ***Creating Controllers*** on page 21-2.)
15. Once the Controller is in the 1Hz flash mode, assign the Alarm Zone you created for the Controller and hardware in Step 13, in the **Event Response** tab of the Controller Properties screen.
16. Link the devices to the Controller.
    (See ***Linking devices to Controllers*** on page 21-48 for procedure.)
    As each device is assigned to the Controller, assign it the Alarm Zone created in Step 13.
    Continue this step until all the hardware is linked.
    Note: For each new Controller created, create a new Alarm Zone specific to that Controller.
17. Create Doors (see ***Creating Doors*** on page 22-2 for procedure) ensuring they are in the same Alarm Zone as the Controller Hardware.
18. Create Inputs and Outputs (see ***Creating Inputs and Outputs*** on page 21-50 for procedure).
19. Link the Inputs and Outputs to devices (see ***Linking Inputs and Outputs to devices*** on page 21-56 for procedure).
20. Create any additional Schedules (see ***Schedules*** on page 12-1 for procedure).
21. Create Access Zones (see ***Access Zones*** on page 10-1 for procedure). Temporarily give the access zone a schedule set to free during install. This will help with commissioning the site.

22. Setup Cardholders (see ***Adding a new Cardholder*** on page 32-2 for procedure).
23. Setup Access Groups (see ***Access Groups*** on page 34-1 for procedure).
24. Once you have tested that everything is working, (i.e. alarms and events, schedule door control, etc.), create Site Plans (see ***Site Plans*** on page 18-1 for procedure).
25. Setup Action Plans (see ***Action Plans*** on page 15-1 for procedure).

Wizards

Introduction

The Wizards provide a user interface to assist operators in the configuration of Command Centre. The most frequent use of the wizards will be for new site configuration, but can also be used for the addition of hardware and cardholders to existing sites.

The Wizards enable you to easily configure a number of items for your site. You step through the Wizards using the **Next** button to access each wizard page, accepting default settings or customising appropriately. The **Finish** button can be clicked at any time to create the item without stepping through each page. At any stage you can backtrack via the **Back** button, or stop the configuration process by choosing the **Cancel** button (which also exits the particular wizard without offering to save changes).

It is recommended that only one operator invoke wizards at any one time to avoid inconveniences such as duplicate name clashes.

Operator Privileges

The Startup Wizard will only be enabled if you have the "Advanced User" operator privilege. Operators require the "Edit Site" operator privilege to run the wizards on the Configuration Wizard and wizard templates.

Operators require the "Edit Cardholder", "Modify Access Control" and "View Site" operator privileges (all in the correct division) to run the Cardholder Wizard and successfully add cardholders with cards.

This section covers the following topics:

- ***Startup Wizard*** (on page 5-6)
- ***Configuration Wizard*** (on page 5-9)
- ***Wizard Templates*** (on page 5-29)

Startup Wizard

Introduction

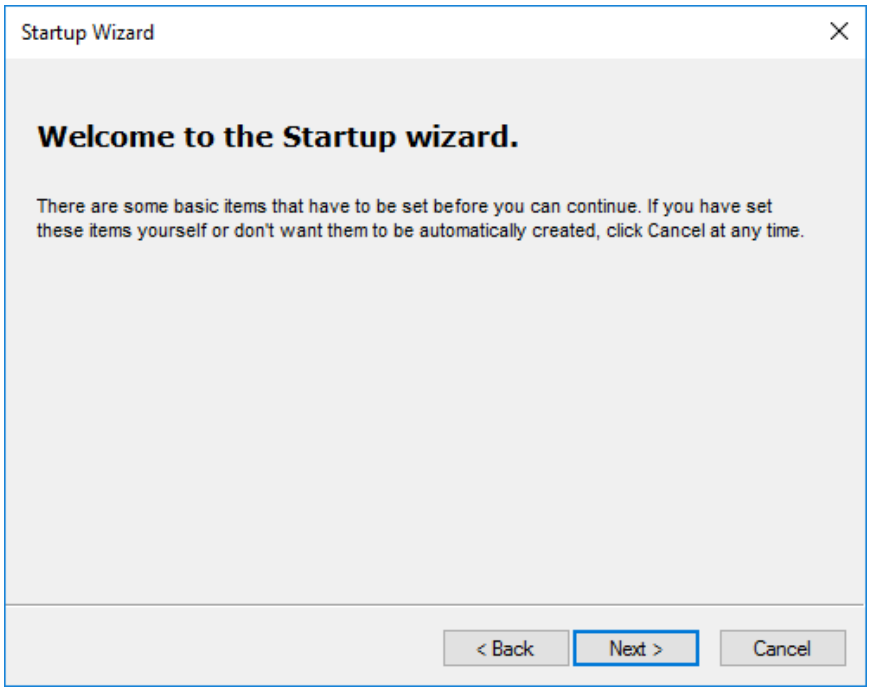
The **Startup Wizard** enables you to easily configure basic settings for your site, (i.e. create an Access Group, Alarm Zone, Day Categories, Access Zones and Card Types, and update the default Calendar and default Schedule).

This wizard is only available when the system is a new installation, on which no core setup has been done, (i.e. no default Alarm Zone, Access Group, Card Type, or Day category).

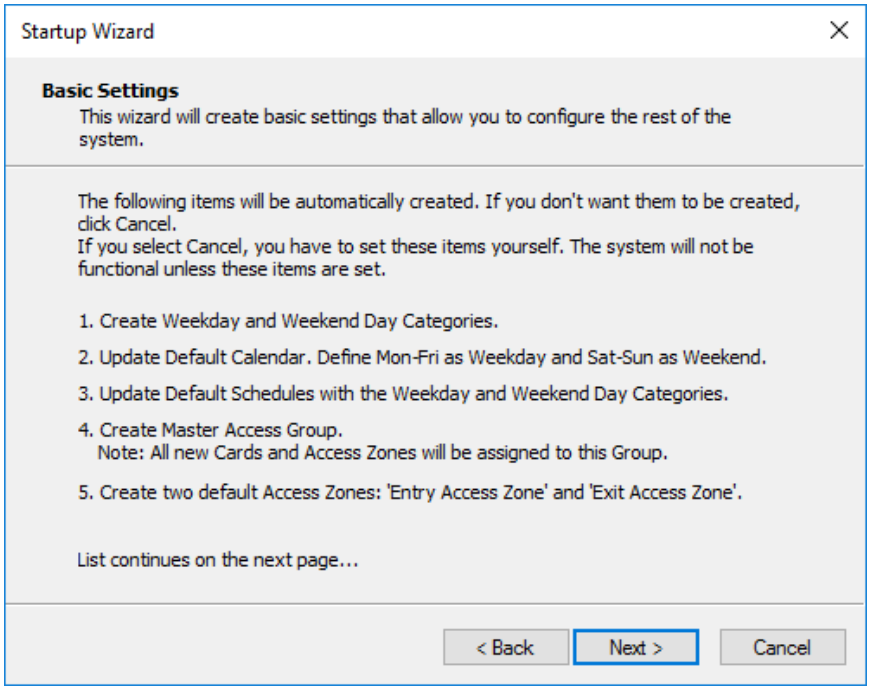
Procedure

Configuring Basic Settings

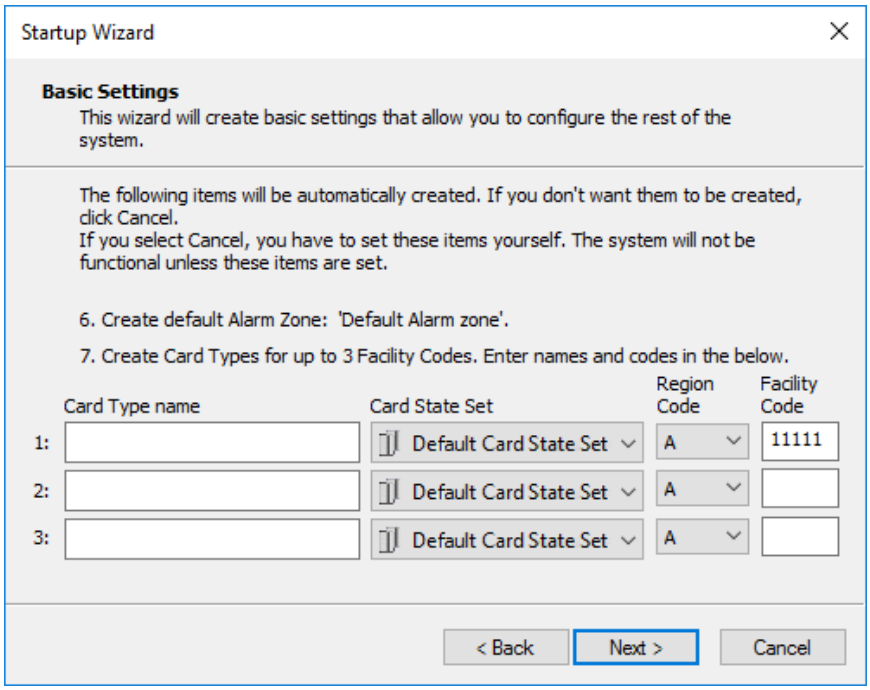
1. Click **Wizards** from the menu bar.
2. Click **Startup Wizard**.
   The Welcome screen of the Startup Wizard displays if the items required are not already present.



3. Click the **Next** button.
   A screen of basic settings that will allow you to configure the rest of the system displays.

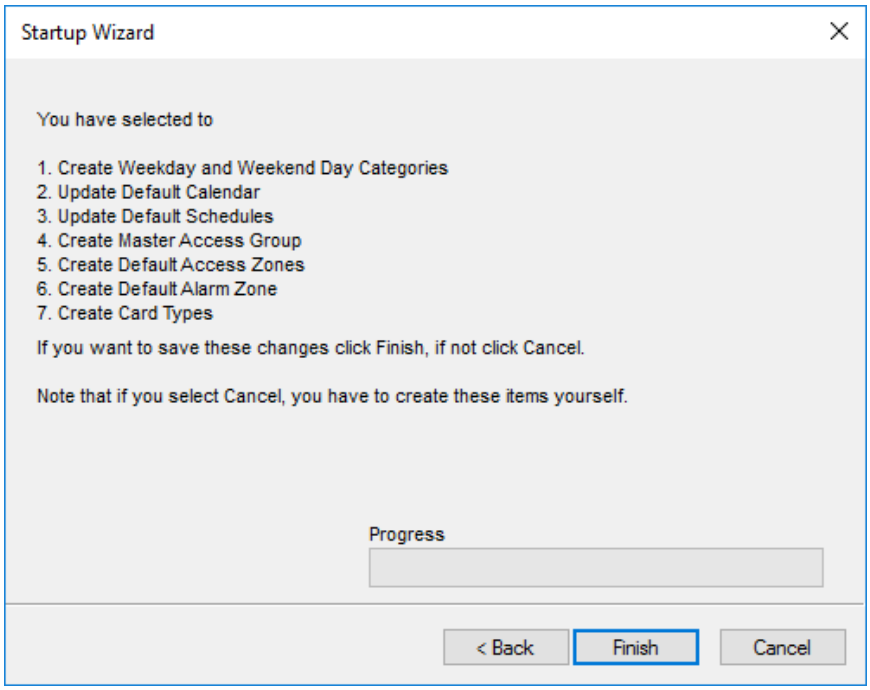


4. Click the **Next** button.
   Another screen of Basic Settings displays.



5. Create Card Types for up to three Facility Codes by naming the Card Type, selecting the Card State Set (if only one exists it will default) and allocating the Region and Facility Codes in the appropriate fields. These are provided by Gallagher.
   Note: The first Facility Code will be auto-populated if a Facility Code is defined in your license file.

6. Click the **Next** button.
   The following screen displays indicating what you have selected to create.



7. Click the **Finish** button to save your changes.
   Once the Progress bar reaches the end this indicates that the following basic settings have been configured for your system:
   - A Weekday and Weekend Day Category have been created
   - The Default Calendar has been updated
   - The Default Schedule has been updated
   - An Access Group has been created
   - A Default Access Zone has been created
   - Card Types have been created
   - A Default Alarm Zone has been created

   Note:
   These will all now appear in their relevant list windows.

Configuration Wizard

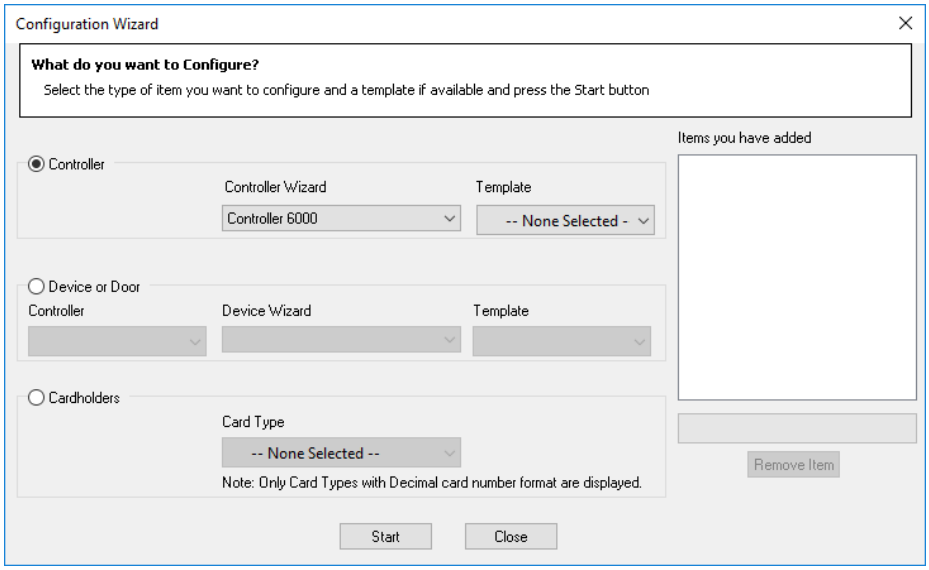
Introduction

The **Configuration Wizard** enables you to easily configure the following for your site:

- Controllers
- Doors
- Cardholders with cards

Procedure

1. Click **Wizards** from the menu bar.
2. Click **Configuration Wizard**.
   The Configuration Wizard launch page displays:



Note: In brand new systems, the fields in the **Device or Door** section of the Configuration Wizard launch page will be blank, until such time as a Controller has been created.

3. What do you want to create?

If...	then...
a Controller	a) Select the **Controller** radio button. b) Select the Controller type you require for your system from the **Controller Wizard** drop-down list. c) Optionally select an already saved **Template** from the drop-down list.
a Door	a) Select the **Device or Door** radio button. b) Select the Controller you require from the **Controller** drop-down list.

If...	then...
	The **Device Wizard** drop-down list is populated with all the door wizards that can be used with the selected Controller. c) Select the Wizard you require from the **Device Wizard** drop-down list. d) Optionally select an already saved **Template** from the drop-down list. **Notes:** • Only Controllers in divisions that you have the "Edit Site" operator privilege for, will appear in the drop-down list. • To create a Door you must select either a Controller 6000.
Cardholders	go to ***Creating Cardholders*** (on page 5-26) for the rest of this procedure.

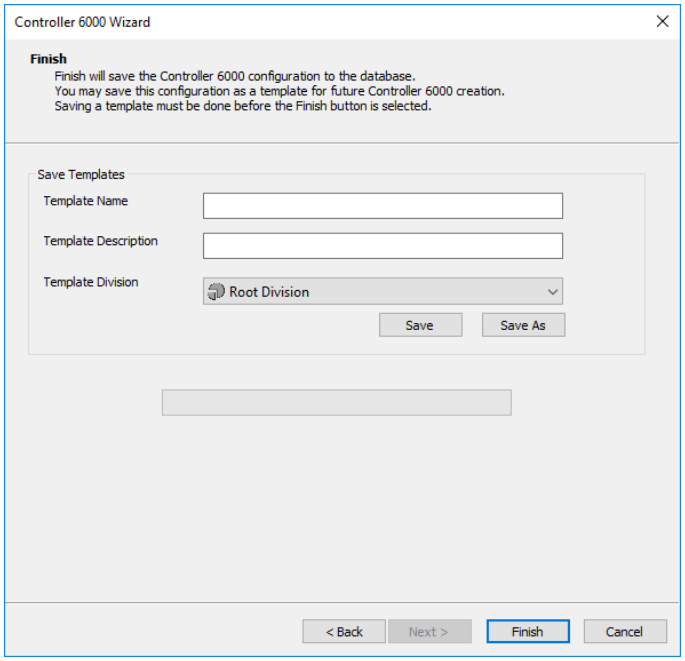
4. Click the **Start** button.
   The first screen of the appropriate wizard displays. Click the **Next** and **Back** buttons to step through the wizard.
   Notes:
   - The **Finish** button can be clicked at any time to create the item without stepping through each page. It brings you directly to the 'Finish' page where you can also create a template.
   - There are a number of configuration options common to all Controller and Door wizards, as follows:

Option	Description
Name and **Description** fields	Enter a name and description for the item being created. **Notes:** • The name can be up to 60 characters long, and the description, which is optional, can be up to 200 characters long. • As you type in the Name field, the Prefix field will also change to be the same.
Prefix field	This field appears on the first page of each of these wizards. It allows you to specify a naming prefix for any child items of the item you are creating. The wizard will use this prefix when creating default names for child items, (e.g. if you entered Door-1 as the prefix, any child inputs would be labelled Door-1 Input 1, Door-1 Input-2, etc.). **Note:** A prefix can be up to 60 characters long. If a child item's name (determined by the prefix and a suffix) is longer than 60 characters, then the prefix will be truncated.

Option	Description
CCC code field	These fields will only appear if your site is licensed for the Contact ID feature. Items that are required to report Contact ID events need to be configured to do so by assigning CCC codes to them. Change the code in the **CCC** field if required (3 Hex digits 0-9, B-F). **Notes:** • By clicking the Autofill button the wizard will pick the next available code for you. • 000 can be used to indicate that no specific zone or user information applies.
Icon Set list	This drop-down list is populated with all the icon sets that can be applied to the item being created. Select the icon set required.
☑ tick-box	By default, the ☑ tick-box beside an item indicates that it is selected. For any unused items, uncheck the appropriate tick-box.
Restore Defaults button	This button restores everything on that page to how it was when you first entered the page.

5. Refer to the relevant topic for details relating to the particular item you selected.
   Creating Controllers (on page 5-14)
   Creating Doors (on page 5-20)

'Finish' page

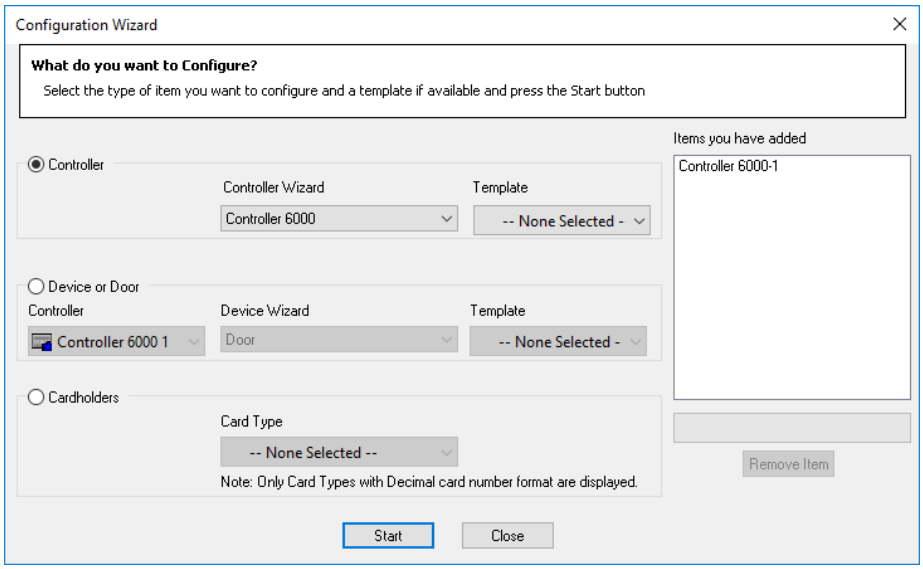


The final wizard page is titled 'Finish'.
Note: If the wizard was invoked with a template selected (at Step 3 of this procedure), then the fields on this screen will be populated, (i.e. they will display the name, description and division of the template selected). Otherwise they will be blank.

6. Do you want to save this configuration as a template for future use?

If...	then...
yes	Enter a Name and Division for the template, and optionally a Description. **Notes:** • If this wizard was started by opening an existing template, the **Template Name** field shall default to the name of the template. If you change the name, click the **Save As** button to create a new template, and the existing one will not be overwritten. If you click the **Save** button, the existing template will be overwritten. • Some fields in the wizards are not saved in the template as they are unique to that item, (e.g. **MAC** and **IP Address**).
no	go to Step 7.

7. Click the **Finish** button to create the items configured/chosen in the wizard and save them to the database.
Once the Progress bar reaches the end, the Configuration Wizard launch page re-displays.



You will notice that the item you created now appears in the **Items you have added** list on the right of this screen.
If you open the relevant list window, (i.e. **Hardware** or **Door** list window), the item will also appear there.
Note: If you have made a mistake, you can choose to remove the item by clicking on it in the **Items you have added** list and clicking the **Remove Item** button. All child items that were created in the wizard will also be removed, (e.g. inputs, outputs, readers, etc.).

8. You can now add further items to the system, (i.e. hardware devices, doors or cardholders), by either:
   - repeating Steps 3 through to 7, or
   - using an existing template if one has been saved for the type of item you want to add.
     See ***Wizard Templates*** (on page 5-33) for the procedure.

Notes:

- If you click the **Close** button now, you will exit the **Configuration Wizard**, and you can create further items later.
- Once you have configured the hardware, you can run a wiring report which provides instructions on how to wire the hardware items. See Wiring Report for further detail.

Creating Controllers

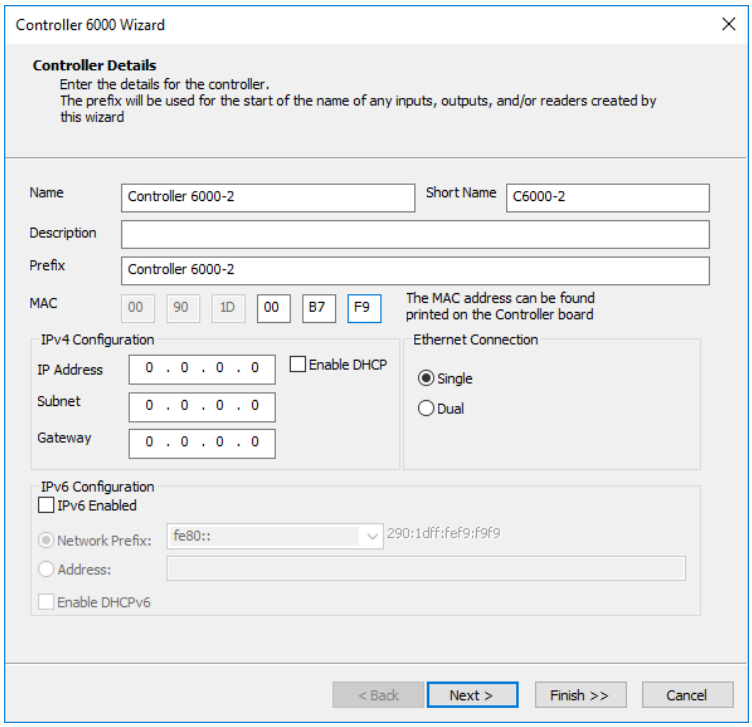
Introduction

The **Controller Wizard** offers the operator default choices with which to set up a Controller. The data configured in the wizard is the required basic information to configure a Controller in Command Centre.

Controller Wizard

The **Controller Wizard** contains a number of pages which prompt you to enter certain information to create a Controller.
Follow the instructions displayed.

'Controller Details' page



1. Enter a **Name**, **Description** and **Prefix** for the Controller.
   Refer to Step 4 of the ***Configuration Wizard*** (on page 5-9) procedure for details.
2. Enter the **MAC** Address for the Controller.
   The MAC Address can be found on a white sticker on one edge of the Controller.
3. What is the Controller configured for?

If…	then…
IPv4,	enter the **IP address**, **Subnet** and **Gateway** for the Controller.

If…	then…
IPv6,	**a)** Tick the **IPv6 Enabled** check box. The Network Prefix and the Address fields activate. **b)** Select an IPv6 address from the **Network Prefix** drop-down menu or, **c)** Select the **Address** radio button. **d)** Enter the IPv6 in the **address** field.
IPv4 or IPv6 using DHCP,	refer to the Enable DHCP for a new Controller 6000 using Wizard topic.

This information will be provided by the IT Department for the organisation, or the IT provider of the network. If there is no IT support for the site, and it is a localised and dedicated LAN built for Command Centre, there are some standards that you can apply to the configuration of the Controllers, as described below:

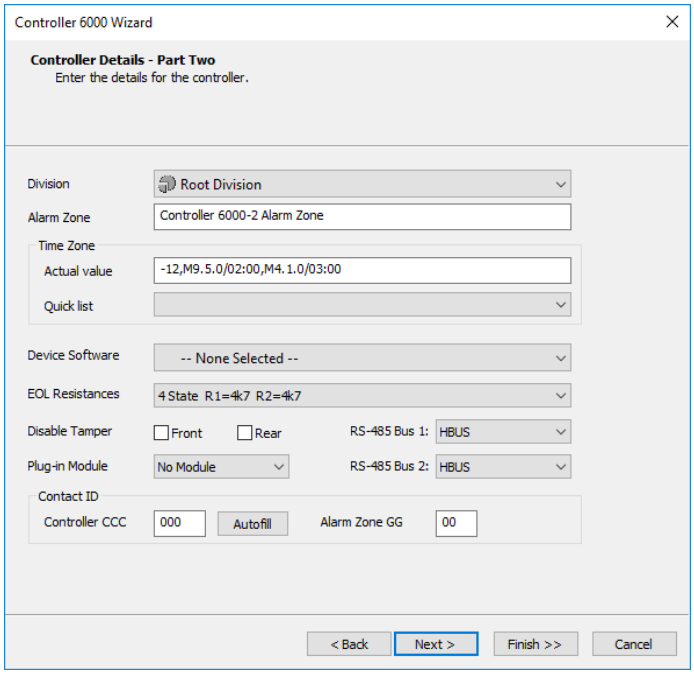
Configuration Parameter	Description
IP Address	The Internet Assigned Numbers Authority (IANA) has reserved several blocks of TCP-IP address space for private networks. These TCP-IP addresses have been set aside specifically for use when it is not necessary (or desirable) for the attached devices to be available on the Internet. If one of these TCP-IP addresses were accidentally broadcast on the Internet they would be ignored by the routing firewall server and would cause no conflict issues. To simplify IP range selection use the Class B range: Class B From 172.16.0.0 to 172.16.254.255 **Note:** Each device, (i.e. Computer, Printer, Controller) on the localised LAN must have a unique TCP-IP address. Each address used must however be in the same Subnet Mask range. This means when using the Class "B" TCP-IP address range, each TCP-IP address assigned to the localised LAN must start with 172.16 and then be unique, (e.g. 172.16.0.1, 172.16.0.2, 172.16.0.3, 172.16.0.4, etc.)
Subnet	There are default Subnet Mask settings for class categories. The Class B setting is: Class B From 172.16.0.0 to 172.16.254.255 Default Subnet Mask is 255.255.0.0 Use the associated Subnet Mask appropriate for the TCP-IP class used. The Subnet Mask differentiates between the network and client parts of the TCP-IP address. The "255's"

Configuration Parameter	Description
	identify the network section and the "0's" identify the clients. For a Class "B" TCP-IP address the network identification numbers are "172.16" and will be identical for each TCP-IP address on that network. The following two numbers of the TCP-IP address uniquely identify each device on the network.
Gateway	Gateway settings when used in general LAN configurations provide a path to a different network environment. In a localised LAN environment for Gallagher there is no physical connection to a different network, so the Gateway setting is ineffective. For single Subnet installations, it is recommended the Gateway information be set exactly as the TCP-IP address used.

Notes: The **MAC** and **IP Address** fields cannot be defined in a template and must be entered by the operator.

4. Select the radio button to choose **Single** or **Dual** as your ethernet connection.
5. Click the **Next** button.

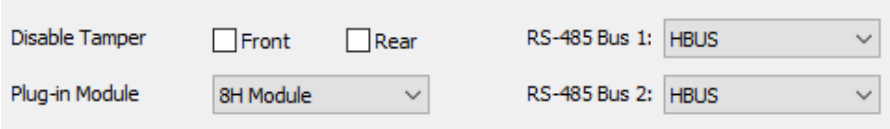
'Controller Details - Part Two' page



6. Assign the Controller to an existing **Division** from the drop-down list.
7. The **Alarm Zone** field is automatically populated with the assigned Alarm Zone name.
   Note: If you entered a prefix on the previous wizard screen, then the name of the Alarm Zone will be changed to "[Prefix] Alarm Zone".

8. Enter the **Timezone** string for the country your site is in by selecting the appropriate string from the drop-down **Quick list**.
9. The **Device Software** field is populated by default with the **-- None Selected --** option, giving you the flexibility to decide when the software on the Controller should be updated.

   You will be able to select a version of device software to be downloaded from the drop-down list.
10. The **EOL Resistors** drop-down list is populated with all EOL Resistance values available for the Controller type.
    Select the appropriate EOL Resistance.
11. If the Controller is not mounted in a cabinet, continuous tamper alarms will be generated. To prevent this from happening, tick the **Front** and/or **Rear** check box.
12. Select the appropriate **Plug-in Module** from the drop-down list.
    Options are No Module, 4R Module, 8R Module, 4 HBUS Module and 8 HBUS Module.

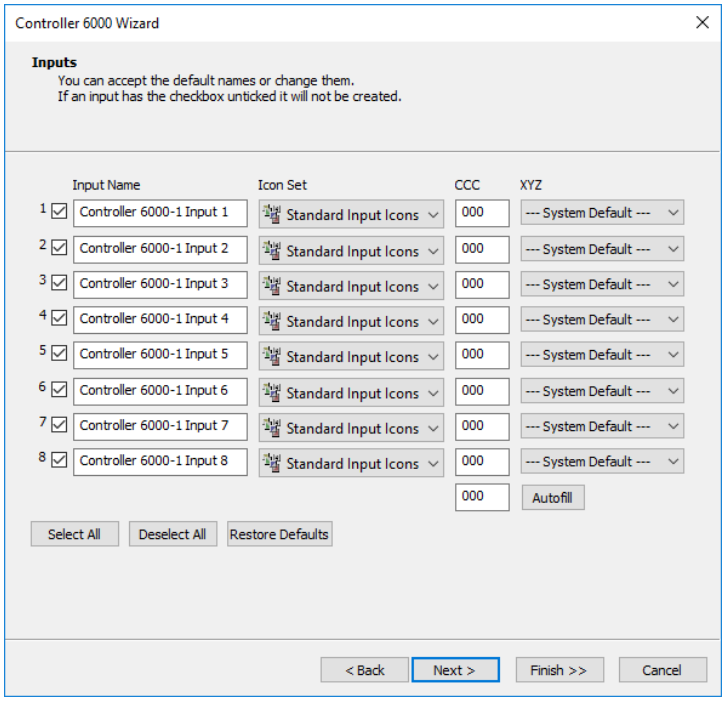


13. Select the appropriate Bus Type from the **RS-485 Bus 1** and **RS-485 Bus 2** drop-down lists.
    Both default to "HBUS", and have options for Aperio and Sensors.
14. Do the **Controller CCC** and **Alarm Zone GG** fields appear at the bottom of this screen?

If...	then...
yes	your site is licensed for the Contact ID feature. Refer to Step 4 of the ***Configuration Wizard*** (on page 5-9) procedure for details regarding the CCC code. Go to Step 15.
no	your site is **not** licensed for the Contact ID feature. Go to Step 16.

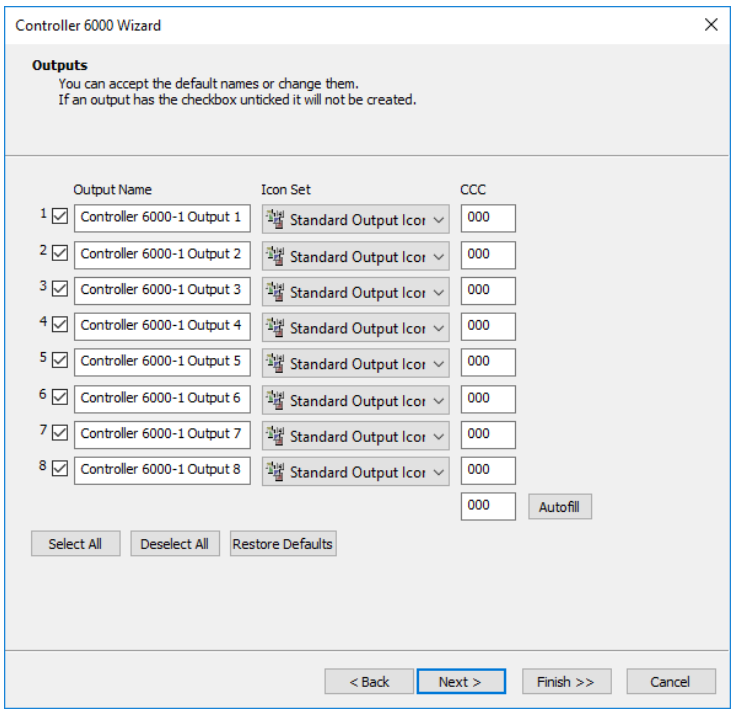
15. The Alarm Zones that are used for Contact ID need to have GG codes assigned to them.
    Change the code in the **Alarm Zone GG** field if required (2 Hex digits 0-9, B-F).
    Note: 00 can be used to indicate that no specific group or partition information applies.
16. Click the **Next** button.
    Note: For Controller 6000, If you do not select a Plug-in Module, you will not have the option to configure Inputs in the next page, then the next page to display is the **HBUS Devices**.

'Inputs' page



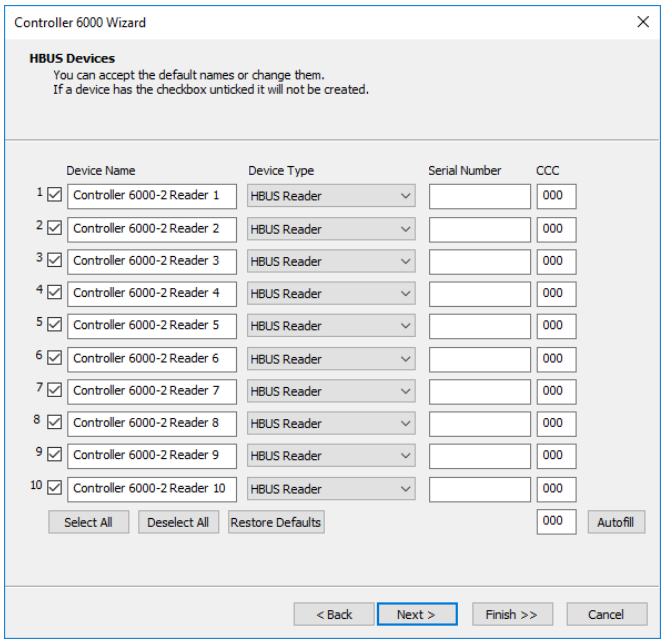
17. Either accept the default names for the Inputs, or change them as required.
    Note: The Controller 6000 Input numbers change depending on the selected Module. **Controller 6000** with **4H** and **4R** module have two pages of Inputs, **Controller 6000** with **8H** and **8R** Module have three pages of Inputs, (i.e. Inputs 1-8 on the first page, Inputs 9-16 on the second page and Input 17-24 on the third page).
18. Click the **Next** button.

'Outputs' page



19. Either accept the default name for the Output, or change it as required.
    Notes:
    - You can select on **Autofill** to automatically fill the CCC fields or fill each CCC field manually.
    - The Controller 3000-4R and Controller 6000 with 4H or 4R Module have Outputs 1-4.

'HBUS Devices' page



20. Either accept the default device names, or change them as required.
21. Select a **Device Type** from the the drop-down menu.
    The default device type is HBUS Reader.
22. Enter a unique Serial Number (optional) for each device.
23. Click the **Next** button.

'Finish' page

This wizard page is the same for Controllers and Doors, and provides the same options. Refer to ***'Finish' page*** (on page 5-12) in the 'Configuration Wizard' procedure for further detail.

Creating Doors

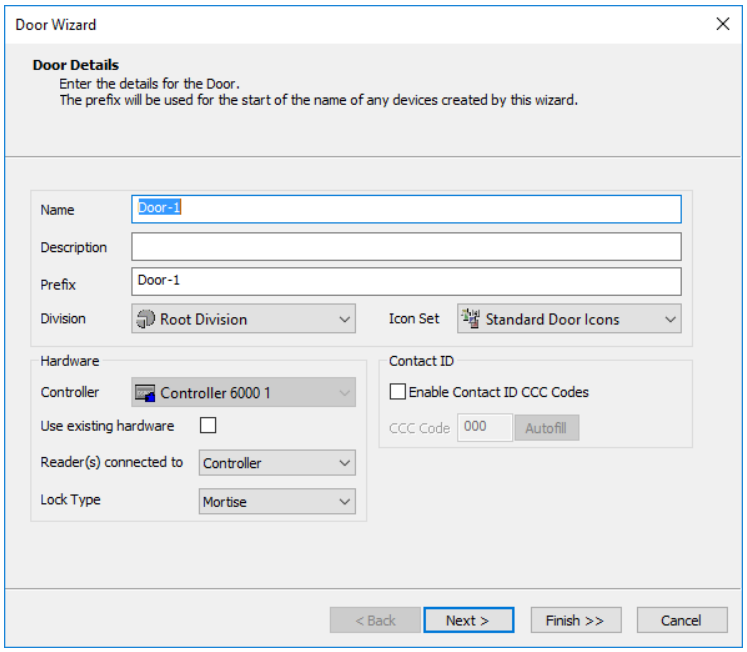
Introduction

The **Door Wizard** allows operators to easily create Doors in Command Centre.

Door Wizard

The **Door Wizard** contains a number of pages which prompt you to enter certain information to create a Door.
Follow the instructions displayed.

'Door Details' page



1. Enter a **Name**, **Description** and **Prefix** for the Door.
   Refer to Step 4 of the ***Configuration Wizard*** (on page 5-9) procedure for details.
2. Select the **Division** the Door is to be created in from the drop-down list.
   Notes:
   - By default the Controller's division populates the **Division** field.
   - The **Division** drop-down will list all the divisions for which you are privileged to create doors in. If you change the division here, this resets only the door's division. All other items, (e.g. inputs, readers, etc.) will be created under the Controller's division.
3. If the wizard was started from the Configuration Wizard (thus a controller must have been selected) then the **Controller** field will be 'read only' and the assigned controller will be selected. Otherwise the field will not be 'read only' and the **-- None Selected --** entry selected.

4. Do you want to use existing hardware or create new hardware items for this Door?

If you want to...	then...
use existing hardware,	check the **Use existing hardware** checkbox. The **Reader(s) connected to** field becomes disabled.
create new hardware,	from the **Reader(s) connected to** drop-down list, select what the door's hardware items will be connected via, (i.e. 'Controller').

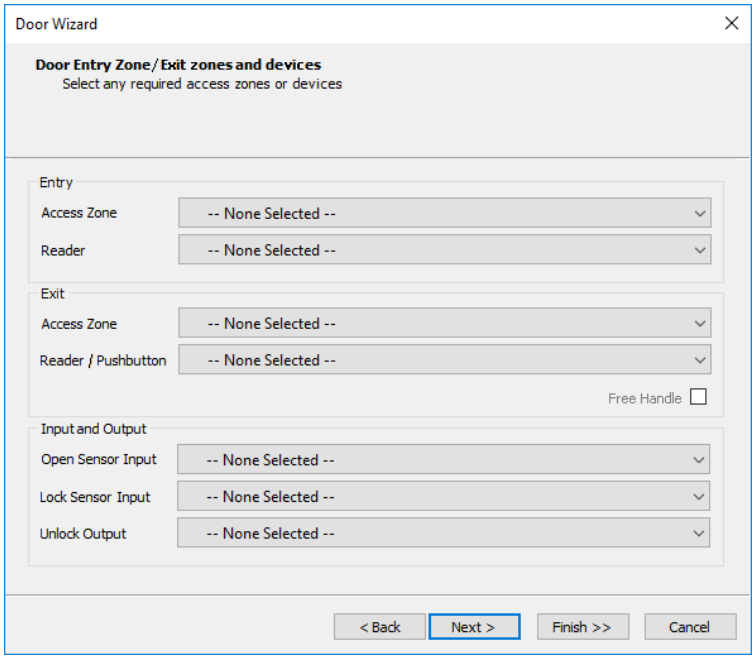
5. Select the appropriate **Lock Type** from the drop-down list:

Lock Type	Description
Shear	When configured as a Shear Lock and a valid card is presented the door unlocks. If the door is not physically opened it will relock after the "Door unlock time" is exceeded. If the Door is opened, the lock relay remains active until the Door open sensor recloses, (i.e. the Door closes). **Uses:** Electronic bolts or double doors that do not have to rebate to prevent the inactive door locking prior to the active door.
Mortise	When configured as a Mortise Lock and a valid card is presented the door unlocks. If the door is not physically opened it will relock after the "Door unlock time" is exceeded. If the Door is opened the lock relay resets immediately when the Door Open sensor switches open. When the Door physically closes the lock is in a state that immediately re-secures the Door. **Uses:** - Most standard lock situations - Magnetic clamp locks
Automatic	When configured as an Automatic Lock the lock relay will always be activated for the user configured time. This time is set by the use of the **Door unlock time** option. All other settings will be as for the other lock types. **Uses:** Magnetic clamp door with only one Input.

6. If your site is licensed for the Contact ID feature, check the **Enable Contact ID CCC Codes** checkbox.
   The **CCC Code** field is enabled. Refer to Step 4 of the ***Configuration Wizard*** (on page 5-9) procedure for details.

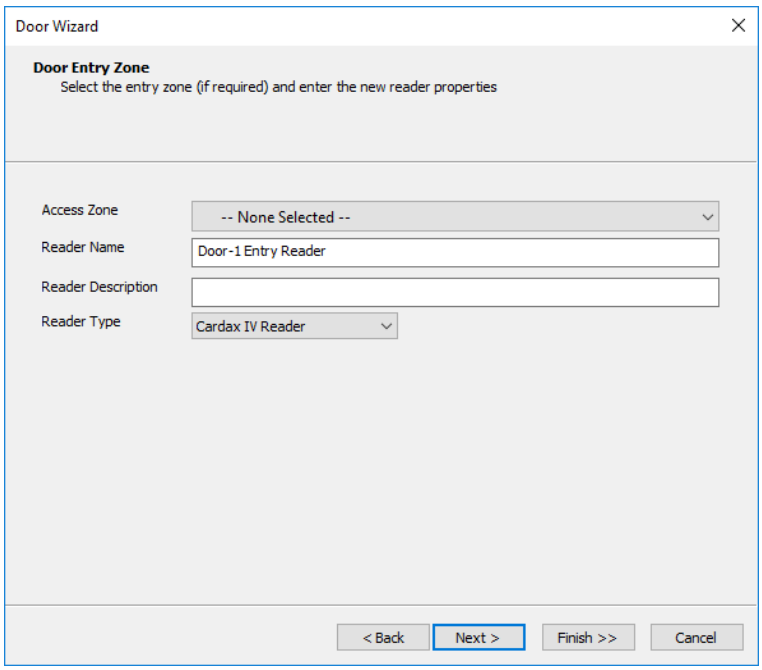
7. Click the **Next** button.
8. Did you check the **Use existing hardware** checkbox?
   If **no**, go to Step 13.
   If **yes**, then the 'Door Entry/Exit zones and devices' page displays.

   'Door Entry/Exit zones and devices' page



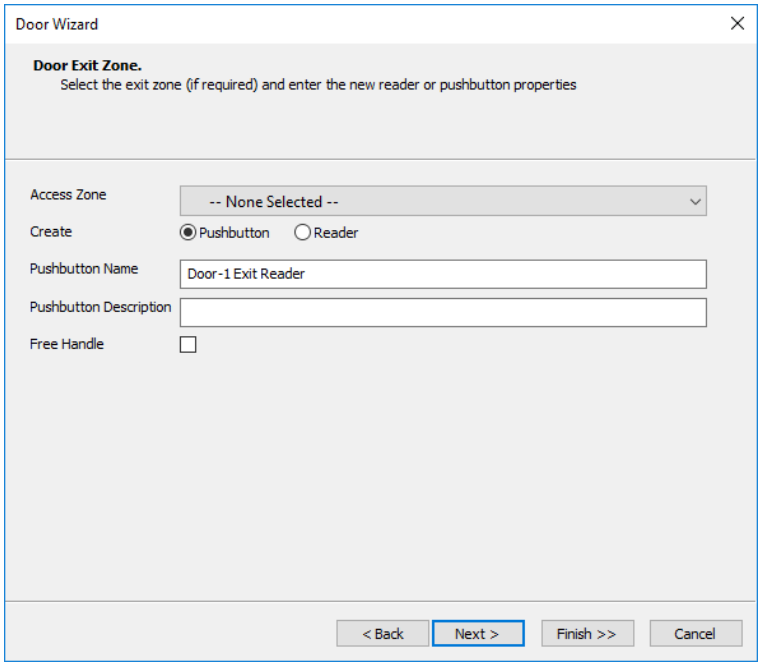
   The Entry and Exit **Access Zone** drop-down lists are populated with all Access Zones you have access to. Unless otherwise stated, all of the other drop-down lists are restricted to items on the Controller (specified on the 'Door Details' page), and are also restricted to items which are not already on a door.
9. In the 'Entry' section of this page, select the **Access Zone** you enter into and the associated **Reader** from the drop-down lists.
10. In the 'Exit' section of this page, select the **Access Zone** you exit to and the associated **Reader/Pushbutton** from the drop-down lists.
    If you selected an item that can be assigned to a door as a Pushbutton rather than a Reader, the additional **Free Handle** option is enabled. This can be used for doors where the lock does not need to be unlocked for exit. If you enable (check) this option, and a valid exit request is made, the doors lock relay will not activate (doors outside handle will remain locked), in order to suppress the forced door alarm.
11. In the 'Input and Output' section of this page, select the Inputs and Outputs for this door.
12. Click the **Next** button.

'Door Entry Zone' page



13. Select the **Access Zone** you enter into from the drop-down list.
14. Enter a **Reader Name** and **Description** if applicable.
15. Select a **Reader Type** from the drop-down list.
    Note: The options available in this drop-down list depends on what you selected previously for the readers to be connected to. If you assigned this door to a Controller 6000 (on the 'Door Details' page) there will be an additional 'HBUS Reader' type available. If you select 'HBUS Reader', a **Reader Serial Number** field appears, allowing the serial number of the HBUS Reader to be entered.
16. Click the **Next** button.

'Door Exit Zone' page

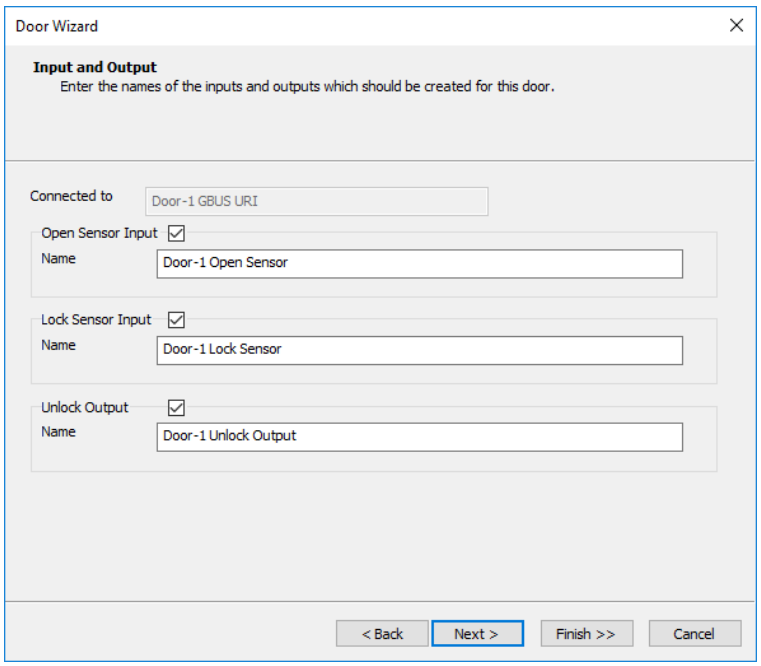


17. Select the **Access Zone** you exit to from the drop-down list.
18. Select whether exit is controlled by a **Pushbutton** or **Reader**, by clicking the appropriate radio button.
19. Enter a **Name** and **Description** for the Pushbutton/Reader.
20. Which radio button did you select?

If you selected...	then...
Pushbutton	an additional **Free Handle** option is available. This can be used for doors where the lock does not need to be unlocked for exit. When this option is enabled (checked), and a valid exit request is made, the doors lock relay will not activate (doors outside handle will remain locked), in order to suppress the forced door alarm.
Reader	a **Reader Type** drop-down list is available. The options available in this drop-down list depend on what type of connection device, (i.e. Controller) you selected earlier. See Step 12.

21. Click the **Next** button.

'Input and Output' page



22. Enter the names of the inputs and outputs to be created for this door.
23. Click the **Next** button.

'Finish' page

This wizard page is the same for Controllers and Doors and provides the same options. Refer to ***'Finish' page*** (on page 5-12) in the Configuration Wizard procedure for further detail.

Creating Cardholders

Introduction

The **Cardholder Wizard** allows you to create cards and cardholders. Operators require the "Edit Cardholder", "Modify Access Control" and "View Site" operator privileges (all in the correct division) to run the Cardholder Wizard.

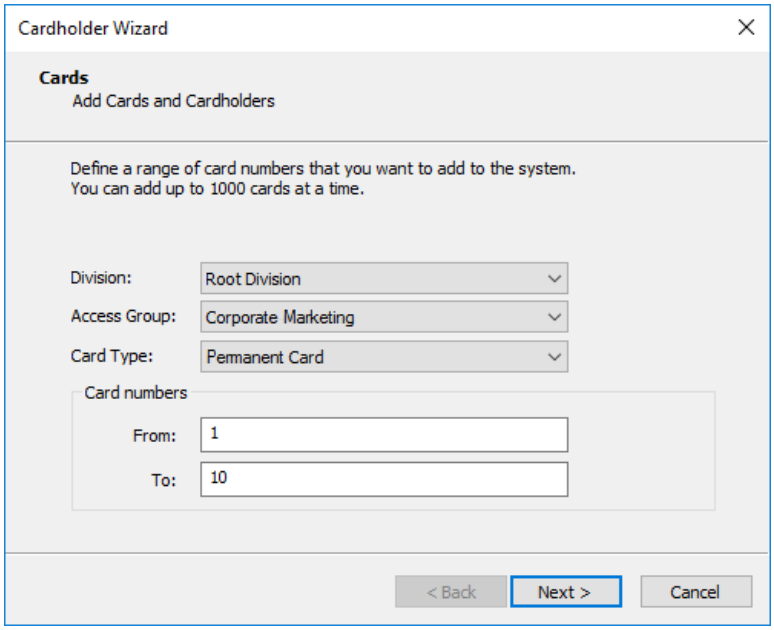
Cardholder Wizard

The **CardholderWizard** contains a number of pages which prompt you to enter certain information to create Cardholders.
Follow the instructions displayed.

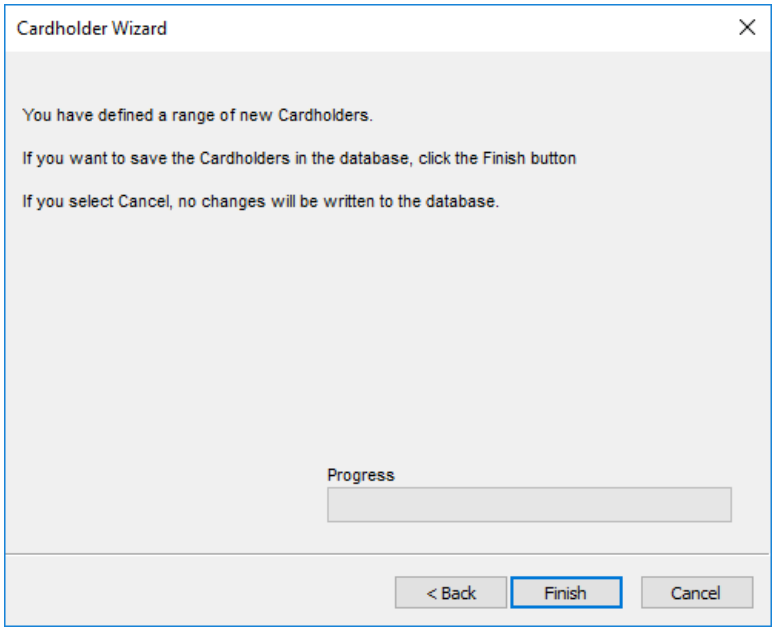
Procedure

1. Click the **Cardholders** radio button.
2. Select the type of card you want to create from the **Card Type** drop-down list.
3. Click the **Start** button.

'Cards' page



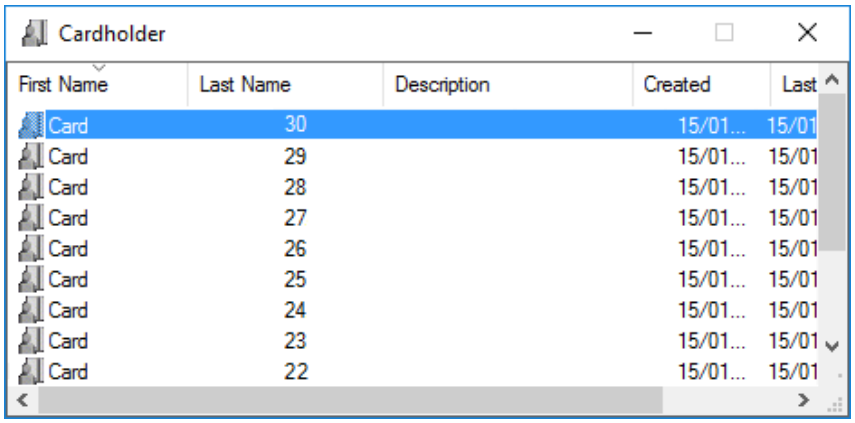
4. Configure the details as appropriate.
5. Click the **Next** button.
   The final screen of the **Cardholder Wizard** displays.



6. Click the **Finish** button.
   Once the Progress bar reaches the end, the Configuration Wizard launch page re-displays.

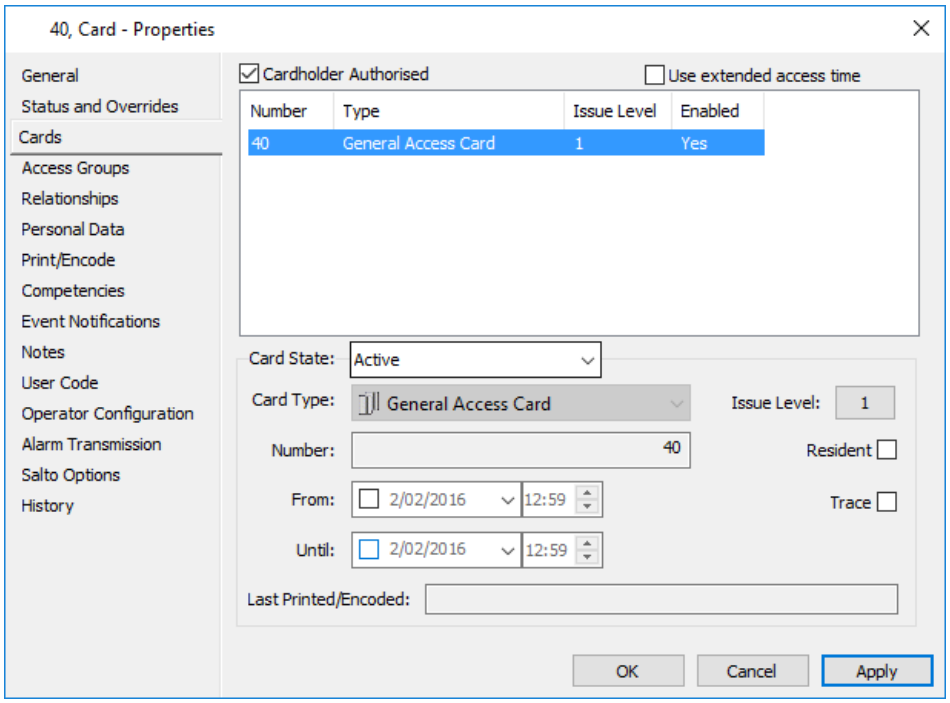
Note

The **Cardholder** wizard allows you to create cards and cardholders. You define a range of card numbers to add to the system (with a limit of 1000 cards at a time), and as a result the Cardholder list window is populated with the same amount of cardholders as cards created, (e.g. if you created a range of card numbers from 1 to 300, there would be 300 new cardholders displayed).



The cardholders appear with the word "Card" as the **First Name** and the card number as the **Last Name**. Now when you replace these with actual cardholders names, the process is a lot quicker as they have already got card numbers assigned to them, and they are assigned to an Access Group.

The cardholders are configured as shown below, (i.e. they have Issue Level 1. the cardholders are authorised, they have no expiry date and the 'Resident' and 'Card Trace' options are not set).



If you enter card numbers that already exist, cardholders are only created for the numbers up to the first one that already exists, and then no more are created. An error message will display when the first existing card is found, and card creation stops.

Examples:

- Cards 1 to 10 already exist. An operator tries to create cards 5 to 50. None are created.
- Cards 1 to 10 and 20 to 40 already exist. An operator tries to create cards 11 to 70.
  Only cards 11 to 19 are created.

Wizard Templates

Introduction

Wizard templates are intended to standardise Command Centre implementations and improve the install time for sites. Installation companies may create themselves a set of standard templates that may be re-used for the majority of their sites. These templates can be copied from site to site using the export/import feature of the templates.

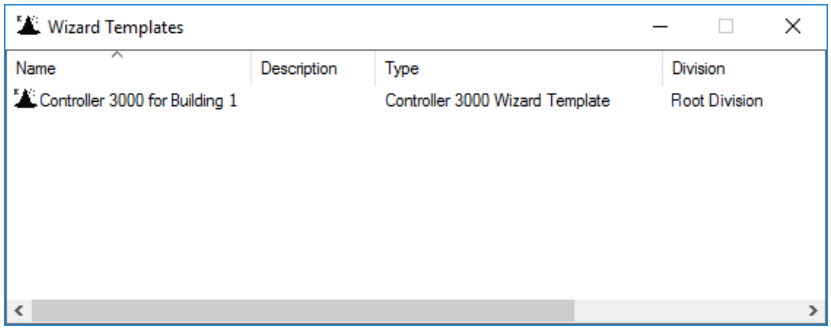
From within the **Wizard Templates** List Window you can set up new wizard templates, and you can view, modify and delete existing wizard templates.

Operators require the "Edit Site" operator privilege in the appropriate Division to be able to create, edit import or export wizard templates.
Note: Localbus hardware device and Cardholder wizards do **not** support templates.

Procedure

Opening the Wizard Templates window

1. Click **Wizards** from the menu bar.
2. Click **Wizard Templates**.
   The **Wizard Templates** List Window displays:



3. Go to the procedure you want to perform next.
   - ***Creating a new wizard template*** (on page 5-33)
   - ***Creating an item using an existing wizard template*** (on page 5-34)
   - ***Importing/Exporting wizard templates*** (on page 5-35)

Creating a new wizard template

1. **Right click** and select **New**.
   The Configuration Wizard launch page displays.
2. Select what type of template to create by selecting the type of hardware, and click the **Start** button.
   The first page of the wizard displays.

3. Work your way through the wizard, until you reach the 'Finish' screen.
4. Enter a **Template Name**, and optionally a **Template Description** for the template.
5. Select a **Template Division** for the template from the drop-down list.
6. Click the **Save** button.
   The new wizard template is saved and displays in the **Wizard Templates** List Window.
7. Do you want to create the Command Centre item you've just configured?

If...	then...
no	click the **Cancel** button. The Command Centre item is not created. The Configuration Wizard launch page re-displays.
yes	click the **Finish** button. The Command Centre item is saved to the database. The Configuration Wizard page re-displays, with the item you've just created appearing in the **Items you have added** list on the right.

8. Click the **Close** button.

Creating an item using an existing wizard template

1. **Double-click** on the wizard template you want to use.
   The first page of the wizard displays.
   Notes:
   - Some fields in the wizards are not saved in the template as they are unique to that item, (e.g. **MAC** and **IP Address**).
   - If the **Name** of the item being configured has a number on the right-hand end of it, then the system increments the number by one from the highest number in use, for the name, in the system.
     For example:
     If controllers named **Bldg1 Controller1** to **Bldg1 Controller7** exist on the system, by default, the next one would be named **Bldg1 Controller8**.
2. Work your way through the wizard, until you reach the 'Finish' screen.
3. Click the **Finish** button to create the items configured/chosen in the wizard and save them to the database.
   The wizard closes, and if you open the relevant List Window, (i.e. **Hardware** or **Door** List Window), the items will now appear there.

Importing/Exporting wizard templates

Wizard templates can be exported to another Command Centre installation, or you can import wizard templates that have been saved from another Command Centre system.

Note: Importing/exporting templates does not delete them from the source, it only copies them to the target location.

1. **Right click** in the List Window and select the required option, (i.e. **Import** or **Export**).
2. Which option did you select?

If...	then...
Import	**a)** From the displayed pop-up window, path your way to the Command Centre wizard template(s) you wish to import. **b)** Select the division to import the templates into from the **Division** drop-down. **c)** Click the **Open** button. The template(s) are imported and appear in the **Wizard Templates** List Window. **Notes:** • If any templates of the same name already exist, then no templates are imported and an error message displays. • The contents of all the files are validated. If a template fails the validation test then no templates are imported an error message displays.
Export	**a)** From the displayed **Browse for Folder** dialog, path your way to the directory to export the template(s) to. **b)** Click the **OK** button. A message displays indicating that the selected wizard template(s) have been exported. The name of the file(s) is the name of the template(s), with the file extension **.FTWizardTemplate**.

Chapter 6: Server Properties

Properties of the Command Centre Server effect the complete system; they are system-wide settings. The information you set here filters down through the complete system, with the exception of the **Icons** and **Notes** tabs.
This section covers the following topics:

- ***Opening the Server Properties window*** (on page 6-3) The General tab displays by default when the Server Properties window is opened.
- ***Licensing*** (on page 6-4)
  Here you can view your sites current Command Centre license details and/or update it without stopping the server and/or services.
  Note: This tab is only visible if you have the "Advanced User" operator privilege in the Root Division.
- ***Event Priorities*** (on page 6-7)
  Here you can set the lowest alarm priority that is considered an actual alarm.
- ***Alarm Flooding*** (on page 6-9)
  Here you can configure alarm flooding.
- ***Alarm Zone states*** (on page 6-11)
  The required terminology when referring to the Alarm Zones is set here.
- ***Event Defaults*** (on page 6-12)
  Site wide default action plans that will be followed when individual items are set to use the default.
- ***Alarm Instruction Defaults*** (on page 6-14)
  Alarm Instructions inform a workstation operator of what needs to be done in the eventuality of an alarm.
- ***Alarm Transmission*** (on page 6-15)
  On this tab you can assign XYZ value of Contact ID Event Codes to Event Groups.
- ***Alarm Notes*** (on page 6-17)
  This tab is used to configure mandatory alarm notes.
- ***Operator Defaults*** (on page 6-19)
  Password and/or Operator restrictions are set via this tab.
- ***User Codes and PINs*** (on page 6-23)
  This tab allows the minimum length of User Codes to be set, and credentials to be disabled when a PIN is entered incorrectly at a T2x reader too many times.
- ***Competency Messages*** (on page 6-24)
  Here you can modify the system-wide default messages for competencies.
  Note: This tab only displays if your site is licensed for the Cardholder Competencies feature.
- ***State Names*** (on page 6-26)
  The messages displayed in the Event window when inputs and outputs change state can be configured within this tab.
- ***Measurement Units*** (on page 6-28)
  Sites can select their preferred measurement units for Gallagher Security Electric Fence Controllers and Taut Wire Sensor properties on this tab.
- ***Advanced*** (on page 6-30)
  Here you can enable/disable the Activity Indicator and configure how much memory the SQL Server uses, set default mappings for Logic Blocks and set old alarms to automatically process.

- ***Web Services*** (on page 6-33)
  Here you can replace the web service certificate with an alternate certificate, when using the Mobile Client, and configure the server base port for the REST API.
- ***Card Security*** (on page 6-37)
  The site security information is set vis this tab.
- ***Notifications*** (on page 6-47), ***Outgoing Email*** (on page 6-49), ***Incoming Email*** (on page 6-52) and ***Mobile/SMS Notifications*** (on page 6-53)
  These tabs are used to configure event, alarm, and expiry notifications. **Note:** These tabs only display if your site is licensed for the Notifications feature.
- ***Import*** (on page 6-55)
  This tab is only used when importing Cardholder info into Command Centre.
- ***Database Maintenance*** (on page 6-56)
  This tab is used to set the parameters for when cardholder history and/or expired visits will get purged from the system.
- ***Controller Defaults*** (on page 6-58)
  This tab allows system-wide software settings to be configured for Controllers.
- ***Controller Web Server*** (on page 6-60)
  This tab allows sites to export the CA Certificate and generate CA.
- ***Reserved Input Defaults*** (on page 6-62)
  This tab allows sites whose Controller 7000s are housed in cabinets to use physical tamper inputs (rather than optical tampers), and to also reserve power supply inputs and create alarms with the Controller as a source.
- ***Challenge*** and ***More Challenge*** (on page 6-63)
  These two tabs allow the Challenge feature to be configured for the site.
- ***Standards*** (on page 6-64)
  This tab is used to configure specific system-wide behaviour with respect to alarm system standards.
- ***Data Retention*** (on page 6-72)
  This tab allows the removal of events and other data related to cardholders from Command Centre, and will only display if your site is licensed for either PII Redaction or Data Retention.
- ***Mobile Access Settings*** (on page 6-73)
  This tab allows you to configure the site wide defaults for readers using Mobile Connect.
- ***HBUS Terminal Defaults 1 and 2*** (on page 6-76)
  These two tabs allow you to specify the site wide Alarms List Defaults, Arming Defaults, Idle screen images and Mimic Panel LED Settings for all HBUS Terminals (HBUS Terminals and HBUS Alarms Only Terminals).
- ***SIP Settings*** (on page 6-79)
  This tab is enabled by the licensed SIP Integration, and contains system-wide SIP settings. **Note:** This tab will only display if your site is licensed for the SIP Integration feature.
- ***Icons*** (on page 6-80) This tab shows the Icon Set assigned to the Server.
- ***Custom Fields*** (on page 6-81)
  This tab allows you to add and assign a custom field value to the site item.
- ***Notes*** (on page 6-85)
  Notes about the Server Properties can be recorded on this tab.

The arrows ▲ ▼ enable you to move through the tabs.

Opening the Server Properties window

Introduction

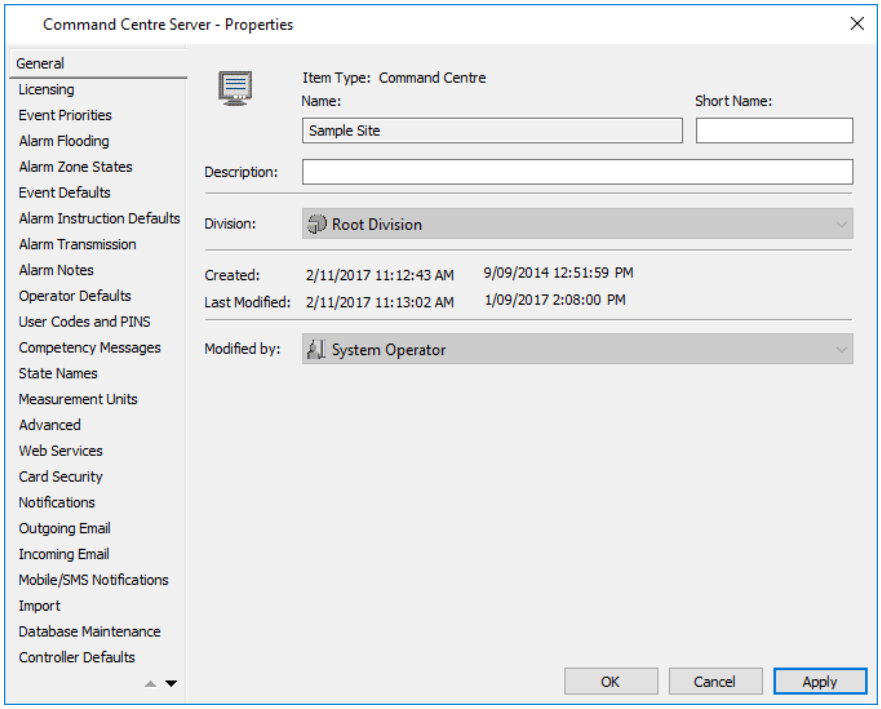
Within the Server Properties window you can modify the system-wide settings of the Command Centre Server.

Procedure

1. Click **File** from the menu bar.
2. Click **Server Properties**.

Result

The Command Centre Server Properties window displays:
(The **General** tab is automatically displayed by default.)



Note: The only fields that are not "read-only" on this screen are **Short Name** and **Description**. For further detail see ***General tab*** (on page 3-18).

Hint

An alternative method of opening the Server Properties is:

1. Click **Configure** from the menu bar.
2. Click **Hardware**.
3. Highlight the Command Centre **Server** icon , (i.e. the very top item in the tree view list).
4. **Right click** and select **Properties**.

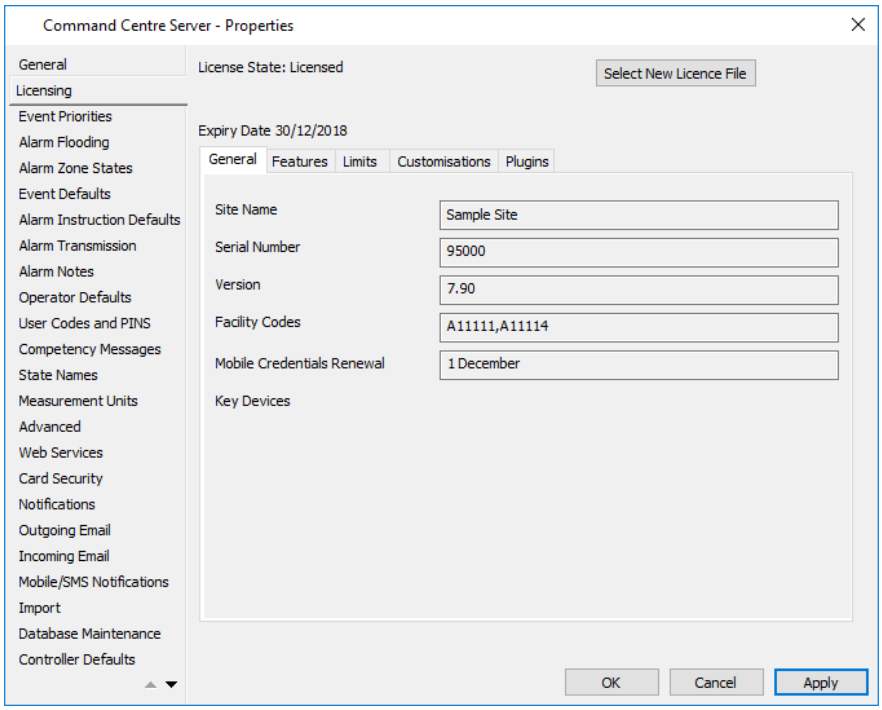
Licensing

Introduction

This tab is only visible to operators with the "Advanced User" operator privilege in the Root Division. It enables them to view their sites current Command Centre license details and/or update the license without stopping the server and/or services.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Licensing** tab.



Displayed at the top of the screen of this screen is the current state of the attached license and it's expiry date. There are three possible states, (i.e. Licensed, Unlicensed, or License has expired but is still operating within a grace period).

Below that are five "read-only" sub-tabs each providing information about the attached license.

The **General** sub-tab displays by default. It provides the following general license data:

Field	Description
Site Name	The name of the attached license.
Serial Number	The serial number of the attached license.

Field	Description
Version	The software version the license is applicable to.
Facility Codes	Made up of the The Region Code (A - P) + Facility Code (00000 - 50000) A Facility Code is an identification number stored on the access token. Each site or facility normally has their own unique facility code.
Mobile Credentials Renewal	The annual renewal date for sites licensed for Mobile Credentials. If a site is not licensed for Mobile Credentials, the field will be blank.
Key Devices	One or more 'key devices' (Controllers). While at least one of the key devices is online the site is considered licensed and functions normally. If all key devices are offline the site enters a grace period (usually 30 days). When the grace period expires the site becomes unlicensed and all Controllers will be disconnected.

The other four sub-tabs each provide the following information about the attached license:

Sub-tab	Lists alphabetically...
Features	the features in the license and indicates whether they are enabled or disabled.
Limits	the item types in the license, with the associated limits and current count for each item type.
Customisations	any customisations included in the license, including the version of the customisation, whether it is licensed and what it applies to.
Plugins	the plugins in the license.

3. Do you want to replace the license file?

If...	then...
no	go to Step 4.
yes	**Note:** For license replacement to succeed, the service account should be granted full access to the license file and the services should be running as administrator. **a)** Click the **Select New Licence File** button.

If...	then...

b) From the displayed pop-up window, path your way to the license file you wish to replace your existing one with.

c) Click the **Open** button.

d) Click the **Apply** button.
The license details on each of the sub-tabs change accordingly.
Notes:

- An error message will display if the selected license file is not valid for the version of Command Centre installed.
- Some additional features in the selected license file may require either a restart of the client, or a stop/start of services to enable them.

4. Click the **OK** button to exit.

Event Priorities

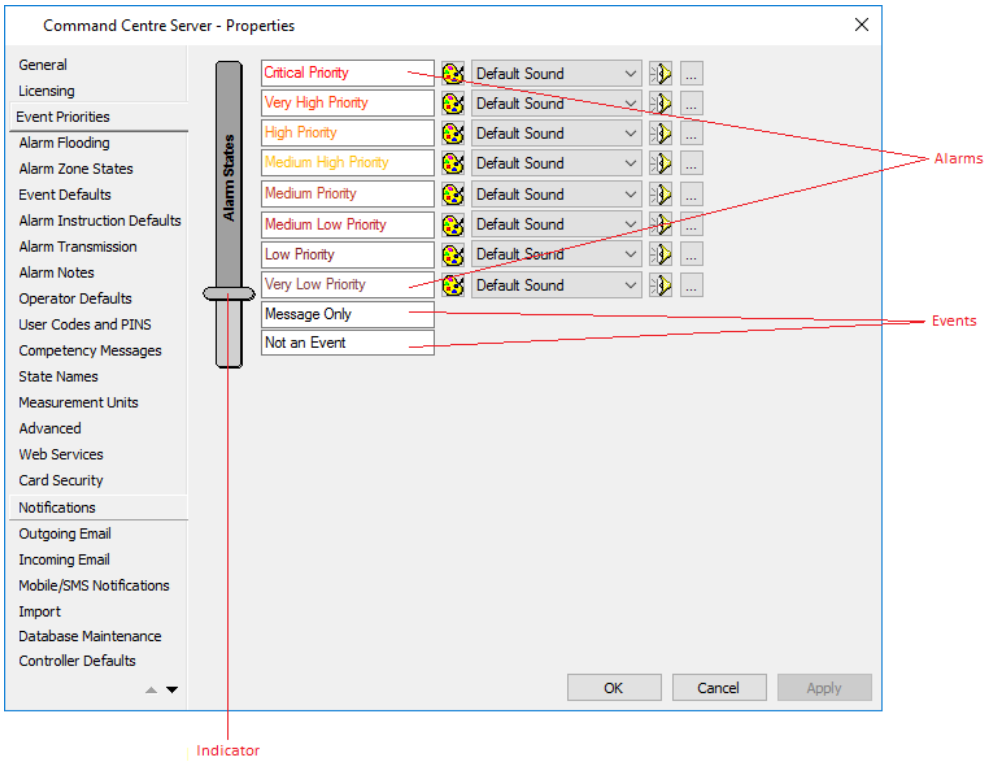
Introduction

There are 10 levels of messages within the Command Centre system. Each level is allocated a logical name, colour and alarm sound (optional); you can change these from their defaults.

You also set which message level is the lowest alarm priority. Those levels above the indicator will generate an alarm, those levels below the indicator will generate an event message.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Event Priorities** tab.



3. Move the mouse pointer to the **indicator** on the Alarm States bar. Click and hold down the mouse button. Drag the indicator to point to the **lowest alarm priority** you want to generate an actual alarm.
   Note: The indicator will only allow a minimum of two event priorities and one alarm priority.
4. To change the message level **name**, click within the appropriate edit box and **edit the text** as required.
5. To change the **colour**, click on the **colour palette icon** beside the appropriate message.

From the displayed colour swatch select the **required colour** to represent the event priority and click **OK**.

The drop-down menu boxes beside each message level display "Default Sound", which will be used for alarm sounds.
Notes:

- An alarm sound is optional, therefore "No Sound" is the other option in the list.
  Note though that if two alarms occur and the lower priority alarm has an alarm sound configured, but the higher priority alarm has "No Sound" configured for that event priority, then no alarm sound will play. Therefore, we recommend that you do NOT turn off alarm sounds for an event priority if there are lower event priorities that have an alarm sound configured.
- The 'Message Only' and 'Not an Event' priorities cannot have alarm sounds configured as they can never be alarms.

6. If you want to change the alarm sound for a particular message level, click the corresponding **Sound File Browse** button.
   A **Select Audio File** dialog displays showing only **WAV files** (***.wav**) as they are the only file type that can be used for alarm sounds.
7. Path your way to the appropriate audio file and click the **Open** button.
   The name of the audio file displays in the corresponding sound file name drop-down list.
   Note: Any **WAV files** (***.wav**) selected should:
   - have a play time of no more than two seconds, as the Alarm Viewer replays an alarm sound every two seconds. Very short files, (e.g. that say "Duress", or "Critical", or play only a few notes) are ideal.
   - be PCM format. If you select a non-PCM format WAV file, the following error message displays:
     "Sound file must be PCM format."
   - be less than 500KB in size. If you select a ***.wav** file over this size the following error message displays:
     "The file cannot be loaded as it exceeds the limit imposed by the system."
8. To listen to a selected alarm sound before confirming your selection, click the **Sound Preview** button to play the corresponding sound.
   Note:
   If an alarm sound has a play time of more than two seconds, when you preview it here it will play from start to finish.
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.

Alarm Flooding

Introduction

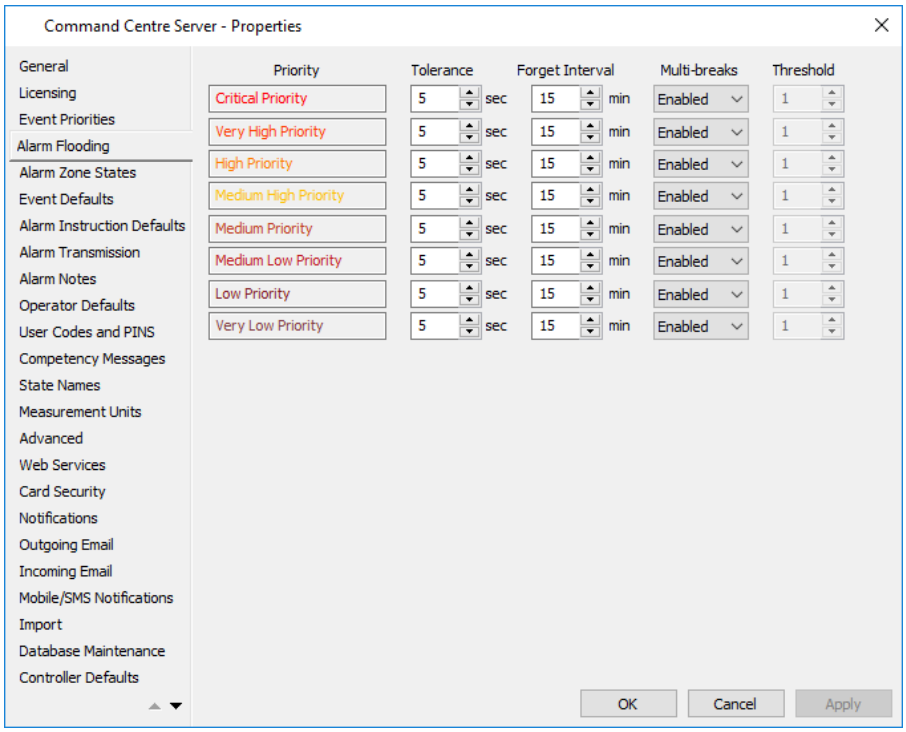
Alarm Flooding occurs when the same alarm is generated numerous times and fills up the Alarm Viewer window. Alarms qualify as "Flood Alarms" when the following conditions apply:

- There exists a previous alarm which has the following identical fields:
  - Priority
  - Source
  - Event Type
  - In the case of Card alarms, the card details (card number, facility code) must also be matched
- The alarm occurs within a specified number of seconds after the previous alarm. Where the number of seconds is the "tolerance" for the priority at which the alarm occurred.
- The previous alarm has not been acknowledged.

This procedure allows you to specify time periods during which Command Centre will summarise multiple occurrences of the same alarm. Operators require the "Edit Site" operator privilege to perform this procedure.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Alarm Flooding** tab.



3. Enter times (in seconds) in the **Tolerance** column for the Alarm Priorities required. If you set the tolerance time to 0, alarm flooding will not operate for that priority of alarm.

   The **Tolerance** time is the period of time allowed between repeated alarms to constitute an Alarm Flood. Repeated alarms that occur outside of the tolerance time will constitute new alarms, whereas unprocessed repeated alarms inside the tolerance time will become part of an Alarm Flood.

4. Enter times (in minutes) in the **Forget Flood Intervals** column for the Alarm Priorities required.

   The purpose of the **Forget Flood Interval** time is to remind operators that an alarm is still occurring, therefore if a new occurrence of an alarm occurs after the **Forget Flood Interval** time specified, the alarm (flood) is moved to the top of it's priority in the Alarm Viewer window.

   For example:
   If the Forget Flood Interval is set to 10 minutes, and an alarm occurs at 2:00pm and keeps reoccurring, the first occurrence of the alarm after 2:10pm will move the alarm flood to the top of it's priority in the Alarm Viewer window.

5. Select the appropriate option from the **Multi-breaks** drop-down lists, for the Alarm Priorities required:

Option	Description
Enabled	Each alarm activation and restoral is transmitted. This is the default behaviour.
Latched	Only the first activation of an alarm from any one source is transmitted and the restoral is sent according to the Action Plan's Deactivate rule. If the Alarm Zone changes from its known state to any other state, then multi-breaking will be reset.
Unlatched	When Unlatched is selected, the **Threshold** field becomes enabled. This setting allows the number of alarms whose activation and restoral is transmitted to be changed from 1 only to a nominated number up to 10 before multi-breaking is reset. Multi-breaking will also be reset on expiry of the confirmation time if 'Enable confirmed alarms' is selected on the **Standards** tab. If the **Threshold** is set to 1, only the first alarm activation and restoral is transmitted. If the Alarm Zone changes from its known state to any other state, or the alarm is acknowledged, then multi-breaking will be reset.

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

Result

The selected Tolerances and Forget Flood Intervals have been configured.

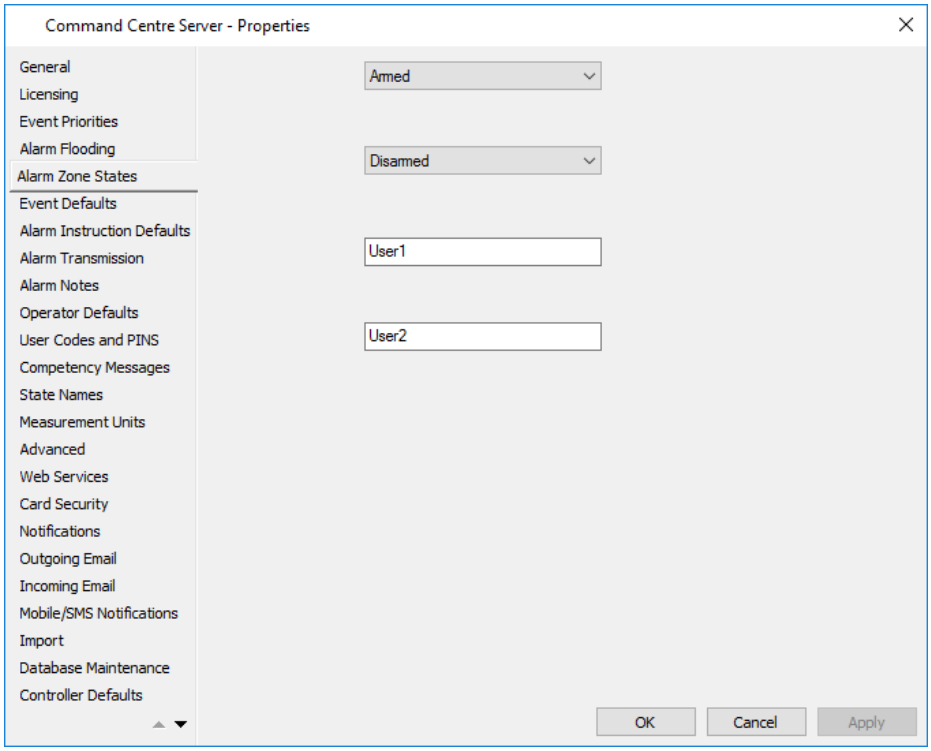
Alarm Zone States

Introduction

Command Centre provides a maximum of four Alarm Zone States. Within this tab set your naming (terminology) of these states.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Alarm Zone States** tab.



3. For the first two Alarm Zone States, click on the button to display the **drop-down menu list**.

   Select the terminology to use throughout the Command Centre system.
   - Armed or Set
   - Disarmed or Unset

4. If you wish to rename the remaining two Alarm Zone States, (i.e. User1 and User2), do so by highlighting the state and typing in the new name.
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.

Event Defaults

Introduction

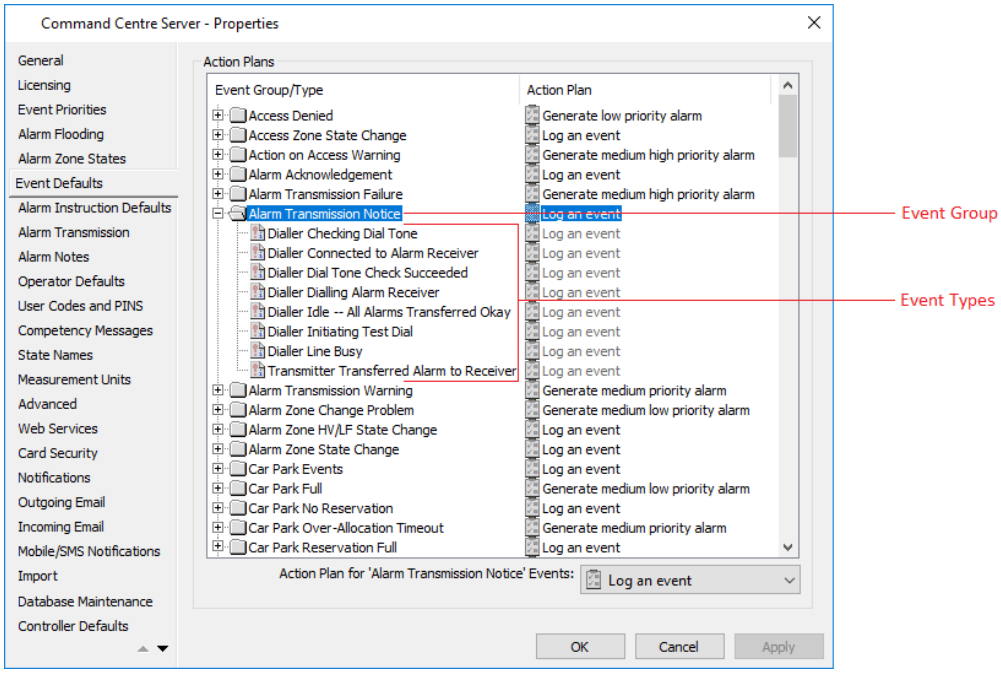
Site item events can be individually linked to Action Plans. These individual settings take priority over the site-wide default settings.

Site item events can also be set up to use the default Action Plan ("Use Default"). In this situation Command Centre references this Event defaults option and uses the Action Plan set here.

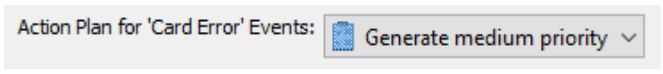
If an Action Plan is assigned to an Event Group, all Event Types in that group will default to the group Action Plan, unless overridden at the Event Type level within that group.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Event Defaults** tab. All available Event Groups are displayed.



3. Highlight the Event Group/Type you want to set the Action Plan.
The edit box is then enabled. This box displays the set Action Plan for the selected Event Group/Type.



Note: The default Action Plan for the 'Unit on Door Tampered' Event Type (under the 'Tamper' Group) is **Log an event**. Command Centre will display a 'Unit on Door Tampered' event whose source is a door, when an associated reader or door sensor goes into a tamper state.

This event can be configured as an alarm here instead so that these alarms will display elsewhere in Command Centre as being against the door, (e.g. if a site only has doors on their Site Plans they will show against the door. Note that if the associated reader or sensor is also on the Site Plan the alarm will show against them as well).

If your site only requires this functionality against specific door(s), this can be configured on the **Event Response** tab of the Door(s) concerned instead.

4. Click the drop-down menu list box to display the available Action Plans. Select the required Action Plan.
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.

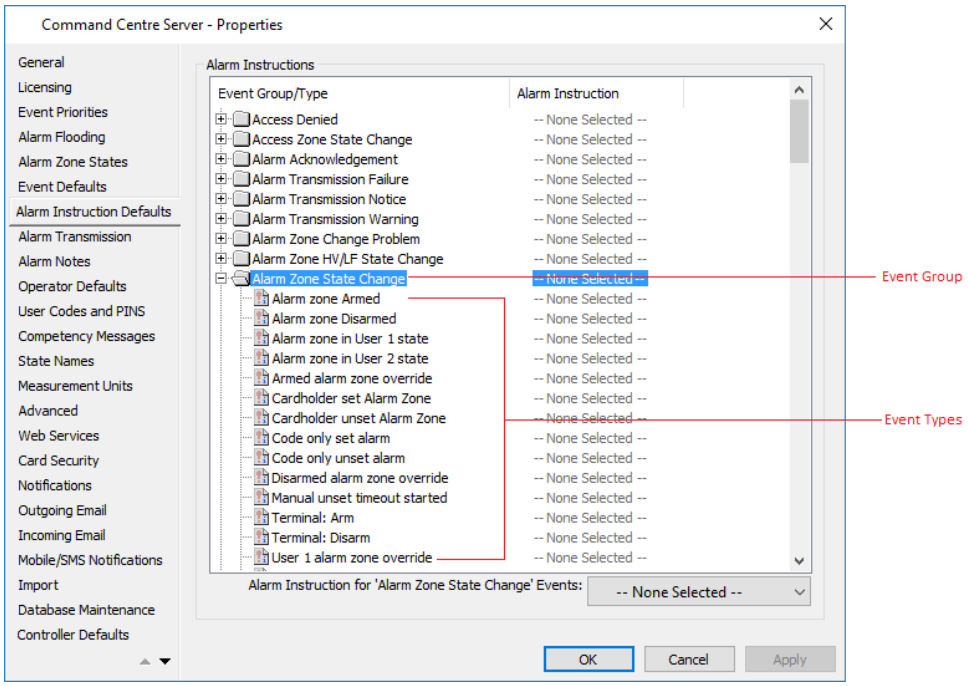
Alarm Instruction Defaults

Introduction

This tab enables you to assign Alarm Instructions to each of the Event Types and/or their Event Group. If an Alarm Instruction is assigned to an Event Group, all Event Types in that group will default to the group Alarm Instruction, unless overridden at the Event Type level within that group.
Note: These Alarm Instructions assignments can be overridden for individual items as required. See ***Alarm Instructions tab*** (on page 3-22) for further details.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Alarm Instruction Defaults** tab.



3. Highlight the Event Group/Type you wish to assign an Alarm Instruction to. The Edit box is enabled.
4. Click the drop-down menu box to display the available Alarm Instructions. (These Alarm Instructions are defined in the Alarm Instruction window.) Select the required Alarm Instruction.
5. Repeat Steps 3 - 4 as necessary.
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.

Note: If you change the assignment of alarm instructions for items already in alarm, they will not show the change of alarm instruction until the workstation is logged off and on again. Any new alarms that come in will however adopt the changes straight away.

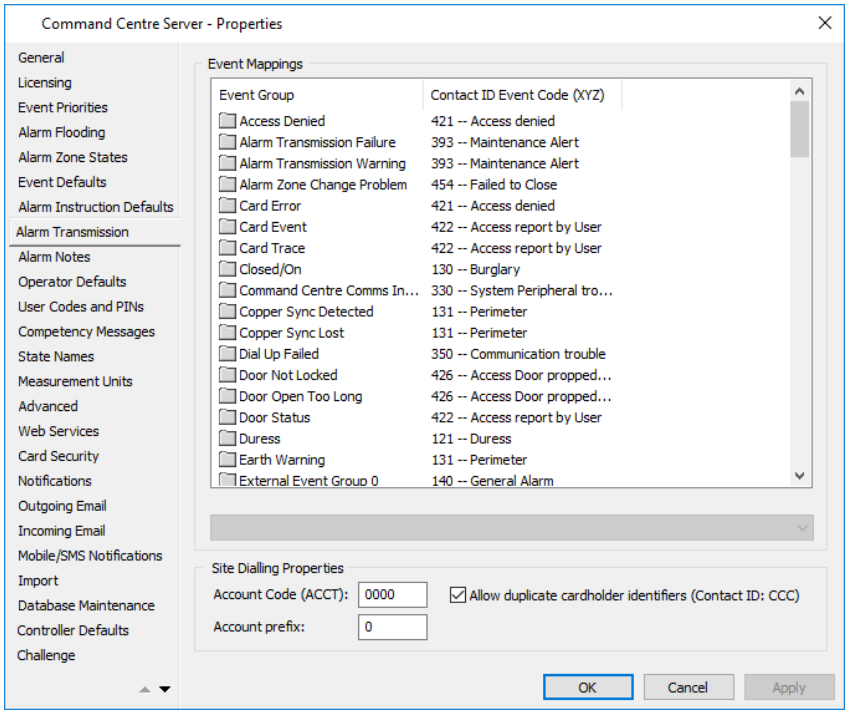
Alarm Transmission

Introduction

This tab enables you to assign the XYZ value of Contact ID Event Codes to Event Groups. See ***External Alarm Monitoring*** (on page 29-1) for an explanation of what Contact ID is, and for instructions on what else needs configuring for Contact ID.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Alarm Transmission** tab.



This tab displays the default event mappings of the XYZ Event Codes for Contact ID, (i.e. the Event Groups they are assigned to).

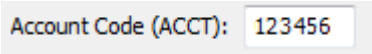
3. Change any of the event mappings if required by clicking on the Event Group concerned and then selecting the appropriate Contact ID code from the drop-down list.

IMPORTANT:
Although these default event mappings can be changed, it is recommended you leave them as the defaults. If you do change any, all the Event Types in a Group will also be affected. See XYZ Event Mappings for further details.

4. If you require a site wide account number to be used, enter either a four or six digit code in the **Account Code (ACCT)** field.
   - DC-09 protocol requires a 4 digit Account Code and CSV protocol requires a 4 OR 6 digit Account Code.
   - 0-9 and B-F are acceptable entries for the account code.
   - Leading zeros are acceptable.

   Notes:

   - If the Account Code is configured here, then all transmissions will use this account number unless it is overridden at Alarm Zone level.
   - Where DC-09 protocol is used for alarm transmission, the four least significant figures will be transmitted if the Account Code is longer than 4 digits, e.g.

     3456 would be used.

5. If you require user identifiers (CCCs) to be non-unique (so different Cardholders can have the same user identifier), select the **Allow duplicate cardholder identifiers (Contact ID: CCC)** checkbox.
   Notes:
   - To deselect this check box, you must first make all existing user identifiers (CCCs) unique. Existing duplicates will **not** be automatically made unique.
   - To manually make all user identifiers (CCCs) unique, perform the following:
     a) Create a Cardholder Report grouped by Contact ID to identify Cardholders that have the same user identifier (CCC).
     b) Manually find and amend all duplicate user identifiers (CCCs) so that they are unique.
     c) Deselect the **Allow duplicate cardholder identifiers (Contact ID: CCC)** checkbox so that no future duplicates are created.
6. The **Account prefix** is for third party Alarm Receivers that support utilising the DC-09 "Line Card" station identification.

   When set to any value other than "0", the Transmitter ID (configured on the **Alarm Receivers** tab of the Alarm Transmitter properties) in the message to the receiver is no longer used and will be replaced by a combination of the **Account prefix** and the **Account Code**. This allows for an expanded range of station identifiers to be provided.
   Notes:
   - This is global default, which can be overridden for individual Alarm Zones, via their **Alarm Transmission** properties tab.
   - When using the Gallagher Alarm Receiver the **Account prefix** must be 0.
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.

Alarm Notes

Introduction

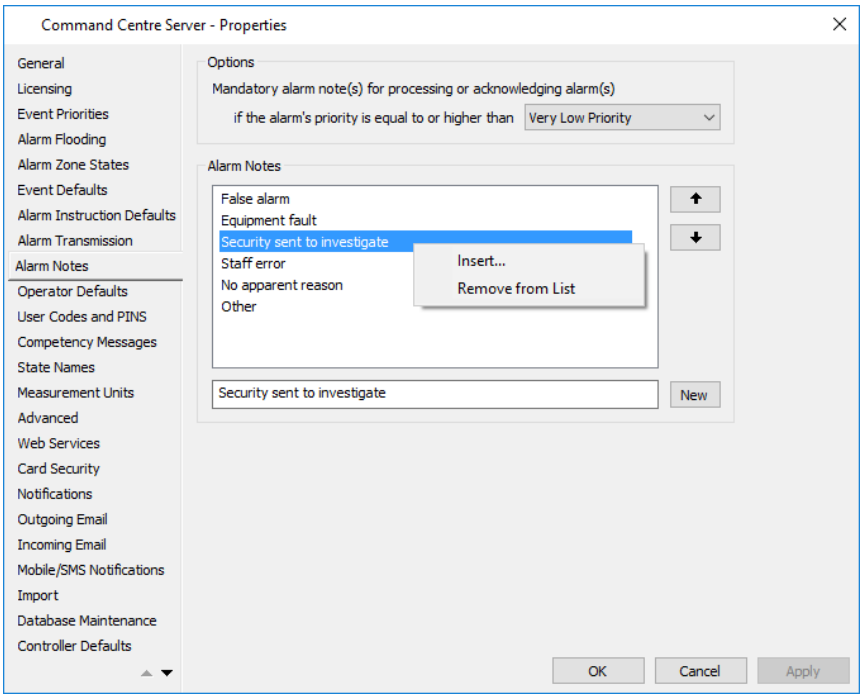
This tab enables operators with the “Edit Site” (or higher) operator privilege to configure mandatory alarm notes. All fields will be ‘read-only’ for operators with the “View Site” operator privilege.

The Alarm Notes are configured by default, and they are optional by default. If your site does not wish to use Alarm Notes they can all be removed from here.

Enabling alarm notes ensures that operators record notes against specific types of alarms before acknowledging, processing or quick processing them.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Alarm Notes** tab.



By default, the **Alarm Notes** listbox is populated with six pre-defined alarm notes.

Notes:

- When you select an alarm note from the **Alarm Notes** listbox, the selected text displays in the textbox below it (as shown in the above screen shot). If you change the textbox contents, the changes are immediately updated in the **Alarm Notes** listbox.

- For alarm notes that are too long to fit within the listbox, a tooltip displays when you move the mouse over them.

3. To add a new alarm note to the list, either:
   - **right click** anywhere within the **Alarm Notes** field, and select **Insert** from the context menu, or
   - click the **New** button.
4. To delete an alarm note, select the alarm note you want to delete, and either:
   - **right click** and select **Remove from list** from the context menu, or
   - press the <**Delete**> key on your keyboard.
5. Sort the **Alarm Notes** list if required.
   This is done by selecting an alarm note you want to move up or down the list, and clicking the appropriate **arrow** button to the right of the list box.
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.

Note:
At least two alarm notes are required in the Alarm Notes listbox, if one or more Operator Groups has a "Required alarm notes" option set on the **Configuration** tab (see Setting up Operator Groups), otherwise the following error message displays on saving the changes:
"At least two alarm notes required for Operator to acknowledge or process alarms."

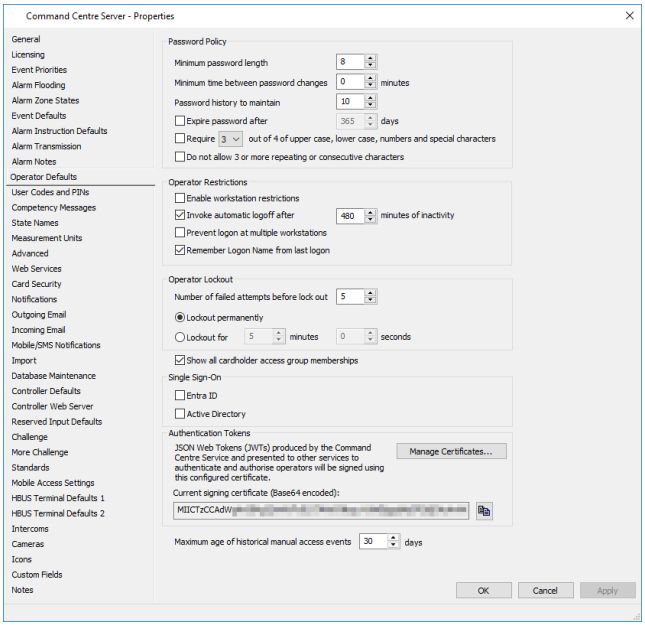
Operator Defaults

Introduction

This tab enables you to set some Password and/or Operator restrictions.
If your site is licensed for Active Directory Single Sign-on, the server connected to the workstation that an operator will be launching the application from has to be enabled for it. This is configured on this tab also.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Operator Defaults** tab.



3. Configure the **Password Policy** as required.

Field	Description
Minimum password length	This is the minimum number of characters allowed for passwords. (Default = 8. Range = 6 - 99) **Note:** On a clean install for sites with a NPSA license, the default value will be 9. If this is changed the new value will be retained after an upgrade.
Minimum time between password changes	This prevents users from changing passwords regularly. The default is set to '0'. This is the minimum time between password resets. This stops users from changing their passwords several times to wipe the history and get back to their old password if password history checks are made. (Default = 0. Range = 0 - 9999 minutes) **Note:** This applies to self-selecting passwords only.
Password history to maintain	A figure here indicates the number of successive password changes required before a password can be repeated. (Default = 10. Range = 0 - 999)
Expire password after	Checking this allows a number of days to be set for passwords to expire after. This forces users to change their passwords periodically. (Range = 0 - 365 days)

Field	Description
Require x out of 4 of upper case, lower case, numbers and special characters	Checking this option enforces passwords to use at least three or all four of the four available character types, (i.e. lower case letters, upper case letters, numbers and symbols), depending on whether you select **3** or **4** from the drop-down. **Notes:** • When this setting is selected, it will not be possible for passwords to be created that do not include upper case, lower case, a number and a special character. • When this change is applied, the enforcement takes place the next time the Operator changes their password.
Do not allow 3 or more repeating or consecutive characters	Checking this option enforces passwords to not contain 3 or more characters repeated in a row, or 3 or more consecutive characters, regardless of upper/lower case combinations, (e.g. "aaa", "1234abcd").

Note: It is possible to force a one-off change of password for an operator. This is achieved by checking the **Force password change at next logon** checkbox (on the **Operator Configuration** tab of cardholder properties), when you set up a cardholder as an operator. When the operator logs on to Command Centre for the first time the 'Change Password' dialog displays, forcing them to change their password.
Once the change has been forced, the **Force password change at next logon** checkbox will go back to being de-selected, unless either the **EN50131 Compliance** or **SSF1014 Compliance** checkbox is checked on the **Standards** tab of the Server Properties.

4. Click the appropriate checkbox(es) to configure the **Operator Restrictions**, as required.

Field	Description
Enable workstation restrictions	Check this if you want to restrict the Operator Groups on workstations, and to ensure that any new workstations must be created in the **Services & Workstations** List Window (via **Configure** from the main menu bar). Checking this results in an additional **Restrictions** tab displaying on the Workstation properties. See ***Creating a new Workstation Item*** (on page 28-2) for further details on what can be configured on this tab. **Note:** Client Authentication verifies that a workstation is what it claims to be, using a Client Certificate installed on the workstation machine. Enabling workstation restrictions here means that all workstations, except for the server workstation, need to be registered with a registration code. Refer to the "Client Authentication Appendix" in the *Command Centre Release Note* for further detail.
Invoke automatic logoff after	Checked by default. Checking this and specifying a time will mean users get logged off after that period of inactivity. (Default = 480 minutes. Range = 1 minute - 1440 minutes, i.e. 24 hours)

Field	Description
	Note: On a clean install for sites with a NPSA license, the default value will be 15 minutes. If this is changed the new value will be retained after an upgrade.
Prevent logon at multiple workstations	The system considers an operator with multiple sessions logged on from a single Windows session as using one workstation license. Checking the **Prevent logon at multiple workstations** checkbox (under "Operator Restrictions") prevents an operator from logging on from multiple Windows sessions.
Remember Logon Name from last logon	Checked by default. Each time this control is toggled off or on, operators will need to login one additional time before the change takes effect. When **selected**, the last operator **Logon Name** that logged into Command Centre will be displayed in both the Command Centre and Configuration clients Logon window, and the cursor focus will be on the **Password** field. When **unselected**, the **Logon Name** will be blank in both the Command Centre and Configuration clients Logon window, and the cursor focus will be on the **Logon Name** field.

5. Configure **Operator Lockout** as required:
   a) Specify the number of continual failed attempts before lockout action will occur, in the **Number of failed attempts before lock out** field. (Default = 5. Range = 1 - 20)
   b) Click the appropriate radio button to indicate how long the operator will be locked out after that configured number of failed attempts.

Radio button	This option locks an operator account...
Lockout permanently	immediately (permanently) after the configured number of failed attempts. The account will require a privileged operator to unlock user account. This is the default lockout setting.
Lockout for <specified time>	for a specified period of time, i.e. silently delay (without feedback to the operator) the ability to logon after the configured number of failed attempts. Subsequent failed logon attempts will invoke the same period of time. (Default = 5 minutes. Range = 20 seconds - 60 minutes and 59 seconds)

6. Configure the **Single Sign-on** options as required:

Field	Description
Entra ID	This checkbox only appears if your site is licensed for Entra ID Single Sign-on. If enabled, when an operator launches Command Centre Client on a workstation connected to this server, the system checks if they can be logged on using Entra ID Single Sign-on. Entra ID Single Sign-on is not used for Configuration Client. Operators must be assigned a User ID to use Entra ID Single Sign-on. Refer to ***Linking operators to their Entra ID account*** (on page 72-5)for details.
Active Directory	This checkbox only appears if your site is licensed for Active Directory Single Sign-on. If enabled, when an operator launches either Configuration Client or Command Centre Client on a workstation

Field	Description
	connected to this server, the system checks if they can be logged on using Active Directory Single Sign-on. Operators must be assigned a Windows logon to use Active Directory Single Sign-on. Refer to ***Linking operators to their Active Directory account*** (on page 57-3) for details.

7. Enable/disable the **Show all cardholder access group memberships** checkbox as required.

When…	an operator…
checked,	can see ALL Access Groups assigned to a cardholder as long as the operator can see the cardholder.
unchecked,	can only see the Access Groups associated with the cardholder when they have "Modify Access Control", "Edit Access Groups" or "View Access Groups" privilege in the division of the Access Group. **Note:** Before turning off 'Show all Cardholder access group memberships' it is important to ensure that the site has accurately configured all the Access Groups, Operators Groups, Cardholders memberships with the correct divisions and privileges.

8. The **Authentication Tokens** certificate is used to sign JSON Web Tokens, for services that require operators to be authenticated and authorised using a token. Services that require these tokens are generally optional or licensed, so this certificate may or may not be used for your site.
   If you wish to change this certificate, click the Manage Certificates button and select the required option:

Mode	Description
Default Internal Certificate	The Default Internal Certificate is a self-signed certificate which is generated by Command Centre and stored in the database. It exists to provide a standard option for sites that don't need a custom certificate. The private key is protected by Command Centre's Database Encryption
Custom Certificate	This lets you import your own ECDsa P384 certificate as a PFX or P12 file. The private key will be protected by Command Centre's Database Encryption.
External Certificate	An "External" certificate is loaded from the Windows certificate store rather than Command Centre's database. This option requires that you add an ECDsa P384 certificate with a Friendly Name of 'Gallagher Command Centre Token Signer' to Gallagher Applications\Certificates in the Local Machine certificate store.

9. In the **Maximum age of historical manual access events** field, enter the maximum number of days in the past a manual access event can be, when it is created. This affects what date and time an operator can select when creating a manual access event from a Cardholder Viewer.
   This setting does not delete or affect manual access events that have already been created. For more information, refer to the “Creating manual access events for Cardholders” topic in the *Gallagher Command Centre Online Help.*
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.

User Codes and PINs

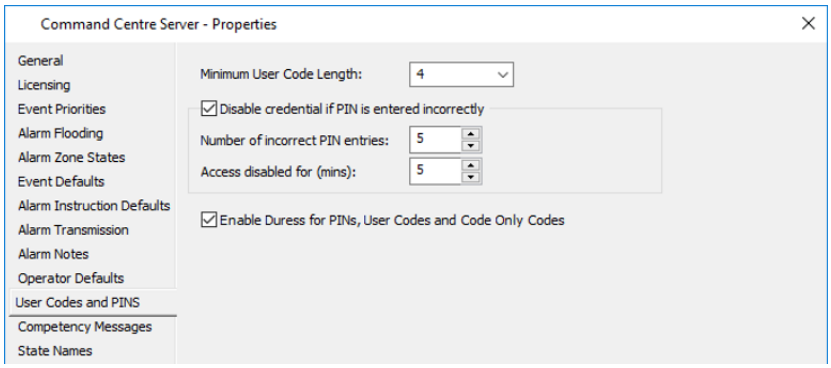
Introduction

This tab allows a site to:

- set the minimum length of User Codes for your site. Cardholders can be assigned User Codes for logging on to Remote Arming Terminals with no associated readers. User Codes can be 4-8 digits in length.
  Note: User Codes can also be used as PINs for any reader with a keypad. This is set via a checkbox on the **Connections** tab of the reader properties.
- disable a card or credential when a PIN has been entered incorrectly at a T2x reader too many times.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **User Codes and PINs** tab.



3. Select the minimum number of digits you require for your sites user codes from the drop-down list.
4. If you require credentials to be disabled when a PIN is entered incorrectly at a T2x reader too many times, ensure the **Disabled credential if PIN is entered incorrectly** checkbox remains checked and enter the appropriate **Number of incorrect PIN entries** allowed and how many minutes **Access disabled for**. **Notes:**
   - This feature also locks out a user if their 'User Code is used as a PIN' and they enter it incorrectly for access.
   - On a clean install for sites with a NPSA license, the default values are: **Number of incorrect PIN entries** = 3, **Access disabled for (mins)** = 15 Any changes made to these default values will be retained after an upgrade.
5. The Enable **Duress for PINs, User Codes and Code Only Codes** checkbox is ticked by default.
   When unticked, system access will not be allowed and Duress Alarms will not be generated upon entering Duress PIN/User Code/Code Only Codes.
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.

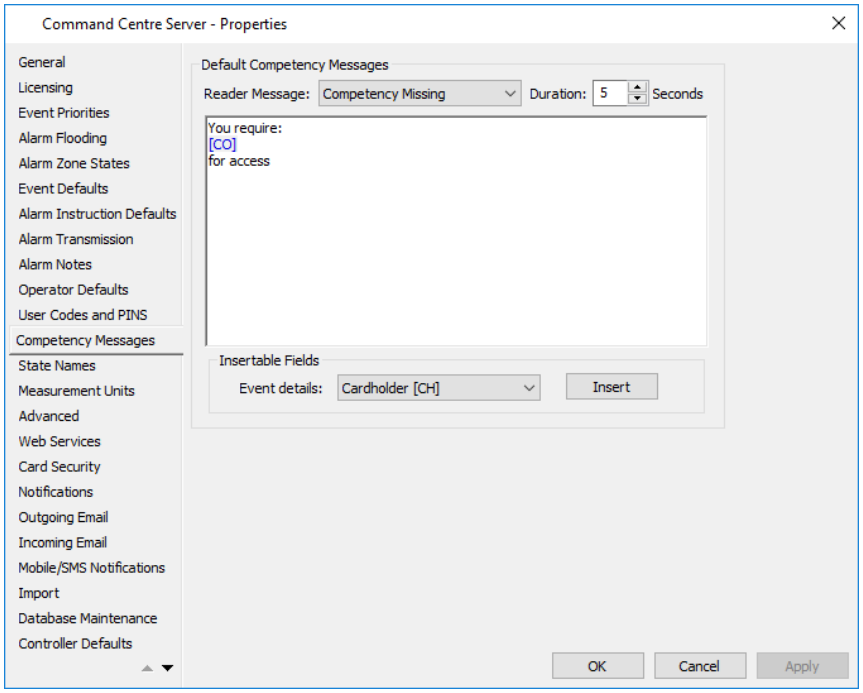
Competency Messages

Introduction

Cardholder Competencies, which is a licensable feature of Command Centre, allows sites to block access to certain zones for Cardholders who lack some certification, or whose certification has expired. This tab, which is only visible if your site is licensed for the Cardholder Competencies feature, allows you to modify the system-wide default messages for competencies.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Competency Messages** tab.



This screen allows you to specify the default competency messages for each 'Message display device' that is required to show these messages. 'Message displays devices' are:

- HBUS Terminal, or
- a secondary display device 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

Note: When a competency is created, the competency's messages are set to the system-wide defaults configured here, however you can alter the messages for each competency.

3. 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
4. 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 string 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.
     - Gallagher Remote Arming Terminals = 5 rows of approximately 20 characters per row (variable width fonts used)
   - 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.
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.

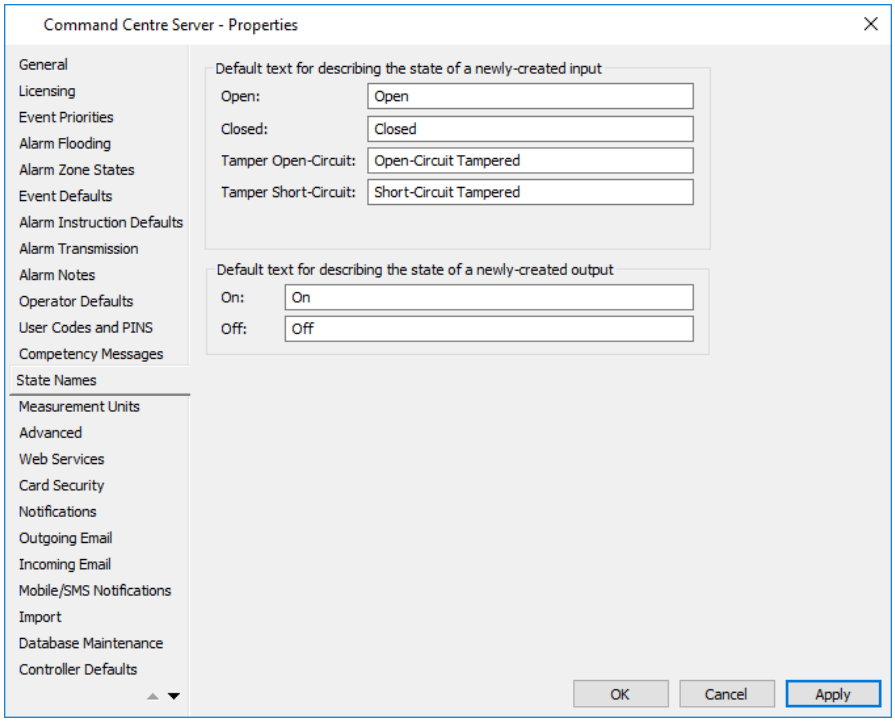
State Names

Introduction

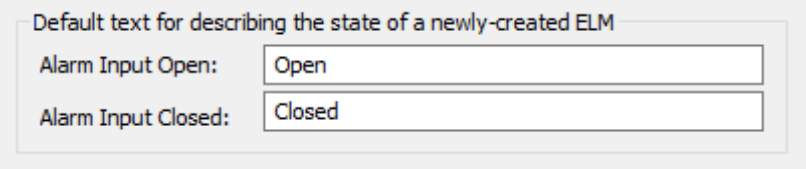
The State Names tab enables you to set the text to display within alarm and event messages when the inputs and outputs are activated.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **State Names** tab.



3. Type in the **preferred text** (if different from the default), to be displayed throughout the Command Centre system when newly created **inputs** are activated and deactivated.
4. If your site is licensed for Class 5 End-of-Line Modules (ELMs), there will be an additional section on this screen, as shown:



Type in the preferred text (if different from the default), to be displayed throughout the Command Centre system when newly created ELMs are activated and deactivated.

5. Type in the **preferred text** (if different from the default), to be displayed throughout the Command Centre system when newly created **outputs** are activated and deactivated.
   Note: Any inputs, outputs and ELMs already created prior to changes being made on this tab will continue to use the old defaults.
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.

Measurement Units

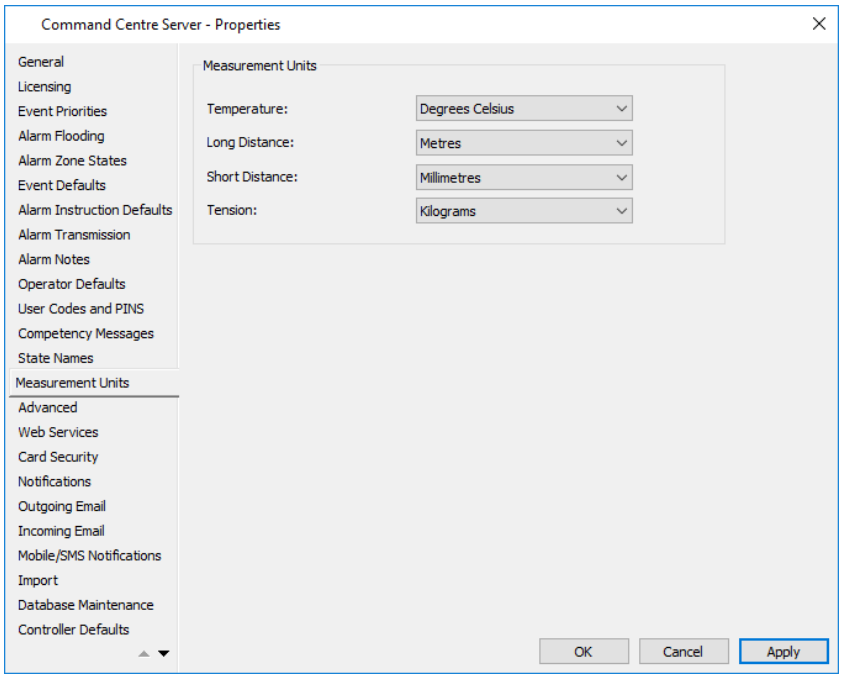
Introduction

This tab allows a site to select their preferred measurement units for Gallagher Security Electric Fence Controllers and Taut Wire Sensor properties. The selected units are displayed on:

- Fence Controller and Fence Zone property pages,
- Voltage and Temperature Reports, and
- Taut Wire Sensor property pages.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Measurement Units** tab.



The default values in installation are displayed in the above screenshot. The values available in the drop-down lists are:
Temperature: "Degrees Celsius" or "Degrees Fahrenheit"
Long Distance: "Metres" or "Feet"
Short Distance: "Millimetres" or "Inches"
Tension: "Kilograms" or "Pounds"

The selected **Temperature** Unit is applied to the following settings of the F31, F32, F41, F42 and F22 Fence Controllers:

- "High Temperature Output Threshold" settings (including operator modified event and Site Configuration Report)

- "Temperature Data Logging" settings (including operator modified event and Site Configuration Report)

3. Configure the settings on this screen as required.
4. 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.

Advanced

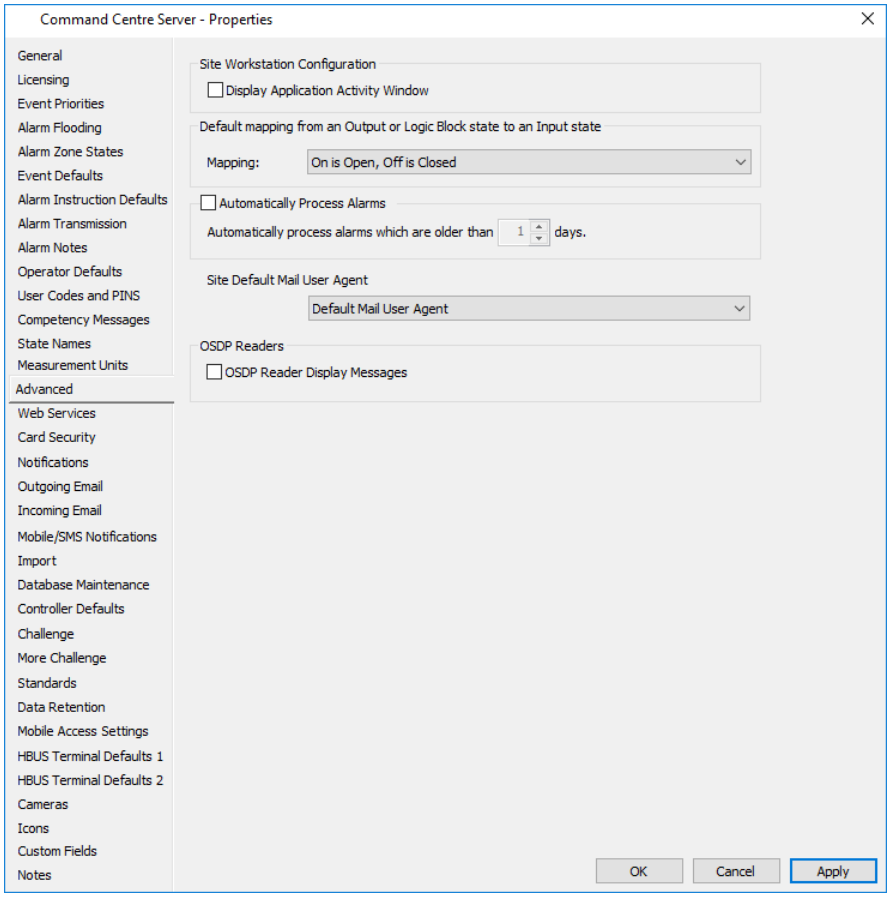
Introduction

The Advanced tab enables you to:

- enable/disable the Activity Indicator .
  If enabled, the Activity Indicator is always visible while Command Centre is running and responding, and provides operators with confirmation that the Command Centre application has not ceased operation.
- set the default mapping when a Logic Block or Output is used as an Input.
- have old inactive alarms automatically processed by the system. The purpose of this functionality is to clear the alarm buffer regularly for sites that do not manage alarms via Command Centre.
- change the password for the controller diagnostic web interface.

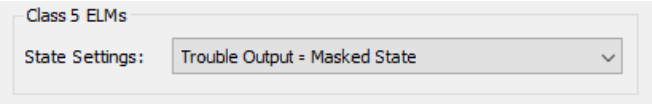
Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Advanced** tab.



3. Check the **Display Application Activity Window** checkbox if you want the Activity Indicator to display while Command Centre is running.
4. From the **Mapping** drop-down list, select the default state translation to be used when a Logic Block, Output or Virtual Output is used in place of an Input.

5. Check the **Automatically Process Alarms** checkbox if you want the system to automatically process old inactive alarms, and indicate the time period to keep inactive alarms before they are auto-processed. By default, all inactive alarms older than a day (24 hours) will be processed. (Range = 1 - 999 days)
   Notes:
   - The minimum period that an alarm must exist before it can be auto-processed is 1 day.
   - The event history of each auto-processed alarm will be updated with the time of processing and a statement that it was auto-processed. Each daily auto-processing run will log a start and completion event.
6. The **Site Default Mail User Agent** is for use when generating Visitor Management Email Invitations sent through Notifications.
   Select the appropriate Site Default Mail User Agent from the drop-down list if required.
7. If your site is licensed to create Gallagher Class 5 End-of-Line Modules (ELMs), an additional **Class 5 ELMs** section will be visible on this tab.

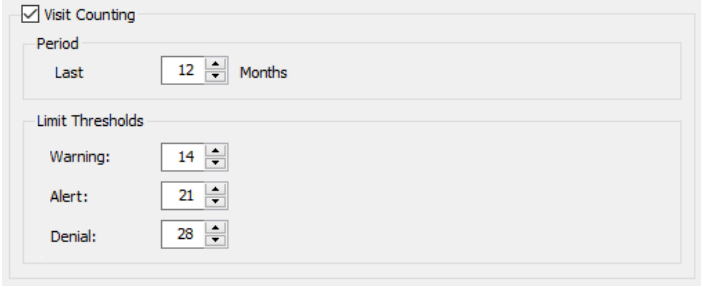


   Select the required global state for Class 5 ELMs from the **State Settings** drop-down list. The options are:

Option	Description
Trouble Output = Masked State	This option indicates the Masked state, and is the default setting.
Trouble + Alarm Outputs = Masked State; Trouble Output = Fault State	Selecting this option means that trouble and alarm means Masked, and trouble alone indicates Fault.

   Note: Individual ELMs can be configured differently. See ***Configuring a Class 5 ELM*** (on page 62-2) for further detail.

8. If you want OSDP and Morpho Biometric Readers to display access & status messages on their screens (if they have screens) by default, then select the **OSDP Reader Display Messages** checkbox. Otherwise, deselect it.
   This setting defines what an OSDP or Morpho Biometric Reader does when it has the 'Use site default settings' checkbox selected on its **Advanced** (OSDP) or **Advanced Settings** (Morpho Biometric) tab.
9. The **Visit Counting** section displays and the fields are enabled if your site is licensed for the 'Visit Count' feature.



On a new installation, the Visit Counting fields will be populated with default values. On an upgrade, the visit count will be pre-populated if previously made visits are within the configurable period.

This feature is only editable for operators with the 'Edit Site' privilege or higher.

Field	Description
Period	The Period length is configurable. A warning message displays when 0 is entered. (Default = 12 months. Range = 1-999).
Warning	A warning message displays in Visitor Management when the number of visits by a visitor (in the **Period** specified) are greater than or equal to the **Alert** or **Denial** Threshold. (Default = 14 visits)
Alert	A warning message displays in Visitor Management when the number of visits by a visitor (in the **Period** specified) are greater than or equal to the **Denial** Threshold. (Default = 21 visits)
Denial	A warning message displays in Visitor Management when the number of visits by a visitor (in the **Period** specified) has met the **Denial** Threshold. (Default = 28 visits)

Note: Thresholds can be configured 'off' by setting values to '0', however at least one threshold must be configured.

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.

Web Services

Introduction

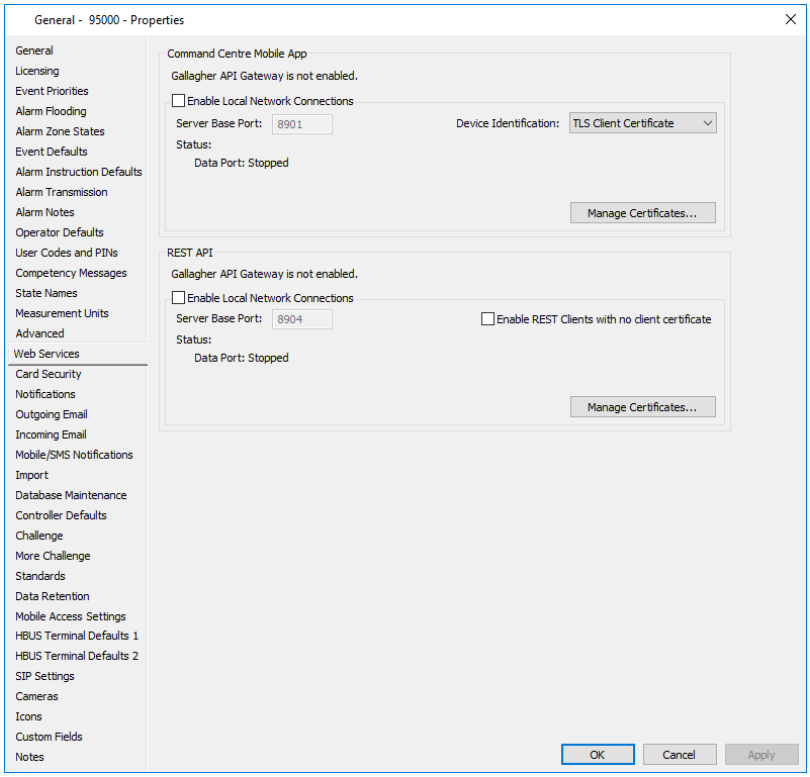
The Web Services tab allows you to replace the web service certificate with an alternate certificate, when using the Mobile Client, and configure the server base port for the REST API.

REST is short for REpresentational State Transfer. It is a resource-based API that allows developers to perform requests and receive responses via HTTP protocol. REST API requires the following licence strings to be able to use it:

- `RESTEvents=1`
- `RESTCardholders=1`
- `RESTOverrides=1`
- `RESTStatus=1`
- `RESTCreateEvents=1`

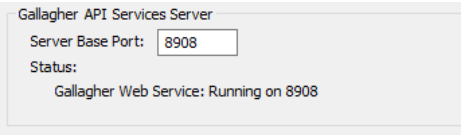
Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Web Services** tab.

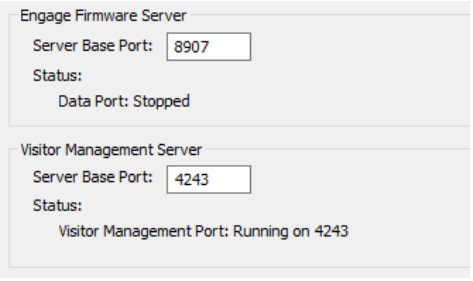


3. If you wish to change the **Command Centre Mobile App** certificate:
   a) Tick the **Enable Local Network Connections** checkbox,
   b) Change the port in the **Server Base Port** field, then
   c) Select the appropriate **Device Identification** from the drop-down.
   Refer to ***Changing the Web Services*** (on page 6-34) for further instructions.
4. If **REST API** is required, tick the **Enable Local Network Connections** checkbox.

5. Change the **Server Base Port** if required.
   Note (if changing the port): You will also need to reconfigure the SSL certificate. Refer to ***Changing the Web Services*** (on page 6-34) for further instructions.
   IMPORTANT: If the **Enable REST Clients with no client certificate** checkbox is unchecked (default), REST API items **must** have a Client Certificate Thumbprint assigned to them to work. Gallagher STRONGLY recommends leaving it unchecked, as requiring client certificates greatly increases security.
   If this checkbox is checked, REST Client items do not need a Client Certificate Thumbprint assigned to them, but they may have one. If they do have one, it must be valid.
   Whether this checkbox is checked or not, any certificate thumbprint entered in a REST Client item's **Client Certificate Thumbprint** field must match the client certificate (must be valid).
   The 'Status' section updates to show the REST start-up state, (e.g. running, failed to start), and any relevant error information.
6. The 'Gallagher API Services Server' settings are enabled if your site is licensed for the ***Gallagher SIP Integration*** (on page 67-1).



   Change the Gallagher API Services Server **Server Base Port** if required. This is the port used by the Gallagher SIP Endpoint Service to communicate with the Command Centre Server. The port you set here must match the port you specify in the ***Gallagher SIP Setup Utility*** (on page 67-3). Default is 8908.
7. If you have enabled the REST API port by completing Steps 4 and 5, you also need to create a REST Client item. See ***Creating a REST API Client item*** (on page 28-13) for further detail.
8. The 'Engage Firmware Server' and 'Visitor Management Server' settings are enabled if your site is licensed for either of these.



   Change the Server Base Port for either of these if required.
   See ***Visitor Management Application Installation Instructions*** (on page 50-3) for further detail.
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.

Changing the Web Services

This topic describes how you can replace the default Mobile Client and REST API web service TLS certificate with an alternative certificate, and how to update the certificate settings if the web service ports are altered.

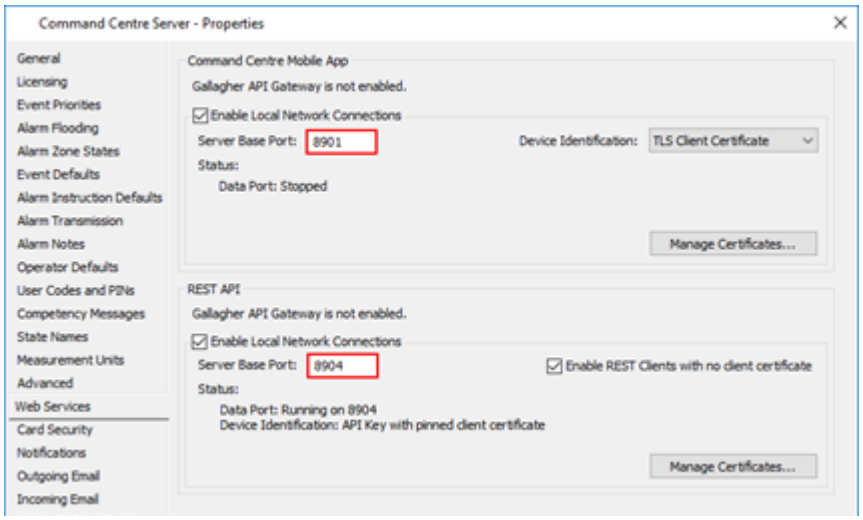
- Replacing the web service certificate does not increase the security of the solution. Typically, this is done to satisfy corporate policy.
- Altering the ports is only required to avoid collisions with other third-party software, or to satisfy corporate policy.

Select the item below that you require further detail on:

- ***Changing the TCP ports that the web service listens on*** (next)
- ***Replacing the web service certificate with an alternative certificate*** (on page 6-35)

Changing the TCP ports that the web service listens on

1. Open the **Web Services** tab of the Server Properties in the Configuration Client, and enter the new data port numbers in the **Server Base Port** fields as appropriate.

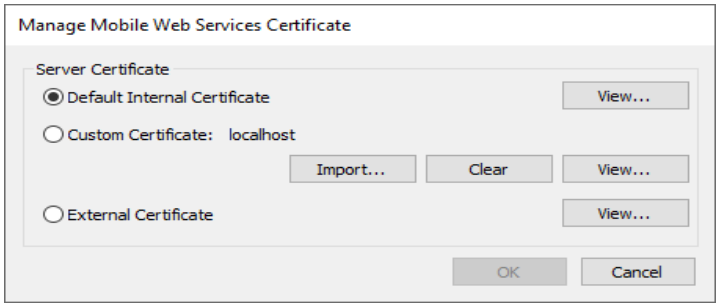


Note: For Mobile Client, the web service data port is the one you specify here. The enrolment port is always that port plus one.

2. Click **Apply**.
   You should see the status update to reflect the port change. No further steps should be required in Command Centre, although it is likely you will need to reconfigure Windows Firewall, or any other third-party Firewall software, to allow the new ports.

Replacing the web service certificate with an alternative certificate

1. Open the **Web Services** tab of the Server Properties within the Configuration Client.
2. Click the **Manage Certificates** button for either the Mobile Web Service or REST API. The Manage Mobile Web Services Certificate dialog displays.



3. Select **Custom Certificate** and click **Import...**
   Note: See below for an explanation of the three certificate modes that are available on this dialog.
4. Use the file browser to find your PFX or P12 file containing the certificate and its associated private key, and then when prompted enter the password.
   Note: If you do not have a certificate in a PFX/P12 file, and instead have two separate files for the certificate and private key, you will need to convert them to a PFX/P12 file first. This can be easily done using OpenSSL or other tooling.
5. Click the **OK** button. The Manage Mobile Web Services Certificate dialog closes.

   IMPORTANT: The new certificate will not be saved to the database and will not take effect until you click the **Apply** button on the main **Web Services** tab, so it is likely you will wish to do this too.

Note: If you have existing devices running the Command Centre Mobile App, they will see the certificate change as a potential malicious attack and block connections to the server. You must re-enrol them. This does not affect the Mobile Connect App or Mobile Credentials.

Certificate Mode explanations

Mode	Explanation
Default Internal Certificate	The Default Internal Certificate is a self-signed certificate which is generated by Command Centre and stored in the database. It exists to provide a standard option for sites that don't need a custom certificate. The private key is protected by Command Centre's Database Encryption.
Custom Certificate	This lets you import your own certificate as per the instructions above. The private key will be protected by Command Centre's Database Encryption.
External Certificate	An "External" certificate is loaded from the Windows certificate store rather than Command Centre's database. **Note:** If both the Mobile Client and REST API features are set to the "External" mode, then there is only one single external certificate which will be shared, but in either of the other modes they have distinct certificates.

Card Security

Introduction

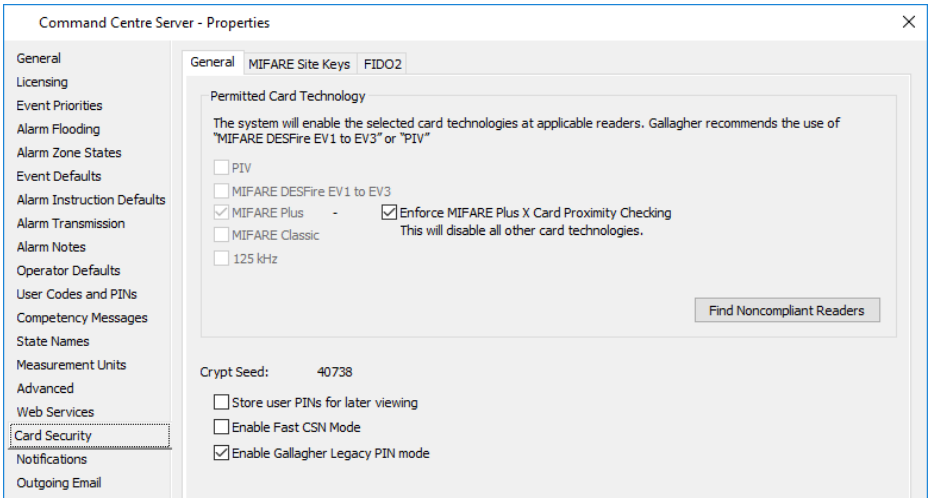
MIFARE® high security cards, (i.e. MIFARE Plus® and MIFARE® DESFire® EV1 to EV3 are currently the only MIFARE high security cards supported), which are a replacement for the MIFARE (classic) card, feature multiple certified security levels, including Advanced Encryption Standard (AES) encryption.
Note: Command Centre only encodes MIFARE Plus cards to Security Level 3.

This tab enables you to set the site security information, as follows:

- site security information for encoding MIFARE high security cards,
- the MIFARE Enhanced Security feature which ensures MIFARE readers are able to prevent access through the use of replicated cards,
- MIFARE Plus/DESFire encoding information,
- configure readers to accept Admin cards,
- set the card technologies permitted on site,
- PIN settings for user PINs. The **Crypt Seed** number is used for PIN numbers, and is supplied by the Gallagher Group Limited, and
- enable a fast scan mode for Card Serial Number (CSN) on TSeries readers

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Card Security** tab.
   The **General** sub-tab displays by default.



3. Perform the required function(s):

Setting permitted card technologies

In the Permitted Card Technology section, by default **MIFARE DESFire EV1 to EV3** is selected, and **PIV** for sites with a PIV license.
Important: Gallagher recommends the use of MIFARE DESFire EV1 to EV3 or PIV card technologies. Some of the other options have known security vulnerabilities.

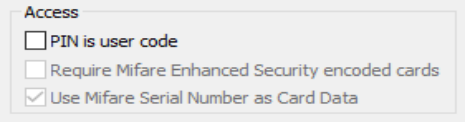
1. If you require other card types to be accepted at readers, select the appropriate checkboxes.

2. If your site is using MIFARE Plus cards with the 'X' feature set and you wish to prevent relay attacks occurring over HBUS, check the **MIFARE Plus** checkbox to enable **Enforce MIFARE Plus X Card Proximity Checking** checkbox.
3. Check the **Enforce MIFARE Plus X Card Proximity Checking** checkbox. The terminal will perform proximity checks when reading a MIFARE Plus X card.
   Notes:
   - Checking this option disables all other card technologies.
   - The MIFARE Plus X Card Proximity Checking feature will only work if the site that issued the card is using the same MIFARE Plus/DESFire key seed as your site.
   - Operators need "Edit Site" privilege to be able to amend this setting.
4. Click the **Find Noncompliant Readers** button to locate any readers that differ from your settings. The Find tool displays listing applicable readers.

Note: 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.

PIN Settings

1. Check the **Store user PINs for later viewing** checkbox.
   Checking this option means that user PINs will be encrypted and stored so that operators with the "View PIN's" operator privilege will be able to later decrypt and display them, if necessary. See "View PINs" operator privilege for further detail describing the criteria for viewing PINs.
   Note: If a number already populates the **Crypt seed** field, this means that it was configured in your license file when Command Centre was installed.
   CAUTION: You can change the 5-digit Crypt Seed, however new PINs will have to be issued to every authorised cardholder.
2. Do you require a fast scan mode for CSN on TSeries readers, so that if no Gallagher data is found on a card, the reader will immediately read the CSN rather than reading every sector on the card?
   Note: This feature does not apply to TSeries readers connected as Cardax IV.

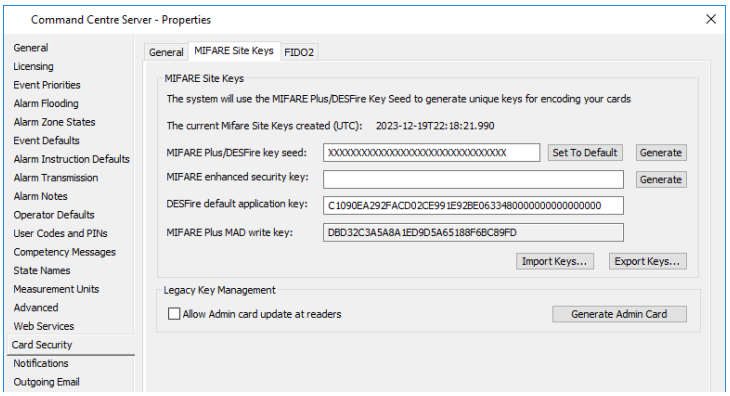
If…	then…
no,	Go to Step 3.
yes,	check the **Enable Fast CSN mode** checkbox. Checking this results in the following on the **Advanced** tab for all TSeries Readers: - the **Require MIFARE Enhanced Security encoded cards** and **Use MIFARE Serial Number as Card Data** options will be disabled, and - **Use MIFARE Serial Number as Card Data** will be checked  If **Require MIFARE Enhanced Security encoded cards** was previously checked, it will now be unchecked. If **Enable fast CSN mode** is unchecked again on the server settings, those fields on the readers will no longer be disabled, and the setting on the readers will return to their earlier state. Note: The reader firmware must be updated, via vGR7.90.104 (or later) in order for the feature to work.

Disabling Legacy PINs

By default, the **Enable Gallagher Legacy PIN mode** checkbox is enabled on an upgrade. For clean Installs, or sites upgrading with a NPSA license, the checkbox is disabled. If a Card Type has PINs enabled and a card of that type is not assigned a PIN, a PIN is calculated for it based on the Crypt Seed in the database, and that Card Number which can be seen using the **View PIN** button in both Command Centre and Configuration Client.

On a controller when a card is badged, and a PIN is required, if the card doesn't have a PIN this legacy mode is utilised and any PIN entered is checked against calculated PIN.

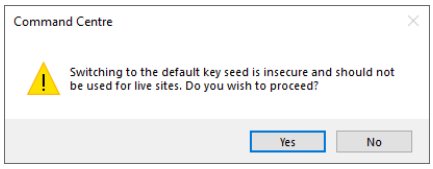
4. Click the **MIFARE Site Keys** sub-tab.



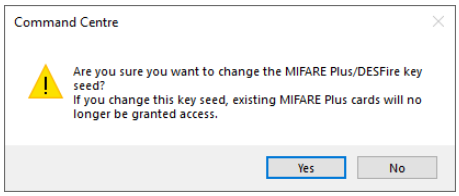
5. Perform the required function(s):

Generate a custom key seed or import a key

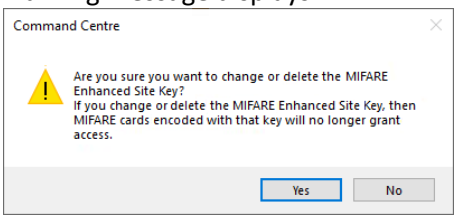
1. Do you want to use a default MIFARE Plus/DESFire key seed for encoding MIFARE high security cards?
   Note: See ***MIFARE DESFire Key Migration*** (on page 6-43) for the full procedure on migrating away from using the default MIFARE® key seed on DESFire® cards, to using a unique MIFARE® key seed.

If...	then...
yes,	click the **Set To Default** button. The following warning displays:  Click the **Yes** button.
no,	populate the **MIFARE Plus/DESFire key seed** field with a 32 hexadecimal character string and click the **Apply** button to save the key. **Note:** 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. When the **Apply** button is clicked, the 32 characters are converted to 32 X's, (i.e. the key is hidden).

2. The MIFARE Plus/DESFire key seed is updated, as indicated by the message that displays in the lower part of the screen.
3. The MIFARE DESFire card key migration window by default will be for a period of one month from today's date. Change the end date if required.
4. What readers do you want to use for migration?

If…	then…
All Readers,	click the **All Readers** radio button.
Selected Readers,	1. Click the **Selected Readers** radio button. 2. Drag and drop the readers you want into the grid. If you click **Apply** now, a warning message displays:  See ***MIFARE DESFire Key Migration*** (on page 6-43) for the full procedure on migrating away from using the default MIFARE® key seed on DESFire® cards, to using a unique MIFARE® key seed.

5. Do you want to encode MIFARE cards with the MIFARE Enhanced Security feature?

If…	then…
no,	go to Step 6.
yes,	1. Populate the **MIFARE enhanced security key** field with a 32 hexa- decimal character string and click the **Apply** button to save the key. **Note:** 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. When the **Apply** button is clicked, the 32 characters are converted to 32 X's, (i.e. the key is hidden). The following warning message displays:  2. Click **Yes** to go to Step 6.

6. The DESFire Default Application Key field is editable and can be imported and exported (including for bureau encoding) using the **Import Keys…** and **Export Keys…** buttons as appropriate.
   On upgrade to a version that supports key migration, (i.e. v8.30 onwards), the MIFARE DESFire Default Application Key is set to a value derived from the MIFARE Plus/DESFire key seed. If a key file from a pre-8.30 version of Command Centre is imported into a version v8.30 or later, the Default Application Key is overwritten with one that is derived from the MIFARE Plus/DESFire key seed.
   Note: The **MIFARE Plus MAD write key** read-only field displays a 32 hexa-decimal character key that allows third parties or other Gallagher sites to re-encode and update the MAD for MIFARE Plus cards issued by this site. It will change whenever the key is changed.

Export MIFARE keys

1. Click the **Export Keys…** button. A 'Please choose a password' dialog displays.
2. Enter a password. **Note:** The password must be at least eight characters long, and can be a maximum of 32 characters.
3. Click the **OK** button.

4. Click the **OK** button.
   A 'Save As' dialog displays with a default filename **MifareKeys.txt**
5. Change the default filename if required, and path your way to the location where you want to save the Site Key file.
6. Click the **Save** button. The message *"Key successfully exported and protected by your password"* displays.
   A "[SiteSerial]" section will also be created in the file under [MifareSiteKey] section including three fields: 1)Serial 2)Encryption and 3)KeyDerivation. Serial number is encrypted to a random hex string 32 characters long in the same way MIFARE Plus/DESFire key seed does so that it can be verified which particular site the exported file belongs to.

Import MIFARE keys

1. Click the **Import Keys…** button.
2. Path your way to the location where the MIFARE key file you want to import is located and click on the MIFARE key file you want to import.
3. Click the **Open** button. An 'Enter password' dialog displays.
4. Enter the correct password for the selected MIFARE key file (this password will need to be supplied by the site that exported the MIFARE key).
5. Click the **OK** button. The MIFARE Plus/DESFire key seed field displays the text 'XXXXXXXXX IMPORTED KEY XXXXXXXXX' to confirm the key has been imported successfully.
   Note: Keys exported by earlier versions than vEL8.00 of Command Centre cannot be imported.
6. Click the **Apply** button to save the new key.

Encode an Admin card

An Admin card is required if the site needs to update T series readers with the MIFARE key and/or needs to load a list of Facility Codes on a T series reader to support multiple applications. See the **Sharing MIFARE Classic and Plus cards between sites.pdf** document located in the `'Documentation'` directory of the Command Centre installation files for more information regarding multiple apps. The **Allow Admin card update at readers** checkbox allows you to put T series readers into a mode that will allow the MIFARE key or facility code list of the reader to be changed via an Admin card. This checkbox should be disabled after all the sites T series readers MIFARE key or facility code list have been updated with an Admin card.
Note: An Admin card should only be presented at a T series reader configured for Cardax IV.

1. Do you want to encode an Admin card to update readers MIFARE key and/or facility code list?

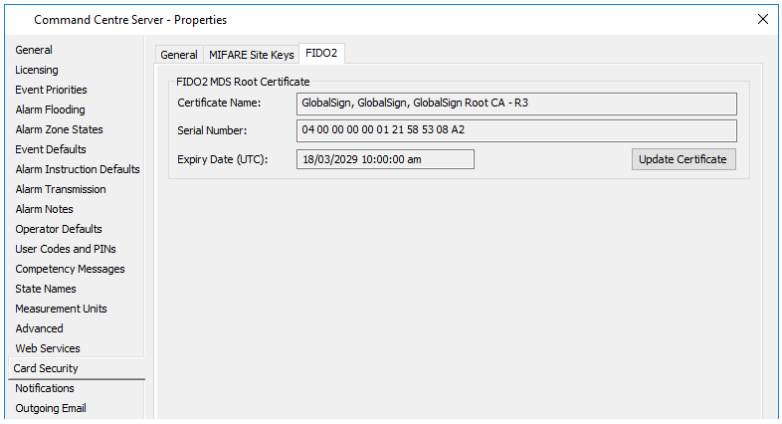
If…	then…
no,	go to Step 4.
yes,	a) Check the **Allow Admin Card update at readers** checkbox. b) Click the **Generate Admin Card** button. The 'Generate Reader Configuration Card' dialog displays. c) Select the appropriate encoder from the Encoder drop-down list, (i.e. either *SCM Microsystems Inc. SDI010 Contactless Reader 0* or *SCM Microsystems Inc. SDI011G Contactless Reader 0*).

If...	then...
	The **Encode Card** button becomes enabled. **Note:** If no USB Encoder is attached to the workstation, the message *"No USB Encoder was detected"* appears in the Status bar.

d) Check the **Update facility code list** checkbox (depending on whether you want key change only, facility code list only, or key change and facility code list).

e) Click the **Encode Card** button to encode a MIFARE Plus or MIFARE DESFire EV1 to EV3 card, and encode the MIFARE key seed to it, which when presented at a T series reader (when **Allow Admin card update at readers** is checked), will update the MIFARE key on the reader.
IMPORTANT: Should you need to return T series Cardax IV connected readers to the factory default settings, this can be done by clicking the **Reset to Factory Defaults** button (on the **Status and Overrides** tab) for each individual reader. An event will be generated stating who returned the readers to the factory default settings. The **Reset to Factory Defaults** button only appears for users with the "Maintenance Override" operator privilege, and either the "Edit Site" or "View Site" operator privilege.
Note: You should NOT re-encode Admin cards.

6. Click the **FIDO2** sub-tab.



7. The **FIDO2 MDS Root Certificate** section allows operators with the "Manage Keys" privilege to load a new MDS (Meta Data Service) Root Certificate.

   It displays the Embedded Certificate Name, Serial Number and Expiry Date. The **Update Certificate** button is used to load new certificates (when FIDO Alliance update their blob and sign it with certificate chained to a different root).

   Note: The Update Certificate button will be disabled if you do not have the "Manage Keys" privilege.

   1. Click the **Update Certificate** button.
   2. Locate and select the certificate you want.
   3. Click the **Apply** button to save the new certificate.
      The MDS Root Certificate will be validated once FIDO2 credentials are enrolled against a Cardholder.

   Note: An Invalid or expired certificate cannot be loaded. If attempted a warning message will display, (e.g. *"FIDO2 Certificate is not a valid PEM format"*, *"New FIDO2 MDS Root Certificate has expired"*).

8. Click the **OK** button

MIFARE DESFire Key Migration

Introduction

Site may want to change their card key if their current key is easily identifiable, (e.g. default key seed), or if the key is compromised. Keys may be migrated:

- per cardholder during normal card use, or
- by an admin bulk-migrating cards by badging them

This procedure describes how a site can migrate away from using the default MIFARE® Site Key on DESFire® cards to using a unique MIFARE® Site Key.

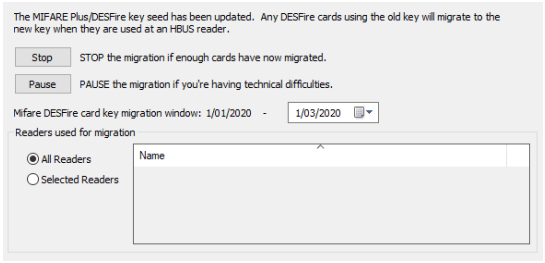
Notes:

- Further information is available in the **Migrating keys on MIFARE DESFire cards TIP.pdf**, located in the `'Documentation'` folder of the Command Centre installation files.
- If you need to identify cardholders with unmigrated cards following a Key Migration, see ***Identifying unmigrated cardholders after Key Migration*** (on page 6-45) for the further detail.

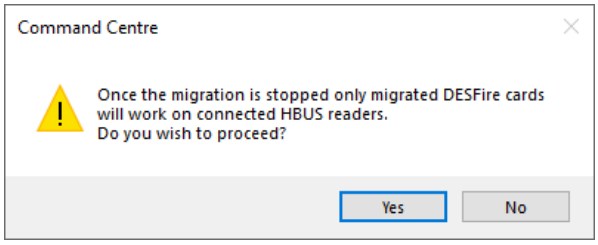
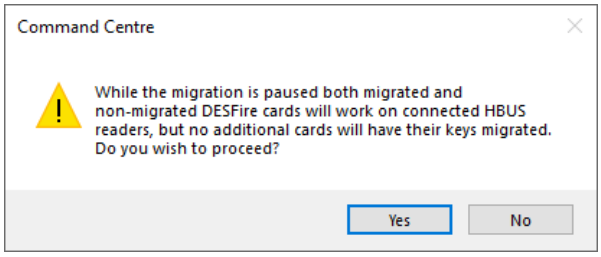
Procedure

1. Generate a custom key seed or import a key and set the migration period, then **Apply** the changes.
   See the "Generate a custom key seed or import a key" part of ***Card Security*** (on page 6-37) for the procedure.
2. Does a warning message display indicating the site has Cardax IV readers?
   If **no**, go to Step 3.
   If **yes**, cards migrated to a custom key are only compatible with HBUS readers and will not work on Cardax IV.
   Do you want to continue?

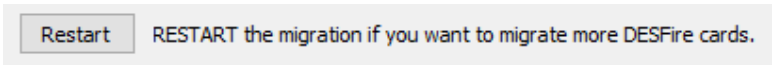
If…	then…
no,	click **No**, and do NOT apply changes. Key migration is cancelled and the settings return to the default.
yes,	click **Yes**, and apply the changes. **Note:** Cards that migrate from the original key will not work on Cardax IV readers. Migration to the new key initiates, and this message displays: *"The MIFARE Plus/DESFire key seed has been updated. Any DESFire cards using the old key will migrate to the new key when they are used at an HBUS reader."*



3. You can **Stop** or **Pause** the migration if necessary, (e.g. you may want to **Stop** migration if enough cards have been migrated, or **Pause** migration if you are having technical difficulties).

If you click the…	then…
Stop button,	the following message displays:  Do you want to continue? If **no**, click **Cancel**. If **yes**, click **OK**. Migration is stopped.
Pause button,	migration is paused and the following message displays:  Do you want to continue? If **no**, click **Cancel**. If **yes**, click **OK**. Migration is paused. Both migrated and non-migrated DESFire cards will work on connected HBUS readers. No cards will have their keys migrated while migration is paused.

The **Stop** and **Pause** buttons are replaced with a **Restart** button which can be used to migrate more DESFire cards.



4. Click the **Restart** button to continue migrating more DESFire cards.
   Note: If you had changed the expiry date of the migration period from the default, when you **Restart** the migration the date will return to the default date.
5. Click the **Apply** button.

Result

The site has migrated away from using the default MIFARE® Site Key on DESFire® cards to using a new unique MIFARE® Plus/DESFire Key Seed.

Note: Once the migration period ends, MIFARE Plus® and un-migrated DESFire® cards will be denied access.

Identifying unmigrated cardholders after Key Migration

Introduction

During or after a key migration, this procedure describes how to identify cardholders with unmigrated cards (cards that haven't been presented at a reader and are still using the old keys).

Prerequisites

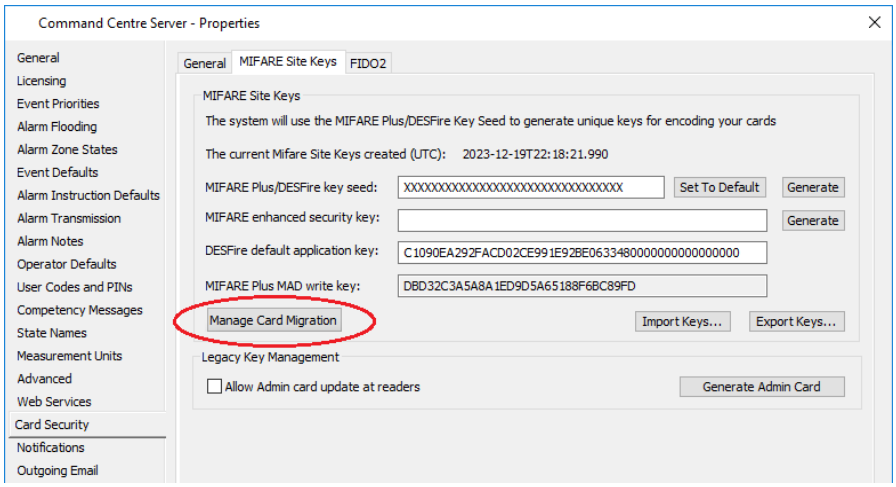
Before proceeding with this procedure ensure:

1. Your Command Centre system is upgraded to vEL8.50 and controllers are updated with the relevant software, and
2. A Key Migration has been performed after upgrading to vEL8.50.
3. You have the "Manage Keys" operator privilege.

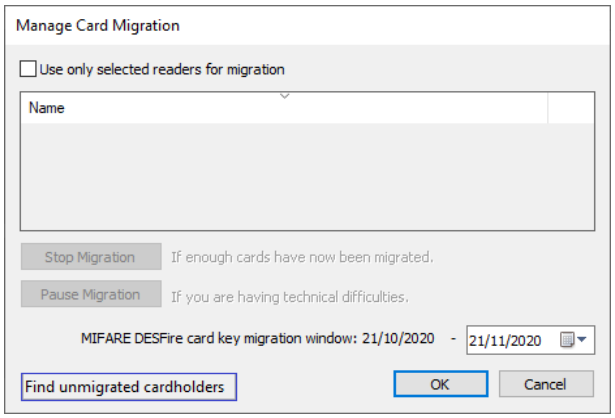
   Note: For migrations being performed across multiple servers in a multi-server system, this procedure should be performed on the server that first started the migration.

Procedure

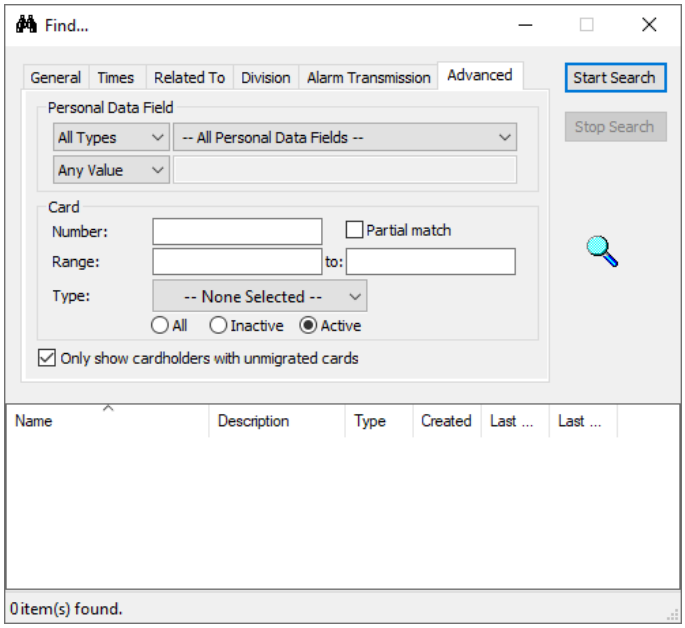
1. Click **File** > **Server Properties**.
2. Click the **Card Security** tab, then the **MIFARE Site Keys** sub-tab.



3. Click the **Manage Card Migration** button.
   The Manage Card Migration dialog displays.



4. Click the **Find unmigrated cardholders** button.
   The Find Tool opens with the **Advanced** tab displayed.



   The **Active** radio button will be selected, and an **Only show cardholders with unmigrated cards** checkbox is ticked.
   Note: The **Find unmigrated cardholders** button (on the Manage Card Migration dialog), and the **Only show cardholders with unmigrated cards** checkbox will only display if a Key Migration has been performed after upgrading Command Centre to vEL8.50 and controllers have been updated with the relevant software.

5. Click the **Start Search** button. If the site is using multiple card types or technologies, you should use the card 'Type' filter to only display results for the relevant DESFire card type.
   The Search grid displays a list of cardholders that meet the unmigrated criteria.

   Note: The list of cardholders can be dragged from the Find Tool Search grid into a "dummy" Access Group in Configuration Client that can be used later as criteria for a broadcast notification in Command Centre Client.

Notifications

Introduction

Completing the details on this tab allows an operator to configure:

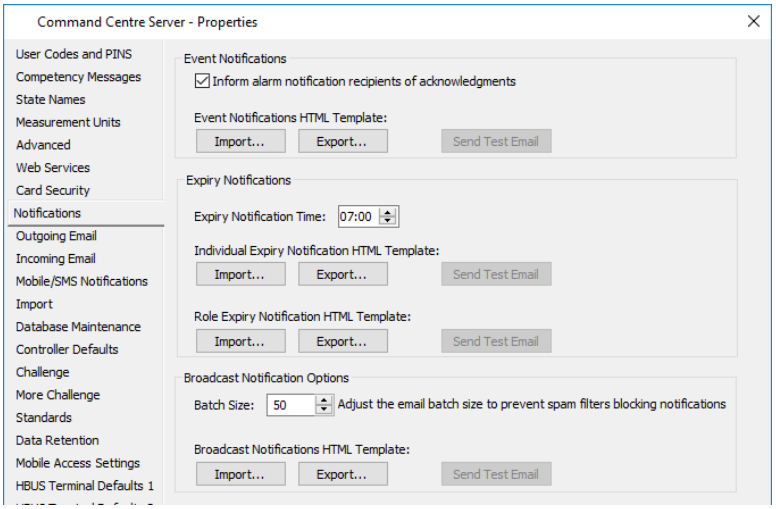
- whether or not alarm notification recipients will be informed of acknowledgements;
- the time (each day) that Card and Competency expiry warnings are sent to individuals and people in a role, (e.g. Manager);
- the number of emails sent per batch, when sending a broadcast notification; and
- custom HTML email templates for Event, Expiry and Broadcast notifications:
  - **Event Notifications**
    Cardholders are notified of any event as determined by the operator (e.g. access denied duress, escalated alarm).
  - **Expiry Notifications** (for an Individual or a Role)
    Cardholders are notified of Cardholder and Competency expiries as an Individual or within a Role (as appropriate). These are sent at a pre-determined time each day.
  - **Broadcast Notifications**
    The operator can set up general notifications to send to any number of specified Cardholders, (e.g. to alert them of a fire drill, to remind them to complete a certain action).

    Note: Broadcast Notifications can also be set up in Command Centre.

Custom Notifications are configured using HTML text. Default HTML email templates are included in the Configuration Client and are accessible via the **Notifications** tab of the Server Properties window (**File** > **Server Properties)**. Users are able to send themselves test emails from this tab to ensure that the email has been configured according to their requirements. For further detail refer to **HTML Help.pdf** located in the `'Documentation'` folder of the Command Centre installation files.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Notifications** tab.
3. The **Inform alarm notification recipients of acknowledgments** checkbox is ticked by default.
   Leave this checked if you want this to occur.
4. Set an **Expiry Notification Time** if required, for the daily running of Card and Competency expiry notifications (Default = 7:00am).
   Note: A new notification will be sent every day only if there is a change, (e.g. another cardholder is added to the warnings). The Expiry Notification Time only applies to Expiry Notifications, not Event or Broadcast Notifications.



Two types of Expiry Notifications can be sent:

- **Your Security Access Expires**
  Emails for warnings of personal/individual expiries. New entries appear in **bold**.
- **Security Access Expiry Report**
  Cardholders that are in 'Roles' will be notified of expiries for their staff. New entries appear in **bold.**

5. Open the relevant email template by navigating to **`C:\Program Files (x86)\Gallagher\Command Centre\EmailTemplates`**

   Notes:
   - Templates whose file names begin with "Custom" contain colour formatting and a PDF with the Gallagher logo.
   - We recommend that before importing any templates, you back them up by copying and pasting them to a location of your choosing. This is to prevent users from accidentally editing the default templates, because then in order to revert the templates back to their original versions, you will need to re-install them from the Command Centre installation files.

6. Enter the number number of emails to be batched, when sending a broadcast notification, in the **Batch Size** field.

   The batch size determines the maximum number of email recipients that can be placed in a single email, and the maximum number of recipients that can be listed in the details of a single event (Default = 50).

   Notes:
   - Recipients of emails are sent in batches for performance reasons, but are listed in the BCC field of the email so as to not disclose the recipient's address to other recipients.
   - Reduce the batch size if your email server is configured to block messages with 50 or more recipients (due to spam filtering).
   - The maximum batch size is 199.

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.

Outgoing Email

Introduction

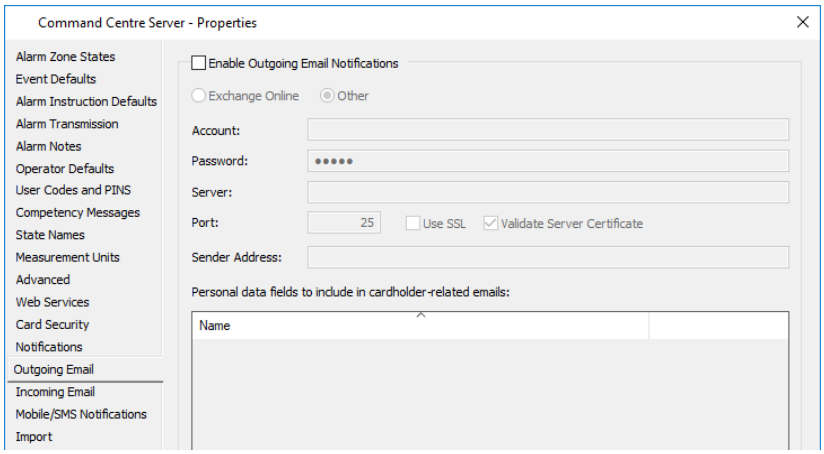
Completing the details on this tab allows a site to send email notifications of events/alarms to various cardholders/operators.

When emails are generated from Configuration Client, they need to pass through this email account to be sent to the recipient. From the recipient's perspective, it will appear that the email has been sent from this outgoing email address.

Note: This tab is only visible if your site is licensed for the Notifications feature.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Outgoing Email** tab.



3. Check the **Enable Outgoing Email Notifications** checkbox.
   All other fields on this screen become enabled.
4. Authentication with your email server can be achieved with Exchange Online authentication or Other (basic) authentication.
   Note: Exchange Online email cannot use 'Other' authentication as of September 2025 (see "*Deprecation of Basic authentication in Exchange Online*" on Microsoft Learn).

   To configure via **Exchange Online**, go to Step 5.
   To configure via **Other**, go to Step 6.
5. Configure the **Exchange Online** authentication fields as indicated:

Field	Description
Tenant ID	Paste the Tenant ID of an Entra ID tenant. This can be found in Entra ID under Properties.
Client ID	Paste the Client ID of your Entra ID application. To register an Entra ID application, refer to the topic "*Quickstart: Register an application with the Microsoft identity platform*" on Microsoft Learn.

Field	Description
	The application's Client ID can be found in Entra ID under **App registrations** > **All applications** > **[name of your application]** > **Overview**. The Application must have the following permissions: Mail.Send for the Microsoft Graph API SMTP.SendAsApp for the Office 365 Exchange Online API Refer to "*Update an app's requested permissions in Microsoft Entra ID*" on Microsoft Learn.
Client Secret	Paste on of your Entra ID application's client secrets. You can only view a client secret immediately after it is created. If you saved a client secret elsewhere, you can enter it here. Otherwise, create a new one in Entra ID. Refer to the topic "*Quickstart: Register an application with the Microsoft identity platform*" on Microsoft Learn, and see the "Add a client secret" section.

6. Configure the **Other** authentication fields as indicated:

Field	Description
Account	An outgoing email account (username@domain). **Note:** If an Account is required, but the username/password are incorrect, the user will get an alarm. If no Account is required, but the username/password is provided (even if incorrect), emails will still send without an alarm being generated.
Password	A password is only needed if SSL is required. **Note:** If SSL is required, check the Use SSL checkbox also.
Server	The email server DNS name or IP address.
Port	The port number.
Validate Server Certificate	Check the **Validate Server Certificate** checkbox to allow Command Centre to verify the certificate provided to encrypt emails. **Note:** The **Use SSL** checkbox must be checked to enable this step.

Note: If your site wishes to connect to an SMTP server not supporting authentication, the **Account** and **Password** fields should be left blank.

7. Enter an email address in the **Sender Address** field if required.
This address will appear as the 'From' address in the email notifications.

   Note: If you have selected **Exchange Online**, the **Sender Address** field is required. Do the following with the email address you enter here:

   - In Microsoft 356 Admin Centre, enable **Authenticated SMTP** for the Microsoft account who owns this email address, under **Active users** > ***[user]*** > **Mail** > **Manage email apps**.

- Register the Entra ID application's service principal in Exchange. Use this email address when giving the service principal access to a mailbox. Refer to the "*Register service principals in Exchange*" section on Microsoft Learn.

Note: If you have selected **Other**, and the **Sender Address** field is left blank, what appears as the 'From' address (in the email notifications) is determined as follows:

If 'Incoming Email' is...	then the...
set up,	'Incoming Email' **Account** will be used to populate the 'From' address.
NOT set up, and the 'Account' is NOT blank,	**Account** will appear as the 'From' address (including '@<servername>' if the **Account** does not include an '@' character).
NOT set up, and the 'Account' is blank,	address of 'security@<servername>' will appear as the 'From' address.

8. Cardholder-related Email Notifications can optionally contain Personal Data Field details.
   Drag and drop any Personal Data Fields that you want to be included with the event/alarm email notifications (if the Personal Data Field is populated for the cardholder), into the grid.
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.

Incoming Email

Introduction

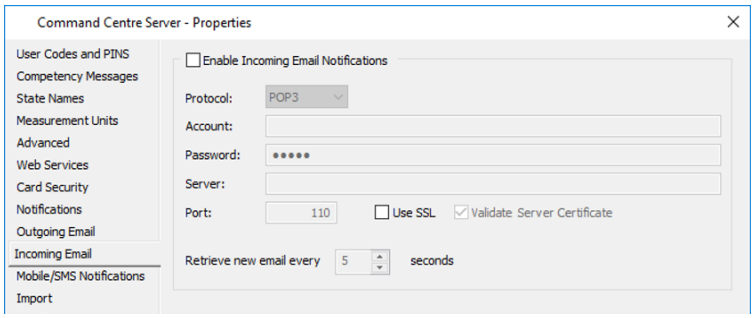
Completing the details on this tab gives a site the ability to acknowledge alarms through replying to the SMS/email.
Note: This tab is only visible if your site is licensed for the Notifications feature.

Before you begin

Before you begin this procedure, ensure you have enabled and configured the outgoing email notifications on the previous tab. See ***Outgoing Email*** (on page 6-49) for further detail.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Incoming Email** tab.



3. Check the **Enable Incoming Email Notifications** checkbox.
   All other fields on this screen become enabled.
4. Configure the following fields as indicated:

Field	Description
Protocol	Defaults to POP3.
Account	An incoming email account (username@domain). Ensure this account is only used by Command Centre as email will be removed once processed. **Note:** Defaults to the same account as the outgoing account.
Password	A password is only needed if SSL is required. **Notes:** • SSL is recommended for incoming email. • If SSL is required, check the Use SSL checkbox also.
Server	The email server DNS name or IP address.
Port	The port number.

   Note: If your site wishes to connect to an SMTP server not supporting authentication, the **Account** and **Password** fields should be left blank.
5. Check the **Validate Server Certificate** checkbox to allow Command Centre to verify the certificate provided to encrypt emails.
   Note: The **Use SSL** checkbox must be checked to enable this step.
6. Set how often the Command Centre Server is to Retrieve new email from the email server. (Default = 5 seconds; Range = 1 - 999 seconds)
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.

Mobile/SMS Notifications

Introduction

Completing the details on this tab allows a site to send SMS notifications of events/alarms to various cardholders/operators. This tab also allows a site to enable Mobile Notifications for Mobile Client users. Mobile Notifications are sent over the internet from the Command Centre Cloud, and do not require outgoing SMS notifications to be enabled.

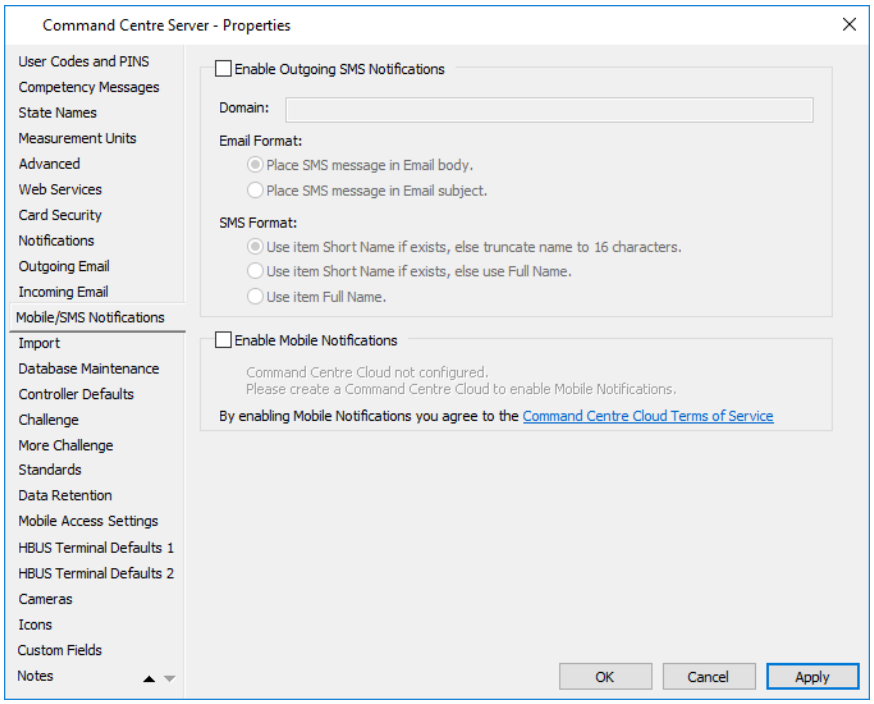
SMS Notifications are sent via email using a Bulk SMS Service Provider. This service provider converts the incoming email sent by Command Centre to an SMS message and delivers it to the appropriate mobile network provider.

Sites using this feature must choose and subscribe to a Bulk SMS Service. Command Centre formats the message suitable for delivery via SMS.

Note: This tab is only visible if your site is licensed for the Notifications feature.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Mobile/SMS Notifications** tab.



3. If enabling Mobile Notifications for Mobile Client users, read the Command Centre Cloud Terms of Service. If you agree with the terms, select the **Enable Mobile Notifications** checkbox. No further configuration on this tab is required.
   Before using this feature you need to create a Command Centre Cloud item. See ***Connecting to the Cloud*** (on page 28-7) for the procedure.

4. Check the **Enable Outgoing SMS Notifications** checkbox.
   All other fields on this screen become enabled.
5. Enter the Email-to-SMS Service Provider's Domain Name in the **Domain** field.
6. Click the appropriate **Email Format** radio button to place the SMS message in either the Email body or the Email subject.
   Note: One or other option will work best depending on your Bulk SMS Service Provider. It is recommended you trial both options.
7. Set the required format for the Command Centre item name portion of the SMS message, by clicking the appropriate **SMS Format** radio button.
   Notes:
   - If there is no Short Name for the item, then the first option will use and truncate the normal (or full) Name to 16 characters, whereas the second option will use the full Name in entirety.
   - The first option allows the full message of any of Command Centres events or alarms to fit within the common 160 character SMS length. The second and third options may attempt to generate an SMS message longer than 160 characters. Depending on your SMS Bulk Service provider, such a message may be truncated at 160 characters, or may be delivered as two (or more) messages.
   - If there is a Short Name for the item, and either the first or second option is selected, then ALL event/alarm SMS messages will fall within the 160 character limit.
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.

Import

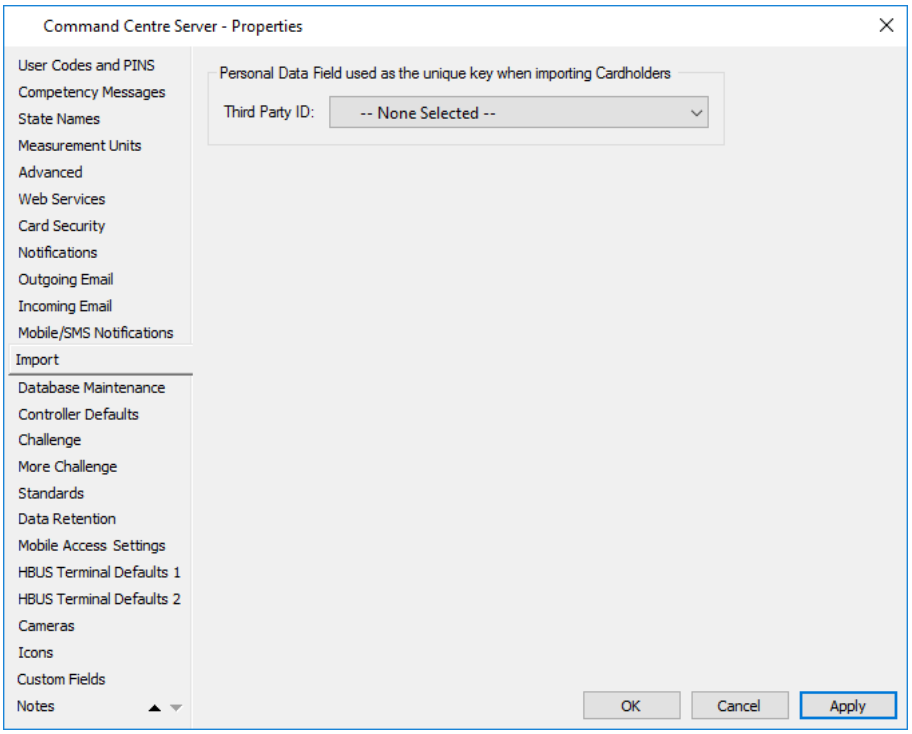
Introduction

The Import/Export Utility, which is a licensable feature of Command Centre, provides the functionality for the import of cardholder details. It allows sites to link the Command Centre system to external systems without the need to re-key cardholder information.

The Import tab enables you to specify the Personal Data Field to be used as a unique Cardholder identifier when performing cardholder imports.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Import** tab.



3. From the **Third Party ID** drop-down list, select the Personal Data Field you wish to use as the unique cardholder identifier.
   Note: The Import Service will only operate against Text or Numeric Personal Data Fields that are defined with the 'Unique' option. The drop-down list on the **Import** tab is restricted to Personal Data Fields that match these constraints.
4. 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.

Database Maintenance

Introduction

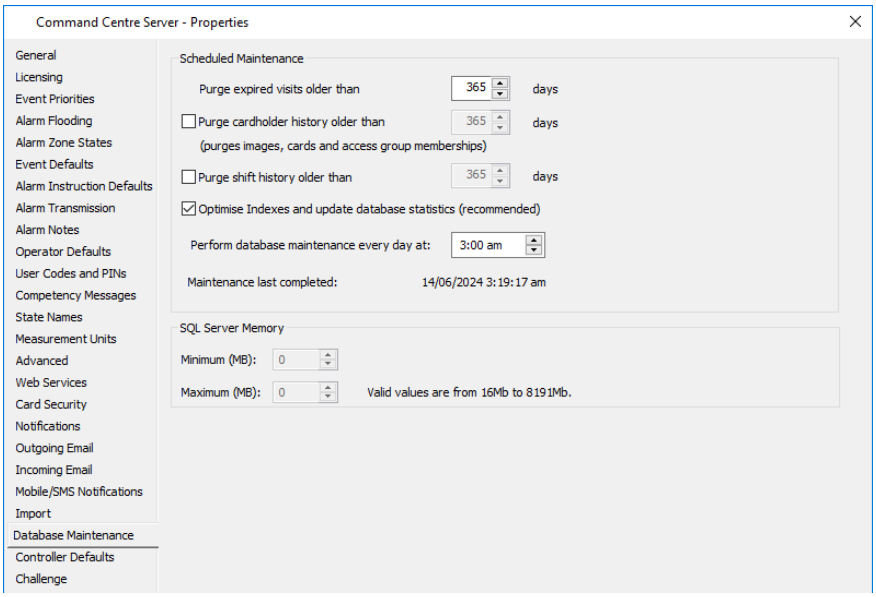
This tab allows a site to:

- initiate a daily update of database statistics.
- purge Cardholder history, and/or if a site is licensed for the Visitor Management feature, they can set the parameters for when expired visits will get purged from the system.
- configure how much memory SQL Server uses.

If you have the "View Site" operator privilege, you will be able to view this tab, but you will not be able to alter any of the fields. However, the "Edit Site" operator privilege allows you to view and edit fields on this tab.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Database Maintenance** tab.



3. If your site licensed for Visitor Management, enter the length of time that visits are to be kept before they become eligible for purging, in the **Purge expired visits older than** field.
   (Default = 365. Must be a whole number between 1 and 9999 inclusive)

   Note: The "purge process" for expired visits is run every day and cannot be disabled.
4. Do you want to purge Cardholder history?

If...	then...
no	go to Step 5.
yes	check the **Purge cardholder history older than** checkbox, and enter the length of time cardholder history is to be kept before it becomes eligible for purging. (Default = 365. Must be a whole number between 1 and 9999 inclusive)

5. If your site is licensed for Shifts, the **Purge shift history older than** option displays. Do you want to purge Shift history?

If...	then...
no	go to Step 6.
yes	check the **Purge shift history older than** checkbox, and enter the length of time shift history is to be kept before it becomes eligible for purging. • If a Shift item was deleted more than this many days ago, it will be purged so that it can no longer appear in Time Reports and Time Report - Overviews that report on historical periods. • If a Cardholder was un-assigned from a Shift more than this many days ago, the association between the Cardholder and the Shift is purged, so that Time Reports and Time Report - Overviews that report on historical periods can no longer report this Cardholder as having worked this Shift. Default = 365. Must be a whole number between 1 and 9999 inclusive.

6. Tick the **Optimise Indexes and update database statistics** checkbox. Gallagher recommend sites optimise indexes and update statistics daily at a time when the system is least busy.
   Note: A Database Maintenance Error event will be raised if the statistics update errors due to database permissions, lack of disk space, database corruption or other reason.
7. The time of day in the **Perform database maintenance every day at** field relates to updating statistics and purging cardholder history. It will also include purging expired visits if your site is licensed for Visitor Management.
   Enter a suitable time of day for database maintenance to run.
   (Default purge time = 3:00am local time; according to the time zone of the server).
   Note: The date and time shown in the 'read-only' **Maintenance last completed** field allows you to check that the database maintenance is running as expected on a daily basis.
8. Are the SQL Server Memory fields read-only or editable?

If...	then CCFT has been installed using the...
read-only,	'Network Service' service accounts. These fields cannot be changed.
editable,	'NT Authority\System' service account. Configure how much memory SQL Server uses by altering the **Minimum** and/or **Maximum** values. **Note:** By setting the maximum amount of memory SQL Server can use, this will ensure other applications are able to run and perform well.

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.

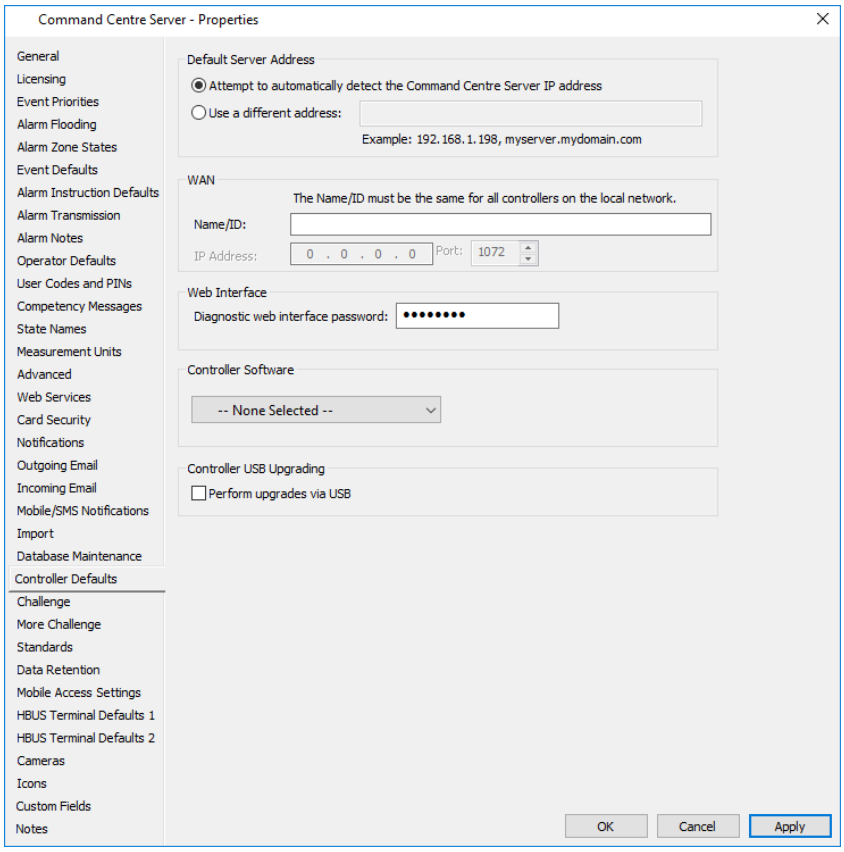
Controller Defaults

Introduction

This tab enables you to configure system-wide software settings for Gallagher Controllers.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Controller Defaults** tab.



3. The **Default Server Address** will affect the server address of all new and existing controllers on the site. The **Use a different address** field accepts either a DNS hostname or IP address.
   Note: If the "Default" server address is selected on a controller's Network property page, that controller will use the server address provided in the global default server address field.
4. The **WAN** section only needs configuring if a remote Controller needs to connect to the Command Centre server using WAN.
   Refer to ***Add WAN Configuration to the Command Centre Server*** (on page 21-34) for further detail.
5. If you want to change the controller diagnostic password, you can enter a new password in the **Diagnostic web interface password** field.

Notes:

- The password follows the password complexity requirements configured on the Server Properties **Operator Defaults** tab, excluding password history settings.
- If the new password is one that is not allowed, (i.e. it is listed in either the **DisallowedPasswords.txt** or **ContextSpecificPasswords.txt** file), an error message will display.
  The **DisallowedPasswords.txt** and **ContextSpecificPasswords.txt** files are pre-installed with Command Centre to allow sites to control allowed passwords.
  For further details see **Preventing context specific passwords** (on page 2-22).
- Controllers need to be online to receive the new password. If they are offline they will not receive the new password until they are online again, or they are reset to the default with a Dip Switch 2 restart.
- Operators who can edit the server properties can change the password. It is not necessary to know the previous password.

6. The **Controller Software** section allows Controller software to be set system-wide.
   The software that appears in the drop-down list will match the **Device Software** List Window.
   Select the required software version from the drop-down list.

   Note: The upgrade process may install new device software, and will change this property if it does.
7. Check the **Perform upgrades via USB** checkbox if you want the code for all Controller 6000s and 7000s to be upgraded via USB, (i.e code for Controller 6000s and 7000s cannot be upgraded via the LAN).
   Note: This is not applicable to the Controller 7000 Single Door.
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.

Controller Web Server

Introduction

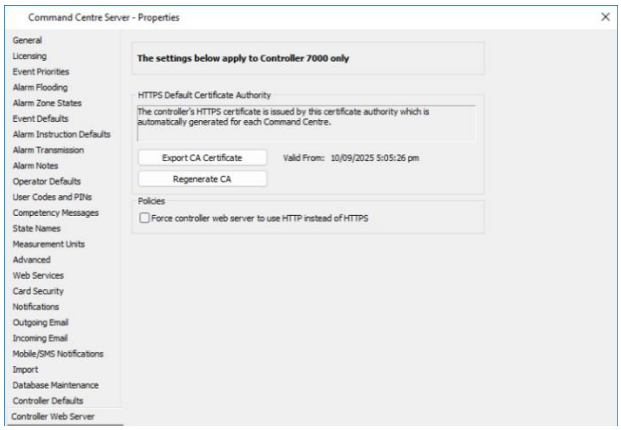
All Controller 7000 devices must now use the **HTTPS protocol** instead of HTTP by default. As a result, the diagnostics web page is only accessible via: https://<controller>/debug.
This tab provides options to:

- Export the CA Certificate - This action will download the current CA certificate.
- Regenerate CA - This action will regenerate CA and automatically deploy new certificates to all controllers, replacing the existing ones.

Additionally, there is an option to force the controller's web server to use HTTP instead of HTTPS, if required.

Procedure

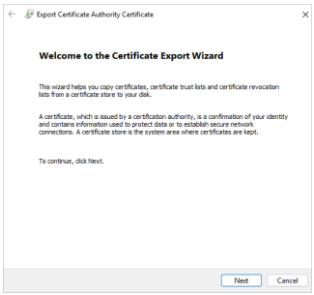
1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Controller Web Server** tab.



3. Perform the required function(s):

   To export CA certificate

   a) Click the **Export CA Certificate** button. The Certificate Export Wizard opens.



   b) Click **Next** to continue.
   c) Select DER encoded binary X.509 (.CER) then click **Next**.
   d) Browse desired location, then enter filename and click **Save**.
   e) Click **Next** and then click **Finish**.
      A message will appear confirming the export was successful. See instructions below for how to install the certificates.

   To generate CA

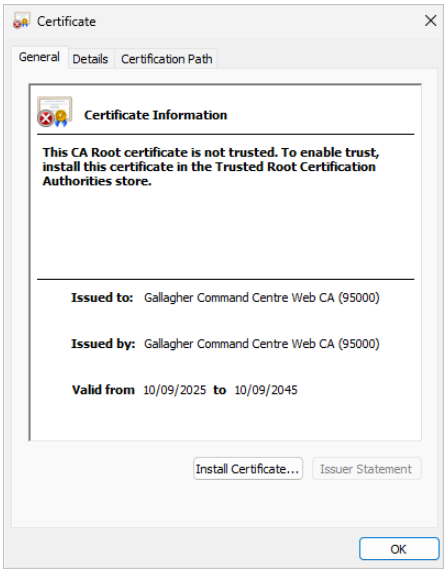
   a) Click the **Regenerate CA** button.
   b) Click **Yes.** **Note:** The Valid date is updated.

4. To force the controller web server to use HTTP, rather than HTTPS, click on the checkbox and then click **Apply**.
5. Installing CA certificate into Trusted Root Certification Authorities removed invalid CA error when opening debug web page on a browser.

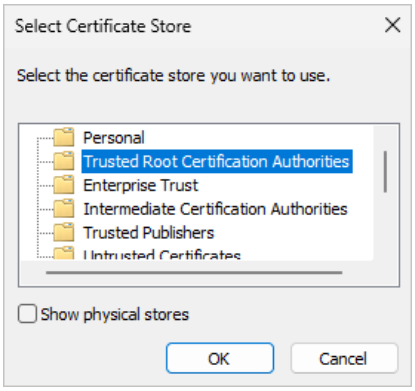
   Note: If the CA is not installed on the computer you are using to access the debug web page, the browser will display a strikethrough HTTPS indicator marked as *Not Secure*. This indicates that the page is still being accessed over HTTPS, but the CA is not trusted or valid.

   To install the CA:

   a) Open the certificate file folder where it was saved.



   b) Click the **Install Certificate…** button.
   c) Select the store location where you want to save the certificate.
   d) Click **Next**.
   e) Tick **Place all certificates in the following store**.
   f) Click on **Browse**, and select the **Trusted Root Certificate**.



   g) Click **OK**, then **Next**.
   h) Click **Finish**. A Security warning displays.
   i) Click **Yes** to proceed with installation.
   A message will appear confirming the export was successful.
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.

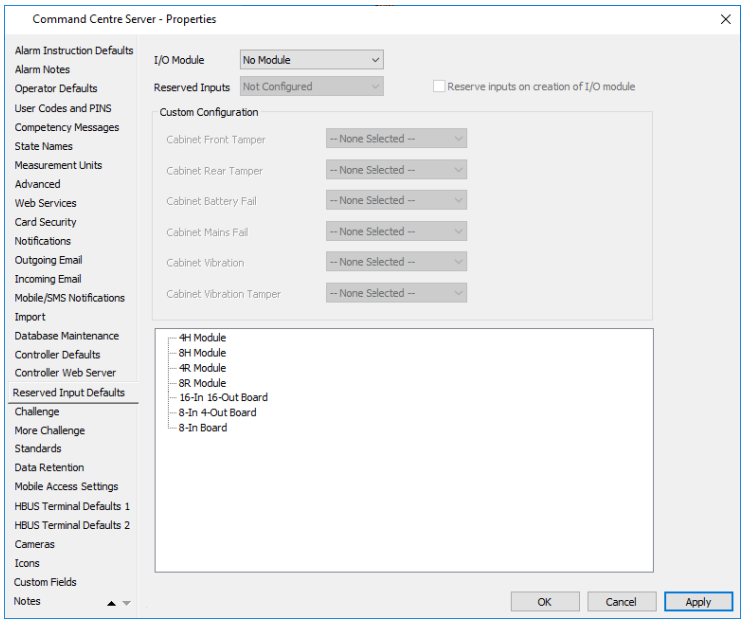
Reserved Input Defaults

Introduction

This tab allows sites whose Controller 7000s are housed in cabinets to use physical tamper inputs (rather than optical tampers), and to also reserve power supply inputs and create alarms with the Controller as a source.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Reserved Input Defaults** tab.



3. Select the appropriate option from the **I/O Module** drop-down list. The **Reserved Inputs** field becomes enabled.
4. Select from "Not Configured", "First 6 Inputs", "Last 6 Inputs" or "Custom Configuration" from the **Reserved Inputs** drop-down list. If "Custom Configuration" is selected, the **Custom Configuration** section becomes enabled.
   Note: If you tick the **Reserve inputs on creation of I/O module** checkbox, the Reserved Inputs you select here will already be configured when a plug-in module is selected on a Controller 7000 or an I/O module of the selected type is created.
   The window shows the defaults selected for each module type supporting reserved inputs.
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.

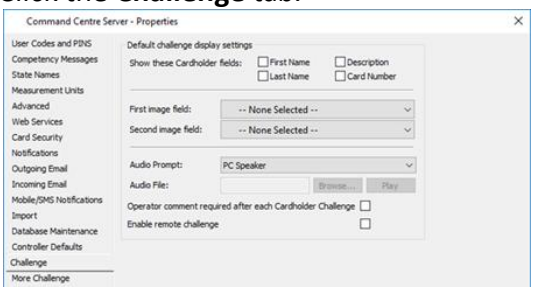
Challenge and More Challenge

Introduction

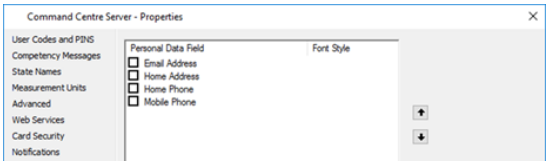
The Command Centre Challenge feature allows you to contest Cardholders as they attempt to gain access through a Door. You may use the feature to visually confirm the identity of each Cardholder before manually granting access to a secure area. These two tabs enable you to configure the site wide default settings for the Challenge feature. These settings can be overridden for individual Doors as required. See Configuring Challenge for details.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Challenge** tab.



3. Tick the checkboxes for the **Cardholder fields** you wish to be displayed in a Viewer window, (i.e. First Name, Last Name, Description and Card Number).
4. If you require Image based PDFs to be displayed in a Viewer window, select a **First image field** and a **Second image field** from the drop-down lists.
5. If you require an audio sound to be played whenever a Cardholder challenge occurs, select an **Audio Prompt** form the drop-down list.
6. If you require a short explanation from an operator after granting or denying access to each Cardholder, tick the **Operator comment required after each Cardholder Challenge** checkbox.
7. If you require this server's Challenge Doors to send Challenge events to remote servers, (i.e. in multi-server environments), select the **Enable remote challenge** checkbox. With this checkbox selected, Challenge viewers on remote servers will receive challenge events for this server's Challenge Doors, as well as Challenge viewers on the local server.
8. Click the **More Challenge** tab.



9. From the list of text and numeric Personal Data Fields (PDFs), select those you wish to be displayed in a Viewer by checking the tickbox beside the PDFs.
10. Configure a simple font style against each selected PDF.
11. Sort your selection of PDFs by using the **arrow** buttons to the right of the list box if required. The order you define will be retained when information is shown in the Challenge Viewer.
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.

Standards

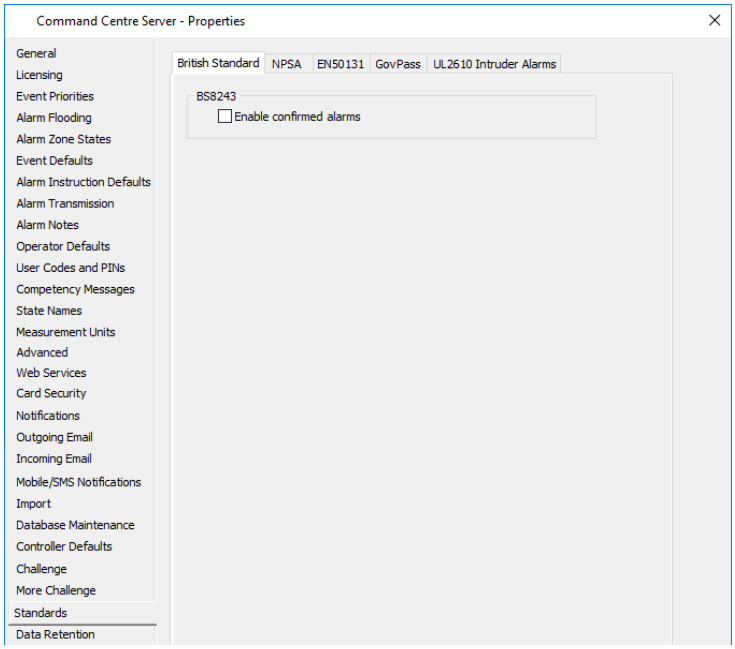
Introduction

This tab enables operators with the "Edit Site" (or higher) operator privilege to:

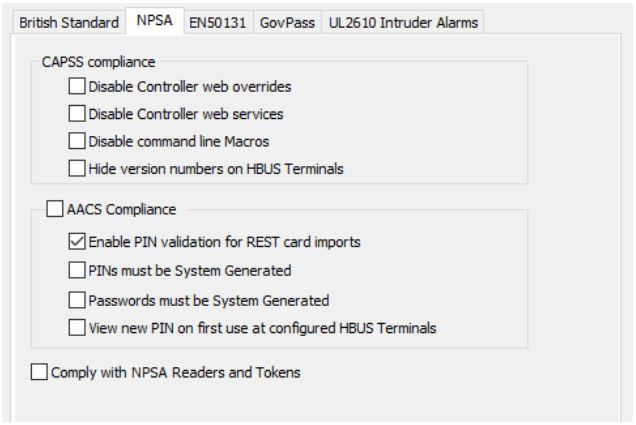
- configure specific system-wide behaviour with respect to alarm system standards. All fields in the **Support for alarm system standards** section will be 'read-only' for operators with the "View Site" operator privilege.
- configure **NPSA and CAPSS compliance** settings for extra security, if required.
  Note: To be able to configure these settings on sites licensed for NPSA, (i.e. `NPSA=1` appears in the licence file), operators need to log into Command Centre using FIDO2 Authentication.
- configure the system so that when controllers are being upgraded, any readers connected to those controllers will display a unique flash pattern, (i.e. 4 rapid red flashes).

Procedure

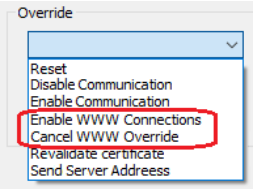
1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Standards** tab. The **British Standard** sub-tab displays by default.



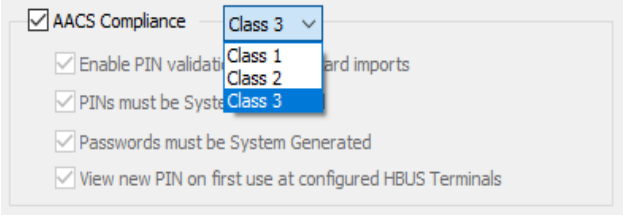
3. Ticking the **Enable confirmed alarms** checkbox has the following effects throughout the system:
   - enables the transmission of sequentially confirmed alarms.
   - maintains a confirmation state for all Alarm Zones, such that entry delay will be prevented if confirmed alarms are not inhibited in the zone.
   - causes inputs in an Alarm Zone to be automatically isolated if they are still active when the confirmation time expires. An additional Contact ID restoral message is also transmitted on expiry of the confirmation time.
4. Click the **NPSA** sub-tab.



5. Configure the **CAPSS Compliance** settings if required.
   Note: These checkboxes will all be checked by default if your site is licensed for CAPSS.

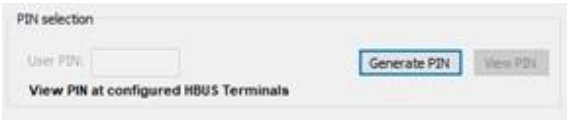
Checkbox	Description
Disable Controller web overrides	With this option checked, the **Enable WWW Connections** and **Cancel WWW Override** overrides for Controllers will be removed from the workstation menu. Uncheck this option if you want these overrides to be available. 
Disable Controller web services	With this option checked, the **Dip Switch 1 controls the diagnostic web interface** checkbox (on the **Setup** tab of Controller properties) will be greyed out so it cannot be enabled. Uncheck this option if you want this to be available.
Disable command line macros	With this option checked, the Macro command lines cannot be inserted. Uncheck this option if you want to be able to insert Macro command lines.
Hide version numbers on HBUS Terminals	With this option checked, the Firmware version numbers will not appear on an HBUS Terminal screen. Uncheck this option if you want Firmware version numbers to appear on an HBUS Terminal screen when the **#** button is pressed several times.

6. Check the **AACS Compliance** checkbox if your site needs to comply with AACS standards. When the **AACS compliance** option is enabled, a "Class" option becomes available to choose from, and based on the selected "Class" the following options will either be enforced or available to modify:



Note: If your site is licensed for CAPSS all the options will be ticked and enforced by default, with **Class 3** option selected.

When AACS Compliance option is unchecked, the below options will still be available to select/deselect.

Checkbox	Description
Enable PIN validation for REST card imports	• is enabled by default • when unticked it will disable the PIN validation (sequences and repeating characters) for REST card imports • enforced for Class 1, Class 2 and Class 3 AACS
PINs must be System Generated	• is disabled by default and the user is allowed to Assign PIN manually when ticked the user cannot Assign PIN manually through **Cardholder**>**Print/Encode** in Configuration Client OR **Cardholder Viewer**>**Cardholder Cards tile**>**Assign PIN** in Command Centre Client • enforced for Class 1, Class 2 and Class 3 AACS
Password must be System Generated	• is disabled by default and the user is allowed to change the password manually • when checked the Password textbox becomes "read-only" and cannot be typed manually through **Cardholder**>**Operator configuration**> **New Password** option and **Manage**>**Change Password**>**New Password** option in Configuration Client OR **Burger Menu**> **Change Password** and **Cardholder Viewer**>**Logon details** option in Command Centre Client • enforced for Class 2 and Class 3 AACS but enabled and available to modify for Class 1 AACS
View new PIN on first use at configured HBUS Terminals	• is disabled by default • when checked the **Allow assigning of system generated PIN** checkbox (in the 'PIN Handling' section on the **Advanced** tab of the HBUS terminal properties) becomes available to select. When selected the system generated PIN can be viewed on the configured HBUS terminal when a card is badged for the first time • when checked 'View PIN' functionality is disabled, (i.e. the **View PIN** button is disabled, and a *"View PIN at configured HBUS Terminals"* message displays when the **Generate PIN** button is clicked  • enforced for Class 3, eanbled and available to modify for Class 2 and unchecked for Class 1 AACS

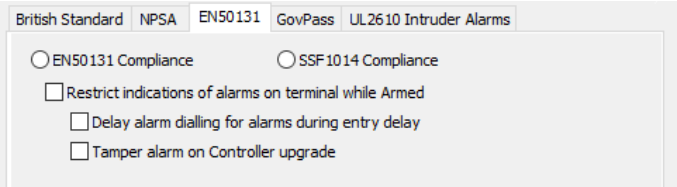
7. Check the **Comply with NPSA Readers and Tokens** checkbox if your site needs to comply with NPSA Readers and Tokens. If you enable this option, the following changes also occur for other properties:
   a. **Card Security** tab (Server Properties):
      The "Enable Fast CSN Mode" and "Allow Admin card update at readers" checkboxes, and the **Generate Admin Card** button all become disabled/un-editable.
   b. **PINs** tab (Card Type properties):

The "Use PINs" checkbox becomes ticked by default, as new card types should be created to use PINs with a minimum of 4 digits.

c. **Mobile Access Settings** tab (Server Properties and Reader properties): Mobile connect settings become disabled/un-editable.

d. **Advanced** tab (Reader properties):
"Require MIFARE Enhanced Security encoded cards" checkbox is ticked and becomes disabled/un-editable.
"Use MIFARE Serial Number as Card Data" checkbox becomes disabled/un-editable.
The **Permitted Card Technology** is forced to only allow the "Mifare Desfire EV1 to EV3" option.

8. Click the **EN50131** sub-tab.

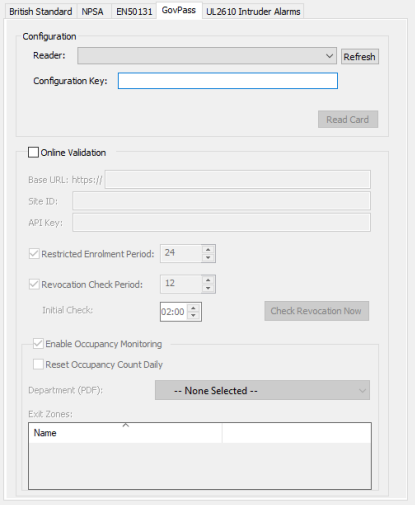


9. Check the **EN50131 Compliance** or **SSF1014 Compliance** checkbox depending on which standard your site needs to comply with.
These options are only applicable to sites wanting to comply with UK standards (EN50131), or Swedish standards (SSF1014), and makes it easier to configure a site for compliance.
In its simplest form it would be checked by the installer before any other site configuration, would auto-select most of the other options on the **EN50131** tab and otherwise would simply change the defaults for various other settings. When checked, most of the EN50131 and SSF1014-required configuration is applied at once.
Note: Installers will still need to configure Divisions, Operator Groups, etc. appropriately.

10. Configure the fields as required:

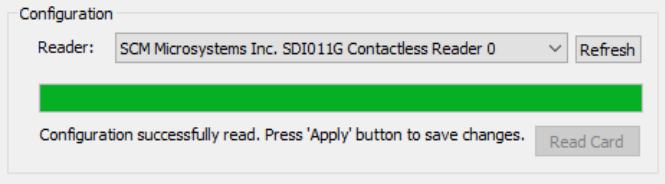
Checkbox	Description
Restrict indications of alarms on terminals while Armed	Checking this option removes all visual and audio indicators on the 'Welcome' screen of a terminal (i.e. any active alarms while the Alarm Zone is armed).
Delay alarm dialling for alarms during entry delay	With this option checked, any alarm activations that occur during entry delay will have immediate local indications, (i.e. relays, etc.), according to their Action Plan setup. However, remote notification via alarm dialling will be delayed until the end of entry delay, or 30 seconds, whichever is greater. The alarm activations will not be remotely noti-fied if un-setting occurs successfully before the expiry of entry delay.
Tamper alarm on Controller upgrade	With this option checked, an alarm will be created whenever Controller firmware is upgraded. When enabled, an active tamper condition is created when a download starts. This alarm is made inactive by any event that indicates the end of a download. This includes both successful and unsuccessful completion.

11. Click the **GovPass** sub-tab.
    Note: This sub-tab will only display if your site is licensed for GovPass (i.e. the licensed file contains `UKGovPass=1`). There is no limit to the number GovPass card flows and card types a site can have.



12. The **Reader** drop-down list displays all the readers connected to Command Centre. Select the appropriate reader from the Reader drop-down list.
13. Manually type in the **Configuration Key**, or copy and paste it in.
14. Present a GovPass configuration card to the USB MIFARE reader connected to the Command Centre Server PC with the key to be used to read the Cardholders cards.

Once the card is read successfully, a green bar displays and a completed message displays asking you to click the **Apply** button to save the changes.



Note: The following table describes the errors that can occur:

Error Message	Problem
Authentication failed with supplied key(s).	The key entered (or read from previous Configuration card) does not match this Configuration card.
The Configuration Key must be exactly 32 characters long.	The key entered for the first Configuration card read is not the correct size.
Timeout waiting for card read. No Card detected.	The encoder/reader did not detect a valid card to read.
Detected card does not appear to be a valid GovPass Configuration card.	The card is a non-GovPass card (Classic, Plus, PIV).
Card application not found.	The card is not a ***valid*** GovPass Configuration card. This is a different error to the above as it is a valid DESFire card but is lacking one or more GovPass applications.
The data necessary to complete this operation is not yet available.	Something went wrong talking to the encoder/reader. If you try to read the card again it should work on the second or subsequent attempt(s).

15. Tick the **Online Validation** checkbox if your site intends using the GovPass REST API. All fields become enabled, allowing you to set up all the values required to communicate with the GovPass REST API.

Note: If this box is unticked, any cards subsequently enrolled will have Status = Active, and cards with Unverified status will be changed to Active. The following warning will display if unticked:



16. Configure the fields as required:

Field / Button	Description
Base URL *	This is the address of the endpoint we need to connect to. This field accepts alpha-numeric and special characters. (Maximum limit = 100 characters) **Note:** Operators require the "Manage Keys" privilege to edit this field, otherwise it will be "read-only".
Site ID *	Also known as the Building ID, this is the identifier for the site. If there is more than one Access Control System per site, a Site ID will be issued per system. This field accepts alpha-numeric and special characters. (Maximum limit = 50 characters. **Note:** Operators require the "Manage Keys" privilege to edit this field, otherwise it will be "read-only".
API Key *	This is the key required to authenticate with the GovPass REST API to enable usage. This is an alpha numeric value, with no special characters, and must be exactly 40 characters. **Note:** Operators require the "Manage Keys" privilege to edit this field, otherwise it will be "read-only".
Restricted Enrolment Period	When Restricted Enrolment Period is selected and a time period specified (from 1 to 999 hours), if the GovPass Check Service was unable to be contacted at the time of enrolment and this condition lasts for longer than the specified time the card becomes disabled with card state "Suspended (Not Verified)". Command Centre will continue to attempt to contact the GovPass Check service and once successful will update the card state to the correct value (which may result in the card becoming Active). When Restricted Enrolment Period is not selected, cards may be enrolled with the service offline and may remain in the "Unverified" state indefinitely. (Default = 24 hours) **Note:** Operators require the "Configure Site" privilege to edit this field.
Revocation Check Period	When selected, Command Centre will contact the GovPass Check Service with the specified period (from 1 to 24 hours), starting at the specified Initial Check time. Any cards found to be revoked will be disabled Revoked (GovPass), Inactive, Expired (GovPass) or Lost (GovPass). It depends on what the revocation status is. (Default = 12 hours) **Note:** Operators require the "Configure Site" privilege to edit this field.

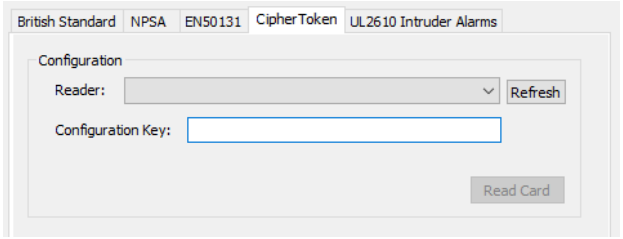
Field / Button	Description
Initial Check	This is only enabled when the Revocation Check Period is ticked, and specifies the starting time for the Revocation Check. (Default = 2 hours. Range = 0 - 23:59)
Check Revocation Now	When this button is clicked a revocation check is carried out immediately.
Enable Occupancy Monitroing	Occupancy Monitoring can be turned off by unchecking this option. When turned off: ▪ the Occupancy Count will no longer be updated to the GovPass API, and ▪ the reset occupancy count, department and exit zones will be disabled as these are all related to occupancy counting. (Default = Checked)
Reset Occupancy Count Daily	When this checkbox is ticked, the occupancy count for each department is reset every midnight (12:00am) and is passed on to the GovPass Check Service. **Note:** Although occupancy is based on Cardholder location in Command Centre, locations will not automatically update at midnight because this might interfere with other functionality in Command Centre, (e.g. Evacuation Reports). Cardholders are only marked as outside for the purpose of occupancy counting at midnight and their location according to their status will not be changed.
Department (PDF)	This is the Personal Data Field (PDF) that will be used to identify which GovPass Department a cardholder belongs to. It is used to report the number of cardholders belonging to each department who are currently on-site, known as Building Occupancy. **Note:** Only "Text" or "Text - List" PDF types can be selected.
Exit Zones	Access Zone(s) can be dragged in this grid to be used as Exit Zones. When a cardholder's location changes to one of these zones or to the special "Outside the system" zone, the occupancy count for the cardholder's department (or Unconfigured) is decremented.

* Mandatory fields.

Note: A site can untick the **Online Validation** checkbox at any point, should they choose to opt out of the validation. All 'Unverified' cards will automatically be set to 'Verified', and any queued messages to the GovPass REST API will be cleared.

17. Click the **CipherToken** tab.

    Note: This sub-tab will only display if your site is licensed for CipherToken, (i.e. the license file contains `CipherToken=1`). There is no limit to the number of CipherToken card flows and card types a site can have.

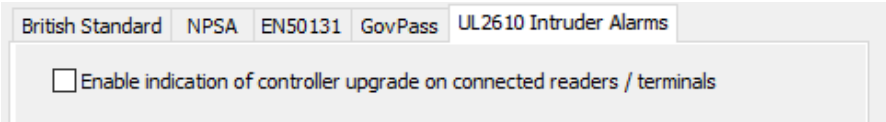


18. The **Reader** drop-down list displays all the readers connected to Command Centre. Select the appropriate reader from the Reader drop-down list.
19. Manually type in the **Configuration Key**, or copy and paste it in.
20. Present a CipherToken configuration card to the USB MIFARE reader connected to the Command Centre Server PC with the key to be used to read the Cardholders cards.

    Once the card is read successfully, a green bar displays and a completed message displays asking you to click the **Apply** button to save the changes.
    Note: The following table describes the errors that can occur:

Error Message	Problem
Authentication failed with supplied key(s).	The key entered (or read from previous Configuration card) does not match this Configuration card.
The Configuration Key must be exactly 32 characters long.	The key entered for the first Configuration card read is not the correct size.
Timeout waiting for card read. No Card detected.	The encoder/reader did not detect a valid card to read.
Detected card does not appear to be a valid CipherToken Configuration card.	The card is a non-CipherToken card (Classic, Plus, PIV).
Card application not found.	The card is not a ***valid*** CipherToken Configuration card. This is a different error to the above as it is a valid DESFire card but is lacking one or more CipherToken applications.
The data necessary to complete this operation is not yet available.	Something went wrong talking to the encoder/reader. If you try to read the card again it should work on the second or subsequent attempt(s).

21. Click the **UL2610 Intruder Alarms** sub-tab.



22. Check the **Enable indication of controller upgrade on connected readers/terminals** checkbox if you want users to be made aware when controllers are upgrading by way of a 4 rapid red flash pattern on the readers connected to the controller.
23. 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.

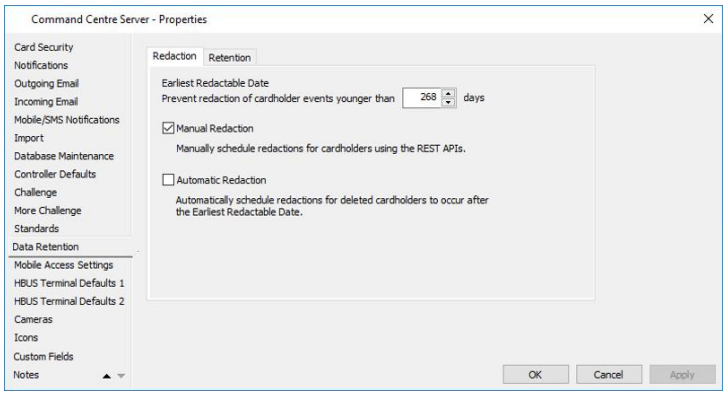
Data Retention

Introduction

This tab allows the removal of events and other data related to cardholders from Command Centre. **Note:** This tab will only display if your license file contains either `PIIRedaction=1` or `DataRetention=1`.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Data Retention** tab. The sub-tabs that display depend on what your site is licensed for, (i.e. for the **Redaction** sub-tab to display your license file must contain `PIIRedaction=1`, and for the Retention sub-tab to display your license file must contain `DataRetention=1`).



3. 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.
   If your site intends using this functionality, refer to ***Redaction Configuration in Command Centre*** (on page 68-3) for the procedure.
4. Click the **Retention** sub-tab if displayed.
5. Configure the fields as required.

Field	Description
Limit Data Retention	When ticked, this enables the system to purge events as defined in the Schedule. If the server is offline, events are purged once the server comes back online. (Default = unticked)
Purge all Cardholder activity older than	When ticked, the system will remove all Cardholder activity for the period indicated.
Purge all events older than	This is the age of the events that will be removed from the system. (Default = 7 years. Range = 1 to 99 years)
Remove cards (*) that are unused for more than	When ticked (default), this is the age of the unused cards that are removed from the system. (Default = 7 years. Range = 1 to 99 years)

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.

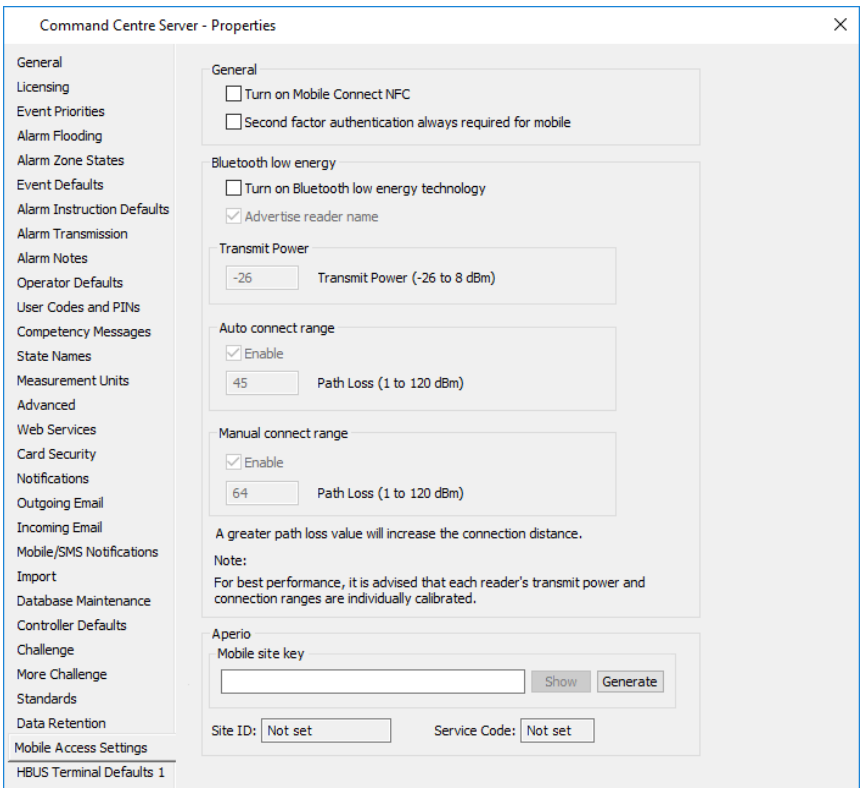
Mobile Access Settings

Introduction

This tab enables you to specify the site wide settings for Mobile Connect.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Mobile Access Settings** tab.



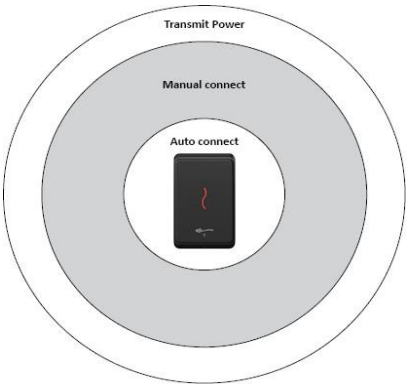
3. Configure the **General** settings as required.

Field	Description
Turn on Mobile Connect NFC	When checked, Android devices will use NFC to request access at the readers. NFC applies to Auto Connect only. If the user has NFC disabled on their device, their device will revert to Bluetooth® to make the access request. Default is OFF.
Second factor authentication always required for mobile	When checked, presentation of a second authentic-cation factor is required at all Bluetooth® enabled readers, unless the access mode is set to 'Free-No PIN'. Default is OFF. Second factor authentication is enforced for mobile credentials only. **Note:** If the access mode is set to 'Free-No PIN' and a personalised action has been assigned to the user, a second authentication factor **will** be required. Refer to ***Configuring Personalised Actions for Access Zones*** (on page 10-34) for details on how personalised actions work. NFC works over a short range, hence a user may take their device out of range to provide their second factor. When this happens, the App displays an icon encouraging the user to re-enter the field.

4. Configure the **Bluetooth low energy** settings as required.

Field	Description
Turn on Bluetooth low energy technology	When checked, Bluetooth® comms are enabled. Default is OFF.
Advertise reader name	When checked, the reader's name will be displayed in the Gallagher Mobile Connect App. Default is ON. If the reader has been configured with a Short Name, the Short Name will be used. Names longer than 26 characters will be truncated. If set to OFF, a generic identifier incorp-orating part of the reader's HBUS serial number will be shown in the Gallagher Mobile Connect App, (e.g. Reader: 12345).
Transmit Power	Controls the Bluetooth® signal strength. Default is -26 dBm. **Notes:** • Increasing the transmit power will increase the Bluetooth® connection distance. • Reducing the transmit power can be used to prevent closely located readers from interfering with each other Bluetooth® communications.
Auto connect range	When checked, all mobile devices will automatically initiate an access request when they sense a signal stronger than this value. Lower values indicate a stronger signal, and thus higher values will allow access from farther away. Default is 45 dBm. Auto connect will be disabled when the: • Door that this reader is assigned to has no Access Zone assigned to it, or • Door that this reader is assigned to has one Access Zone that is in access mode 'Free-No PIN', or • reader is assigned to an Elevator with all floors in access mode 'Free-No PIN'. • Door's Emergency Release has been triggered. • **Note:** Auto connect may not be suitable for all reader installations, (e.g. if a user is situated close to the reader, continual connection attempts from the reader will reduce the device's battery).
Manual connect range	When checked, the user will be able to manually initiate an access request from this range (which must be a longer range than the auto-connect range), using the Gallagher Mobile Connect App. Default is 64 dBm.

Notes:



- Increasing the path loss value will increase the reader's Bluetooth® read range.
- Consideration should be given to the installation environment, as environmental factors may reduce the reader's Bluetooth® read range. It is advised that each reader's transmit power and connection ranges are individually calibrated. The Gallagher Mobile Client App can be used to calibrate the signal strength for each reader.
- Consideration should be given to the signal strength of readers that are installed back-to- back. For example, a reader installed at the front door is set to 'Secure-PIN' and the exit reader on the other side of the wall is set to 'Secure', a user could connect to the exit reader and gain entry without entering a PIN.
- If a reader is assigned to an Elevator, the user will be required to enter a second authentication factor, if any of the Elevator's floors require a PIN.

5. When licensed, the **Aperio** section will appear in the lower part of this screen. Configure as required if your site wants to use mobile credential access at Aperio locks.

   Note: These settings will be used in the Aperio Programming Application to configure mobile credentials for Aperio locks. See ***Configuration for Mobile Connect*** (on page 75-67) for further detail.

Field	Description
Mobile site key	Populate this field with a 32 character hexadecimal string. Characters accepted are only A-F and 0-9. 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 and enable the **Apply** button. If the **Apply** button is clicked now, the 32 characters are converted to 32 X's. **Notes:** • Clicking the **Show** button will display the key that you have entered. Clicking the **Apply** button changes the text back to X's and the **Show** button is enabled again. An operator event is also logged. • If the site key has somehow been compromised you can change an already saved key by clicking the **Generate** button. If you do this the following warning message will display: *"Are you sure you want to change the Aperio mobile site key? Changing the Aperio mobie site key will require manual reconfiguration of all Aperio doors on site. Mobile credential access to these doors will no longer be granted until this has been done."*
Site ID and Service Code	Once you have added a mobile credential these 'Read-only' fields are popluated. Site ID: 8 character hexidecimal format Service Code: 2 digits

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.

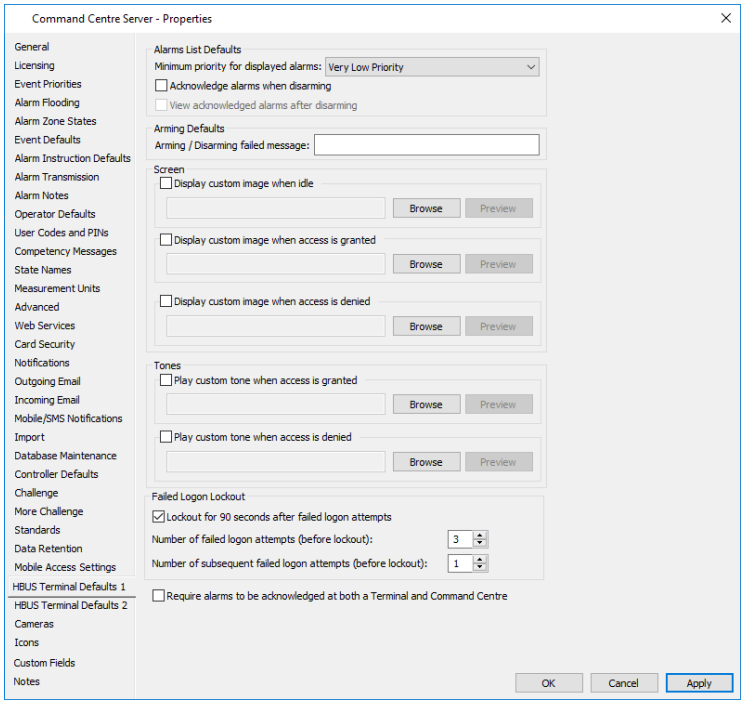
HBUS Terminal Defaults

Introduction

These tabs enable you to specify the site wide Alarms List Defaults, Arming Defaults, Idle Images and Mimic Panel LED Settings for all HBUS Terminals or HBUS Contact Card Readers.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **HBUS Terminal Defaults 1** tab.



3. Configure as required.

Field	Description
Alarms List Defaults	When the **Acknowledge alarms when disarming** checkbox is checked, all terminals configured to use the default settings will acknowledge all alarms at or above the selected priority, for the Alarm Zone(s) the Cardholder disarms using the terminal. The acknowledged alarms will only display if the **View acknowledged alarms after disarming** checkbox is checked. **Notes:** • This is the default setting for all terminals however this setting can be changed on individual terminals. • This functionality does not apply when the terminal is configured for access, (i.e. when the terminal is assigned as a reader, or disarming as part of an access decision). • The alarms displayed and acknowledged are determined by the Alarm Zones assigned to the Cardholder's Access Group(s) and the Terminal Privileges configured within these Access Groups.
Arming Defaults	This field enables you to enter an arming/disarming failed message. All terminals configured to use the default settings will display this

Field	Description
	message when an arming/disarming failed event occurs at the terminal. Maximum 60 characters. **Note:** This is the default setting for all terminals however this setting can be changed on individual terminals.
Screen	These options allow you to display a custom image, (e.g. company logo) on the terminal Welcome screen when idle, (i.e. when logged off), and/or a custom icon when access is granted or denied. The idle image will be displayed when the terminal has been idle for 10 seconds. Check the appropriate checkbox(es) for when you want an image to display, (i.e. **Display custom image when idle**, **Display custom image when access is granted** and/or **Display custom image when access is denied**), then either type in the name of the image file to be displayed or click the **Browse** button to locate the image file. **Notes:** • Only **.png**, **.jpg** and **.jpeg** files can be displayed. • The image size should be 320x240 pixels. • Select the **Preview** button, to preview how the image will look when displayed. • This is a default setting for all terminals however this setting can be changed on individual terminals.
Tones	These options allow you to play a custom tone on the terminal when access is granted and/or denied. Check the appropriate checkbox(es) for when you want a tone to play, (i.e. **Play custom tone when access is granted** and/or **Play custom tone when access is denied**), then either type in the name of the sound file to be played or click the **Browse** button to locate the sound file. **Notes:** • Only **.wav** and **.mp3** files can be played. • The sound file will play for a maximum of 3 seconds, and will be no bigger than 100 kilobytes. • Select the **Preview** button to review the selected tone. • Tones can be distorted by the limited T20 speaker, therefore it is recommended custom tones are tested on T20 hardware. • This is a default setting for all terminals however this setting can be changed on individual terminals.
Failed Logon Lockout	When the **Lockout for 90 seconds after failed logon attempts** checkbox is checked, all terminals configured to use the default settings will be locked for a period of 90 seconds after the **Number of failed logon attempts** has been exceeded. Default 3. Range 3-10 If required, enter the **Number of subsequent failed logon attempts** to occur before the terminal is locked out again. Default 1. Range 1-10. **Notes:** • The default will be off for sites that already have terminals installed. For sites installing new terminals the default will be on. • The repeated use of the same user code or PIN will only count as a single attempt. • If the number of failed logon attempts reaches a certain number, then a tamper alarm is raised. This number is either the total of the two configurable amounts plus 1, or 7 attempts - whichever is reached first. The terminal will display the message "*Temporarily locked out*" with a red "X" on screen.

Field	Description

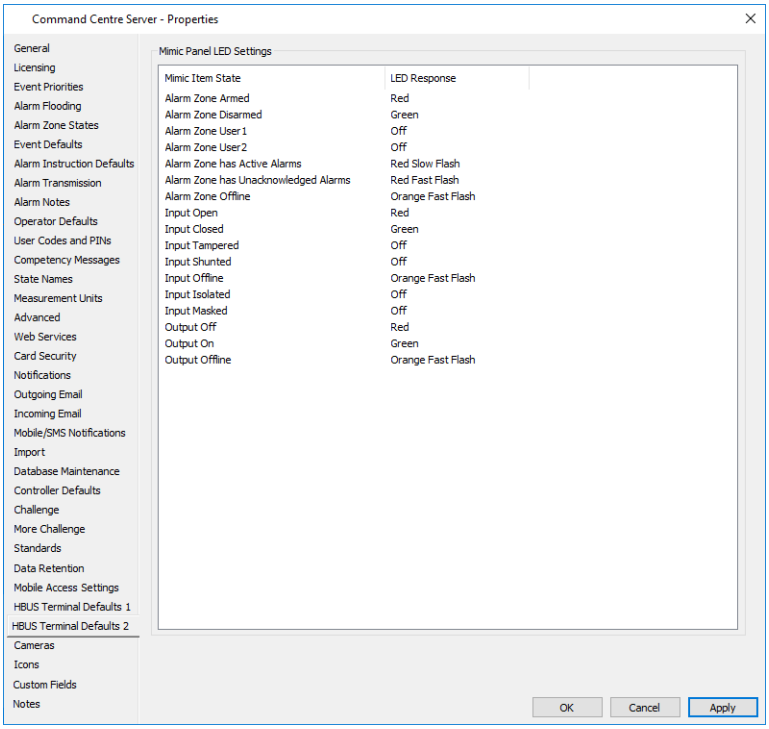
- The above settings are not applicable when using a PIV card at an HBUS Contact Card Reader. The PIV card will be locked after 5 consecutive failed PIN entries.

4. The **Require alarms to be acknowledged at both a Terminal and Command Centre** option is for sites wanting to ensure an alarm is acknowledged or processed locally (by the guard) whilst still requiring the monitoring station to manage alarms in the normal way.

   Ticking this checkbox means alarms that are acknowledged at a T20 or T21 will not display as acknowledged in Command Centre. Likewise, alarms that are acknowledged or processed in Command Centre will not be removed or display as acknowledged at the T20 or T21. **Notes:**

   - Sirens (or other outputs) will only be silenced when the alarm is acknowledged at the T2x and not when it is acknowledged in Command Centre.
   - Events indicate whether the acknowledge or processing was undertaken at the T2x or Command Centre.

5. Click the **HBUS Terminal Defaults 2** tab.



6. Configure the Mimic Panel LED Response for each item state.
   LED Responses are:

   - Off
   - Red
   - Green
   - Orange
   - Red Slow Flash
   - Green Slow Flash
   - Orange Slow Flash
   - Red Fast Flash
   - Green Fast Flash
   - Orange Fast Flash

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.

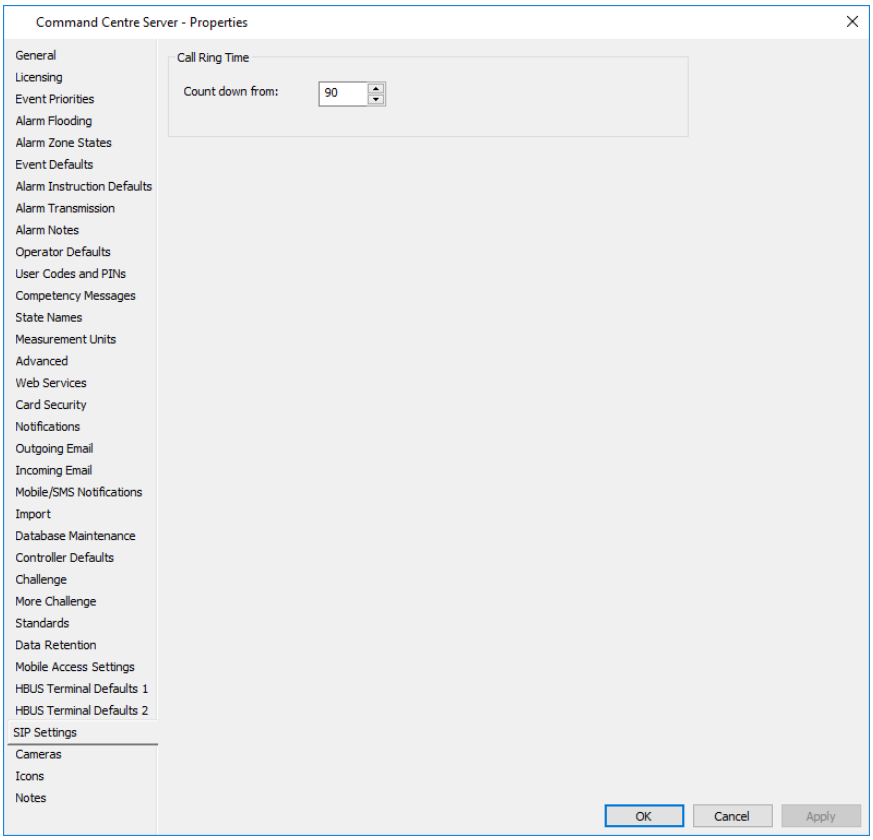
SIP Settings

Introduction

This allows you to edit system-wide settings of the licensed SIP Integration.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **SIP Settings** tab.



3. Configure as required.

Field	Description
Count down from	The **Count down from** setting applies to all SIP Devices. This setting defines the initial 'Seconds Remaining' value for a ringing call in an Intercom Viewer. In other words, it defines how many seconds a call from a SIP intercom will ring for (without being answered) before it is disconnected. Range is 10-600 seconds. **Note:** If an intercom device is configured with its own call timeout, the call will end as per that timeout even if the 'Seconds Remaining' timer has not run out.

4. 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.

Icons

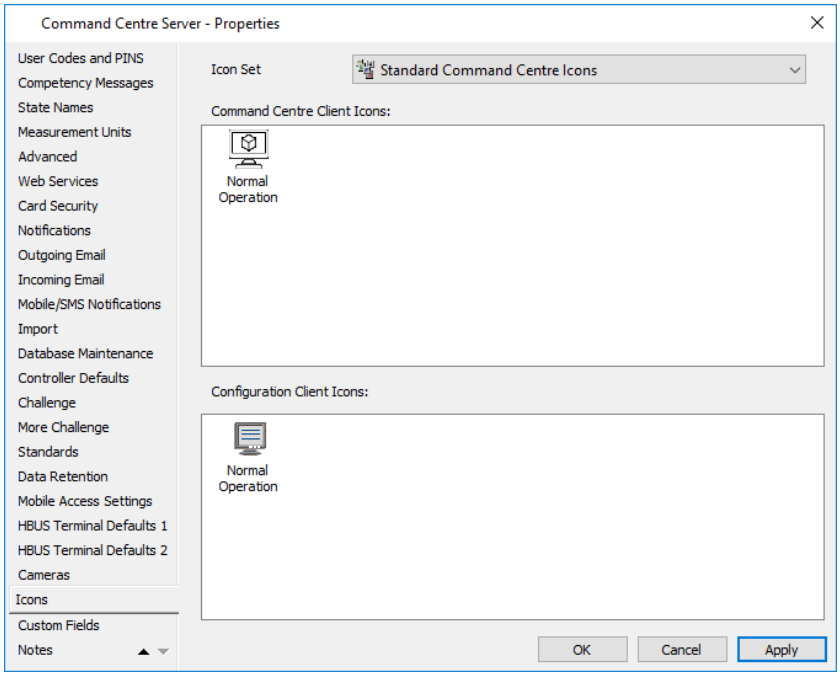
Introduction

This tab enables you to assign an appropriate Icon Set to this Command Centre item. Unlike the rest of the Server Properties tabs, information you set on this tab (and the **Custom Fields** and **Notes** tabs) does not filter through and affect the complete system.

Note: All Command Centre items that can be placed, as an icon, on a Site Plan have the same generic **Icons** tab in their properties.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Icons** tab.



The Icon Set that this Command Centre item belongs to displays in the **Icon Set** field, and the icon(s) that display in the grids represent the various states of this Command Centre item, (i.e. the upper grid displays the icons for the Command Centre Client and the lower grid displays the icons for the Configuration Client).

Note: If there are other Icon Sets that this Command Centre item can belong to, the **Icon Set** drop-down list will display them.

3. If you want to change the Icon Set for this item, select one from the drop-down list. If however there is only the one Icon Set available, you can create a new Icon Set to be used with this item. See ***Creating a new Icon Set*** (on page 19-2) for the procedure.
4. 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.

Custom Fields

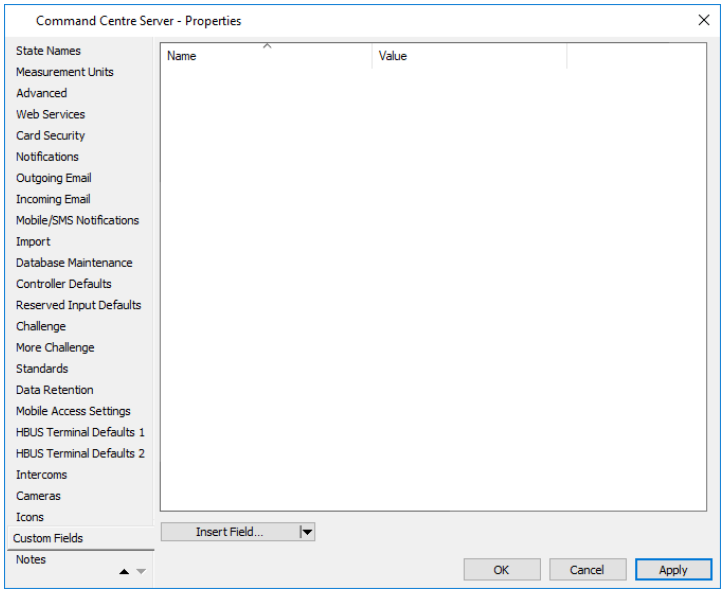
Introduction

All site items with the exception of Cardholders, include a **Custom Fields** tab in their Properties window. This tab allows you to add and assign a custom field value to the site item. Unlike the rest of the Server Properties tabs, information you set on this tab (and the **Icons** and **Notes** tabs) does not filter through and affect the complete system.

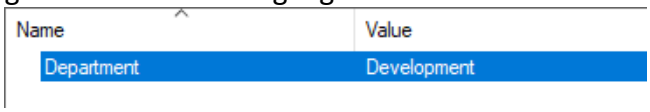
Note: Definitions need to be created first in the Custom Field Types window. See ***Creating a new Custom Field*** (on page 6-83) for instructions.

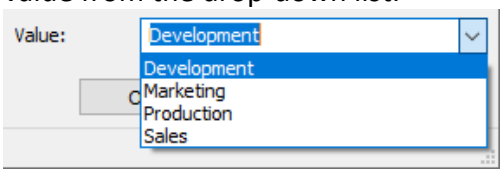
Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Custom Fields** tab.



3. Click on the ▼ of the **Insert Field...** field.
   Note: If no Custom Field Types have been defined in the Custom Field Types window, **Insert Field...** will be disabled.
4. Select a custom field from the drop-down list.
   Note: The drop-down list will include all custom fields that have been created in the Custom Field Types window.
5. Configure as appropriate for the type of custom field you selected.

If it is a...	then...
'Text - List' field,	by default the first **Value** will display for the 'Text - List' custom field in the grid. a) If you require another value, click on the custom field in the grid so it becomes highlighted.  A **Value** drop-down will be presented.

If it is a...	then...
	b) Click on the **Value** field arrow and select the appropriate value from the drop-down list.  c) You can keep adding Custom Fields of the same type with different Values until you have all the values you want. **Notes:** • You can also have fields without values, which will be taken as all values. • The maximum number of values in a 'Text - List' item is ten.
'Boolean' field,	a **Value** checkbox will be presented. Check or uncheck the checkbox. **Note:** You cannot insert a 'Boolean' field more than once.
'Text' field,	a **Value** text box will be presented. Type in your text. **Note:** You cannot insert a 'Text' field more than once.

6. Repeat Step 3 - 5 as necessary.
   Notes:
   - Multiple entries of the same 'Text - List' custom field is allowed as long as each entry has a different **Value**, otherwise the following message will display:
     "Duplicate Custom Fields are not allowed"
   - Entries can be removed by right-clicking on them and selecting **Remove from List**.
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.

Creating a new Custom Field

Introduction

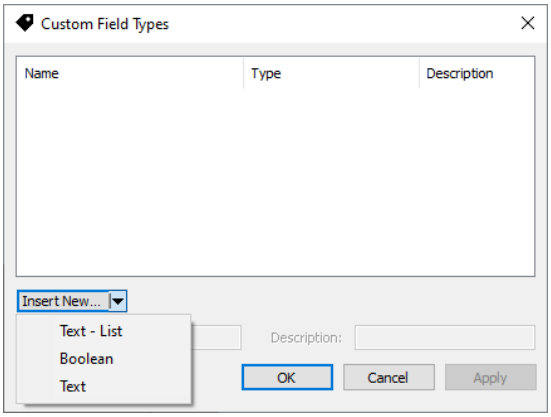
The Custom Field Types provide the ability to tag items in Command Centre for quick identification and in the future, reporting and searching. This procedure describes how to create a Custom Field.

To create or modify a Custom Field and its definitions, operators require the "Edit Site" privilege in the division in which the Custom Field is to be created or modified.

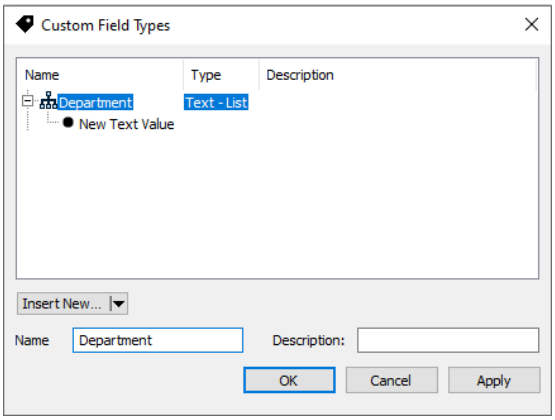
Note: The only item that currently supports Custom Field Types is **Locker**. See ***Locker Management Solution*** (on page 62-1) for more details.

Procedure

1. Click **Configure** from the menu bar, then **Custom Field Types**.
   The **Custom Field Types** Window opens.
2. Click on the ▼ of the **Insert New...** field, and select the appropriate option from the drop-down list.



3. Type in a **Name** (limited to 40 characters) for the custom field, and an optional **Description** (limited to 128 characters).



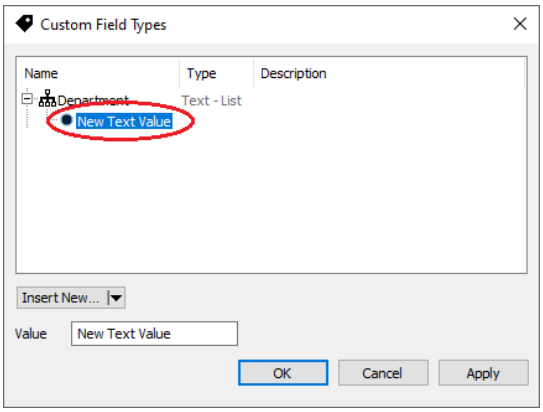
4. Did you select 'Text - List'?

If...	then...
no,	go to Step 5.

If...	then...

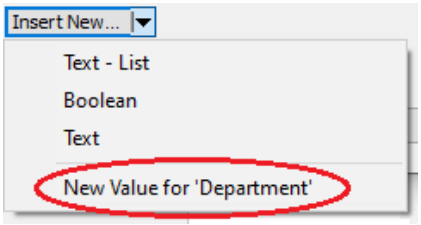
yes,

a) Click on the **New Text Value** in the grid.
A **Value** field displays.



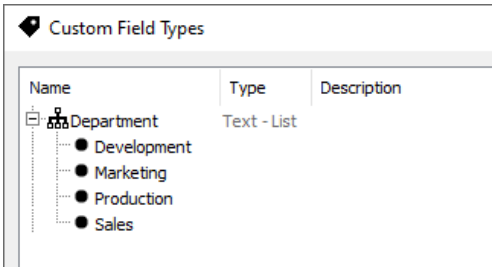
b) Enter a value into the **Value** field.

c) To enter another value, click on the ▼ of the **Insert New...** field.
A new option displays in the drop-down list.



d) Click the **New Value for '<Name>'** option.

e) Repeat Steps c) and d) as necessary.



Note: Entries can be removed by right-clicking on them and selecting **Remove from List**.

5. Repeat Steps 2 - 4 as necessary.
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.

Notes

Introduction

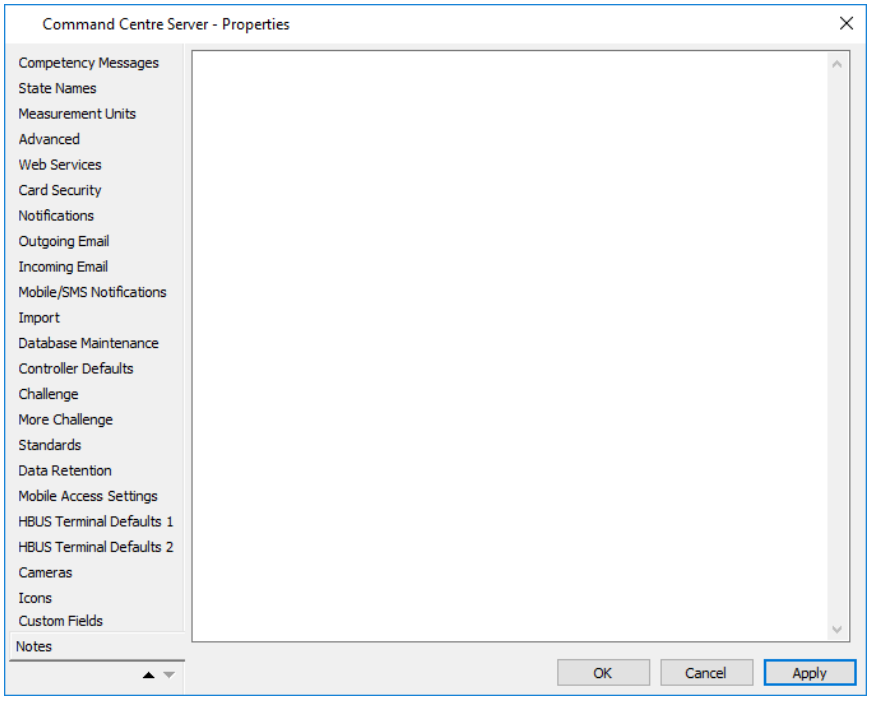
This tab enables you to record notes against this Command Centre item. Unlike the rest of the Server Properties tabs, information you set on this tab (and the **Icons** and **Custom Fields** tabs) does **not** filter through and affect the complete system.

Note: All Command Centre items and Cardholders have the same generic **Notes** tab in their properties. Operator privileges determine whether you can edit the **Notes** tab, (i.e. add information), or only view the **Notes** tab, (i.e. the Notes field will be greyed out, indicating that you cannot edit this tab, but you can see any information already added by other operators). The operator privileges required are as follows:

Action	Operator Privilege required
view Cardholders **Notes** tab	"View Cardholder Notes"
edit Cardholders **Notes** tab	"Edit Cardholder Notes"
view an Command Centre item's **Notes** tab	the appropriate View privilege, (i.e. "View Site" for most Command Centre items, "View Schedules" for Schedules, and "View Access Groups" for Access Groups.
edit an Command Centre item's **Notes** tab	the appropriate Edit privilege, (i.e. "Edit Site" for most Command Centre items, "Edit Schedules" for Schedules, and "Edit Access Groups" for Access Groups.

Procedure

1. Open the **Command Centre Server Properties** window. ***How?*** (see "***Opening the Server Properties window***" on page 6-3)
2. Click the **Notes** tab.



3. Enter any note(s) you want to record. **Notes:**
   - The scroll bar can be used to move through the text, or the normal navigation keys can be used, (i.e. Up and Down Arrows, Page Up and Down, and Home and End).
   - **Right clicking** anywhere in the Notes field will display a context menu with the following options:

Option	Description	Short-cut
Undo	Text can be removed by clicking this prior to clicking **OK** or **Apply**.	Ctrl-Z
Cut	Only enabled when text is selected. The selected text can be cut to the Windows clipboard.	Ctrl-X
Copy	Only enabled when text is selected. The selected text can be copied to the Windows clipboard.	Ctrl-C
Paste	Only enabled when the Windows clipboard contains text, (i.e. text has already been cut or copied). The text can be pasted from the Windows clipboard to the current text-edit cursor position.	Ctrl-V
Delete	Only enabled when text is selected. The selected text will be deleted if clicked.	
Select All	Only enabled when **no** text is selected. Clicking it will select all the text in the Notes field.	

4. 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: Saving changes results in an operator event being created, identifying the cardholder/Command Centre item that was changed, who changed it and when, but not what the changes were.

Chapter 7: Card Types

Card Types are required in order to allow you to create New Cards for Cardholders. This option creates card types that will be used in the Command Centre system.

Inactive Card Expiry

The "card expiry" feature allows the life of a card to be specified by defining a "From" time and date as well as an "Until" time and date. Cards with these defined are therefore enabled between those two points in time and are referred to as Scheduled Card Expiry. The "Inactive Card Expiry" feature provides additional flexibility in the way card expiry can be defined.

Inactive Card Expiry enables the automatic disabling of cards, invoked after a period of card inactivity, within a Command Centre controlled site. The length of the period of inactivity is user configurable. This feature applies to both Controller and Commander technologies.

A card that has the Inactive Card Expiry feature enabled shall be disabled if no successful access events occur for that card over the configured inactivity timeout for the card's type. A successful access event is one of:

1. "Door Access Granted"
2. "Elevator Access Granted"
3. "Card Exit Granted"

A number of card authorisation features take precedence over Inactive Card Expiry, as follows:

- If a cardholder is de-authorised, (i.e the "Cardholder Authorised" checkbox is unchecked on the **Card** tab), then all of the cardholder's cards are disabled, irrespective of the "Inactivity" status.
- If a card is disabled, (i.e the "Card Enabled" checkbox is unchecked on the **Card** tab), then that card is disabled irrespective of the "Inactivity" status.
- If a card is expired according to the configured "From/Until" activation period on the **Card** tab, then the card is expired irrespective of the "Inactivity" status.

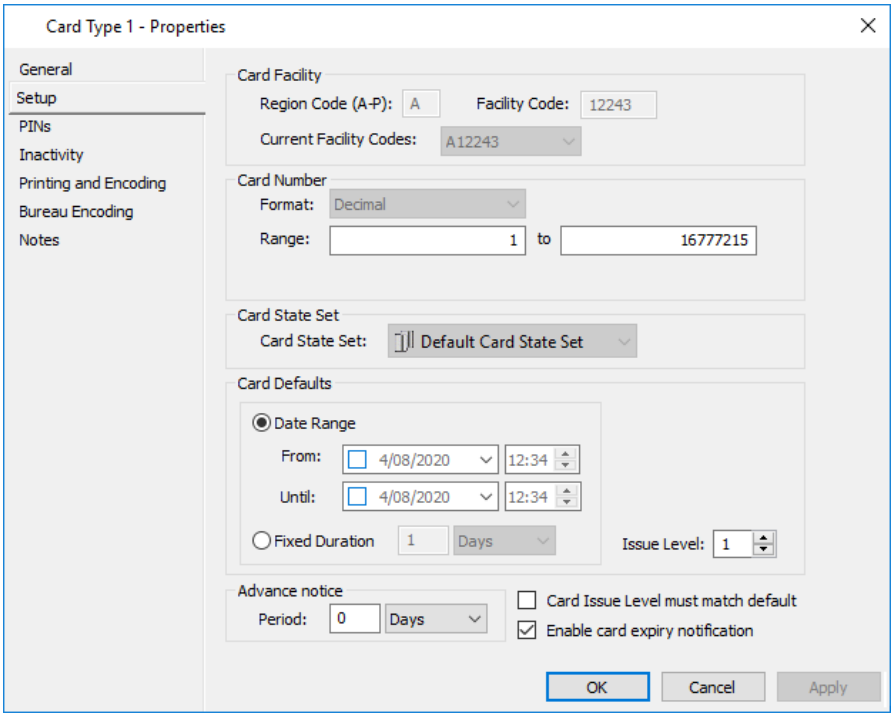
Setting up Card Types

Introduction

This procedure details how to set up a new Card Type. The "Configure Site" or "Edit Card Types" operator privilege is required to perform this procedure.

Procedure

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...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.



Your site Facility Code is entered in the **Card Facility** section on this tab. Command Centre references the Facility Code to identify cards for use on site.

Gallagher Group Limited supply sites with Facility Codes, and ensure different sites have different facility codes. This allows several sites to use identical card numbers.

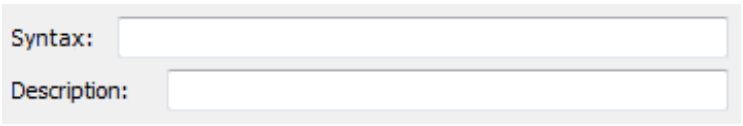
5. If your site Facility Code has already been entered, then select it from the **Current Facility Codes** drop-down box.
   OR
   If you wish to enter your Facility Code, then enter the letter representing the **Region Code** for your Facility Code, and enter the number in the **Facility Code** field.

Notes:

- Facility Codes can only be used on one card technology.
- One Facility Code cannot be used by two card types that have different card number formats. This is due to the difficulty in converting the byte array representation of a card number to its displayable string representation.
- Gallagher Command Centre can support up to 256 Facility Codes on Gallagher Controller 6000s and 7000s.

6. The settings configured in the **Card Number** and **Card Defaults** sections will be used when you allocate a new card to a cardholder. They can then be overwritten if required.

   In the **Card Number** section select the appropriate option from the **Format** drop-down list:
   Note: The **Format** drop-down list is disabled once the Card Type is created and saved.

If you select...	then...
Decimal	the following additional fields display in the **Card Number** section:  Enter the range in the **Range** fields. The Minimum Card Number is 1, and the Maximum is limited to approximately 605 characters in length, which is the number of digits for the result of 2^2008. (Defaults = 1 to 16,777,215) **Note:** For 24-bit Gallagher cards, the number range has a limit of 1 to 16,777,215. For Magstripe card types, the number range has a limit of 1 to 65,500.
PIV	no additional fields populate the **Card Number** section.
Text	the following additional fields display in the **Card Number** section:  **a)** If you want to force the card number format to fit a regular expression for the Card Type, enter a syntax string into the **Syntax** field. This string will be used to validate a card number that is entered by an Operator. **Notes:** • Refer to ***Sample Regular Expressions*** (on page 7-8) for a list of example regular expressions. • The syntax string can be changed after the Card Type

If you select...	then...
	is saved, allowing the Operator to initially configure a strict pattern and later add additional patterns if requirement changes. ***For example:*** Card Numbers for alphanumeric vehicle number plates may initially support 2 English letters and 4 number digits, (e.g. 'AB1234') and later support 3 English letters and 3 number digits, (e.g. 'ABC123').

b) Enter a description of the syntax in the **Description** field.
Note: This message will be displayed to an operator if the value entered cannot be saved because it doesn't meet the regular expression validation.

7. Select the appropriate **Card State Set** (if only one exists it will default) to be associated with this card type, from the drop-down box.
Note: Once the Card State Set is assigned to the Card Type here and saved, it cannot be changed. Bulk changes can be used to change the Card Type if an alternative set of Card States is required.
8. In the **Card defaults** section you can activate the card 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 cards of this type will be activated and expire in the From and Until fields. **Notes:** • If you do not enter a date in the **From** field, when a cardholder is issued a card of this type and the card is enabled, activation will be immediate. • If you do not enter a date in the **Until** field, the card 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 will be determined from the assignment date with the configured offset / duration.

When a card of this type is assigned to a Cardholder, (i.e. on the **Cards** tab of a Cardholder's properties in Configuration Client, or on the **Cardholder Cards** tile in Command Centre Client), the **Until** Date will reflect the expiry date configured here.

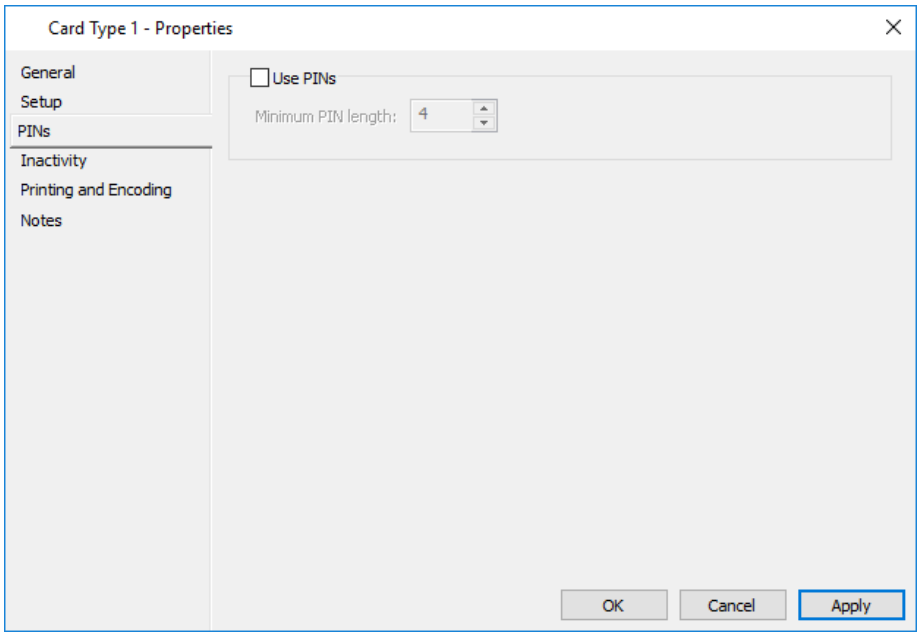
9. The **Issue Level** field allows the issue number to be incremented if a card is replaced, instead of needing to go through the process of creating a new card. (Range = 1 to 15)

For example: A card may need to be replaced if the cardholder has lost their card.

10. The **Advance notice** 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.
11. Check the **Card Issue Level must match default** checkbox if required.
    Notes:
    - When checked, the **Issue Level** field becomes disabled.
    - This setting can be changed again after the Card Type is saved if required.
    - If you are using the Salto integration and card numbers in 26 bit Wiegand format, changing the Issue Level on a card assignment will have no impact on a Cardholder's ability to gain access through a Salto Door. Hence it is advised that you configure a default Issue Level (i.e. '1') by checking the **Card Issue Level must match default** checkbox for all encoded cards using the 26 bit Wiegand format.
12. Do you want to enable card expiry notification?

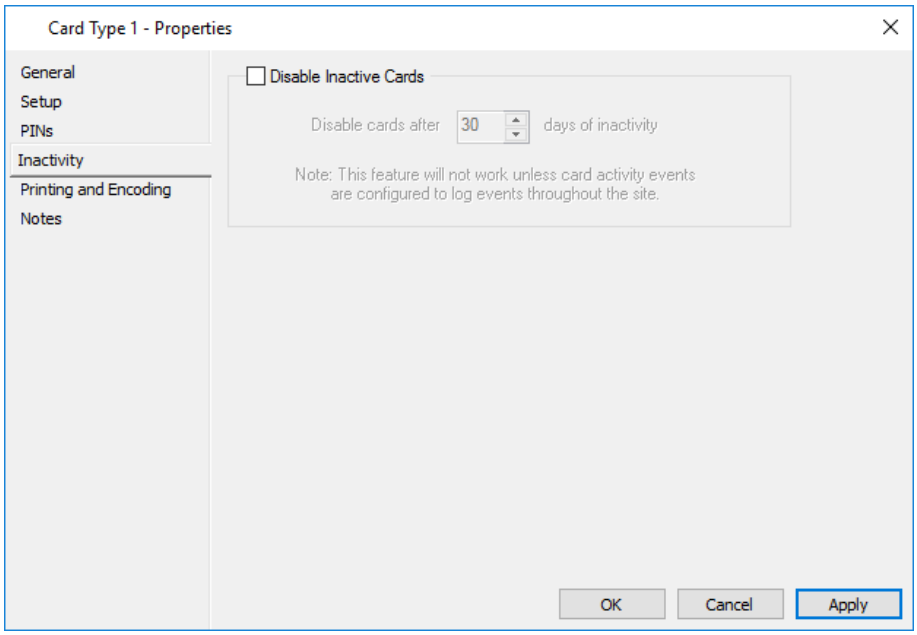
If...	then...
yes	**a)** Set the **Period** to the value that is required to represent the number of days, weeks, months or years prior to card expiry to initiate the warning notification. **b)** Ensure the **Enable card expiry notification** checkbox remains checked.
no	leave the **Period** as 0 days, and uncheck the **Enable card expiry notification** checkbox.

13. Click the **PINs** tab.



This screen enables you to define whether PINs are enabled or disabled for the card type. If you choose not to use PINs, when cards of this type are encoded a user defined PIN cannot be entered by the operator.

14. If you want to use PINs, check the **Use PINs** checkbox and set the Minimum PIN length.
    (Default = 4 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 for this Card Type.
    - 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.
15. Click the **Inactivity** tab.



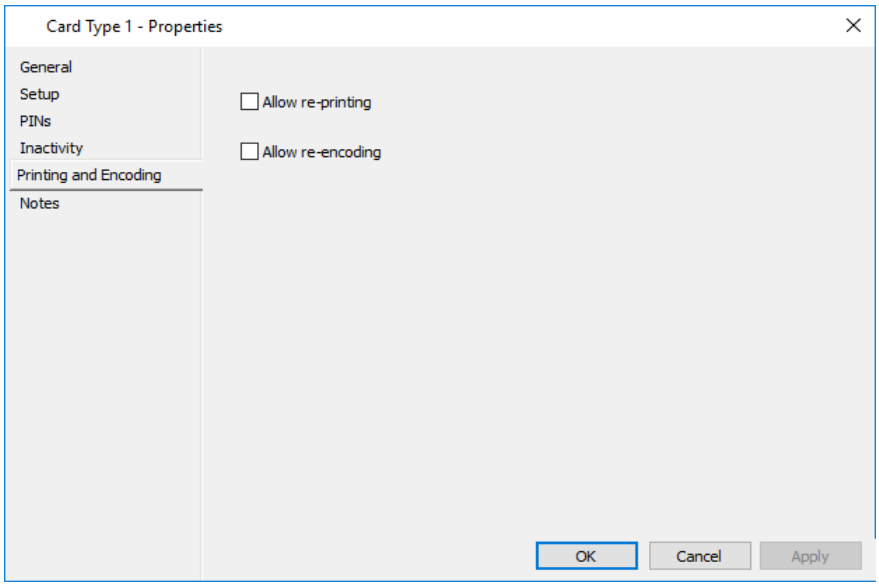
16. Do you wish to enable the Inactive Card Expiry feature?
    Note: All cards of a particular type shall share a common inactivity timeout if enabled.

If...	then...
yes	Check the **Disable Inactive Cards** checkbox. Go to Step 16.
no	Leave the **Disable Inactive Cards** checkbox unchecked. Go to Step 17.

17. 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 27/11/2003 at 16:10:15; if not used these cards become disabled on 28/11/2003 at 16:10:15).

- This feature will not work unless card activity events are configured to log events throughout the site. Cardholders will expire regardless of activity because the system can't see the event activity. (Refer to ***Event Defaults*** on page 6-12 for further detail.)

18. Click the **Printing and Encoding** tab.
    Note: The **Printing and Encoding** tab will only be visible if your site has Photo ID with card encoding included in their license file.



    This screen enables you to define whether PINs are enabled or disabled for the card type.

19. By default the system prevents the identification details, (i.e. Facility Code, Card Number and Issue Level) of a card from being re-printed or re-encoded, as it is generally not desirable to allow two physical cards to be printed or encoded with the same details. This prevents the situation where there are two physical cards with the same ID that can be used to gain access and to prevent additional cards being printed and used fraudulently as visual ID. However, there are some types of cards a site may need to be able to re-print and/or re-encode the details of unrestricted. In this situation, check the **Allow re-printing** and/or **Allow re-encoding** checkboxes to override this behaviour when a Print or Encode action is selected for a Card of this type.
20. Click the **Custom Fields** tab if you want to add and assign a custom field value to this card type. 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 this card type. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
22. Click **OK** to 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 Card Type is configured and ready for use.

Sample Regular Expressions

The following table shows some sample regular expression syntaxes that may be configured as the syntax strings for a Card Type of the Text Card Number Format:

Pattern	Sample Card Numbers	Description
(empty)		The syntax string is unspecified. Effectively the same as " ^.*$" (any characters).
^[A-Z]{2}[0-9]{4}$	AB1234	Vehicle number plate with 2 English upper case letters plus 4 decimal digits, (e.g. the old 'normal' New Zealand vehicle plate number).
^[A-Z]{3}[0-9]{3}$	ABC123	Vehicle number plate with 3 English upper case letters plus 3 decimal digits, (e.g. the new 'normal' New Zealand vehicle plate number).
^([A-Z]{2}[0-9]{4}|[A-Z]{3}[0-9]{3})$	AB1234 ABC123	The combination of the above two.
^[A-Z0-9]{1,6}$	A 0 A1 1A A1A 1A1 A12B 1ABC2 A12345 AB1234 ABC123 ABCDEF 123456 123ABC 12ABCD	• Vehicle number plate with 1 to 6 alpha-numeric characters. • English letters and decimal numbers can appear anywhere in the string. • English letters are in upper case.

Below are some of the best practice suggestions for configuring a regular expression syntax string:

- Always specify the start of the string, (i.e. '^') and the end of the string, (i.e. '$').
- For alph-anumeric Automatic Number Plate Recognition (ANPR) purpose, use either upper cases or lower case, not both at the same time.

Chapter 8: Enrolment Wizard and Templates

The Enrolment Wizard feature is made up of two parts:

- An Enrolment Template, (i.e. a configuration tool for defining the Card Type and some of the behaviour of the Enrolment Wizard), and
- The Wizard itself.
  The Wizard is intended for use on large sites such as universities and allows them to print and encode cards during enrolment in minimum time.

The Enrolment Template must be configured before using the Enrolment Wizard.

Configuring Enrolment Templates

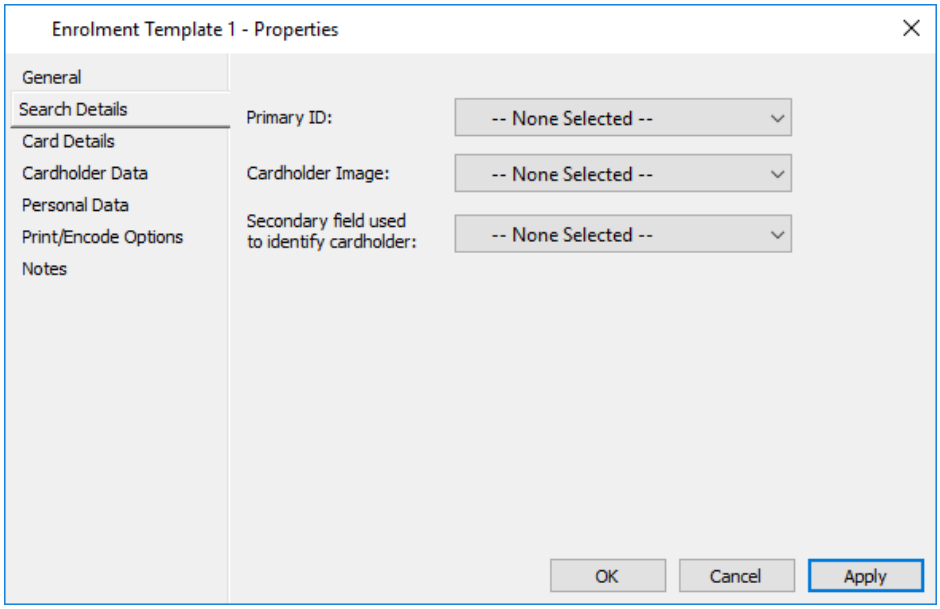
Introduction

Enrolment Templates encapsulate all of the information that makes a particular type of Enrolment Wizard unique. Your license file has stored in it the maximum number of Enrolment Templates your site is allowed. Once that number is reached, the option to add new Enrolment Templates is disabled.

You must have the "Edit Enrolment Template" operator privilege to create, edit and delete Enrolment Templates.

Procedure

1. Click **Configure** from the menu bar, then **Enrolment Templates**.
   The **Enrolment Template** List Window opens (in grid view).
2. **Right click** and select **New...Enrolment Template**.
   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 **Search Details** tab.

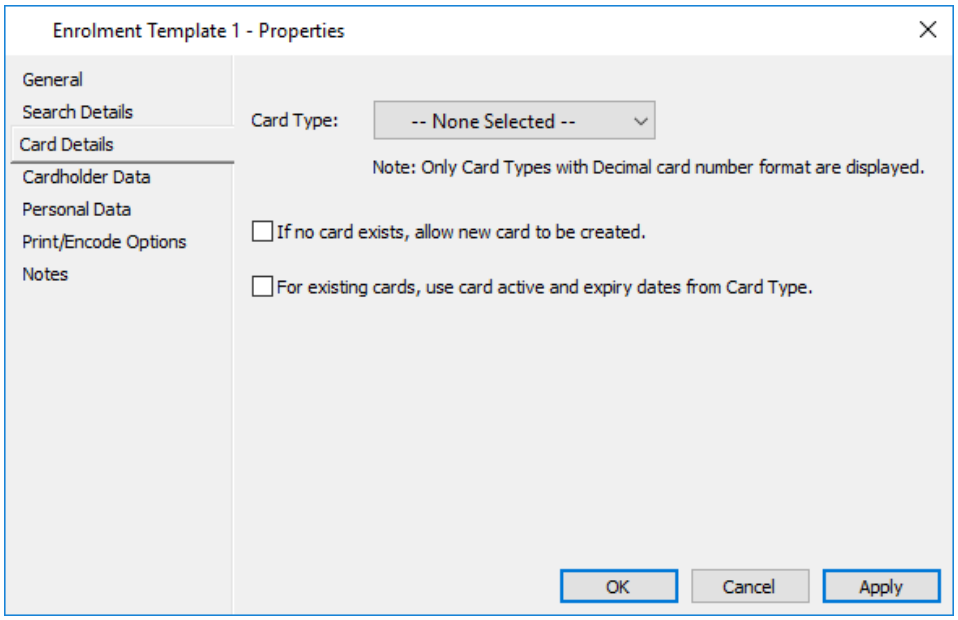


5. Set the search criteria as required.

Field	Description
Primary ID	The PDF selected here will be used as the primary cardholder identifier. **Note:** The selection of a Primary PDF is compulsory and can not be an image PDF.

Field	Description
Cardholder Image	The PDF selected here from a list of image PDFs, will store the cardholder image. **Note:** The selection of a Cardholder Image PDF is not compulsory.
Secondary field used to identify cardholder	The PDF selected here will be used to provide additional information for identifying the cardholder when a search returns multiple matching records. **Note:** The selection of a secondary PDF is not compulsory and can not be an image PDF, or the same PDF used for the Primary ID.

6. Click the **Card Details** tab.

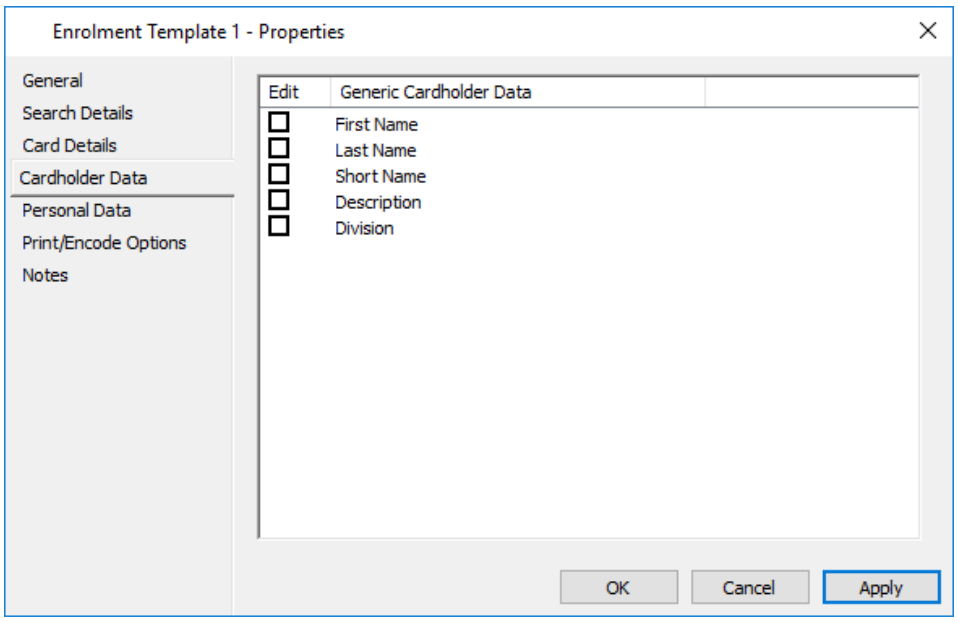


7. Set the card details as required.

Field	Description
Card Type	The card type selected here shall limit existing or new card details that are displayed or created in the Enrolment Wizard to cards of the selected Card Type. Selection of a Card Type is compulsory. **Note:** The Card Type selection is limited to those with Decimal card number format.
If no card exists, allow new card to be created	If this tick-box is checked, a new card can be created if there is no existing card data (of the appropriate Card Type), for a selected Cardholder.

Field	Description
For existing cards, use card active and expiry dates from Card Type	If this tick-box is checked, the active and expiry dates from the Card Type will be used for existing card details, when retrieved in the Enrolment Wizard.

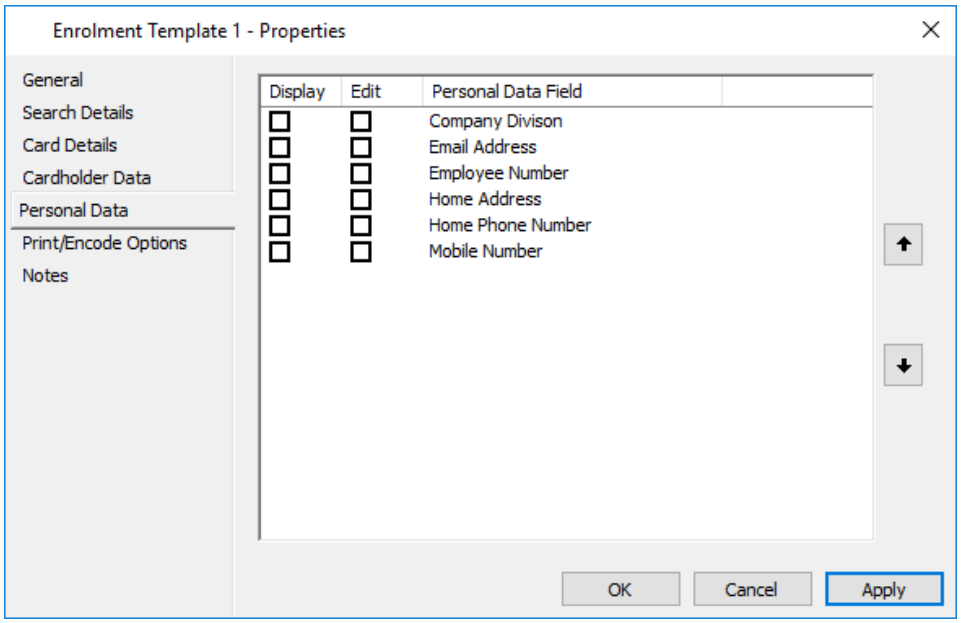
8. Click the **Cardholder Data** tab.



This screen displays a list of generic cardholder data. Each field has a corresponding checkbox to specify whether or not the operator running the Enrolment Wizard will be able to edit the fields.

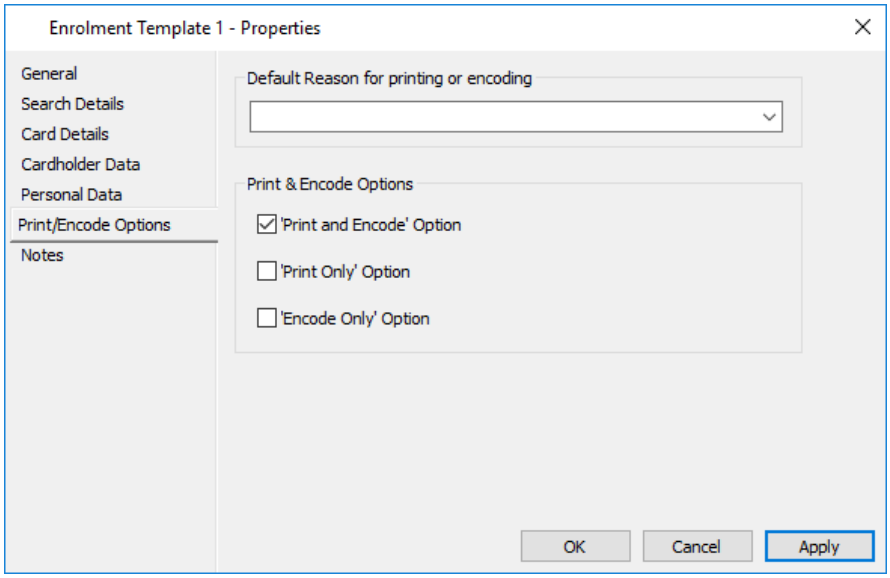
9. Check the **Edit** tick-boxes for the fields you wish to be editable in the Enrolment Wizard.

10. Click the **Personal Data** tab.



This screen displays a list of non-image PDFs and tick-boxes that specify whether each field may be edited or displayed.
Note: "Revealable" and "Revealable and Editable" Personal Data Fields are not supported options in Enrolment Templates. They are displayed as "Edit".

11. Check those **Edit** and **Display** tick-boxes for the fields that you wish to be visible/editable in the Enrolment Wizard.
12. Sort your selection of PDFs by clicking on a PDF and using the **arrow** buttons to the right of the list box to move it.
The order you define here will be the order in which the PDFs will display (excluding the Primary ID PDF), when the Enrolment Wizard is run.
13. Click the **Print/Encode Options** tab.



14. Set the options as required.

Field	Description
Default Reason for printing or encoding	A default reason for printing and/or encoding can be selected from the drop-down list, or you can type a default reason in this field. This reason will be displayed in the Enrolment Wizard before a card is printed and/or encoded. **Note:** The drop-down list of reasons are pre-configured via **Configure**>**Photo ID**.
Print & Encode Options	One or more of these options can be selected so they become available in the Enrolment Wizard. **Note:** Rather than use the Enrolment Wizard to print and/or encode cards, you may wish to use it to update cardholder information. If this is the case, by not selecting any of these options, when you use the Enrolment Wizard you will **not** be given the option to print and/or encode.

15. Click the **Notes** tab if you want to add a note(s) about this Enrolment Template.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
16. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

A new Enrolment Template is created.
Notes:

- Each Enrolment Template that is created will show as an entry in the **Wizards** menu on the main window. When an operator logs on, Command Centre queries for all the available wizards and places them into the **Wizards** menu. This means that if you create or delete a wizard template the change will not be reflected in the **Wizards** menu until you log off and then back on again.
- If any of the compulsory fields have not been set, an error message will display and the Template will not be saved.

Using the Enrolment Wizard

Introduction

Enrolment Wizards allow you to search for and identify a cardholder, then encode and print a card specific to that cardholder. The Wizards work in conjunction with Photo ID, which determines the layout of the card type. Refer to Photo ID for further detail.

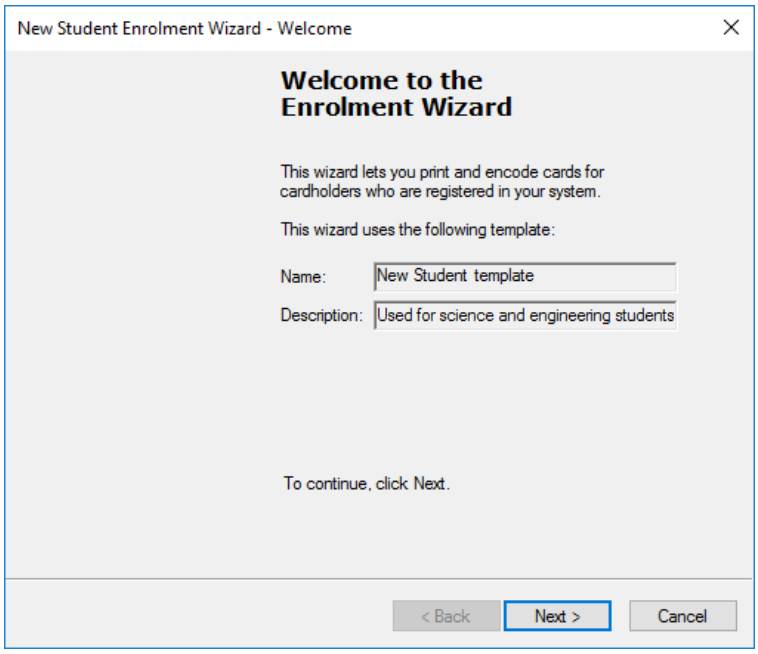
Before you begin

- An Enrolment Template must be configured first. See ***Configuring Enrolment Templates*** (on page 8-2) for the procedure.
  Each Enrolment Template created will have a separate entry on the **Wizards** menu, which when selected starts the Enrolment Wizard with the associated Template options applied.

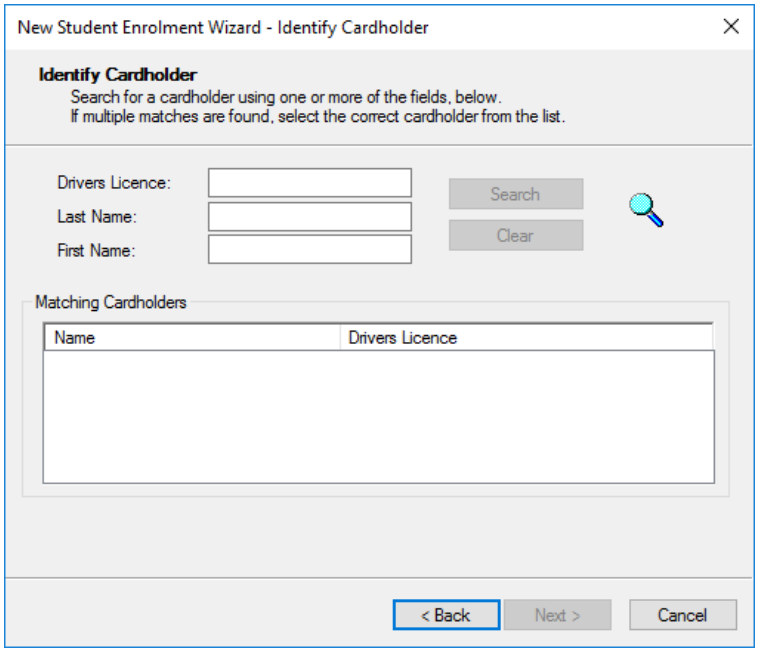
  Note: If you do not configure the Enrolment Template prior to using the Enrolment Wizard you will not be given any Enrolment Wizard options in the **Wizards** menu.
- For Enrolment Wizard entries to display on the **Wizards** menu you must have the "View Cardholders" operator privilege and the associated Enrolment Template must be within your Division.

Procedure

1. Click **Wizards** from the menu bar.
   Each Enrolment Template that has been created will show as an entry in the **Wizards** menu.
2. Click the appropriate **Enrolment Wizard** entry.
   The **Welcome** screen of the Enrolment Wizard displays, indicating which Enrolment Template is being used in the Name field and in the Title bar of each screen of the wizard.



3. Click the **Next** button.
   The **Identify Cardholder** screen of the Enrolment Wizard displays.



   This screen can be used to search for and identify the cardholder for which a card will be printed.

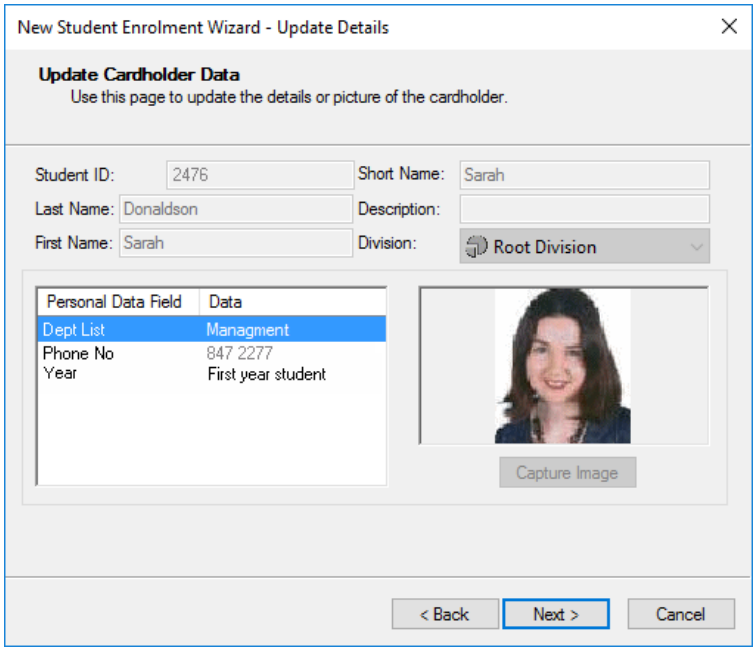
4. To locate the cardholder, enter the First and/or Last Names of the Cardholder, and/or the PDF which was selected as the 'Primary ID' in the Enrolment Template. In the case of the example screen above, the 'Primary ID' PDF is **Personal Data Field**.

   Notes:

   - If no data is entered in a particular field, that field will be excluded from the search.

- If the Primary ID is a numeric PDF, wild card searches will not work. Instead, the exact number must be entered.
- The search is not case sensitive.

5. Click the **Search** button.
6. If the search retrieves more than one cardholder, highlight the required Cardholder record. This can be done by either moving the pointer to the correct record and clicking the mouse, or by using the arrow keys to move up or down within the list.
   Note:
   Only the first one hundred matches are returned.
7. Click the **Next** button.
   The **Update Cardholder Data** screen of the Enrolment Wizard displays.



   Details of the identified Cardholder populate this screen along with an Image PDF if defined in the Template.
8. Update any Cardholder data that is incorrect or incomplete.

   Notes:

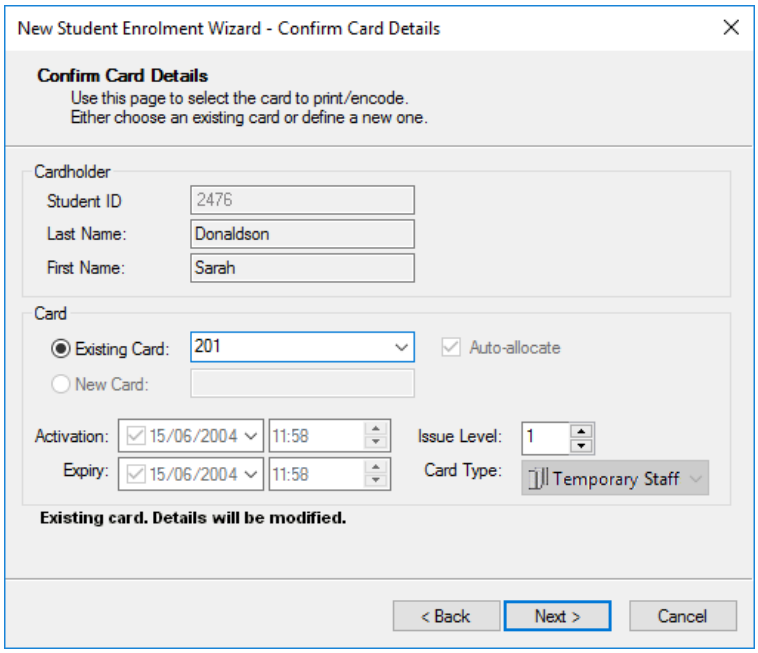
   - This is only possible for fields that have been configured as editable in the Enrolment Template.
   - For “text - list” Personal Data Fields you can highlight the PDF and make a selection from the drop-down list (pressing <**Alt**>+<**DownArrow**> expands the drop-down list).
9. Is the existing Image PDF displayed the one you wish to use, or would you like to update the existing Image PDF?

If you wish to...	then...
use the Image PDF displayed	go to Step 15.
update the existing Image PDF	click the **Capture Image** button. The **Capture Image** window displays. It will be blank if it is the first time you have captured or loaded an image on this workstation, otherwise it will default to the last method of capturing you used.

10. If you have a blank Capture window, or you want to change the method of capture, click within the drop-down selection box and select the camera you want from the list of devices attached to the PC.
11. Click the **Capture...** button.
12. You can either load an existing image, or capture a new image.

If you want to...	then...
load a previously saved image	• Select **Load from file...** from the drop-down list. The **Select image to load** window displays. • Path your way to the location of the image you require, and click the **Open** button. The image displays in the **Capture Image** window. **Note:**  To adjust the contrast and/or brightness of a saved image, right click and move the indicator as necessary.
capture a new image	depending on how the camera you are using has been installed on the PC, it may give you 'live' video, in which case if you are cropping you have to crop a moving image. Alternatively, the camera may display it's own window in which case you 'acquire' the image, which then brings it back to the **Capture Image** window as a static picture which you can then re-crop. **Note:** If you need to adjust the appearance of the image, right click with the image displayed, and click **Configure Source**. A window displays which enables you to adjust the image, (e.g. sharpness, brightness, colour, etc.)

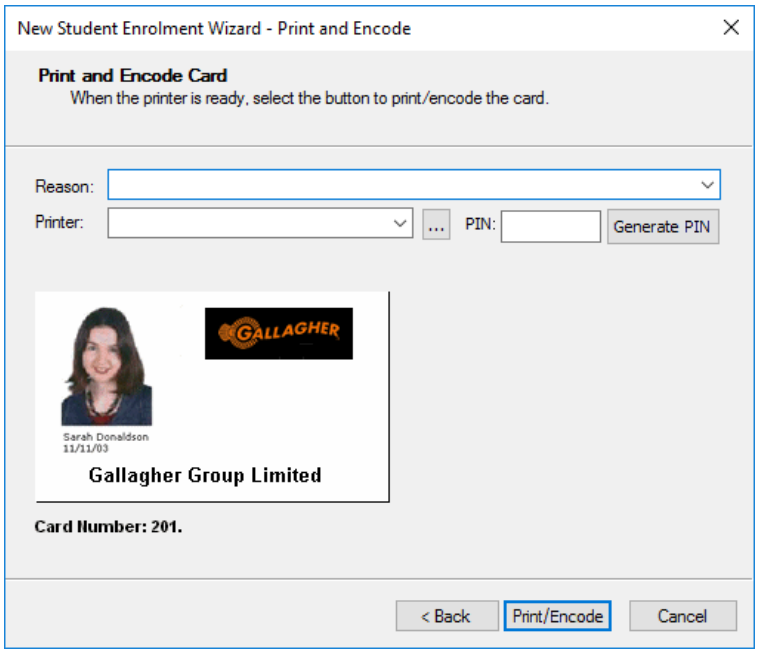
13. Reposition the cropping frame.
14. Click the **OK** button.
    The **Capture Image** window closes.
    The captured image now displays in the **Update Cardholder Data** screen of the Enrolment Wizard.
15. Click the **Next** button.
    The **Confirm Card Details** screen of the Enrolment Wizard displays.



The details of the card to be printed/encoded display on this screen. Depending on the settings configured on the **Card Details** tab of the Enrolment Template either:

- one of the radio buttons will be enabled, (i.e. **Existing Card** or **New Card**), or
- neither radio button will be enabled if the cardholder has no existing cards and the Enrolment Template has not been set up for new cards to be created.

16. Confirm the details displayed, and change any that are incorrect.
17. Click the **Next** button.
    The **Print and Encode Card** screen of the Enrolment Wizard displays.



A default reason for printing and/or encoding the card will be displayed if this was configured in the Enrolment Template.
If there are other reasons for printing and/or encoding configured in Command Centre, you can select another one from the drop-down list or type in your own reason into the text field. The reason selected will be logged in the event details.

18. Select the required **Printer** from the drop-down list.
    Note:
    You can only select a printer/encoder that is appropriate for the action you are performing, (e.g. if your card has no encoding object, then no encoding printers will appear in the drop-down list).

19. If PINs have been enabled for the Card Type the **PIN** field and **Generate PIN** button will be enabled.
    Either:

    - manually type a PIN number into the **PIN** field.
      Note: The PIN will display as a row of X's and as you enter a PIN the message *"PIN must be between <number> and 8 digits"* appears, <number> being the length set against the Card type. 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 while in the Print and Encode Card step of the wizard. If you have checked the **Store user PINs for later viewing** checkbox (on the **Card Security** tab of the Server Properties), the PIN will be stored and can therefore be re-viewed. Generated PINs will be of length equal to the minimum PIN length set against the Card type.

20. Select the **Print and Encode option**, (i.e. 'Print and Encode', 'Print Only' or 'Encode Only'), from the drop-down list provided.
    Note:
    This field will only appear if more than one of the Print and Encode options were selected in the Enrolment Template.
21. Click whichever of the following buttons is displayed:

Button	The card...
Print/Encode	is encoded and prints to the default printer.
Print	prints to the default printer.
Encode	is encoded by the default printer.
Next	and/or cardholder details are updated.

Result

The Enrolment Wizard automatically returns to the **Identify Cardholder** screen, ready for another Cardholder to be identified.

Chapter 9: System Division

Understanding System Division

System Division allows one site to be divided into smaller divisions and sub-divisions. Each sub-division can manage their own security needs. It is especially desirable for:

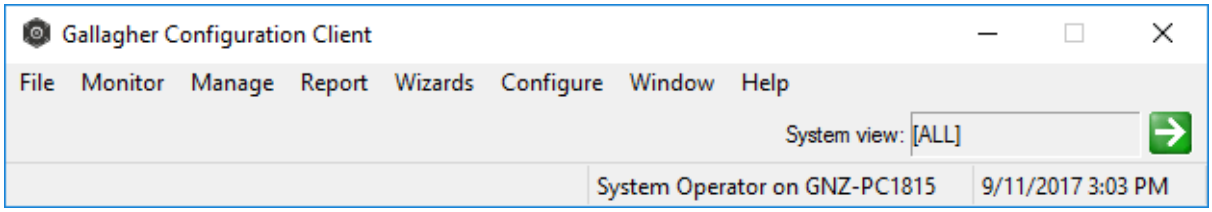
- multi-tenanted buildings where each tenant wishes to manage and monitor their own security
- very large enterprise-wide systems where it is more practical to divide the site up for ongoing management and monitoring, (e.g. dividing the site up into geographic zones).

Your site licence will determine the number of divisions you can have.

Operators and Divisions

Operators are only able to view, manage and report on the components in their division, in line with their operator privileges. Generally, they do not have access to components in other divisions except in certain situations, (e.g. enabling cardholders to have access through a shared foyer area in a multi-tenanted building). See ***Cardholder Management across Divisions*** (on page 9-5) for further detail.

With the "Select System View" privilege an operator is able to restrict their view of the system. When they logon to Command Centre their system view selection, retained from their last log off, displays in the **System view** field on the main window. See ***Restricting System View*** (on page 2-11) for further details.



Refer to ***Operator Privileges*** (on page 37-1) to check you have the correct operator privilege level for working with Divisions.

Creating new items

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

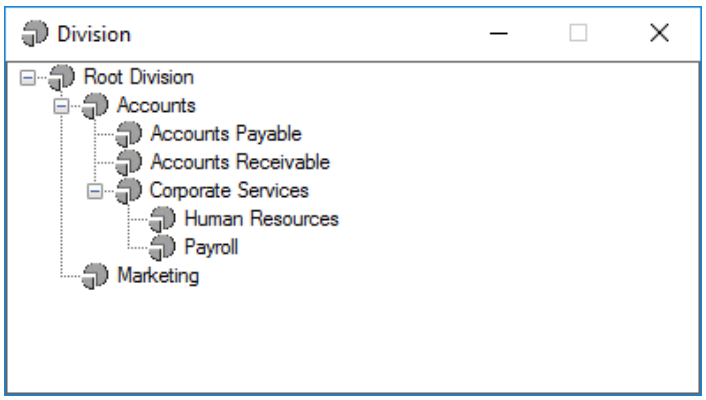
Divisions and Lineage

Lineage is a concept concerned with the inheritance of privileges between parents and children, and affects two areas of Command Centre:
- Access Groups
- Divisions

The procedure for setting up Lineage is the same for both Access Groups and Divisions. However, to some degree, lineage works in opposite ways for these two areas. This topic explains how lineage works for Divisions. See ***Access Groups and Lineage*** (on page 34-2) for an explanation of how it works for Access Groups.

Inheritance of Division Privileges

Privileges in a Division come courtesy of membership of an Operator Group. As a member of an Operator Group, if you have privileges in a particular Division, you automatically have those same privileges in its child division(s).



In this example let's say that you belong to an Operator Group that gives "Edit Cardholders" privilege in the Corporate Services Division. This means you will also have "Edit Cardholders" privilege in the Human Resources and Payroll Divisions (because they are child Divisions of the Corporate Services Division).

You would not have "Edit Cardholders" privilege in either the Accounts or Marketing Divisions as they are at the same level in the hierarchy to the Corporate Services Division.

Notes:

- Take notice of the **Root Division** in the above example. If you belong to an Operator Group that gives a privilege in the Root Division, you have this privilege in every Division (as every Division is a child of the Root Division).
- The **Division** List Window displays in tree view, which is achieved via the **Lineage** tab when you set up System Divisions.

As part of the configuration of a Division you can configure Lineage functionality. See ***Setting up System Divisions*** (on page 9-3) for the procedure.

Setting up System Divisions

Introduction

Entities that can be divided include:

- Cardholders
- Access Groups
- Site Items, e.g. doors, relays, alarm zones
- Reports
- Action Plans
- Operators and Workstations
- Calendars

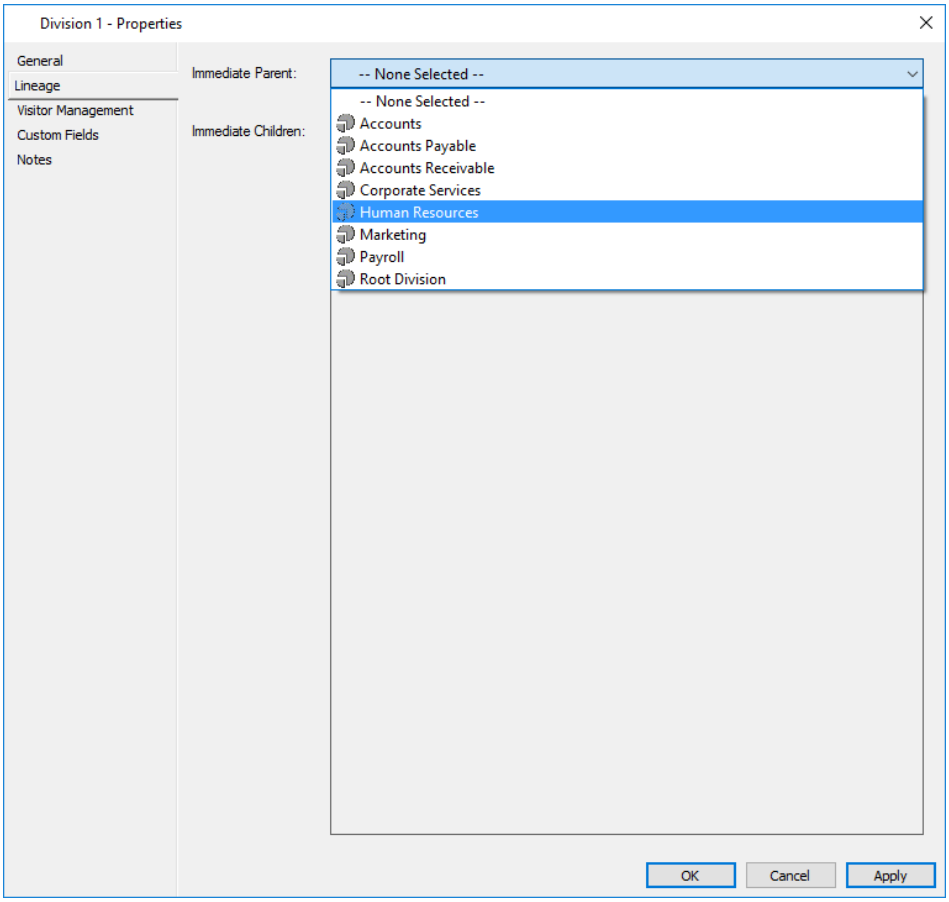
The "Configure Site" or "Edit Divisions" operator privilege is required to set up divisions.

Notes

- It is important that any divisions are formalised prior to the commencement of configuration work.
- Your site license will determine the number of divisions you can have, therefore once you have added all you are allowed, the option to create more will be disabled.

Procedure

1. Click **Configure** from the menu bar, then **Divisions**.
   The **Division** List Window opens (in tree view).
2. **Right click** and select **New...Division**.
   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 **Lineage** tab.



5. Select the "Immediate Parent" division from the drop-down list.
6. Click the **Custom Fields** tab if you want to add and assign a custom field value to this division.
   For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
7. Click the **Notes** tab if you want to add a note(s) about this division.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
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 new system division is created.

Note:
This new Division defaults into the "Immediate Children" box on the Lineage tab of the Division you selected as the "Immediate Parent".

Cardholder Management across Divisions

Introduction

This topic details how to deal with divisions when setting up:
- multi-tenanted buildings, and
- multiple sites with common Cardholders

Multi-tenanted building

In a situation where the system is split across multiple divisions, there may be a common shared door that all Cardholders need access to, (e.g. this may be a Foyer door). For tenants to be given access by the Tenant Operator the system may be set up as follows:

Explanation

Have a 'Root' Operator add Access Groups for each tenant, then add the common door access to that. The Access Group will be in the Tenant Division which is visible to the Tenant Operator and able to be applied to the Tenant Cardholders. Because Access Zone(s) and Schedule(s) are in the 'Root' Division, the Tenant Operator will not be able to add them to the Access Group.

Warning: The Tenant Operator can 'see' any Access Zone and Schedule, and they may be able to remove them. However, if they are accidentally removed, they would have to be restored by the 'Root' Operator.

Example

1. Log on as 'Root' user.
2. Remain in the root division, assuming "Common Door 1" has a Door, Access Zone, Schedule and Access group that is in the root division.
3. Create an Access Group for each Tenant to be used for the Common Area. (See Setting up Access Groups for procedure.)
4. Copy (or drag and drop) the "Common Door 1" Access Zone and Schedule which is the root division [1] into each of the previously created Common Access Groups.

   Common Access Group Tenant 1 - Division [2]
   Common Access Group Tenant 2 - Division [3]
   Common Access Group Tenant 3 - Division [4]
5. Log on as Tenant 1 (restricted to Division [2]).

6. Add (or modify) Cardholders, applying Common Access Group Tenant 1. These Cardholders will now have access to enter the Common Door 1 Zone using the times governed by the applied Schedule.

Multi-site system with common Cardholders

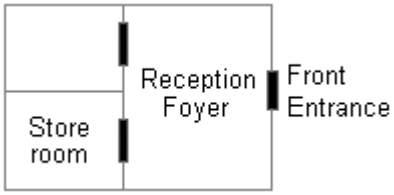
Card Management Operators can be configured so they can see every Cardholder in the system no matter which division they are in. They can copy any Cardholder into their own Access Group(s), thereby allowing Cardholders from other sites to gain entry to the doors/elevators within the view of that Operator. They can fully edit Cardholders in their own division but are unable to edit the Cardholders from other divisions.

Chapter 10: Access Zones

The Access Zone is **where** the cardholder is allowed access. A zone represents an area that has one or more access controlled doors controlling access into the area.
An Access Zone is a physical area - although it need not be constrained by walls, and it is possible to have nested zones, (i.e. access zones which are contained within another access zone). See ***Understanding Access Zones*** (on page 10-2) for further detail and an example of nested access zones.

Understanding Access Zones

The following example provides further detail regarding nested access zones. A store room may have an access-controlled door connecting it to the rest of the building. There is no other way in or out of the store room. There are times during which the store room door should be locked, regardless of the state of the main building, however at other times this is not required, as long as the main building is secure. If the store room door were to be configured with the entry zone being the store room and the exit zone being the main building, then the store room door would always be locked whenever the main building is in secure access mode. To achieve the effect that the store room door can be unlocked when the main building is secure, the store room door should have its exit zone set to "None Selected". This will mean that the door is only locked when the store room is in secure access mode, regardless of the state of the main building.



There is nothing to be gained by configuring an exit zone on a door that has an entry reader, but no exit reader, unless you really want the door to be locked whenever the exit zone is secure. This is because the main purpose of the access zone is to determine how card access attempts are processed and for tracking purposes (which only works when access cards are used). Avoiding unnecessary assignment of exit zones will often avoid the above problem because the store room probably doesn't have an exit reader.

Adding a new Access Zone

Introduction

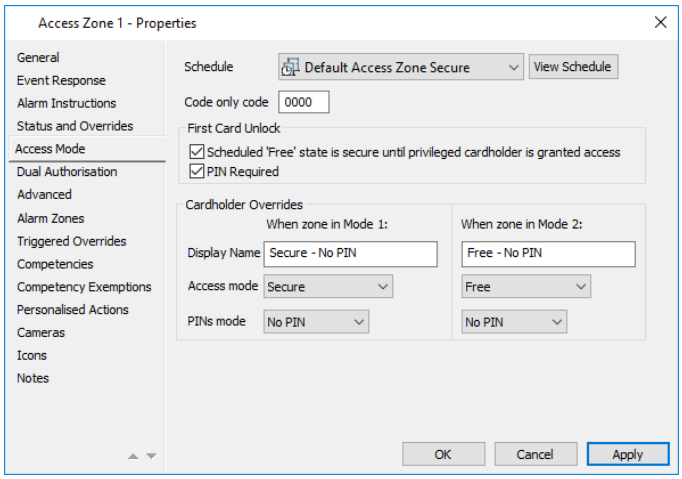
Details about the different Access Zones the cardholders can access must be set up within Command Centre.
Ensure the following components have already been set up:

Divisions
Refer to **Setting up System Division** (on page 9-3).

Schedules
Refer to ***Schedules*** (on page 12-1).

Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. **Right click** and select **New...Access Zone**.
   By default the **General** tab displays.
3. Complete the fields as required. For further detail see ***General tab*** (on page 3-18).
   Note: In a multi-level building, it is useful to include the number of the floor level in the access zone name and/or description. This is so an operator can quickly identify the floor an access zone is on.
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20). **Notes:**
   - Only assign Alarm Zones to Access Zones if there is alarm functionality in that zone, (e.g. PIR). Otherwise, leave the "Alarm Zone for all Events" in the default setting of --None Selected--.
   - If the Access Zone is required to unset an Alarm Zone this is where this relationship should be defined. This is often the case when the Access Zone and Alarm Zone cover the same geographical area. The Alarm Zone may contain a movement detector, or a safe reed switch, etc. If a cardholder badges to enter this Access Zone and the Alarm Zone is armed then the cardholder must have the "Change to the Disarmed state" Access Group privilege before being allowed into the Access Zone. This prevents cardholders from entering the Access Zone when the Alarm Zone is armed. Cardholders are then able to arm the Alarm Zone associated with this Access Zone, as they leave the Access Zone by performing a local override at a reader.
5. Click the **Access Mode** tab.
   One property of an Access Zone is the access mode. The access mode defines the method of access to the zone, (i.e. how the doors in this specific zone behave).



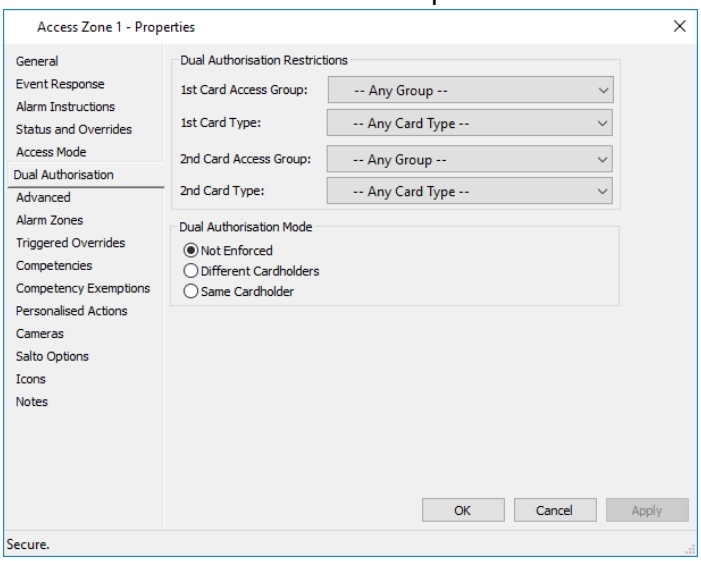
6. Click within the **Schedule** field.
7. A drop-down menu displays all the Access Zone Schedule types you are allowed to see. Select the Access Zone Schedule that is to apply to this Access Zone.
   Note: Clicking the **View Schedule** button opens the **View Calendar** tab of the selected Schedule.
8. First Card unlock mode allows an Access Zone to remain in a SECURE state until a member of a selected access group is granted access on or after the scheduled FREE state change. Configure the **First Card Unlock** as required.

Checkbox	Description
Scheduled 'Free' state is secure until privileged cardholder is granted access	When checked the operator has the ability to select the secure access mode the 'free' will be until a cardholder with the required privileges is granted access. **Note:** Checking this option enables the PIN Required option.
PIN Required	The Operator has the ability to additionally enforce that a PIN be required when the First Card Unlock mode is in force.

9. The 'Cardholder Overrides' area of this screen determines what happens when a cardholder overrides the access mode for the zone. Otherwise the access mode is determined by the Schedule. It relates to Access Groups with the "Lock and unlock access zones" privilege. This privilege enables members to override the access mode, (e.g. from secure to free), by performing a local override at a reader. (For further details refer to ***Configuring Local Overrides at Card Readers*** on page 45-14.)
   Note: The default Action Plan for **Access Zone State Change** events is "Log an event". It is possible however to change the default to "No event recorded", which can be configured from either the Server Properties (**Event Defaults** tab), the Door properties (**Event Response** tab), or the Alarm Zone properties (**Event Defaults** tab).
10. Specify the methods of access to this zone, when the access mode is overridden to Mode 1 or Mode 2. **Notes:**
    - The 'Display Name' is viewed on the HBUS Terminal only. The 'Display Name' enables you to describe the access mode, (e.g. After Hours). If using an HBUS Terminal, enter the Display Name for each access mode.

- If the access mode is "Code or Card", you need to enter an appropriate four digit number in the 'Code only code' field on this screen. This means anyone will be able to gain access through a door by entering the four digit code and then pressing the **IN/Enter** button on the reader.

11. If you require this Access Zone to have the dual-authorisation access mode, click the **Dual Authorisation** tab. If not, go to Step 13.
    Dual Authorisation is as access mode that requires two different valid credentials to be presented at an Access Zone's entry reader(s), in order to be granted access. **Examples:**
    - Two separate authorised Cardholders must present a valid credential at the reader to open the door.
    - One authorised Cardholder must present two separate valid credentials at the reader to open the door.



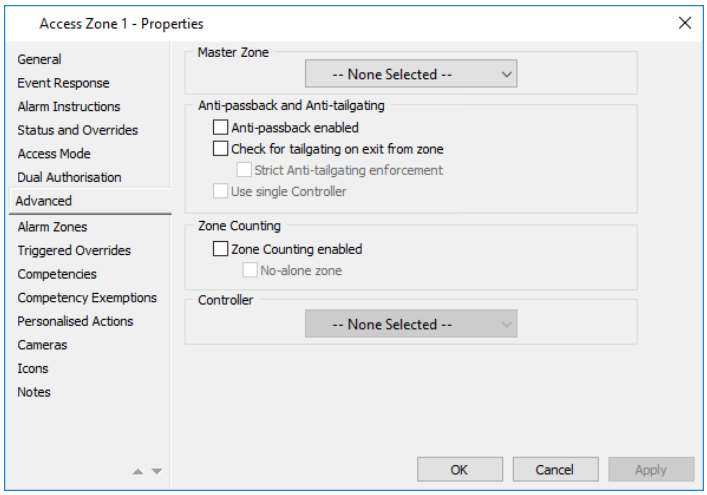
    If required, perform the following procedure to configure Dual Authorisation for this Access Zone: **Notes:**
    - Dual Authorisation is not supported for Elevator use.
    - Dual Authorisation functionality is not enabled unless the Access Zone is in either of the 'Dual Auth - No PIN' or 'Dual Auth - PIN' access modes. An Access Zone can be put into a Dual Auth access mode using Access Zone Schedules or Overrides.

12. Configure the **Dual-authorisation** tab as required.

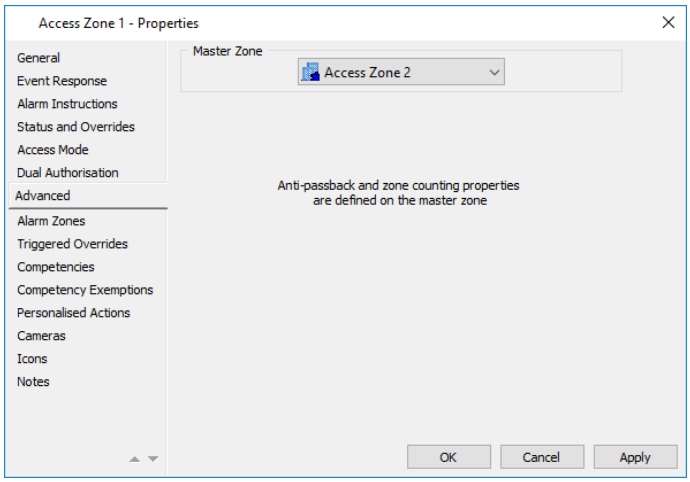
Field	Description
1st Card Access Group	From the **1st Card Access Group** drop-down list: ▪ select the Access Group that the 1st credential must belong to, or ▪ select -- *Any Group* -- to let the 1st credential belong to any valid Access Group.
1st Card Type	From the **1st Card Type** drop-down list: ▪ select the Card Type, Mobile Credential Type, or Morpho Biometric Type that the 1st credential must be, or ▪ select -- *Any Card Type* -- to let the 1st credential be any valid Card Type.

Field	Description
2nd Card Access Group	From the **2nd Card Access Group** drop-down list: ▪ select the Access Group that the 2nd credential must belong to, or ▪ select -- *Any Group* -- to let the 2nd credential belong to any valid Access Group.
2nd Card Type	From the **2nd Card Type** drop-down list: ▪ select the Card Type, Mobile Credential Type, or Morpho Biometric Type that the 2nd credential must be, or ▪ select -- *Any Card Type* -- to let the 2nd credential be any valid Card Type. **Note:** The **2nd Card Type** can be the same as the **1st Card Type** if required.
Dual Authorisation Mode	Select the required Dual Authorisation Mode: ▪ **Not Enforced:** The first and second credential badges can come from the same Cardholder or different Card-holders. The zone count will increase by 1 if both credentials belong to the same Cardholder. The zone count will increase by 2 if the credentials belong to different Cardholders. ▪ **Different Cardholders:** In this mode, the first and second credentials must belong to different Cardholders. The zone count will increase by 2. ▪ **Same Cardholder:** In this mode, the first and second credentials must belong to the same Cardholder. The zone count will increase by 1. **Note:** While one Cardholder can perform both badges (de-pending on which option you select), the Card-holder must badge two different credentials; not the same one twice.

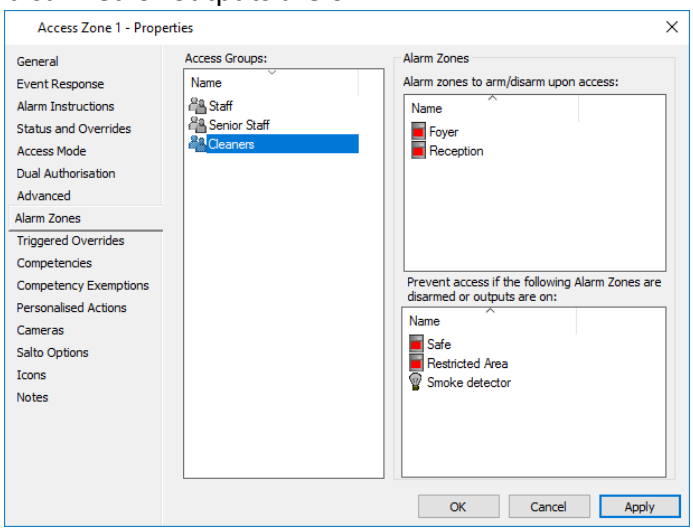
13. Click the **Advanced** tab.



14. Do you want this Access Zone to be a member of an Access Zone Group?
    If **no**, go to Step 15.
    If **yes**, click within the **Master Zone** field and select the appropriate Access Zone from the drop-down list.
    The Anti-passback and Zone Counting sections disappear from this tab, as these properties will be defined on the Master Zone.



15. Configure anti-passback for this Access Zone if required. (See ***Configuring Anti-passback*** on page 10-15 for procedure.)
16. Configure Zone Counting for this Access Zone if required. (See ***Enabling Zone Counting*** on page 10-22 for procedure.)
17. Click the **Alarm Zones** tab if you want to configure the Alarm Zones to be armed/disarmed upon access or prevent access if the Alarm Zones are disarmed or outputs are on.



In this tab you can add Access Groups, then for each Access Group you can:

- Specify Alarm Zone(s) to be armed/disarmed when access is granted (in the top grid).
- Specify Alarm Zone(s), and/or Output(s) that will result in denial of access if the Alarm Zone is disarmed, or the output is on (in the bottom grid).

Note: This feature uses the Access Group privileges to arm/disarm the Alarm Zones. Therefore, to enable the Cardholders to arm/disarm the Alarm Zones specified here, the Alarm Zones must be assigned to the Cardholders' Access Group.

18. Click **Manage** from the menu bar, then **Access Groups**.
    The Access Group List Window opens. Select the appropriate Access Group(s), and drag and drop them into the **Access Groups** grid.
19. Click on the appropriate Access Group to select it.
    The Alarm Zone grid is displayed.

20. Click **Configure** from the menu bar, then **Alarm Zones**.
    The Alarm Zone List Window opens.
    Select the required Alarm Zones, and drag and drop them into the appropriate **Alarm Zones** grids as follows:
    - Top grid, to arm (via double badge) and disarm upon access.
    - Bottom grid, to prevent access if the Alarm Zones are disarmed or outputs are on.
21. Open the **Hardware** List Window, and drag and drop the Output(s) required into the **Alarm Zones** bottom grid.
22. Click the **Triggered Overrides** tab if you want to configure pushbutton overrrides or lockdown functionality for this Access Zone. (See ***Configuring Pushbutton Overrides*** on page 10-34 or ***Setting a Lockdown Source*** on page 10-10 for procedure.)
    Note: You can configure EITHER pushbutton overrides OR lockdown functionality for an Access Zone, (i.e. you cannot use both features for the one zone).
23. Click the **Personalised Actions** tab if you want to configure cardholder specific actions for this Access Zone. See ***Configuring Personalised Actions for Access Zones*** (on page 10-36) for the procedure.
24. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Access Zone. For further details see ***Cameras tab*** (on page 3-24).
25. Click the **Icons** tab if you want to change the Icon Set for this Access Zone. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
26. Click the **Notes** tab if you want to add a note(s) about this Access Zone. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
27. 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 Access Zone is added to the Command Centre system.
All access controlled doors within the selected zone will all behave in the same manner. When cardholders attempt access to the zone the doors will all require the same method of access.

Hint

Access Zones (and hence their attached Access Zone Schedule) are one of the three elements of setting up Access Groups.

Editing and Deleting Access Zones
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Access Zones.
Note: You cannot delete any Access Zones that are currently assigned to doors, elevator cars or macros, or are configured on a Tag Board Tile in Command Centre Client. Likewise, if you attempt to delete an Access Zone that is a 'Master Zone', (i.e. it has other Access Zones associated with it), the following error message will display:
"This Access Zone cannot be deleted, as it still contains another Access Zone."

Access Zone Lockdown

Introduction

The Access Zone "lockdown" mode allows a site to very quickly and easily deny entry to an Access Zone to all but selected cardholders, while still allowing cardholders to exit the zone.
The lockdown status of an Access Zone can be changed by either:
- a lockdown override, or
- the cancelling of a lockdown override, or
- changing the state of a lockdown input, or
- running a macro to override the Access Zone.

Lockdown behaviour

When an Access Zone is in lockdown mode cardholders are only allowed entry if they belong to at least one Access Group that allows scheduled access at the current time, and that also conveys the "Entry allowed during lockdown" privilege (on the **Privileges** tab of the Access Group properties).
When entry to an Access Zone in lockdown mode is provided from an elevator car, the elevator car floor level buttons for the Access Zones that are in lockdown remain disabled when a cardholder badges their card, unless the cardholder also has the "Entry allowed during lockdown" privilege for that floor/Access Zone.

Scenarios

Refer to ***Scenarios using Logic and Virtual Outputs*** (on page 25-4) for worked examples of lockdown configuration.

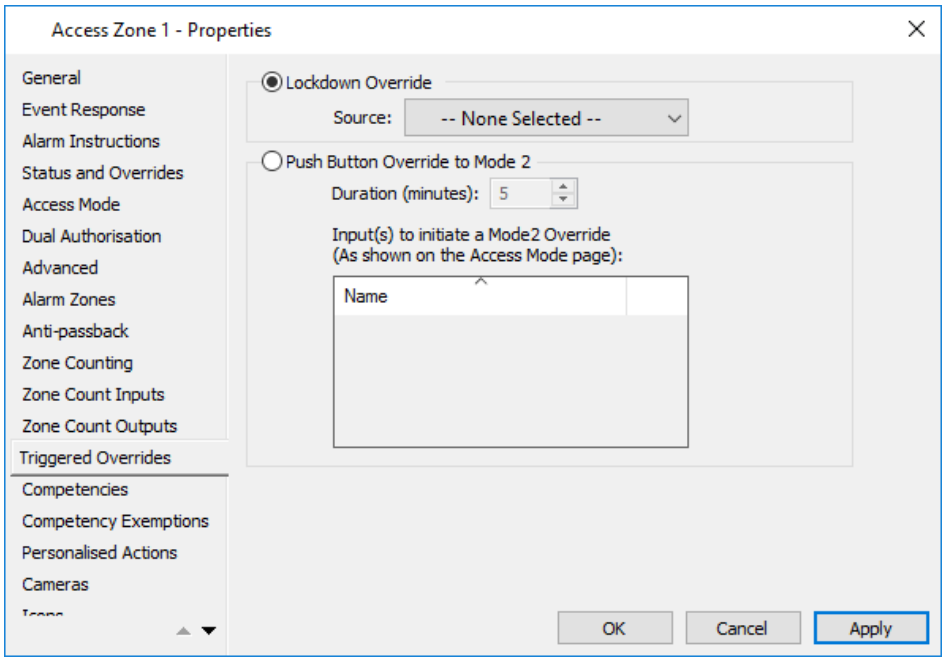
Setting a Lockdown source

Introduction

This procedure allows operators to select an input source to be used for placing an Access Zone into or out of lockdown mode.

Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to perform a lockdown override on.
3. Right click and select Properties.
4. Click the Triggered Overrides tab.
   Notes:
   - By default the **Lockdown Override** radio button is enabled.
   - This tab allows you to configure EITHER pushbutton overrides OR lockdown functionality for an Access Zone, (i.e. you cannot use both features for the one zone).



5. Select the appropriate input source from the Source drop-down list.
   Notes:
   - The lockdown input source can be an input, an output, a virtual output or a logic block.
   - The **Source** field will be 'read only' if you do not have the appropriate privilege to edit the Access Zone.
6. Click **OK** to exit and save your changes.

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

Result

A lockdown source has been configured for placing this Access Zone into or out of lockdown mode.
Notes:

- *Adding lockdown sources*
  When adding a lockdown source to an Access Zone, the zone will change to what the source is telling it to do, (e.g. if a zone is locked down and an output that is "off" is added, the zone will return to the previous state, i.e. not locked down).
- *Removing lockdown sources*
  If an Access Zone is locked down at the time the lockdown source is removed, the zone will remain locked down. The lockdown needs to be manually cancelled.

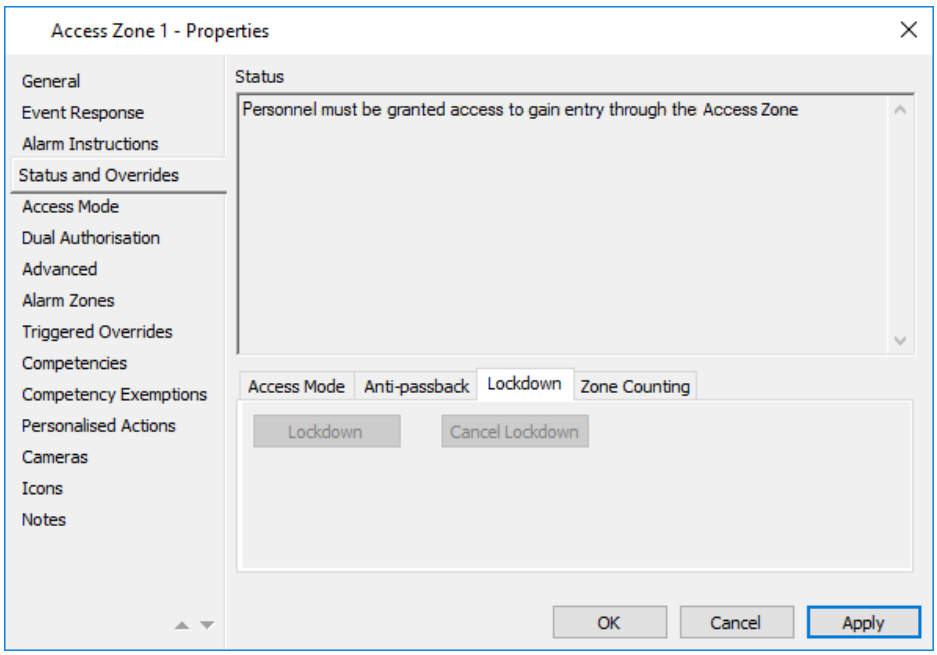
Performing a Lockdown Override

Introduction

This procedure allows operators with the "Override" privilege in an Access Zone's division to set or reset the lockdown state of an Access Zone.
Note: If a site wants to be able to determine which operator performed a lockdown override, they can review the event log which will have either an operator event saying who locked the Access Zone down, or a state change message for a lockdown input. If the site has a large number of events this may not be practical, so another alternative is to use the Access Zone **Notes** tab. The operator who performed the lockdown would need to update the Access Zone **Notes** tab to tell others why the lockdown has occurred and who to contact, if necessary.
If the lockdown is performed by an input, the input lockdown event can be configured as an alarm, and the associated alarm instructions can be used to tell other operators what they need to do.

Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to perform a lockdown override on.
3. Right click and select Properties.
4. Click the Status and Overrides tab.
5. Click the **Lockdown** tab within this screen.



6. Click the **Lockdown** button.
   The status message will change to include the following text:

"The access zone is locked down. Only Cardholders with the Entry during lockdown privilege can enter."

Notes:

- When a **Lockdown** override occurs, the following event is logged:
  Operator '[Name]' requested a Lockdown Override for access zone '[Name]'

  and then when you perform a **Cancel Lockdown** override, the following event is logged:
  Operator '[Name]' requested a Cancel Lockdown Override for access zone '[Name]'

  If you have the "Access Zone State Change" Event Group set to 'log an event' (via the **Event Defaults** tab of the Server Properties), in addition to the events above, the following event will **also** be logged at the time of a **Lockdown** override and a **Cancel Lockdown** override:
  [Access Zone] changed to [access mode] [PINs mode] at [Door]
- While a lockdown override is in force, other overrides of the Access Zone can occur, (e.g. to other access modes).

7. Click the **OK** button.

Result

The Access Zone has been overridden to "lockdown" mode. The lockdown override will remain in force until it is cancelled, (i.e. the **Cancel Lockdown** button is clicked).

Note:
Once a lockdown override is cancelled, the Access Zone will return to either:

- it's scheduled state if no other overrides of the Access Zone are active, or
- it will return to the overridden state if other overrides are currently active.

Anti-Passback

The anti-passback feature prevents a cardholder from re-entering an Access Zone if they have not made a valid exit from that zone. It is designed to stop a cardholder from passing their credential back to another person to allow them access to the zone at a later time.
Anti-passback should only be enabled for Access Zones where a high level of security is required, where the access mode of the zone is never free-access and for which all exit-doors have exit readers.
Notes:

- Anti-passback is not supported for elevator cars since it is not possible to prevent tailgating in this case and because Command Centre cannot determine the exit zone for an elevator car.
- If a door is configured for auto-forgive (on an Access Zones **Anti-passback** tab) and zone counting is also configured for the same Access Zone, then if a cardholder exits via that door, the zone count will not be updated.

Anti-Passback Forgive

Included with anti-passback is "Anti-Passback Forgive" which allows one or all authorised cardholders to re-enter one or all anti-passback zones, even though valid exits have not been made.
Anti-Passback Forgive allows the following:

- an auto-forgive timeout to be specified per Access Zone
- an auto-forgive-all time to be scheduled per Access Zone
- an operator to forgive a specific cardholder, or all cardholders (as an override) for an Access Zone.

Configuring Anti-passback

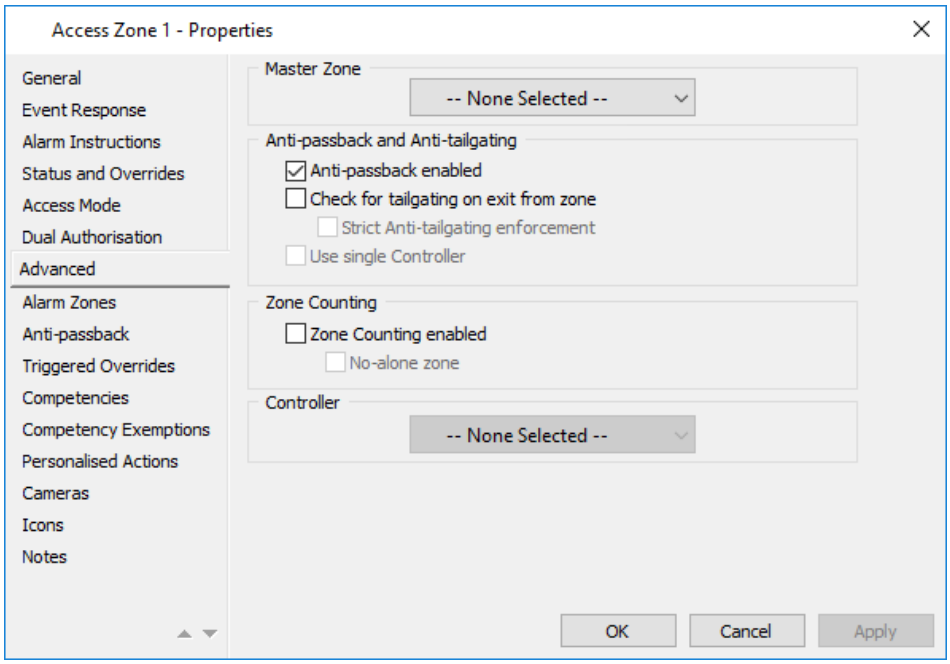
Introduction

This procedure describes how to enable anti-passback, set the 'auto-forgive' timeout and select an 'auto-forgive-all' time for an Access Zone.

You must have the "Edit Site" operator privilege, and be in the same Division as the Access Zone (or a parent Division).

Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to configure anti-passback for.
3. Right click and select Properties.
4. Click the **Advanced** tab.



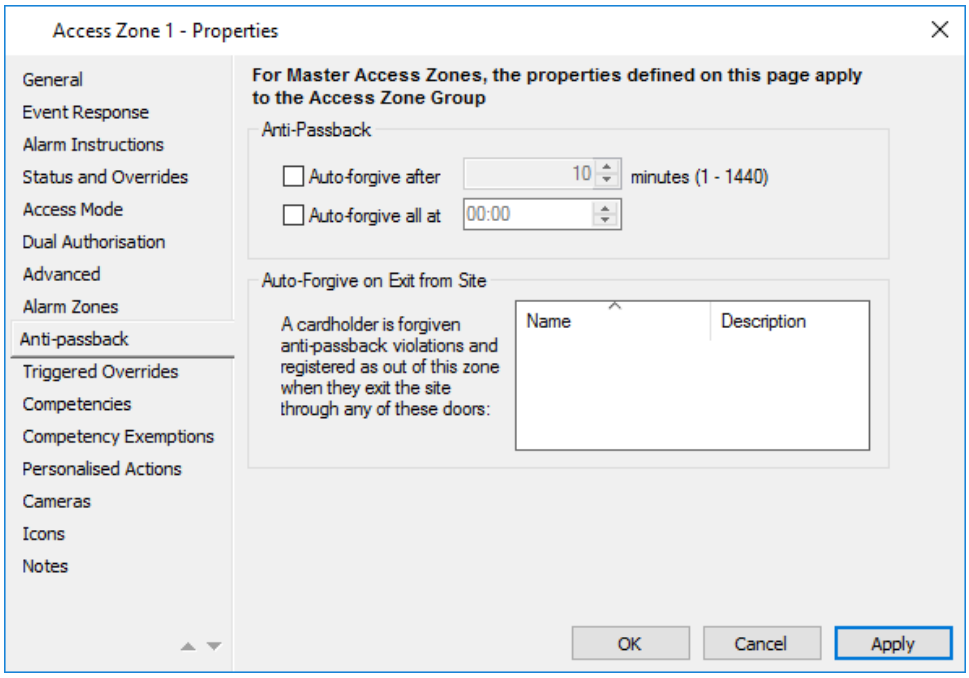
5. Configure the Anti-passback properties as required.

Checkbox	Description
Anti-passback enabled	When checked, the Controller will maintain a list of the Cardholders that are currently within the Access Zone. If the Access Zone is part of an Access Zone Group, then only one "in zone" list is maintained for the Master Zone of the Access Zone Group. The **Use single Controller** checkbox becomes enabled and a new **Anti-passback** tab appears.

Checkbox	Description
Check for tailgating on exit from zone	When checked, the Controller will maintain an "out of zone" list of Cardholders for the Access Zone. If the Access Zone is part of an Access Zone Group, then only one "out of zone" list is maintained for the Master Zone of the Access Zone Group. The **Use single Controller** checkbox becomes enabled and a new **Anti-passback** tab appears. **Note:** While this is configured here on the Access Zone, the anti-tailgating response is configured on the Access Group.
Use single Controller	When checked, the **Controller** selection box becomes enabled so you can select a single Controller to store the "in zone" and "out of zone" lists on. **Note:** This helps with performance for sites that require anti-passback on Access Zones with high throughput at specific times.

Note:
If you want to configure zone counting for this Access Zone also, refer to Enabling Zone Counting (on page 10-22) for the procedure.

6. Click the **Anti-passback** tab.



Note: If this Access Zone is a Master Zone for an Access Zone Group, then the properties configured here will apply to all Access Zones in the group.

7. If required, check the **Auto-forgive after** checkbox and enter the

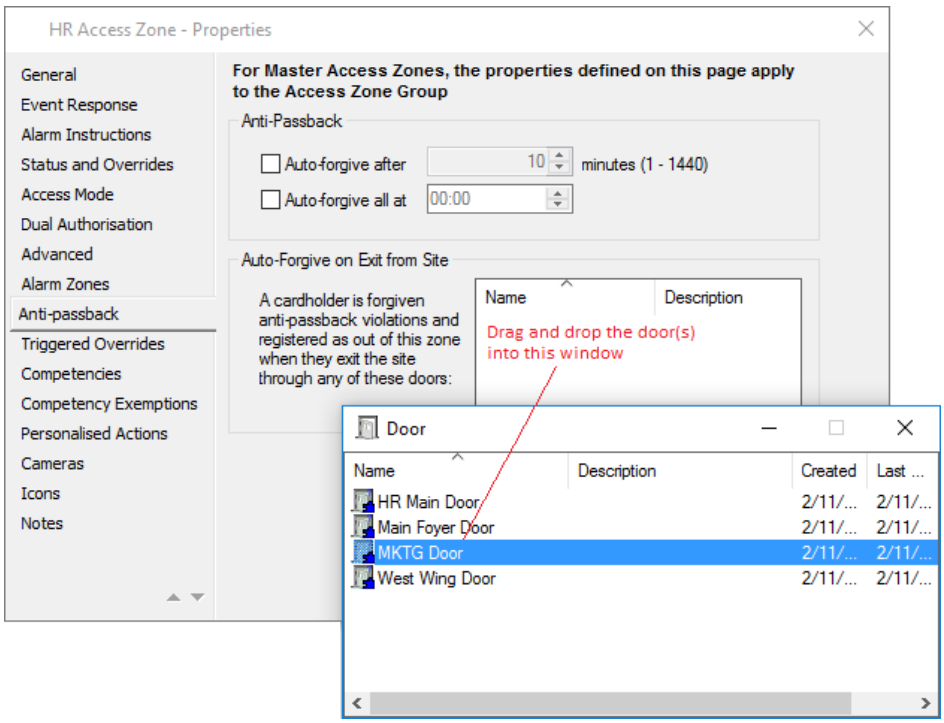
appropriate time (in minutes) in the Time box 

. This will allow an authorised cardholder to re-enter the anti-passback zone after the time set, even though they have not made a valid exit from that zone. The **Auto-Forgive** time starts from the time of valid entry, (i.e. if it is set to 3 minutes and a cardholder presents their credential after 3 minutes from the original valid entry, they will be allowed back in the zone).

8. If required, check the **Auto-forgive-all at** checkbox and enter the appropriate time in the Time box 

using the 24 hour clock. This will allow all authorised cardholders to re-enter the anti-passback zone after the time of day indicated, regardless of any previous anti-passback restrictions.
Note: Anti-passback continues operating as normal after the time indicated.

9. The **Auto-Forgive on Exit from Site** section is used to list all the Door(s) that a cardholder can exit the site through, and they will be forgiven anti-passback violations and registered as "out of zone".
Open the **Door** List Window and highlight the door(s) you want to be used by this Access Zone and drag and drop them into the **Auto-forgive on Exit from Site** grid.



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

Anti-Passback has been configured for the Access Zone.

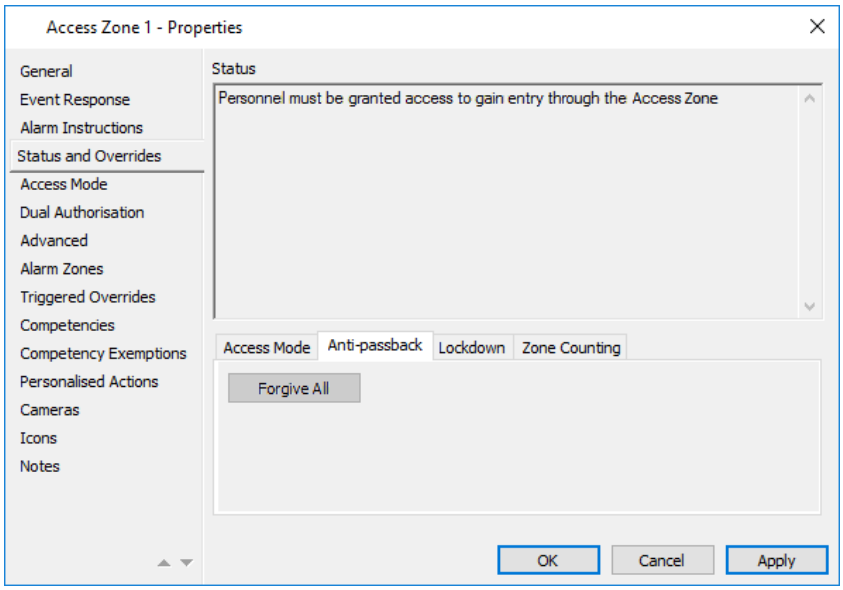
Forgive All Cardholders

Introduction

This procedure describes how to perform an "Anti-Passback Forgive" override for all cardholders, which will allow them to re-enter anti-passback zones even though they have not made valid exits.
You must have the "Override" operator privilege and be in the same Division as the Access Zone (or a parent Division).

Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to override.
3. Right click and select Properties.
4. Click the Status and Overrides tab.
5. Click the **Anti-passback** tab within this screen.



6. Click the **Forgive All** button.
   Notes:
   - The **Forgive All** button will only be enabled if the Access Zone uses anti-passback.
   - If the Access Zone is a member of an Access Zone Group, the following message will display underneath the **Forgive All** button:
     These overrides apply to the access zone group: <Master Zone Name>

Result

The next time any cardholder presents their card at a door leading into this Access Zone they will be granted access, if all other criteria are satisfied.

Forgive a specific Cardholder

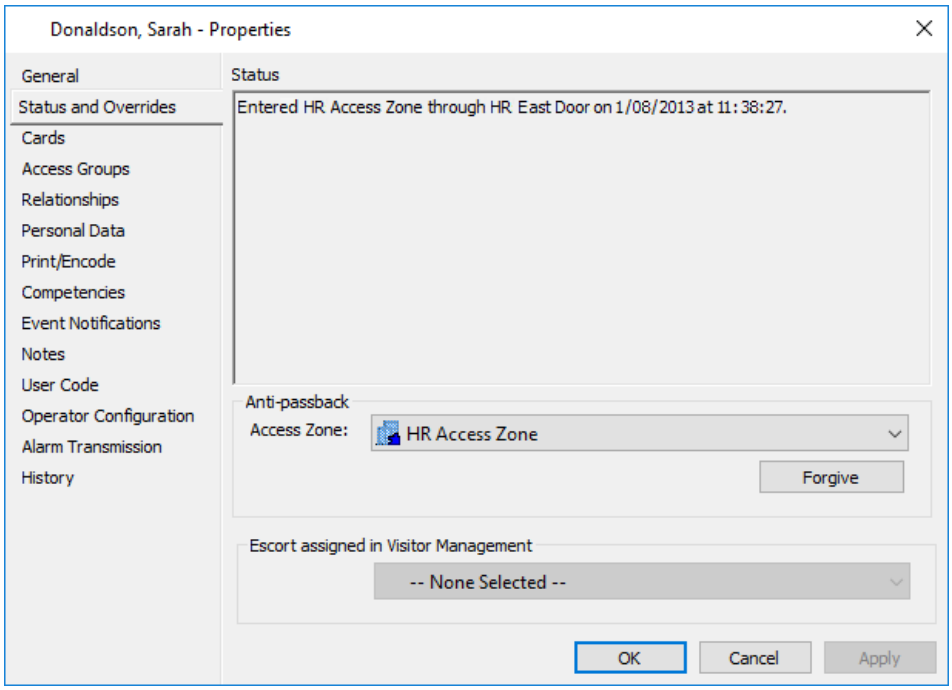
Introduction

This procedure describes how to set up "Anti-Passback Forgive" for a specific cardholder, which will allow that cardholder to re-enter an anti-passback zone even though they have not made a valid exit.

You must have the "Override" operator privilege, and be in the same Division (or a parent Division) as both the Access Zone and the Cardholder.

Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Highlight the Cardholder you require.
3. Right click and select Properties.
4. Click the Status and Overrides tab.



5. Select the Access Zone you want to override from the drop-down list, then click the **Forgive** button.
   Note: If the Access Zone selected is a member of an Access Zone Group, the following message will display beside the **Forgive** button:

   Forgive applies to the master zone: <Master Zone Name>

Result

The next time this cardholder presents their card at a door leading into this Access Zone, they will be granted access if they have that privilege.

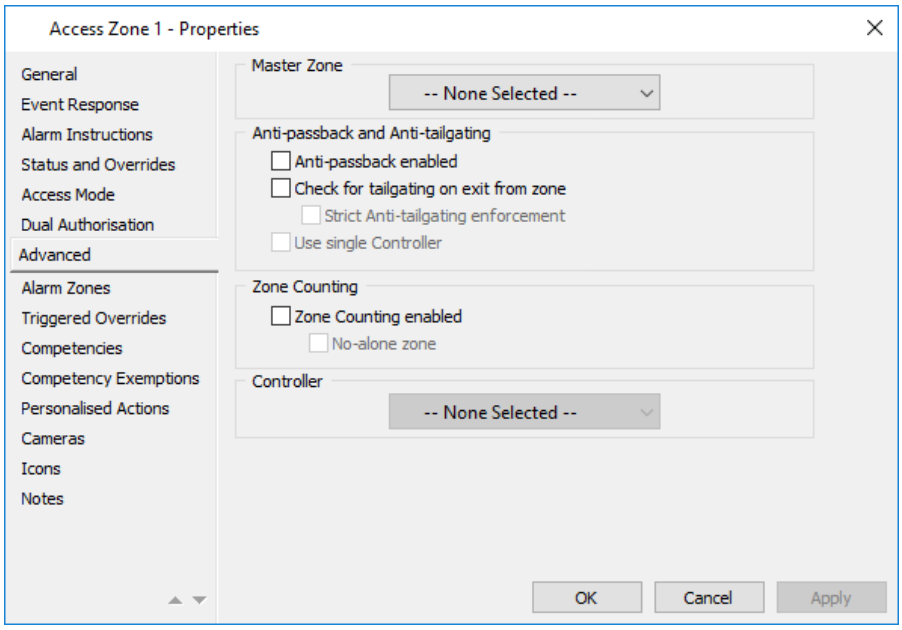
Configuring Strict Anti-tailgating

Introduction

The 'Strict Anti-tailgating' feature enables sites to disallow cardholders to exit from a zone if they are not recorded as having entered the zone.

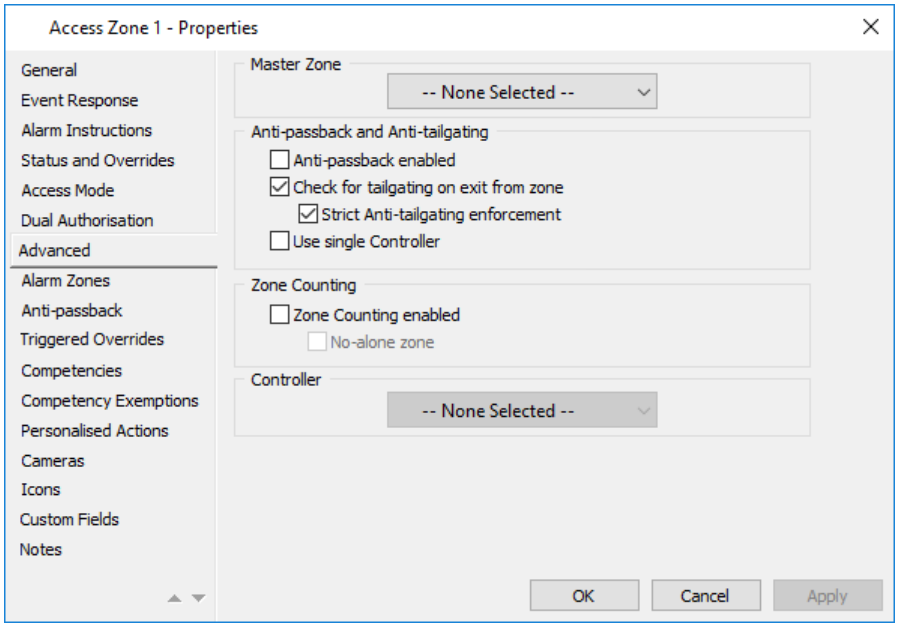
Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to enforce strict anti-tailgating for.
3. Right click and select Properties.
4. Click the **Advanced** tab.



5. Check the **Check for tailgating on exit from zone** checkbox.
   The **Strict Anti-tailgating enforcement** and **Use single Controller** checkboxes become enabled and a new **Anti-passback** tab appears.

   The Controller will maintain an "out of zone" list of Cardholders for the Access Zone. If the Access Zone is part of an Access Zone Group, then only one "out of zone" list is maintained for the Master Zone of the Access Zone Group.
   Note: While this is configured here on the Access Zone, the anti-tailgating response is configured on the Access Group
6. Check the **Strict Anti-tailgating enforcement** checkbox.



While the **Check for tailgating on exit from zone** option only disallows exit if someone has already exited, the **Strict Anti-tailgating enforcement** option disallows exit for anyone who is not recorded as having entered. To achieve this, it persists the list of who is in the zone (Controller 6000 and 7000 variants).

The list is also persisted for anti-passback (Controller 6000 and 7000 variants), so with Controller restarts it no longer forgets that the cardholder has already entered. Zone counts are also persisted (Controller 6000 and 7000 variants), so with Controller restarts the zone count will not be set back to zero, and outputs triggered by different zone count states will remain in the same state as prior to the restart. If you have anti-passback enabled for a while and then turn on anti-tailgating, it should work as intended straight away because it will have already tracked who is in the zone. However, make sure you do not turn that off, apply, and then turn on strict anti-tailgating, because the instant you apply changes with them off, the persistence will be cleared.
Hence upon enabling the option, anyone already in the zone may be denied exit. To mitigate this issue, you can do any of the following:

- Turn on anti-passback for perhaps a day first, so that it can work out who is in the zone (as it uses the same list), OR
- Only turn the option on at a time when the zone is empty, OR
- Change the anti-tailgating response on Access Groups to the "No action" or "Log an event" setting, until say about one day has passed, before changing it back again. This is the least preferable option as you would have to change all access groups that grant access into that zone.

Note: The controller persistence list is cleared by turning off anti-passback and strict anti-tailgating. There is no need to turn off standard anti-tailgating.

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.

Enabling Zone Counting

Introduction

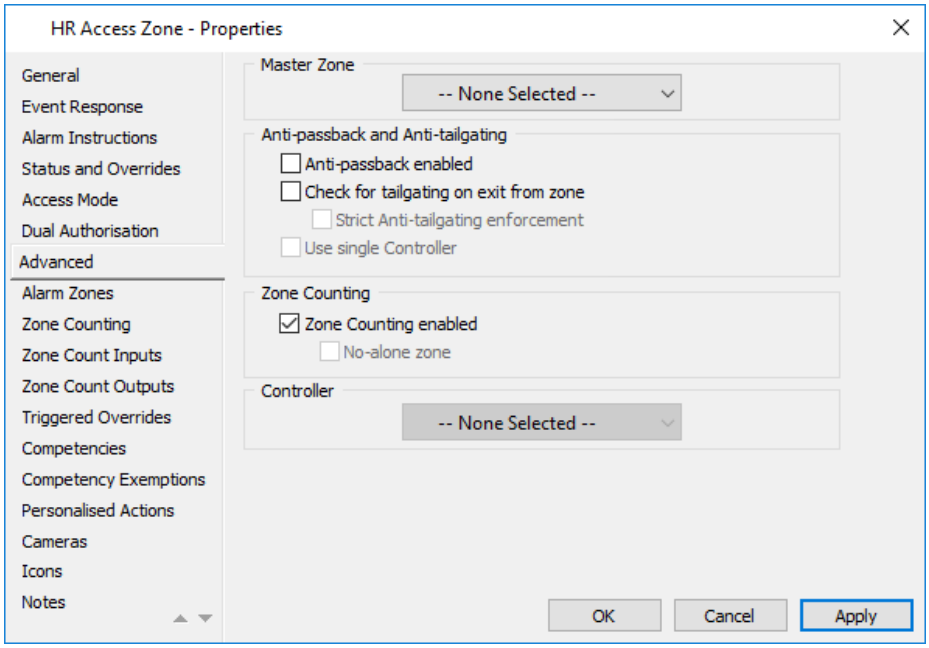
Zone Counting enables sites to keep a continuous count of the number of cardholders in an Access Zone, or Access Zone Group. "No-alone zones", which are sometimes required for security or safety reasons, use zone counting in conjunction with dual authorisation.

Notes:

- A count zone may span multiple Controllers, however this may reduce the accuracy of the count.
- If a door is configured for auto-forgive (on an Access Zones **Anti-passback** tab) and zone counting is also configured for the same Access Zone, then if a cardholder exits via that door, the zone count will not be updated.
- Dual Authorisation is not supported for Elevator use.
- If the Controller is restarted, zone counting will be persisted.

Procedure

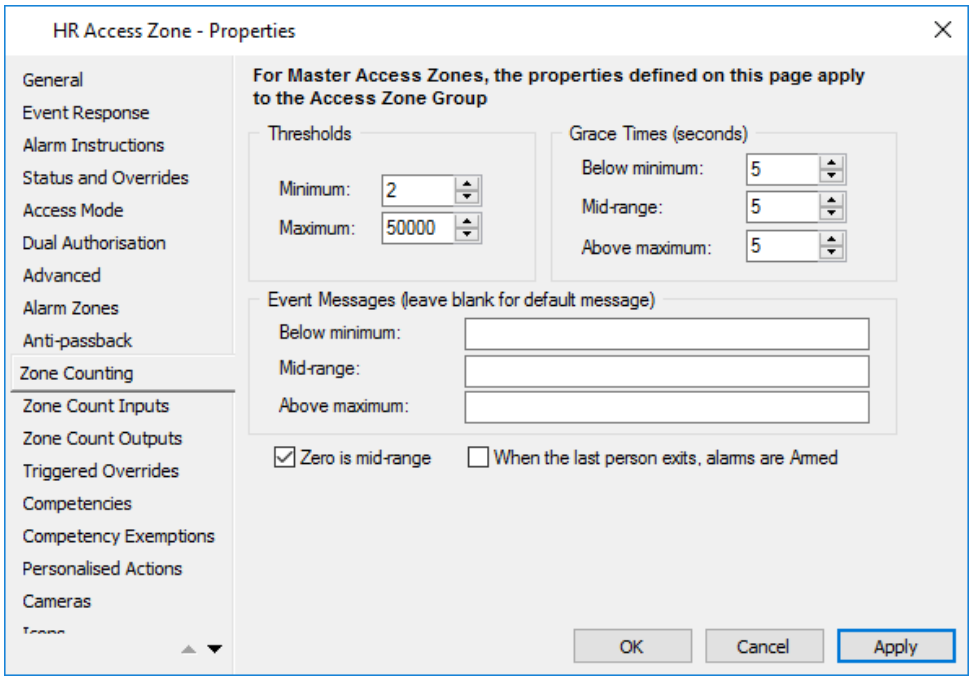
1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to configure zone counting for.
   Note:
   If the Access Zone is a member of an Access Zone Group, zone counting needs to be defined on the Master Zone for the group. If this is the case, you will need to open the properties of the Master Zone, and the zone counting properties configured for the Master Zone will apply to all Access Zones in the group.
3. **Right click** and select **Properties**.
4. Click the **Advanced** tab.
5. Check the **Zone Counting enabled** checkbox.
   The **No-alone zone** checkbox becomes enabled and three new tabs appear, (i.e. **Zone Counting**, **Zone Count Inputs** and **Zone Count Outputs**).



6. Check the **No-alone zone** checkbox if cardholders are not allowed to be in this zone alone.
   If this is to be a 'No-alone Zone', see ***Configuring No-alone Zones*** (on page 10-28) for complete procedure.

7. Select a **Controller** from the drop-down list.
   Note: There are no specific rules for selecting a Controller, but for optimum performance you should select the Controller that manages the largest part of the system, (i.e. the one that has the most doors).

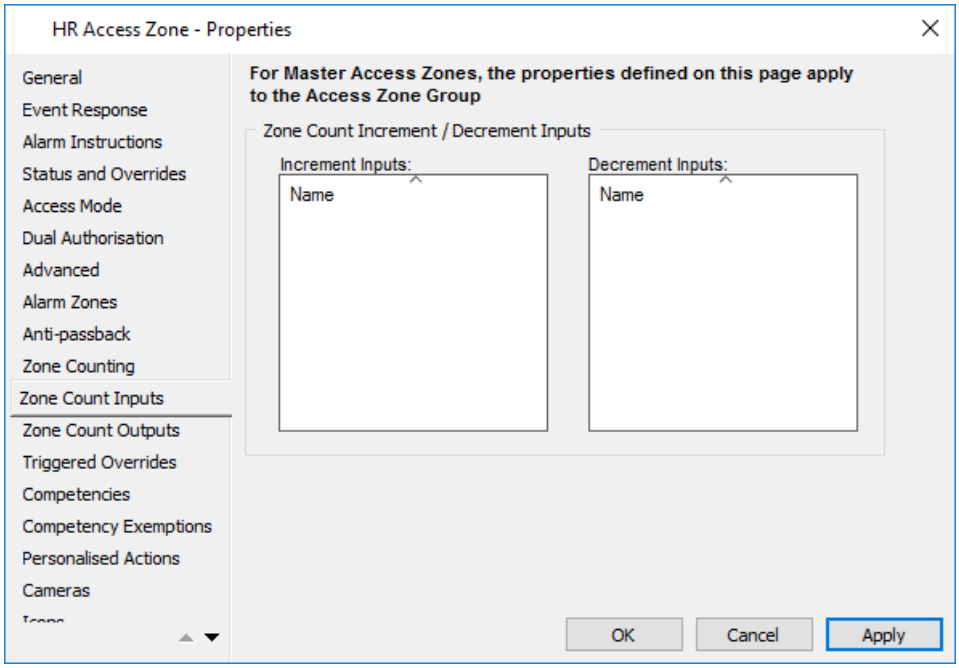
8. Click the **Zone Counting** tab.



9. Configure zone counting as required.

Option	Description
Thresholds	Sets the minimum and maximum threshold for the count zone. The two threshold values define three ranges: low, medium and high, which mean respectively, below-minimum, mid-range and above-maximum.
Grace Time	This is the period that must elapse before generating an event because the zone count has reached a threshold value or zero. **Note:** This allows short transition periods for people to change places between zones, (e.g. with dual-authorisation when a zone must have a minimum of two people, but zero is OK, we cannot expect two cardholders to enter or leave simultaneously). This gives time for two people to leave or enter without generating an alarm.
Event Messages	Allows messages to be defined for display in event or alarm, (e.g. "Carpark full").
Zero is Mid-range	Ticking this checkbox will mean that the zone count of zero will be treated in the same way as mid-range.
When last person exits alarms are Armed	Ticking this checkbox will mean that when the last person leaves the Access Zone the alarms will be armed.

10. Click the **Zone Count Inputs** tab.



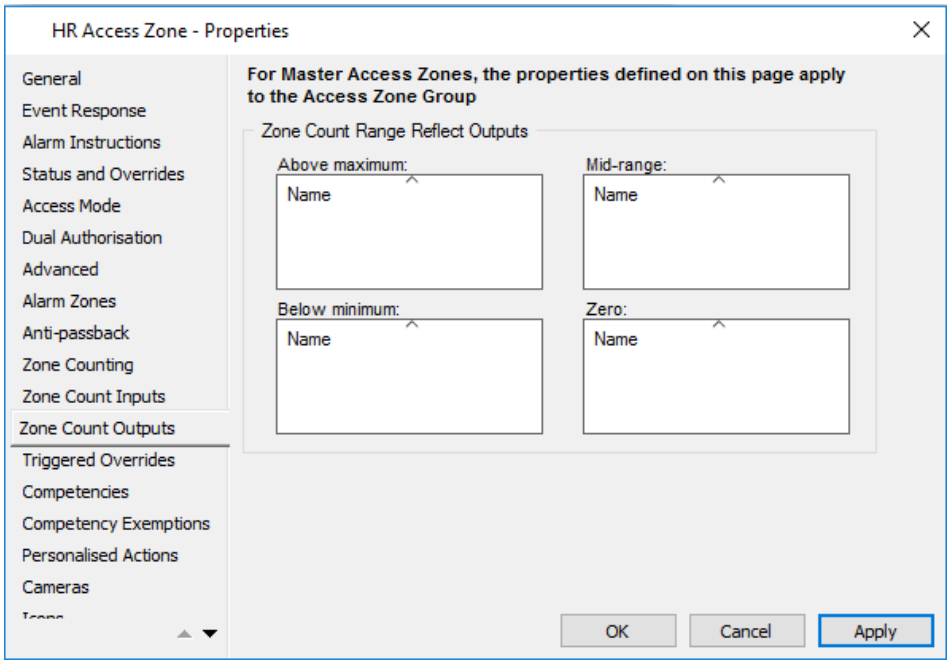
Inputs, outputs and/or logic blocks can be configured to increment and/or decrement the zone count for this Access Zone.

Examples of when this could be used:

a) When a sensor is used to count people passing by, (i.e. the zone count is not actually associated with access control, just counting people in or out of an area).

b) In a multi-tenanted car park, when an owner wants to restrict entry to a particular tenant once they have used all the car parks allocated to them. In this case, the input will in fact be a virtual output that is triggered when a particular tenant leaves the car park. Refer to ***Logic Blocks and Virtual Outputs*** (on page 25-1) for further detail regarding virtual outputs.

11. From the **Hardware** List Window, select the input(s) and/or output(s) to be used for incrementing the zone count.
    Note: The number of inputs, outputs and logic blocks that can be configured to increment the zone count is unlimited.
12. Drag and drop them into the 'Increment Inputs' grid on the **Zone Count Inputs** tab.
    Note: If an input is not inverted (via the **Advanced** tab of the input's properties), then when the input transitions from closed to open the zone count for this Access Zone is incremented.
    If an input is inverted, then the reverse occurs, (i.e. when the input transitions from open to closed the zone count is incremented).
13. Repeat Steps 11 and 12 for the input(s) to be used for decrementing the zone count.
    Notes:
    - The number of inputs, outputs and logic blocks that can be configured to decrement the zone count is unlimited.
    - If an input is not inverted (via the **Advanced** tab of the input's properties), then when the input transitions from closed to open the zone count for this Access Zone is decremented.
      If an input is inverted, then the reverse occurs, (i.e. when the input transitions from open to closed the zone count is decremented).
14. Click the **Zone Count Outputs** tab.



This tab allows at least four relays per zone count range to be configured to reflect the zone count state being in each of the three ranges and/or zero. The relays will reflect when the zone count reaches the following values:

Value	Description
Above maximum:	This relay will be on when the zone count exceeds the maximum threshold value, otherwise it will be off.
Mid-range:	This relay will be on when the zone count is not greater than the maximum threshold value and not less than the minimum threshold value.
Below minimum:	This relay will be on when the zone count is less than the minimum threshold value, otherwise it will be off.
Zero:	This relay will be on when the zone count is zero, otherwise it will be off. This relay will never be on by itself because either the 'Mid-range' or the 'Below Minimum' relay will also be on depending on the 'Zero is Mid-range' setting on the **Zone Counting** tab, (i.e. if 'Zero is Mid-range' is checked, then the Mid-range and Zero relays will be on together, otherwise it will be the Zero and Below minimum relays that are on together).

Notes:

- All relays can be set up to operate in reverse, the same as any other relay.
- The output will not necessarily reflect the correct state immediately after being configured, but it will after the next zone count state change.

  It is possible to force a state change by manually setting the zone

count to a different threshold. See ***Manually Resetting Zone Counts*** (on page 10-32) for the procedure.

15. Drag and drop the outputs to use for reflecting the zone count states.
16. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

Zone counting has been enabled for the Access Zone, or Access Zone Group.

Configuring No-Alone Zones

Introduction

Access Zones can be configured to prevent a single Cardholder being alone in a Zone. Command Centre counts the number of Cardholders in a Zone and sets the access mode to Dual Authorisation when the Zone is empty (i.e. two Cardholders are required to access the Zone). When there are only two Cardholders in the Zone, dual authorisation is required to exit the Zone.
This feature also allows multiple No-Alone Zones to be configured adjacent to each other. Whenever access is requested into a No-Alone Zone, Command Centre will check the count of Cardholders in each Zone to ensure no Cardholder is alone.
If all three remaining Cardholders in a No-Alone Zone need to move to an adjacent and empty No-Alone Zone, the third Cardholder will be given a configured grace period to leave the Zone before an alarm is raised. If the third Cardholder does not leave within the grace period, the exit access Zone will change to dual authorisation (i.e. the Cardholder will not be able to exit).
This procedure describes how to configure an Access Zone as a 'No-alone Zone'.
Notes:

- 'No-alone zone' is not functional for Access Zone Groups, (i.e. an Access Zone that is already a Master Zone cannot then be configured as a 'No-alone zone'. Likewise, you cannot select an already configured 'No-alone zone' as a Master Zone).
- The minimum Zone count should be set to two for this feature to function as described.

Recommendations

- The 'No-alone Zone' feature is not recommended for turnstiles or pushbutton release, and cannot be used for elevator control.
- The situation may arise where an individual cardholder is trapped in a 'No-alone Zone' on their own, and is therefore unable to leave. It is recommended that a panic button be installed so operators can be alerted if this occurs.
- It is recommended that your site has procedures in place for correcting the zone count when events occur that may render the zone count inaccurate, (i.e. override Access Zones to free, open door override or emergency release).
- It is recommended that your site has procedures in place so tailgating is not allowed when physically exiting a 'No-alone Zone'.

Procedure

Door Set-up

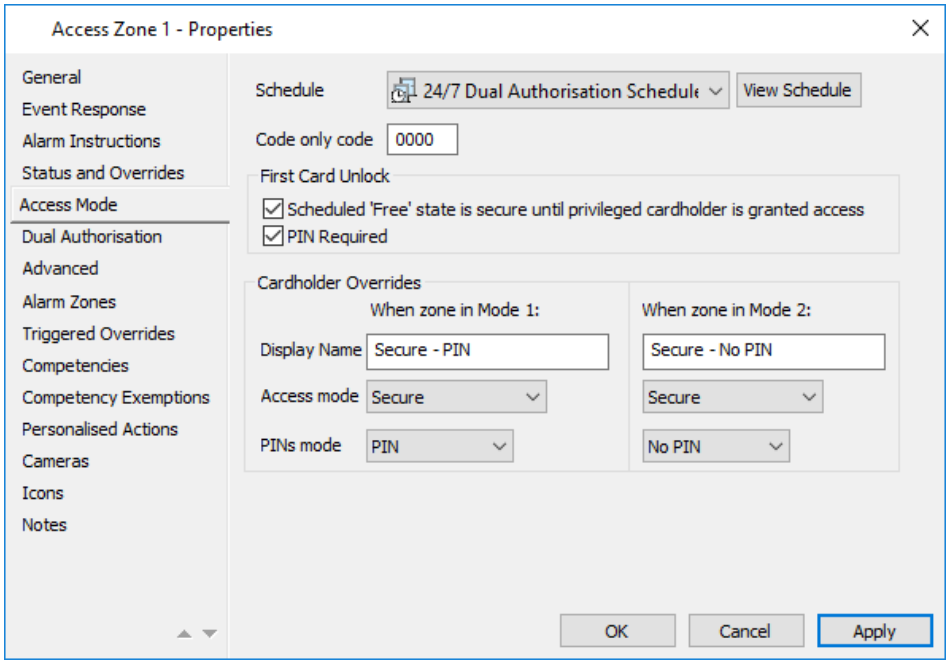
This part of the procedure needs to be repeated for each Door.

1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens (in grid view).
2. Open the properties of the Door.
3. Click the **Devices** tab and select Inputs for the open sensor, lock sensor and an Output for the unlock output, as required.
4. Click the **Entry Zone** tab and select an Entry Access Zone and an Entry Reader.
5. Click the **Exit Zone** tab and select an Exit Access Zone and an Exit Reader.
6. Click **OK** to exit and save your changes.
7. Repeat Steps 2-6 for each Door.

Entry Access Zone Set-up

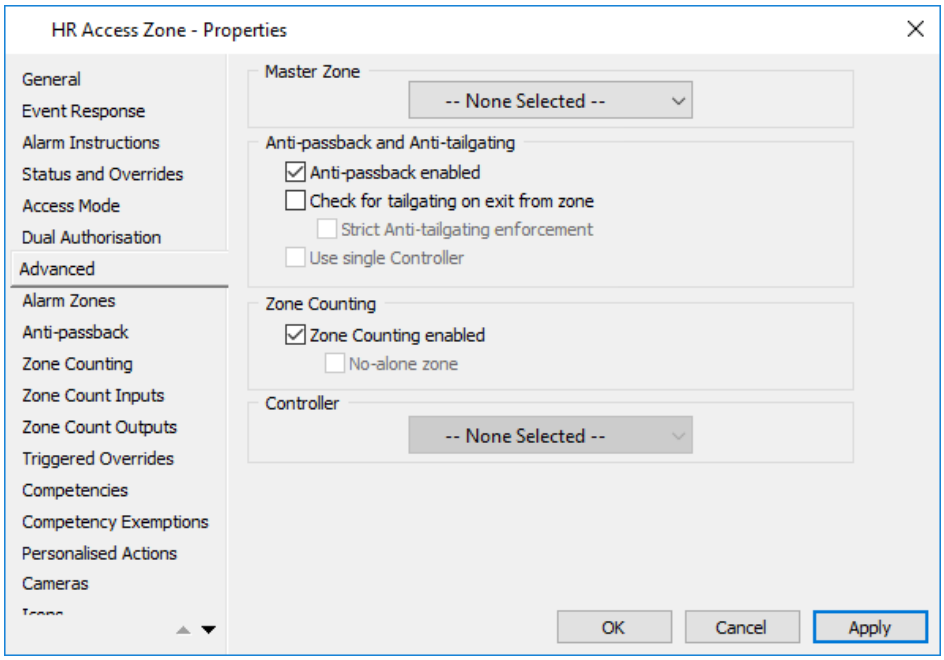
This part of the procedure needs to be repeated for each Access Zone you want to configure as a 'No-alone Zone' Entry Access Zone.

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone to be configured as a 'No-alone Zone'.
3. **Right click** and select **Properties**.
4. Click the **Access Mode** tab.

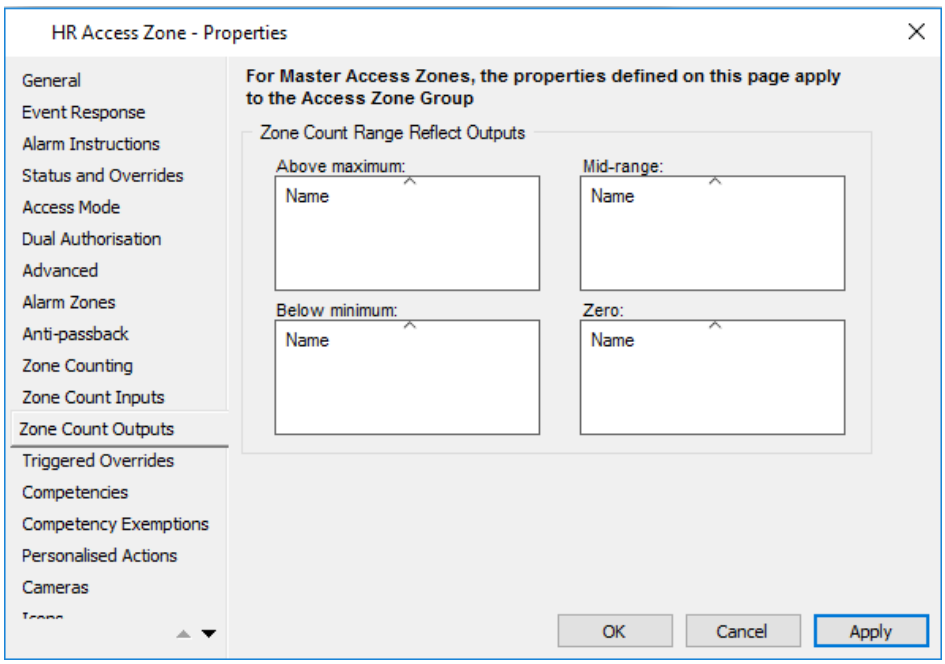


5. From the **Schedule** drop-down list, select an appropriate Schedule for the hours you require 'No-alone Zone' to be enabled for.
   Ideally a 24 hour dual-authorisation Schedule should be used.
   Note: Dual Authorisation is not supported for Elevator use.
6. In the 'Cardholder Overrides' section change the Mode 2 Access mode to Secure.

7. Click the **Advanced** tab.
8. Check the **Zone Counting enabled** checkbox.
   The **No-alone zone** checkbox and the **Controller** drop-down list become enabled, and two new tabs appear, (i.e. **Zone Counting** and **Zone Count Outputs**).



9. Check the **No-alone zone** checkbox.
10. Select a **Controller** from the drop-down list.
11. Click the **Zone Count Outputs** tab.



12. Drag (or copy and paste) the required outputs to use for reflecting the zone count states.

13. Click **OK** to exit and save your changes.
    Note: The 'Save' will fail if **No-alone Zone** has been checked without a Controller being selected. In this case you have to re-enable the checkbox before removing the outputs from the **Zone Count Outputs** tab.
14. Repeat Steps 2-13 for each Access Zone to be configured as a 'No-alone Zone' Entry Access Zone.

Exit Access Zone Set-up

This part of the procedure needs to be repeated for each Access Zone you want to configure as an Exit Access Zone.

1. Open the properties of the Access Zone you want to configure as an Exit Access Zone.
2. Click the **Access Mode** tab.
3. From the **Schedule** drop-down list, select an appropriate Schedule for the hours you require 'No-alone Zone' to be enabled for.
   Ideally a 24 hour dual-authorisation Schedule should be used.
   Note: Dual Authorisation is not supported for Elevator use.
4. In the 'Cardholder Overrides' section change the Mode 2 Access mode to Secure.
5. Click **OK** to exit and save your changes.
6. Repeat Steps 1-5 for each Access Zone to be configured as an Exit Access Zone.

Result

An Access Zone has been configured as a 'No-alone Zone'.

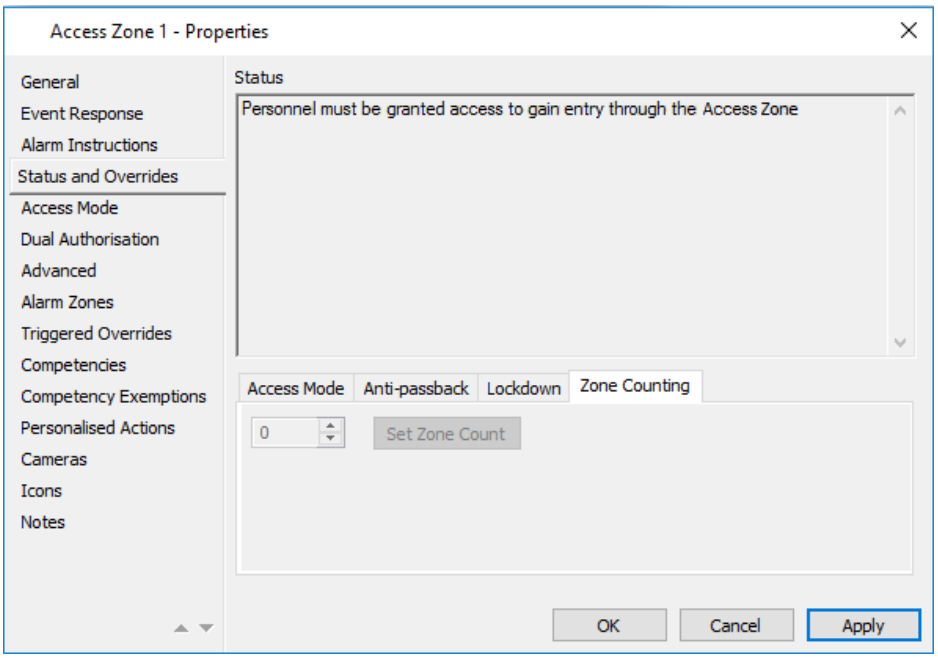
Manually Resetting Zone Counts

Introduction

This procedure enables an operator with the "Override" operator privilege to force a state change by manually setting the zone count to a different threshold.
When an Access Zone is part of an Access Zone Group which has zone counting active, any zone count change shall be applied to the Access Zone Group, not only the individual Access Zone.
Hint:
Placing all members of an Access Zone Group into one of the panes on the Status Viewer makes it easy to check that the zone count has been changed for all members of the group.

Procedure

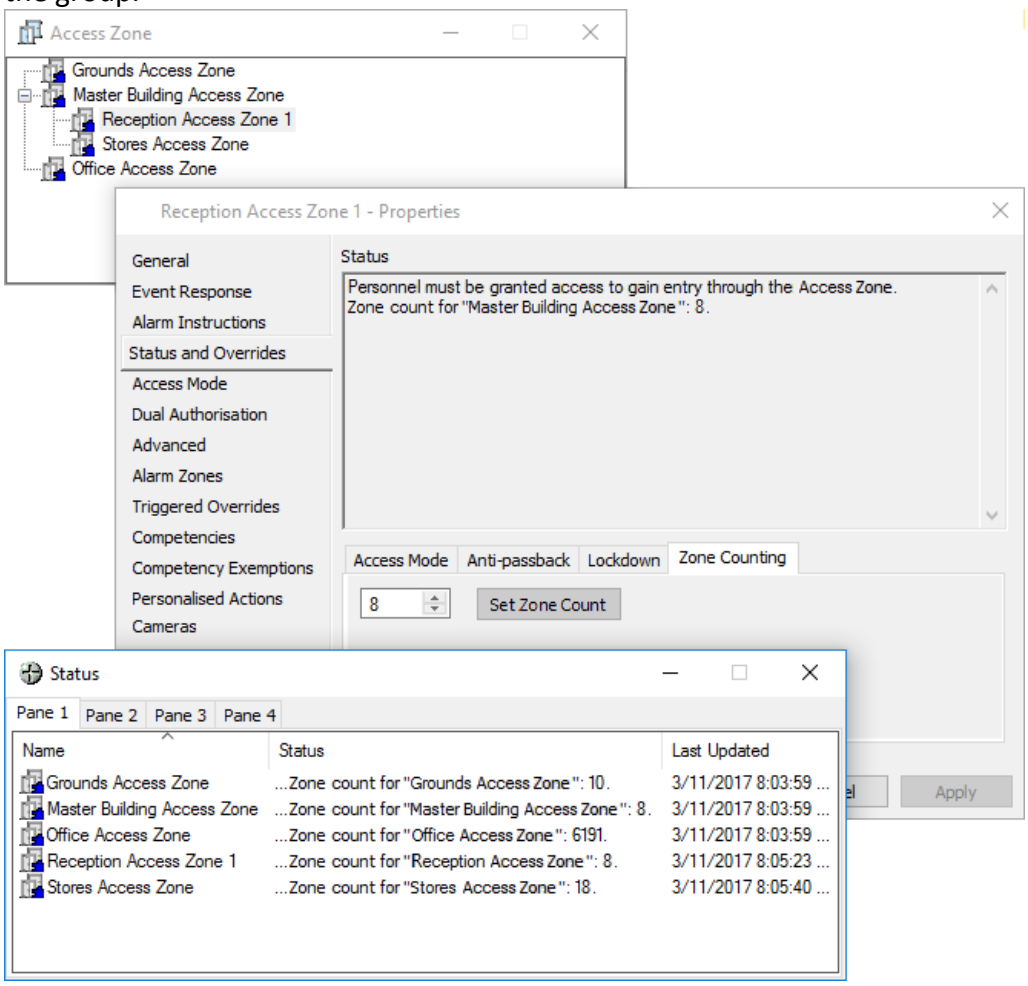
1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to manually reset the zone count state for.
3. **Right click** and select **Properties**.
4. Click the **Status and Overrides** tab.
5. Click the **Zone Counting** tab within this screen.
6. Enter the number of people in the Access Zone in the zone count  field.



7. Click the **Set Zone Count** button.

Result

The zone count state is changed for the Access Zone. If the Access Zone is a member of an Access Zone Group, the zone count change is applied to all other members of the group also.
On the Access Zone properties (the **Status and Overrides** tab as shown in the above screen shot), the value of the zone count is updated in the Status section.
If you have placed all the members of an Access Zone Group into one of the panes on the Status Viewer, the zone count has changed for all members of the group.



Configuring Pushbutton Overrides

Introduction

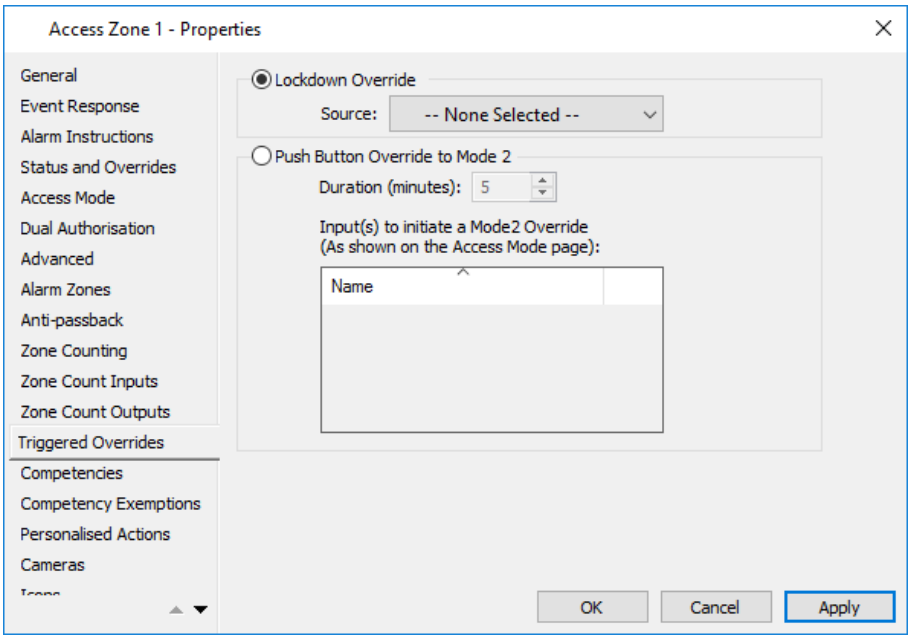
The pushbutton override feature can be used to temporarily set an Access Zone (or an elevator floor) to free access for a defined period of time to allow visitors to travel to the correct floor in a building.

For example:
On arrival at an apartment building, a visitor calls the apartment they wish to visit using the intercom system. To allow the visitor entry, the tenant activates a pushbutton which unlocks the apartment building front door and enables the elevator floor button for the required floor.

This procedure allows you to configure a pushbutton override and the time period that the zone will be in free access.

Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to configure pushbutton override functionality for.
3. **Right click** and select **Properties**.
4. Click the **Triggered Overrides** tab.
   Notes:
   - By default the **Lockdown Override** radio button is enabled.
   - This tab allows you to configure EITHER pushbutton overrides OR lockdown functionality for an Access Zone, (i.e. you cannot use both features for the one zone).



5. Click the **Push Button Override to Mode 2** radio button.
   The fields in this section of the screen become enabled.
6. Set the override time, (i.e. how long the zone will be in free access), in the **Duration** field.
   Note: The default time is 5 minutes.
7. Drag (or copy and paste) the input source required to initiate the override into the grid.
   Note: The input source can be an input, an output, a virtual output or a logic block.
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.
9. All Access Zones (or elevator floors), in the building need to have an input source assigned to them to perform the override function. Therefore, repeat Steps 2 - 8 for every Access Zone.

Result

The pushbutton override feature has been configured for the building.

Hint

Event Reporting
By default, the pushbutton override will NOT generate an event. However, if you do require events to be generated, this can be achieved by setting up Action Plans for the input sources, (i.e. inputs, outputs, virtual outputs and/or logic blocks) used for pushbutton overrides, as follows:

1. Open the properties for the input source.
2. Click the **Event Response** tab.
3. Assign the appropriate Action Plan to the 'Closed' Event Group.
4. Repeat Steps 1 - 3 for each input source used for pushbutton overrides.

Configuring Personalised Actions for Access Zones

Introduction

The Personalised Actions feature allows specific actions to be triggered for specific cardholders, upon being granted access to an Access Zone.

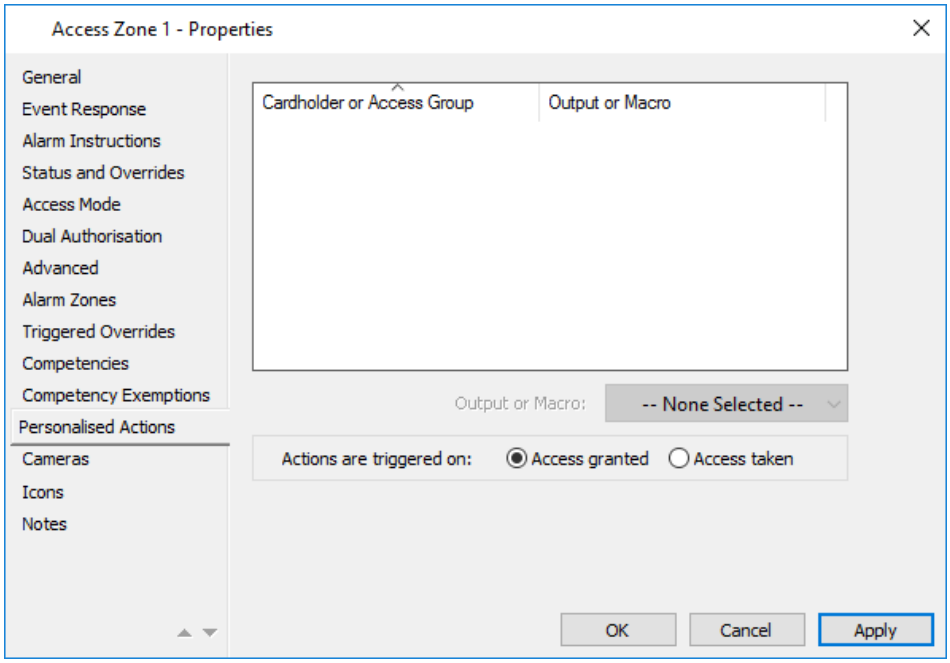
This procedure allows operators with "Edit Site" operator privileges to configure Personalised Actions. The available actions are running a Macro or Output status change. These actions can be assigned directly to a Cardholder or to an Access Group.
Note: The Personalised Actions feature does not support Lift Cars.

IMPORTANT:

- For personalised action macros to run successfully, the Controllers must be online with the CCFT server. If the CCFT server is shutdown or otherwise offline at the time of an access then any configured macro actions will not be run.
- For personalised action outputs to be switched successfully, the Controller hosting the output must be contacted by the Controller hosting the door. This means that if there is a network outage at the time of the access then any configured output actions will not be run if the outputs are on a remote Controller. Ideally, personalised action outputs should be located on the same Controller that is hosting the door hardware that provides the access.

Procedure

1. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
2. Highlight the Access Zone you want to configure Personalised Actions for.
3. **Right click** and select **Properties**.
4. Click the **Personalised Actions** tab.



The grid on this screen allows you to create a list of Personalised Actions for this Access Zone.

5. Drag and drop either individual Cardholders or Access Groups, as required, from the appropriate List Window into the grid.
6. Highlight the Cardholder or Access Group you wish to assign an action to. The **Output or Macro** drop-down list becomes enabled.
7. Select the required **Output or Macro** from the drop-down list.
   Alternatively, drag and drop an output or macro from the appropriate List Window.
   Note: The following table provides a list of the types of pre-configured actions that can be assigned to Cardholders and/or Access Groups:

Pre-configured action	can be achieved by...
Trigger one or more outputs	assigning the output(s) directly to a Cardholder or Access Group on this tab.
Trigger a macro (to print a report, run a command or trigger further outputs	• assigning the macro directly to a Cardholder or Access Group on this tab, or alternatively • a macro can be triggered via an Action Plan associated with an output.
Trigger an override of any sort, (e.g. Access Zone, Alarm Zone, output)	• assigning an output with an associated Action Plan that triggers a macro override, or • assigning the macro override directly to a Cardholder or Access Group on this tab.
Raise an alarm from an output	assigning an output to a Cardholder or Access Group on this tab.

8. Repeat Steps 5 - 7 for other Personalised Actions as required.
   Notes:
   - For individual Cardholders, the action will only happen when that Cardholder accesses the zone. However, for Access Groups the action will happen when any member of that group accesses the zone.
   - Multiple actions can be configured for a single Cardholder or Access Group by creating additional list entries.
   - There is a limit of 250 unique Cardholders and Access Groups in the list of personalised actions. Each Cardholder or Access Group is counted only once, even if they appear multiple times, (e.g. an Access Group has eight actions against it but is only counted once).
9. Click the appropriate "Actions are triggered on" radio button to define what will trigger the personalised actions, as follows:
   - **Access granted** = Actioned on access granted to the zone.
   - **Access taken** = Actioned on access granted and taken to the zone.

   Note: This setting will apply to **all** the personalised actions for this Access Zone.
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.

Chapter 11: Day Categories

Days are assigned to Categories on a schedule, (e.g. Monday to Friday could use a "Weekday" category, while Saturdays and Sundays may require a category each).

Specific dates such as holidays are also assigned categories, which override the repeating schedule for that day. Holidays display by default in all new schedules and can be configured as required.

Refer to ***Operator Privileges*** (on page 37-1) to check you have the correct operator privilege level for the activity you wish to perform.

Adding a new day category

Introduction

This procedure enables you to add a new day category to Command Centre.

Procedure

1. Click **Configure** from the menu bar, then **Day Categories**.
   The **Day Categories** List Window opens (in grid view).
2. **Right click** and select **New...Day Categories**.
   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 **Colour** tab.
5. Select a new colour by clicking the **Change Colour** button.
6. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Day Category.
   For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
7. Click the **Notes** tab if you want to add a note(s) about this Day Category.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
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 new Day Category is created.

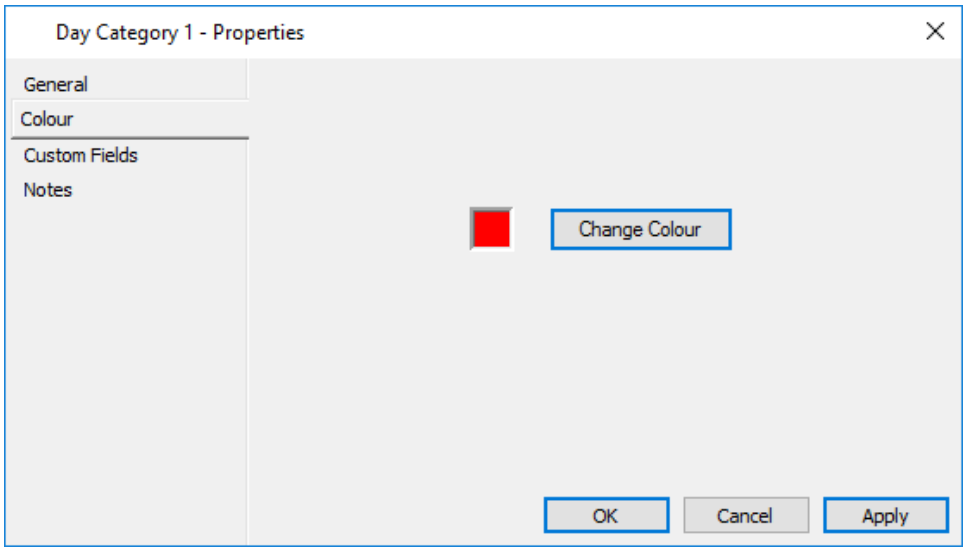
Changing the day category colour

Introduction

This procedure enables you to change the colour of a day category.

Procedure

1. Click **Configure** from the menu bar, then **Day Categories**.
   The **Day Categories** List Window opens (in grid view).
2. **Right click** and select **New...Day Categories**.
3. Click the **Colour** tab.



4. Click the **Change Colour** button.
5. From the displayed colour swatch, select the required colour.
6. Click **OK**.

Result

The selected colour now displays within the colour tab.

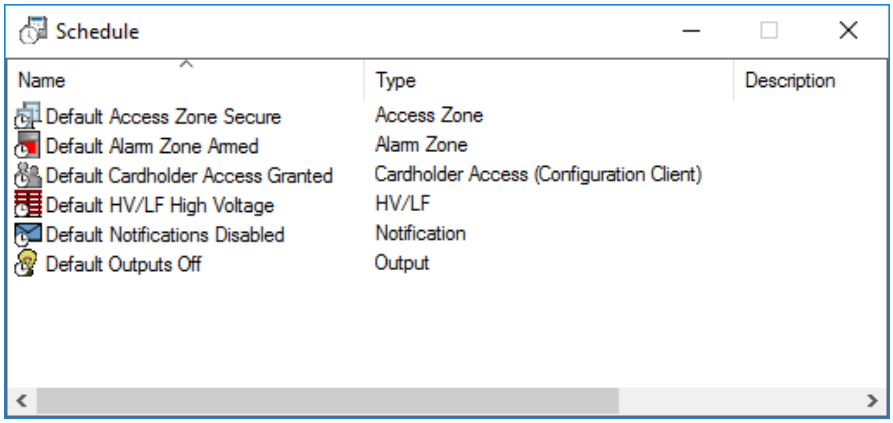
Any calendar days currently set to this day category are updated to reflect the change in colour.

If the Schedules window currently contains this Day Category, it is updated to reflect the change in colour.

Chapter 12: Schedules

Schedules are one of the three prerequisites of Access Groups. You must have the Schedules set up before you can link cardholders to Access Groups.

A Schedule is a "list of times and states that control an item". By default, there are six "Default Schedules" already configured in the system, (i.e. one for each of the six Schedule Types; Access Zone, Alarm Zone, Cardholder Access, Notification and Output).
Note: The Notification Schedule only appears if your site is licensed for Notifications.



Schedules Types indicate what attribute they relate to. For example:
Cardholder Access type schedules relate to access = when the cardholder has access.
Alarm Zone type schedules relate to Alarm Zones = when items change state.

Example:
Using schedules you can set an alarm zone to unset at the same time an associated access zone changes to free access.

Before setting Schedules you must ensure ***Day categories*** (on page 11-1) and ***Calendar days*** (on page 13-1) (Day Categories assigned to Calendar) are already set up.
Note:
Schedules and active Day categories in the default calendar need to stay in sync. To do this, update schedules so that they reflect the active day categories assigned to the default calendar.

Refer to ***Operator Privileges*** (on page 37-1) to check you have the correct operator privilege level for the activity you wish to perform.

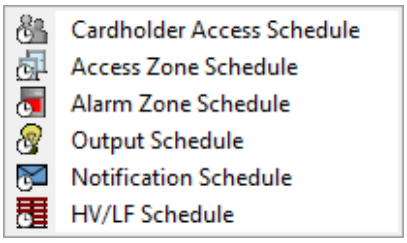
Creating a new Schedule

Introduction

This procedure enables you to set up a new schedule.

Procedure

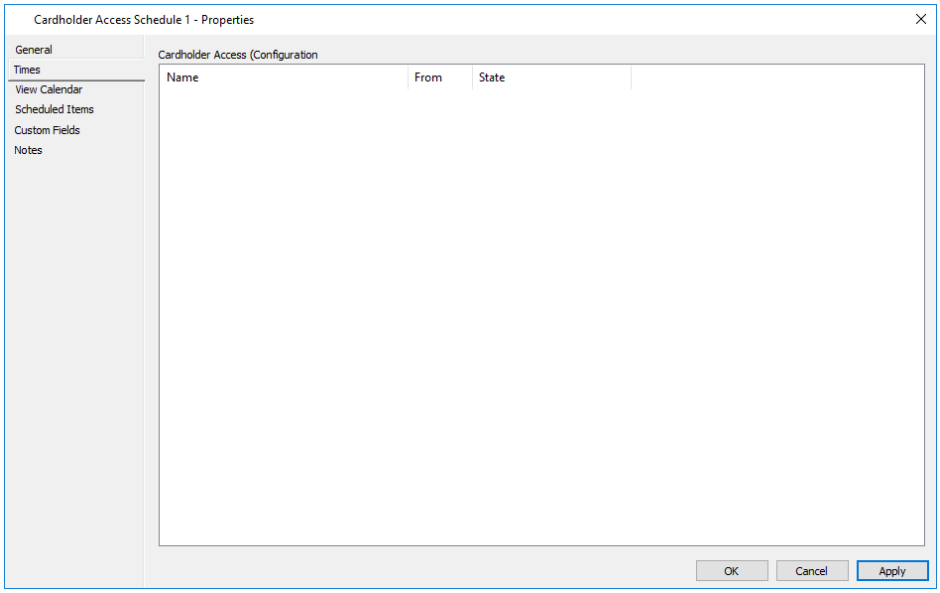
1. Click **Configure** from the menu bar, then **Schedules**.
   The **Schedule** List Window opens (in grid view).
2. **Right click** and select **New...**
   The following context menu displays, listing the six schedule types available.



Notes:

- The Notification Schedule type only appears if your site is licensed for Notifications.
- The HV/LF Schedule type only appears if your site is licensed for Fence Controllers.

3. Select the type of Schedule required.
   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 **Times** tab.



This tab provides a grid where 'From' times and states can be entered/edited for each Day Category. Initially the grid will be blank.

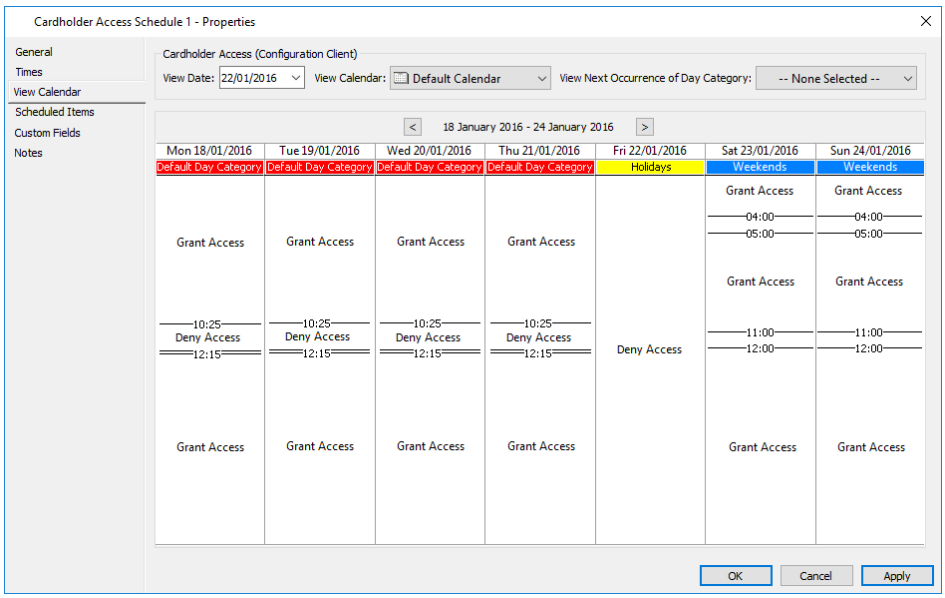
6. Add and remove any other Day Categories required for this Schedule. See ***Adding Day Categories to Schedules*** (on page 12-6) and ***Removing Day Categories from Schedules*** (on page 12-7) for procedure.

   Note: Ensure you are consistent in the use of day categories between calendars and schedules.

7. Add, remove or change the times and states of each Day Category as required. See ***Changing times and states within Schedules*** (on page 12-8) for procedure.

   Note: If the times and states for one Day Category are required for another Day Category, these can be duplicated (copied) to another Day Category to speed up the process. See ***Duplicating Day Category entries*** (on page 12-12) for the procedure.

8. Click the **View Calendar** tab.

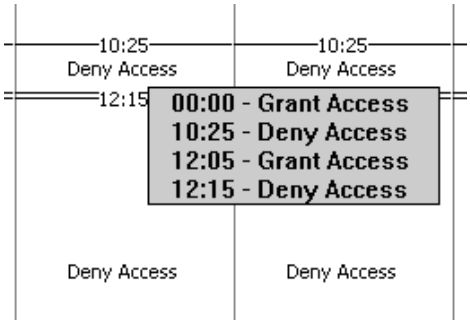


This tab is "read-only" and displays the following:

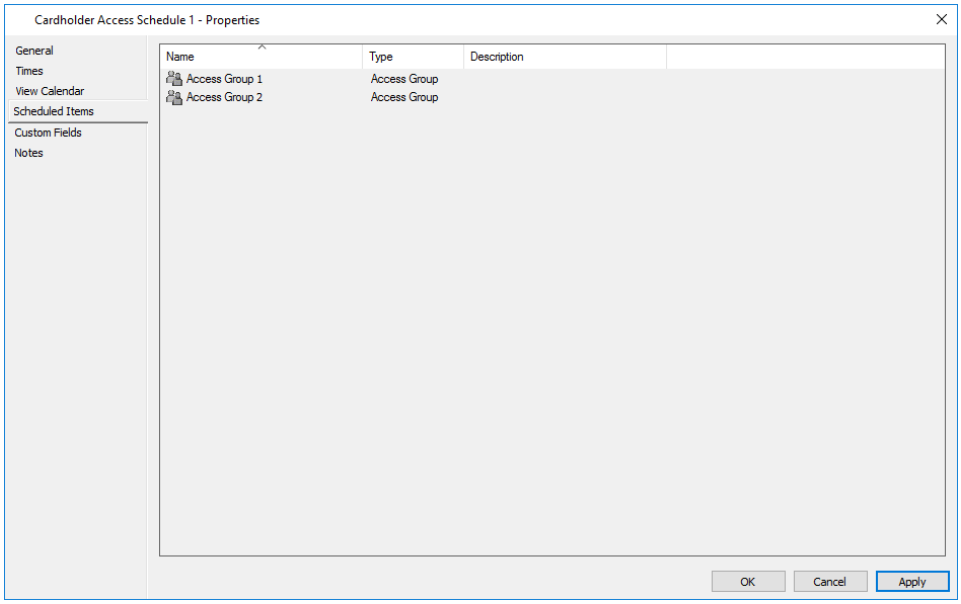
- Weekly view of the states in existence for the Schedule
- Each day will display the active Day Category
- Scroll mechanism(s) to change the active week view (Monday will always be the left-most column)
- A Calendar control to view any Special Calendars that may exist
  Note: The "View Calendar" field does not appear on the **Calendar** tab for a Notification Schedule.
- An ability to quickly find the next occurrence of a particular Day Category

Note: If state changes are so close together due to there only being a short interval between them, the time cannot be displayed legibly inside

the interval. Therefore, by hovering the mouse over the day, a summary of the times and states for that particular day display. In the following example, **12:05 - Grant Access** only displays when you hover over the day.



9. Click the **Scheduled Items** tab.



This tab shows a "read-only" list of items that the schedule is attached to. The items listed will depend on the Schedule type, as follows:

Schedule Type	Description of Listing
Cardholder Access	Access Groups that have some zone access controlled by the Schedule.
Access Zone	Access Zones associated with the Schedule.
Alarm Zone	Alarm Zones that are controlled by the Schedule.
Output	Output items that are controlled by the Schedule.
Notification	Cardholders that have the Schedule on a filter/schedule assignment.
HV/LF	Alarm Zones (assigned to a Fence Zone) associated with the Schedule.

10. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Schedule.
    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 Schedule.
    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.

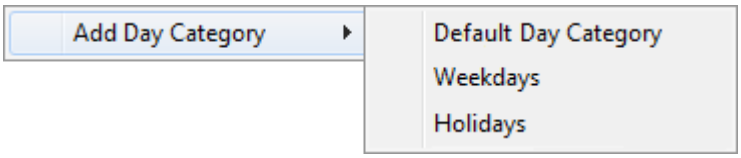
Hint

Editing and Deleting Schedules
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Schedules.
Note: If a schedule has items which depend upon it for proper operation, you are prompted for confirmation and cannot delete it even when **Yes** is clicked. A message explaining why you cannot delete the schedule displays.

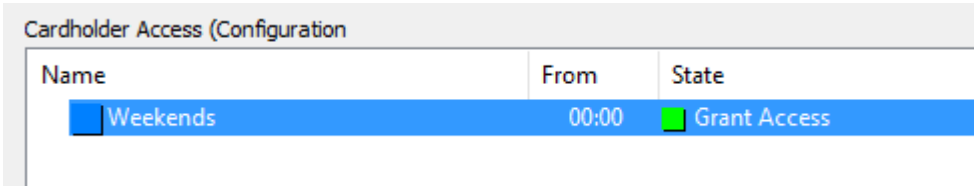
Duplicating Schedules
Operators privileged to create schedules can also duplicate schedules, which makes the task of setting up multiple schedules that are very similar much quicker. This is achieved by **right clicking** on the schedule in the Schedule List Window and selecting **Duplicate...**
Note: If multiple schedules are highlighted when you select **Duplicate...**, then they will all be duplicated.

Adding Day Categories to Schedules

1. Click **Configure** from the menu bar, then **Schedules**.
   The **Schedule** List Window opens (in grid view).
2. **Right click** on the required schedule, and select **Properties**.
3. Click the **Times** tab.
4. **Right click** and select **Add Day Category**.
   A context menu with all the Day Categories set up in the system display.



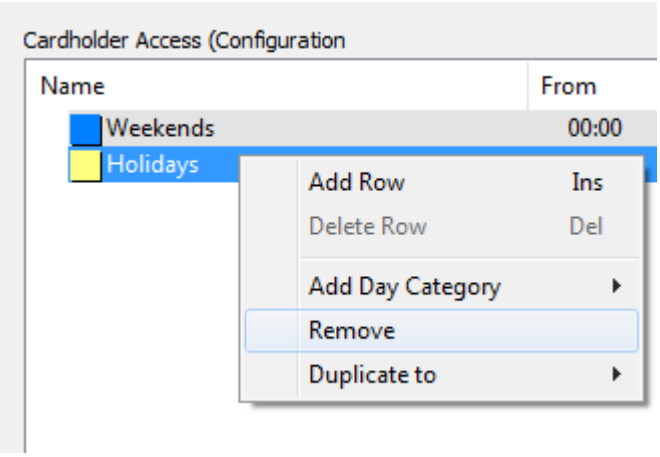
5. Select the required Day Category.
   The Day Category now displays in the grid.



   The first record/row will display the non-updatable **From** time of 00:00 (midnight). The **State** will display the default state, and is editable for this first and all successive rows. See ***Changing times and states within Schedules*** (on page 12-8) for the procedure.
6. Repeat Steps 4-5 for each Day Category you wish to add to the schedule.
   Note:
   If all Day Categories are added to the Schedule, the **Add Day Category** button is no longer enabled.

Removing Day Categories from Schedules

1. Click **Configure** from the menu bar, then **Schedules**.
   The **Schedule** List Window opens (in grid view).
2. **Right click** on the required schedule, and select **Properties**.
3. Click the **Times** tab.
4. Highlight the Day Category you want to remove, and **right click** on it.
   A context menu displays.
5. Select **Remove** from the context menu.

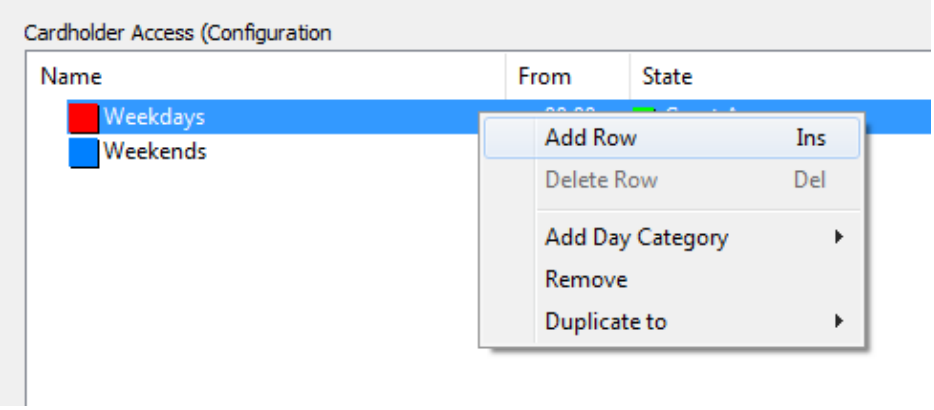


   A confirmation window displays.
6. Click **Yes** to remove the Day Category.
   The Day Category no longer displays on this tab.

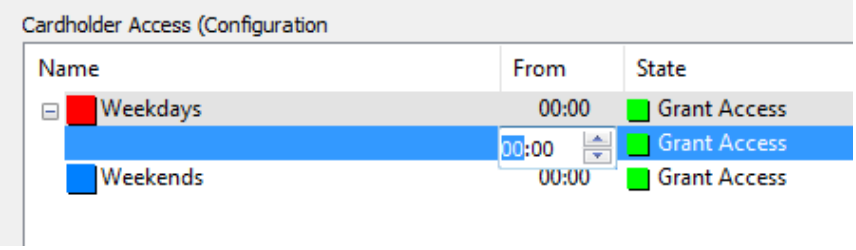
Changing times and states within Schedules

You can change the state of any of the time-state list options as required.

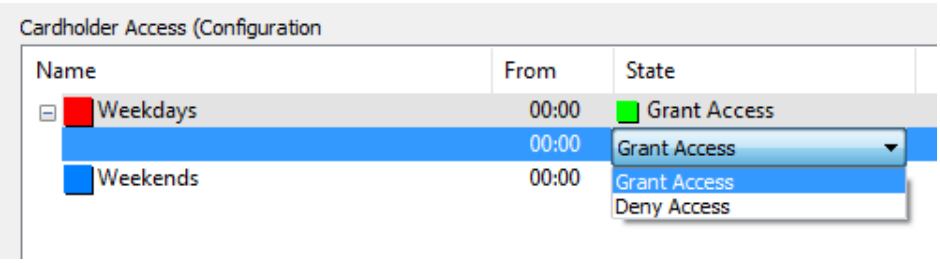
1. Click **Configure** from the menu bar, then **Schedules**.
   The **Schedule** List Window opens (in grid view).
2. **Right click** on the required schedule, and select **Properties**.
3. Click the **Times** tab.
4. **Right click** on the Day Category you want to make a state change to, and click **Add Row** from the context menu.



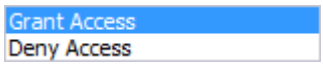
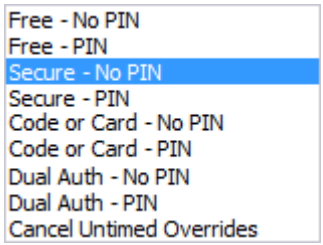
A new row is added to the Day Category with the Time Box on that row enabled.
Note: The **From** time of 00:00 (midnight) on the first row of a Day Category cannot be changed, however the State can be.

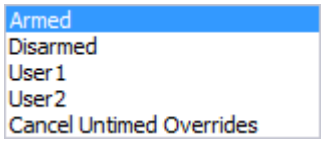
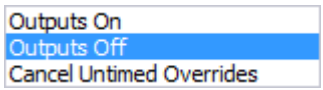
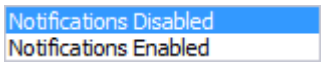
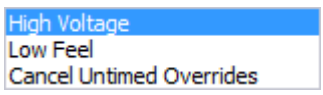


5. Alter the Time Box to the time you want the State to change from, and click on the State on that row.



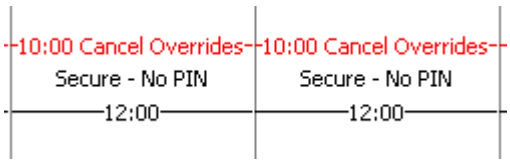
A drop-down box appears providing a list of the available states for the Schedule type.
The available states will depend on the Schedule type, as follows:

Schedule Type	Possible States (Note: The default state is highlighted)
Cardholder Access	 Access can be "Granted" or "Denied".
Access Zone *	 The various modes available set the access mode for the Access Zone, (e.g. Free - No PIN, Secure - No PIN, Secure - PIN, etc.). The access mode controls the credentials required in order to identify a Cardholder at the reader. **Note:** The access mode also controls the action required when performing an Access Zone or Alarm Zone override at the reader. For an HBUS Terminal, the Log On Credentials on the **Welcome Screen** tab control the action required when performing an Access Zone or Alarm Zone override at the terminal using the **Arm** or **Mode** keys. However, the access mode controls the action required when performing a double card override at an HBUS Terminal. *For example:* **Free - No PIN** With this mode the door is in free access. To perform an override you need to press the appropriate function key on the reader, (i.e. **Arm** or **F1** for Alarm Zones and **Mode** or **F2** for Access Zones), and present a valid access card. **Free - PIN** With this mode the door is in free access. To perform an override you need to press the appropriate function key on the reader, (i.e. **Arm** or **F1** for Alarm Zones and **Mode** or **F2** for Access Zones), present a valid access card and enter your PIN. **Secure - PIN** With this mode the door is secure. For access present a valid access card and enter your PIN. To perform an override you need to press the appropriate function key on the reader, (i.e. **Arm** or **F1** for Alarm Zones and **Mode** or **F2** for Access Zones), present a valid access card and enter your PIN.

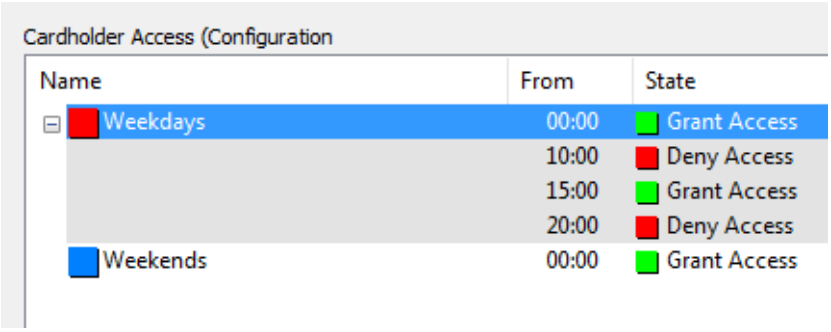
Schedule Type	Possible States (Note: The default state is highlighted)
	Code or Card - No PIN With this mode, for access you can either enter the 4 digit code (set on the 'Access Mode' tab of the Access Zone Property pages), or present a valid access card. To perform an override you need to press the appropriate function key on the reader, (i.e. **Arm** or **F1** for Alarm Zones and **Mode** or **F2** for Access Zones), and present a valid access card. **Dual Auth - No PIN** With this mode, access is gained by two authorised Cardholders, each presenting a valid access card. To perform an override you need to press the appropriate function key on the reader, (i.e. **Arm** or **F1** for Alarm Zones and **Mode** or **F2** for Access Zones), and present a valid access card. **Note:** Dual Authorisation is not supported for Elevator use.
Alarm Zone *	 (or as defined in Server Properties, **Alarm Zone States** tab) All items in the Alarm Zone change to the same state (set/unset, armed/disarmed) at the same time.
Output *	 Sets the action (on, off, etc.) of the outputs that are assigned to this Schedule. This is where you would configure a Time Clock Relay.
Notification	 Notifications can be "Disabled" or "Enabled". If in "Disabled" state, then cardholders with this Schedule will not receive notifications during this time.
HV/LF *	 Set the action (High Voltage, Low Feel or Cancel Untimed Overrides) for all Alarm Zones that this Schedule has been assigned to.

***** Included in the list of list of States is the option to **Cancel Untimed Overrides**. A **Cancel Untimed Overrides** instance entered at a particular time of day returns the state of an Access Zone, Alarm Zone, Output or HV/LF type Schedule to the scheduled state.

A **Cancel Untimed Override** instance entered on a Schedule acts to cancel any non-timed override in existence for all items controlled by that Schedule. As it does not have a time interval it appears on the **Calendar** tab as a single thin red line, so it is easily recognised as a cancel override.



6. Select the required State from the drop-down list.
7. Repeat Steps 4-6 for each state change you want to make to any of the Day Categories on this Schedule. The following screen shot is an example of how the screen will start to look as you add state changes.

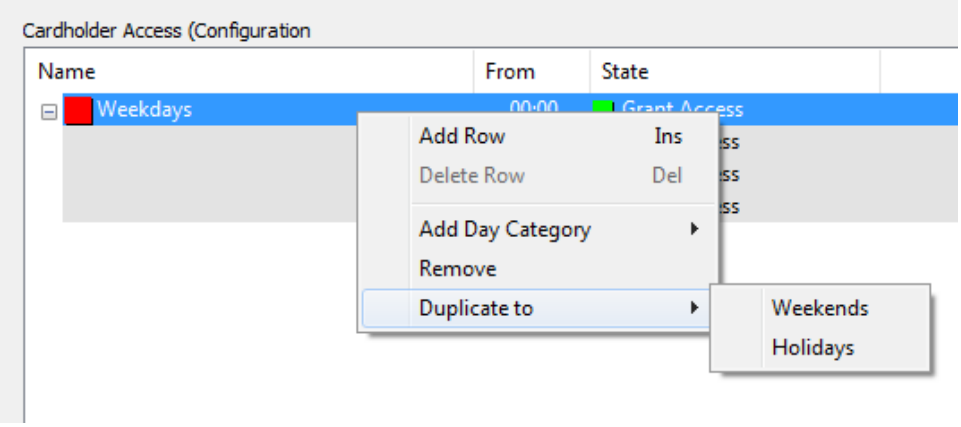


Note: Each Day Category can be collapsed to minimise the space taken up on the grid. This is achieved by clicking the ⊟ icon. The icon changes to ⊞, which can be clicked to expand the Day Category again.

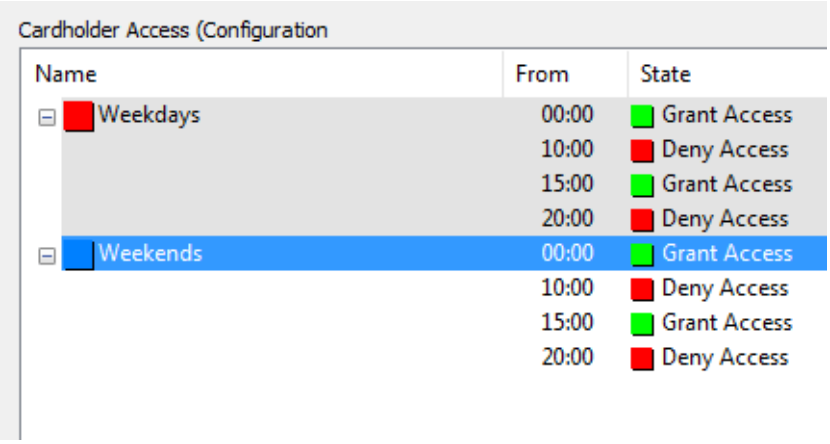
Duplicating Day Category entries

You can duplicate/copy all entries including times and states entered against one Day Category, to another.

1. Click **Configure** from the menu bar, then **Schedules**.
   The **Schedule** List Window opens (in grid view).
2. **Right click** on the required schedule, and select **Properties**.
3. Click the **Times** tab.
4. **Right click** on the Day Category you want to copy the entries for, and click **Duplicate to** from the context menu.
   Another context menu displays listing all the Day Categories that are not already on the **Times** tab.



5. Click on the Day Category you want to duplicate the entries to.
   The Day Category you selected populates the grid with all the same times and states of the Day Category you copied from.



Chapter 13: Calendars

Using calendars, you assign Day Categories to days of the year.

Example:
Assign Monday to Friday to the Day Category "Weekday".
Assign Statutory holidays to the Day Category "Holiday".

There are two types of Calendars in Command Centre, as described below:

Calendar Type	Description
Default Calendar	Only one default system-wide calendar can exist. Day categories can be assigned to a specific date or a particular day of the week within the default calendar. Changes to the day of the week day categories made at the default calendar level automatically apply system-wide.
Special Calendar	Multiple special calendars can exist. Special calendars cater for organisations that span multiple geographic areas by allowing their local operators to administer the scheduling of special days, (e.g. public holidays), applicable to their region or site. Special calendars display the same day categories that are assigned to a particular day of the week in the default calendar. Special calendars are assigned to an appropriate system division so they are viewable to operators that manage a certain physical region within the network.

Notes:

- While you can add or delete special calendars, you are not able to remove the default calendar.
- Day categories and calendar(s) should be set up before creating and assigning schedules. Any new day categories assigned to the calendar after creating schedules will need to be added to each existing schedule individually.
- It is recommended that any calendar changes are made out of normal business hours as they can result in system performance issues, (e.g. events get slower and slower, and then a barrage of events flood through).

You can move through the months displayed on the calendar by using the up and down arrow keys on your keyboard.

Refer to Operator Privileges to check you have the correct operator privilege level for the activity you wish to perform.

Viewing/Editing the Default Calendar

Introduction

This procedure enables you to view, and edit if necessary, the default calendar.

Procedure

1. Click **Configure** from the menu bar, then **Calendars**.
   The **Calendar** List Window opens (in grid view).

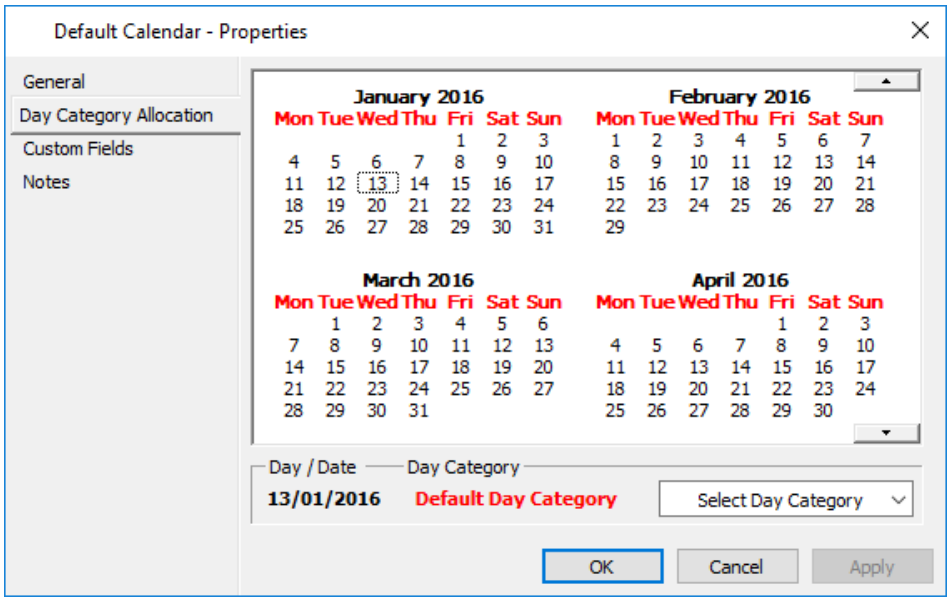
   Note: There are two slight variations of the calendar icon so you can easily identify special calendars from the default calendar.

   The  icon represents the default system-wide calendar, and the  icon represents special calendars.

2. **Right click** on the Default Calendar, and select **Properties**.
   The **General** tab of the Default Calendar displays.

   Note: You can alter the Name and/or Description of the Default Calendar and select another Division if required.

3. Click the **Day Category Allocation** tab.



   Today's date and the Day Category that applies displays in the lower part of the screen.

4. Edit if necessary.
   See ***Assigning Days to Day Categories*** (on page 13-5) and ***Resetting Dates*** (on page 13-7) for further details.

5. Click the **Notes** tab if you want to add a note(s) about the default calendar.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).

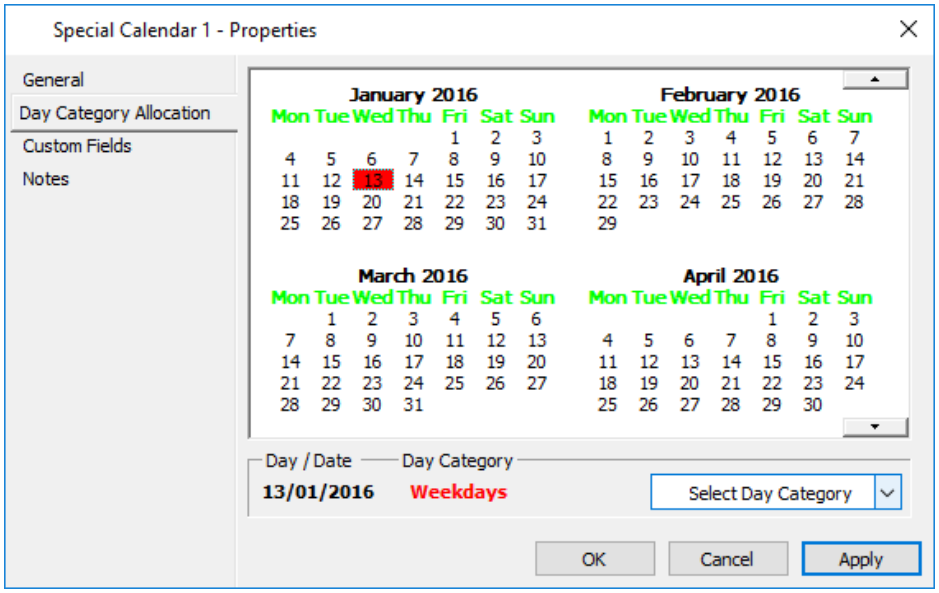
Creating a Special Calendar

Introduction

This procedure enables you to create a special Calendar. You must have the "Configure Site" operator privilege to perform this procedure.

Procedure

1. Click **Configure** from the menu bar, then **Calendars**.
   The **Calendar** List Window opens (in grid view).
2. **Right click** and select **New...Special Calendar**.
   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 **Day Category Allocation** tab.



5. Configure the special Calendar as required.
   See ***Assigning Days to Day Categories*** (on page 13-5) and ***Resetting Dates*** (on page 13-7) for further details.
6. Click the **Custom Fields** tab if you want to add and assign a custom field value to this special Calendar.
   For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
7. Click the **Notes** tab if you want to add a note(s) about this special Calendar.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
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 special Calendar is created.

Hints

Deleting Special Calendars
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete a Special Calendar.

Assigning Special Calendars to Controllers
One special calendar may be assigned to each Controller in the system (via the **Setup** tab of the Controller properties). Refer to ***Creating Controllers*** (on page 21-2) for further detail.

Assigning Days to Day Categories

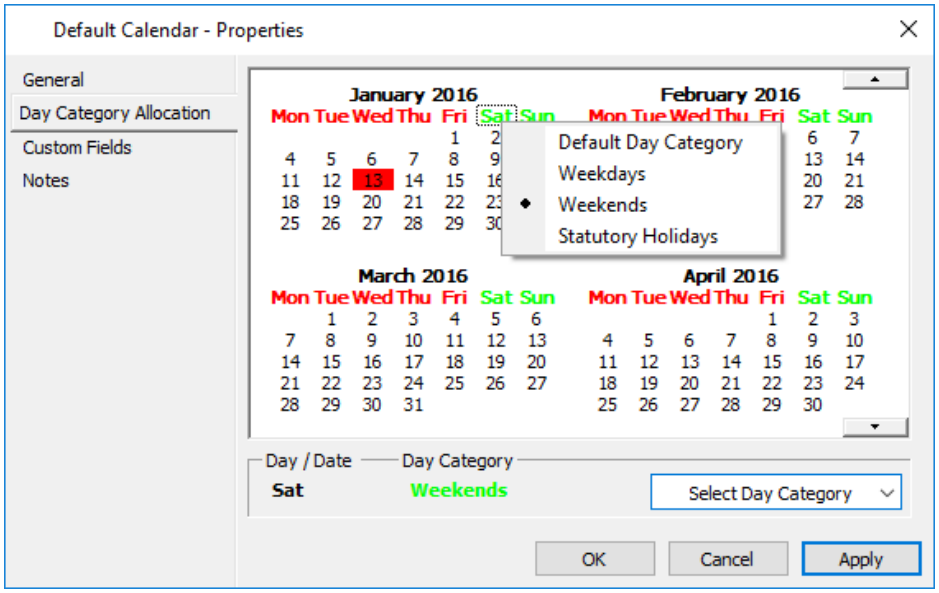
Introduction

The following procedures enable you to assign days to Day Categories.
Note: Individual dates, (e.g. Monday 25 October) can be assigned to Day Categories on any Calendar, whereas particular days, (e.g. All Saturdays) can be assigned to Day Categories only on the Default Calendar.

Procedure

Assigning particular days to Day Categories

1. Click **Configure** from the menu bar, then **Calendars**.
   The **Calendar** List Window opens (in grid view).
2. **Right click** on the Default Calendar, and select **Properties**.
3. Click the **Day Category Allocation** tab.
4. **Right click** on the Day name.
5. From the displayed pop-up menu, select the required Day Category.

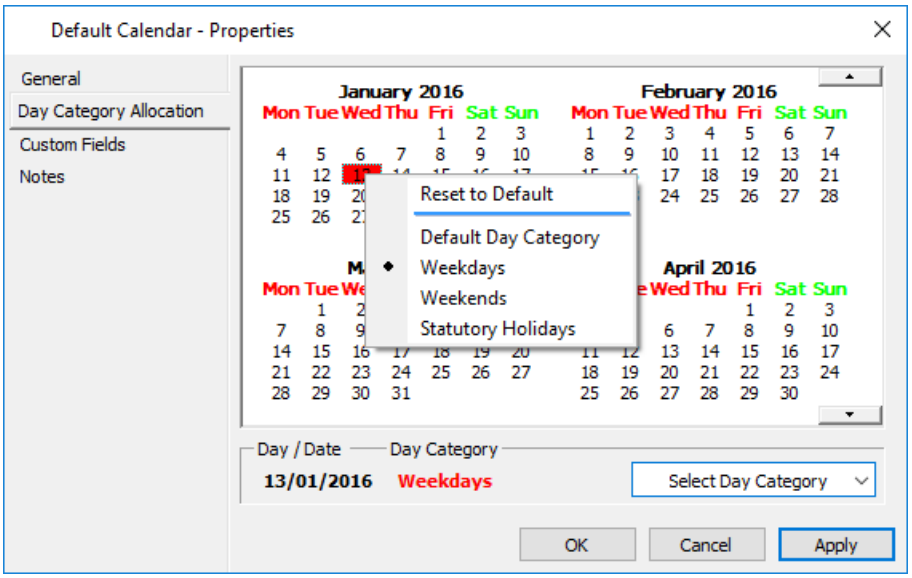


6. Click **OK** to exit and save your changes.
   Click **Cancel** to exit without saving your changes.
   Click **Apply** to save your changes and stay in this window.

Assigning individual dates to Day Categories

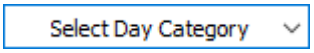
1. Click **Configure** from the menu bar, then **Calendars**.
   The **Calendar** List Window opens (in grid view).
2. **Right click** on the appropriate Calendar, (i.e. either the Default Calendar or a Special Calendar), and select **Properties**.

3. Click the **Day Category Allocation** tab.
4. Either:
   - **Right click** on the specific date.
     From the displayed pop-up menu, select the required Day Category.



   OR:

   - Click on the specific date.

     From the **Select Day Category** drop-down list 

     select the appropriate Day Category.

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

The day(s) selected change colour to reflect the colour you assigned to that Day Category.

Notes:

- How individual dates display once assigned to a Day Category depends on the type of Calendar used.

  15 A special day will display like this in the calendar it was defined in.

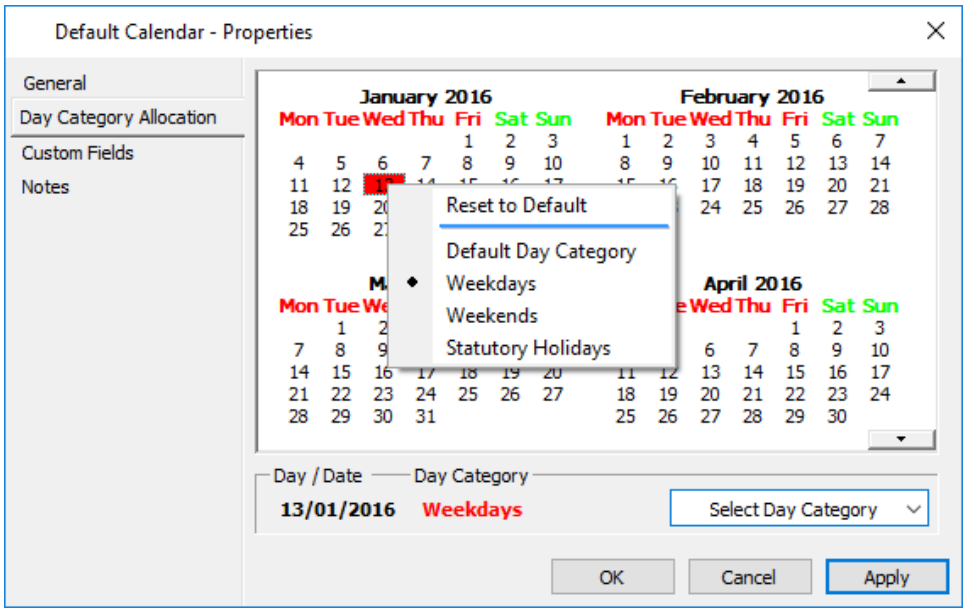
  15 A special day defined in the default calendar will display like this in a special calendar, but cannot be edited or 'Reset to Default' from the special calendar.

- There is a limit of 400 special days in the default calendar and 400 in each special (regional) calendar. This allows a total of 800 special days to be defined for any one special calendar. When the limit is reached, the system will remove special days in the past without warning, until all newly selected days can be added. If all special days in the past have been removed and the limit is still exceeded, the extra newly selected days will not be added and a warning message will display.

Resetting Dates

Procedure

1. Click **Configure** from the menu bar, then **Calendars**.
   The **Calendar** List Window opens (in grid view).
2. **Right click** on the required calendar, (i.e. the calendar the day was originally assigned in), and select **Properties**.
3. Click the **Day Category Allocation** tab.
4. **Right click** on the specific date you wish to change.
5. From the pop-up menu select **another Day Category** or **Reset to Default**.
   Note:
   A date that has already been assigned a Day Category in the default calendar can be overridden from the special calendar.



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

Result

The date is changed to the Day Category you selected.

Chapter 14: Alarm Zones

Understanding Alarm Zones

An Alarm Zone is a grouping of objects or entities whose states need to be armed and disarmed together.

Example 1 - *Localised Zone:*
When a staff member presents their card, they gain access to a specific Access Zone and the associated Alarm Zone is automatically disarmed. All the PIRs in that zone are deactivated, however PIRs in other Alarm Zones will be unaffected. At the end of the day the last person in the Alarm Zone can then arm the zone.

Example 2 - *Site wide zone:*
Doors entering a stairwell on each level are controlled by the Controller(s) on that floor. The Alarm Zone is spanned across multiple Controllers since the sensors for the various doors are on different Controllers. This Alarm Zone, although not recommended, can be spanned across multiple Controllers. See 'Alarm Zones shared across multiple Controllers' below for further detail.

The Alarm Zones can be set up to change automatically (via the Schedule) or manually (via a keyswitch or override from a allagher keypad reader).

Alarm Zones shared across multiple Gallagher FT Controllers

Alarm Zones are known to operate reliably when shared (spanned) across multiple Controllers. If however one or more of the Controllers go offline due to network failure, then the Alarm Zone will remain in the state it was in when the Controller(s) went offline. Any manual Alarm Zone overrides attempted during this time will fail. This manual state change can be reapplied once the Controller(s) are back on line.

If an Alarm Zone state change is scheduled, and the Controller(s) is offline, then the Alarm Zone state will remain unchanged until all of the Controller(s) sharing that Alarm Zone are back on line; in which case the Alarm Zone will change to the scheduled state within 60 seconds.

Arming Alarms Zones using the T20 Terminal

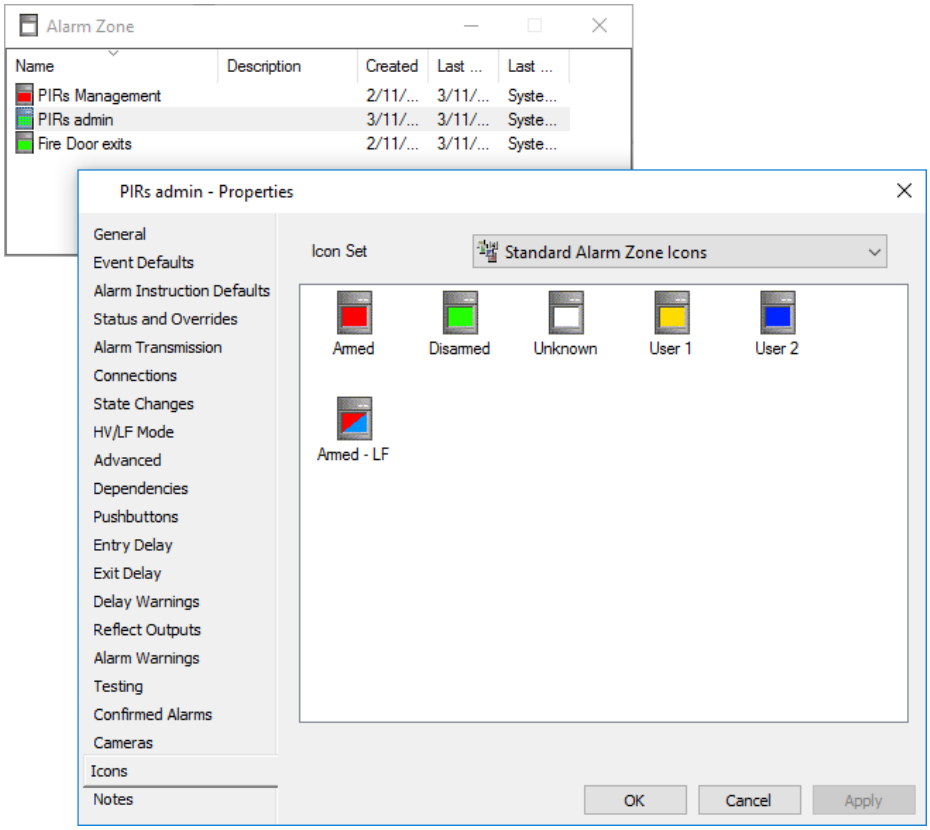
It is not possible to collectively or individually arm Alarm Zones in User 1 or User 2 state from a T20 Terminal without disarming the Alarm Zones first. When arming all Alarm Zones (of which some zones are in User 1 or User 2 state), the User 1 and User 2 zones will not be armed.

Terminology

Your system is configured to display your preferred terminology regarding Alarm Zones (Armed/Disarmed OR Set/Unset). Refer to "Alarm Zone States" within Server Properties.

Alarm Zone States

There are different icons for the states of Alarm Zones, so you can see from this window what state an Alarm Zone is in, depending on how you have your icon set configured, (e.g. green for disarmed, red for armed, white for unknown, etc.). Opening the **Icons** tab of an Alarm Zone's properties shows the different icons for each state.



For each Alarm Zone state you can select different priorities, outputs to switch and escalation times.

Set / Armed
In this mode the alarms are set. The alarm will be triggered if inputs change state and/or unit events are generated. This can be considered the active state for the Alarm Zone.

Unset / Disarmed
In this mode the alarms are unset.

User 1 and User 2
If required, you can set up these additional two Alarm Zone states to suit.

Setting up Alarm Zones

Introduction

You need to create an Alarm Zone for each grouping of objects or entities whose states need to be armed and disarmed together.
This procedure is split into three parts, as follows:

- Creating an Alarm Zone, (i.e. providing the minimum information required to create a new Alarm Zone)
- Configuring an Alarm Zone,
  (i.e. linking the various components to it - Divisions, Schedules, Action Plans and Alarm Instructions are the components of an Alarm Zone).
- Initialising Alarm Zone functionality,
  (i.e. associating inputs with the Alarm Zone so they recognise any Alarm Zone state changes).

You can create a new Alarm Zone, then configure it at a later stage, once you have set up the necessary components for it.
Note: To maintain system integrity in the event of a communications failure, it is recommended that you have an independent Default Alarm Zone for each Controller, and that entities used in an Alarm Zone are from the same Controller, where possible. Although it is physically possible to use entities from different Controllers to build Doors or Alarm Zones, if there is a communications failure, access or intruder alarm monitoring can be compromised.

Procedure

Creating the Alarm Zone

1. Click **Configure** from the menu bar, then **Alarm Zones**.
   The **Alarm Zone** List Window opens (in grid view).
2. **Right click** and select **New...Alarm 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 **Apply** button, and the Alarm Zone is created.

   The rest of the procedure allows you to fully configure the Alarm Zone.

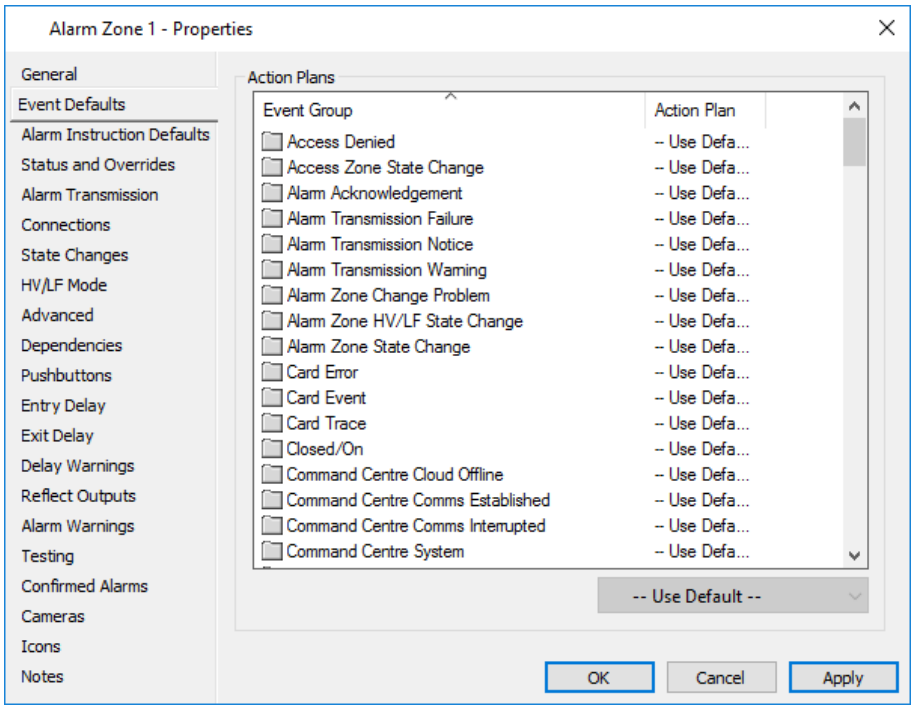
Configuring the Alarm Zone

5. Ensure the following information has already been set up:
   Divisions
   Refer to ***Setting up System Division*** (on page 9-3).
   Schedules
   (if you want Alarm Zone state changes to be controlled by Schedules)
   Refer to ***Schedules*** (on page 12-1).

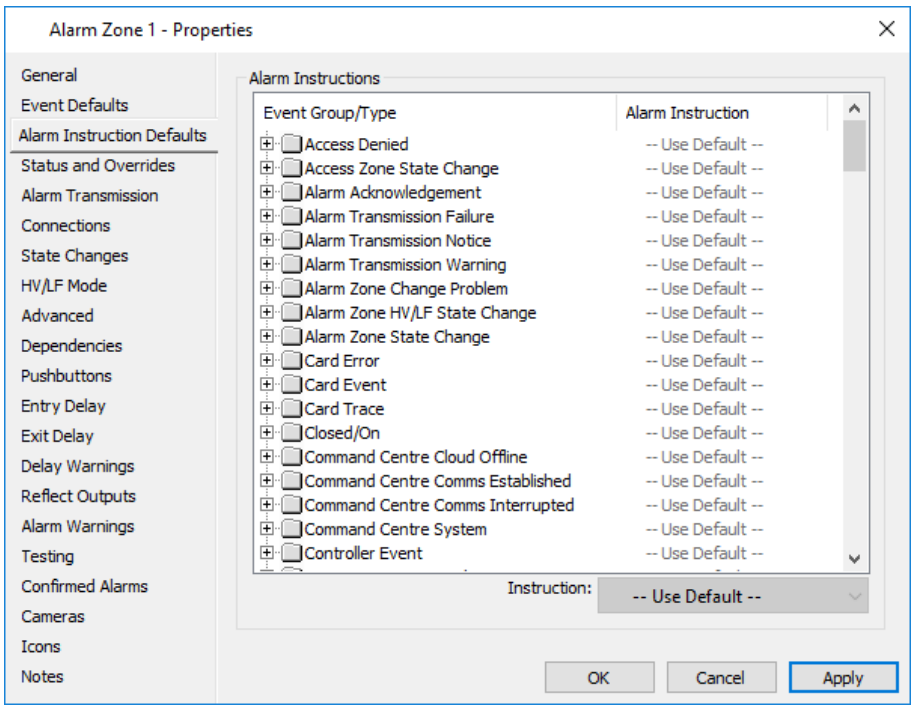
Action Plans
Refer to ***Creating a new Action Plan*** (on page 15-4).

Alarm Instructions
Refer to ***Creating a new Alarm Instruction*** (on page 16-2).

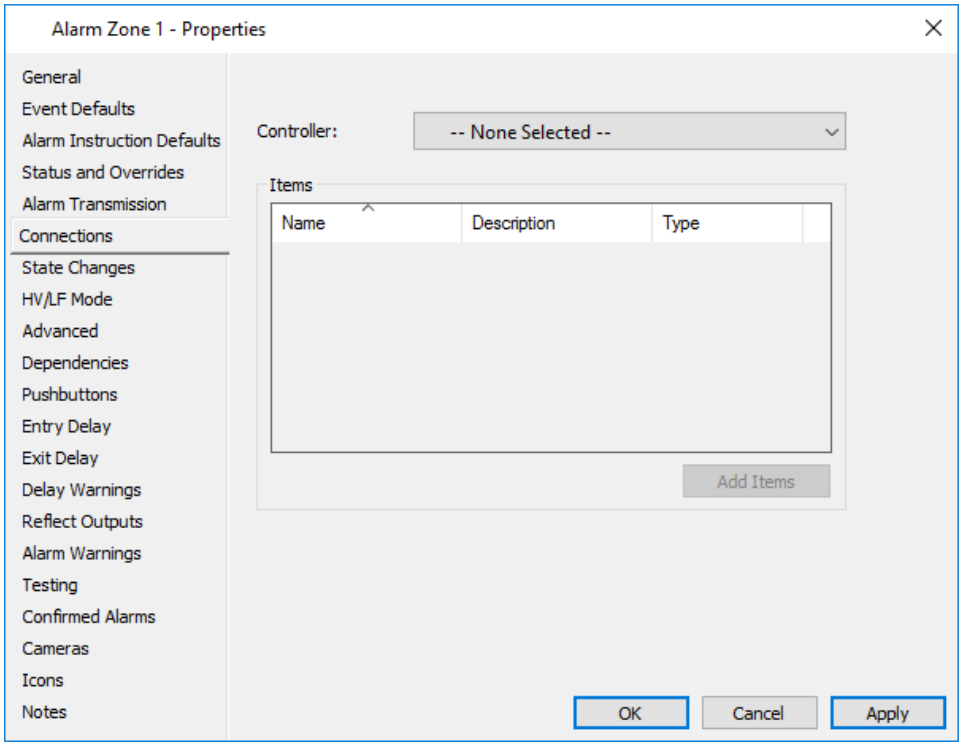
6. Select the appropriate Division from the drop-down list.
7. Click the **Event Defaults** tab.



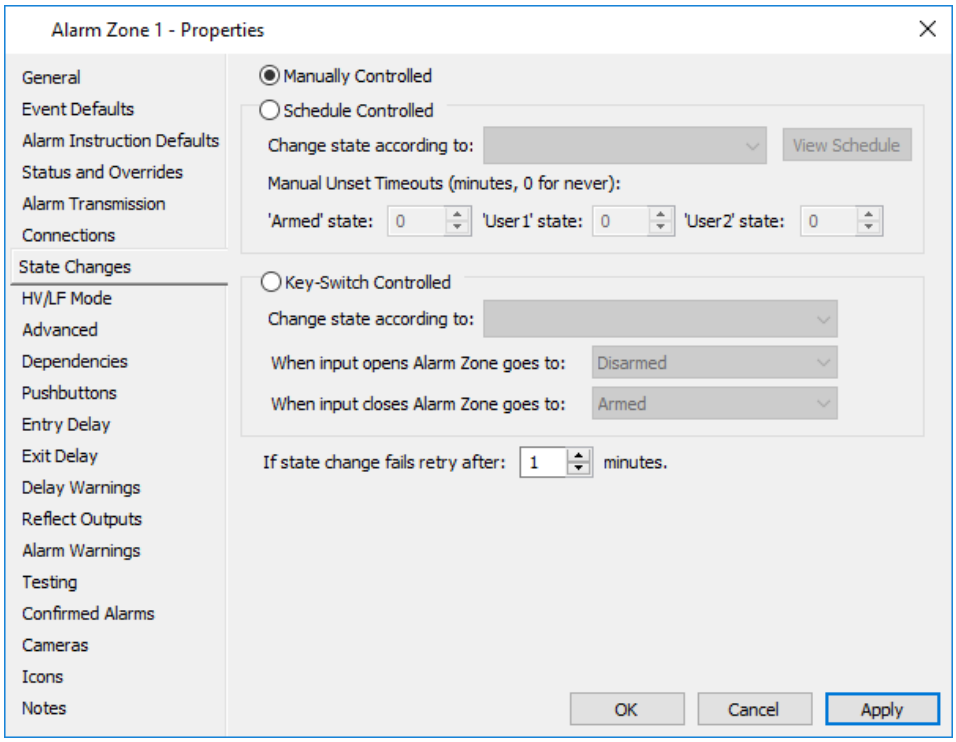
8. Assign the appropriate Action Plan to the desired Event type.
9. Click the **Alarm Instruction Defaults** tab.



10. Assign the appropriate Alarm Instruction to the desired Event type and group.
    Once the Alarm Zone has been created and configured, it is necessary to go to the associated hardware, (e.g. PIR's), and put them in the Alarm Zone.
    Note: For the Alarm Zone "State Change" to activate and the "Reflect Output" to initiate, (i.e. switch on), there **must** be either an input, output, door or Controller in the Alarm Zone.
11. Click the **Connections** tab.



12. Select the appropriate Controller from the drop-down list, (i.e. the Controller that has the majority of site items on this Alarm Zone).
    Note: A Controller must be selected in order for the state of the Alarm Zone to be set.
13. The Items grid shows a "Read-only" list of all Command Centre items that are connected to or contained in the Alarm Zone, (i.e. connected via their **Event Response** property page).
    If you want to add any items to the grid, refer to ***Adding multiple items to Alarm Zones*** (on page 14-18) for the procedure.
14. Click the **State Changes** tab.



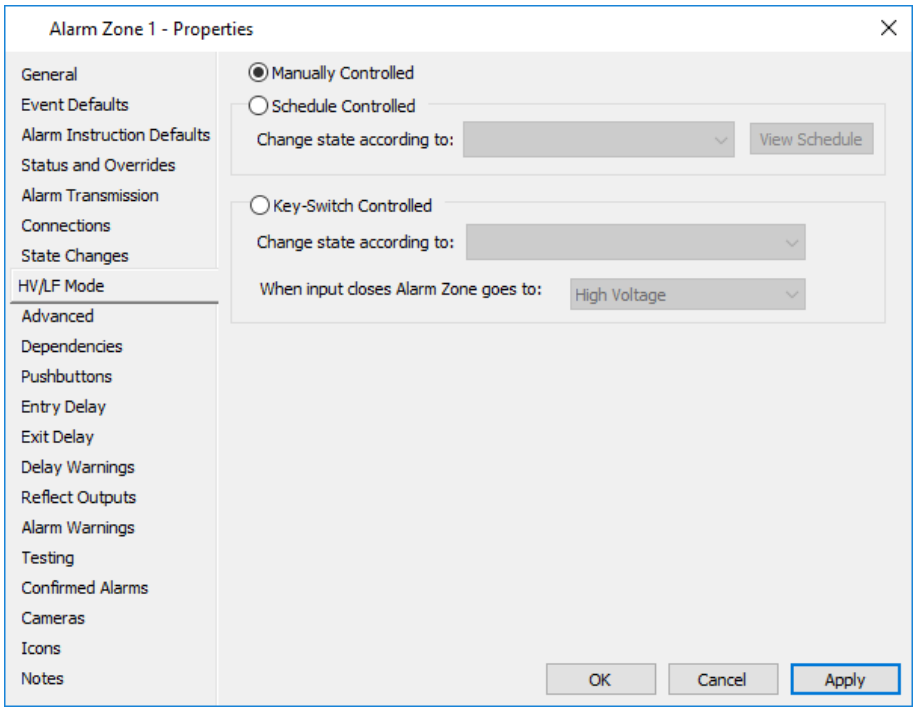
15. Click the appropriate radio button, i.e. (Manually Controlled, Schedule Controlled or Key-Switch Controlled), to indicate what controls the Alarm Zone state change.

Select...	if the Alarm Zone is to...
Manually Controlled	only have its state changed using either a terminal, any reader or a pushbutton attached to Command Centre. It will not be affected by Schedule changes.
Schedule Controlled	be set and unset automatically. To configure the times at which the Alarm Zone sets and unsets, assign the appropriate schedule from the **Change state according to** drop-down list. For the **Manual Unset Timeouts**, enter the expiry times (range is 0-1440 minutes, i.e. max 24hrs) for each of the states that the Alarm Zone can be manually overridden via a terminal, any reader or a pushbutton, before the Alarm Zone tries to go back into the Scheduled state. **Note:** The Alarm Zone state change can be configured so that the length of the expiry period depends on the time of day that the manual override takes place. For example, when a manual override (unset) occurs out of hours the override expiry might be 30 minutes, whereas if the unset takes place during office hours (between 9am-5pm), the expiry period is ignored. At the end of normal office hours the alarms are again set by the schedule.

Select...	if the Alarm Zone is to...
	When the override timeout tries to go to Scheduled state it will use the exit/entry delay as usual. If the manual override timeout is set to zero, this means it is disabled. **Note:** Schedules are configurable and can have alarms set for 24 hours or unset for 24 hours. If the Alarm Zone is to be set and unset by Cardholders who have the appropriate Cardholder privileges, then the default state of the Alarm Zone should be "Set 24 hours". This is assigned by selecting a schedule from the **Change state according to** drop-down list that has been configured with the Alarm Zone state "Set 24 hours". The Alarm Zone is then only unset by a Cardholder when badging their card at the entry reader for the zone. The Alarm Zone can then be set by a Cardholder performing a local override at a reader.
Key-Switch Controlled	be manually set and unset using keyswitches, (i.e. inputs).

Note: New alarm zones will remain permanently disarmed until one of these modes is selected to determine their state. If it is required for an alarm zone to be permanently disarmed, then an appropriately configured schedule should be provided.

16. In the **If state change fails retry after** box, enter the appropriate time. If the alarm zone state cannot be changed for any reason, the set attempt will be repeated at intervals equal to this time. (Range is 0-10 minutes, although a setting of 0 minutes will mean the Alarm Zone will never retry after state change failure.)
    Notes:
    - This figure should be increased if repeated alarm zone state change failed alarms occur with details of "Network failure".
    - If this Alarm Zone is dependant on other Alarm Zones, then this figure should be as low as possible, (e.g. If this figure is set to 1, and the Controller hosting this Alarm Zone resets, then this dependant Alarm Zone will attempt to set within 1 minute).
17. Will this Alarm Zone be assigned to a Fence Zone associated with an F31, F32, F41, F42 or F22 Fence Controller?
    If **yes**, go to Step 18.
    If **no**, go to Step 20.
18. Click the **HV/LF Mode** tab.
    Note: This tab will only be displayed if your site is licensed for Fence Controllers.

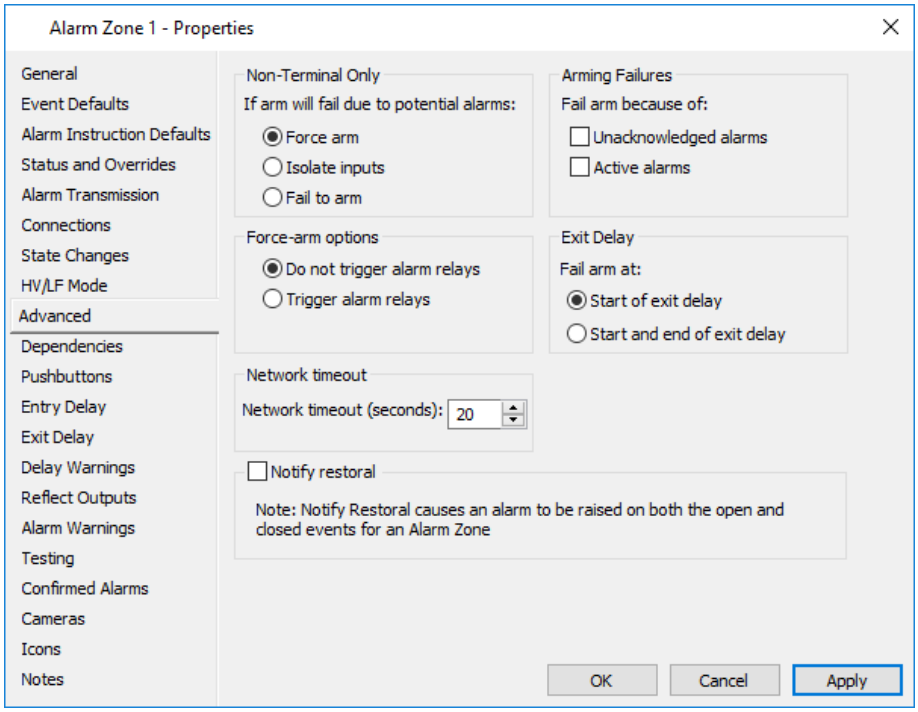


19. Click the appropriate radio button, (i.e. Manually Controlled, Schedule Controlled or Key-Switch Controlled), to indicate what controls the HV/LF mode change.

Select...	**if the Alarm Zone is to...**
Manually Controlled	change between High Voltage and Low Feel using only a terminal attached to Command Centre. It will not be affected by Schedule changes.
Schedule Controlled	change between High Voltage and Low Feel automatically. To configure the times at which the Alarm Zone changes between High Voltage and Low Feel, assign the appropriate HV/LF Schedule from the **Change state according to** drop-down list. **Note:** An HV/LF Schedule is configurable and can be set to High Voltage for 24 hours or Low Feel for 24 hours. if the Alarm Zone HV/LF mode is to be changed by Cardholders who have the appropriate privileges, then the default mode of the Alarm Zone should be "High Voltage" for 24 hours.
Key-Switch Controlled	be manually changed between High Voltage and Low Feel using keyswitches, (i.e. inputs).

Note: When a new Alarm Zone is created, the default HV/LF mode is High Voltage for 24 hours. If it is required for an Alarm Zone HV/LF mode to be Low Feel for 24 hours, then an appropriately configured schedule should be provided.

20. Click the **Advanced** tab.



21. Click the appropriate radio button for the required option.

If you click the...	this means that the...
Force arm radio button,	Alarm Zone will be forced to change state even if this would generate an alarm. **IMPORTANT:** The Alarm Zone will fail to change state if the Alarm Zone is spanned over multiple Controllers, and one or more of the Controllers goes offline.
Isolate inputs radio button,	Inputs will stop generating alarms until the next state change. The Inputs will however still be capable of triggering other activity. If an exit path is configured and a point on the exit path in alarm state, the isolation should occur at the end of the exit delay as this is when these points are Armed. If an exit path is configured and a point **not** on the exit path in alarm state, the isolation should occur at the **beginning** of the exit delay as this is when these points are Armed.
Fail to arm radio button,	Alarm Priority on the **Disarmed** tab of the corresponding Action Plan must be of a lower priority, (i.e. message only), for this function to work.

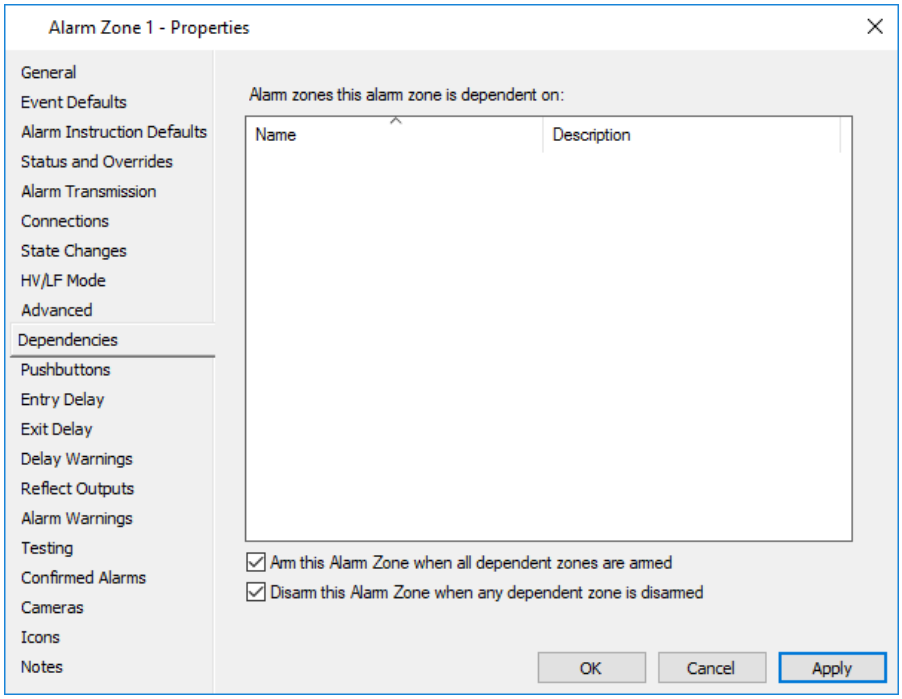
22. If you want to prevent the Alarm Zone from arming because of either **Unacknowledged alarms** and/or **Active alarms** in the zone, tick the checkbox(es) as appropriate.
23. Select the appropriate **Force-arm option**.
    Note: The **Force-arm options** control what will happen if a Force Arm is initiated at a terminal, and whether or not the relay is triggered, (i.e. the other alarm actions are still done regardless of which option is chosen). The **Force-arm options** allow for the situation where it is not desirable for a force-arm to trigger the relay, (e.g. when being force-armed from a terminal on site by a guard, the guard would not want the sirens to go off, but would want the monitoring station to know that the alarms had been armed).

If an...	then the...
exit path is configured and a point on the exit path in alarm state,	isolation should occur at the end of the exit delay as this is when these points are Armed.
exit path is configured and a point **not** on the exit path in alarm state,	isolation should occur at the **beginning** of the exit delay as this is when these points are Armed.
exit delay is configured and the Alarm Zone is force armed due to a point being in alarm state,	relays associated with the point in alarm will not be triggered.
exit delay is configured and a point goes into alarm state during the exit delay,	relays associated with the point in alarm **will** be triggered.

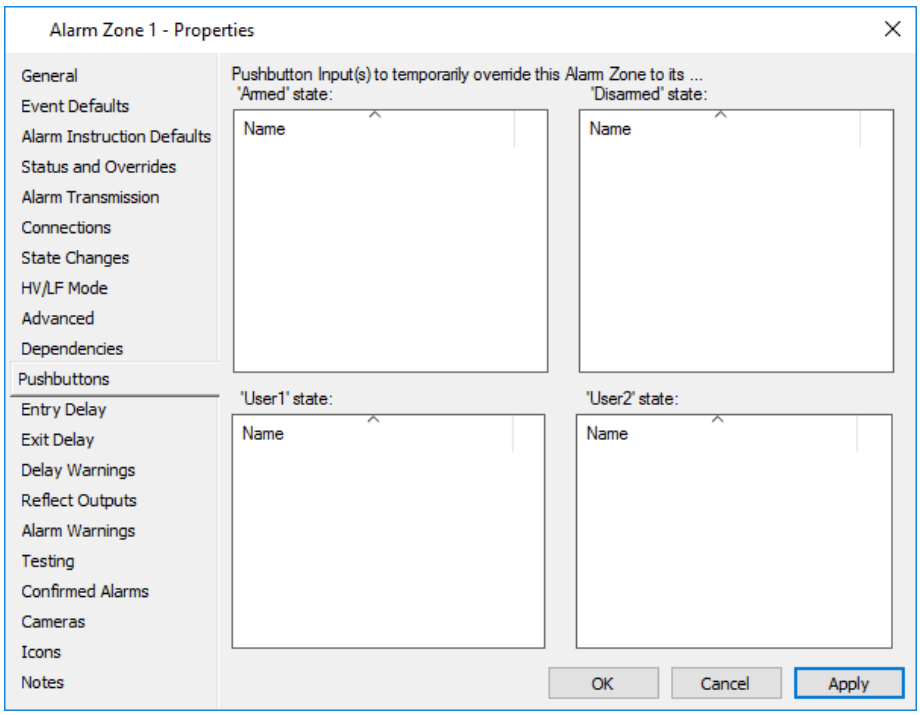
24. Click the appropriate **Exit Delay** radio button, so in the event of an alarm occurring that is either:
    - **not** on the exit path, and the alarm occurs during exit delay, or
    - **on** the exit path, and still in alarm at the end of exit delay, then

    at the end of the exit delay, depending on your configuration, Command Centre will check if the Alarm Zone is still able to arm.

    The **Start of exit delay** radio button is selected by default. However, if either the **EN50131 Compliance** or **SSF1014 Compliance** checkbox on the **Standards** tab of the Server Properties is checked, then the **Start and end of exit delay** radio button will be selected.
25. Indicate a **Network timeout** in seconds, and tick the **Notify restoral** checkbox if required.
    The Notify restoral behaviour applies to all points within an Alarm Zone which may enter an alarm state, (e.g. door open too long, forced door, etc.), and will cause an alarm to be raised on both the open and closed events for this Alarm Zone.
    Refer to ***Notify Restoral*** for further explanation.
26. Click the **Dependencies** tab.



27. Drag and drop the Alarm Zones (a maximum of 20), that this Alarm Zone is to be dependent on.
28. The two checkboxes allow you to configure whether this Alarm Zone will automatically arm when all dependent zones are armed, automatically disarm when any dependent zone is disarmed, neither, or both.
    Tick or untick the option(s) as required.
29. Click the **Pushbuttons** tab.

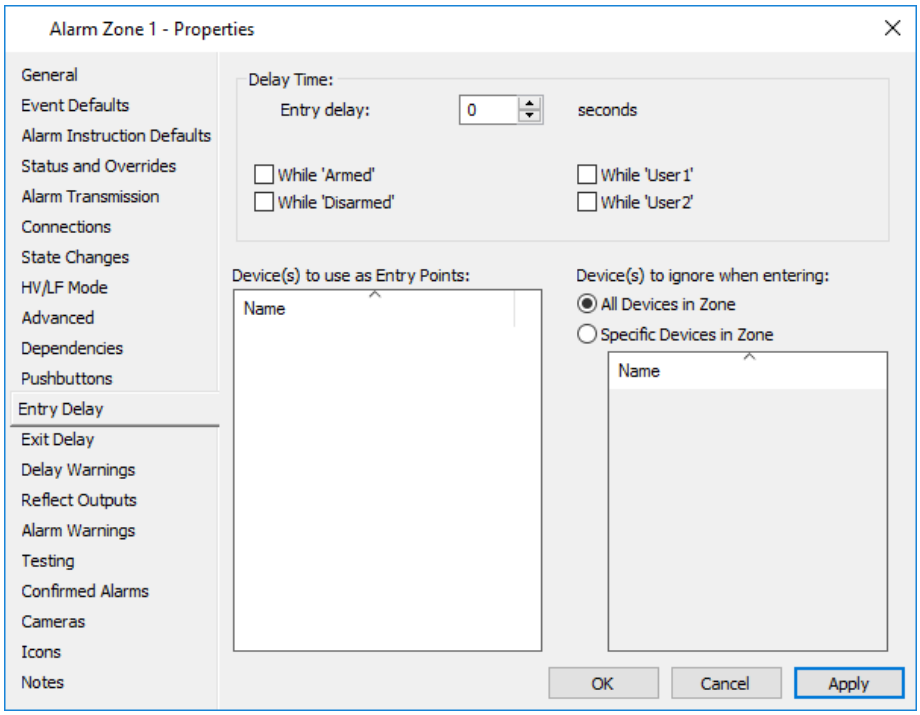


30. Drag and drop an Input to use as a pushbutton to override the Alarm Zone to its "Armed" or "Disarmed" state for Pushbutton exits.

Inputs should normally be wired open as the zone will change state on the transition between open and closed. If this does not suit, the input can be inverted and the alarm will change state as it goes closed to open.

Note: State changes made by Inputs on this property page will be overridden by scheduled state changes.

31. Click the **Entry Delay** tab.



If you unset an Alarm Zone using a Reader or Pushbutton, and that Reader or Pushbutton is physically located inside the Alarm Zone, you need to set a **Delay Time** for "While Armed" and add a device as the Entry Point by dragging it into the **Device(s) to use as Entry Points** box. (An Entry Point can be an Input or a Fence Zone that triggers an entry delay by opening. It does not have to be in the same zone as the zone that has the entry delay.)
By default the **Entry Delay Time** is 0 seconds and all state checkboxes are unchecked.
Note: You cannot specify an entry delay time without checking at least one state checkbox. Likewise, if you check any of the state checkboxes you must specify an entry delay time.

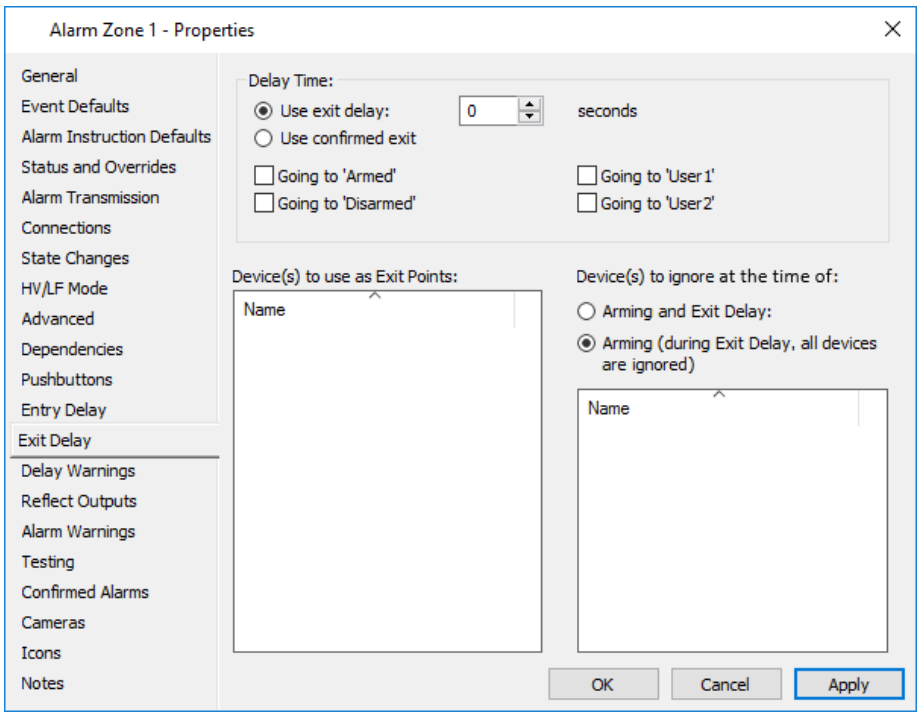
Remember: If you require instant alarms after the entry timer has started you need to create dependent Alarm Zones, (i.e. an Entry Path). This can be achieved on the **Dependencies** tab.

32. If unsetting is completed from within the Alarm Zone, a route from the entry point to the means of unsetting needs to be defined under **Device(s) to ignore when entering**. This can be achieved by either:

    - clicking the **All Devices in Zone** radio button (which is the default), OR
    - clicking the **Specific Devices in Zone** radio button and dragging the required entry route inputs (and the entry point input) into the grid.

During entry delay, input activations from the entry route will be ignored while all other zone input activations will cause immediate alarms according to their Action Plan setup.

33. Click the **Exit Delay** tab.



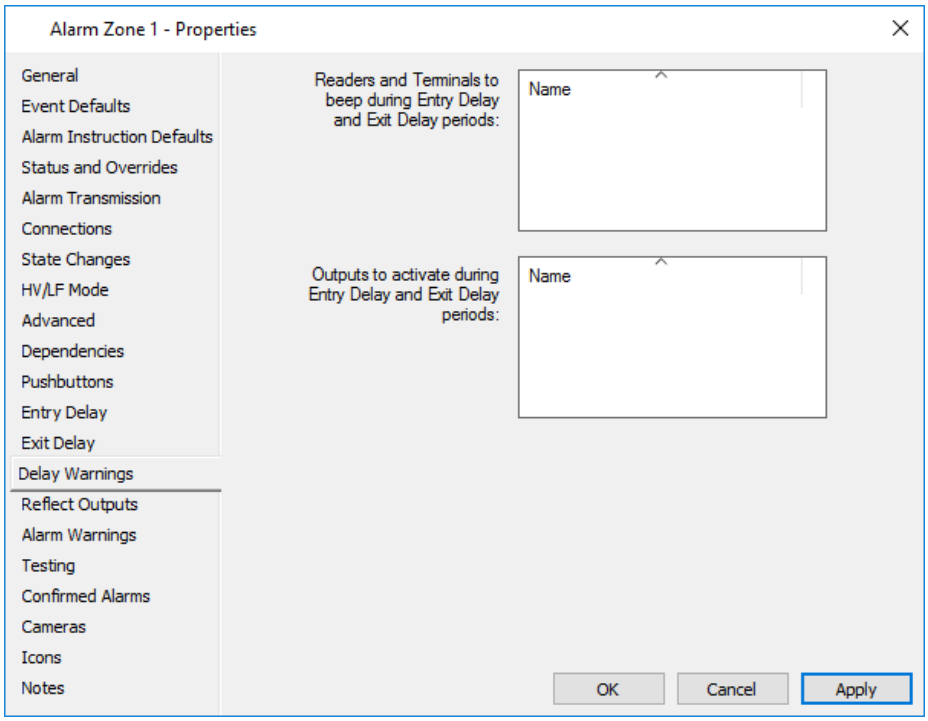
34. If you set the Alarm Zone using either a Reader or a Pushbutton that is located inside the Alarm Zone, you need to configure **Delay Times** to provide enough time to exit the zone before the Inputs activate an alarm. Ensure the **Use exit delay** radio button is selected, and enter an appropriate delay time.
    By default the **Delay Time** is 0 seconds and all state checkboxes are unchecked.

    Note: You cannot specify an exit delay time without checking at least one state checkbox. Likewise, if you check any of the state checkboxes you must specify an exit delay time.

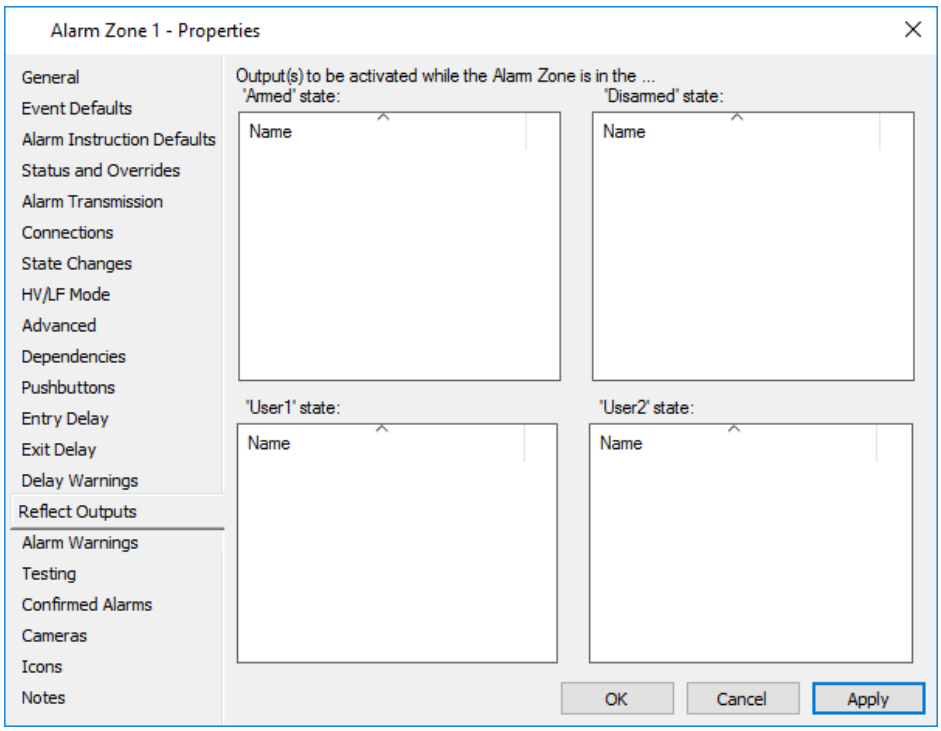
35. If you do **not** want the exit delay to timeout, select the **Use confirmed exit** radio button. This will cause the Alarm Zone to have an exit delay that does not timeout, but only completes when one of the exit points activates.

    Important: With the **Use confirmed exit** mode selected, the zone will never set if one of the exit points does note activate. For this reason, this mode should never be used for zones that have an arming schedule defined, as there is no guarantee that someone else will be present at the time of auto-arming (to terminate the exit delay), and therefore the zone may not set.

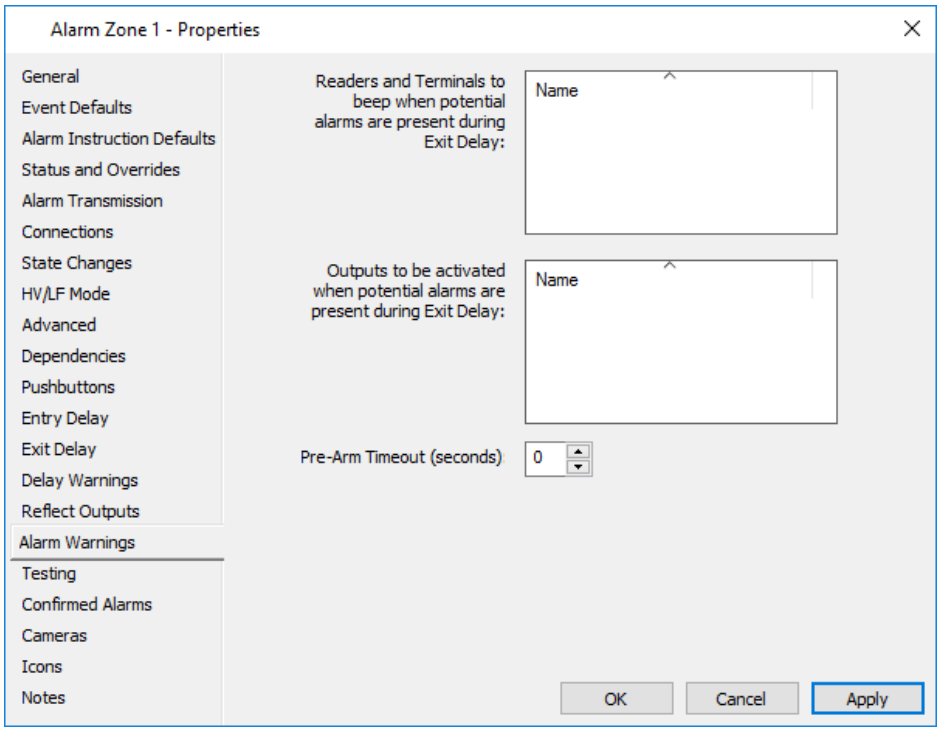
36. Drag any Inputs, (e.g. Door Sensor), into the **Device(s) to use as Exit Points** box to end the Exit Delay period. This removes the need for people to wait longer than is needed to verify the Alarm Zone is set. The Exit Delay will cancel and the zone will arm when the exit point closes.
    Note: Inputs that have already been used as Entry Points on the **Entry Delay** tab can also be used as Exit Points on this tab. Because entry delays are triggered by 'Input Open' events and exit delays are ended by 'Input Closed' events, these cases can be distinguished.
    If an Input is used for both entry and exit delay, the Input and the Alarm Zone must co-exist on the same Controller.
37. Under **Device(s) to ignore at the time of**, configure a list of devices which will be ignored either when a request is made to arm the Alarm Zone or during the arming and while exiting from the Zone.
    If you select the **Arming and Exit Delay** option the Exit Path will be made up of any devices in the 'Ignored devices' grid plus any devices in the 'Exit Points' grid.
    If you select the **Arming (during Exit Delay, all devices are ignored)** option (which is the default), all devices in the Alarm Zone will be ignored during Exit Delay regardless of what has been put into the 'Ignored devices' grid.
    Notes:
    - Exit path configuration is supported by Controller 6000s and 7000s.
    - It is recommended you do this if your site has PIRs facing terminals, or card readers used to set alarms.
    - If you do not have the "Isolate" privilege, the arming will fail.
38. Click the **Delay Warnings** tab.



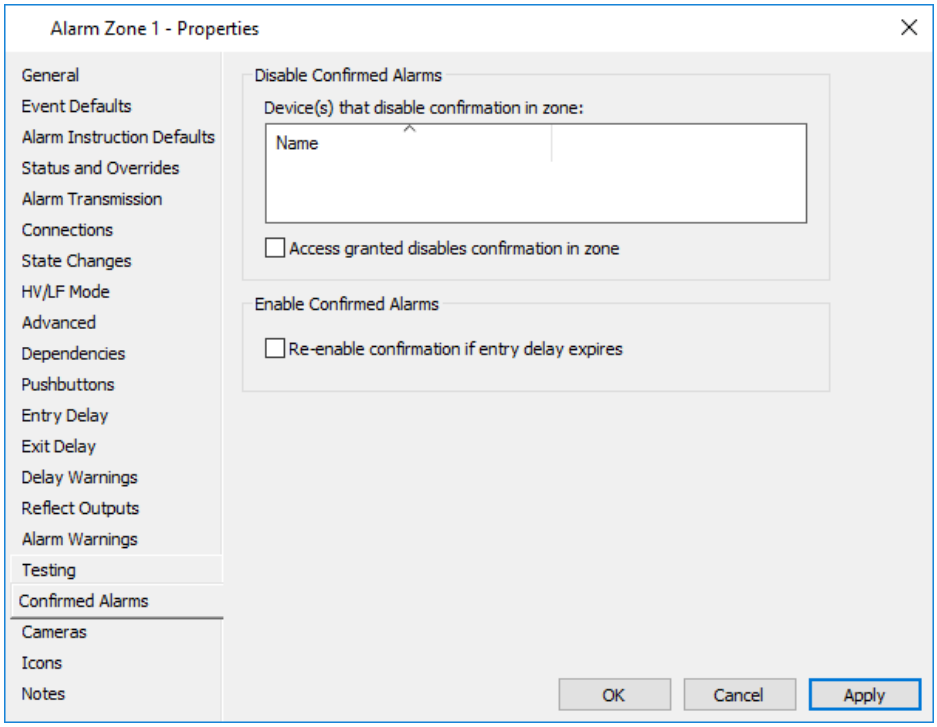
39. Configure **Readers, Terminals** and **Outputs** as required (drag and drop). These items will now provide an audible indication of an entry/exit delay event.
40. Click the **Reflect Outputs** tab.



41. Configure **Outputs** as required (drag and drop).
    Outputs turn on while in the Alarm Zone state the outputs are placed in.
42. Click the **Alarm Warnings** tab.



43. Configure **Readers, Terminals** and **Outputs** as required (drag and drop). These items will now be activated during exit delay when potential alarms are present.
44. In the **Pre-arm Timeout** box, enter an appropriate period that you want Controllers to ignore alarms for, (i.e. 0-60 seconds).
    Note: A pre-arm timeout will need to be configured if the Alarm Zone is being used to control the state of Fence Zones. The pre-arm timeout will allow enough time for the Fence Zones to turn on and measure their output voltage before any alarms are raised. A value of approximately 5 seconds is suggested.
45. Click the **Confirmed Alarms** tab.



46. If you want to disable confirmed alarms, drag any devices, (e.g. Door Sensor), into the **Device(s) that disable confirmation in zone** box. This disabling of confirmed alarms shall apply until the zone is disarmed (or changed to some other state) and then re-armed. If entry delay expires, the zone status will show as "Zone is armed. Alarms are INHIBITED." If 'Re-enable confirmation if entry delay expires' is **not** enabled, or "Zone is armed. Entry delay expired.".
47. If you want granting access to disable the sending of confirmed alarms, check the **Access granted disables confirmation in zone** checkbox.
48. Check the **Re-enable confirmation if entry delay expires** checkbox if required. When checked, instead of confirmed alarms being inhibited, confirmed alarms will still occur after entry delay has expired.

    Note: Items on this page will only affect the system if "Enable Confirmed Alarms" is selected on the **Standards** page of the Server Properties. See Standards for further detail.

49. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Alarm Zone.
    For further details see ***Cameras tab*** (on page 3-24).
50. Click the **Icons** tab if you want to change the Icon Set for this Alarm Zone.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
51. Click the **Notes** tab if you want to add a note(s) about this Alarm Zone.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
52. 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.

    Initialising Alarm Zone functionality

    Once the Alarm Zone configuration work is complete, you need to associate the inputs, (e.g. PIRs, reed switches, etc.) with the Alarm Zone so they recognise any Alarm Zone state changes.

    Note: The Inputs need an appropriate Action Plan assigned to them. Refer to ***Creating a new Action Plan*** (on page 15-4) for details.
53. Click **Configure** from the menu bar, then **Hardware**.
54. Select the appropriate input.
55. **Right click** and select **Properties**.
56. Click the **Event Response** tab, and select the Alarm Zone that the input should be associated with.

    The Access Zone(s) that the inputs are in, (i.e. physical areas that they are located), must also be associated with the Alarm Zone. The Access Zone must recognise the set and unset state of the Alarm Zone to prevent accidental cardholder entry into an Access Zone with set alarms.
57. Click **Configure** from the menu bar, then **Access Zones**.
58. Select the Access Zone the inputs are in.
59. **Right click** and select **Properties**.
60. Click the **Event Response** tab, and select the Alarm Zone that the input should be associated with.

Result

A new Alarm Zone is configured and will operate under the command of the Alarm Zone configuration as established.

Hint

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

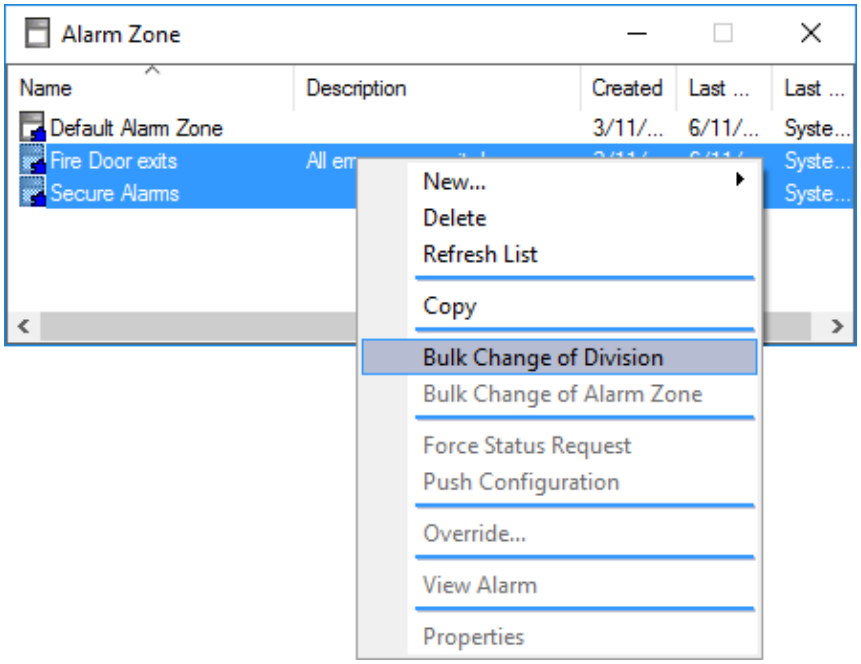
Adding multiple items to Alarm Zones

Introduction

This procedure allows an operator with the "Bulk Change" privilege to add multiple Command Centre items to an Alarm Zone.

There are three methods of performing this procedure. You can either use:

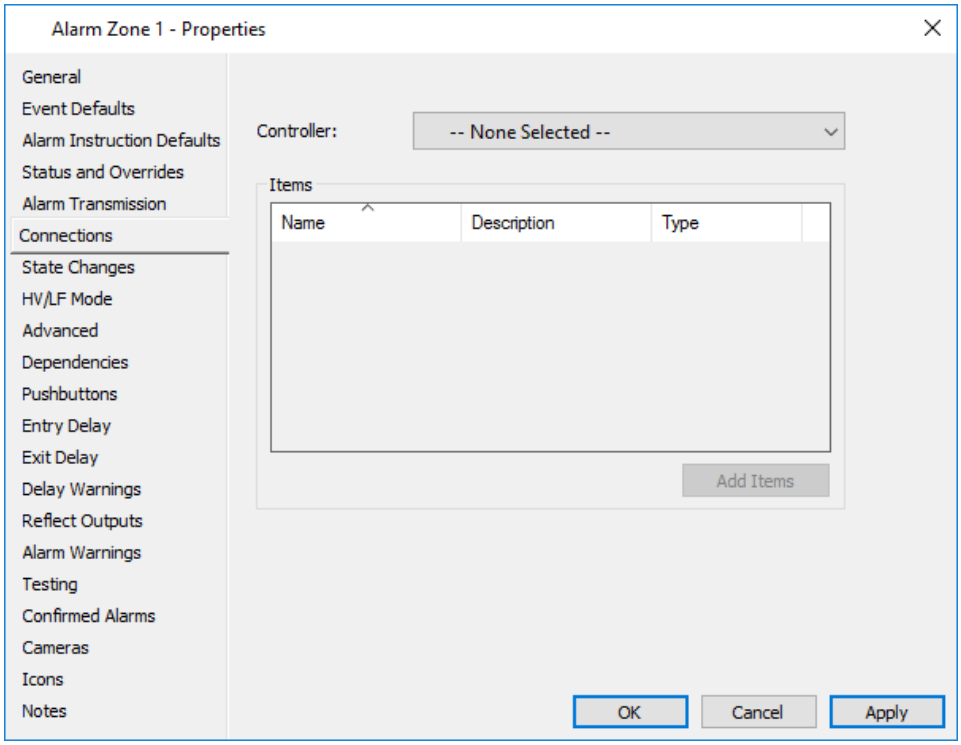
- the **Add Items** button on the **Connections** tab of the Alarm Zone properties, or
- the General Change Wizard, or
  Note: For this method refer to Initiating a new Alarm Zone Bulk Change for the procedure.
- the context menu option available from an items List Window or from the Find Tool search results.
  Using this method, you select the items that are to be added to an Alarm Zone, **right click** and select **Bulk Change of Alarm Zone** from the context menu.
  The "Change Alarm Zone" screen of the Bulk Change of Alarm Zone Wizard displays.
  Select the new Alarm Zone to be assigned to the items from the drop-down list, and go to Step 6 in the following procedure to complete a bulk change of alarm zone using this method.



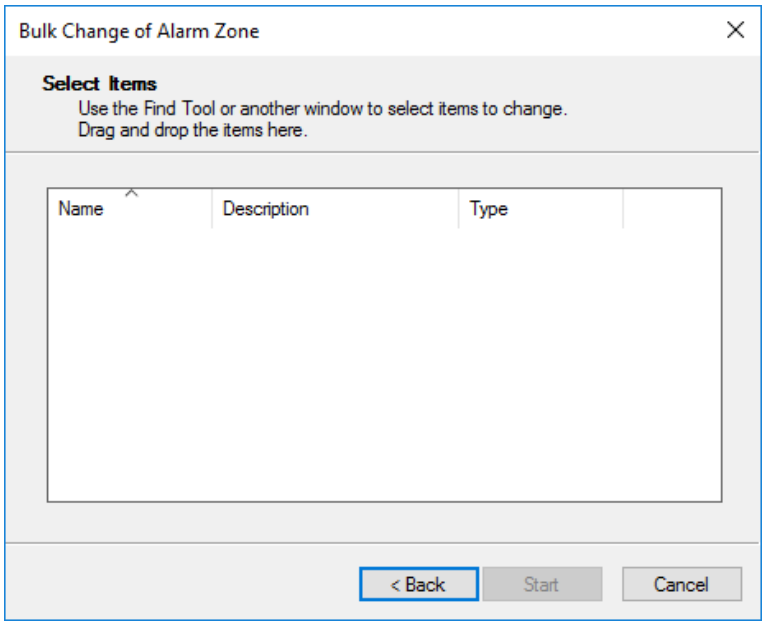
Procedure (using the 'Add Items' button)

1. Click **Configure** from the menu bar, then **Alarm Zones**.
   The **Alarm Zone** List Window opens (in grid view).

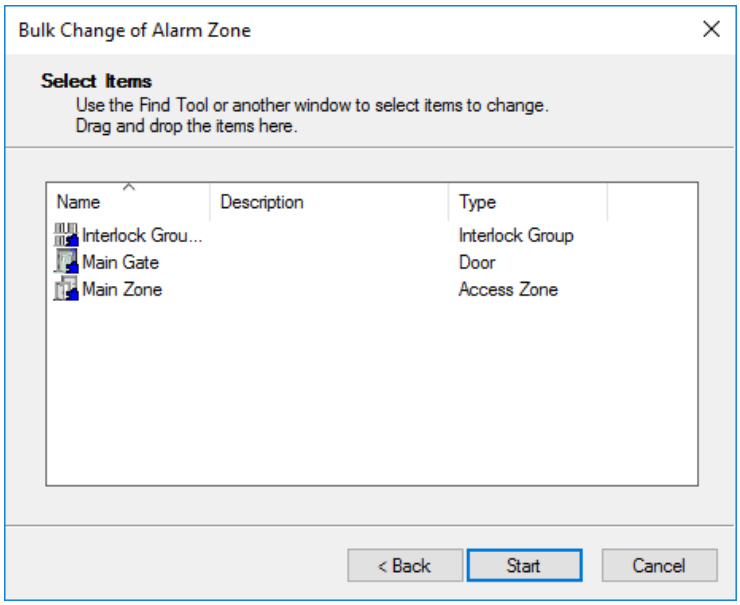
2. **Right click** on the required Alarm Zone, and select **Properties**.
3. Click the **Connections** tab.



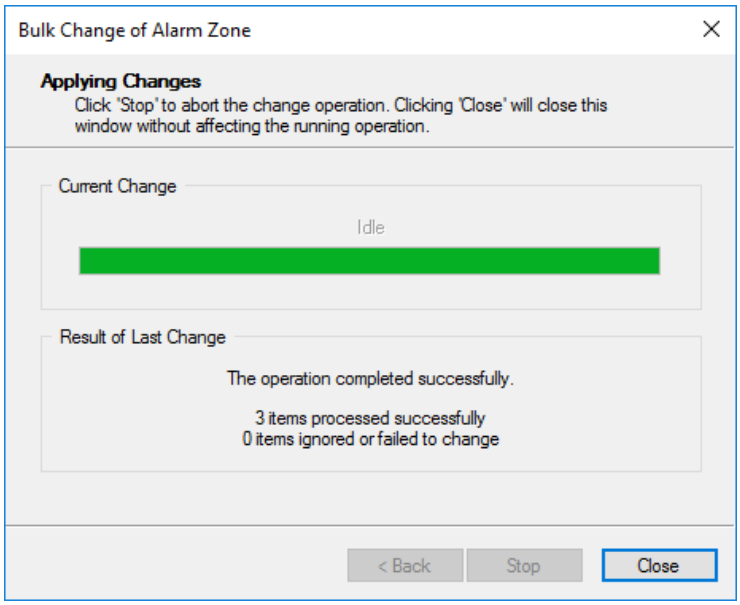
4. Click the **Add Items** button.
   Note: The **Add Items** button will only be enabled if you have the "Bulk Change" operator privilege.
   The "Select Items" screen of the Bulk Change of Alarm Zone Wizard displays.



5. Place all the items to be added to the Alarm Zone onto this screen, by dragging and dropping them from the appropriate List Window, or by using the Find Tool.



6. Click the **Start** button.
   The "Applying Changes" screen of the Bulk Change of Alarm Zone Wizard displays.



   This screen shows the progress of the bulk change. While this screen displays, the bulk change will appear in the **Bulk Changes** List Window with a system-generated name. While in progress, the status of this bulk change will show as 'Active' in the **Bulk Changes** List Window, and if it completes successfully it will show as 'Successful', at which time the system will delete it.
   Note: While a Bulk Change of Alarm Zone is active, or if it fails, it will remain in the **Bulk Changes** List Window until an operator deletes it.

Result

A Bulk Change of an Alarm Zone has been initiated, and the selected items have been added to the Alarm Zone.

Chapter 15: Action Plans

What is an Action Plan?

An Action Plan defines what is going to happen when an event in your security system occurs. When an event occurs the Action Plan defines the following:

- Assigns an alarm priority (e.g. message only, high priority, etc.)
- Operates the appropriate outputs, Digital Cameras and/or macros
- Escalation time

Types of Action Plans

There are three different types of events in Command Centre, (i.e. Command Centre events, Controller events and Commander events), for which the alarm behaviour can be configured via Action Plans. To configure an Action Plan for a specific type of event, use only the relevant property pages (tabs), as follows:

Event Type	Action Plan tabs to configure	Description
Command Centre	**Command Centre** tab	Command Centre events can be created by any part of Command Centre, (e.g. workstation, central server, communications server, etc.). Command Centre is responsible for executing Action Plans for all Command Centre events. The only Action Plan behaviour supported for Command Centre events is configurable alarm priorities and automatically triggered macros. In addition, the Action Plan's 'Command Centre' configuration is always used, regardless of the state of the Alarm Zone.
Controller	**Armed** (or **Set**) tab **Disarmed** (or **Unset**) tab **User 1** tab **User 2** tab **Escalation** tab	The Controller is responsible for executing Action Plans for Controller events. If the Action Plan cannot be fully handled by the Controller, (e.g. if it is configured to generate a report), then the Controller sends a message to the Command Centre to trigger the 'Command Centre' part of the Action Plan.

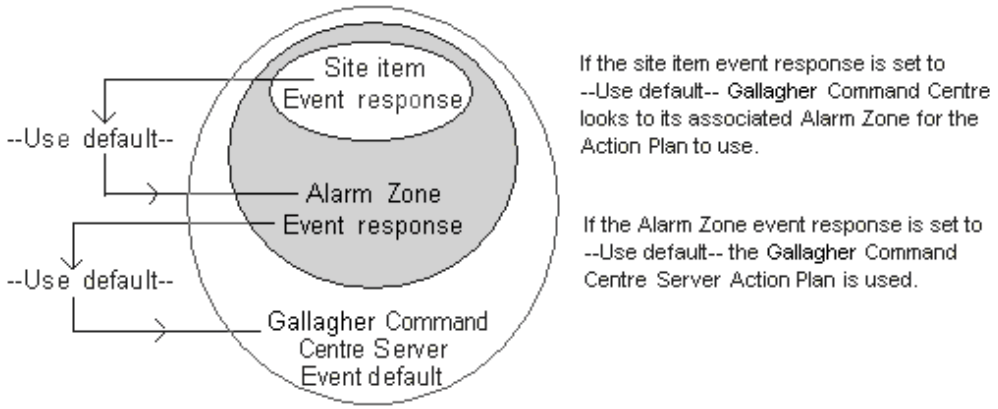
Notes:

- The **General** tab should also be configured for all event types, and the **Notes** tab if required.
- To find out what generates an event, (i.e. Command Centre, Controller or Commander), refer to the "Event/Alarm Messages" online help file via the **Help** menu bar in Command Centre.

Which Action Plan to follow?

Every possible event that can occur within the system can be linked with an Action Plan. You link the Action Plan within the Event Response tab:

- Some events may require no action.
  For example: when an employee opens a window during working hours, no event is recorded. This event type is linked to the Action Plan "No event recorded".
- Specific events may require a specific Action Plan.
  An Action Plan is assigned to the event at the site item level.
  For example: Security lighting switches on and a message is generated when staff exit from the staff entrance.
- Events can be set to respond to default Action Plans.
  The following diagram shows the hierarchy Command Centre follows when determining which Action Plan takes priority.



Escalation

If, after a preset time, the guard has not acknowledged the alarm, the alarm will automatically be escalated in priority.
Note: When an Alarm Zone changes state, (e.g. from *Disarmed* to *Armed*), where *Armed* uses escalation rules, the alarm will not always escalate. There are two situations where the behaviour is different, but in both cases escalation does not take place. They are:

- Where the Action Plan is set up for *Disarmed* as 'Message Only', going to *Armed* which is 'Low Priority', escalating to 'High Priority' if the input is still active after 10 seconds.
- Where the Action Plan is set up for *Disarmed* as 'Low Priority', going to *Armed* which is 'Medium Priority', escalating to 'High Priority' if the input is still active after 10 seconds.

Escalated alarms can be shown in a separate viewer from the main Alarm Viewer. For further details regarding the "Escalated Alarm Viewer" see Alarm Viewers.

Link with Alarm Zones

The Action Plan to follow may differ depending on the state of the Alarm Zone the item is grouped with.

For example:

- During working hours, when the Alarm Zone is Unset/Disarmed, only a message is necessary.
- After hours when the Alarm Zone is Set/Armed, a high priority alarm is generated.

Creating a new Action Plan

Introduction

When creating a new Action Plan you perform the following steps:

- Within the **Action Plan** List Window, create a new Action Plan.
- Define the 'course of action' for each of the Alarm Zone States, (i.e. specify relays to be deactivated when an alarm is not active, and set the Escalation details).

Operators require the "Edit Alarm Configuration" operator privilege to perform this procedure, and must be in the same or parent Division of the Action Plan.

Notes:

- If the Action Plan is to operate an Output, camera and/or macro, ensure these items are already configured.
- The alarm behaviour can be configured specifically for the types of events in Command Centre, (i.e. Command Centre events and Controller events), therefore you need only configure the property pages relevant for a particular event type, as indicated in Step 5.

Procedure

Opening the Action Plan window

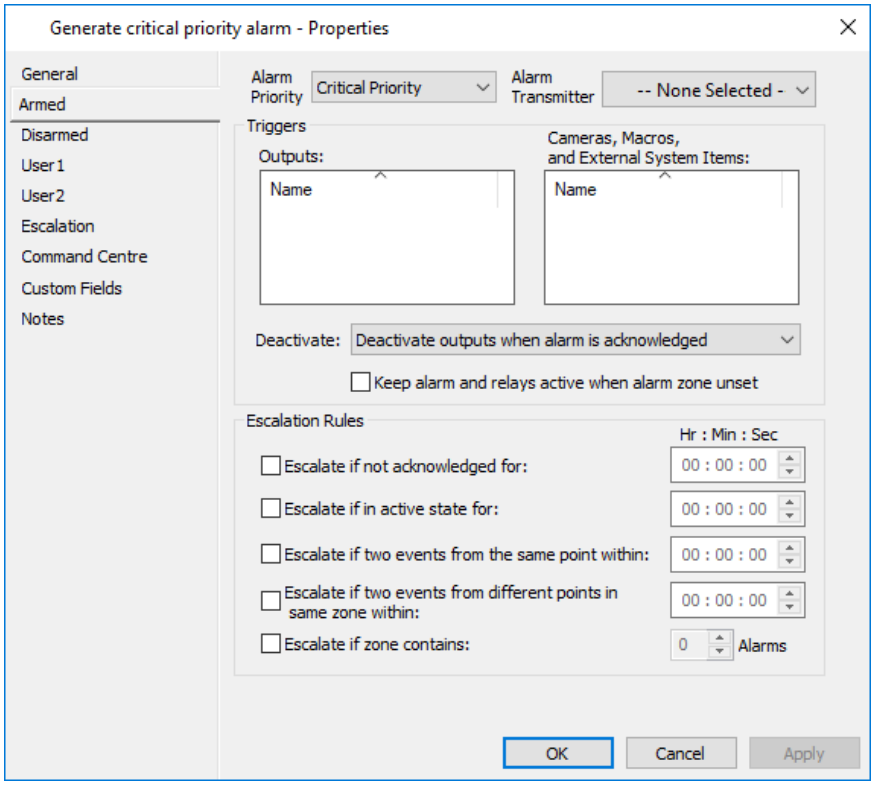
1. Click **Configure** from the menu bar, then **Action Plans**.
   The **Action Plan** List Window opens (in grid view).
2. **Right click** and select **New...Action Plan**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
   Note: The next four tabs will reflect the Alarm Zone States in use in your Command Centre system, (i.e. as configured on the **Alarm Zone States** tab of the Server Properties).
   Each of these tabs will be named according to the user-configurable names of the four Alarm Zone States. For example, the **Armed** and **Disarmed** tabs will display as **Set** and **Unset** if you changed these in the Alarm Zone States tab of the Server Properties. Refer to Alarm Zone States for further detail.
4. What type of Action Plan are you creating, (i.e. for what type of event)?

If...	then go to...
Controller	Step 5
Command Centre	Step 21

Defining the Action Plan

The response to the event may differ depending on the state of the Alarm Zone the item is grouped with.

5. Click the **Armed** (or **Set**) tab.
   These settings define the responses when the item's Alarm Zone is armed.



6. Specify the priority of events or alarms generated, from the **Alarm Priority** drop-down list.
   When an event occurs and it has this associated Alarm Zone state, the response will be of this priority.
   Note: The drop-down list will be populated with alarm priority names configured for the overall Command Centre system.

7. The Alarm Dialler field relates to Contact ID. If required, click within the Alarm Dialler field to display the available options, and from the list select the appropriate **Alarm Dialler** for Contact ID.
   See ***External Alarm Monitoring*** (on page 29-1) for an explanation of what Contact ID is, and for instructions on configuring Contact ID.

8. Drag and drop the outputs that are required to activate into the **Output** grid.
   Note: If the Alarm Priority is set to "Not an Event" or "Message Only", the output(s) will not be activated.

9. Drag and drop the DVR Cameras (Gallagher or third-party), Macros and/or External System Items to be triggered into the **Cameras, Macros, and External System Items** grid.
   Note: When the Action Plan is executed:

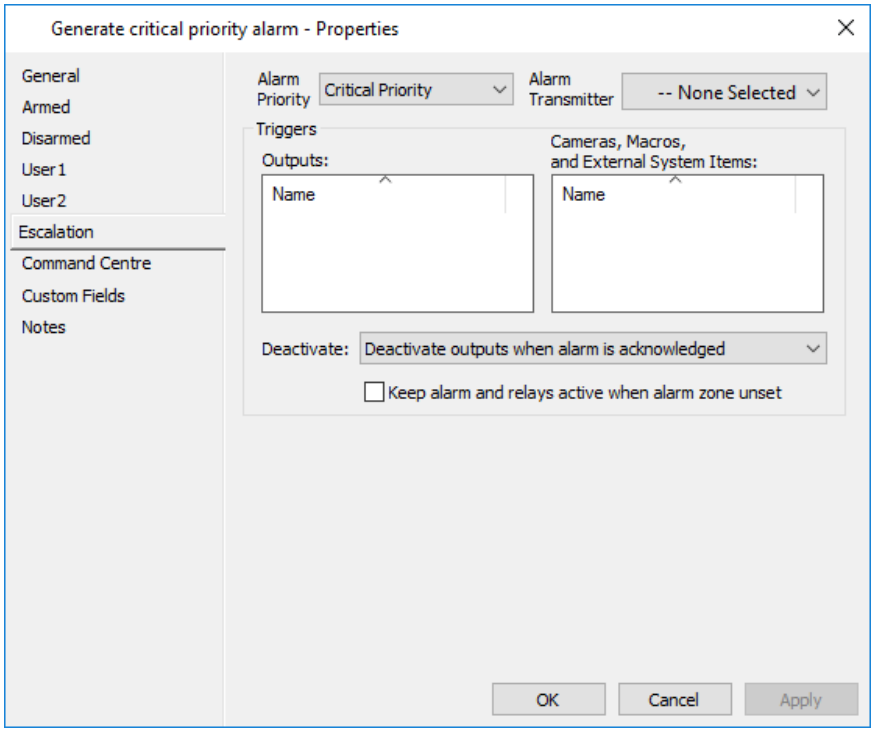
- The footage recorded by the cameras in this grid at the time of the event/alarm is associated with the event/alarm. As a result, when viewing an event/alarm in Command Centre client, a camera tile can show footage taken by these cameras at the time which the alarm occurred.
- The string(s) on the **Trigger -- Events** tab of the cameras and External System Items in this grid are sent to those devices' third-party systems.
- Note that when Macros in this grid are run, they will not run a bulk change if triggered from an Action Plan.

10. Macros that run a bulk change will not occur from an Action Plan.
11. Select the appropriate option from the **Deactivate** drop-down list. There are three options available, and your selection will determine when outputs (that are activated when an alarm occurs), are deactivated. The options are:
    - when an alarm is acknowledged,
    - when an alarm is acknowledged **or** becomes inactive,
    - when an alarm is acknowledged **and** becomes inactive.
12. By checking the **Keep alarm and relays active when alarm zone unset** checkbox this will ensure that outputs (defined on this Action Plan tab) that are active when the Alarm Zone changes state, will remain active after the state change (provided the alarm has not been acknowledged).
13. Tick the appropriate checkbox for the 'course of action' for an escalated event or alarm. **Escalation Rules** are as follows:

Rule	Description
Escalate if not acknowledged for:	The alarm will escalate if it is not acknowledged within the specified time.
Escalate if in active state for:	The event or alarm will escalate if it remains active for the specified time.
Escalate if two events from the same point within:	The event or alarm will escalate immediately if an event from the same point and event group occurred within the previous time specified.
Escalate if two events from different points in same zone within:	The event or alarm will escalate immediately if an event from another point in the point's alarm zone with the same event group occurred within the previous time specified. **Warning:** Any points generating events in the same group can contribute to this rule, including outputs. To avoid unintentional escalation, outputs should not be assigned an alarm zone or be assigned an alarm zone where this escalation rule is not used.
Escalate if zone contains:	The event or alarm will escalate immediately if the alarm stack already contains the specified number of unacknowledged alarms from points in the Alarm Zone.

Note: Escalation will only work if the Inputs in an Alarm Zone are on the same Controller, and the Alarm Zone is not spanned.

14. Click **Apply** to save your changes.
15. Click the **Disarmed** (or **Unset)** tab, and repeat Steps 6-13.
    These settings define the responses when the item's Alarm Zone is disarmed.
16. Repeat Steps 6-13 for the next two tabs also, (i.e. **User 1** and **User 2** tabs, unless these have been renamed in the Server Properties).
17. Click the **Escalation** tab.
    These settings define the 'course of action' for an escalated event or alarm. The only difference between this tab and the other Alarm Zone State tabs is that the escalation options are not available as the event or alarm has already been escalated.

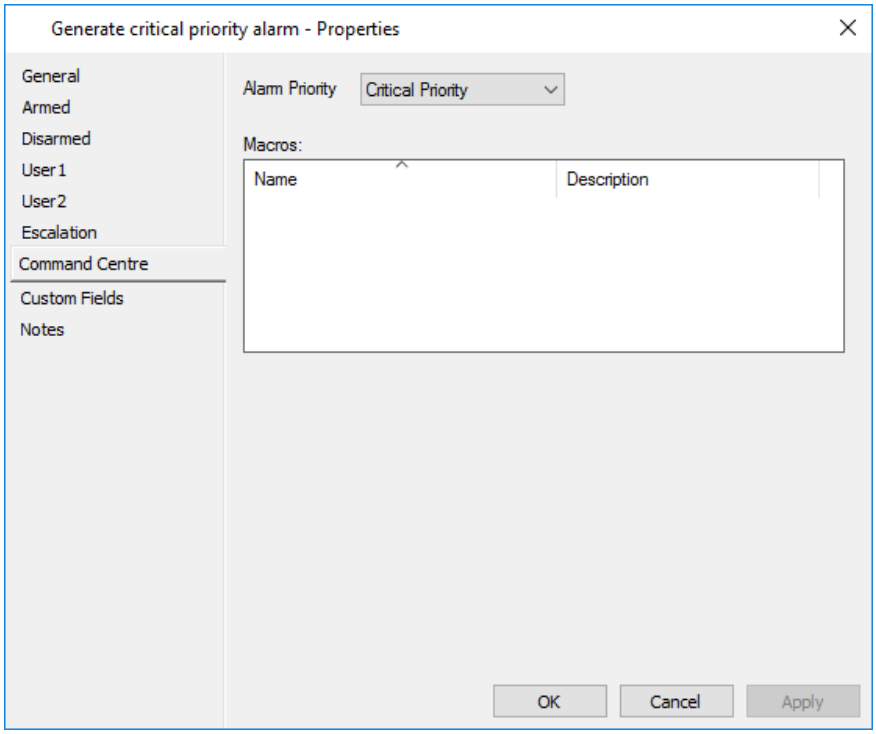


18. Select the appropriate Escalation **Alarm Priority**.
    Escalation will occur if this setting has a higher priority than the "Alarm Priority" setting within the Alarm Zone tabs.
    Note: All events and alarms that escalate to the escalated priority will:
    - also appear in the **Escalated Alarm Viewer**, and
    - display as "Escalated" in the Alarm Details.
19. The Alarm Dialler field relates to Contact ID. If required, click within the Alarm Dialler field to display the available options and from the list select the appropriate **Alarm Dialler** for Contact ID.
    See ***External Alarm Monitoring*** (on page 29-1) for an explanation of what Contact ID is, and for instructions on configuring Contact ID.

    Note: Alarms will be sent as many times as an Alarm Dialler appears on an Action Plan for the various priorities involved in an escalation.

For example:
If a "Forced Door" alarm uses a very high priority Action Plan with an Alarm Dialler attached, it will escalate to a critical priority that also has the Alarm Dialler attached. The "Forced Door" alarm Contact ID message will then be sent twice, (i.e. once for each priority).

20. When the event is escalated to a higher priority, you can set outputs to operate by dragging and dropping those required into the **Outputs** grid.
21. Drag and drop the DVR Cameras (Gallagher or third-party), Macros and/or External System Items required to be triggered into the **Cameras, Macros, and External System Items** grid.
    Note: When the Action Plan is executed:
    - The footage recorded by the cameras in this grid at the time of the event/alarm is associated with the event/alarm. As a result, when viewing an event/alarm in Command Centre client, a camera tile can show footage taken by these cameras at the time which the alarm occurred.
    - The string(s) on the **Trigger -- Events** tab of the cameras and External System Items in this grid are sent to those devices' third-party systems.
    - The Macros in this grid are run. Note that Macros that run a bulk change will not occur from an Action Plan.
22. Click the **Command Centre** tab.



23. 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.
    Note: The drop-down list will be populated with alarm priority names configured for the overall Command Centre system.

24. Drag and drop the macro(s) to be triggered if this Action Plan causes an alarm to be generated, into the **Macros** grid.
    Note: Macros that run a bulk change will not occur from an Action Plan.
25. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Action Plan.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
26. Click the **Notes** tab if you want to add a note(s) about this Action Plan. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
27. 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 Action Plan is created.
When an event is generated - that is linked to this Action Plan, those cameras and outputs will activate and an alarm message is displayed to the operator - with the set priority. If the alarm is not acknowledged it will escalate in priority.
Note: All macros that run from an Action Plan should be tested to ensure they do not cause a loop to occur. If a loop is triggered, either delete the macro from the Action Plan or set the Alarm Priority to 'Not an Event'.

Hint

Deleting Action Plans
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete an Action Plan.

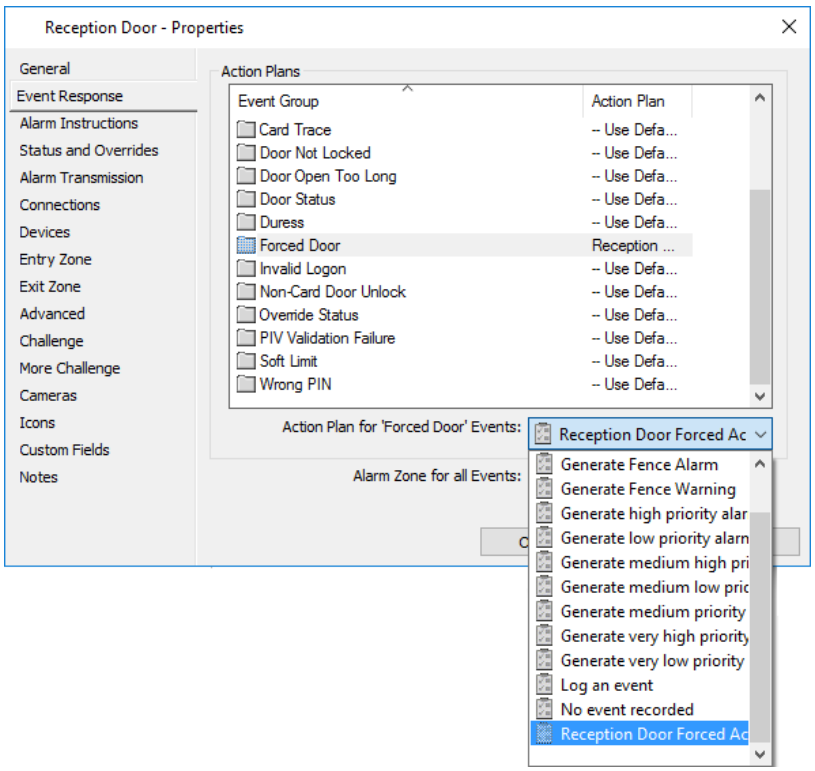
Assigning Action Plans to Events

Introduction

Action Plans are linked to system events, and can be assigned to any item that has an **Event Response** tab.
The following procedure describes how to assign Action Plans to Doors. This same procedure is used to assign Action Plans to the other items mentioned above. The only difference is at Step 2, where you select the appropriate item.

Procedure

1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens (in grid view).
2. **Right click** on the required Door, and select **Properties**.
3. Click the **Event Response** tab.
4. Highlight the Event Group that you wish to assign an Action Plan to.
   The edit box is then enabled.
5. Click the drop-down menu box and select the required Action Plan.



6. Repeat Steps 4 - 5 as necessary.
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

Action Plans are now assigned to a Door.

Chapter 16: Alarm Instructions

Introduction

An Alarm Instruction is a simple set of textual instructions that inform a workstation operator of what needs to be done in the eventuality of an alarm. Alarm Instructions are presented to an operator through the alarm details window (see Viewing alarm details).

To avoid unnecessary duplication of common information between Alarm Instructions, the text of an instruction can include insertion tags (see ***Insertion Tags*** on page 17-1 for further detail).

Assigning Alarm Instructions

Alarm Instructions can be assigned to any item that is capable of reporting events, (e.g. Alarm Zones, Doors, Inputs, etc.). See ***Alarm Instructions tab*** (on page 3-22) for further detail.

Refer to ***Operator Privileges*** (on page 37-1) to check you have the correct operator privilege level for the activity you wish to perform.

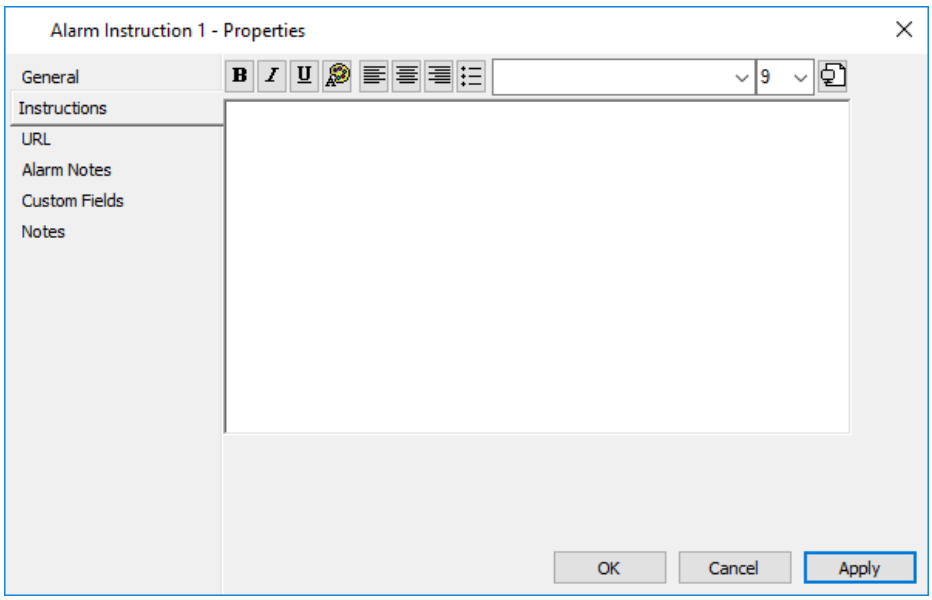
Creating a new Alarm Instruction

Introduction

This procedure details how to create an Alarm Instruction.

Procedure

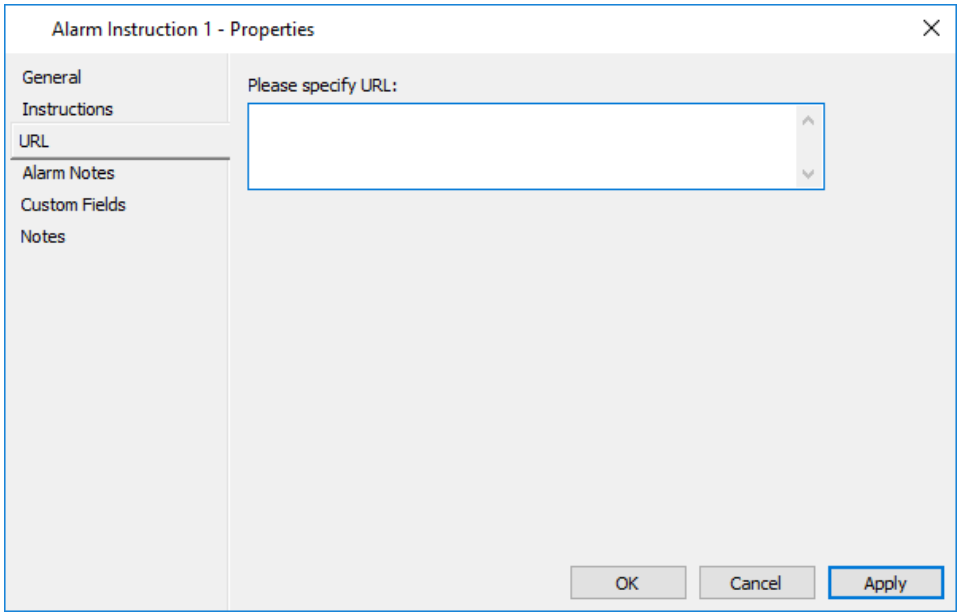
1. Click **Configure** from the menu bar, then **Alarm Instructions**.
   The **Alarm Instruction** List Window opens (in grid view).
2. **Right click** and select **New...Alarm Instruction**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Instructions** tab.



5. Enter the appropriate text for the instruction an operator is to undertake when an alarm occurs.
   Use the Formatting Toolbar on this window as necessary.
   Notes:
   - You can enter your text in any application that supports RTF, (e.g. Word, WordPad), and then paste it into the entry field on this screen with formatting.
   - Image files can be added to Alarm Instructions, however they can have a negative impact on performance. Therefore, it is recommended that images are **not** embedded in Alarm Instructions.
6. Add any applicable insertion tags for this Alarm Instruction.
   (See ***Adding an Insertion Tag to an Alarm Instruction*** on page 17-3 for the procedure.)

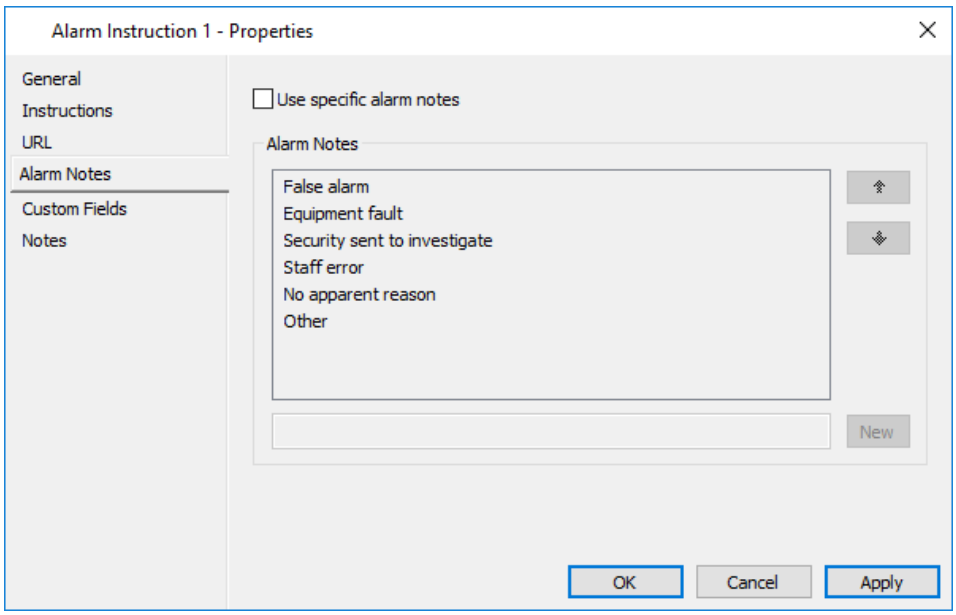
Note: Use the toggle button to view the alarm instruction as it would appear in the Alarm Properties.

7. Click the **URL** tab.



This tab supports the "Related URL" mode available when configuring URL Tiles in Command Centre Client. It provides the ability to specify a related URL against Alarm Instructions.

8. Specify a related URL for this Alarm Instruction if required.
9. Click the **Alarm Notes** tab.



This tab allows you to select specific alarm notes to be displayed for every alarm that has this Alarm Instruction assigned. By default, the **Alarm Notes** listbox is populated with whatever pre-defined alarm notes are configured in the server settings.

10. To use specific alarm notes, check the **Use specific alarm notes** checkbox. The pre-defined alarm notes disappear from the list.

To...	either...
add new alarm note(s),	• **right click** anywhere within the **Alarm Notes** field, and select **Insert** from the context menu, or • click the **New** button.
delete an alarm note, select the alarm note to be deleted, and	• **right click** and select **Remove from list** from the context menu, or • press the <**Delete**> key on your keyboard.

Notes:

- Unchecking the **Use specific alarm notes** checkbox and clicking **Apply** restores whatever alarm notes are configured in the server settings. Rechecking the checkbox restores the previously configured specific alarm notes.
- For alarm notes that are too long to fit within the listbox, a tooltip displays when you move the mouse over them.
- The **Alarm Notes** list can be sorted by selecting an alarm note you want to move up or down the list, and clicking the appropriate arrow button to the right of the list box.

11. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Alarm Instruction.
    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 Alarm Instruction.
    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 Alarm Instruction is created.

Hint

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

Chapter 17: Insertion Tags

An Insertion Tag is a container for commonly inserted data into an Alarm Instruction. When creating Alarm Instructions you can use Insertion Tags as place-holders for common data.
Insertion Tags are replaced with the information they reference by the Alarm Instruction object when it is displayed to the user.
For example:
'Call the Police on xxxxxxx' would be an insertion tag that could be applied to a number of Alarm Instructions. If the phone number for the police changes, only the insertion tag substitution string needs to be modified. The system would then automatically update each Alarm Instruction that has this insertion tag attached.

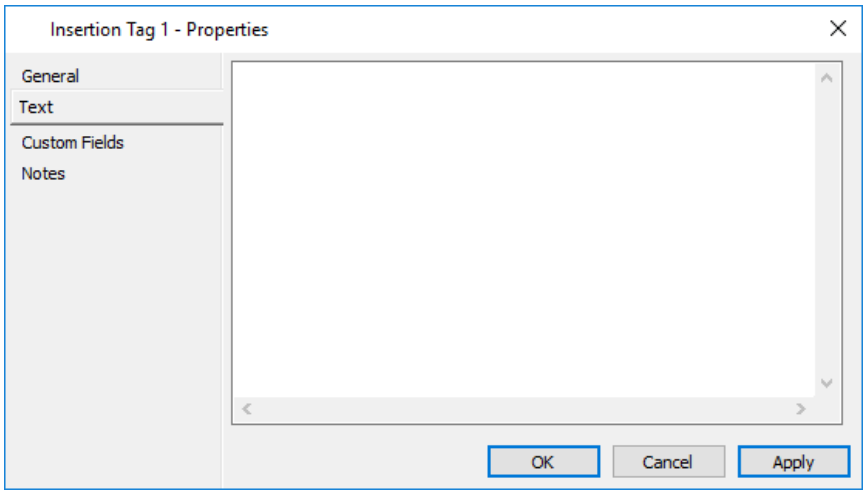
Creating an Insertion Tag

Introduction

This procedure details how to create an Insertion Tag.

Procedure

1. Click **Configure** from the menu bar, then **Insertion Tags**.
   The **Insertion Tag** List Window opens (in grid view).
2. **Right click** and select **New...Insertion Tag**.
   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 **Text** tab.



5. Type in the appropriate text for this Insertion Tag.
6. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Insertion Tag.
   For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
7. Click the **Notes** tab if you want to add a note(s) about this Insertion Tag.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
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

An Insertion Tag is created.

Hint

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

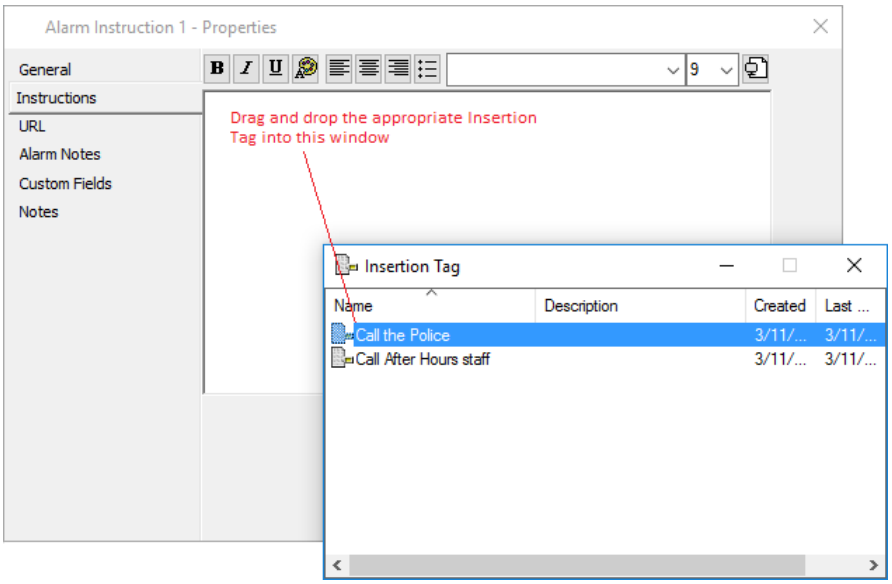
Adding an Insertion Tag to an Alarm Instruction

Introduction

This procedure enables you to add an Insertion Tag object onto an Alarm Instruction.

Procedure

1. Click **Configure** from the menu bar, then **Alarm Instructions**.
   The **Alarm Instruction** List Window opens (in grid view).
2. Highlight the Alarm Instruction you wish to add an Insertion Tag to.
3. **Right click** and select **Properties**.
4. Click the **Instructions** tab.
5. Open the **Insertion Tag** List Window.
   Select the Insertion Tag you wish to attach to this Alarm Instruction.
   Drag and drop it into the Instructions tab window.



Note: Clicking the Toggle Insertion Tags button allows you to swap between viewing the Insertion Tag by its name or message on the **Instructions** tab.

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

Result

An Insertion Tag has been added to an Alarm Instruction.
Note: To delete an Insertion Tag from an Alarm Instruction:
1. On the **Instructions** tab highlight the Insertion Tag.
2. **Right click** and select **Delete**.

Chapter 18: Site Plans

Understanding Site Plans

Site Plans show the layout and/or relationship of units to one another. Site Plans use (import) map images and allow graphical representations of Site Items to be placed on the map image. These Site Items can be placed on the map images as they are located in the real world and can be hardware units, (e.g. I/O Interfaces), or logical entities, (e.g. Access Zones). The following items can be placed on a Site Plan:
- All hardware devices
- Servers
- Access Zones
- Alarm Zones
- Doors
- Interlock Groups
- Elevator Cars and Elevator Car HLIs
- Services and Workstations
- External Systems
- Intercom Systems
- Macros
- Logic Blocks
- Links to other Site Plans

Site Items can be represented by icons or regions and are all able to convey information about their current state.

Site Items can be added, deleted, modified and viewed, depending on operator privileges.

For example:
Site Plans in Command Centre can be layered. An example of layered Site Plans would be to have an Overall (or Parent) Site Plan representing a complete Site with links to Site Plans that represent specific areas (sections) within that Site.

Each linked Site Plan is a section of the Overall Site Plan, containing site icons for that area and/or links to other Site Plans.

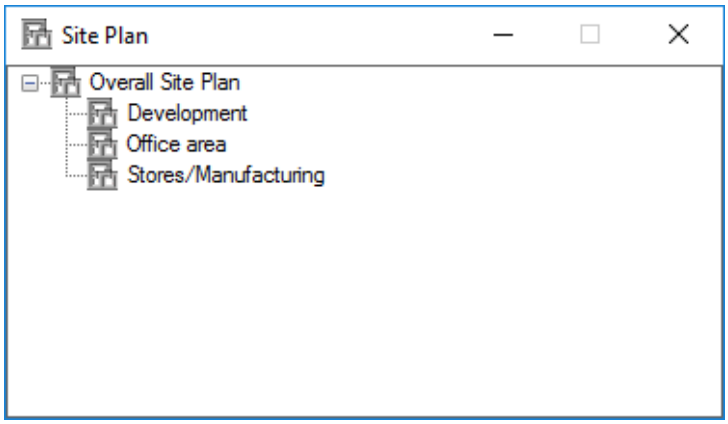
When an alarm occurs:

- The guard is viewing the Overall Site Plan.
- On this plan, a Site Plan icon flashes to indicate an alarm has occurred.
- The guard right-clicks this Site Plan icon and selects 'View Site Plan with Alarm' to access the layered Site Plan.

- The layered Site Plan window opens showing further details.
- The guard can now view what the alarm is and where the alarm occurred.
- Once the appropriate action has been taken and the alarm processed, the guard can return to the Overall Site Plan.

Site Plan List Window

The **Site Plan** List Window opens in tree view, which is achieved via the **Lineage** tab when you set up Site Plans.



Site Plans containing items in alarm will flash on this window. If the Site Plan that has items in alarm is a child Site Plan, the parent Site Plan will flash also.
Note:
Double-clicking on a Site Plan in alarm from here results in the Site Plan opening as long as it is a legacy Site Plan, (i.e. a Site Plan created in Configuration Client). You can then double-click the flashing icon on the Site Plan to open the Alarm Properties window for that item.

If a Site Plan was created in Command Centre Client, the following message will display when you double-click on it:
"This site plan is edited or viewed in the Command Centre Client"

Pop-up Menu

As well as the common menu options available by right clicking within the Site Plan window, there are also some other options specific to Site Plans.

View in New Window

Displays the site plan in "View" mode, (i.e. with **no** red line border around the site plan). You are unable to do anything in this view until you click the "Site Plan Editing Mode"  button.

Edit

Opens the Site Plan in "Edit" mode, (i.e. with a red line border around the site plan), so you can edit site items.

View Alarm

Displays the details of an alarm on the Site Plan, without changing the current Site Plan.
Note: This button is disabled if there are no alarms on the Site Plan.

View Site Plan with Alarm

Displays the Site Plan containing an alarm.
Note: This button is disabled if there are no alarms on the Site Plan.

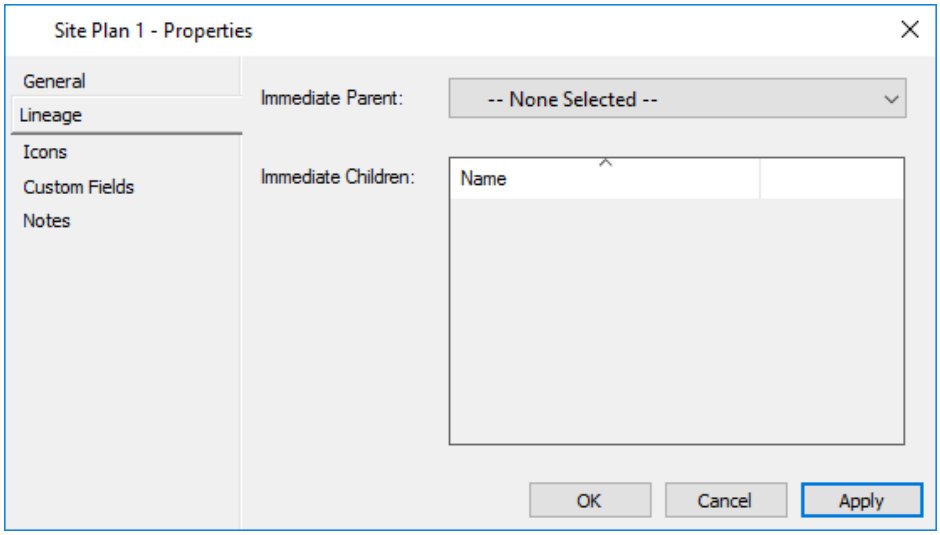
Creating a New Site Plan

Introduction

This procedure describes how to create a new Site Plan.

Procedure

1. Click **Configure** from the menu bar, then **Site Plans**.
   The **Site Plan** List Window opens (in tree view).
2. **Right click** and select **New...Site Plan**.
   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 **Lineage** tab.



5. If this Site Plan is part of a hierarchy, select the "Immediate Parent" Site Plan from the drop-down list.
   Note:
   This new Site Plan (once saved) will default into the "Immediate Children" box on the Properties of the Site Plan you selected as the "Immediate Parent".
6. Click the **Icons** tab if you want to change the Icon set for this Site Plan. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
7. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Site Plan.
   For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
8. Click the **Notes** tab if you want to add a note(s) about this Site Plan.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).

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 new Site Plan is created and now displays in the **Site Plan** window.

Hint

Deleting Site Plans
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete a Site Plan.

Site Plan "Edit" and "View" modes

Introduction

Legacy Site Plans, (i.e. Site Plans created in Configuration Client) can be opened in either "Edit" or "View" mode. If you try to open a Site Plan that was created in Command Centre Client in either of these modes, the following message will display:
"This site plan is edited or viewed in the Command Centre Client"

Both modes display a graphical image or map of a site, or part of a site. As the names of these modes suggest, one allows you to just view Site Plans, while the other allows you to edit Site Plans.

Touch screens

Site Plans is the only feature in Gallagher to support the use of touch screens, and is only applicable when in "View" mode, (i.e. it does not work in "Edit" mode). The implementation of single/double click is an added feature for the touch screen support.

If the users touch screen software currently "enables right click on hold", they do not need to do anything to enable the feature in Command Centre (right click on hold means if they hold their finger on the screen it will be the same as right clicking a mouse).

If the users touch screen does not "enable a right click on hold", they can contact Gallagher Tech Support for assistance.

Procedure

Opening a Site Plan in "View" mode

From the **Site Plan** List Window, either:

- **Double click** the Site Plan, or,
- Highlight the Site Plan, **right click** and select **View in New Window**.

The Site Plan opens in "View" mode.

Opening a Site Plan in "Edit" mode

1. From the **Site Plan** List Window, highlight the Site Plan.
2. **Right click** and select **Edit**.

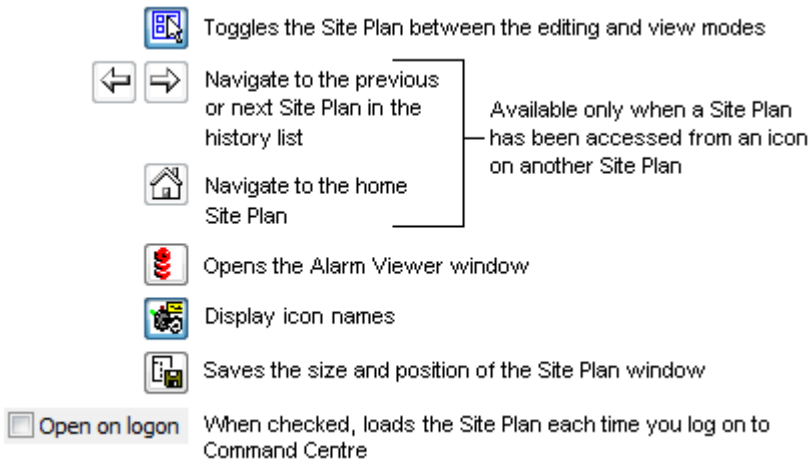
The Site Plan opens in "Edit" mode.

Note:

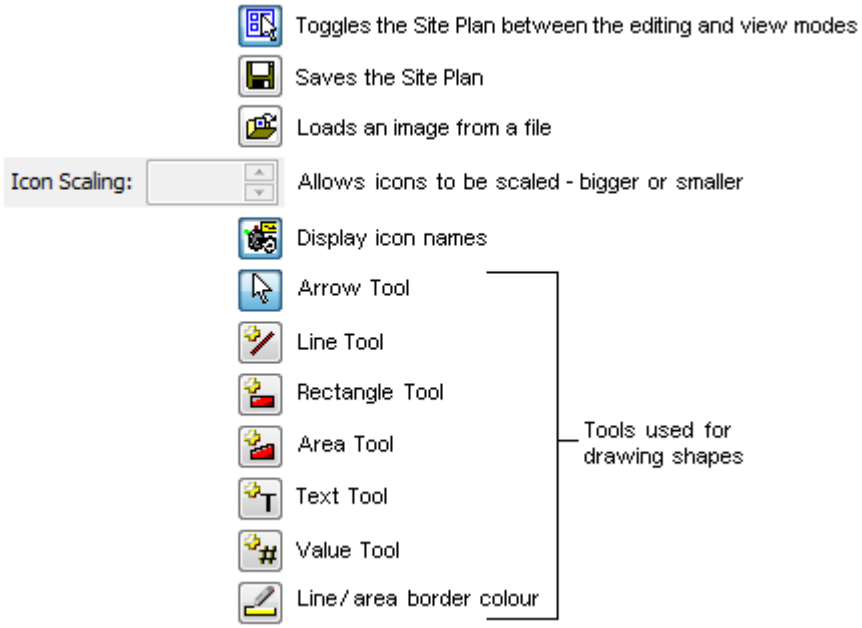
When you are in "Edit" mode there is a red line border around the Site Plan layout.

Toolbars

Toolbar - "View" mode



Toolbar - "Edit" mode



Editing a Site Plan

Introduction

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

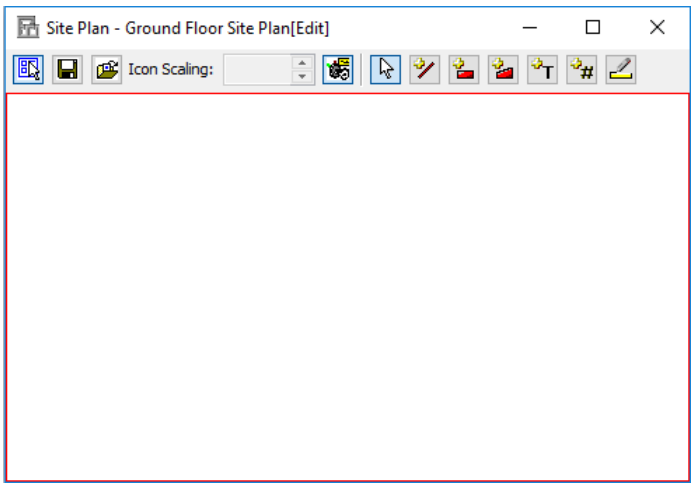
- Opening the Site Plan in "Edit" mode
  Note: The Site Plan needs to be in "Edit" mode and be a Legacy Site Plan, (i.e. created in Configuration Client) to perform the rest of the steps.
- Adding a Background
- Adding Areas, Rectangles and Lines.
  See ***Drawing on Site Plans*** (on page 18-12) for further details.
- Adding items to a Site Plan
- Scaling Icons
- Linking other Site Plans

Note: You cannot have a Site Plan in "Edit" mode and the properties for that same Site Plan open together when editing. If you try to save any changes to either, a message will display indicating that the object is already locked for editing.

Procedure

Opening the Site Plan in "Edit" mode

1. Click **Configure** from the menu bar, then **Site Plans**.
   The **Site Plan** List Window opens (in tree view).
2. Highlight the Site Plan you want to edit.
3. **Right click** the mouse button, and select **Edit**.
   The new Site Plan opens in "Edit" mode, (i.e. there is a red line border around the Site Plan grid.)



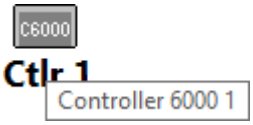
Adding a Background

4. Click on the  icon.
5. From the displayed pop-up window, path your way to the Background file you wish to import and click the **Open** button. The Background file can be any of the following formats:
   - .wmf
   - .emf
   - .bmp
   - .jpeg
   - .gif

Adding items to a Site Plan

The following items can be placed on a Site Plan, as they are located in the real world and can be hardware devices or logical entities:
All hardware devices, Servers, Access Zones, Alarm Zones, Doors, Interlock Groups, Elevator Cars and Elevator Car HLIs, Services and Workstations, External Systems, Intercom Systems, Macros and Logic Blocks.

6. Open the List Window of the item type you want to add to this Site Plan.
7. Drag the required item(s) onto the displayed Site Plan.
   Notes:
   - When you drag items onto the Site Plan, they scale appropriate to the background size.
   - If the size of the Site Plan is too small when dragging items on, it may end up with a grey area (to the right or below) where you cannot drop items. You are less likely to see a grey area if you have the Site Plan as large as possible when dragging items on. This grey area only appears when in "Edit" mode.
8. Close the List Window of the item you added.
   By default, the item names display underneath the icons.
   If the item has a Short Name this displays on the Site Plan, with the Full Name appearing as a "Tool Tip" when you hover the cursor over the icon, as shown in the example below:



Notes:

- Short Names are not displayed when a Site Plan is opened in Command Centre Client. Instead, the items Full Name displays, as shown in the example below:



Controller 6000 1

- Item names can cause a Site Plan to become quite cluttered, so you have the option of being able to turn the names off by clicking the  button. With the names turned off, the Full Names will still appear as "Tool Tips" when you hover the cursor over the icons.

Scaling Icons

The following steps allow you to alter the size of the icons on this Site Plan. This is another way of making Site Plans look less cluttered.

9. Alter the percentage in the Icon Scaling field 

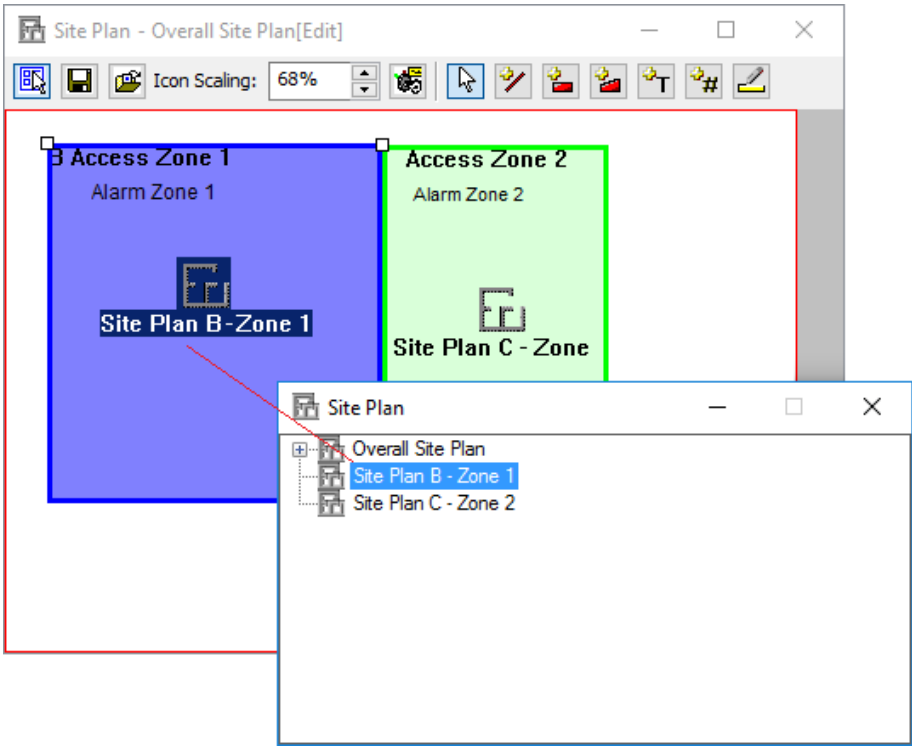
as required.

10. Press the <**Enter**> key on the keyboard.
The icons and their names (if you have the names turned on so they display) on the Site Plan alter in size accordingly, while the size of the Site Plan itself remains the same.
Note:
Scaling is limited to 10% and 500%. Even if a Site Plan is reduced in size, the icons will not scale below 10%.

Linking other Site Plans

11. From the **Site Plan** List Window, select the Site Plan to which you wish to establish a link.
Drag and drop it onto the Site Plan.

Note: You can drag and drop Site Plans created in Command Centre Client onto Legacy Site Plans, however when you try to open the link in Configuration Client the following message will display:
"This site plan is edited or viewed in the Command Centre Client"
Opening them in Command Centre Client will work correctly.



12. Click the button to save your changes.
13. **Close** the Site Plan.
    Note:
    If you do not do Step 12, a confirmation window displays.
    Click **Yes** to save your changes.

Hints

Importing background images
If you import a background image the icons on the Site Plan automatically resize. This is due to screen resolutions.

Sizing and Positioning Site Plans
The size and position of a Site Plan can be altered to suit your purposes. The position of a Site Plan can be altered by clicking on the title bar, holding down the mouse button and then dragging it to the desired position. To resize a Site Plan, see ***Sizing the windows*** (on page 3-9) for the procedure.
These settings will be saved by the system for your logon only, (i.e. the size and position of a Site Plan saved by one operator will not affect another operator).
Note: Resizing a Site Plan scales the icons relative to the size of the Site Plan, and the percentage in the "Icon Scaling" field alters accordingly.

Drawing on Site Plans

Introduction

When a Site Plan is in "Edit" mode, it is possible to draw shapes and/or add text to Site Plans. Lines and areas as shapes on Site Plans can represent site items, (i.e. they can change colour depending on their state and also flash when alarms occur).
The drawing tools available are:

 Line Tool
 Text Tool
 Rectangle Tool
 Value Tool
 Area Tool
 Line / area border colour

This topic includes the following procedures relating to drawing on Site Plans:

- ***Adding lines or areas*** (on page 18-13)
- ***Adding rectangles*** (on page 18-13)
- ***Moving or Resizing shapes*** (on page 18-14), (i.e. lines, areas and rectangles)
- ***Editing shape properties*** (on page 18-15), (i.e. lines, areas and rectangles)
- ***Hiding/Displaying icons*** (on page 18-17)
- ***Adding text objects*** (on page 18-18)
- ***Adding values*** (on page 18-19)
- ***Moving text objects*** (on page 18-22)
- ***Editing text object properties*** (on page 18-22)
- ***Deleting shapes and text*** (on page 18-22)

Hint

It is recommended you load a background on to a Site Plan, then add large objects like areas and rectangles, then add lines, icons and lastly text.
All text objects shall appear in front of (above) all icons, which shall appear in front of (above) all lines, which shall appear in front of (above) all areas.

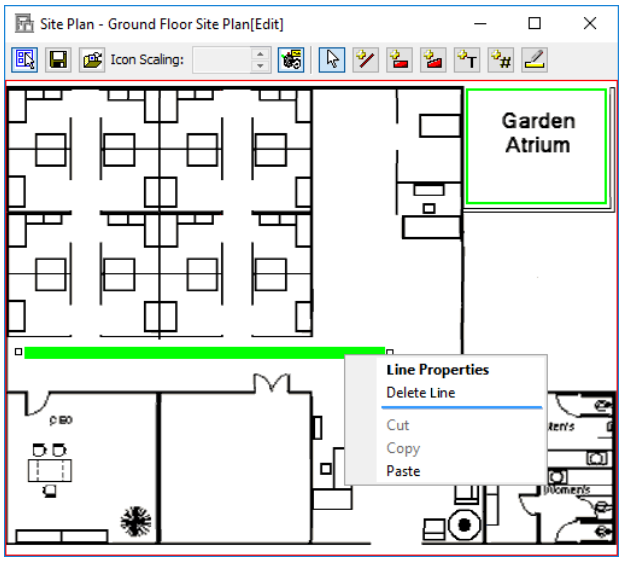
Layer	Item
1. Top	Text
2. Upper	Icons
3. Middle	Lines
4. Lower	Areas

Within each layer the order of the items is determined by the order in which they were first added to the site plan: hence older icons will appear to be behind more recently added icons **if** they overlap. Likewise, for older versus newer lines and areas. This ordering is also used to determine which item is being clicked when the cursor is on top of overlapping items.

Adding lines or areas

1. Open the Site Plan you want to add a line or area to.
2. Click the  icon.
   The Site Plan opens in “Edit” mode, (i.e. there is a red line border around the Site Plan grid).
3. Click on the  icon to draw a line, or the  icon to draw an area.
   When you move the cursor onto the Site Plan grid, the cursor changes to a  tool to indicate that drawing mode has started.
4. Place the  cursor on the spot where you want the line to start, then left click and move the mouse to the next point.
   Note: You can click at any point in the line and move the cursor in another direction.
5. When you reach the last point in the line, double-click to mark the line end. The  cursor remains, allowing you to move the starting point for a second line.

Note: To exit the drawing mode, you can click the  button or **Esc**, or alternatively you can choose another drawing tool.

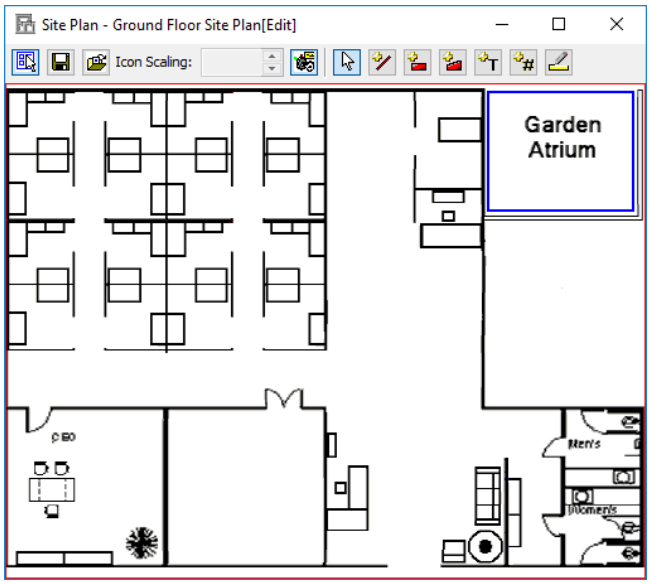


A line and area have been drawn onto this Site Plan, with the "line/area border colour" set to green.

Adding rectangles

1. Click on the  icon.
   When you move the cursor onto the Site Plan grid, the cursor changes to a  tool to indicate that drawing mode has started.

2. Place the cursor where you want to draw a rectangle, then left click and drag the cursor diagonally in the direction you want.



A rectangle has been drawn onto this Site Plan, with the "line/area border colour" set to blue.

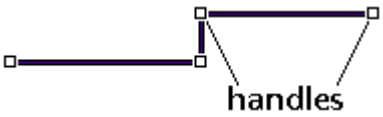
Moving or Resizing shapes

A line, area or rectangle can be:

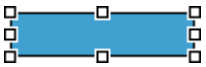
- repositioned as a whole (retaining the relative size and orientation), or
- resized

1. Click the icon.
2. Click anywhere on the line, or anywhere in the area or rectangle.

Handles appear at every “point” on the line,
or,



around the outer edge of the area or rectangle

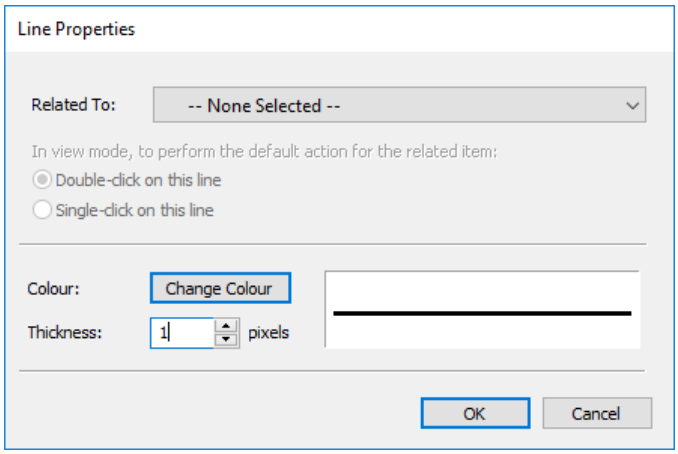


3. What do you want to do to the shape?

If...	then...
move / reposition	ensuring the cursor is pointing at the line, or anywhere in the area or rectangle, and **not** one of its handles, drag the shape to its new position.
resize	ensuring the cursor is pointing on one of the handles, drag the handle until the line, area or rectangle becomes the desired size.

Editing shape properties

1. Click the  icon.
2. Click anywhere on the shape, (i.e. line, area or rectangle), so that the handles appear.
3. Right click and select the **Properties** option, (i.e. **Line Properties**, **Area Properties** or **Rectangle Properties**).
   Note: The properties dialog is very similar for each type of shape. The screen example shown below is that of the Line Properties.



   The **Related To** drop-down list includes any site items that are currently on the Site Plan, including links to other Site Plans.
4. Do you want to associate the shape with a site item?

If...	then...
no	go to Step 5.
yes	**a)** Select the required site item from the **Related To** drop-down list. The two radio buttons are enabled. **b)** Select the appropriate radio button for the action you require when the Site Plan is in "View" mode, as follows: • Selecting the **Double-click on this line** radio button will allow a double-click on this line to execute the default action for the related site item. • Selecting the **Single-click on this line** radio button will allow a single-click on this line to execute the default action for the related site item.

   Note: If you do associate a shape with a site item, you then have the option to hide the icon behind the shape if you want. See ***Hiding/Displaying icons*** (next) for details.
5. The **Colour** of a line, or the **Fill Colour** of an area or rectangle, can be altered.

If you want to change the colour of the shape, click the **Change Colour** button.
A colour swatch displays which allows you to change the colour of the shape.
Notes:

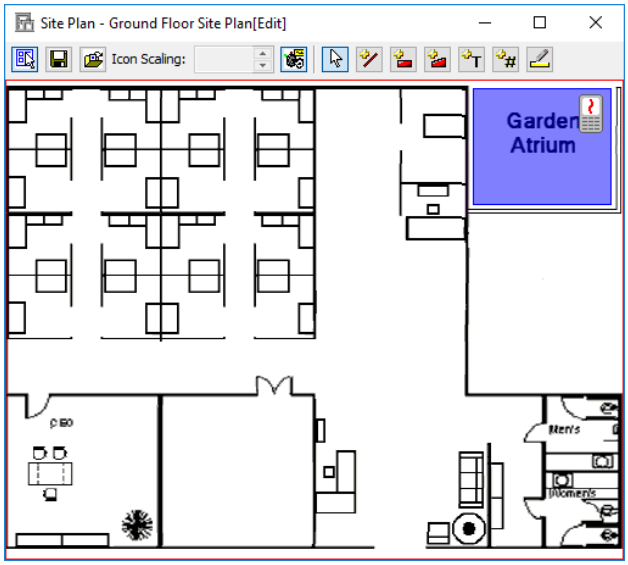
- Only the standard 48 colours are available. The custom colour option is disabled.
- If a site item is selected in the **Related To** field, this button is not available, and is replaced with the text:
  "Colour defined by Icon Set".

6. Click on the colour required, then click the **OK** button.
   The colour of the shape in the preview pane changes, displaying the new colour selected.
   Note:
   The border colour shown in the preview pane is the current Site Plan border colour, and does not change by clicking the **Change Colour** button.
   You can change the border colour by clicking the  icon. A colour swatch displays allowing you to change the border colour on all the shapes on this Site Plan.
7. What type of shape are you altering?

If it is a...	then you can alter...
line	the **Thickness** of the line if required. The line thickness is defined in pixels, excluding the thickness of the border. **Note:** As you alter the pixels, the preview pane shows the line thickness changing.
rectangle or area	the **Transparency** of the shape if required. The shape transparency is defined as a percentage. **Note:** As you alter the percentage, the preview pane illustrates the effect of transparency. The text "Background" is shown behind the coloured rectangle. This text is hidden when the transparency is 0%, and progressively appears as the transparency increases to 100%.

Hints:

- The more transparent a shape is, the better the visibility.
- It is recommended that you do not choose colours (these colours are defined on your icon sets), that are the same as your alarm priority colours, as the alarm will flash the same colour as the line/area making it difficult to see.
- Shapes should not be drawn to cross over themselves, as the entire area will flash in alarm state, rather than just the border, and if the alarm colour is the same as the area colour you may not see any change.



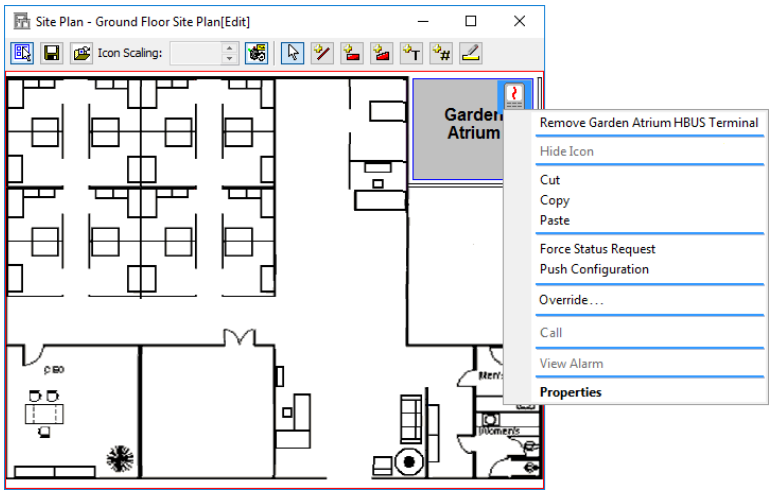
- The rectangle drawn on this Site Plan has had the "Garden Atrium HBUS Terminal" associated with it (from the **Related To** drop-down list), and the **Transparency** set to 50 percent.

Hiding/Displaying icons

Site items that are associated with a shape (via the **Related To** drop-down list on the Properties dialog of the shape), can be hidden behind the shape or displayed in front of the shape, as follows:

Hiding icons

1. Select the item you want to hide.
2. **Right click** the mouse button to display the pop-up menu.
3. Select the option **Hide Icon**.



The icon can no longer be seen in front of the shape.

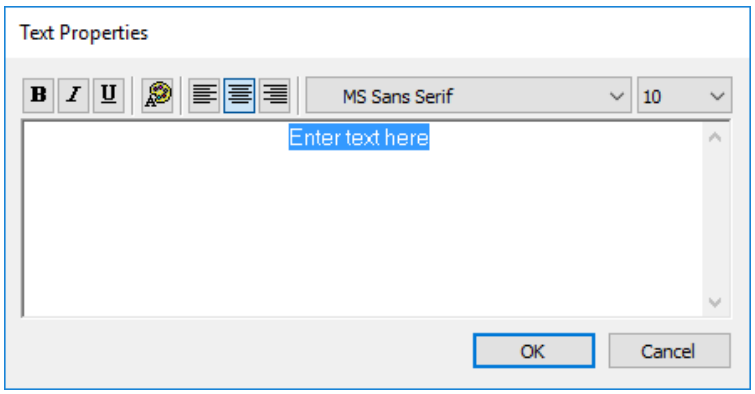
Displaying icons

1. **Right click** on the shape.
2. From the pop-up menu displayed, select the option **Display Icon**.
   The icon appears in front of the shape.

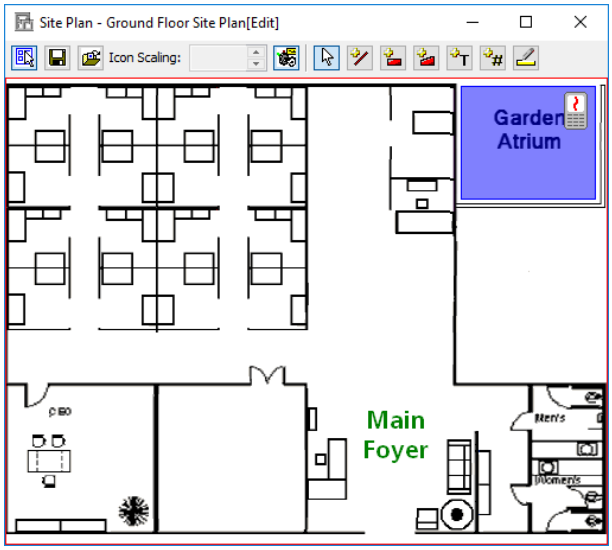
Adding text objects

Operators can enter stand-alone text objects for display on a Site Plan. Such text objects are additional to the names associated with icons.

1. Click on the  icon.
   When you move the cursor onto the Site Plan grid, the cursor changes to a  tool to indicate that drawing mode has started.
2. Place the  cursor where you want to enter text, then left click and drag the cursor diagonally in the direction you want.
   The **Text Properties** dialog displays:



3. Enter the text required, then use the formatting tools across the top of this dialog to format the text how you want it to appear on the Site Plan.
   Notes:
   - Standard copy, cut and paste commands can be used to enter text.
   - If you want to add “white” text (probably because the site plan has a dark background), type in the text, and then change the colour of it to white. If you change the colour first, you will not be able to see the text as you type it.
4. Click the **OK** button.
   The text displays on the Site Plan.
   Note: You may need to resize the text box to see the entire text.

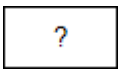


The text "Main Foyer" has been added to this Site Plan, with the colour of the text set to green.

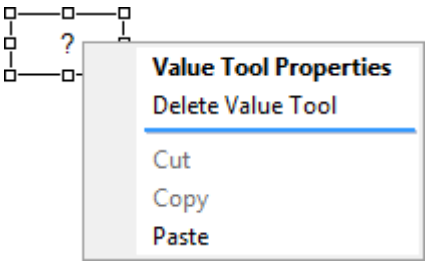
Adding values

This tool enables an operator to have values visible on a Site Plan for Zone Counts and Fence Voltages.

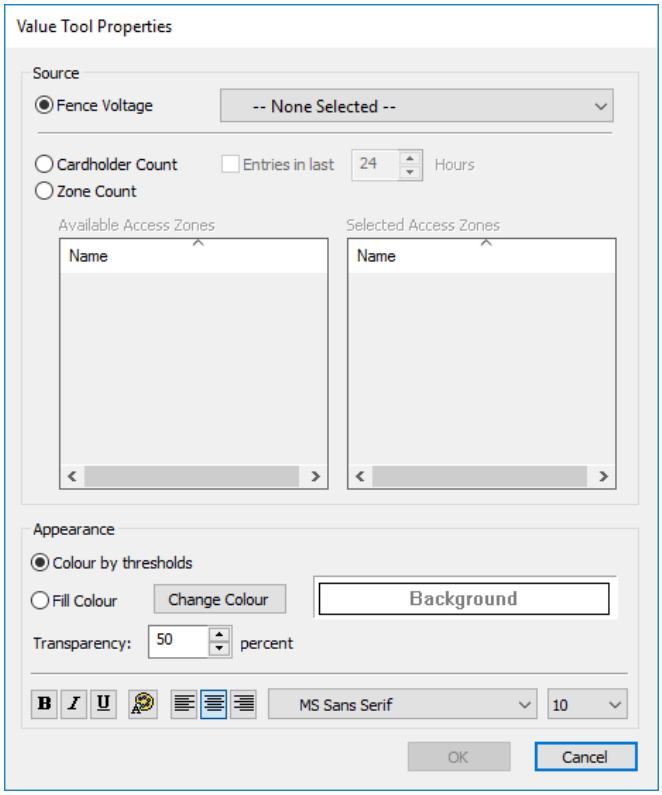
1. Click the  icon.
   When you move the cursor onto the Site Plan grid, the cursor changes to a  tool to indicate that drawing mode has started.
2. Place the  cursor where you want to place the value tool, then left click and drag the cursor diagonally in the direction you want.

   A rectangle appears with a question mark in the centre of it: 

3. Right click in the rectangle so that handles appear around the outer edge, and select **Value Tool Properties** from the context menu.



The **Value Tool Properties** dialog displays:



4. Click the appropriate radio button for the option you want values to display for, (i.e. **Fence Voltage**, **Cardholder count** and **Zone Count**).

5. What option did you select?

If you selected...	**then...**
Fence Voltage,	select a Fence Zone from the available Fence Zone drop-down list.
Cardholder count,	**a)** If you want to configure a time span, check the **Entries in last <x> Hours** checkbox, and enter the appropriate figure. Cardholders will be removed from the count if their entry to the zone occurred more than <x> hours in the past, and if there are multiple zones being monitored and the person moves between those internal zones. **b)** Move the zone(s) you require from the 'Available Access Zones' grid to the 'Selected Access Zones' grid by selecting the zone and dragging it across. **Note:** The 'Available Access Zones' grid is only populated with Access Zones that are already on the Site Plan.
Zone Count,	move the zone(s) you require from the 'Available Access Zones' grid to the 'Selected Access Zones' grid by selecting the zone and dragging it across.

The **OK** button is enabled.

6. The colour of the item on the Site Plan can be customised or driven by thresholds.
   If required, click the **Colour by thresholds** radio button.
   The background of the rectangle will change based on the value displayed.
   The core colour of the rectangle will be controlled by value thresholds, as follows:

Option	Threshold colours
Fence Voltage	Green = Fence Warning - Low Voltage Yellow = Fence Warning - Mid-range Red = Fence Warning - High Voltage
Cardholder count	Green = zero Red = above zero
Zone Count	Green = Zone Count Minimum Yellow = Zone Count Mid-range Red = Zone Count Maximum

7. The **Fill Colour** of a rectangle can be altered.
   If you want to change the colour of the shape, click the **Change Colour** button.
   A colour swatch displays which allows you to change the colour of the shape.

8. Click on the colour required, then click the **OK** button.
   The colour of the shape in the preview pane changes, displaying the new colour selected.

   Note: The border colour shown in the preview pane is the current Site Plan border colour, and does not change by clicking the **Change Colour** button. You can change the border colour by clicking the  icon. A colour swatch displays allowing you to change the border colour on all the shapes on this Site Plan.

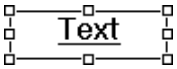
9. Alter the **Transparency** of the rectangle if required.
   The rectangle transparency is defined as a percentage.

   Note: As you alter the percentage, the preview pane illustrates the effect of transparency. The text "Background" is shown behind the coloured rectangle. The text is hidden when the transparency is 0%, and progressively appears as the transparency increases to 100%.

10. Use the text formatting tools at the bottom of this dialog to format how you want the values to appear on the Site Plan. Select the options that you want to apply, such as font style and font size.

Moving text objects

A text object can be repositioned as a whole (retaining the relative size and orientation), as follows:

1. Click the  icon.
2. Click on the text object.
   Handles appear around the outer edge of the text object: 

3. Drag the text object to its new position.

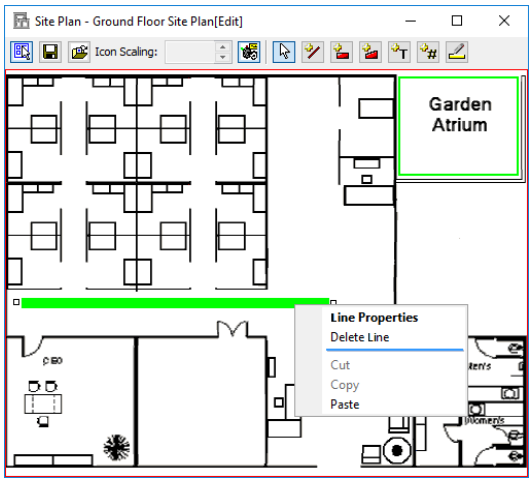
Editing text object properties

1. Click the  icon.
2. Click anywhere on the text object so that the handles appear.
3. Right click and select the **Text Properties**.
   The **Text Properties** dialog displays.
4. You can alter the format of the text, (e.g. make it **bold** or *italics*, change the font and/or size, etc.), and change the content of the text itself.
5. Click the **OK** button.

Deleting shapes and text

You can delete shapes, (i.e. lines, areas and rectangles) and/or text that have been placed on a Site Plan, as follows:

1. Select the shape or text you want to delete.
2. **Right click** the mouse button to display the pop-up menu.
3. Select the appropriate **Delete** option, (e.g. **Delete Rectangle**, etc.)



The shape or text is deleted from the Site Plan.

Note: If a shape on a Site Plan has a site item associated with it, when you delete the shape, the icon will reappear. See ***Removing Icons from Site Plans*** (on page 18-24) if you want to remove the icon also.

Navigating between linked Site Plans

Introduction

This procedure describes how to navigate between linked Site Plans. The procedure for linking Site Plans is described as part of the procedure under ***Editing a Site Plan*** (on page 18-8).

Note: If a linked Site Plan was created in Command Centre Client, the following message will display when you try to open it using this procedure: *"This site plan is edited or viewed in the Command Centre Client"*

Procedure

1. Open any linked Site Plan.
2. Place the cursor on the icon of a linked Site Plan, and either:
   - Right click and select **View in New Window**.
     The linked Site Plan opens, and the first Site Plan remains open also. Using this method does not activate the **Home** and **Arrow** navigation buttons on the toolbar.

   Or,

   - Double-click on the icon.
     The first Site Plan closes and the linked Site Plan opens.
     Also observe that on the Site Plan window toolbar, the **Home** navigation button and one of the **Arrow** navigation buttons are activated. These buttons allow you to move between the linked Site Plans as required.

     Note:
     If the Site Plan is in "Edit" mode, and you accidentally drag the cursor slightly before you double-click on a linked Site Plan icon, the following message displays:
     "You have made changes to the site plan you are currently editing. Do you want to save those changes?"
     Click either the **Yes** or **No** button, and the linked Site Plan opens. Only use the **No** button if you are certain you have not made any changes.
3. If a Site Plan icon is contained on the Site Plan just opened, click on that.
4. Assuming there are more linked Site Plans, repeat Step 3 to select additional Site Plans as required.
   Remember that the **Arrow** and **Home** navigation buttons can be used to move between the linked Site Plans.

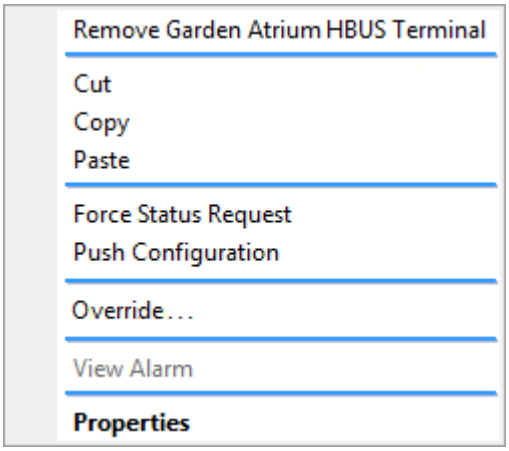
Removing Icons from Site Plans

Introduction

You can remove icons that have been placed within a Site Plan.

Procedure

1. Open the correct Site Plan.
2. Click on the  Site Plan editing icon.
   The Site Plan window is now in "Edit" mode.
3. Select the icon you want to remove.
4. **Right click** the mouse button to display the pop-up menu.
5. Select the option **Remove <item name>**.
   In the case of the example below, the option is **Remove Garden Atrium HBUS Terminal**.



Chapter 19: Icon Sets

Understanding Icon Sets

An Icon Set is a set of icons that is assigned to a particular object. The number of icons in a set can vary depending on the type of object. For example, an Input has three icons in its set to depict the various states, (i.e. Open, Closed and Tampered).

There are default Icon Sets for all FT items that can appear as an icon on a Site Plan. Operators with the "Edit Icon Sets" operator privilege can create new Icon Sets, as well as view, edit and delete existing Icon Sets. This gives operators more control over how icons are displayed on a Site Plan.

Note:
There are a number of Icon Editor software programs readily available online, via the Internet. To locate a suitable Icon Editor for editing and/or creating Icon Sets, go to Internet Explorer and search on "Icon Editors".

Creating a new Icon Set

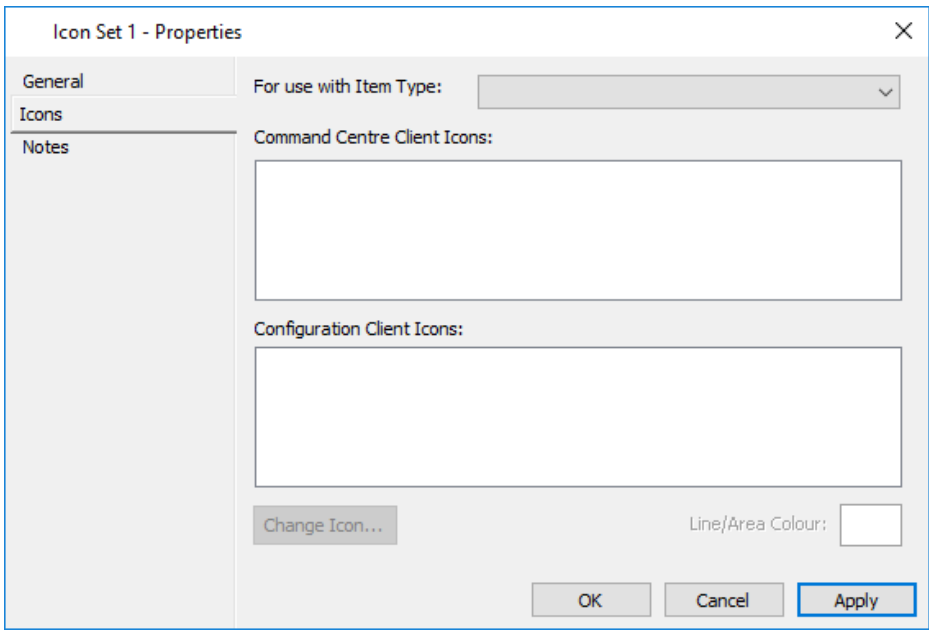
Introduction

This procedure details how to create a new Icon Set in Gallagher Command Centre.

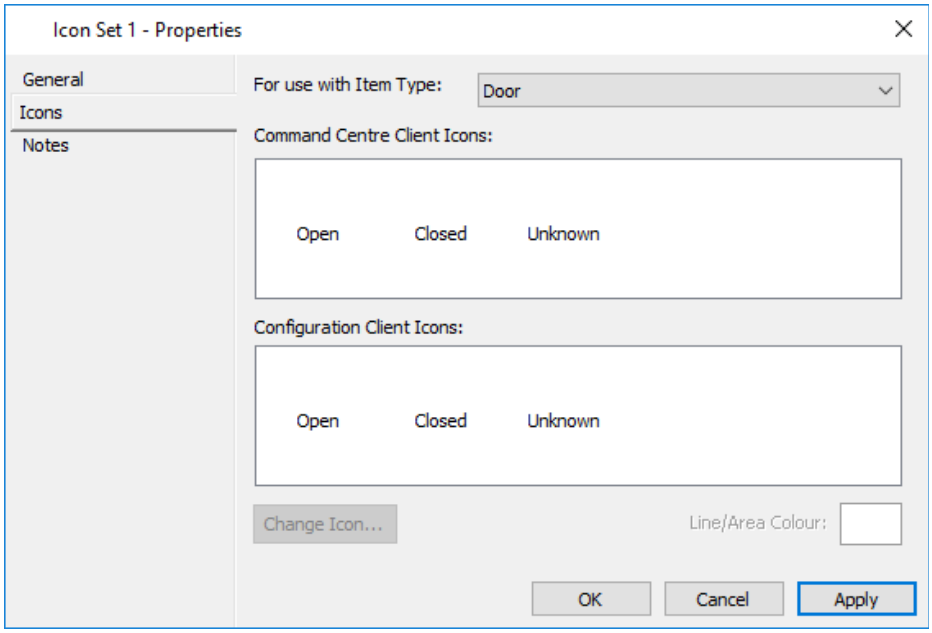
Note: Standard Gallagher Icon Sets are created with dimensions of 32 x 32 pixels, so when creating new Icons Sets these same dimensions, and 256 Colour format, should be used. Other dimensions can be made to work but will cause scaling to be applied which may reduce the effectiveness of the icons.

Procedure

1. Click **Configure** from the menu bar, then **Icon Sets**.
   The **Icon Set** List Window opens (in grid view).
2. **Right click** and select **New...Icon Set**.
   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 **Icons** tab.



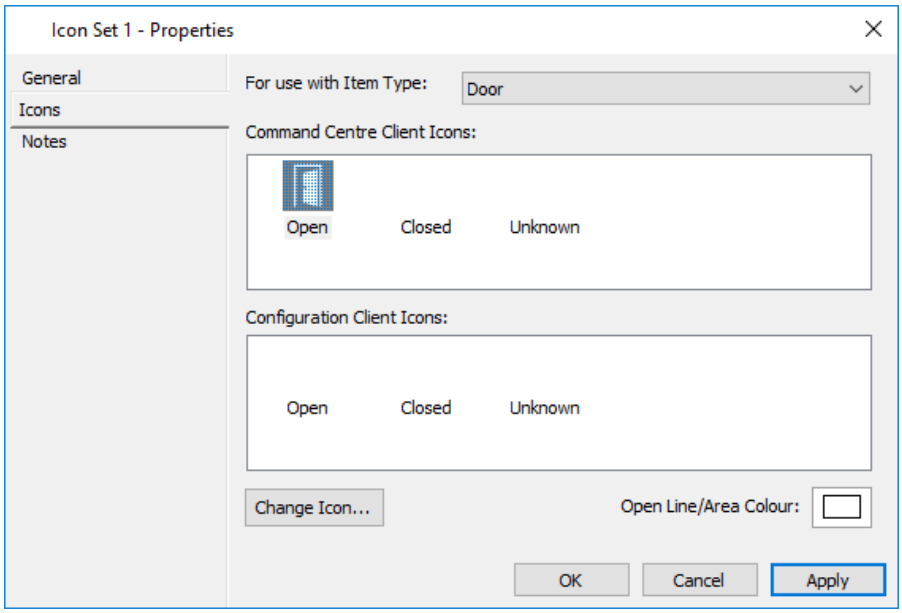
5. From the drop-down list, select the Item Type that this Icon Set will be used with.
   Note:
   The drop-down list displays licensed items only, however the main **Icon Set** List Window displays all items.



The grids become populated with the two sets of icon state(s) applicable to that Item Type, (i.e. the upper grid displays the icons for the Command Centre Client and the lower grid displays the icons for the Configuration Client).

Note: The number of states that display in the main grid will depend on the type of item that the Icon Set represents. For example, in the screen above, 'Door' was selected, therefore the various states of a Door display, (i.e. Open, Closed and Unknown).

6. In the appropriate grid for either the Command Centre Client or Configuration Client icons, click on the icon state you want to select a new icon for.
   The state name becomes highlighted Open, and the **Change Icon...** button and the **Open Line/Area Colour...** field become enabled.
7. Click the **Change Icon...** button.
   A dialog displays for you to select an icon file from.
   Note: This dialog automatically displays the default icons which are stored by default in an Icons folder (this may differ depending on your installation) under:
   `"...\Gallagher\Command Centre"`
8. Path your way to the directory where the icon file you require is stored.
   Note: Only ***.ico** and ***.png** Icon image files can be used.
9. Select the icon file and click the **Open** button.
   The icon displays above the icon state.



10. Repeat Steps 6-9 for all icon states.
    Note: If you try to save your changes before selecting a state for each icon, a message will display:
    "An icon has not been selected for the <name> state"
11. Click on the **Open Line/Area Colour...** field.
    A colour swatch displays allowing you to change the colour of the line/area.
    Note: Only the standard 48 colours are available. The custom colour option is disabled.
12. Click on the required colour, and click the **OK** button.
    The colour of the line/area in the preview pane changes, displaying the new colour selected.
13. Click the **Notes** tab if you want to add a note(s) about this Icon Set.
    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 Icon Set has been created.

Hint

Deleting Icon Sets
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete an Icon Set.
Note: The system will allow an Icon Set to be deleted providing it is not currently used by a site item, or it is the only Icon Set for an Item Type. If an Icon Set cannot be deleted, one of the following messages explaining why will display: *"This Icon Set cannot be deleted, as it is still used by a site item."* OR *"This Icon Set cannot be deleted, as it is the only icon set assigned to a type of item."*

Modifying an existing Icon Set

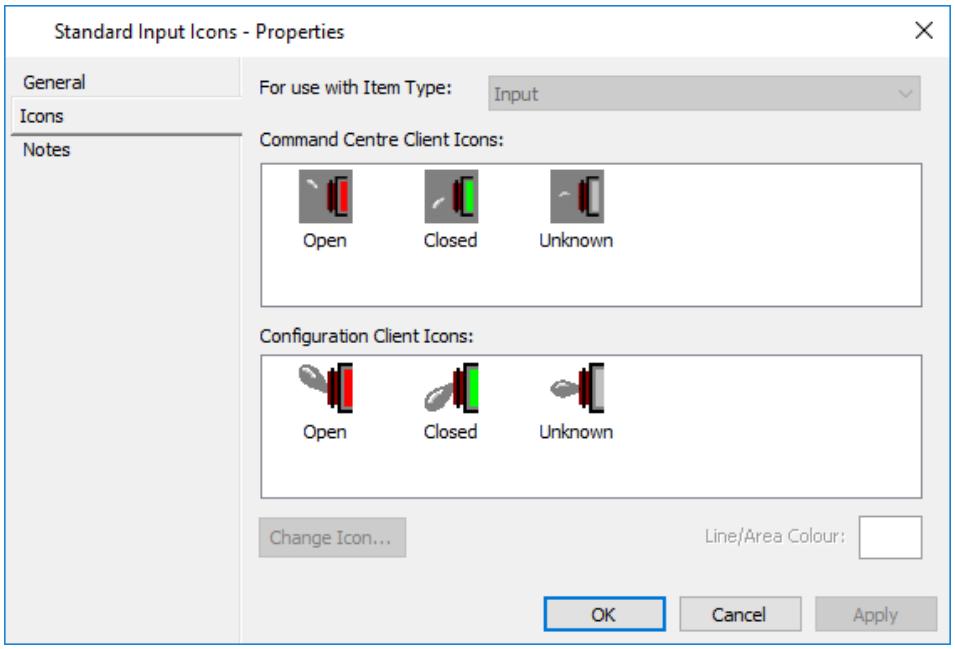
Introduction

This procedure details how to modify an existing Icon Set.

Note: Although the screen shots shown in the following procedure are for the "Standard Input Icons", the procedure is exactly the same for modifying any Icon Set.

Procedure

1. Click **Configure** from the menu bar, then **Icon Sets**.
   The **Icon Set** List Window opens (in grid view).
2. Highlight the Icon Set you want to change.
3. **Right click** the mouse button, and select **Properties**.
4. Click the **Icons** tab.



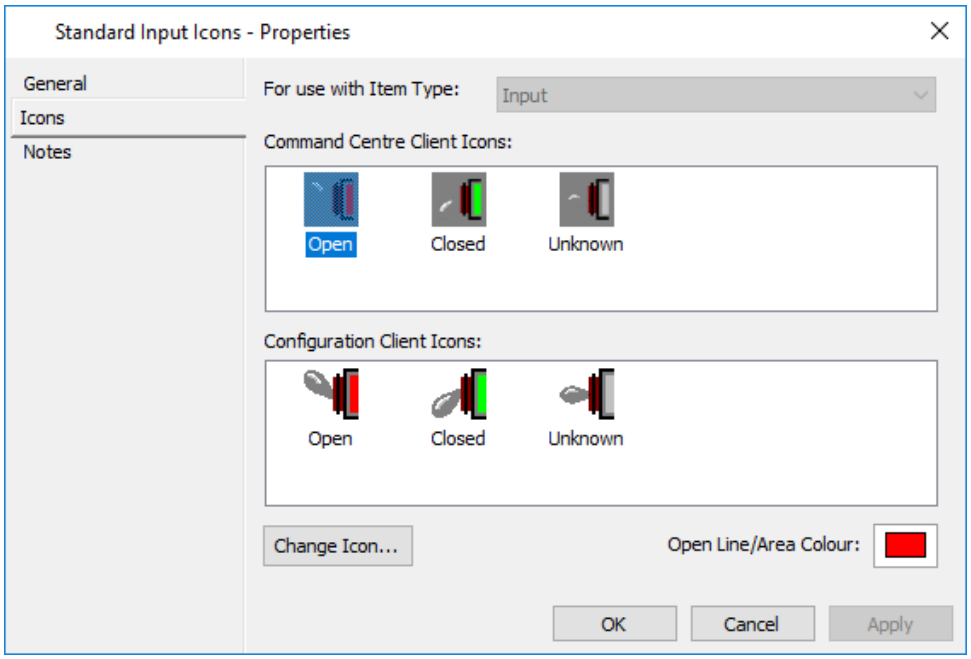
5. In the appropriate grid for either the Command Centre Client or Configuration Client icons, click on the icon state you want to select a new icon for.

   The icon state becomes highlighted Open, the buttons on this screen become enabled, and the colour of the icon state displays in the preview pane.
6. Click the **Change Icon...** button.
   A dialog displays for you to select an icon file from.

Note:
This dialog automatically displays the default icons which are stored by default in an Icons folder (this may differ depending on your installation) under:
"...\Gallagher\Command Centre"

7. Path your way to the directory where the icon file you require is stored.
   Note: Only ***.ico** and ***.png** Icon image files can be used.
8. Select the icon file and click the **Open** button.
   The selected icon now displays above the icon state, replacing the original one.



9. Repeat Steps 5-8 for any other icon states you want to select a new icon for.
10. Click the **Notes** tab if you want to add a note(s) about this Icon Set. 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

An existing Icon Set has been modified, and the changes will be reflected through the rest of the system, (i.e. where ever that Icon state appears in Command Centre, the new icon will display).

Chapter 20: Macros

Understanding Macros

Macros can be created for scheduling a set of pre-programmed overrides or for scheduling a bulk change. Macros provide the ability to group and schedule them for a specific time and for specific durations, either on a one-off basis or for events that repeat on a daily or weekly basis.

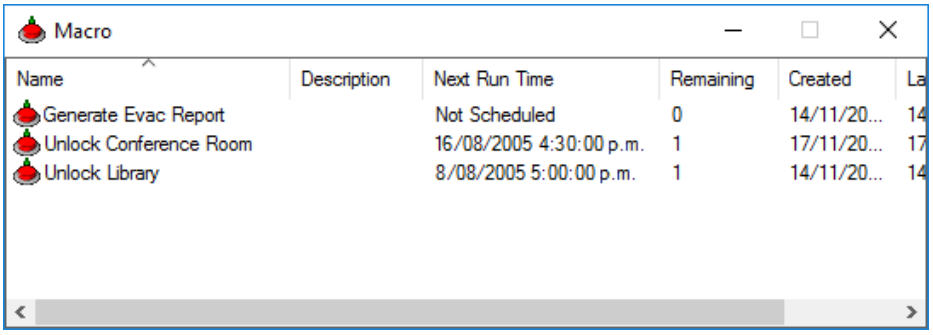
Such overrides would cater for special after-hours events that require changes to the normal security settings for the site. For an after-hours event, an area, (e.g. a conference venue), must be set to free access, and the associated Alarm Zone disarmed for the duration of the event. It may also require switching lights or air-conditioning on for the duration of the event, and it is not convenient to have an operator on-site to perform these overrides at the required time.

For some sites, some pre-programmed overrides may be a repeating event, (e.g. a class held every Tuesday evening for 10 weeks).

Macros reside on and run from the server. If the server goes offline at the time a macro is scheduled to run, the macro will only run if the server comes back online within one minute of the scheduled run time. If it is not run, when the server comes back online an event will be generated.

Macro List Window

The **Macro** List Window opens in grid view.



Notes:

- The Macros in this window are initially sorted by the **Next Run Time** column, with the earliest time first, and "Not Scheduled" Macros last.
- The **Next Run Time** column displays the next scheduled run time for a Macro. If a Macro has no scheduled times in the future, "Not Scheduled" displays instead.
- The **Remaining** column lists the total number of times the Macro is scheduled to run.

Creating a new Macro

Introduction

This procedure details how to create a new macro in Command Centre. To perform this procedure operators need the following operator privileges:

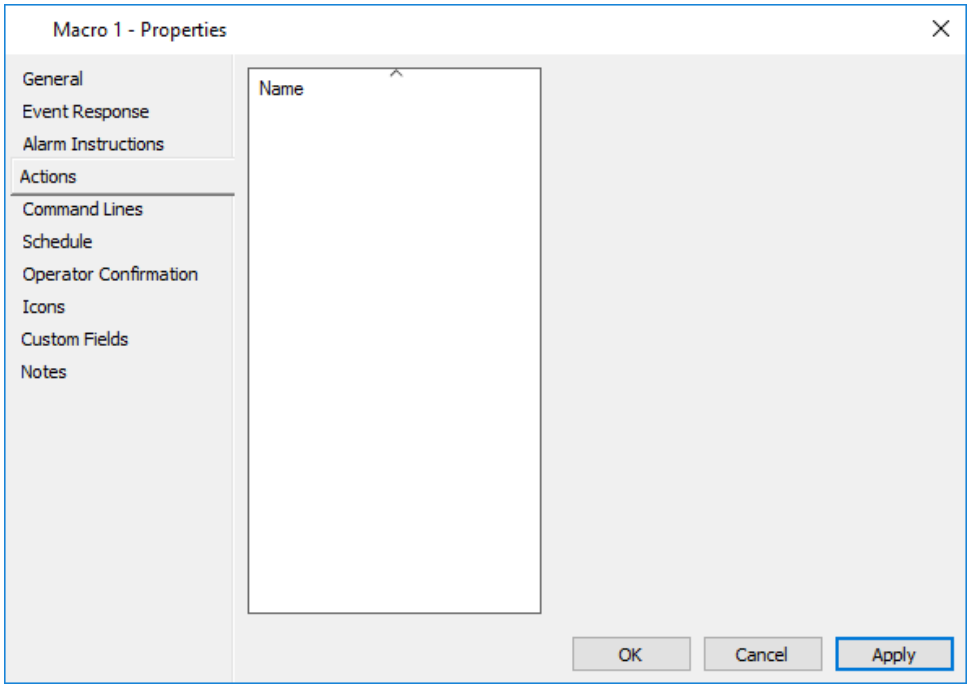
- The "Edit Macros" privilege within a macro's division.
- To be able to configure the actions for the item(s) you have included, you also require another privilege, as indicated below:

For...	you also require the...
Outputs, Access Zones and Interlock Groups	"Override" privilege
Alarm Zones	"Override" privilege, and the "Bulk Process Alarms" privilege if you intend selecting an Alarm Processing option
Logic Blocks	"Maintenance Override" privilege
Doors	"Override - Open Door" privilege
Bulk Changes	"Bulk Change" privilege
Guard Tours	"Manage Guard Tours" privilege
Controllers	"Configure Site" and "View Site" privilege
Exception Reports	"View Events and Alarms" OR "View Site" privilege
Cardholder Reports	“View Cardholders” and “Edit Report Descriptions” privilege
Activity and Guard Tour Reports	"View Events and Alarms" privilege
Evacuation Reports	"Edit Evacuation Report" privilege
Workstations	"Disable Workstation" or "Enable Workstation" privilege, depending on which override action you configure.

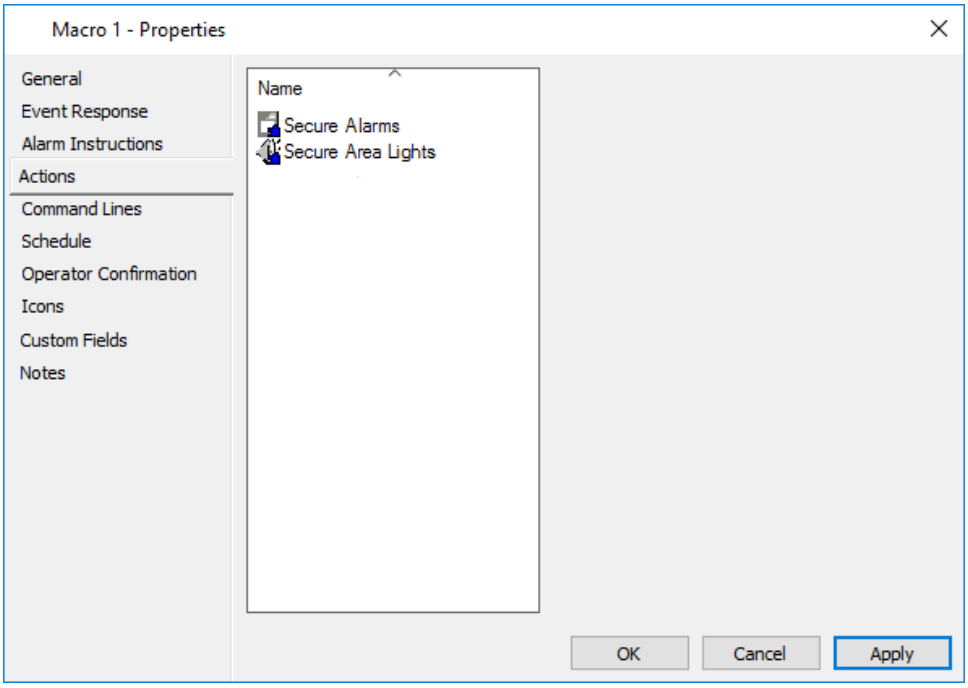
Procedure

1. Click **Configure** from the menu bar, then **Macros**.
   The **Macro** List Window opens (in grid view).
2. **Right click** and select **New...Macro**.
   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 **Actions** tab.

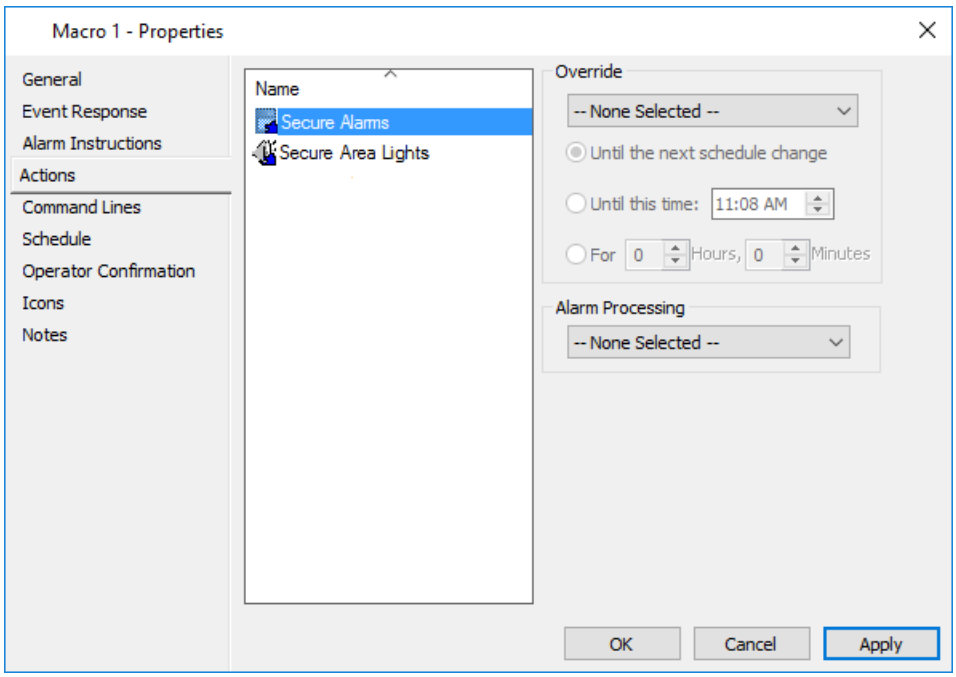


7. Drag and drop the Command Centre items you want to perform actions on for this macro into the **Name** grid.
   Note: Only Command Centre items that can be supported by macros, and to which you have the correct privilege(s), can be dragged into this field, (i.e. Outputs, Access Zones, Alarm Zones, Interlock Groups, Logic Blocks, Doors, Broadcast Notifications, Bulk Changes, Guard Tours, Controllers, Fence Zones, Macros, Morpho Biometric Readers, Workstations, Evacuation Reports, Exception Reports, Activity Reports, Guard Tour Reports and Cardholder Reports).



These Command Centre items need to have actions configured for them.
Note: Right clicking on an item in the **Name** grid displays a context menu. This allows you to view the items Properties or you can remove the item by selecting **Remove from List**.

8. Select the first item in the list.
The pane to the right of the **Name** grid populates, and changes to reflect the currently configured action for that item.

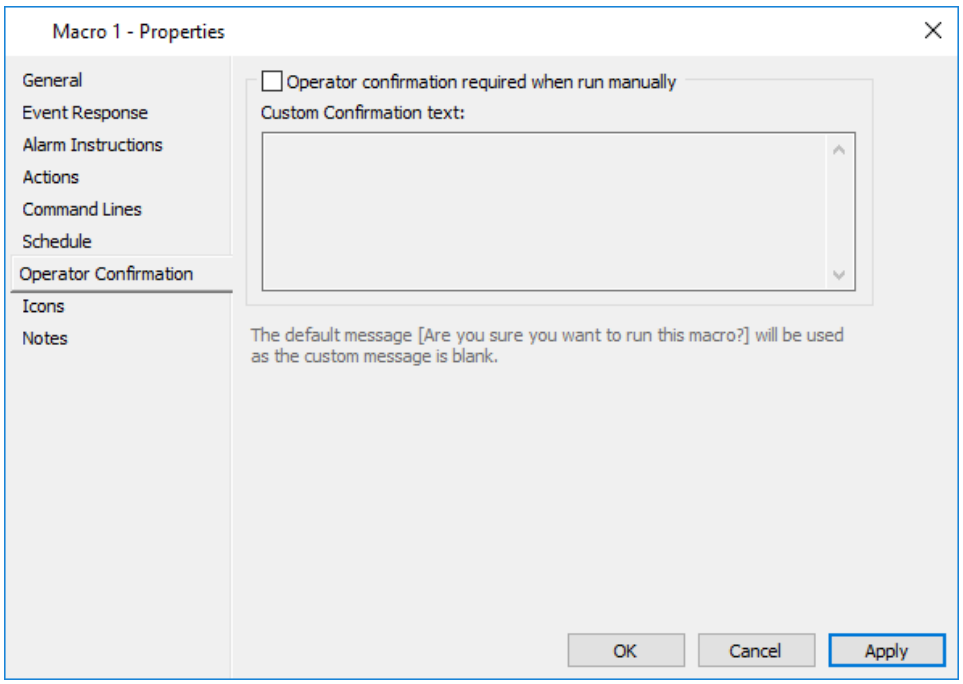


Notes:

- Some items only support one action, (e.g. for doors you can "Open Door", for bulk changes you can "Run Bulk Change", and for Controllers you can "Re-sync Databases"). However, for items that support more than one action, (e.g. items supporting override actions), then the default action is "None Selected".
- For Alarm Zones, the **Alarm Processing** drop-down list (as shown on the above screen) only displays if you have the "Bulk Process Alarms" privilege. By selecting "Acknowledge All" or "Process All", all existing alarms for the Alarm Zone will be acknowledged or processed, respectively. By selecting "Auto-Acknowledge All", all subsequent alarms for the zone will be auto-acknowledged, up until the point where all alarms on the zone have been processed.
IMPORTANT: These options bypass both mandatory alarm notes and the option to disalllow an operator from processing escalated alarms.
- For Evacuation, Exception, Activity, Cardholder and Guard Tour Reports the settings that have been saved for the report display. These settings can be changed (if you have the operator privilege to edit the report in the report's Division), by right clicking on the Report in the **Name** grid and selecting **Properties**.
- For Exception, Activity, Cardholder and Guard Tour Reports, you need

to select the report in the **Name** grid in order for its Division to be selected automatically.

9. Click the **Override** field and select the appropriate status from the drop-down list.
   Notes:
   - If you do not configure actions for each of the items, or leave --None Selected-- in the **Override** field, the following message will display when you try to save the macro:
     "One or more action items have no actions configured."
   - The actions available from the **Override** drop-down list are identical to the overrides available via the **Status and Overrides** tab on the Properties for each Command Centre item.
   - Where an override is initiated from a macro the new override takes precedence over, (i.e. replaces) any existing override for that item.
   - Multiple overrides can be selected for items that support multiple simultaneous overrides, (e.g. Access Zones - the access mode can be overridden, Anti-passback forgive can be applied, the Zone Count can be set and the Access Zone can be overridden to "Lockdown" or "Cancel Lockdown").
10. Click the **Schedule** tab if you want to schedule the macro now.
    See ***Scheduling a Macro*** (on page 20-7) for a detailed procedure.
    Note: To be able to schedule a macro you need the "Schedule & Run Macros" operator privilege.
11. Click the **Operator Confirmation** tab if you want operators to be presented with a confirmation dialog prompt before the macro runs.
    Note: Confirmation dialogs only display when macros are manually-triggered by an operator.



12. Check the **Operator confirmation required when run manually** checkbox. The "Confirmation text" field is enabled.
13. Alter the confirmation text if you want something different from the default, (i.e. "Are you sure you want to run this macro?"), to appear on the confirmation dialog.
    Note:
    This field is limited to 200 characters, and while multiple lines are allowed, new lines take up two characters.
14. Click the **Icons** tab if you want to change the Icon Set for this macro.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
15. Click the **Notes** tab if you want to add a note(s) about this macro.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
16. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

A new macro has been created to perform a number of actions quickly with minimal operator interaction. This macro can now be placed on a Site Plan for future execution if required. See ***Placing a Macro on a Site Plan*** (on page 20-17) for the procedure.

Note:
If **OK** or **Apply** is clicked and the macro contains items and actions that you do not have sufficient privileges to save, then an error message will display informing you of the disallowed items, and the changes will not be saved.

Hint

Deleting Macros
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete a Macro.
Note: A macro cannot be deleted if it is on a Site Plan or is used in an Action Plan. Likewise, operators, workstations and site items that appear on a macro's **Schedule** or **Actions** tabs cannot be deleted from the system.

Scheduling a Macro

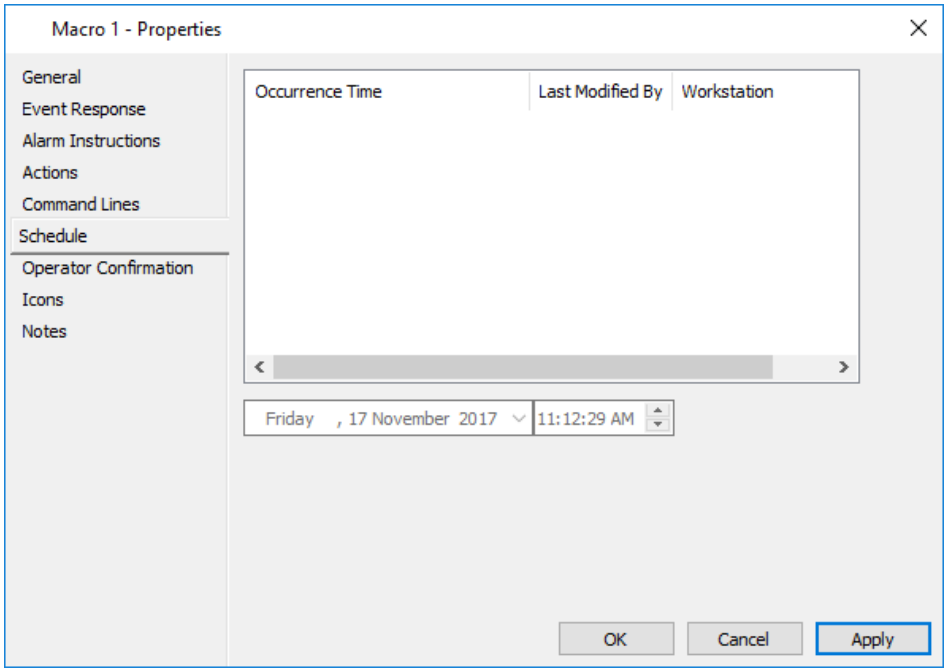
Introduction

To be able to schedule macros requires the "Schedule & Run Macros" operator privilege (a separate privilege from running a macro), because the ability to schedule macros means an operator could potentially unlock secure areas after hours, allowing unauthorised people access.

This procedure details how to schedule the date and time for a macro to run.

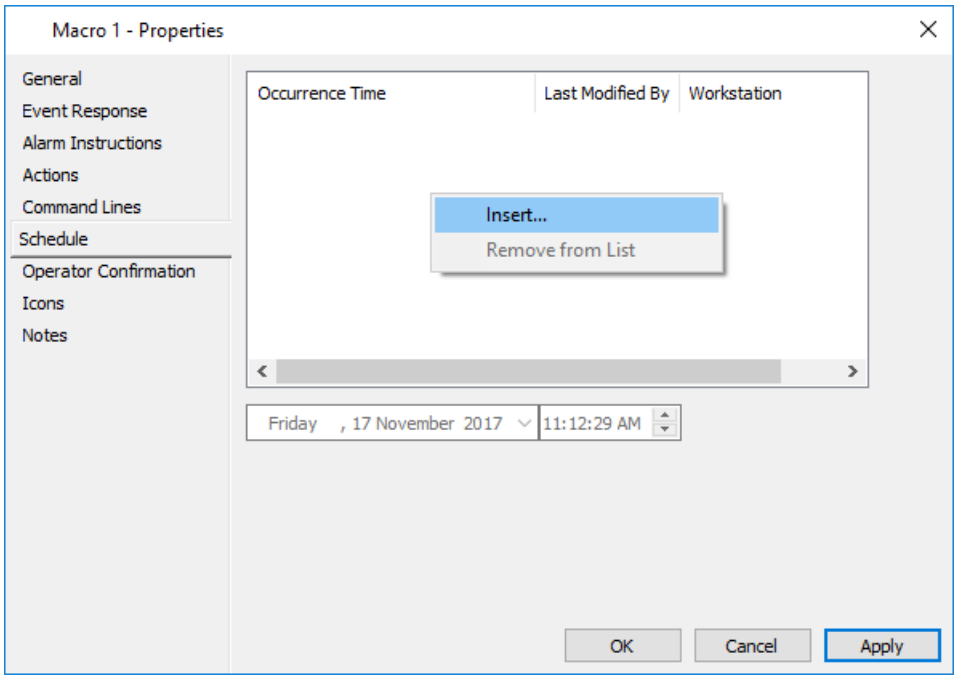
Procedure

1. Click **Configure** from the menu bar, then **Macros**.
   The **Macro** List Window opens (in grid view).
2. Highlight the macro you want to schedule.
3. **Right click** the mouse button, and select **Properties**.
4. Click the **Schedule** tab.

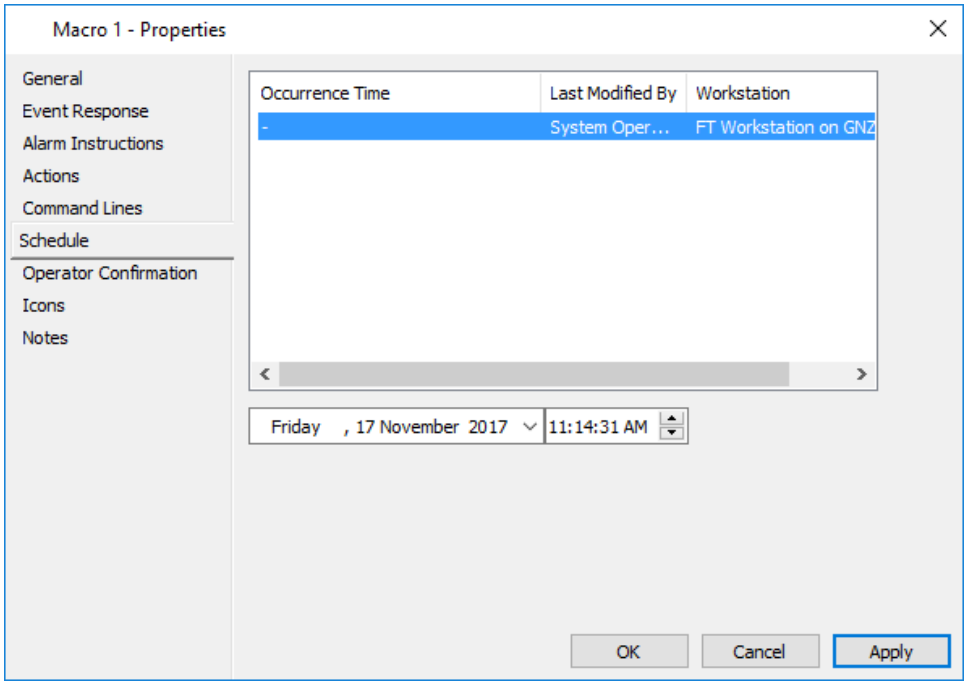


Note: If this macro was configured in the Command Centre Client with a schedule, rather than the Configuration Client, the grid (shown in the above screen shot) will not display. Instead, it will be replaced with the following message:
"Macro is on a repeating schedule and should be configured in Command Centre."

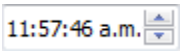
5. **Right click** anywhere with the grid, (i.e. on a column header, on the scroll bar or in the blank area), and select **Insert**.



A new entry is added to the grid and highlighted. This entry includes your name in the "Last Modified By" column and your workstation in the "Workstation" column.
The Date and Time controls are enabled, and display the current date and time.



6. Do you want the macro to run today?
   If **yes**, go to Step 7. When you select the time, today's date will automatically default into the Occurrence Time column.
   If **no**, click the date drop-down list and select the date you want the macro to run, from the calendar displayed.
   Note: Dates and times in the past cannot be selected.

7. Alter the Time Box  to the time you want the macro to run.
   The date and time display in the Occurrence Time column.
8. If you require this macro to run on other dates/times, repeat Steps 6 and 7 as necessary.
   Note:
   There is no limit to the number of times a macro can be scheduled to run.
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 macro has been scheduled. The **Macro** List Window displays the next scheduled run time and the number of future run times for this macro.
Note:
Once a scheduled run time is reached and the macro is run, the entry is removed from the list on the **Schedule** tab.

Editing/Removing Actions for a Macro

Introduction

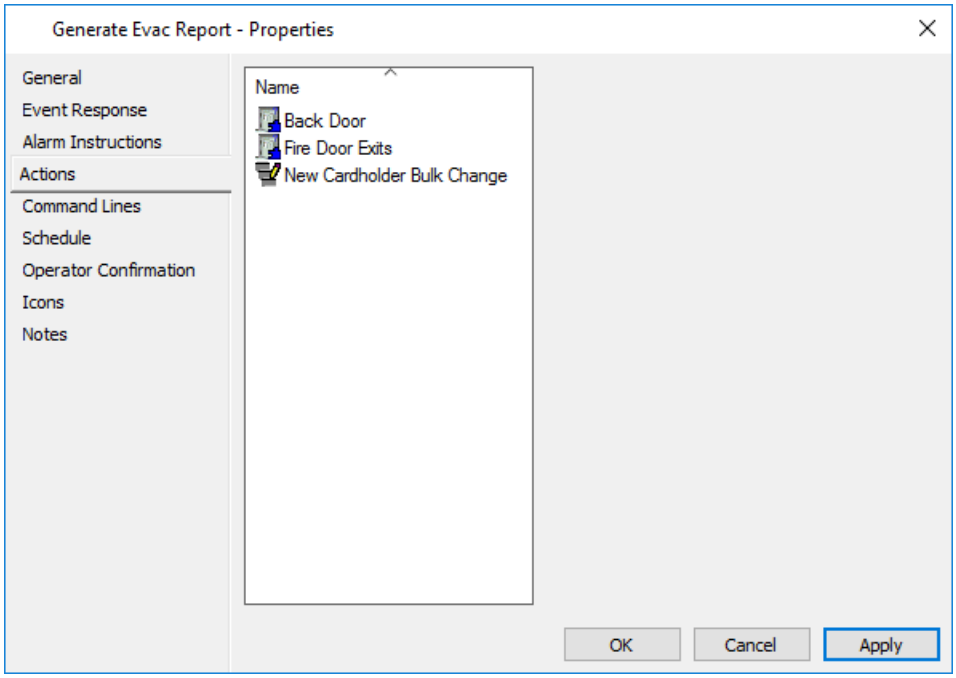
This procedure details how to edit or remove 'Actions' for a macro. To perform this procedure operator's need the following operator privileges:

- The "Edit Macros" privilege within a macro's division.
- To be able to edit or remove the actions for the item(s) you have included, you also require another privilege, as indicated below:

For...	you also require the...
Outputs, Access Zones, Alarm Zones and Interlock Groups	"Override" privilege
Logic Blocks	"Maintenance Override" privilege
Doors	"Override - Open Door" privilege
Bulk Changes	"Bulk Change" privilege
Guard Tours	"Manage Guard Tours" privilege
Controllers	"Configure Site" and "View Site" privilege
Exception Reports	"View Events and Alarms" OR "View Site" privilege
Cardholder Reports	“View Cardholders” and “Edit Report Descriptions” privilege
Activity and Guard Tour Reports	"View Events and Alarms" privilege
Evacuation Reports	"Edit Evacuation Report" privilege

Procedure

1. Click **Configure** from the menu bar, then **Macros**.
   The **Macro** List Window opens (in grid view).
2. Highlight the macro you want to edit.
3. **Right click** the mouse button, and select **Properties**.
4. Click the **Actions** tab.
   Note:
   The grid on this tab will be disabled if you do not have the correct operator privilege for any one of the Actions listed, (as shown below). If this occurs, you will not be able to edit or remove anything from this tab.



5. Do you want to edit or remove an Action?

If...	then...
edit	select the item in the list. The pane to the right populates with the currently configured override action for that item. Edit the override action as appropriate.
remove	**right click** on the item and select **Remove from List**.

6. Repeat Step 5 if there are other Actions you want to edit or remove.
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

The appropriate Action(s) have been edited or removed for the macro.

Editing/Removing Scheduled run times for a Macro

Introduction

This procedure details how to change or remove the date and/or time a macro is scheduled to run. To perform this procedure you need the "Schedule & Run Macros" operator privilege.

Procedure

1. Click **Configure** from the menu bar, then **Macros**.
   The **Macro** List Window opens (in grid view).
2. Highlight the macro you want to edit or remove.
3. **Right click** the mouse button, and select **Properties**.
4. Click the **Schedule** tab.
5. Do you want to edit or remove a scheduled run

time?**If...**	**then...**
edit	select the "Occurrence Time", and edit the date and/or time from the Date drop-down box and/or Time Box as appropriate.
remove	**right click** on the "Occurrence Time" and select **Remove from List**.

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

Result

The scheduled run time has either been changed or removed from the macro. If the run time was changed, the operator's name in the "Last Modified By" field would also be changed to the current operator's name.

Adding Command Lines for Macros

Introduction

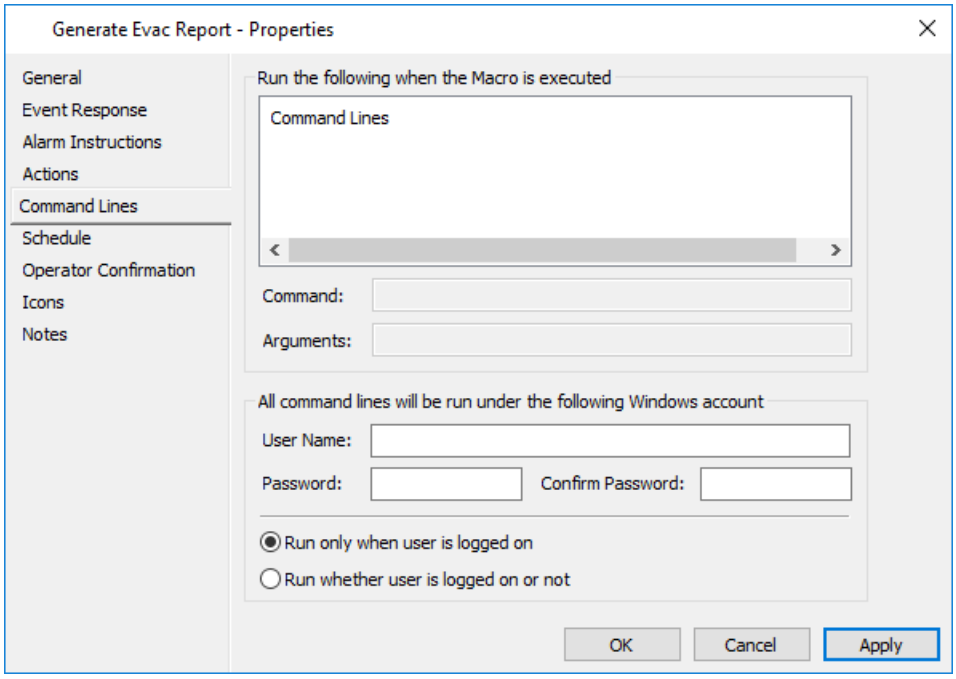
A macro can be configured to execute a user-specified command line action at the Command Centre Server, when the macro is run, (e.g. emailing a person a specific message on receipt of an event in Command Centre, or running an application that closes down specific workstations). Multiple command line entries can be added to a single macro, and other items and actions that macros currently perform can also be added to the same macro.

This procedure allows you to add a command line to a macro.
Notes:

- The **Command Lines** property page does not display for a CAPSS site, (i.e. when `NPSA=1` appears in the licence file Features section). Command line macros cannot be run for such sites.
- You need to know a valid logon name and password for the Server PC to be able to run command lines.

Procedure

1. Click **Configure** from the menu bar, then **Macros**.
   The **Macro** List Window opens (in grid view).
2. Highlight the macro you want to add Command Line(s) to.
3. **Right click** the mouse button, and select **Properties**.
   By default the **General** tab displays.
4. Click the **Command Lines** tab.



5. **Right click** anywhere within the Command Line grid and select **Insert**. The lower fields of this screen are enabled and cleared of any previous content, and a new entry is added to the Command Line list.

   Note: There is no limit to the number of command lines that can be added to the Command Line grid.

6. Complete the fields as appropriate:

Field	Description
Command	Specify the executable or batch file to initiate when the macro is run. The application or file specified does not have to be limited within Command Centre, (i.e. any file name or extension is acceptable). The command line can, optionally, include up to 300 characters free text entry, used to specify the parameters associated with the file to be run from the command line. The free text entry can include ASCII characters, (e.g. #, % and /). These parameters, if configured, are passed to the command line, in addition to the file that is called when the macro is run. (Maximum length = 260 characters)
Arguments	Specify the additional command line arguments that are passed to the executable. (Maximum length = 300 characters)
User Name	To configure a command line with a domain account, you must prefix the 'User Name' with the domain name plus a slash character, (e.g. Gallagher 1\FTUser). (Maximum length = 280 characters)
Password and Confirm Password	The password for the Windows User Account must be typed in both the 'Password' and the 'Confirm Password' fields. The password will not be made visible during configuration or when the macro properties are viewed. (Maximum length = 260 characters)

Note:
The Windows user account specified on the 'Command Lines' tab of the Macro requires the ‘Replace a process level token’ Local Security Policy. It also requires *one* of the following two policies:

- 'Allow log on locally'
  This allows interactive access, and any program run from a macro (from another workstation) will show running actively on the server monitor.

- 'Log on as a batch'
  This allows the program to execute in the background on the server (need to view through Task Manager).

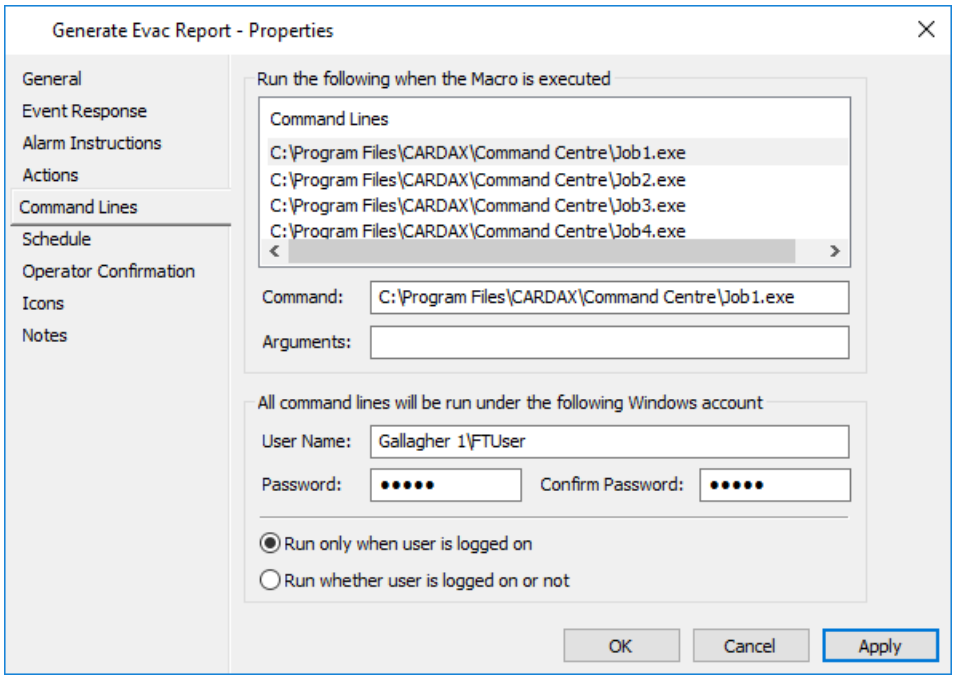
  OR

- NOT be "denied access from the network" as this will stop an executable running if the user doesn't also have the "Allow log on locally" privilege.

To assign a user to a policy, go to **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Local Policies** > **User Rights Assignment**. Open a policy and assign the required user on the 'Local Security Setting' tab.

7. Click the appropriate radio button for how you want the command lines to be executed.

Option	Description
Run only when the user is logged on	This option will only run the command lines if you are actively logged into Windows when the macro executes. If a command line has a GUI component it will be visible. **Note:** This option only works if the Command Centre service is running as “Local System”.
Run whether user is logged on or not	This option runs the command lines regardless of whether you are logged into Windows, but all commands will be run in the background, (i.e. any GUI component in a command will not be visible).



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 macro has been configured to execute a user-specified command line(s) when the macro is run.

Note: When macros with command line(s) are run, problems may occur if there are 32 user accounts on the server that are used to run separate macros. This is due to a restriction in your operating system.

Hint

Editing Command Lines
Only one Command Line entry can be edited at once. Therefore, if none of the Command Line entries are selected, or multiple entries are selected, the **Command** and **Arguments** fields are disabled.

You must re-enter the account password to log onto the Server's operating system. If you do not re-enter the account password you will be prevented from saving any changes to the Command Line configuration.

Removing Command Lines
Command Line entries can be removed by right clicking on the entry you want to remove, and then selecting **Remove from List**.

Local Policies
If you are running 'FT Command Centre Service' as a specific user, apply that user to "Replace a process level token" (via **Control Panel** > **Administrative Tools** > **Local Security Policy** > **User Rights Assignment**), to allow you to run all Macros that require local system or Network service privileges.

Missing or inaccessible target file
If the Macro fails to execute due to a missing or inaccessible target file, try creating a batch file that runs the target file, and then command the Macro to run that batch file.

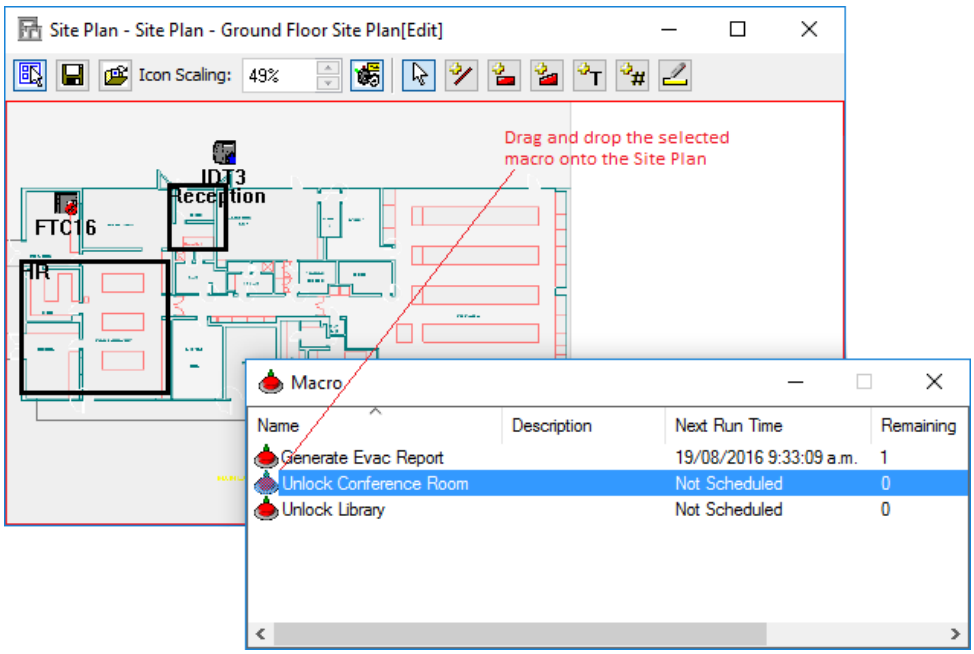
Placing a Macro on a Site Plan

Introduction

Macros can be placed on to Site Plans for future execution.

Procedure

1. Open the **Site Plan** window, and **right click** on the appropriate Site Plan.
2. From the displayed pop-up menu, select **Edit**.
   The Site Plan opens in "Edit" mode.
3. Click **Configure** from the menu bar, then **Macros**.
   The **Macro** List Window opens.
4. Select the macro you want to place on a Site Plan.
   Drag and drop it onto the Site Plan.



Result

The macro has been placed onto a Site Plan for running at any given time. See ***Running a Macro*** (on page 20-18) for details.

Running a Macro

Introduction

While macros can be scheduled to run at specific dates/times, an operator can run a macro at any given time.
Operators need the "Run Macros" or "Schedule & Run Macros" operator privilege within a division in order to run a macro in that division.

Procedure

Running Macros from Site Plans or Status Viewer

On the Site Plan or Status Viewer, either:

- **Right click** on the macro icon  and select **Run Macro**.

  Or:

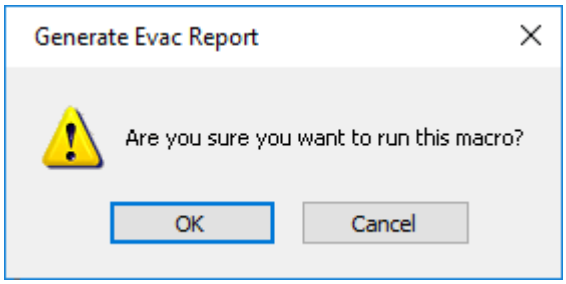
- **Double click** the macro icon .

Running Macros from the Context Menu

1. Click **Configure** from the menu bar, then **Macros**. The **Macro** List Window opens.
2. Highlight the macro you want to run.
3. **Right click** the mouse button, and select **Run Macro**.

Result

If the macro has the "Operator confirmation required when run manually" option selected (on the **Operator Confirmation** tab of the Macro's properties), then the following dialog will display:



Note: This screen shot shows the "default" message. However, the message may differ if a different message has been specified on the **Operator Confirmation** tab of the Macro's properties.

Click the **Yes** button.

The Macro icon changes image for several seconds  as an indication the macro has run.

Notes:

- Regardless of which method an operator uses to run a macro, an "Operator Ran Macro" event will be generated.
- When a macro runs it is possible that some of its actions cannot be carried out, (e.g. when a macro is set-up a relay may support pulse overrides, however when the macro runs this could have been changed). In such cases, if the macro was run (from a schedule or by an operator), then an event is generated indicating which item(s) and action(s) could not be carried out.
- If the server goes offline at the time a macro is scheduled to run, the macro will only run if the server comes back online within one minute of the scheduled run time. If it is not run, when the server comes back online an event will be generated.

Duplicating a Macro

Introduction

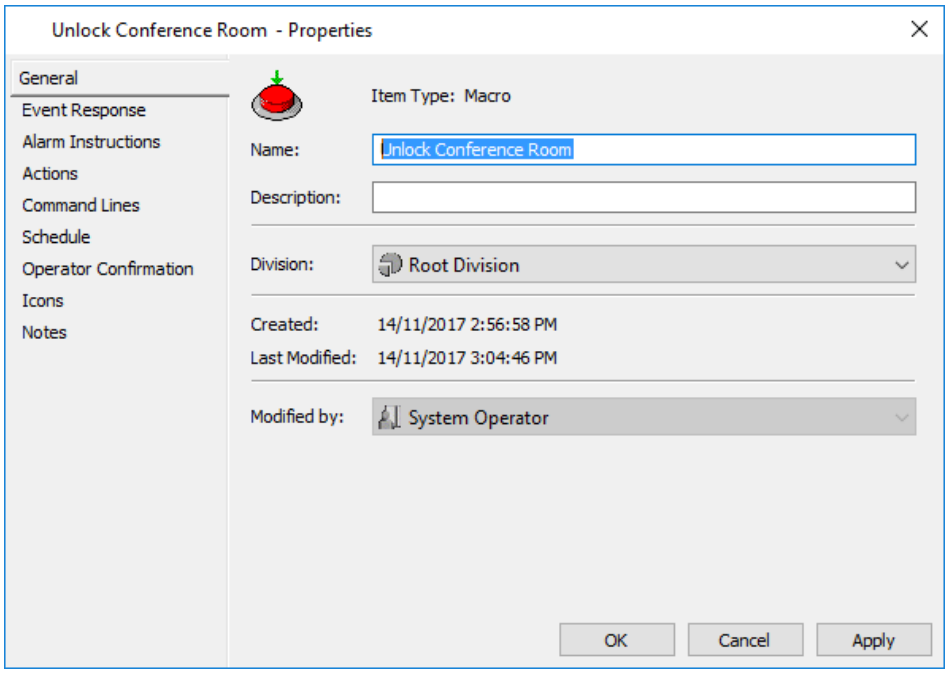
This procedure describes how to duplicate (copy) the content of an existing macro, so a new macro is created within the same division as the copied macro.

To perform this procedure operator's need the "Edit Macros" operator privilege, and the appropriate privilege(s) for the item(s) included in the **Actions** tab, as follows:

For...	you also require the...
Outputs, Access Zones, Alarm Zones and Interlock Groups	"Override" privilege
Logic Blocks	"Maintenance Override" privilege
Doors	"Override - Open Door" privilege
Bulk Changes	"Bulk Change" privilege
Controllers	"Configure Site" and "View Site" privilege
Guard Tours	"Manage Guard Tours" privilege

Procedure

1. Click **Configure** from the menu bar, then **Macros**.
   The **Macro** List Window opens (in grid view).
2. Highlight the macro you want to duplicate.
3. **Right click** the mouse button, and select **Duplicate...**
   The properties display for a new macro.



The information on the **Action** tab is copied, but the information on the **Schedule** tab is not. All information on the **Command Lines** tab is copied with the exception of the Account Password if one is configured for a command line.
Note:
The name of the existing macro that you copied displays in the 'Name' field.

4. Change the name of the macro as appropriate, and division if necessary.
   Note:
   Each macro must have a unique name, so if you attempt to save the macro without changing the name, the following message will display: *"The name '<macro name>' is already used for an existing macro."*
5. Click the **Command Lines** tab, and make any changes as necessary.
6. Click the **Schedule** tab if you want to schedule the macro now.
   See ***Scheduling a Macro*** (on page 20-7) for a detailed procedure. **Note:** To be able to schedule a macro you need the "Schedule & Run Macros" operator privilege.
7. Click the **Icons** tab if you want to change the Icon Set for this macro. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
8. Click the **Notes** tab if you want to add a note(s) about this macro.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).

Result

The selected macro is duplicated.

Chapter 21: Hardware

After all the equipment is physically installed on site you need to configure Command Centre to match.

You can add the devices (via the **Hardware** List Window), in any order. However, it is important you link them together to accurately represent your site.

Note: It is important that any System Divisions are formalised **prior** to the commencement of configuration work. See System Divisions for procedure.

You must have the correct operator privilege level to configure Gallagher FT Hardware. Refer to Operator Privileges.

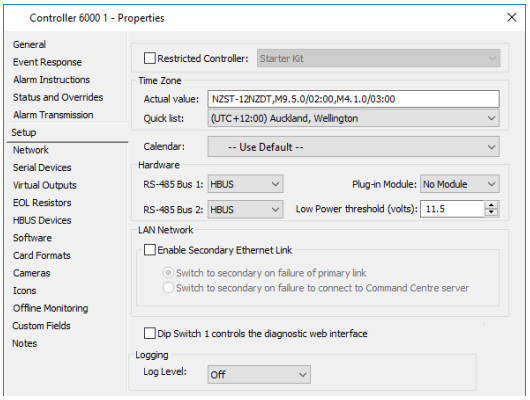
This topic includes the following procedures:

- ***Creating Controller 7000s or 6000s*** (on page 21-2)
- ***Creating a Controller 7000 Single Door*** (on page 21-9)
- ***OneLink Configuration*** (on page 21-18)
- ***Configuring Secondary Ethernet operation mode*** (on page 21-20)
- ***Configuring a Controller 7000 or 7000 Single Door for 802.1x*** (on page 21-22)
- ***Adding new or renewing existing certificates to Controllers using 802.1x*** (on page 21-25)
- ***Upgrading a Controller 6000 to a Controller 7000*** (on page 21-27)
  - ***Configuring DNS Servers for Controllers*** (on page 21-31)
  - ***Server Address*** (on page 21-32)
  - ***Configuring Offline Monitoring*** (on page 21-33)
  - ***Configuring a Controller for DHCP*** (on page 21-35)
  - ***Enabling DHCP for a new Controller using the wizard*** (on page 21-37)
  - ***Configurable Ports - NAT Solution*** (on page 21-40)
- ***Creating Devices*** (on page 21-45)
- ***Assigning Device Software to devices*** (on page 21-45)
- ***Configuring EOL Resistors for devices*** (on page 21-46)
- ***Linking devices to Controllers*** (on page 21-48)
- ***Creating Inputs and Outputs*** (on page 21-50)
- ***Linking Inputs and Outputs to devices*** (on page 21-56)
- ***Creating Readers*** (on page 21-57)
- ***Configuring HBUS Devices*** (on page 21-65)
- ***Configuring an HBUS Keypad Reader*** (on page 21-68)
- ***Configuring HBUS Terminals*** (on page 21-74)
- ***Configuring an HBUS Contact Card Reader*** (on page 21-109)
- ***Configuring an HBUS I/O Interface*** (on page 21-127)
- ***Configuring an HBUS QuickSwitch Board*** (on page 21-132)

Creating Controller 7000s or 6000s

Controller 7000s and 6000s are the central field controller for the Command Centre system. They are a processing board for an intruder alarm and access control system. All variants of the Controller 7000 and 6000 can operate on their own, or can have an optional Reader Module connected.

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Controllers** and the appropriate Controller type, (i.e. **Controller 7000** or **Controller 6000**). 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. If this Controller is not mounted in a cabinet or, if the cabinet door opens, continuous tamper alarms will be generated. To prevent this from happening, select the **Status and Overrides** tab and select the **Disable Front Tamper** and/or **Disable Rear Tamper** check box/s.
   Note: The Controller 6000 and 7000 have a **Disable Front Tamper** and a **Disable Rear Tamper** checkbox so the tampers can be enabled/disabled independently.
6. Click the **Setup** tab.



7. If the Controller is a Starter Kit Controller or 2-Door Controller, check the **Restricted Controller** check box and select the Controller type from the drop-down list. **Notes:**
   - Both Controller 6000 Starter Kit and 2-Door are not compatible with versions of Command Centre earlier than vEL7.30
     Both Controller 7000 Starter Kit and 2-Door are only supported from the following Command Centre versions onward:
     - vEL9.00 MR7, - vEL9.10 MR6, - vEL9.20 MR3,
     - vEL9.30 MR1, and - vEL9.40
   - It is not possible to assign more than 2 Doors to a 2-Door Controller.
   - Starter Kit Controllers must be configured as Starter Kit Controllers. 2-Door Controllers must be configured as 2-Door Controllers. Failure to do so will result in an *'Controller with wrong type created'* alarm being generated. The Controller will stop accepting messages from the

Controller Service resulting in *'Part not found problems'*.

- Any Standard, High Spec or PIV High Spec Controller will work normally (even if configured as a Starter Kit Controller or 2-Door Controller), assuming your licence and door limits are not breached.
- Once saved, the **Restricted Controller** type cannot be changed.
- Command Centre must be licensed to use a Starter Kit Controller. Command Centre is limited to communicating with one Starter Kit Controller per system.

8. The **Time Zone** section of the screen is automatically populated with the same time zone the Command Centre Server is in. If you require another city/time zone, you can select one from the drop-down **Quick list**, and the POSIX time zone string in the **Actual value** field will be updated.
   Note: If you change the time zone the Controller will restart when you **Apply** your change. The formatting rules for time zone strings are as follows:

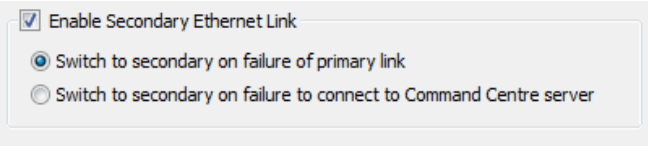
   Time Zone string format is:
   {STDName}{Offset}[{DSTName}{Offset},{Start rule},{End rule}]
   Offsets are in Americocentric form, (i.e. multiplied by -1 in order to make US timezones positive).
   The Start and End rules can be omitted if there is no daylight saving. The rules can be written in one of the following three formats:
   - **Jn** - where n = {1-365} (Day of year, but Feb 29 never counted)
   - **n** - where n = {0-365} (Day of year)
   - **Mm.w.d** - where m=month {1-12}, w=week of month {1-5} (5=last), d=day of week {0(Sun)-6(Sat)}

   These can be followed by an optional changeover time in format:
   /hh[:mm[:ss]] - default is 2:00:00.
   If the daylight savings offset is omitted, then one hour more than the standard offset is assumed.
   Example: New Zealand's timezone string is: NZST-12NZDT,M10.1.0,M3.3.0, which means New Zealand is 12 hours ahead of GMT, our daylight savings (of one hour) starts on the first Sunday of October and finishes on the third Sunday of March, both at the default time of 2am.

9. The **Calendar** drop-down list contains a list of all the special calendars configured in the system for the operator's division. One special calendar may be assigned to each Controller in the system.
   By default, no special calendar will be assigned to the Controller. However, if you require one to be assigned, select the appropriate special calendar from the drop-down list. This Controller will use both the special calendar selected as well as the default calendar for its scheduling operations. The default calendar provides cycle and special day assignments, while the special calendar provides special day assignments only, with the possibility of overriding special day settings from the default calendar.
   Note: Refer to Creating a Special Calendar for further detail about special calendars.
10. The **Hardware** section allows you to:
    - alter the HBUS, Aperio, OSDP, Schlage and Sensor devices used as required, and/or

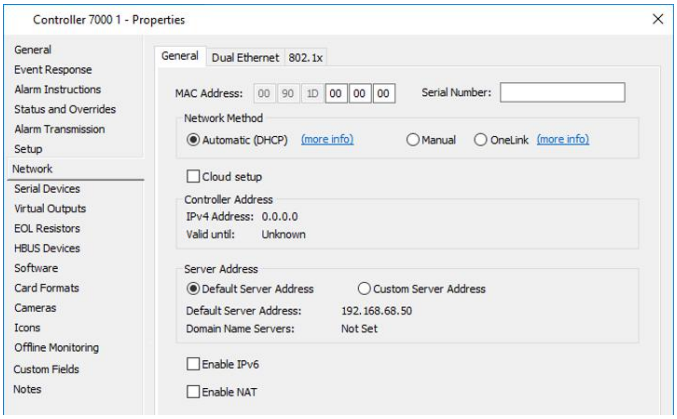
- alter the type of reader board (plug-in module) to be configured. For further explanation see ***Linking devices to Controllers*** (on page 21-48).

11. For a Controller 6000, the **Enable Secondary Ethernet Link** checkbox provides the option to switch to the secondary ethernet link either on failure of the primary link or on failure to connect to the Command Centre server.



When checked, the secondary ethernet link on the Controller is enabled if one is present, otherwise it has no affect.

12. The **DipSwitch 1 controls the diagnostic web interface** checkbox should be ticked if requested by Gallagher Technical Support. Otherwise, leave this option unticked.
Important: If Dip Switch 1 is to be used to control the diagnostic web interface, Dip Switch 1 needs to be physically 'ON' on the Controller as well as this checkbox being enabled.
13. The **Logging** section allows you to configure the verbosity of diagnostic logs from this Controller which are written into the Command Centre log file. The log level can be changed to a value from **Off**, (i.e. least verbose) to **Trace**, (i.e. most verbose).
14. Click the **Network** tab.

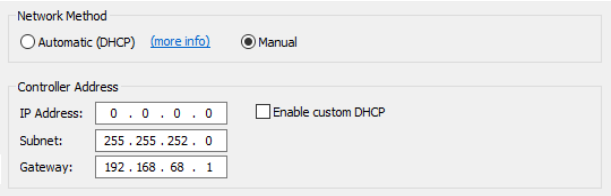


Note: The screenshot above is for the **Network** tab of the Controller 7000. The differences from the Controller 6000 are:

- there is an additional **OneLink** option in the 'Network Method' section on the Controller 7000. OneLink utilises Gallagher Cloud Services to enable Controller 7000s to connect to the on-premises Command Centre Server over the internet. It does not appear for Controller 6000s as they do not support OneLink connection. See ***OneLink Configuration*** (on page 21-18) for further instructions.
- Controller 6000 properties only have the **General** sub-tab, whereas Controller 7000s have two additional sub-tabs:
  - The **Dual Ethernet** sub-tab includes configuration options for a secondary ethernet adapter. See ***Configuring Secondary Ethernet operation mode*** (on page 21-20) for further instructions.

- The **802.1x** sub-tab enables sites to configure Controller 7000s for 802.1x. See ***Configuring a Controller 7000 or 7000 Single Door for 802.1x*** (on page 21-22) for further instructions.

15. Enter the **MAC Address** for the Controller.
    The MAC Address for each Controller is stuck to the actual Controller PCB.
    Note: A MAC address range is included in your license file and will be checked against when a MAC address is saved here. If you receive a "MAC address out of range" error message, check your license file to see what range is valid.
16. Entering the Serial Number of the Controller is optional and can be found printed on one of the Controller labels.
17. Click the radio button for the appropriate **Network Method**, i.e. either **Automatic (DHCP)** or **Manual**.
    Automatic (DHCP) is the preferred method, but if you select **Manual** the **Controller Address** section changes as shown below:

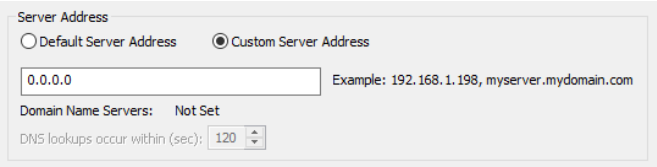


18. Enter the **IP Address**, (i.e. TCP-IP Address), **Subnet** and **Gateway** information for the Controller. This information will be provided by the IT Department for the organisation, or the IT provider of the network.
    Note: By default, the **Subnet** and **Gateway** fields are populated with the first subnet mask and gateway from one of the server's ethernet adaptors with a non-zero gateway.
    If there is no IT support for this site, and it is a localised and dedicated LAN built for Command Centre, there are some standards that you can apply to the configuration of the Controllers, as described next:

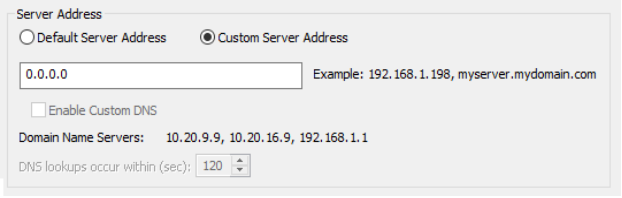
Parameter	Description
IP Address	The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of TCP-IP address space for private networks: Class A From 10.0.0.0 to 10.255.255.255 Class B From 172.16.0.0 to 172.31.255.255 Class C From 192.168.0.0 to 192.168.255.255 These TCP-IP addresses have been set aside specifically for use when it is not necessary (or desirable) for the attached devices to be available on the Internet. If one of these TCP-IP addresses were accidentally broadcast on the Internet they would be ignored by the routing firewall server and would cause no conflict issues. The first block is a single Class "A" network number, the second block is a set of 16 contiguous Class "B" network numbers, and the third block is a set of 256 contiguous Class "C" network numbers. **Notes:** • Each device, (i.e. Computer, Printer, Controller) on the localised LAN must have a unique TCP-IP address. Each address used must

Parameter	Description
	however be in the same Subnet Mask range. This means as an example, if you use the Class "B" TCP-IP address range, each TCP-IP address assigned to the localised LAN must start with 172.16 and then be unique, (e.g. 172.16.0.1, 172.16.0.2, 172.16.0.3, 172.16.0.4, etc.) • Command Centre or Command Centre 9.40 relaxes duplicate IP address restrictions to better support DHCP, NAT, and OneLink configurations. Controllers are no longer blocked from sharing IP addresses, and IP details are no longer cleared when duplicates are detected. Network IP uniqueness remains the responsibility of the site configuration.
Subnet	There are default Subnet Mask settings for the three class categories: Class A From 10.0.0.0 to 10.255.255.255 Default Subnet Mask is 255.0.0.0 Class B From 172.16.0.0 to 172.31.255.255 Default Subnet Mask is 255.255.0.0 Class C From 192.168.0.0 to 192.168.255.255 Default Subnet Mask is 255.255.255.0 Use the associated Subnet Mask appropriate for the TCP-IP class used. The Subnet Mask differentiates between the network and client parts of the TCP-IP address. The "255's" identify the network section and the "0's" identify the clients. For a Class "B" TCP-IP address the network identification numbers are "172.16" and will be identical for each TCP-IP address on that network. The following two numbers of the TCP-IP address uniquely identify each device on the network.
Gateway	Gateway settings when used in general LAN configurations provide a path to a different network environment. In a localised LAN environment for Gallagher there is no physical connection to a different network, so the Gateway setting is ineffective. On single Subnet networks, it is recommended the Gateway information be set exactly as the TCP-IP address used, or alternatively 0.0.0.0
Enable custom DHCP	This checkbox allows sites to use their own Dynamic Host Configuration Protocol (DHCP) service to assign IP addresses to their controllers automatically, without physically needing to be at the controller. See ***Configuring a Controller for DHCP*** (on page 21-35) for further detail.

19. Click the radio button for the appropriate **Server Address**, (i.e. either **Default Server Address** or **Custom Server Address**).
    If you selected **Automatic (DHCP)** for the "Network Method", and you select **Custom Server Address**, this section will change as shown below:



    If you selected **Manual** for the "Network Method", and you select **Custom Server Address**, this section will change as shown below:

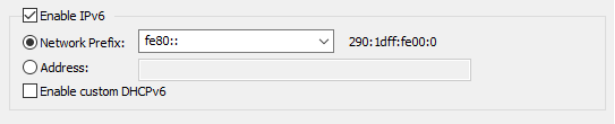


20. If this Controller is separated from the Server by a firewall, so it can still contact the Command Centre Server, enter the IP Address.
21. Controllers must be able to make use of Domain Name Servers (DNS) in disaster recovery situations, especially where backup servers reside on different subnets. See ***Configuring DNS Servers for Controllers*** (on page 21-19) for the procedure.
22. Controller 6000s and 7000s support both IPv4 and IPv6. A Controller that needs to communicate with IPv4 external systems must be assigned IPv4 addresses as per existing configuration procedures.

    To assign an IPv6 address additional to IPv4:

    a) The only supported method of address allocation for the Controller 6000 and 7000 is an auto configuration via router advertisements. The Controller will only accept IPv6 auto configuration if it is either already configured for IPv6 communication or the Controller was booted with DIP switch 2 on.

    b) Check the **Enable IPv6** checkbox. The **Enable IPv6** section changes as shown below if you selected **Manual** as the Network Method above:

    c) Click either the **Network Prefix** or **Address** radio button and enter appropriate details.

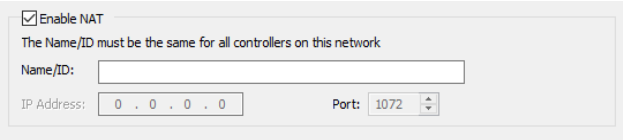
    - **Network Prefix** contains a pre-populated network prefix combo field containing all subnet prefixes available at the Command Centre server machine. The interface identifier of the Controller is pre-populated based on the entered MAC address.
    - The **Address** field is free text field to provide complete IPv6 address instead. The given address shall be from the list of IPv6 addresses assigned to the Controller through the auto-configuration process. Hostname is not supported here.

    To assign only an IPv6 address:

    - IPv4 address can be NULL in this case.
    - DIP switch 3 should be ON as well as DIP switch 2.
    - Reset is the same as above.

    Note: A document providing further technical information about IPv6 (**Gallagher Command Centre IPv6 Support.pdf**) is available in the `'Documentation'` directory of the Command Centre installation files.

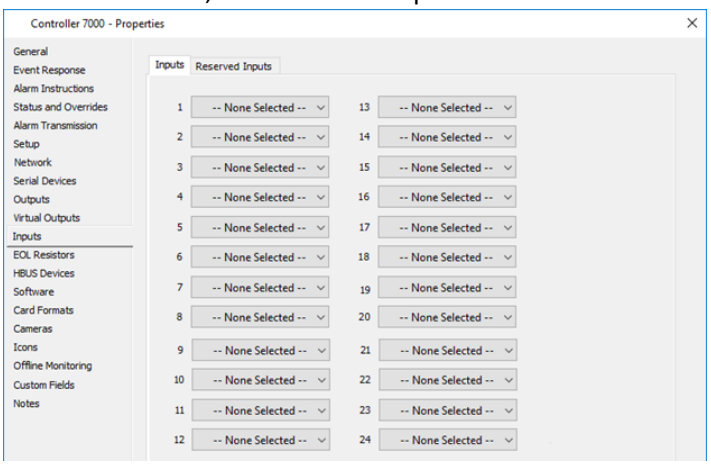
23. Click the **Enable NAT** checkbox if your site wants Command Centre to communicate with multiple Controllers on different networks.
    Selecting **Enable NAT** expands the section as shown next:



Refer to ***Configurable Ports - NAT Solution*** (on page 21-40) for further detail.

24. Click the **Inputs** tab if the Controller has a Plug-in Module connected. This tab allows you to link inputs to the Controller. The number of inputs available will depend on what was selected for the **Plug-in Module** (on the **Setup** tab), as follows:

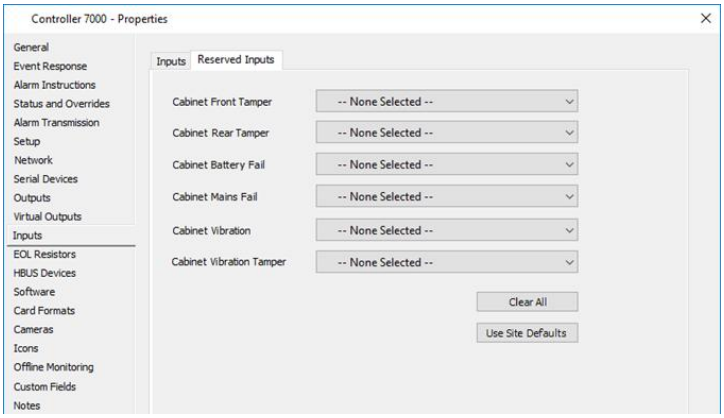
If…	**then there will be a maximum of…**
4H or 4R Module,	12 inputs.
8H or 8R Module,	24 inputs.



The screenshot above is for the **Inputs** tab of the Controller 7000. The **Reserved Inputs** sub-tab allows sites whose Controller 7000s are housed in cabinets to use physical tamper inputs (rather than optical tampers), and to also reserve power supply inputs and create alarms with the Controller 7000 as a source. Notes:

- The Controller 6000 does NOT have a **Reserved Inputs** sub-tab.
- Operators require the "Edit Site" privilege to reserve inputs.

25. Assign each Input to the correct address. For details on how to create an Input, refer to ***Creating Inputs and Outputs*** (on page 21-50).
26. If applicable, click the **Reserved Inputs** sub-tab.



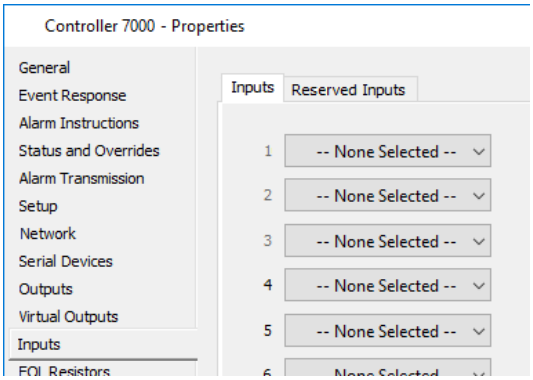
By default, all the Reserved Inputs will have "—None Selected --". They will however already be populated if the **Reserve inputs on creation of I/O module** checkbox has been ticked on the Server Properties **Reserved Input Defaults** tab.

27. If the fields are not already populated or have been changed, and you want to set the site defaults from the Server Properties, click the **Use Site Defaults** button, otherwise select the required input for each field.
    The number of inputs available for each field is determined by what type of Plug-in Module was selected on the **Setup** tab, as follows:

If…	then each field will have…
4H or 4R Module,	Inputs 1 - 12 to select from.
8H or 8R Module,	Inputs 1 - 24 to select from.

    Notes:
    - If Input 1 is already in use, ticking the **Use Input 1 for cabinet tamper** checkbox will generate the following message:
      "Input is assigned as a tamper input. Please remove the first input from this controller."
    - If you attempt to assign an input more than once, the following error message displays:
      "Cannot reserve input, it is already allocated"
    - When reserved inputs are configured for **Cabinet Front Tamper** and **Cabinet Rear Tamper**, the optical tampers on the Controllers **Status and Overrides** tab are disabled, (i.e. the **Disable Front Tamper** and **Disable Rear Tamper** checkboxes).
    - The **Clear All** button can be used to clear reserved inputs and return them to "—None Selected --".

    As inputs are reserved, they become disabled (greyed out) on the **Inputs** sub-tab.



28. The **EOL Resistors** tab allows you to configure End-of-line (EOL) resistances for the Controller. For further detail see ***Configuring EOL Resistors for devices*** (on page 21-46).
29. The **HBUS Devices** tab allows you to assign HBUS devices to the Controller. For further detail see ***Configuring HBUS Devices*** (on page 21-65).
30. The **Software** tab allows you to assign device software to the Controller. Refer to either ***Assigning Device Software to devices*** (on page 27-5), or Upgrading Multiple Controllers (on page 27-10) if you are upgrading the firmware on multiple Controllers.
31. Click **OK**. The Controller now displays within the **Hardware** List Window.

Result

A Controller has been created. The Controller name now displays within the **Hardware** List Window.

Hints

Re-sync Databases

Performing a **Re-sync Databases** action on a Controller (via the Controller context menu), deletes the card database at the Controller and automatically re-populates it.

Purge Pending Messages

Performing a **Purge Pending Messages** action on an offline Controller (via the Controller context menu), will clear the queue of outgoing messages and bring the Controller online. Operators require either the "Advanced User" or "Maintenance Override" privilege in the division of the Controller to perform this action.

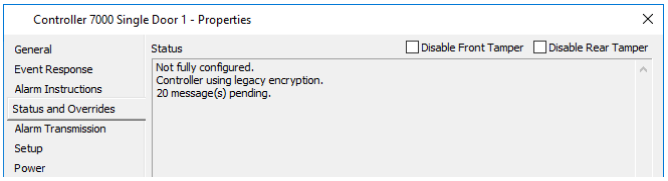
WARNING: The Purge Pending Messages action is only intended to be used on an offline Controller that will be restarted with Dip Switch 2 active. Dip Switch 2 indicates to the server that the Controller wants all configuration data, if the Controller is only offline due to network connectivity and the message queue is cleared then important configuration messages may be purged with this tool.

Creating a Controller 7000 Single Door

The Controller 7000 Single Door is a processing board for an intruder alarm and access control system that can control a single door.

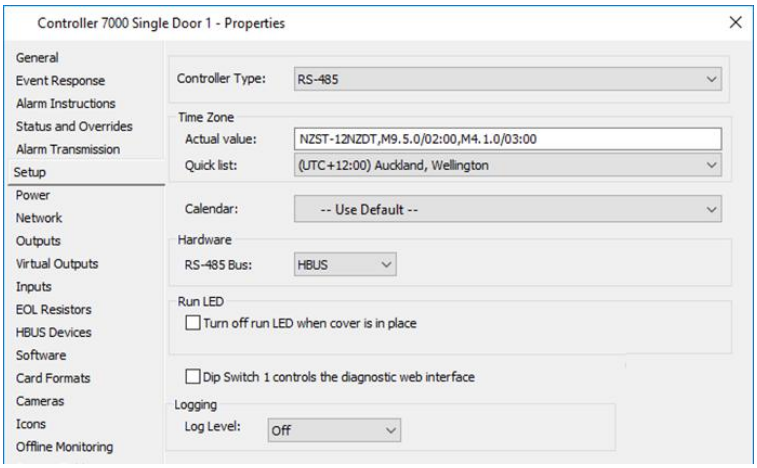
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Controllers** > **Controller 7000 Single Door**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
5. By default, continuous tamper alarms will be generated if the Controller is tampered with, (i.e. a 'Front Tamper' alarm if the cover is removed, or a 'Rear Tamper' alarm if the Controller is removed from the wall).
   Do you want to prevent tamper alarms from happening?

If…	then…
no,	go to Step 6.
yes,	a. Click the **Status and Overrides** tab.



b. Tick the **Disable Front Tamper** and/or **Disable Rear Tamper** checkbox(es).
Note: The Controller 7000 Single Door has a **Disable Front Tamper** and a **Disable Rear Tamper** checkbox so the tampers can be enabled/disabled independently.

6. Click the **Setup** tab.



6. Select the **Controller Type** from the drop-down list, (i.e. either **RS-485** if the physical Controller supports RS-485 devices, or **Wiegand** if the physical Controller supports Wiegand Reader).

Note: If Wiegand is selected, the **HBUS Devices** tab will disappear from the list of tabs on the left.

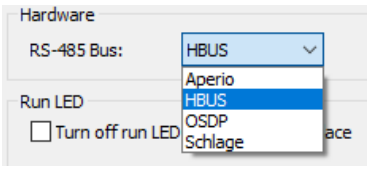
7. The **Time Zone** section of the screen is automatically populated with the same time zone the Command Centre Server is in.
   If you require another city/time zone, you can select one from the drop-down **Quick list**, and the POSIX time zone string in the **Actual value** field will be updated.
   Note: If you change the time zone the Controller will restart when you **Apply** your change.
   The formatting rules for time zone strings are as follows:

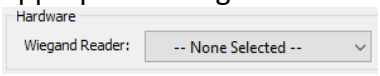
   Time Zone string format is:
   {STDName}{Offset}[{DSTName}{Offset},{Start rule},{End rule}]
   Offsets are in Americocentric form, (i.e. multiplied by -1 in order to make US timezones positive).
   The Start and End rules can be omitted if there is no daylight saving. The rules can be written in one of the following three formats:
   - **Jn** - where n = {1-365} (Day of year, but Feb 29 never counted)
   - **n** - where n = {0-365} (Day of year)
   - **Mm.w.d** - where m=month {1-12}, w=week of month {1-5} (5=last), d=day of week {0(Sun)-6(Sat)}

   These can be followed by an optional changeover time in format: /hh[:mm[:ss]] - default is 2:00:00.
   If the daylight savings offset is omitted, then one hour more than the standard offset is assumed.

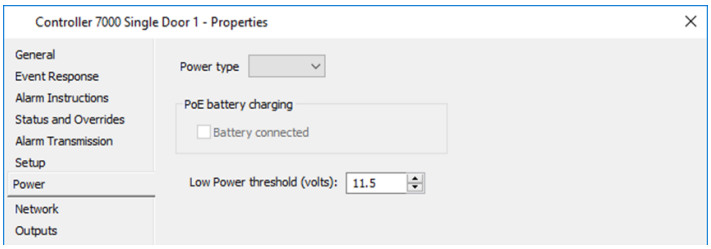
   Example:
   New Zealand's timezone string is: NZST-12NZDT,M10.1.0,M3.3.0, which means New Zealand is 12 hours ahead of GMT, our daylight savings (of one hour) starts on the first Sunday of October and finishes on the third Sunday of March, both at the default time of 2am.
8. The **Calendar** drop-down list contains a list of all the special calendars configured in the system for the operator's division. One special calendar may be assigned to each Controller in the system.
   By default, no special calendar will be assigned to the Controller. However, if you require one to be assigned, select the appropriate special calendar from the drop-down list.
   This Controller will use both the special calendar selected as well as the default calendar for its scheduling operations. The default calendar provides cycle and special day assignments, while the special calendar provides special day assignments only, with the possibility of overriding special day settings from the default calendar.
   Note: Refer to Creating a Special Calendar for further detail about special calendars.
9. The **Hardware** section allows you to alter the devices used as required.
   The options available will depend on the selection you made in the **Controller Type** field, (i.e. either RS-485 or Wiegand), as follows:

If…	then select the…
RS-485,	correct RS-485 Bus type from the drop-down list for the devices connected to the Controller.
Wiegand,	appropriate Wiegand Reader from the drop-down list.

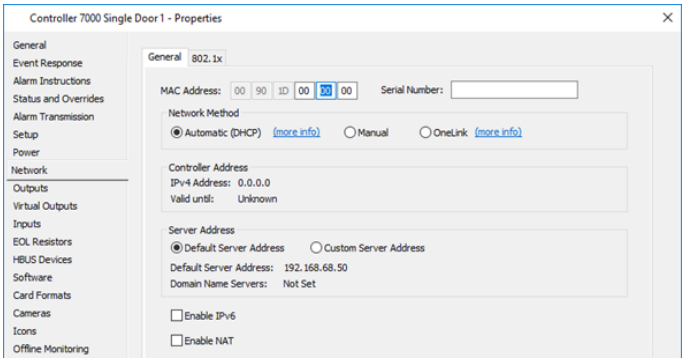




10. If required, tick the **Turn off run LED when cover is in place** checkbox.
11. The **DipSwitch 1 controls the diagnostic web interface** checkbox should be ticked if requested by Gallagher Technical Support. Otherwise, leave this option unticked. **Important:** If Dip Switch 1 is to be used to control the diagnostic web interface, Dip Switch 1 needs to be physically 'ON' on the Controller as well as this checkbox being enabled.
12. The **Logging** section allows you to configure the verbosity of diagnostic logs from this Controller which are written into the Command Centre log file. The log level can be changed to a value from **Off**, (i.e. least verbose) to **Trace**, (i.e. most verbose).
13. Click the **Power** tab.

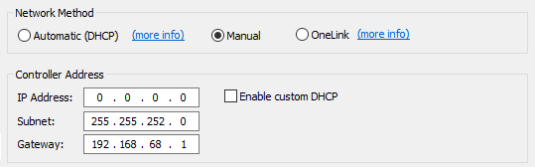


14. Select the appropriate **Power type** from the drop-down list. **Notes:**
    - A power type must be selected otherwise a pop message will display asking you to select one when you click **Apply** or **OK.**
    - If you select PoE+ or PoE the **Battery connected** option becomes enabled, but it remains disabled if you select DC.
15. If you selected PoE+ or PoE, tick the **Battery connected** checkbox if required.
16. The **Low Power threshold** field can be altered to set the level at which a low voltage alarm will be generated for the Controller.
17. Click the **Network** tab. The **General** sub-tab displays by default.



Note: The **802.1x** sub-tab enables sites to configure a Controller 7000 Single Door for 802.1x. See ***Configuring a Controller 7000 or 7000 Single Door for 802.1x*** (on page 21-22) for further instructions.

18. Enter the **MAC Address** for the Controller.
    The MAC Address for each Controller is stuck to the actual Controller PCB.
    Note: A MAC address range is included in your license file and will be checked against when a MAC address is saved here. If you receive a "MAC address out of range" error message, check your license file to see what range is valid.
19. Entering the **Serial Number** of the Controller is optional and can be found printed on one of the Controller labels.
20. Click the radio button for the appropriate **Network Method**, i.e. either **Automatic (DHCP)**, **Manual** or **OneLink**.
    Automatic (DHCP) is the preferred method for controllers connected on the local network, but if you select **Manual** the **Controller Address** section changes as shown below:

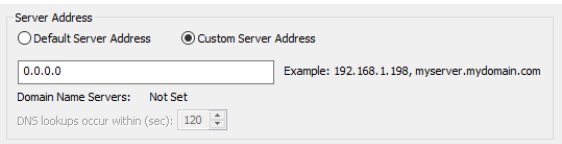


    The **OneLink** method utilises Gallagher Cloud Services to enable Controller 7000s to connect to the on-premises Command Centre Server over the internet. See ***OneLink Configuration*** (on page 21-18) for further instructions.
21. Enter the **IP Address**, (i.e. TCP-IP Address), **Subnet** and **Gateway** information for the Controller. This information will be provided by the IT Department for the organisation, or the IT provider of the network.
    Note: By default, the **Subnet** and **Gateway** fields are populated with the first subnet mask and gateway from one of the server's ethernet adaptors with a non-zero gateway.
    If there is no IT support for this site, and it is a localised and dedicated LAN built for Command Centre, there are some standards that you can apply to the configuration of the Controllers, as described next:

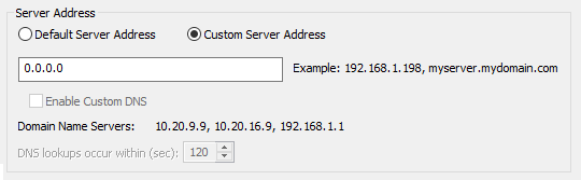
Configuration Parameter	Description
IP Address	The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of TCP-IP address space for private networks: Class A From 10.0.0.0 to 10.255.255.255 Class B From 172.16.0.0 to 172.31.255.255 Class C From 192.168.0.0 to 192.168.255.255 These TCP-IP addresses have been set aside specifically for use when it is not necessary (or desirable) for the attached devices to be available on the Internet. If one of these TCP-IP addresses were accidentally broadcast on the Internet they would be ignored by the routing firewall server and would cause no conflict issues. The first block is a single Class "A" network number, the second

Configuration Parameter	Description
	block is a set of 16 contiguous Class "B" network numbers, and the third block is a set of 256 contiguous Class "C" network numbers. **Note:** Each device, (i.e. Computer, Printer, Controller) on the localised LAN must have a unique TCP-IP address. Each address used must however be in the same Subnet Mask range. This means as an example, if you use the Class "B" TCP-IP address range, each TCP-IP address assigned to the localised LAN must start with 172.16 and then be unique, (e.g. 172.16.0.1, 172.16.0.2, 172.16.0.3, 172.16.0.4, etc.)
Subnet	There are default Subnet Mask settings for the three class categories: Class A From 10.0.0.0 to 10.255.255.255 Default Subnet Mask is 255.0.0.0 Class B From 172.16.0.0 to 172.31.255.255 Default Subnet Mask is 255.255.0.0 Class C From 192.168.0.0 to 192.168.255.255 Default Subnet Mask is 255.255.255.0 Use the associated Subnet Mask appropriate for the TCP-IP class used. The Subnet Mask differentiates between the network and client parts of the TCP-IP address. The "255's" identify the network section and the "0's" identify the clients. For a Class "B" TCP-IP address the network identification numbers are "172.16" and will be identical for each TCP-IP address on that network. The following two numbers of the TCP-IP address uniquely identify each device on the network.
Gateway	Gateway settings when used in general LAN configurations provide a path to a different network environment. In a localised LAN environment for Gallagher there is no physical connection to a different network, so the Gateway setting is ineffective. On single Subnet networks, it is recommended the Gateway information be set exactly as the TCP-IP address used, or alternatively 0.0.0.0
Enable custom DHCP	This checkbox allows sites to use their own Dynamic Host Configuration Protocol (DHCP) service to assign IP address-es to their controllers automatically, without physically needing to be at the controller. See ***Configuring a Controller for DHCP*** (on page 21-35) for further detail.

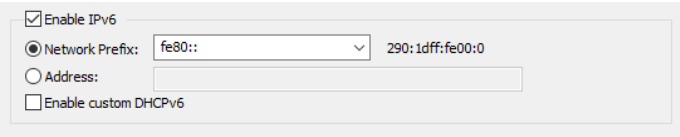
22. Click the radio button for the appropriate **Server Address**, (i.e. either **Default Server Address** or **Custom Server Address**).
    If you selected **Automatic (DHCP)** for the "Network Method", and you select **Custom Server Address**, this section will change as shown below:



If you selected **Manual** for the "Network Method", and you select **Custom Server Address**, this section will change as shown below:



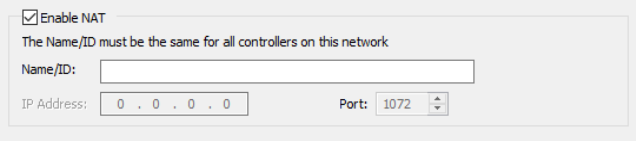
23. If this Controller is separated from the Server by a firewall, so it can still contact the Command Centre Server, enter the IP Address.
24. Controllers must be able to make use of Domain Name Servers (DNS) in disaster recovery situations, especially where backup servers reside on different subnets. See ***Configuring DNS Servers for Controllers*** (on page 21-19) for the procedure.
25. Controller 7000s Single Door support both IPv4 and IPv6. A Controller 7000 that needs to communicate with IPv4 external systems must be assigned IPv4 addresses as per existing configuration procedures.
    To assign an IPv6 address additional to IPv4:
    a) The only supported method of address allocation for the Controller is an auto configuration via router advertisements. The Controller will only accept IPv6 auto configuration if it is either already configured for IPv6 communication or the Controller was booted with DIP switch 2 on.
    b) Check the **Enable IPv6** checkbox. The **Enable IPv6** section changes as shown below if you selected **Manual** as the Network Method above:



    c) Click either the **Network Prefix** or **Address** radio button and enter appropriate details.
        - **Network Prefix** contains a pre-populated network prefix combo field containing all subnet prefixes available at the Command Centre server machine. The interface identifier of the Controller is pre-populated based on the entered MAC address.
        - The **Address** field is free text field to provide complete IPv6 address instead. The given address shall be from the list of IPv6 addresses assigned to the Controller through the auto-configuration process. Hostname is not supported here.

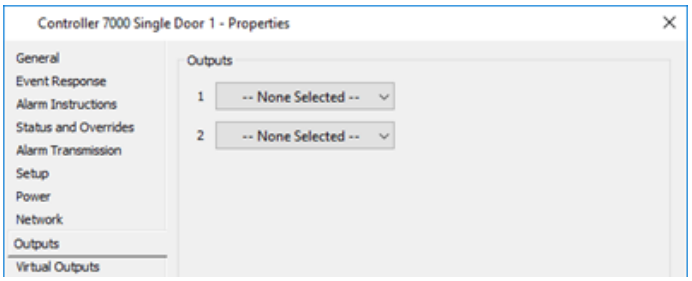
    To assign only an IPv6 address:
    - IPv4 address can be NULL in this case.
    - DIP switch 3 should be ON as well as DIP switch 2.
    - Reset is the same as above.

    Note: A document providing further technical information about IPv6 (**Gallagher Command Centre IPv6 Support.pdf**) is available in the `'Documentation'` directory of the Command Centre installation files
26. Check the **Enable NAT** checkbox if your site wants Command Centre to communicate with multiple Controllers on different networks.
    Selecting **Enable NAT** expands the section as shown below:



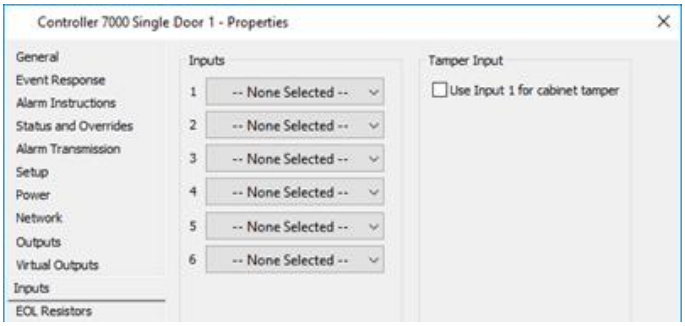
Refer to ***Configurable Ports - NAT Solution*** (page 21-40) for further detail.

27. Click the **Outputs** tab.



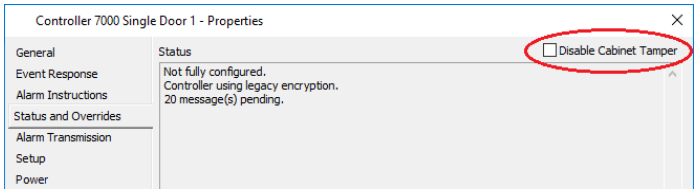
This tab allows you to link a maximum of two outputs to the Controller to activate another device, (e.g. alarms, light switching, doors unlocking).

28. For the appropriate Output, click within the edit box.
    From the displayed drop-down menu, select the output name.
29. Click the **Inputs** tab.



This tab allows you to link inputs to the Controller. The number of inputs available will depend on what **Controller type** you selected on the **Setup** tab, (i.e. a maximum of six inputs if you selected RS-485, or a maximum of five inputs if you selected Wiegand).

30. If you wish to use an input as the cabinet tamper, tick the **Use Input 1 for cabinet tamper** checkbox (which disables the Input 1 field).
    Note: If you tick this option, the **Disable Front Tamper** and **Disable Rear Tamper** checkboxes on the Status and Overrides tab are replaced with a **Disable Cabinet Tamper** checkbox.



31. For the appropriate Input, click within the edit box.
    From the displayed drop-down menu, select the input name.
    Note: If Input 1 is already in use, ticking the **Use Input 1 for cabinet tamper** checkbox will generate the following message:
    "Input is assigned as a tamper input. Please remove the first input from this controller."

32. The **EOL Resistors** tab allows you to configure End-of-line (EOL) resistances for the Controller. For further detail see ***Configuring EOL Resistors for devices*** (on page 21-46).
33. The **HBUS Devices** tab allows you to assign HBUS devices to the Controller. For further detail see ***Configuring HBUS Devices*** (on page 21-65).
34. The **Software** tab allows you to assign device software to the Controller. Refer to either ***Assigning Device Software to devices*** (on page 27-5), or ***Upgrading Multiple Controllers*** (on page 27-10) if you are upgrading the firmware on multiple Controllers.
35. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Controller. For further details regarding the **Cameras** tab, see ***Cameras*** (on page 3-24).
36. Click the **Icons** tab if you want to change the Icon Set for this Controller. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
37. Server to Controller, or Inter-controller offline monitoring can be configured from the **Offline Monitoring** tab.
    See ***Configuring Offline Monitoring*** (on page 21-33) for further detail.
38. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Controller. For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
39. Click the **Notes** tab if you want to add a note(s) about this Controller. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-83).
40. 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 Controller 7000 Single Door has been created. The Controller name now displays within the **Hardware** List Window.

Hints

Re-sync Databases
Performing a **Re-sync Databases** action on a Controller (via the Controller context menu), deletes the card database at the Controller and automatically re-populates it.

Purge Pending Messages
Performing a **Purge Pending Messages** action on an offline Controller (via the Controller context menu), will clear the queue of outgoing messages and bring the Controller online. Operators require either the "Advanced User" or "Maintenance Override" privilege in the division of the Controller to perform this action.

WARNING: The Purge Pending Messages action is only intended to be used on an offline Controller that will be restarted with Dip Switch 2 active. Dip Switch 2 indicates to the server that the Controller wants all configuration data, if the Controller is only offline due to network connectivity and the message queue is cleared then important configuration messages may be purged with this tool.

OneLink Configuration

Introduction

OneLink utilises Gallagher Cloud Services to enable Controller 7000s to connect to the on-premises Command Centre Server over the internet.

Prerequisites

OneLink prerequisites are:

- An active Care Plan and enrolment in CEIP are required in order to activate OneLink connections.
- Ensure an active Care Plan then contact your Gallagher Rep.
- Enable CEIP follow the instructions in the "Product Alerts and Customer Experience Improvement Program" topic in *Command Centre Client help file*.

Minimum versions are vEL9.30 Command Centre and vCR9.30 MR1 for Controller.

Licensing

- OneLink is a subscription service and connections can be activated or deactivated at any time without contacting Gallagher via the Configuration Client.
- Refer to OneLink-Pricing-Flyer.pdf for further information.
- Managing Cloud license allocation and subscription status can be checked via the **Subscription Summary** tab of the Cloud Licensing Viewer in the Command Centre Client. 'Allocation' is the number of connections in use and the number of purchased subscriptions, (e.g. 2/4). Exceeding the number of purchased subscriptions incurs pro-rata charges. Purchased subscriptions remain available for use until the end of the subscription period.
  For further detail, refer to the **Command Centre Web Release Note** in the `'Release Notes'` directory of the Command Centre installation files.

Set up

The OneLink set up process is split into four parts, as follows:

Network Preparation

1. Configure your firewall to allow TCP outbound traffic on port 443 with a source of your internal Command Centre server, and destination of the following DNS or IP addresses.
   Note: There is no need to allow any inbound traffic to your Command Centre server.
   If you are configuring firewall rules based on IP address, please allow the following static IP addresses:

   Australian Command Centre Cloud:

   DNS address: **commandcentre-ap-southeast-2.security.gallagher.cloud**
   IP addresses: **52.62.211.7** and **54.79.91.203**

   Australian Gallagher Gateway Region:

   DNS address: **commandcentre-api-au.security.gallagher.cloud**
   IP addresses: **3.106.1.6** and **3.106.100.112**

   United States Gallagher Gateway Region:

   DNS address: **commandcentre-api-us.security.gallagher.cloud**
   IP addresses: **44.193.42.111** and **3.209.194.103**

Global Cloud Services API Gateway:

DNS address: **services.security.gallagher.cloud**
IP addresses: **15.197.141.103** and **76.223.78.39**

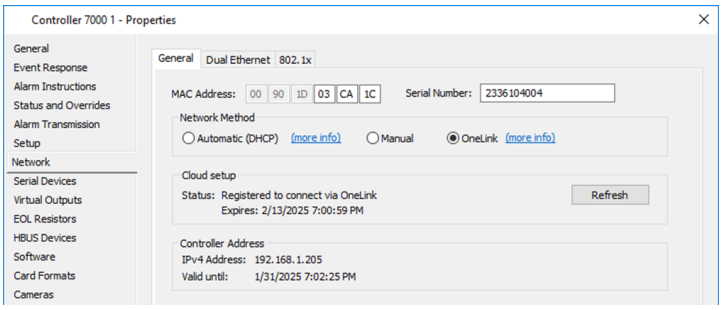
2. The controller requires a stable internet connection and access to DHCP and DNS services. If a firewall is in place, it must allow TCP outbound traffic from the controller to:
   - **Controller Registration Service:** https://controller-onboarding.security.gallagher.cloud:443
   - **Controller Gateway:** wss://controller-gateway.security.gallagher.cloud:443
   - **Trusted Issuer Service:** http://controller-onboarding.security.gallagher.cloud:80

Cloud Configuration

3. Enable a connection to the Gallagher Cloud before configuring a OneLink Connected Controller. See ***Connecting to the Cloud*** (page 28-7) for instructions.
   Note: Command Centre must be connected to the Gallagher Cloud.

Controller Configuration (Registration)

4. Configure the Controller for OneLink as appropriate.
   See ***Creating Controller 7000s or 6000s*** (on page 21-2) or ***Creating a Controller 7000 Single Door*** (on page 21-9) for the complete procedure for configuring a Controller.
5. On the **Network** tab:
   a) Enter the **MAC Address** for the Controller. The MAC Address for each Controller is stuck to the actual Controller PCB.
   Note: A MAC address range is included in your license file and will be checked against when a MAC address is saved here. If you receive a *"MAC address out of range"* error message, check your license file to see what range is valid.
   b) Enter the correct **Serial Number** of the Controller.
   The Serial Number can be found printed on one of the Controller labels.
   c) Click the **OneLink** radio button.
   You will be asked to accept the Cloud Terms and Conditions.
   d) Click the **Apply** button.



In the **Cloud setup** section, the status *"Registered to connect via OneLink"* indicates that the Controller has been registered in the Controller Registration Service in the Gallagher Cloud. Although registered, the Controller still needs to be connected to the server (via the Actication process next) within 14 days or the registration will expire on the date and time given.

Note: If registration does expire, you will need to re-register by clicking the **Refresh** button.

Controller Activation

6. Check the Controller software version is 9.30+.
   Note: This may be indciated on the packaging for recently manufactured controllers, otherwise the controller must be upgraded via Command Centre before it is OneLink capable.
7. Turn DIP Switches 2 and 7 ON.
8. Connect the Controller to an internet connection.
9. Power on the Controller.
10. The Controller will automatically:
    a) Retrieve details of the Controller Gateway URL from the Controller Registration Service.
    b) Connect to the Controller Gateway which will forward the connection request to Command Centre.
    c) Command Centre authenticates the Controller and a connection is established.
    d) Communication between the Controller and Command Centre Server continues through the Controller Gateway.
11. Once the Controller comes online and the Run LED is in a consistent single flash state, (typically this can take up to two minutes), turn the DIP Switches OFF.

Configuring Secondary Ethernet operation mode

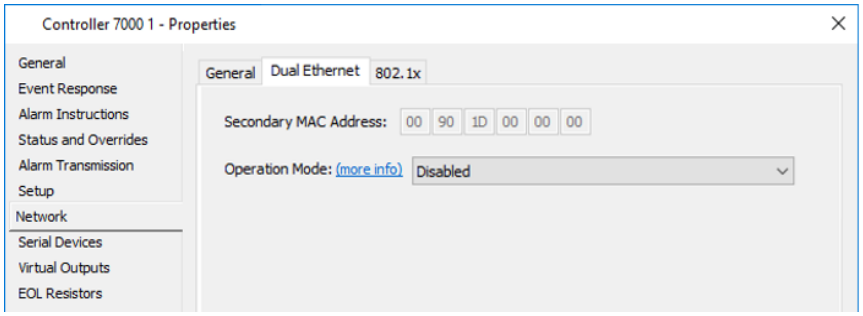
Introduction

This procedure describes secondary ethernet adapter configuration for a Controller 7000. **Notes:**

- **Automatic (DHCP)** on secondary ethernet requires v9.40+ controller firmware.
- The controller can find the server automatically if it is assigned a "gallagherserver" DNS alias.

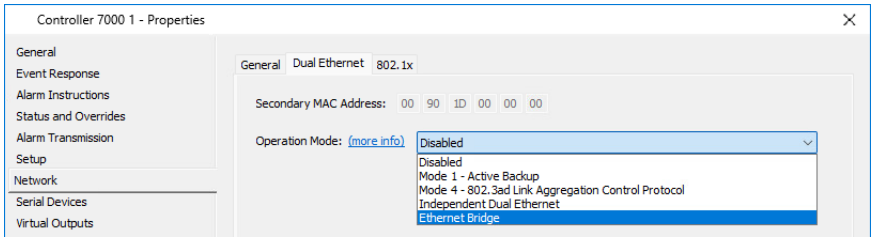
Configuration

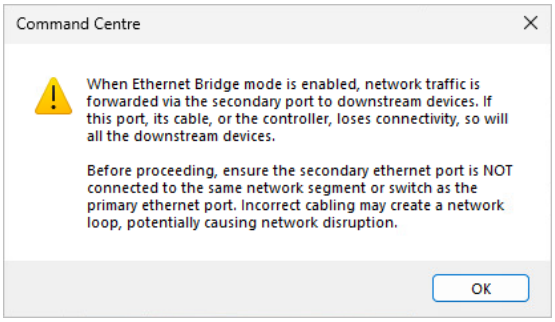
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Controller you want to configure automatic DHCP for.
3. **Right click** and select **Properties**.
4. Click the **Network** tab. The **General** sub-tab displays by default.
5. Click the **Dual Ethernet** tab.



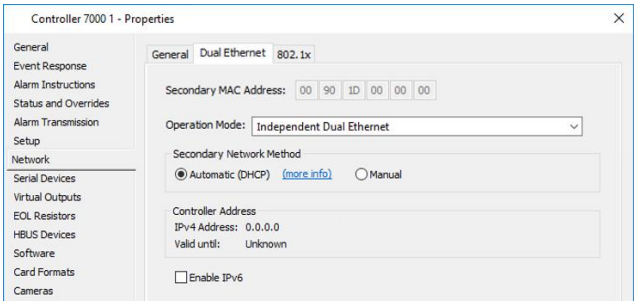
Field	Description
Secondary MAC Address	This field is 'read-only'. Once the controller comes online in Command Centre, regardless of the selected Operation Mode, the Secondary MAC Address will be automatically populated in this field.
Operation Mode	This field is set to 'Disabled' by default and is editable.

6. Select the appropriate **Operation Mode** from the drop-down list.

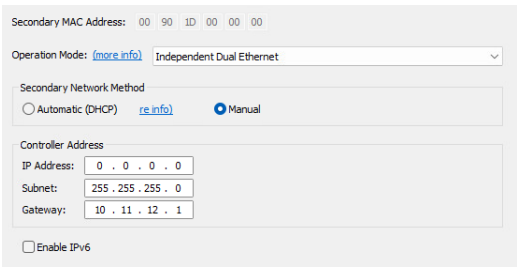


Option	Description
'Disabled', 'Mode 1 - Active Backup', or 'Mode 4 - 802.3ad Link Aggregation Control Protocol',	If any of these options are selected, there will be no other fields shown. Go to Step 10.
'Independent Dual Ethernet'	Go to Step 7.
'Ethernet Bridge'	If this option is selected, there will be no other fields shown. This mode means the Controller will operate as a transparent Ethernet bridge. All network traffic destined for the bridged network will pass through the controller without modification, regardless of traffic type or content. **Note:** This mode only applies to Enhanced and High Sec Controller 7000s. When selected, the following warning displays:  Ensure the secondary ethernet port is NOT connected to the same network segment or switch as the primary ethernet port, and go to Step 10.

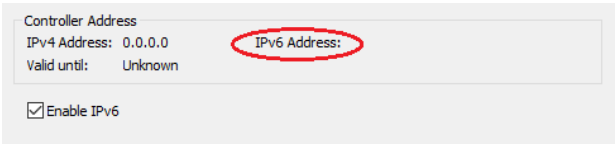
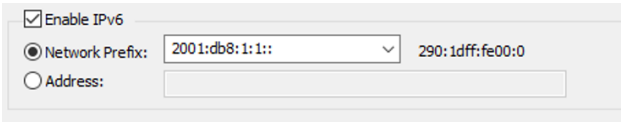
7. By selecting 'Independent Dual Ethernet' for **Operation Mode**, additional sections will appear on this screen, as shown:



8. Click the radio button for the appropriate **Secondary Network Method**, i.e. either **Automatic (DHCP)** or **Manual**.
   Note: Automatic (DHCP) is selected by default and is the preferred method. However, if you select **Manual** the **Controller Address** section changes as shown below:



   The configuration for these fields is the same as described for the **General** sub-tab.
9. What occurs if the **Enable IPv6** checkbox is ticked depends on what **Secondary Network Method** you selected.

Field	Description
Automatic (DHCP),	an **IPv6 Address** field will appear in the **Controller Address** section, and will be automatically populated once the Controller receives an IPv6 address from the DHCP server. 
Manual,	additional fields will appear.  Click either the **Network Prefix** or **Address** radio button and enter appropriate details. • **Network Prefix** contains a pre-populated network prefix combo field containing all subnet prefixes available at the Command Centre server machine. The interface identifier of the Controller is pre-populated based on the entered MAC address. • The **Address** field is free text field to provide complete IPv6 address instead. The given address shall be from the list of IPv6 addresses assigned to the Controller through the auto-configuration process. Hostname is not supported here.

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

Configuring a Controller 7000 or 7000 Single Door for 802.1x

Introduction

802.1X is a widely used industry standard for network access control (NAC) and authentication. It is part of the IEEE 802.1 group of networking protocols and provides a mechanism for controlling access to a local area network (LAN) or a wireless network, enhancing network security by ensuring that only authorized users and devices can connect to the network.

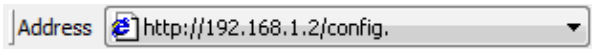
Operators require the "Edit Site privilege to perform this procedure.

Note: The Secondary Ethernet port on a Controller 7000 Enhanced doesn't support 802.1x

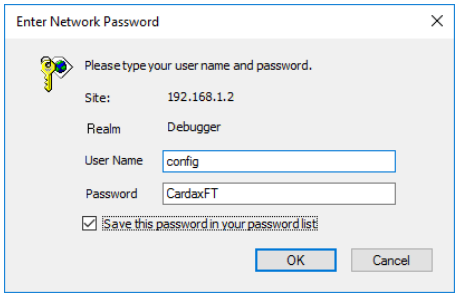
Configuration

The Controller is configured for 802.1x from the Controller Config Webpage, as follows:

1. Connect the Controller directly to your laptop.
2. Turn DipSwitch 1, 2 and 3 ON and restart the Controller.
   Note: If DipSwitch 2 is OFF, access to the 802.1x Configuration page is denied.
3. Open the Internet Browser.
4. In the **Address** field enter the Controller's default IP Address followed by a forward slash, then **config**. See the example below for the correct format.



5. Press the **Enter** key on your keyboard.
   The Enter Network Password screen displays.



6. Enter **config** for the 'User Name' (all in lower case), and **CardaxFT** for the 'Password'. You also have the option to 'Save this password in your password list'.
7. Click the **OK** button. The Gallagher Controller Configuration screen displays.



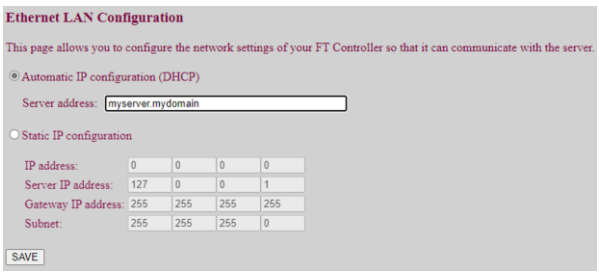
8. Select **Set Current Time**. The 'Time Manager Thread' page displays.
9. Set the Controller's clock to use current time, and click the **Apply** button.
10. Select **802.1x Configuration**. The '802.1x Configuration' page displays.



11. Configure as required.

Field/Button	Description
Domain	This is the domain name of the computer where the Controller is connected to. Valid characters are 0 to 9, a to z, A to Z, and - (Default = blank)
Generate CSR	Clicking this button generates or re-generates CSR (Certificate Signing Request) along with the Controller's private key. The generated CSR can then be submitted to a CA for signing. The CSR contains the MAC address (last 6 digits) as the identity of the Controller it is generated on.
EAP Mode	The drop-down list shows the following options: (Default = Off) **Off =** authentication using 802.1x standard is OFF **TLS =** enables 802.1x with certificate-based authentication.
Identity	The identity used for authorisation. Accepts all characters including special characters. Cannot be left blank. (Default = blank)
Server Certificate	This field is enabled when EAP mode = TLS. This is where you upload all the server certificates. The Server root certificate is required as a minimum. (Default = No file chosen, disabled)
Client Certificate	This field is enabled when EAP mode = TLS. This is where you upload the certificate issued by the CA, based on the CSR. (Default = No file chosen, disabled) **Note:** Error messages will display if the signed certificate is expired, doesn't match the Private Key, or doesn't contain a valid Subject Alternative Name (SAN) or Extended Usage extension as the CSR.

12. Click the **Apply** button.
13. Select **LAN Configuration**. The 'Ethernet LAN Configuration' page displays.



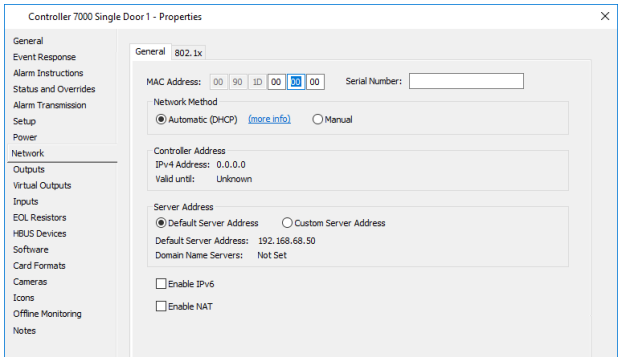
14. You can use either DHCP or Static IP.

If you select…	then…
Automatic IP configuration (DHCP),	Enter the DHCP Server address in the **Server address** field.
Static IP configuration	Assign the Controller an IP by entering it in the **IP**

If you select…	then…
	address field.

Note: Having Command Centre assign the Controller an IP Address via BOOTP is not supported in conjunction with 802.1x.

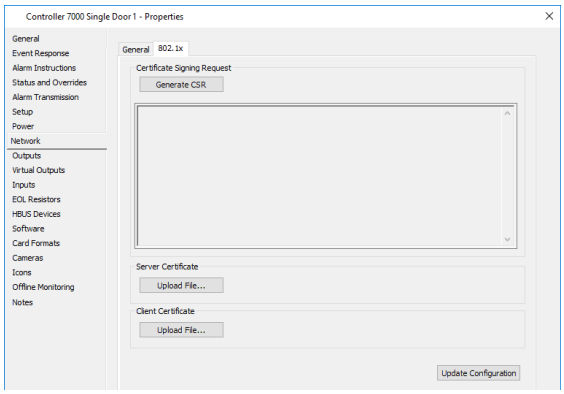
15. Click the **SAVE** button.
16. Turn DipSwitch 1, 2 and 3 OFF.
17. Swap the Controller on to 802.1x network and restart the Controller.
18. In Command Centre, click Configure from the menu bar, then **Hardware**. The **Hardware** List Window opens (in tree view).
19. Right click and select New...Controllers and the appropriate Controller type, (i.e. Controller 7000 or Controller 7000 Single Door).
20. Click the **Network** tab. The **General** sub-tab displays by default.



21. Which option did you select on the 'Ethernet LAN Configuration' page of the Controller Config Webpage?

If you selected…	then click the…
Automatic IP configuration (DHCP),	**Automatic (DHCP)** radio button.
Static IP configuration	**Manual** radio button, and enter the IP address that you already set on the Webpage in the **IP address** field.

22. Click the **802.1x** sub-tab.



Note: The controls will not be enabled on this tab is you haven't yet configured the Controller for 802.1x on the Controller Config Webpage, and the following message will display in the lower part of the screen:

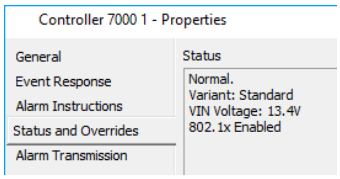
802.1x is not enabled on the controller.

The controls will also be disabled if the Controller is offline, and the following message will display:

802.1x cannot be configured while the controller is offline.

Result

A Controller has been configured for 802.1x.
The status message *"802.1x Enabled"* will display n the **Status and Overrides** tab indicating that it is configured and connected to 802.1x network.



If the Controller is configured but not connected to 802.1x network, then the status message will read *"802.1x Enabled - not connected to 802.1x network"*.

Notes:

- Controller 7000s already connected to Command Centre and online via a **non-802.1x authenticated port** can be updated to use 802.1x, as follows:

  Upating an existing install to 802.1x

  1. Turn Dip switches 1, 2 & 4 ON and restart the Controller.
  2. Make sure the Controller is online with Command Centre.
  3. Access the Controller's config page using it's assigned IP address.
  4. Go to the '802.1x Configuration' page and configure the Controller for 802.1x and save.
  5. Turn DipSwitch 1 and 2 OFF and DipSwitch 4 ON.
  6. Swap the Controller on to 802.1x network, or configure port to require 802.1x and restart the Controller.
  7. In Command Centre, check the Controller status updates to '802.1x - Enabled' on the Controller properties **Status and Overrides** tab.
- If you need to add new certificates or renew existing certificates to the Controller refer to ***Adding new or renewing existing certificates to Controllers using 802.1x*** (next) for the procedure.

Adding new or renewing existing certificates to Controllers using 802.1x

Introduction

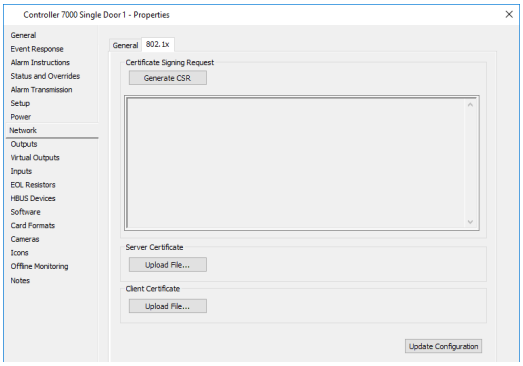
Once a Controller has been configured for 802.1x, new certificates can be added or existing certificates can be renewed in Command Centre Configuration Client using the following procedure.

Note: When renewing a Client certificate, a Certificate Signing Request (CSR) needs to be generated first for the roll-back feature to be supported.

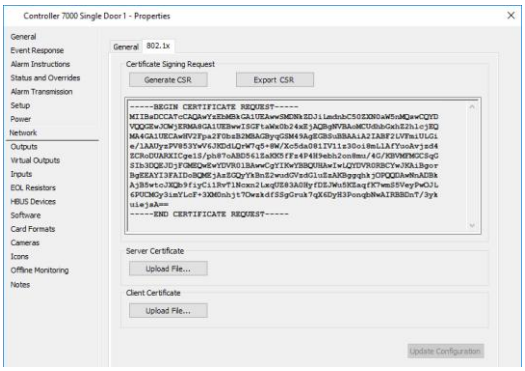
Configuration

1. In Command Centre, click Configure from the menu bar, then **Hardware**. The **Hardware** List Window opens (in tree view).
2. Highlight the Controller you want to add a new certificate to, or renew an existing certificate for.
3. **Right click** and select **Properties**.

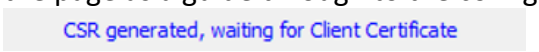
4. Click the **Network** tab. The **General** sub-tab displays by default.
5. Click the **802.1x** sub-tab.



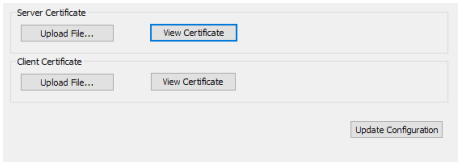
6. Click the **Generate CSR** button.
   A new certificate request is generated in a 'read-only' text format which can be either copied manually to a file, or can be exported using the **Export CSR** option which becomes available once after the CSR is generated.



   When a new CSR is generated, a waiting message appears at the bottom of the page as a guide through to the configuration process.



   When a file has been selected, the **View Certificate** buttons appear to the right of the **Upload File…** buttons, and the **Update Configuration** button is enabled.



   The **View Certificate** buttons enables you to view the recently uploaded certificate, (i.e. Server Certificate or Client Certificate as appropriate).
7. Click the **Update Configuration** button to start the process of downloading the certificates to the Controller.
   Note: Alarms are generated if the signed certificate is expired, doesn't match the Private Key, or doesn't contain a valid Subject Alternative Name (SAN) or Extended Usage extension as the CSR. These alarms can be processed.
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.

Upgrading a Controller 6000 to a Controller 7000

Introduction

This procedure assists sites with the upgrading of a Controller from a C6000 to C7000. It reduces the time taken to configure a C7000 based on the C6000 that it is replacing, allowing sites to create an equivalent C7000 with most of the configuration copied over from the C6000 and linked items re-attached.

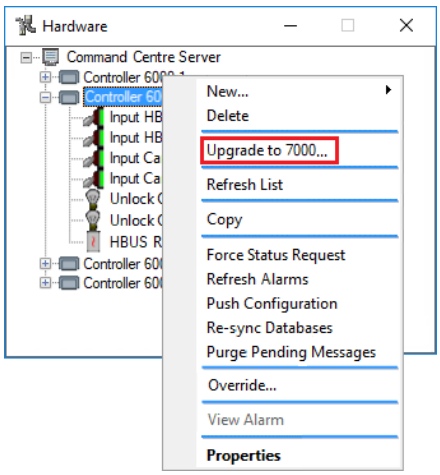
Operators require the "Edit Site", "Launch Configuration Client", and "Maintenance Override" privileges to perform this procedure.

Before you begin

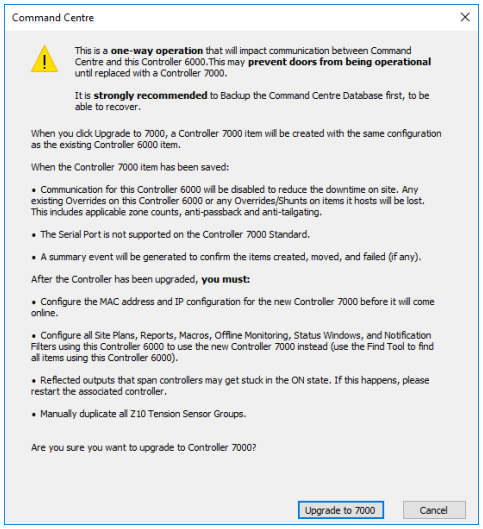
- All customisations will need to be removed from the Controller 6000 prior to the migration to the Controller 7000.
- The Alarm and Event Viewer will be flooded with *"Part - no such type"* (if the controller customisation items are present on the system) once the migrated Controller 7000 software controller is upgraded due to the external system controller customisation being linked to the newly migrated Controller 7000. A compatible controller customisation will need to be applied to the newly migrated Controller 7000 in order to address this issue.

Procedure

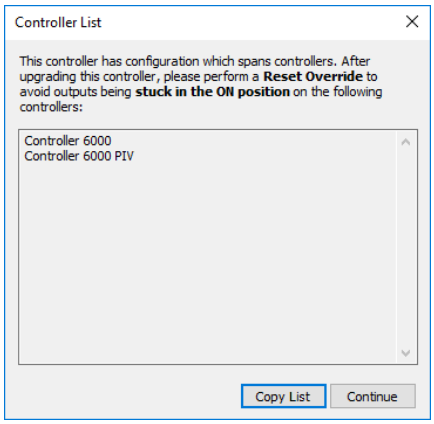
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** on the Controller 6000 that you want to upgrade, and select **Upgrade to 7000...**.



The following warning message displays:



3. Click the **Upgrade to 7000** button.
   Note: The following screen will display if there are Controllers with reflect-ed outputs spanned from the Controller being upgraded. It indicates which Controllers need to be restarted as a list that can be copied and pasted.



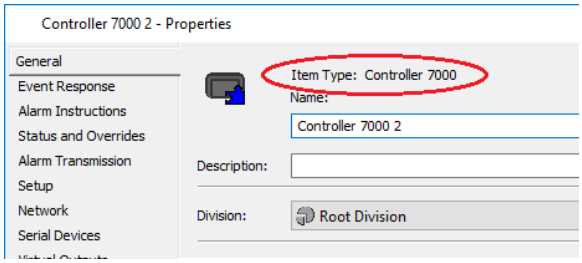
If this screen does display, do the following:

a) Click the **Copy List** button to copy the Controllers list to the clipboard. The following message displays:
"The content has been copied to the clipboard successfully!"

b) Click the **OK** button. The message dialog closes.

c) Paste the copied list to Notepad, etc., and click the **Continue** button to start the upgrade.

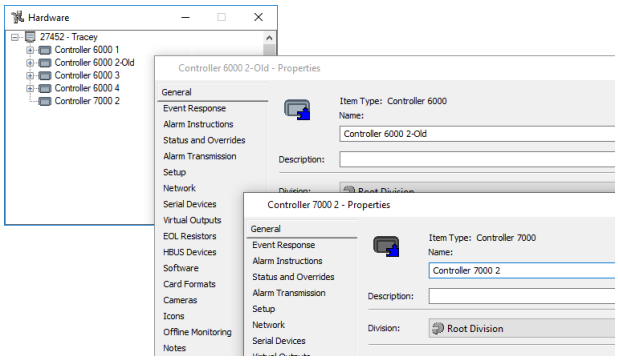
The **General** tab of the Controller properties displays. The **Item Type** is now a Controller 7000.



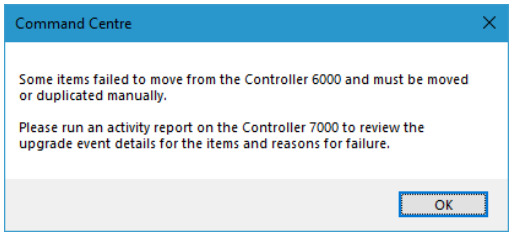
Most of the configuration is copied across from the Controller 6000 item. The exceptions are:

- **Network** tab: Controller MAC Address set to "00 00 00"
- **Software** tab: Fields set to "Use System Default", scheduled upgrade unchecked, USB Use site default checked, HBUS display Language set to "English"
- **Setup** tab: If the Controller 6000 was configured as Starter Kit or 2-Door, when upgraded to C7000 it will set "Restricted Controller" as unchecked and will be disabled by default. This checkbox will only be enabled after clicking the **Apply** or **OK** button.
  To select the restricted controller as “Starter Kit”, you need to remove the C6000 Starter Kit Controller as the customer Command Centre license will only ever allow one Starter kit Controller per site.

4. Change the Controller **Name** if necessary.
   Note: Gallagher recommend that you check the properties of each tab to ensure items are copied over before clicking **Apply**.
5. Click the **OK** or **Apply** button.
   Note: Once you click **OK** or **Apply**, there is no way to undo that action. Communication is disabled for the Controller 6000, (i.e. it is overridden to "Stopped Communication"), to minimise the disrutpion while moving the items over to the Controller 7000. An "Operator Stopped Communication" event is generated.
   Both Controllers display in the Hardware List Window, (i.e. the new Controller 7000 item appears and the Controller 6000 has "**-Old**" added to the end of it’s name).

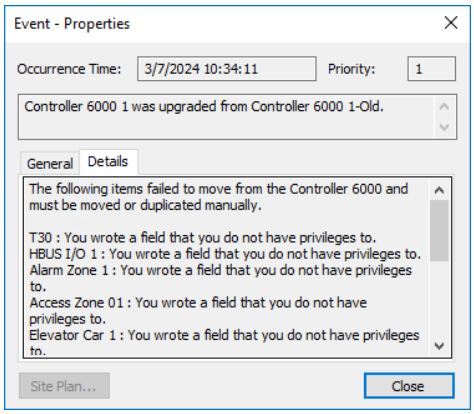


Note: Not all of the configuration is copied over to the C7000, and some items may still be associated with the C6000. Items that are currently under editing cannot be moved during an upgrade. If all items were successfully moved or there were no items to move no message will be shown. However, the summary message below will display advising of any items that were <u>not</u> moved over to the new Controller.

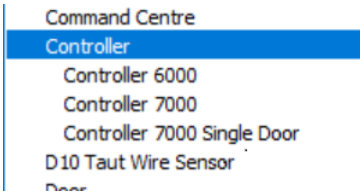


If the C6000 configuration contains FT items that you do not have privileges to write, that FT item will not be updated and the following warning message will display: *"You wrote a field that you do not have privileges to."*

You can open the **Details** tab of the "Controller 7000 Upgraded from Controller 6000" event to see the list of all FT items that you do not have privileges to.



6. On the Controller 7000, click the **Network** tab and provide the correct **MAC Address**.
7. Click the **OK** or **Apply** button.
8. Power off the old Controller 6000.
9. Swap the physical Controller with the new Controller 7000 and devices.
10. Power on the new Controller 7000 with DIP Switch 2 turned on.
    Note: If a DHCP server is present on the network but you want to use BootP to set up the controller, you should enable DIP switch 4 to prevent the controller from obtaining an IP address from the DHCP server.
11. Recheck using the Find Tool to see if all associated items are moved over. Some items may need to be updated manually like Site Plans, Macros, etc.
    Note: You can opt to search either by the different Controller types, or for all Controllers at once.



12. Delete the old C6000. Refer to ***Deleting items*** (on page 3-27) for the procedure.

Result

The Controller 6000 has been upgraded to a Controller 7000.

Note: If software requires updating, refer to ***Device Software*** (on page 27-1) for further detail.

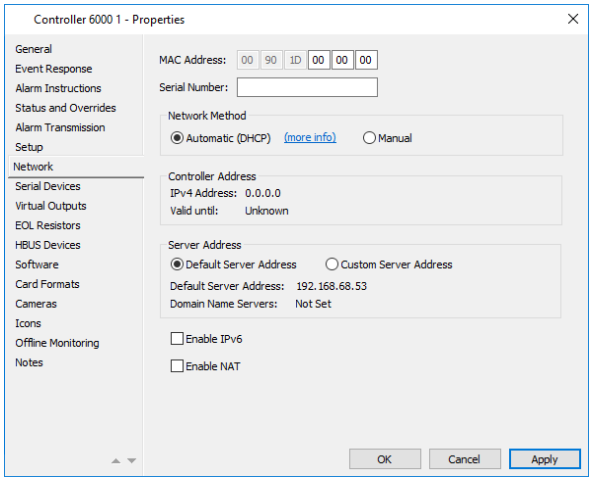
Configuring DNS Servers for Controllers

Introduction

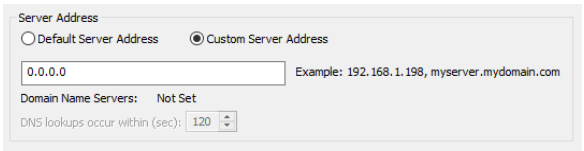
Controllers must be able to make use of Domain Name Servers (DNS) in disaster recovery situations, especially where backup servers reside on different sub-nets. Operators with the “Edit Site” operator privilege can configure DNS at Controller level, (i.e. specifically set for each Controller), using this procedure.

Procedure

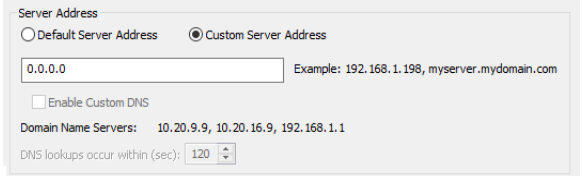
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the Controller you want to configure a DNS Server(s) for.
3. **Right click** and select **Properties**.
4. Click the **Network** tab. By default the fields on this screen are disabled.



5. Click the radio button for the appropriate **Server Address**, (i.e. either **Default Server Address** or **Custom Server Address**).
   If you selected **Automatic (DHCP)** for the "Network Method", and you select **Custom Server Address**, this section will change as shown below:



   Automatic (DHCP) is the preferred "Network Method", but if you selected **Manual**, and you select **Custom Server Address**, this section will change as shown below:



6. Enter either an IP address, (e.g. 192.168.1.198) or a Hostname, (e.g. myserver.mydomain.com), not both.
   Note: The DNS server configuration only appears after you type in a DNS name for the server, as shown below:



7. Tick the **Enable Custom DNS** checkbox if required. Did you tick this option?

If…	then…
no,	the controller will be configured with the same DNS addresses as the server. Go to Step 9.
yes,	the **Primary**, **Secondary** and **Tertiary** fields allow up to three DNS Server IP addresses to be specified, and the order of priority in which they should be referenced, for determining the IP address of the Controller's server. Invalid IP addresses are not accepted. **Notes:** • When the Controller attempts to resolve the hostname the DNS Servers are queried beginning with the Primary one. If that fails to reply, the Secondary one is attempted, and finally the Tertiary. • If all attempts to connect to the specified DNS Servers fail, then the Controller will use the fixed Server IP address it was given. • Only the first IP address returned by a successful DNS reply is used.

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.

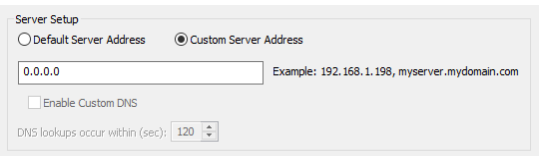
Result

A Controller has been configured for DNS.

Server Address

You can manually assign a server IP address to the controller. This will override the server IP address provided by the DHCP server, given that the controller is online and able to receive communications from Command Centre.
Follow this procedure to assign the server IP address manually.

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** the Controller and select **Properties**.
   The Controller Properties window opens to the **General** tab by default.
3. Click the **Network** tab.
4. Tick the **Custom Server Address** checkbox.
   The server address field activates as shown below:



5. Enter either an IP address, (e.g. 192.168.1.198) or a Hostname, (e.g. myserver.mydomain.com), not both.
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.

Configuring Offline Monitoring

Introduction

This procedure describes how to configure Server to controller offline monitoring, and Inter-controller offline monitoring by assigning several Controllers to a monitoring (or 'parent') Controller. The monitoring Controller will detect when any of the monitored Controllers are not communicating, indicating possible hardware failure.
Note: The number of monitored Controllers that can be assigned to one monitoring Controller is limited to 60. This is to minimise network traffic which could impact on the performance of your Command Centre system.

The main scenarios that require Inter-controller offline monitoring are:

- **Contact ID**
  Where a Controller hosting an Alarm Dialler must detect when other Controllers that can generate alarms that are logged using the same Alarm Dialler, are unable to communicate with it.
  (See ***External Alarm Monitoring*** on page 29-1 for further detail.)
- **Interlocking Doors**
  Inter-controller monitoring can be used to maintain the integrity of Interlock groups in which doors that are interlocked with doors on other monitored Controllers that are out of communication should not be permitted to open.
  (See ***Interlocking Doors*** on page 22-13 for further detail.)

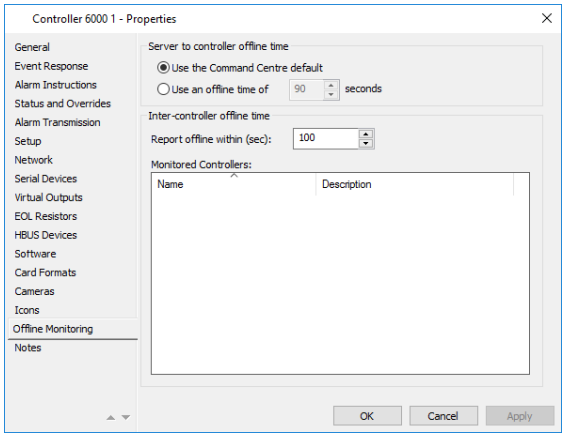
Before you begin

Before you begin this procedure:

- Ensure that the Controllers you want to configure inter-controller monitoring for have already been created in Command Centre (see ***Creating Controllers*** on page 21-2 for the procedure).
- You need to have the “Edit Site” operator privilege for the monitoring Controller and the “View Site” operator privilege for the monitored Controllers.

Procedure

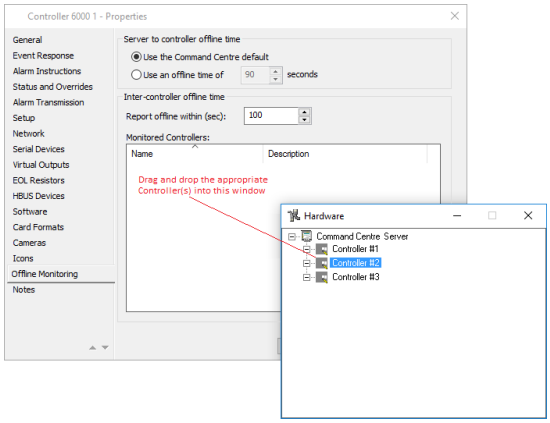
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the required 'parent' Controller, (i.e. the one that you want to configure offline monitoring for).
3. **Right click** and select **Properties**.
   By default the **General** tab displays.
4. Click the **Offline Monitoring** tab.
   Note: All fields on this screen will be read-only if you do not have appropriate privileges to edit Controllers.



5. Do you want to configure Server to controller offline monitoring?
   If **yes**, go to Step 6. If **no**, go to Step 7.
6. Click the appropriate radio button for the **Server to controller offline time**.

Radio button	Description
Use the Command Centre default	This option is set to 90 seconds and cannot be changed.
Use an offline time of	This option allows you to set the offline time. Default = 90 seconds. Valid range = 5 - 360 seconds (6 minutes) **Notes:** • The controller heartbeat interval is inherently set at approximately one third of this time. If three heartbeats fail to detect the controller is online then a Controller Offline alarm will be raised. • If Controller offline time is set to 20 seconds or below the following warning message will display: "Setting the server to controller offline time too low may compromise performance and risk false offline alarms."

7. Do you want to configure Inter-controller offline monitoring?
   If **yes**, go to Step 8. If **no**, go to Step 10.
8. Enter appropriate offline timeout value in the **Report offline within** field.
   Note: The minimum value for this field is 60 seconds and the maximum is 3600 seconds (1 hour). If an out of range value is entered an error message displays. (Default = 100 seconds)
9. From the **Hardware** List Window, select the Controller(s) that you want to be monitored by this Controller.
   Drag and drop them into the **Monitored Controllers** grid.



Note: The monitoring Controller cannot be assigned to itself, (i.e. if you attempt to drag it into the Monitored Controllers grid an error message will display and the assignment will be ignored).

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

A Controller has been configured to monitor other Controller(s) for offline, and the monitored Controller(s) have been configured to send regular heartbeats to the monitoring Controller.
If the monitoring Controller fails to receive a heartbeat from one of the monitored Controllers within the configured timeout period, it creates a "Monitored Controller Offline" alarm in the Alarm Viewer.
Note: It is likely there will be several "Monitored Controller Offline" alarms within a few minutes after applying the initial configuration, or applying any subsequent configuration changes.

Hint

We do not recommend that a group of Controllers be configured to all monitor one another, due to large increases in network traffic. However, if a site does configure Controllers to all monitor each other, the maximum number of Controllers configured this way should probably not exceed 12, but this is dependent on the network quality.

Configuring a Controller for DHCP

Introduction

DHCP (Dynamic Host Configuration Protocol) allows sites to use their own DHCP service to assign IP addresses to their controllers automatically, without physically needing to be at the controller. This procedure describes how to configure DHCP.

Prerequisites

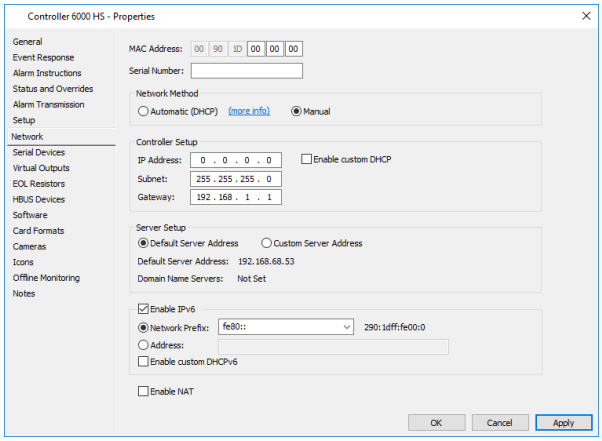
- Ensure that your controller firmware has been updated to the latest version. Refer to either **3E2203 Release Note Controller 6000 vCRx.xx.xxxxxx.pdf** or **3E5746 Release Note Controller 7000 vCRx.xx.xxxxxx.pdf** details. These documents are located in the **`'Documentation'`** directory of the Command Centre installation files.
- For DHCP to work, its configuration must include certain parameters before the Controller will trust the DHCP lease offered to it.
  Refer to **DHCP Server Configuration.pdf** for detailed instructions. This document is located in the **`'Utilities\DHCP'`** directory of the Command Centre installation files.

Procedure

1. Configure **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Are you configuring a new Controller for DHCP, or an existing already configured Controller?

If...	then...
new,	Create the new Controller in Command Centre, as follows: a) Click **Configure** from the menu bar, then **Hardware**. The Hardware List Window opens. b) Right-click **New** > **Controllers** and the appropriate Controller type, (i.e. **Controller 7000**, **7000 Single Door** or **6000**). The Controller Properties window opens to the **General** tab by default. c) Enter the Controller name, short name and description in the **Name**, **Short Name** and **Description** fields. d) Select the appropriate division for the Controller from the **Division** drop-down list. e) Click the **Controller Address** tab. f) Enter the controller's MAC Address in the **MAC Address** field, and go to step 3.
existing,	**Right click** the Controller you want to configure DHCP for, and select **Properties**. The Controller Properties window opens to the **General** tab by default.

3. Click the **Network** tab.



4. Configure the settings on this screen as appropriate.

If you want to enable DHCP for...	then...
IPv4,	tick the **Enable custom DHCP** checkbox. The **IP Address**, **Subnet** and **Gateway** fields deactivate, and a **Valid until** section appears and displays 'Unknown'. **Note:** After you have clicked **Apply**, the **Valid** until value should change from 'Unknown' to a date and time. This date and time is the fixed length of the lease determined by DHCP settings. If **Valid Until** still displays 'Unknown', check that DHCP services are running and configured appropriately.
IPv6,	g) Ensure the **Enable custom DHCP** checkbox is unticked. h) Tick the **IPv6 Enabled** checkbox. The **Network Prefix** and **Address** fields activate. i) Tick the **Enable DHCPv6** checkbox. The **Network Prefix** and **Address** fields deactivate.

If you want to enable DHCP for...	then...
IPv4 and IPv6,	a) Tick the **Enable DHCP** checkbox. The **IP Address**, **Subnet** and **Gateway** fields deactivate and a **Valid until** section appears and displays 'Unknown'. **Note:** After you have clicked **Apply**, the **Valid until** value should change from 'Unknown' to a date and time. This date and time is the fixed length of the lease determined by DHCP settings. If **Valid Until** still displays 'Unknown', check that DHCP services are running and configured appropriately. b) Tick the **IPv6 Enabled** checkbox. The **Network Prefix** and **Address** fields activate. c) Tick the **Enable DHCPv6** checkbox.

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.
6. Refer to the following table to complete your configuration.
   What Controller are you using?

If a...	then...
a deployed and online controller running v7.80 (or later) firmware,	no further action is required. The controller will automatically switch to DHCP as soon as it receives its new configuration from Command Centre.
a new Controller,	a) Power on the Controller. b) When the controller Run LED flashes to indicate normal operation, (i.e. 500ms on, 500ms off), turn dip switches 2 and 3 off.

Note: Once you enable DHCP, and the controller has successfully been assigned an IP address, several fields will be populated on the **Network** tab depending on your DHCP configuration.

Enabling DHCP for a new Controller 6000 using the wizard

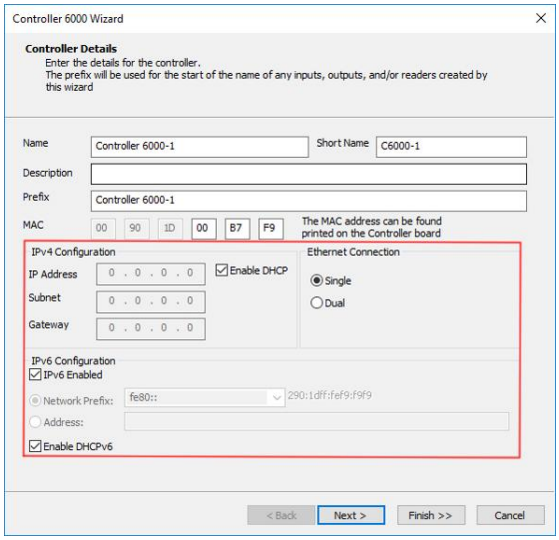
Introduction

When setting up a new controller in Command Centre, you can enable DHCP for IPv4, IPv6, or both. Follow this procedure to access DHCP in Wizard.
Note: For DHCP to work, its configuration must include certain parameters before the Controller will trust the DHCP lease offered to it. Refer to **DHCP Server Configuration.pdf** for detailed instructions. This document is located in the `'Utilities\DHCP'` directory of the Command Centre installation files.

Procedure

1. Click **Wizards** from the menu bar, then **Configuration Wizard**.
2. In the Configuration Wizard window, ensure that **Controller** is selected.
3. From Controller Wizard drop-down menu, select **Controller 6000**.
4. Click **Start**. The Controller details pop-up window displays.

5. In the Controller 6000 Wizard enter controller **Name**, **Short Name** (optional) and **Description** (optional).
6. Enter the Controller MAC Address in the **MAC** field.
7. Select **Single** or **Dual** as Ethernet Connection.



8. Configure as required.

If you want to enable DHCP for...	then...
IPv4,	tick the **Enable DHCP** checkbox. The **IP Address**, **Subnet** and **Gateway** fields deactivate.
IPv6,	a) Tick the **IPv6 Enabled** checkbox. The **Network Prefix** and **Address** fields activate. b) Tick the **Enable DHCPv6** checkbox. The **Network Prefix** and **Address** fields deactivate.
IPv4 and IPv6,	a) Tick the Enable **DHCP** checkbox. The **IP Address**, **Subnet** and **Gateway** fields deactivate. b) Tick the **IPv6 Enabled** checkbox. The **Network Prefix** and **Address** fields activate. c) Tick the **Enable DHCPv6** checkbox.

9. Click **Next**.
10. Complete **Controller Details - Part Two**.
11. Click **Next** to add HBUS Devices to the Controller, otherwise click **Finish**.
12. Do you want to save this configuration as a template for future use?

If...	then...
yes	a) Enter the template name in the **Template Name** field. b) Enter the template description in the **Template Description** fields. c) Select the **Template Division** from the drop-down menu. d) Click **Save**, or **Save As** to save your template.
no	click **Finish**.

Note: For a detailed guide on creating a controller using the Wizard, refer to Configuration Wizard.

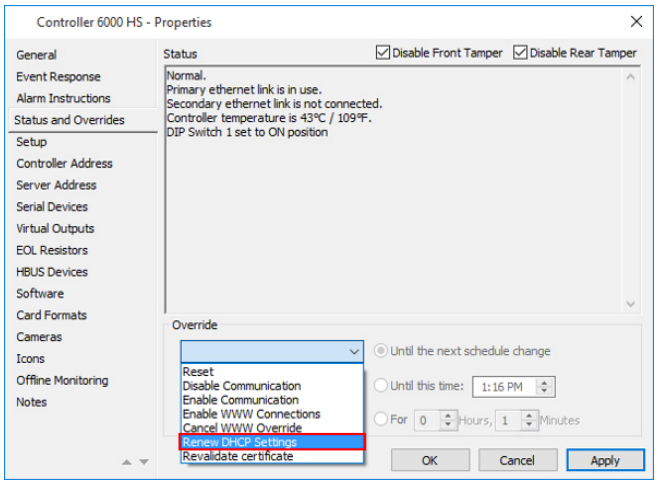
Renewing DHCP Settings

Introduction

Controllers will periodically renew their DHCP leases, but if you need it to happen immediately you can force it with an override.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** the Controller and select **Properties**.
   The Controller Properties window opens to the **General** tab by default.
3. Click the **Status and Overrides** tab.



4. Select **Renew DHCP Settings** from the drop-down list.
   Note: The **Renew DHCP Settings** option will only appear in the drop-down list if **Automatic (DHCP)** was selected as the "Network Method" on the **Network** tab.
5. Click **Override Now**.
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.

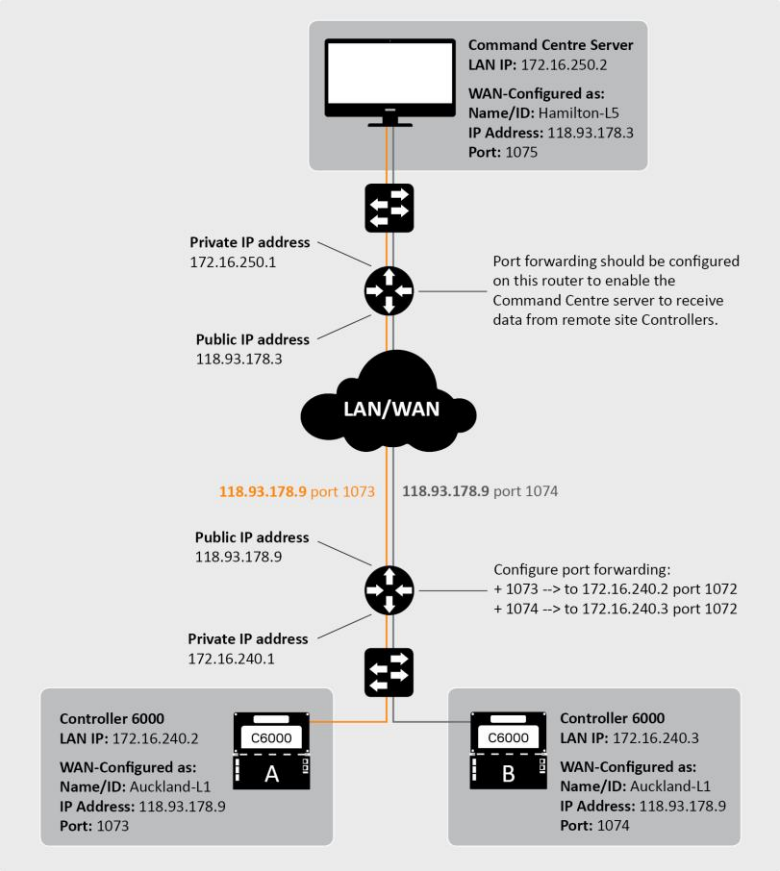
Configurable Ports - NAT Solution

Introduction

The 'NAT Solution' allows Command Centre to communicate with multiple Controllers on different networks. This integration also enables Controllers on different networks to communicate with each other using the WAN IP address and the WAN port. Devices on the same network use the LAN IP address to communicate. If a device has a different WAN ID/Name, it will not be able to communicate with other devices configured with WAN on the same network.

Deployment Architecture

Note: This diagram is a simplified example for a single remote site. Sites with more than one remote site will require additional routing configuration.



Hamilton-L5 network:

- Each device has the same WAN Name/ID.
- Each device has the same WAN IP address (10.2.3.5).
- Each device has a different WAN port.
- Controller C has different WAN Name/ID (Nelson-L3); therefore, it will not be able to communicate with other devices in the Hamilton-L5 network.

WAN Properties	Function
Name/ID	A label which determines the network the device is on. Any value for the Name/ID is acceptable. All devices on the same network must have the same WAN Name/ID. Two networks cannot have the same WAN Name/ID.
IP Address	The WAN IP Address is the NAT's externally-addressable IP address. Also referred to as the public IP address.
Port	The WAN Port for a device must be unique within a network. The device's WAN IP address the and WAN port are used by devices on different networks to establish connection.

Prerequisites

Before you add the WAN configuration to the Command Centre server and the Controllers, it is recommended to set up port forwarding on your local and remote routers.

- Set up port forwarding on your local site router (Command Centre server site) to accept data on port 1072 from remote sites and forward it to Command Centre server. For each remote site, a separate rule is required.
- Set up port forwarding on your local site router (Command Centre server site) to accept data on the appropriate port and forward it to a local Controller.
- Set up similar port forwarding on your remote sites to allow Communication with the local and remote sites.

Configuring remote site Controllers

To minimize configuration error, use one of the following methods to configure a new remote site Controller:

To…	then…
Configure remote site Controller using local subnet,	a) Power on your Controller and bring it online (normally) using the same subnet configuration as the Command Centre server. b) Once the Controller is online, configure the Controller (remote ones only) with the appropriate remote WAN and LAN IP addresses. **Notes:** ▪ Only save your configuration once you have completed configuring both WAN and LAN IP addresses. ▪ Once you have entered the remote IP addresses, the Controller will go offline as it can't relate to those IP addresses. **c)** Ensure that DIP switch 6 is off to avoid loss of Configuration. **d)** Disconnect the Controller from the Local network and connect it to the remote site network. The Controller will come online.
access remote site Controller's default IP interface using a browser,	a) Turn the Controller DIP switches 2 and 3 on. **Note:** DIP switches 2 and 3 sets the Controller to the default settings. b) Connect the Controller to a PC using an ethernet cable. Ensure that the PC is on the same subnet as the Controller. c) Power on the Controller and use a browser to navigate to 192.168.1.199 (Controller's default IP). **Note:** You will require a username and password, contact Gallagher tech support for these credentials. d) Via this interface, configure the LAN IP address of the Controller. e) Turn DIP switches 2 and 3 off. f) On the Command Centre server, create a Controller, then add the WAN configuration. **Note:** Finish all Controller config, then save.

Configuration

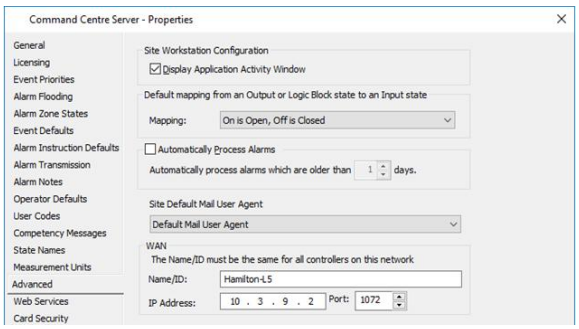
To configure NAT Solution, perform the following procedures:

- ***Add WAN Configuration to the Command Centre Server*** (next)
- ***Add WAN Configuration to the Controllers*** (on page 21-44)

Add WAN Configuration to the Command Centre Server

Note: This configuration is only required if a remote Controller needs to connect to the Command Centre server using WAN.

1. Click **File** from the menu bar, then **Server Properties**.
   The Command Centre Server Properties window displays.
2. Click the **Advanced** tab.

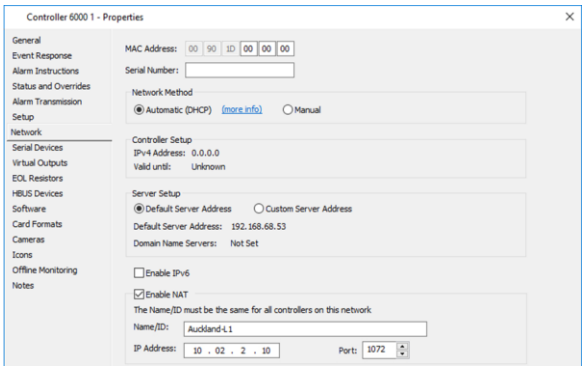


3. Enter the WAN Name/ID in the **Name/ID** field.
   The IP Address and the Port fields activate.
4. Enter the WAN IP address in the **IP Address** field.
5. Enter the WAN port in the **Port** field. The valid range is 1024 – 65535.
6. Select **OK** to save your changes.

Add WAN Configuration to the Controllers

Perform the following procedure to add WAN configuration to the Controller:

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Double-click on the appropriate Controller.
   The Controller Properties window displays to the **General** tab by default.
3. Select the **Network** tab.



4. If not already selected, click the **Enable NAT** checkbox.
   The **Enable NAT** section expands.
5. Enter the WAN Name/ID in the **Name/ID** field.
   The IP Address and the Port fields activate.
   Note: If the Controller is on the same network as the Command Centre server, this field should be the same as in the Server Properties.
6. Enter the WAN IP address in the **IP Address** field.
7. Enter the WAN port in the **Port** field. The valid range is 1024 – 65535.
8. Select **OK** to save your changes.

Creating Devices

Equipment connected to the RS-485 building cabling are classed as devices; Readers, Terminals, Sensors, etc.

These devices are added using the **Hardware** List Window.

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...**
3. From the displayed sub-menu(s), select the appropriate device type.
   For example: **HBUS Devices**>**HBUS I/O**

   By default, the **General** tab displays.
4. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
5. Configure devices as required.
   Note: The HBUS 8-In 4-Out Board and HBUS 8-In Board can be mounted in a Gallagher cabinet and used in conjunction with a Tamper Board. Only one of the expansion boards can be connected to the Tamper Board. Once connected, the Tamper Board will become the monitoring board for the whole cabinet. Therefore, for the expansion boards that are **NOT** connected to the Tamper Board, click the **Status and Overrides** tab and tick the **Disable Tamper** checkbox.
   This will prevent incorrect (or continuous) tamper alarms being generated by the expansion boards not connected to the Tamper Board.
6. Click **OK**.

Assigning Device Software to devices

You can assign device software to Controllers and Digital Cameras.

Refer to ***Assigning Device Software to devices*** under the Device Software topic for the procedure.

Note: It is recommended you link a device to an Alarm Zone before assigning device software to it. Otherwise, the software version number will not display in the **Software** tab of the device's properties.

Configuring EOL Resistors for devices

Introduction

This procedure describes how to configure End-of-line (EOL) resistances for a device in Command Centre. EOL resistances are configurable via Command Centre for the following hardware devices:

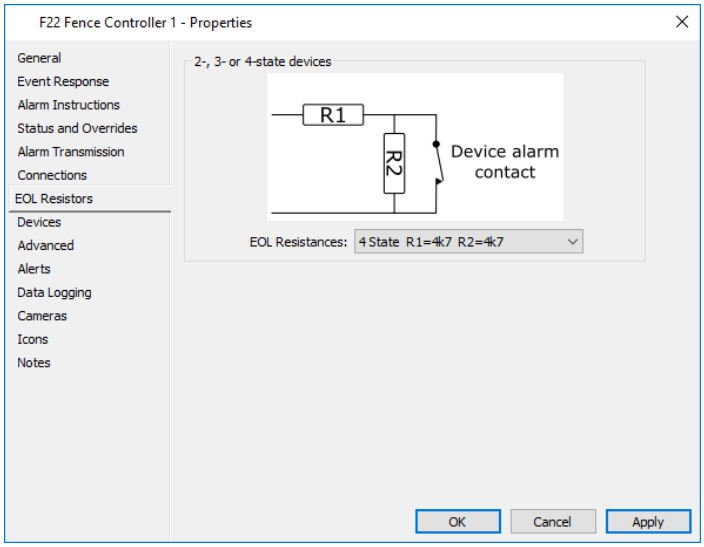
- Gallagher Controller 6000s
- Gallagher Controller 7000s
- Gallagher Controller 7000 Single Door
- Gallagher HBUS I/O Interfaces
- Gallagher HBUS F31/F32/F41/F42 Fence Controllers
- Gallagher HBUS F22 Fence Controllers
- Gallagher QuickSwitch ME1502 Boards

This functionality makes it easier for installers to add Command Centre devices to sites whose input EOL resistor networks are suited to work with legacy Gallagher or competitors equipment.

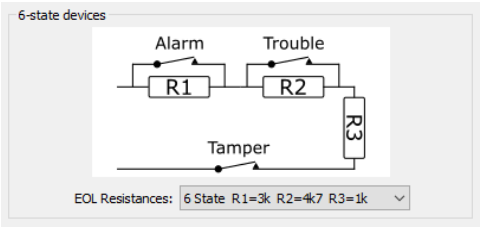
Note: This procedure assumes that the device you want to configure the EOL resistances for has already been created in Command Centre. However, if you have not yet created the device, refer to the appropriate procedure first, (i.e. ***Creating Controllers*** on page 21-2 or ***Creating Devices*** on page 21-45).

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the required device, (i.e. the one you want to configure the EOL resistance for).
3. **Right click** and select **Properties**.
4. Click the **EOL Resistors** tab.
   The following example is the EOL Resistors tab for an F22 Fence Controller.



This tab provides an **EOL Resistances** drop-down list of pre-calculated sets of resistor values for the installer to select a value from, and a circuit diagram to show which resistors are configured with which values.
Note: For most devices, this tab only provides a drop-down list of EOL resistor values for **2, 3 or 4-state devices**. However, for Controller 6000s, Controller 7000s and HBUS I/Os, in addition to resistor values for **2, 3 or 4-state devices**, it also has a drop-down of resistor values for **6-state devices**, shown below:



Each set of resistor values is one of the following:

Set of resistor values	Provides...
6 state Inputs using 3 resistors	for masked, fault, tamper open-circuit, tamper short-circuit, open and closed states
4 state Inputs using 2 resistors	2 kinds of tamper detection
3 state Inputs using 1 resistor	only 1 kind of tamper detection depending on NO or NC selection (Normally Open/Closed)
2 state Inputs using no resistors	no tamper detection

5. Select the required resistor values from the drop-down list.
   Note: The values you select will apply to all the Inputs on that particular device. In the case of Controllers, the resistor values will apply to the Inputs on the Controller itself, and not any attached devices.
6. Click **OK**.

Result

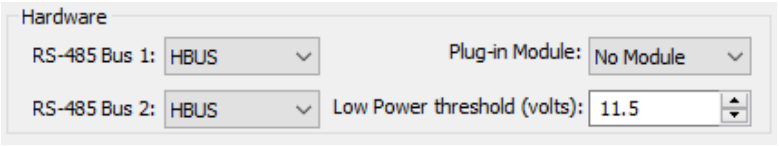
EOL resistance has been configured for a device.

Linking devices to Controllers

The following table indicates the readers and hardware that the Controller supports:

Readers	Hardware
HBUS Reader	HBUS Alarms Only Terminal
HBUS Terminal	HBUS F22 Fence Controller
OSDP Reader	HBUS 8-In 2-Out Door Module
Cardax IV Reader	HBUS 8-In Board
Third Party Reader	HBUS 8-In 4-Out Board
Morpho Biometric Reader	HBUS 16-In 16-Out Board
	HBUS Z10 Tension Sensor Group
	Schlage PIM
	Aperio Door
	Z20 Disturbance Sensor
	D10 Taut Wire Sensor
	Alarm Dialler

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the required Controller, (i.e. the one devices are connected to).
3. **Right click** and select **Properties**.
4. Click the **Setup** tab, and select the correct **RS-485 Bus** type for the RS-485 devices connected to the Controller.



   If the Controller has a Plug-in Module connected, select the correct Plug-in Module. Additional tabs appear in the properties when a Plug-in Module is selected.
   Note: When either of the RS-485 Buses or the Plug-in Module type are changed then an appropriate error message will display if there are any devices configured or detected on the bus/module that would be incompatible with the type of bus/module that is being changed.

   The **Low Power threshold** field can be altered to set the level at which a low voltage alarm will be generated for the Controller.

5. What **Plug-in Module** did you select on the **Setup** tab?

If...	then...
"No Module", "4H Module" or "8H Module"	go to Step 6.

If...	then...
"4R Module" or "8R Module"	click the **Readers** tab. Click within the edit box(es) of the reader number(s) and select the appropriate reader. Go to Step 6.

6. What **RS-485 Bus** type did you select?

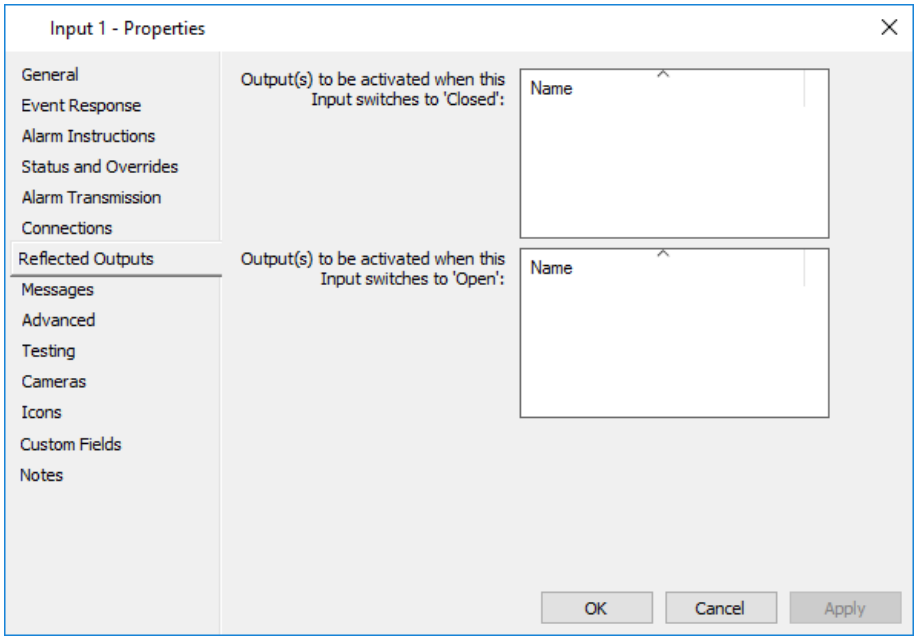
If...	then...
HBUS	refer to the topic ***Configuring HBUS Devices*** (on page 21-65).
Aperio	refer to the topic ***Assigning an Aperio Door to a Controller*** (on page 67-23).
OSDP	refer to the topic ***Assigning an OSDP Compliant Reader to a Gallagher Controller*** (on page 69-6).
Schlage	refer to the topic ***Assigning Schlage devices to a Gallagher Controller*** (on page 68-10).
Sensor	refer to the topic ***Assigning Z20 and D10 sensors to a Controller 6000 or 70000*** (on page 56-20).

7. Click the **OK** button.
8. Repeat the procedure for all devices associated with this Controller.

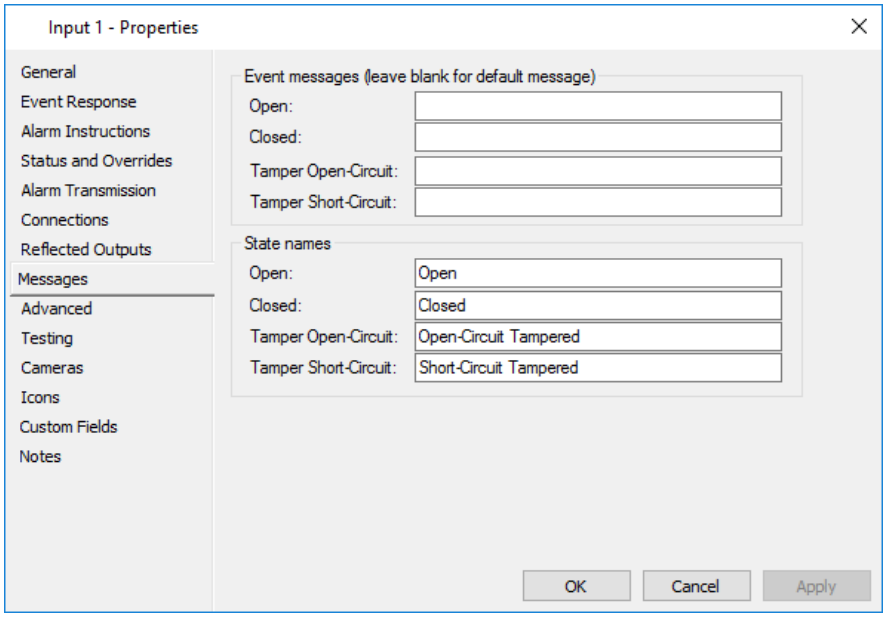
Creating Inputs and Outputs

Inputs monitor a state, Outputs change a state.
Note: Most of the screen shots in this topic are for an Input, and while they may differ slightly for an Output the procedure is still the same.

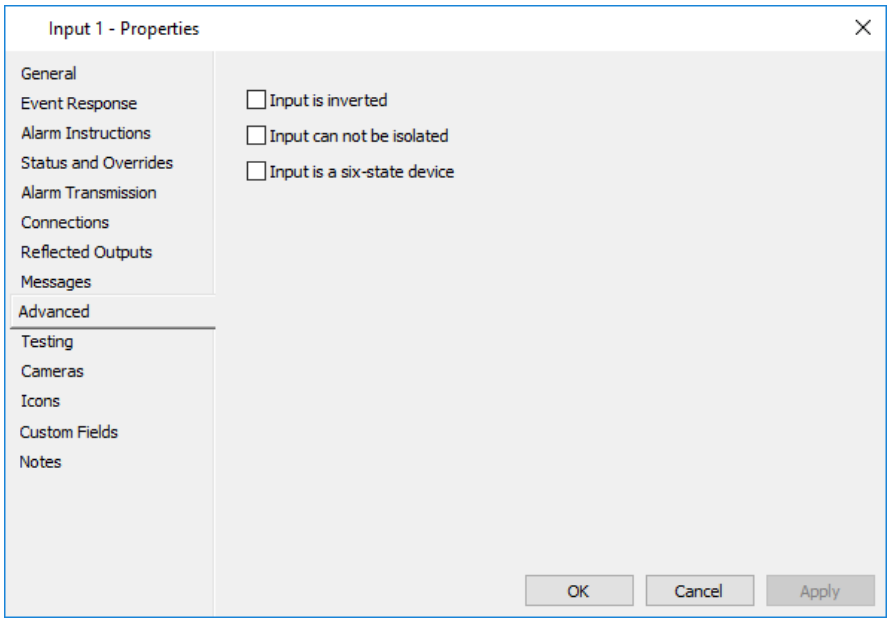
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Input/Output**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 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. Are you creating an Input or an Output?
   If an **Input**, go to Step 7.
   If an **Output**, go to Step 9.
7. Click the **Reflected Outputs** tab.



8. Drag and drop the appropriate Output(s) into the two grids.
   The top grid lists the Output(s) that reflect the current state of the Input, and the bottom grid lists the Output(s) that reflect the opposite state of the Input.
9. Click the **Messages** tab.



10. Enter the state and event names (if different from the site-wide default), that will display in Command Centre when this Input/Output is activated and deactivated.
11. Click the **Advanced** tab.
12. Are you creating an Input or an Output?
    If an **Input**, go to Step 13.
    If an **Output**, go to Step 14.
13. The Input **Advanced** tab displays:

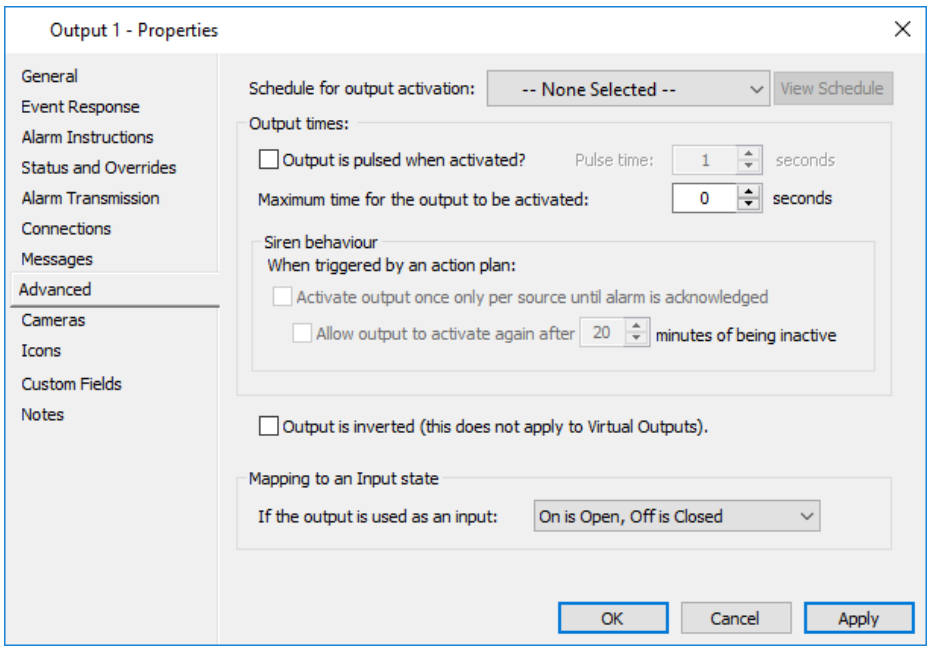


Tick the checkboxes as required, then go to Step 19.

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).

Checkbox	Description
Input cannot be isolated	If checked, the Input will not be ignored when an Alarm Zone is armed with the 'Isolate' option.
Input is a six-state device	If checked, the 6-state EOL Resistance settings will be used for this input. If left unchecked, the 4-state settings will be used.

14. The Output **Advanced** tab displays:



Configure the behaviour of the Output as required.

Field / Checkbox	Description
Schedule for output activation	This drop-down list contains all Schedules in the operators Division(s). The Output can be turned on and off at different times of the day by changing the Schedules Output field. **Note:** The **View Schedule** button beside this field only becomes enabled once a Schedule is selected. When clicked, the **Calendar** tab of the selected Schedule opens.
Output is pulsed when activated?	Valid range is 1 - 86400 seconds (24 hours). Default = unchecked. When checked the default value becomes 1 second. If checked, the following occurs: • the **Maximum time for the output to be activated** field is disabled. • the **Pulse** option is enabled on the Output context menu (via right clicking on the Output from the **Hardware** List Window). Selecting the Pulse option from the context menu activates the Output for the configured number of seconds and then deactivate the Output.

Field / Checkbox	Description
	When this Output is activated (not by manual override), then the Output will stay activated (pulsed) for the configured number of seconds, regardless of whether another event would normally deactivate the Output prior to the pulse time elapsing.
Maximum time for the output to be activated	Defaults to 0 seconds, and the maximum value is 86400 seconds (24 hours). If a value greater than 0 is entered is this field, when the Output is activated (not by manual override), then the Output will deactivate when the configured number of seconds has elapsed, unless the Output is deactivated before that time.
Siren behavior	This allows the operator to specify: • if they want each input in an Alarm Zone to **Activate output once only per source until alarm is acknowledged**, (i.e. an action that would turn off the output if it was turned on due to an alarm source. With default Action Plan configuration, this includes disarming the Alarm Zone as well as acknowledging or processing an alarm). • the reset time, (i.e. **Allow output to activate again after xx minutes of being inactive**). The siren is allowed to re-activate after this many minutes as soon as any alarm happens (i.e. there is no restriction on it having to be from a different source). Default = 20 minutes, and the range is 1 - 720 minutes. **Note:** The Reset time is ignored when the output is triggered by a manual override. The time resets each time the output is triggered. • See the siren behavior diagram (at the end of this procedure) for further explanation of this functionality.
Output is inverted	If checked, this reverses the behaviour of the physical Relay only, (i.e. When an inverted Output is turned ON in Command Centre, the Relay is de-energised. When an inverted Output is turned OFF in Command Centre, the Relay is energised. The messages and status of the inverted Output in Command Centre do not change: Output ON always =  Output OFF always = 

Field / Checkbox	Description
Mapping to an Input state	Allows you to specify the default state translation to be used when the Output is used in place of an Input, (i.e. when the Output is used where an Input is expected). When the Output is used where Command Centre expects an Output, the Output's **Mapping to an Input state** setting is not applied.

15. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Input/Output.
    For further details see ***Cameras tab*** (on page 3-24).
16. Click the **Icons** tab if you want to change the Icon Set for this Input/Output.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
17. Click the **Notes** tab if you want to add a note(s) about this Input/Output.
    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.

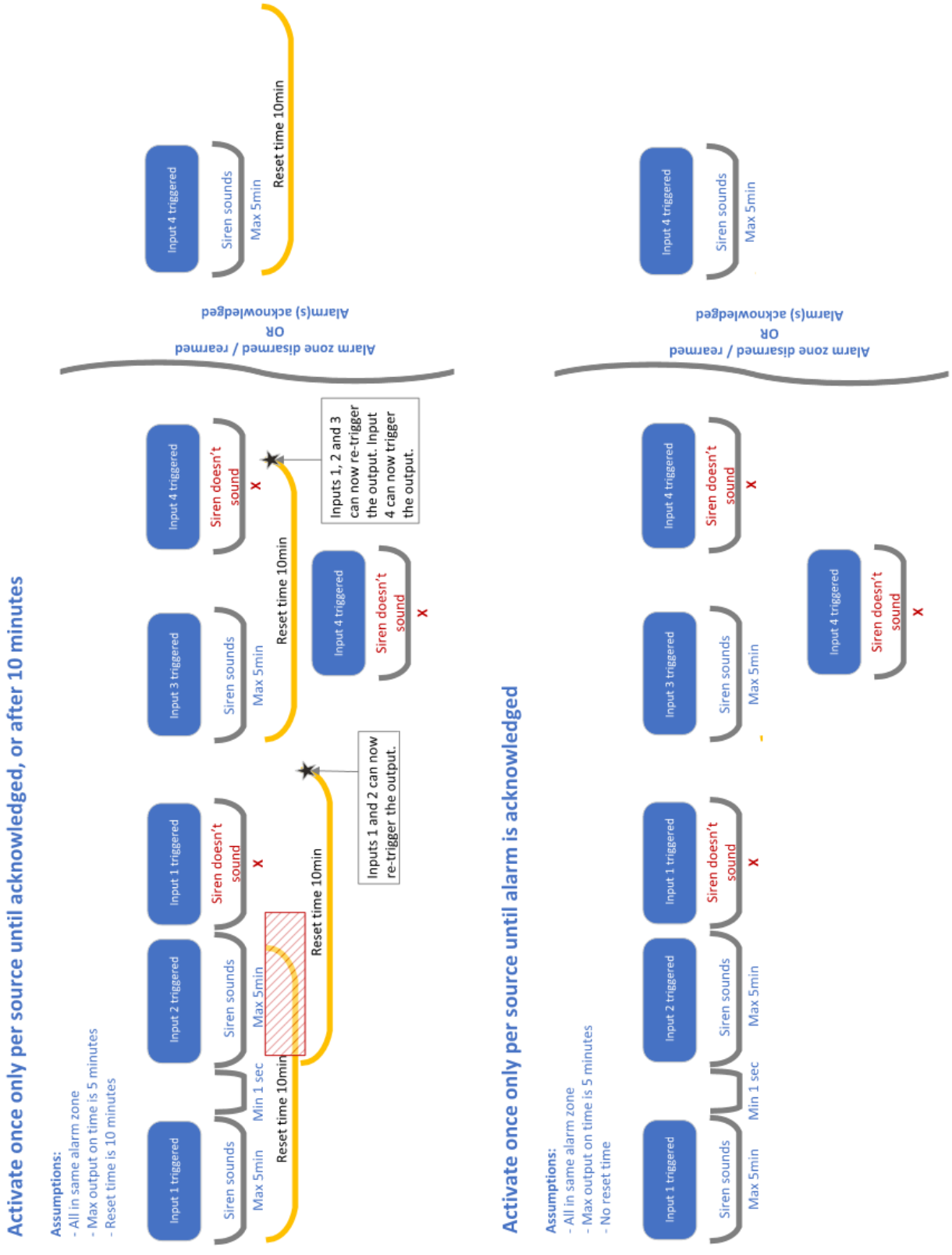
Hint

Manual Overrides
Manual overrides of Outputs to ON or OFF (either from the Outputs context menu, from the Output properties **Status and Overrides** tab, or by a Macro), are not affected by the time values on the Outputs **Advanced** tab.

If a manual override is performed from...	then...
the Outputs context menu	it will remain until the next schedule change (if the Output has a Schedule assigned), otherwise the override will remain until some other event turns the Output OFF, (e.g. an Input closing, a cancel override, etc.).
the Outputs **Status and Overrides** tab	it can be configured either until the next schedule change or for a set period of time (maximum 23 hours, 59 minutes).

You can also configure a Macro to run a Pulse override on an Output, in which case the Pulse time on the Outputs **Advanced** tab is used.

Siren behaviour diagram


Activate once only per source until acknowledged, or after 10 minutes
Assumptions:
- All in same alarm zone
- Max output on time is 5 minutes
- Reset time is 10 minutes
Input 1 triggered
Input 2 triggered
Input 1 triggered
Input 3 triggered
Input 4 triggered
Siren sounds
Max 5min
Min 1 sec
Siren doesn't sound
X
Reset time 10min
Inputs 1 and 2 can now re-trigger the output.
Inputs 1, 2 and 3 can now re-trigger the output. Input 4 can now trigger the output.
Alarm zone disarmed / rearmed
OR
Alarm(s) acknowledged
Activate once only per source until alarm is acknowledged
Assumptions:
- All in same alarm zone
- Max output on time is 5 minutes
- No reset time

Linking Inputs and Outputs to devices

Sensors can connect to any device that contains an Input. Equipment activators can connect to any device that contains an output.

The table below shows which devices contain inputs and outputs, and how many of each.

Device	Inputs	Outputs
Controller 6000/7000		
- 4R/4H	12	4
- 8R/8H	24	8
Controller 7000 Single Door		
- RS-485	6	2 *
- Wiegand	5	2 *
* using a Controller 7000 Single Door Relay Board.		
HBUS 8-In 2-Out Door Module	8	2
HBUS 8-In Board	8	0
HBUS 8-In 4-Out Board	8	4
HBUS 16-In 16-Out Board	16	16
HBUS F31 Fence Controller	2	4
HBUS F32 Fence Controller	3	5
HBUS F41 Fence Controller	2	4
HBUS F42 Fence Controller	3	5
HBUS F22 Fence Controller	3	2

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Locate the device to which you want to link the input/output.
3. **Right click** and select **Properties**.
4. Click the **Connections** tab. The window displayed will vary depending on the device you selected in Step 2.
   Note: Instead of a **Connections** tab, a Controller 6000 with a plug-in module selected, (i.e. 4H, 8H, 4R or 8R module) has an **Outputs** tab (to link Outputs) and an **Inputs** tab (to link Inputs). Click these as appropriate.
5. For the appropriate Input/Output, click within the edit box.
   From the displayed drop-down menu, select the input/output name.
6. Click **OK**.

Creating Readers

Introduction

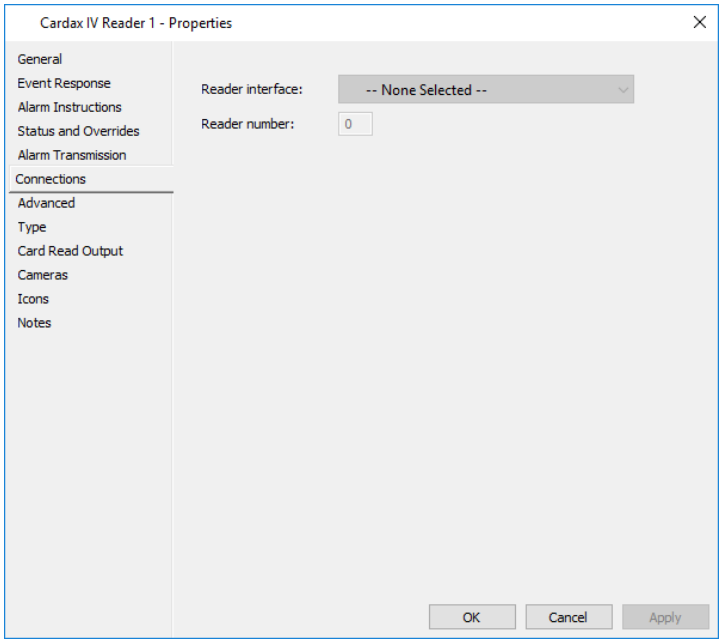
There are a number of different readers that can be configured in Command Centre, as follows:

- Cardax IV Readers
- Third Party Readers
- HBUS Readers
- HBUS Terminals
  Refer to ***Configuring an HBUS Terminal*** (on page 21-75) for the procedure.
- HBUS Contact Card Readers
  Refer to ***Configuring an HBUS Contact Card Reader*** (on page 21-109) for the procedure.
- Morpho Biometric Readers
  Note: Your license file will determine whether or not you can configure biometric readers for your site. Refer to ***Creating a new Morpho Biometric Reader*** (on page 64-9) for the procedure.
- OSDP Readers
  Note: The Open Supervised Device Protocol (OSDP) Integration is covered in the Integrated Systems section. Refer to ***Configuring an OSDP Reader*** (on page 69-2) for the procedure.

This procedure describes how to configure a reader in Command Centre.

Procedure

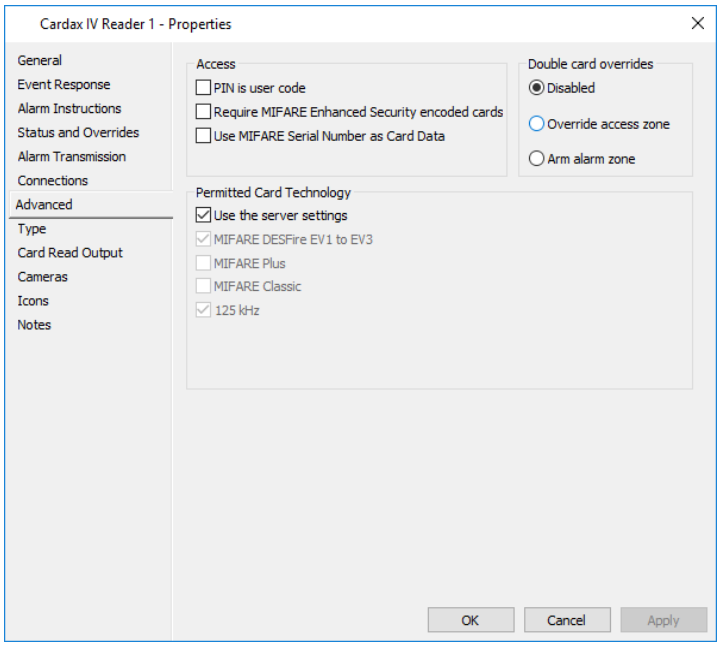
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...**, and then the appropriate reader type.
   By default the **General** tab displays.
   Note: You may need to select the device type from the sub-menu before selecting the reader type, (e.g. HBUS Devices).
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Are you configuring a Third-Party Reader?
   If **yes**, go to Step 7.
   If **no**, go to Step 5.
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.
   Note: The screen example shown is that of the Cardax IV Reader. This tab will look slightly different for other reader types.



The fields that appear depend on the type of reader, as follows:

If a...	then there will be a...
Cardax IV or Third Party Reader,	**Reader interface** and **Reader number** field, which will be populated once you assign this reader to a device, which is explained later in this procedure.
HBUS Reader,	**Controller** and **HBUS Serial Number** field. a) Select the Controller 6000 or 7000 you want to assign this reader or terminal to, from the **Controller** drop-down list. **Note:** HBUS readers and terminals can be created via the **HBUS Devices** tab of a Controller 6000 or 7000. In which case the **Controller** field would be pre-populated with that Controller name. b) Enter a 10 character hexadecimal string in the **HBUS Serial Number** field. **Note:** The HBUS serial number is optional, however the reader or terminal will be considered as not properly configured unless one is entered. c) If you click the **Apply** button, software version numbers display. The **Configured Version** is the version of the device software in the configured Controller FTS file,(i.e. not the version of the Controller software). The **Current Version** is the version of software as last reported by the reader or terminal itself.

8. Click the **Advanced** tab.
   Note: The screen example shown is that of the Cardax IV Reader. This tab will look slightly different for other reader types.

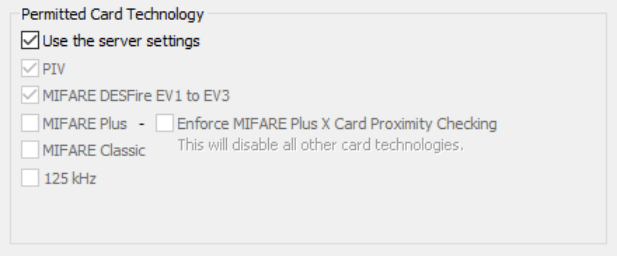


9. Is there a **PIN is user code** option for this reader?
   If **yes**, go to Step 10.
   If **no**, go to Step 12.
10. Terminals can be configured as keypads for readers that have no keypad. As part of this functionality, you can configure a user code to be used for gaining access in place of a PIN, for added security.
    If you want to use this functionality, check the **PIN is user code** checkbox.
11. With **PIN is user code** checked, the user code will be required in place of a PIN for any transactions at the reader which would normally require a PIN. This includes door access, overrides and Terminal logon.
    Note: For Access Mode and Arming local overrides, the HBUS Terminal and HBUS Contact Card Reader uses the Log On Credentials configured on the **Welcome Screen** tab. In this instance the PIN is usercode functionality is not applicable.
12. What type of reader are you creating?

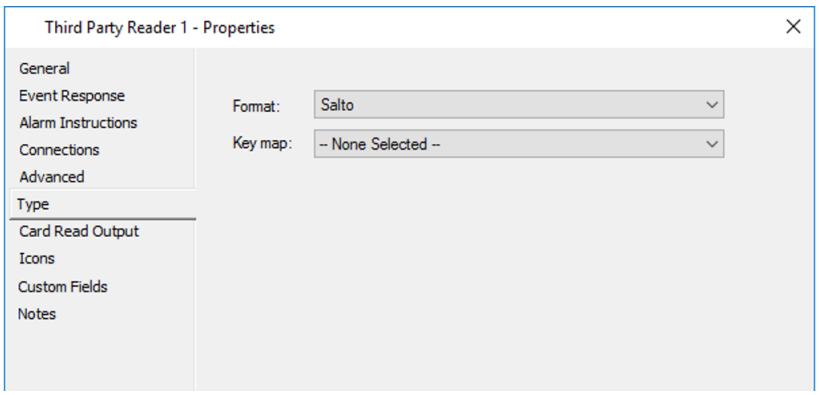
If...	then...
Third Party Reader,	go to Step 13.
Cardax IV or HBUS Reader,	the following two checkboxes are also available. **Note:** These features cannot be used at the same time, therefore when one of these checkboxes is ticked, the other checkbox is disabled. **Require MIFARE Enhanced Security encoded cards** When checked, the reader is instructed to only accept cards that have the enhanced security data when deciding whether to grant a cardholder access. The MIFARE Enhanced security key is configured on the **Card Security** tab of the Server Properties. **IMPORTANT:** When this checkbox is unchecked, the reader will be instructed not to send the enhanced security data to the Controller, even if present.

If...	then...
	Leave this checkbox unchecked in the following situations: 1. When not using the MIFARE Enhanced Security feature or when not using it for part of a site. 2. When some cardholders requiring access using this reader have not yet had their cards re-encoded. It is important to remember to enable the setting once all cards have been re-encoded. Disabling this setting will also allow cards encoded at sites using the MIFARE Enhanced Security feature to be used at sites who are not using this feature. In the event of this being enabled, all types of cards, (i.e. high or low security), will be denied with an event saying *"Denied - MIFARE High Security Card Required at [Door]"*. To enable both types of card to be used uncheck the checkbox for the Door Reader. **Use MIFARE Serial Number as Card Data** HBUS Readers, Cardax IV Readers and IDT MIFARE Readers can be set to read the Card Serial Number (CSN) from a MIFARE Card and use it to identify a Cardholder in Command Centre. When enabled, this allows the reader to send the CSN as Cardholder identification to the Controller if it does not detect any other form of Cardholder identification on the card. For this feature to work for Cardax IV Readers connected to Universal Reader Interfaces (URI), on the URIs **Readers** tab 'Universal' must be selected from the **Format** drop-down list. **IMPORTANT:** If using the Card Serial Number (CSN) functionality with Cardax IV MIFARE cards, the CSN may be transmitted where an incorrect card read of the Gallagher data occurs. **Additional required configuration:** For the Controller to interpret the CSN as a Cardholder's card number, you also need to configure and assign a Universal Card Format. Once this is configured, you can assign cards to Cardholders using the CSN as the card 'Number'. See ***Universal Card Formats for 'Use MIFARE Serial Number as Card Data' (CSN mode)*** (on page 26-11) for the procedure.

13. If you want to configure **Double card overrides** for this reader, se Configuring Local Overrides at Card Readers for further instructions.
14. Is there a **Permitted Card Technology** section for this reader?
    Note: The Permitted Card Technology options are only applicable to Gallagher T series readers.
    If **yes**, go to Step 15.
    If **no**, go to Step 17.
15. In the Permitted Card Technology section, **Use the server settings** is selected by default.
    If you want to select other types of cards to be accepted at the reader, uncheck the **Use the server settings** checkbox and select the appropriate checkboxes.

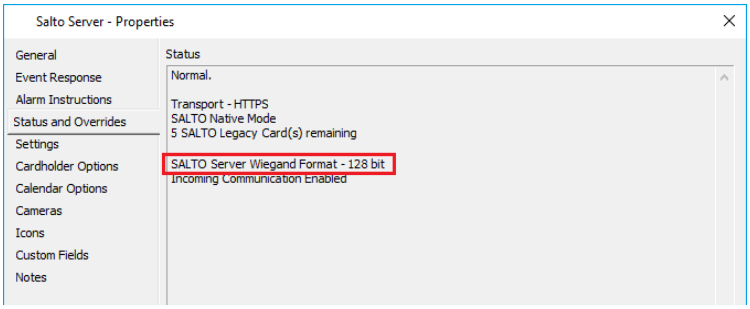


16. If your site is using MIFARE Plus cards with the 'X' feature set and you wish to prevent relay attacks occurring over HBUS, check the **MIFARE Plus** checkbox to enable the **Enforce MIFARE Plus X Card Proximity Checking** checkbox.
17. Check the **Enforce MIFARE Plus X Card Proximity Checking** checkbox.
    The terminal will perform proximity checks when reading a MIFARE Plus X card. **Notes:**
    - Checking this option disabled all other card technologies.
    - The MIFARE Plus X Card Proximity Checking feature will only work if the site that issued the card is using the same MIFARE Plus/DESFire key seed as your site.
    - Operators need the "Edit Site" privilege to be able to amend this setting.
    - For a MIFARE only reader, all 125 kHz cards will be denied.
    - For Cardax IV connected Gallagher T series readers, any changes to the Card Technology Enforcement options will take approximately 40 seconds for the new setting to be sent to the reader.
18. Click the **Type** tab.



19. Select the appropriate **Format** from the drop-down list.
20. Did you select 'Salto' as the Format?
    If **yes**, no **Key Map** is necessary. Go to the next tab.
    If **no**, go to Step 21.

    Note: The current Wiegand Format supported will display on the **Status and Overrides** tab of the Salto Server properties.

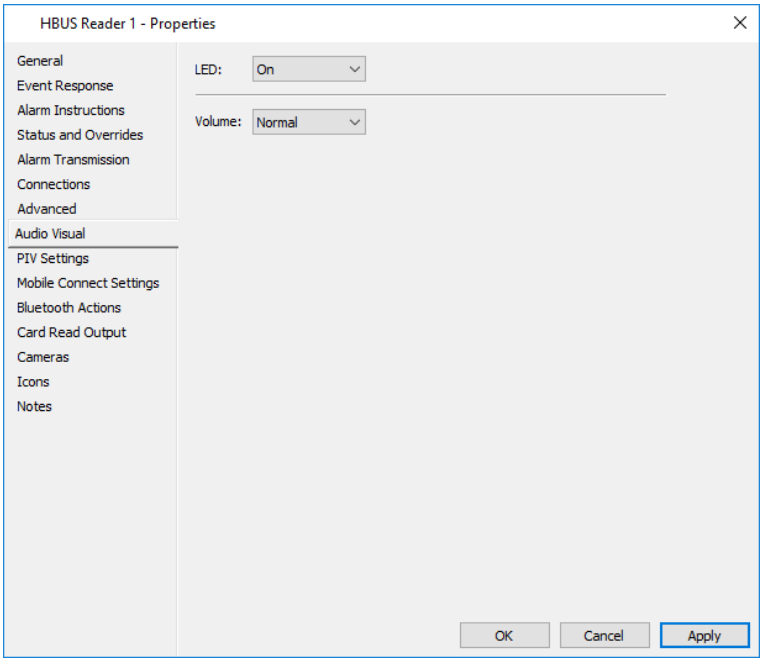


21. Select the appropriate key press mapping option from the **Key map** drop-down list for the type of reader as follows:

For a...	select...
HID iClass Reader	Unbuffered 4-bit burst (e.g. HID iClass RK40/RWK400 Reader).
MR20 Reader	Unbuffered 8-bit burst (e.g. MR20 Magnetic Card Reader).
BQT COTAG Format	Unbuffered 8-bit burts (BQT COTAG)
OSDP Reader	Open Supervised Device Protocol (OSDP)

Note: When a key press mapping option is selected, 12 binary data boxes appear relevant to the selection, allowing you to select a known key press mapping or configure a custom mapping.

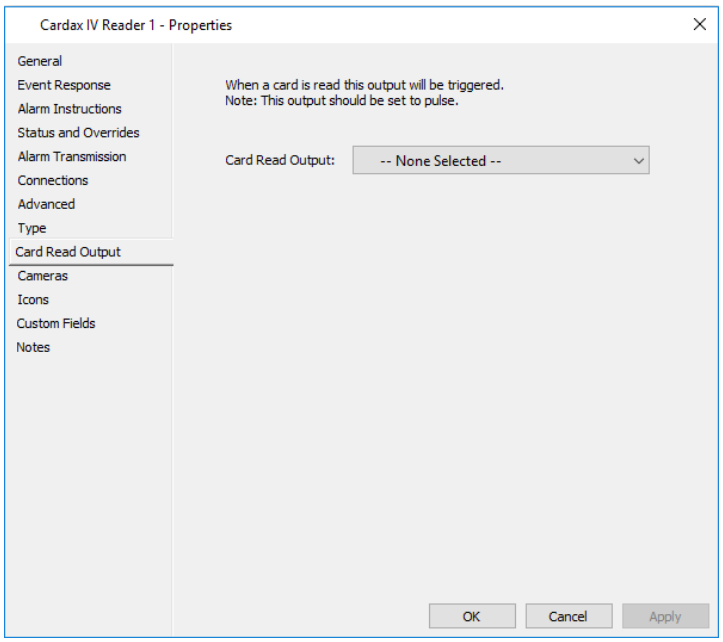
22. Are you configuring an HBUS Reader?
    If **yes**, go to Step 23.
    If **no**, go to Step 25.
23. Click the **Audio Visual** tab.



24. Configure the settings as required.

Field	Description
Volume	This can be set to Off or Normal. (Default = Normal)
LED	This can be set to either Off or On. (Default = On)

25. Are you configuring an HBUS Multi-Tech reader for Bluetooth® connectivity?
    If **yes**, then refer to ***Configuring a reader for Bluetooth® connectivity*** (on page 31-8).
    If **no**, then go to Step 26.
26. Do you want to associate a relay output with this reader, so that when a card is badged at the reader, the relay will be triggered?
    If **yes**, then go to Step 27.
    If **no**, then go to Step 29.
27. Click the **Card Read Output** tab.



28. 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.
    Note: 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.

    Recommendation:
    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.
29. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Reader. For further details see ***Cameras tab*** (on page 3-24).
30. Click the **Icons** tab if you want to change the Icon Set for this Reader. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
31. 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).

32. Click the **Notes** tab if you want to add a note(s) about this Reader.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
33. 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.

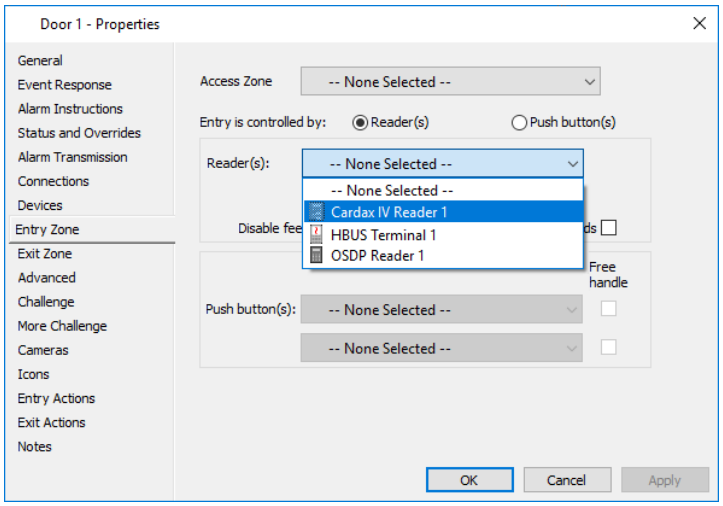
Assigning the Reader

Once configured, you need to assign the reader to the appropriate devices, (i.e. Gallagher Controller, Door, Elevator Car and/or HLI Elevator Car).

34. From the appropriate List Window, highlight the device you want to assign the reader to.
    Note: HBUS Readers, HBUS Terminals, HBUS Contact Card Readers, Cardax IV, and Third Party Readers can be connected directly to a Controller or to reader interface.
35. **Right click** and select **Properties**.
36. What type of device are you assigning the reader to?

If...	then click the...
Controller	**HBUS Devices** tab or **Readers** tab.
Door	**Entry Zone** tab or **Exit Zone** tab.
Elevator Car or HLI Elevator Car	**Connections** tab.

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



37. Assign the reader to the appropriate reader address by selecting it from the relevant **Reader** drop-down list.
38. 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 reader has been configured, assigned to a device, and is ready for use.

Configuring HBUS Devices

Introduction

Controller 6000s that are on-line and configured for HBUS (in the **RS-485 Bus 1** or **2** fields on the **Setup** tab), will auto-detect HBUS devices on the **HBUS Devices** tab. There are three ways of using the auto-detection functionality, as follows:

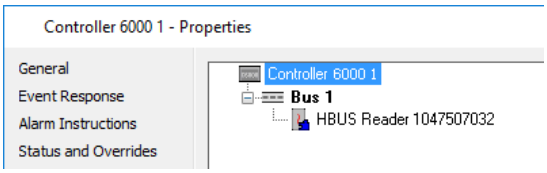
- **Plug-and-play.** Connect an HBUS device to a Controller, which gets auto-detected in Command Centre.
- **Partial pre-configuration.** Create an HBUS device in Command Centre. Assign it to a Controller with NO serial number. Connect an HBUS device to the Controller.
- **Full pre-configuration.** Create an HBUS device in Command Centre. Assign it to a Controller with the correct serial number. Connect an HBUS device to the Controller.

Note: HBUS Readers contain a list of valid facility codes. The card type & facility code must exist in Command Centre before the reader will pass the card read to the Controller.

Procedure

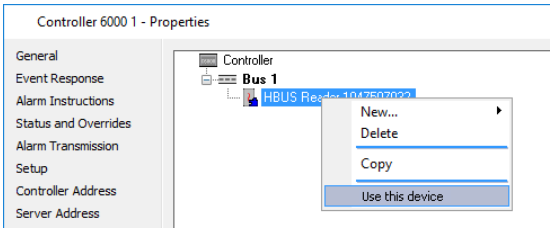
Plug-and-play

1. Physically connect an HBUS device to the Controller's HBUS port, and power on the device.

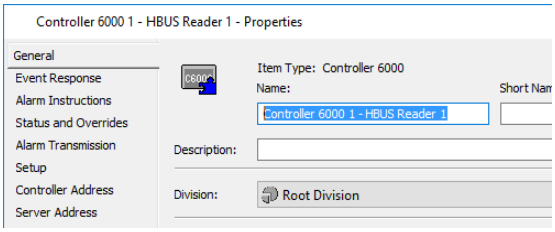


Within 20 seconds a detected item displays in Command Centre, on the Controllers **HBUS Devices** tab under the Bus node, (i.e. RS485 port) it is detected on. The item will have the correct icon for the type of device detected, and the item name displays as:
<Item type detected> <serial number detected>.

2. **Right click** on the detected item and select **Use this device**.



The properties for a new Command Centre item, matching the type of HBUS device detected displays, with the default name:
<Controller name> - <Item type> <number>



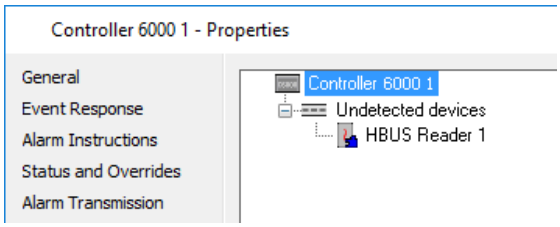
The items **Event Response** tab is populated with the same Alarm Zone as the hosting Controller, and the **Connections** tab is populated with the

hosting Controller and the serial number of the detected HBUS device.
Note: Other tabs for the item contain the default settings for a new item of that type.

3. Click the **OK** button.
   The new item is saved and displays on the **HBUS Devices** tab of the Controller and on the **Hardware** List Window with the new name entered.

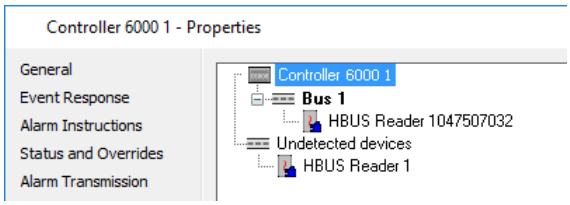
Partial pre-configuration

1. Create a new HBUS device. Either:
   - from the **Hardware** List Window, right click and select **New...HBUS Devices**, OR,
   - from the **HBUS Devices** tab of the Controller the device is to be assigned to, right click in the grid and select **New...**
2. Click the **Event Response** tab of the HBUS device, and enter an Alarm Zone.
3. Click the **Connections** tab of the HBUS device.
4. Assign it to a Controller by selecting the appropriate one from the **Controller** drop-down list, and click the **Apply** button.
5. Open the properties of the Controller you have assigned the HBUS device to, and click the **HBUS Devices** tab.



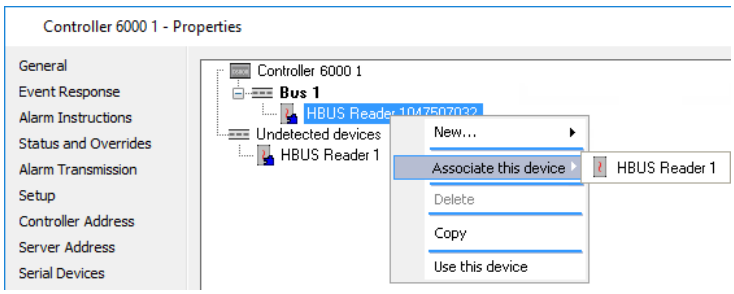
The new item appears under the "Undetected devices" node on the Controllers **HBUS Devices** tab, and below the Controller on the **Hardware** List Window. In both places, the items icon has the unconfigured blue jigsaw overlay.

6. Physically connect an HBUS device of the same type to one of the Controllers RS485 (HBUS) ports.



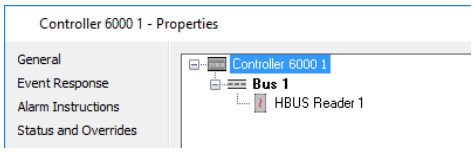
The device is auto-detected and a detected item displays on the Controllers **HBUS Devices** tab under the Bus node that the device was detected on. The items name will display as: *<Item type detected> <serial number detected>*.

7. Right click on either the detected item or the undetected device, and click **Associate this device**.



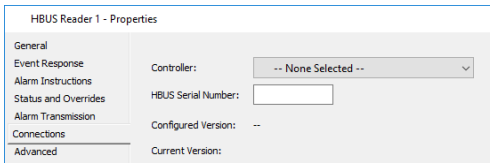
Only items of the same type that are assigned to this Controller, but do not have a serial number entered, will appear in the sub-menu.

8. Select the appropriate item. Alternatively, you can drag and drop the detected item onto the undetected device, but not the other way around. The selected item is removed from the "Undetected devices" node and merged with the detected item. The name of the detected item changes to match the name of the undetected device, and the item's icon and status show as online.

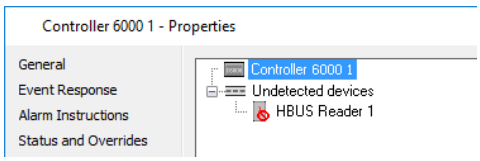


Full pre-configuration

1. Create a new HBUS device. Either:
   - from the **Hardware** List Window, right click and select **New...HBUS Devices**, OR,
   - from the **HBUS Devices** tab of the Controller the device is to be assigned to, right click in the grid and select **New...**
2. Click the **Connections** tab of the HBUS device.

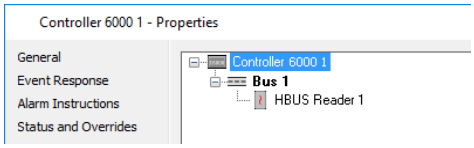


3. Assign it to a Controller by selecting the appropriate one from the **Controller** drop-down list.
4. Enter the serial number of the unconnected HBUS device in the **HBUS Serial Number** field, and click the **Apply** button.
5. Open the properties of the Controller you have assigned the HBUS device to, and click the **HBUS Devices** tab.



The new item appears under the "Undetected devices" node on the Controllers **HBUS Devices** tab, and below the Controller on the **Hardware** List Window. In both places, the items icon shows the not responding red 'banned' overlay.

6. Physically connect the HBUS device with the matching serial number to one of the Controllers RS485 (HBUS) ports.



The device is auto-detected and the configured matching item is removed from the "Undetected devices' node and placed under the corresponding Bus node. The item's icon and status show as online.

Configuring an HBUS Keypad Reader

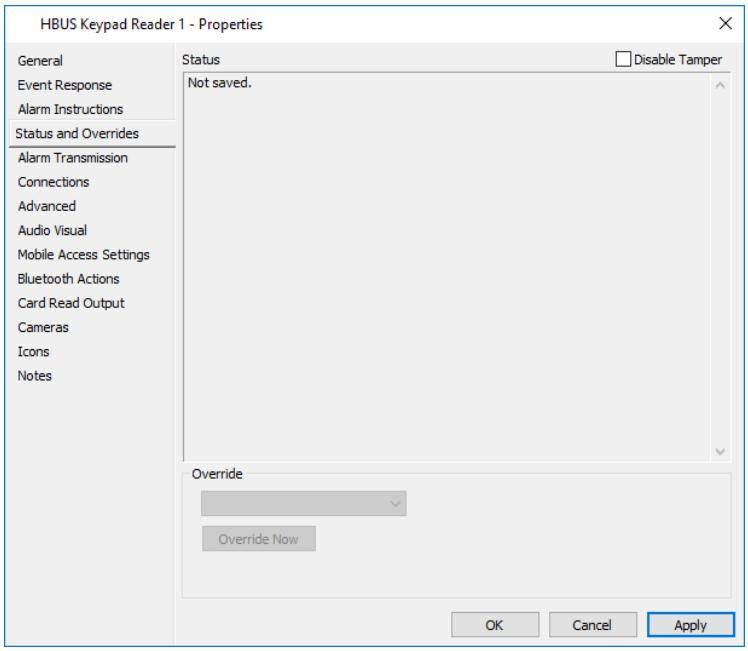
Introduction

This procedure describes how to configure an HBUS Keypad Reader in Command Centre.

Procedure

To configure an HBUS Keypad Reader, perform the following procedures in Gallagher Configuration Client:

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 **HBUS Keypad Reader**.
   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 **Status and Overrides** tab.

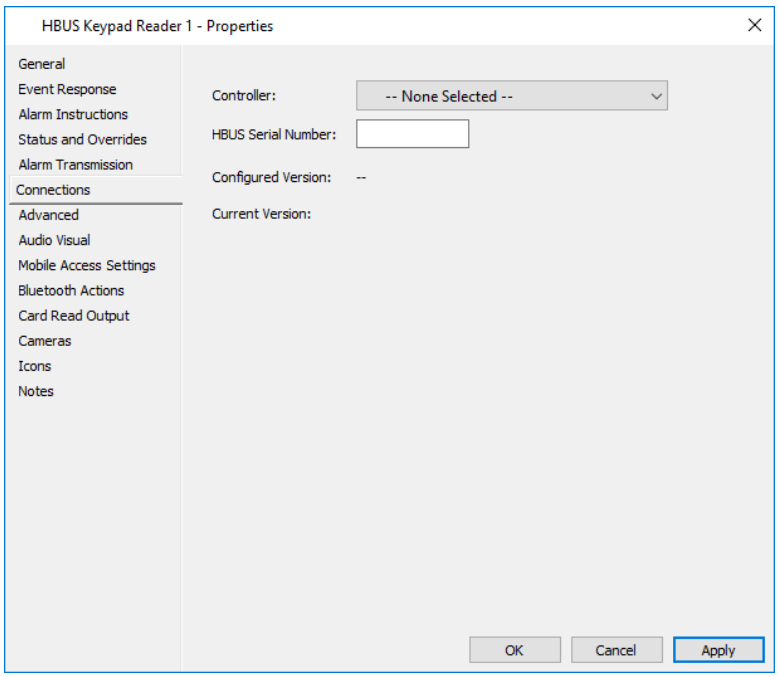


   If the keypad reader is removed (from the wall), a tamper alarm is generated. To disable the tamper, tick the **Disable Tamper** checkbox.
8. To perform an override, click within the **Override** field and select the required override action from the drop-down list, then click the **Override Now** button.

For a description on each of the override actions that can be performed for this device, see ***Performing Overrides*** (on page 45-7).

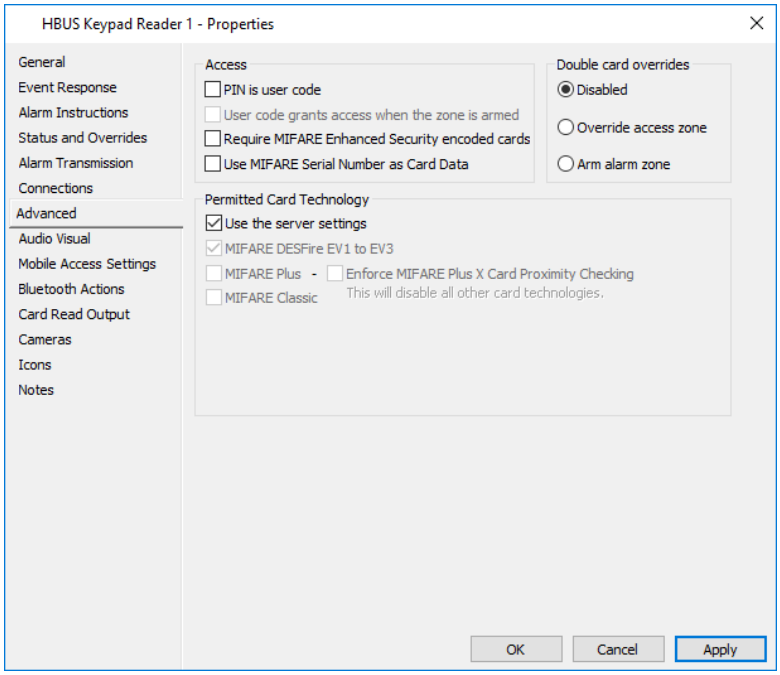
Note: This device does not support timed overrides. All overrides are immediate and persist until specifically cancelled by an operator

9. Click the **Connections** tab.



10. Select the Controller 6000 or 7000 you want to assign this HBUS Keypad Reader to, from the **Controller** drop-down list.
    Notes:
    - HBUS Keypad Readers can be created via the **HBUS Devices** tab of a Controller. In that case the Controller field would be pre-populated with that Controller name. Refer to the topic ***Configuring HBUS Devices*** (on page 21-65).
    - When an HBUS Keypad Reader is connected to a Controller 6000 or 7000 it will automatically be upgraded or downgraded to the version of T30 firmware held by the Controller. This will only happen if the HBUS Keypad Reader is correctly configured. A download bar displays on the **Connections** tab, showing the approximate progress of the download. If the download fails for whatever reason, the HBUS Keypad Reader will revert to the previous version of code. A Code Download Fail event is raised in Command Centre.
11. Enter the HBUS serial number (10 character hexadecimal string) into the **HBUS Serial Number** field.
    This serial number is located on the unit.
    Note: The HBUS serial number is optional, however the HBUS Keypad Reader will be considered as not properly configured unless one is entered.

12. If you click the **Apply** button, software version numbers display.
    The **Configured Version** is the version of the device software in the configured Controller FTS file, (i.e. **not** the version of the Controller software). The **Current Version** is the version of software as last reported by the HBUS Keypad Reader itself.
    Note: For the HBUS Keypad Reader to report its current version of software, an Alarm Zone must be assigned to the **Event Response** tab of the reader's properties.
13. Click the **Advanced** tab.



14. Configure as required.

Field	Description
PIN us user code	When checked the Cardholder's user code will be required in place of a PIN for any access transactions at this reader and the **User Code grants access when the zone is armed** option activates.
User code grants access when the zone is armed	When checked, a Cardholder can gain access to an armed zone using User Code without disarming any Alarm Zone. However, if the Cardholder has the 'Change to Disarmed state' privilege, the Alarm Zone(s) will be disarmed upon access. **Note:** To be able to select this option, you need to select the PIN is user code checkbox first
Require MIFARE Enhanced Security encoded cards	When checked, the reader is instructed to only accept cards that have the enhanced security data when deciding whether to grant a Cardholder access. The MIFARE Enhanced security key is configured on the **Card Security** tab of the Server Properties. **IMPORTANT:** When this checkbox is unchecked, the

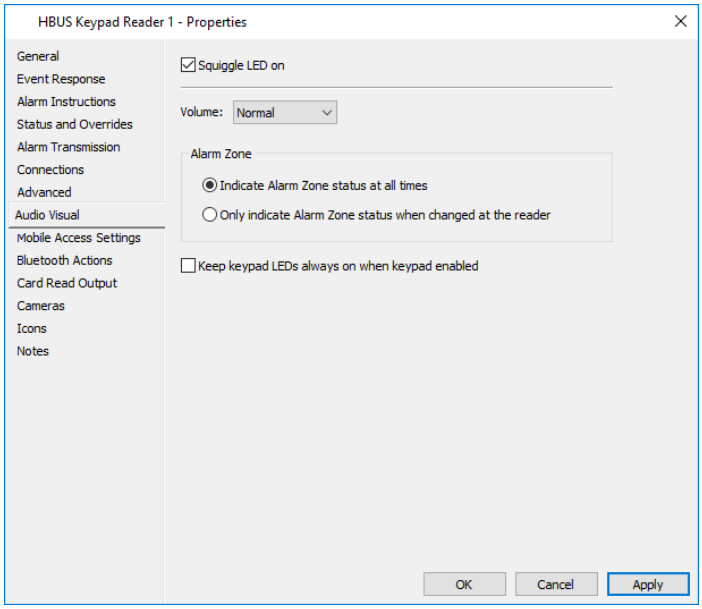
Field	Description
	reader will be instructed not to send the enhanced security data to the Controller, even if present. Leave this checkbox unchecked in the following situations: 1. When not using the MIFARE Enhanced Security feature or when not using it for part of a site. 2. When some Cardholders requiring access using this reader have not yet had their cards re-encoded. It is important to remember to enable the setting once all cards have been re-encoded. Disabling this setting will also allow cards encoded at sites using the MIFARE Enhanced Security feature to be used at sites who are not using this feature. In the event of this being enabled, all low security cards will be denied with an event saying *"Denied - MIFARE High Security Card Required at [Door]"*. To enable both high and low security cards to be used uncheck the checkbox for the Door Reader.
Use MIFARE Serial Number as Card Data	HBUS Keypad Readers can be set to read the Card Serial Number (CSN) from a MIFARE Card and use it to identify a Cardholder in Command Centre. When enabled, this allows the reader to send the CSN as Cardholder identification to the Controller if it does not detect any other form of Cardholder identification on the card. **Additional required configuration:** For the Controller to interpret the CSN as a Cardholder's card number, you also need to configure and assign a Universal Card Format. Once this is configured, you can assign cards to Cardholders using the CSN as the card 'Number'. See ***Universal Card Formats for 'Use MIFARE Serial Number as Card Data' (CSN mode)*** (on page 26-11) for the procedure.

15. If you want to configure Double card overrides for this terminal, see Configuring Local Overrides at Card Readers for further instructions.
16. In the Permitted Card Technology section, by default **Use the server settings** is selected. If you want to select other types of cards to be accepted at the reader, uncheck the **Use the server settings** checkbox. The other card technologies are enabled.
17. Select the appropriate checkboxes for the types of cards to be accepted.
18. If your site is using MIFARE Plus cards with the 'X' feature set and you wish to prevent relay attacks occurring over HBUS, check the **MIFARE Plus** checkbox to enable the **Enforce MIFARE Plus X Card Proximity Checking** checkbox.
19. Check the **Enforce MIFARE Plus X Card Proximity Checking** checkbox.

The terminal will perform proximity checks when reading a MIFARE Plus X card. **Notes:**

- Checking this option disables all other card technologies.
- The MIFARE Plus X Card Proximity Checking feature will only work if the site that issued the card is using the same MIFARE Plus/DESFire key seed as your site.
- Operators need the "Edit Site" privilege to be able to amend this setting.

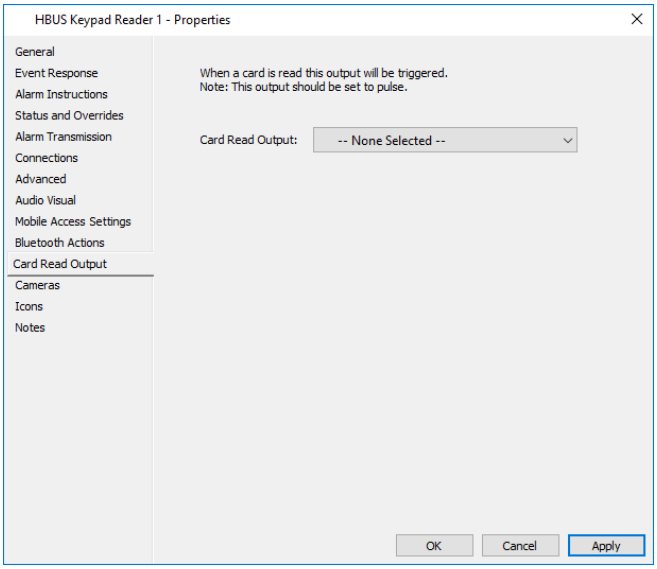
20. Click the **Audio Visual** tab.



21. Configure the settings as required.

Field	Description
Squiggle LED on	The squiggle LED can be set to either Off or On. By default, this option is checked. Uncheck it if you want the squiggle LED to be off.
Volume	This can be set to Off or Normal. (Default = Normal)
Alarm Zone	Click the appropriate radio button for when you want the status of the Alarm Zone to be indicated at the reader: **Indicate Alarm Zone status at all times:** (default) When the reader is armed, the Arm button will be red. When disarmed the Arm button will be green. **Only indicate Alarm Zone status when changed at the reader:** When the Alarm Zone is armed at the reader (via double card override or using the Arm button), the Arm button will indicate the new Alarm Zone status for 10 seconds and then turn off. This gives the user confirmation at the reader that the status change was successful.
Keep keypad LEDs always on when keypad enabled	Check this option if you want the HBUS Keypad Reader LEDs to always be active and dimmed when access mode is 'Code Only'.

22. The **Mobile Connect Settings** tab and **Bluetooth Actions** tab allow you to configure an HBUS Keypad Reader for Bluetooth® connectivity. Refer to ***Configuring a reader for Mobile Connect*** (on page 31-11) for the procedure.
23. Click the **Card Read Output** tab.



24. From the **Card Read Output** drop-down list (which includes virtual Outputs), select the Output to switch on when a card is badged at this reader.
    Note: 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.
    Recommendation: 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.
25. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this reader. For further details see ***Cameras tab*** (on page 3-24).
26. Click the **Icons** tab if you want to change the Icon Set for this reader. 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 reader. 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 reader. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
29. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

An HBUS Keypad Reader has been configured, assigned to a Controller 6000 or 7000, and is ready for use.

Configuring HBUS Terminals

This chapter describes how to configure an HBUS Terminal, (i.e. HBUS Terminals or HBUS Alarms Only Terminals) in Command Centre.

Select the item below that you require further detail on:

- ***Configuring an HBUS Terminal*** (on page 21-75)
- ***Configuring an HBUS Alarms Only Terminal*** (on page 21-91)
- ***HBUS Terminal: Date and time format*** (on page 21-103)
- ***HBUS Terminal: Overriding the Access Mode*** (on page 21-105)
- ***HBUS Terminal: Overriding the Alarm Zone state to armed*** (on page 21-107)
- ***HBUS Terminal: Duress Code*** (on page 21-108)

Configuring an HBUS Terminal

Introduction

This procedure describes how to configure an HBUS Terminal in Command Centre. Other procedures associated with configuring an HBUS Terminal are:

- ***Configuring Access Group Privileges for Terminal Access*** (on page 34-13)
- ***Configuring User Codes for Terminal Access*** (on page 32-23)
- ***HBUS Terminal Defaults*** (on page 6-67)

Notes:

- Operators require the "Edit Site" operator privilege to perform this procedure and must be in the same or parent Division of the HBUS Terminal.
- To change the date and time format, for all terminals, refer to the topic ***HBUS Terminal: Date and time format*** (on page 21-103).
- The language displayed on the terminal, is configured on the **Software** tab of the host Controller's properties. When configured for English text (the default), the terminal displays the month using abbreviations, (e.g. Jan, Feb, Mar). When configured for non-English text, the terminal displays the month as configured for the selected language. **Ensure you configure messages for terminals in the same language as is set on their host Controller's Software tab.**
- Command Centre data, (e.g. Event messages and item states) are sent to the terminal using the language selected on the Command Centre server. Command Centre editable fields, (e.g. Alarm Zone names and Input names) are sent to the terminal, as entered in Command Centre.

Minimum configuration requirements

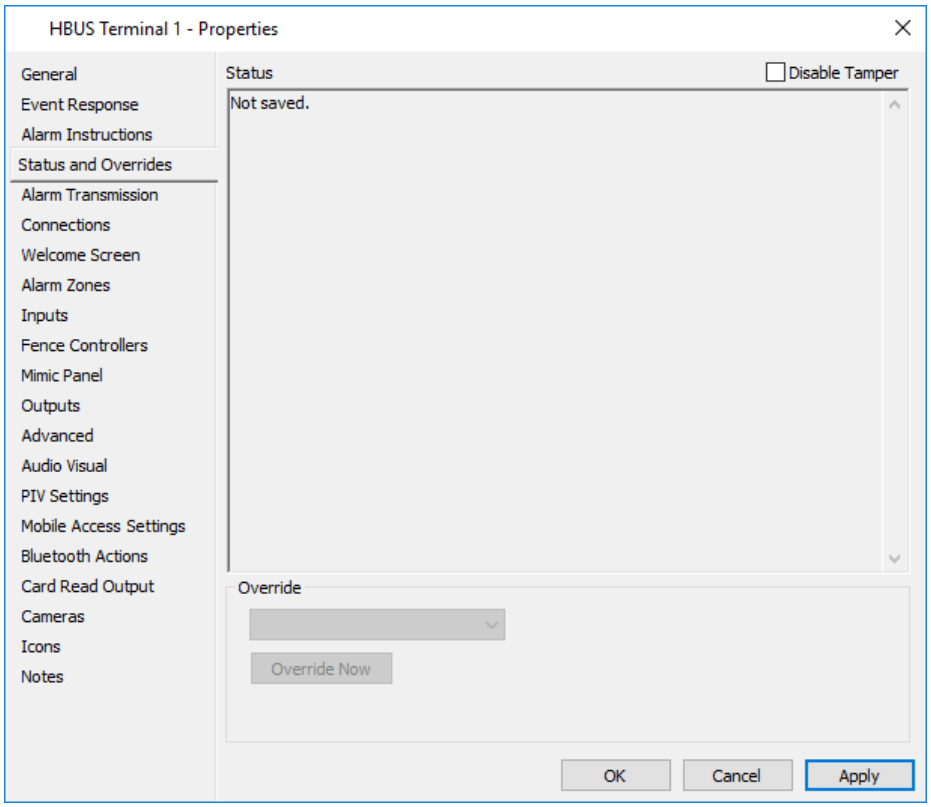
The terminal will display the message "Not Configured" unless the following configuration has been completed:

- On the **Connections** tab, assign the terminal to a Controller 6000 or 7000 and enter the terminal's HBUS serial number (10-character hexadecimal string).
- If using alarms management functionality, on the **Alarm Zones** tab, assign at least one Alarm Zone to the terminal.
  Note: Alarms management functionality is not available when the terminal is assigned as the Reader for an Elevator Car.
- If used for access control, assign the terminal as the Reader for a Door or Elevator Car.

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**.

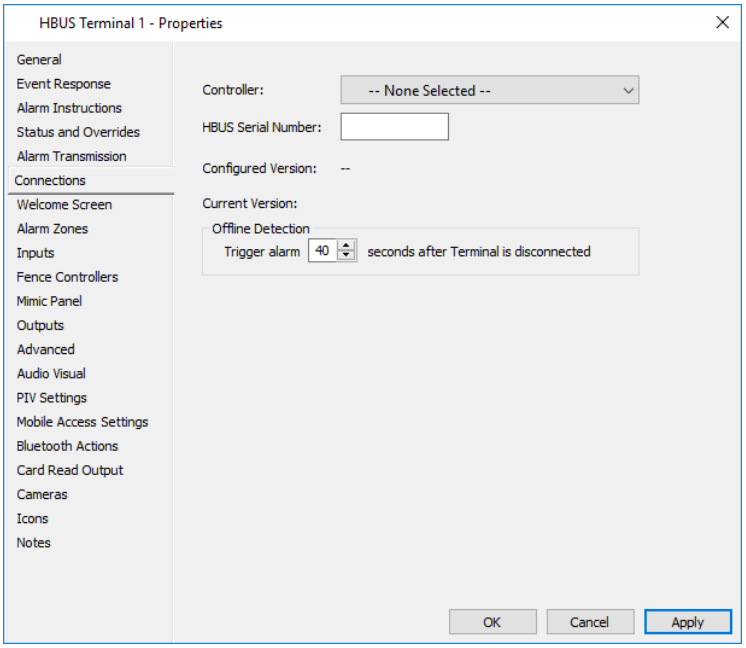
3. Select **HBUS Terminal**.
   By default the **General** tab displays.
4. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
5. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
6. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
7. Click the **Status and Overrides** tab.



   If the terminal is removed (from the wall), a tamper alarm is generated. To disable the tamper, tick the **Disable Tamper** checkbox.
8. To perform an override, click within the **Override** field and select the required override action from the drop-down list, then click the **Override Now** button.

   For a description on each of the override actions that can be performed for this device, see Performing Overrides.

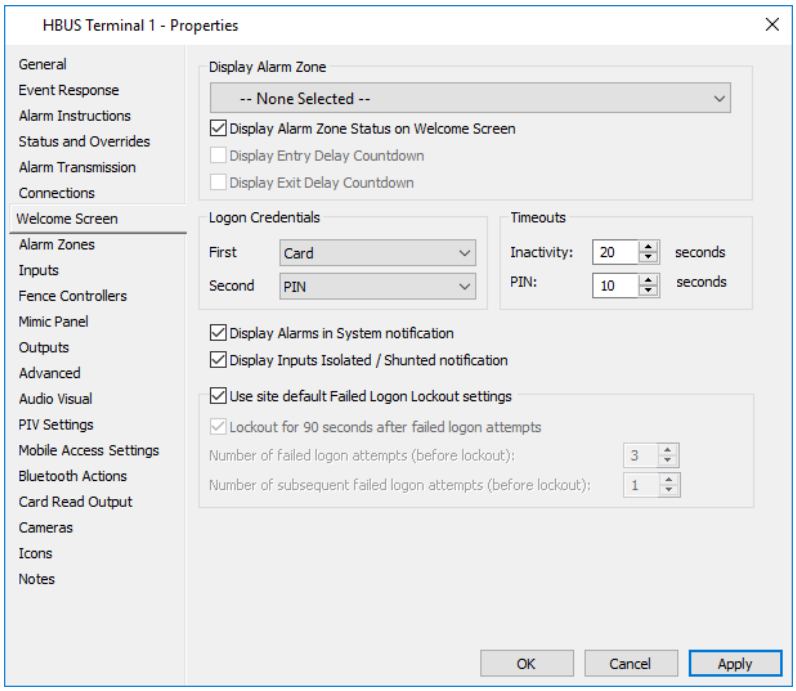
   Note: This device does not support timed overrides. All overrides are immediate and persist until specifically cancelled by an operator.
9. Click the **Connections** tab.



10. Select the Controller 6000 or 7000 you want to assign this terminal to, from the **Controller** drop-down list. **Notes:**
    - HBUS Terminals can be created via the **HBUS Devices** tab of a Controller. In that case the **Controller** field would be pre- populated with that Controller name. Refer to the topic ***Configuring HBUS Devices*** (on page 21-65).
    - When an HBUS Terminal is connected to a Controller 6000 or 7000 it will automatically be upgraded or downgraded to the version of T20 firmware held by the Controller. This will only happen if the HBUS Terminal is correctly configured. A download bar displays on the **Connections** tab, showing the approximate progress of the download. If the download fails for whatever reason, the HBUS Terminal will revert to the previous version of code. A Code Download Fail event is raised in Command Centre.
11. Enter the HBUS serial number (10-character hexadecimal string) into the **HBUS Serial Number** field. This serial number is located on the unit.
    Note: The HBUS serial number is optional, however the terminal will be considered as not properly configured unless one is entered.
12. If you click the **Apply** button, software version numbers display.
    The **Configured Version** is the version of the device software in the configured Controller FTS file, (i.e. **not** the version of the Controller software). The **Current Version** is the version of software as last reported by the terminal itself.
    Note: For the HBUS Terminal to report its current version of software, an Alarm Zone must be assigned to the **Event Response** tab of the terminal's properties.
13. The **Offline Detection** setting determines how long it takes for the Controller to detect that the T20 is offline after it is physically disconnected.

Enter the period of time (in seconds) that it will take before an alarm is triggered after the terminal is disconnected.
(Default = 40 seconds. Range = 10 - 40 seconds)

14. Click the **Welcome Screen** tab.



This screen enables you to display the status of a selected Alarm Zone and control the logon credentials and timeouts for this terminal, when a Cardholder attempts to log on or perform a local override using the function keys on this terminal.

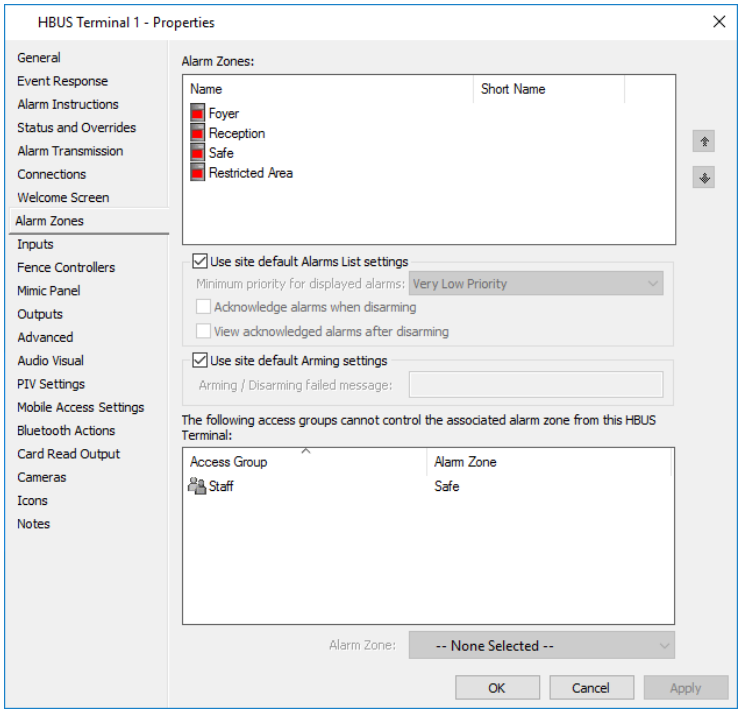
15. Configure as required.

Field	Description
Display Alarm Zone	Select the Alarm Zone that will be displayed on the terminal, from the **Display Alarm Zone** drop-down list. When the Alarm Zone is armed, the armed icon displays. **Notes:** • When assigned as an entry reader, the **Display Alarm Zone** field is populated with the Alarm Zone assigned to the Door's entry Access Zone. When assigned as an exit reader, the **Display Alarm Zone** field is populated with the Alarm Zone assigned to the Door's exit Access Zone. • If not assigned as an entry or exit reader, the choice of Alarm Zone is restricted to only those associated with the terminal on the **Alarm Zones** tab. • Deselect the **Display Alarm Zone Status on Welcome Screen** checkbox, if you want to remove all visual and audio indicators of the system being armed or disarmed. • Check the **Display Entry Delay Countdown** and/or **Display Exit Delay Countdown** checkboxes if required. Displaying the Entry Delay Countdown informs a user of the time left before an alarm is triggered. Displaying the Exit Delay Countdown provides a user arming an Alarm Zone via the T20 an indication of how long they have left until exit delay expires. These checkboxes will be disabled if a Display

Field	Description
	Alarm Zone has not been selected or if the terminal has been assigned as a reader.
Logon Credentials	Specify the first and second **Logon Credentials** required to log on to the terminal. The default **First** logon credential is "Card". The default **Second** logon credential is "PIN". **Notes:** • If you select "Card or Mobile Credential" as the **First** logon credential: ▪ "None" **Second** logon credential allows logging on by badging a Card or Mobile Credential only. ▪ "PIN" or "User Code" **Second** logon credential allows logging on by presenting a: - Card, then PIN or User Code on the HBUS Terminal, or - Mobile Credential, then second authentication factor on the mobile device (e.g. fingerprint). **Note:** The terminal never prompts for second authentication when logging on with a Mobile Credential; Cardholders are prompted on their mobile device. • If you select "User Code" as the **First** logon credential, **Second** logon credential becomes disabled. Logon is allowed by entering a User Code. • If you select "Card or User Code" as the First logon credential, **Second** logon credential becomes disabled. Logon is allowed by badging a Card, Mobile Credential, or by entering a User Code.
Timeouts	In the **Inactivity** timeout field, enter the period of time (in seconds) of inactivity before a Cardholder will be logged off the terminal. Default 20 seconds. **Note:** If the terminal has not been used for 30 seconds, the screen and keypad backlight will dim. Hence if the inactivity period is greater than 30 seconds and the terminal has not been used, the screen and backlight will dim whilst the user is logged on. In the **PIN** timeout field, enter the period of time (in seconds) that a user has to enter their PIN or User Code at the terminal in order to log on. Default 10 seconds.
Display Alarms in System notifications	Deselect the **Display Alarms in System notification** checkbox, if you do not want to display the red alarm notification banner on the Welcome screen or Mimic Panel screen of the terminal.
Display Inputs Isolated / Shunted notification	Deselect the **Display Inputs Isolated / Shunted notification** checkbox, if you do not want to display the yellow isolated/ shunted banner on the Welcome screen of the terminal, when one or more inputs in any of the Alarm Zones associated with the T20 is shunted or isolated. **Notes:** • This option will default to 'off' if either the **EN50131 Compliance** or **SSF1014 Compliance** checkbox is enabled on the **Standards** tab of the Server Properties.

Field	Description
	• If the Input is not assigned to the terminal, the banner will display without the ability for a user to address the issue directly from the terminal.
Use site default Failed Logon Lockout settings	Deselect the **Use site default Failed Logon Lockout settings** checkbox, if you want to configure the failed logon lockout settings specifically for this terminal. Select the **Lockout for 90 seconds after failed logon attempts** checkbox. The terminal will be locked out for a period of 90 seconds after the **Number of failed logon attempts** has been exceeded. Default 3. Range 3-10. If required, enter the **Number of subsequent failed logon attempts** to occur before the terminal is locked out again. Default 1. Range 1-10. **Notes:** • Failed Logon Lockout is configurable via the Server Properties. The default will be off for sites that already have T20s installed. For sites installing new T20s the default will be on. • The repeated use of the same user code or PIN will only count as a single attempt. • If the number of failed logon attempts reaches a certain number, then a tamper alarm is raised. This number is either the total of the two configurable amounts plus 1, or 7 attempts - whichever is reached first. The terminal will display the message "*Temporarily locked out*" with a red "X" on screen.

16. Click the **Alarm Zones** tab.



17. Click **Configure** from the menu bar, then **Alarm Zones**. The Alarm Zone List Window opens.

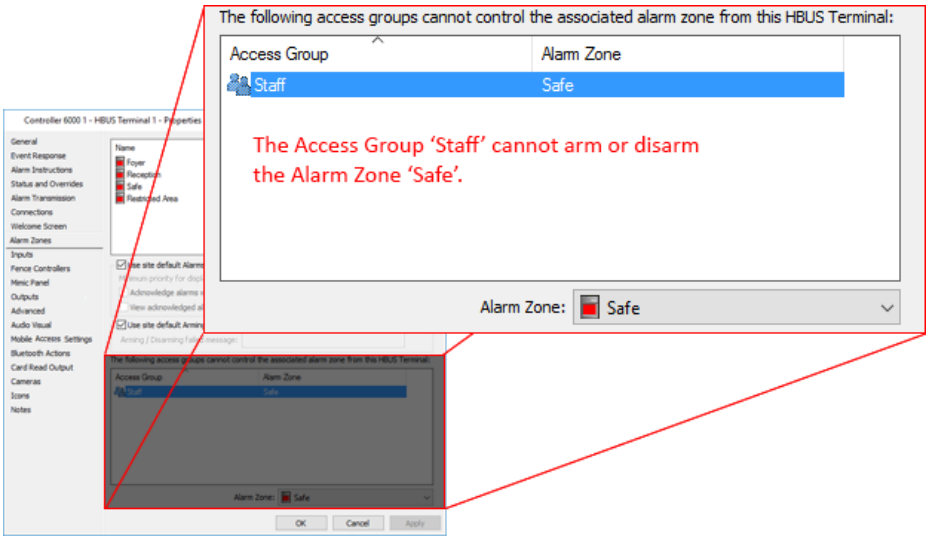
Select the Alarm Zones you wish to associate with this terminal, and drag and drop them into the **Alarm Zones** grid. **Notes:**

- In order to display Inputs, Outputs, Fence Controllers and Fence Zones within the terminal user interface, the Alarm Zones assigned to these items must be assigned to the terminal.
- Up to 50 Alarm Zones can be associated with one terminal. Assigning many Alarm Zones that are hosted by remote Controllers, may impact on the performance of the terminal.
- All inactive/acknowledged alarms and all inactive/processed alarms older than 28 days are not displayed on the terminal.
- Duress alarms are not displayed on the terminal.
- A maximum of 200 alarms are displayed on the Current Alarms screen, listed in order of priority.
- A maximum of 100 alarms are displayed on the Alarm History screen, listed in order of date/time occurrence.
- The terminal cannot be assigned to an Elevator Car or Elevator Car HLI, if Alarm Zones have been assigned to the terminal.
- If a Short Name has been entered for an Alarm Zone, this will be displayed in the terminal user interface, instead of the Name.

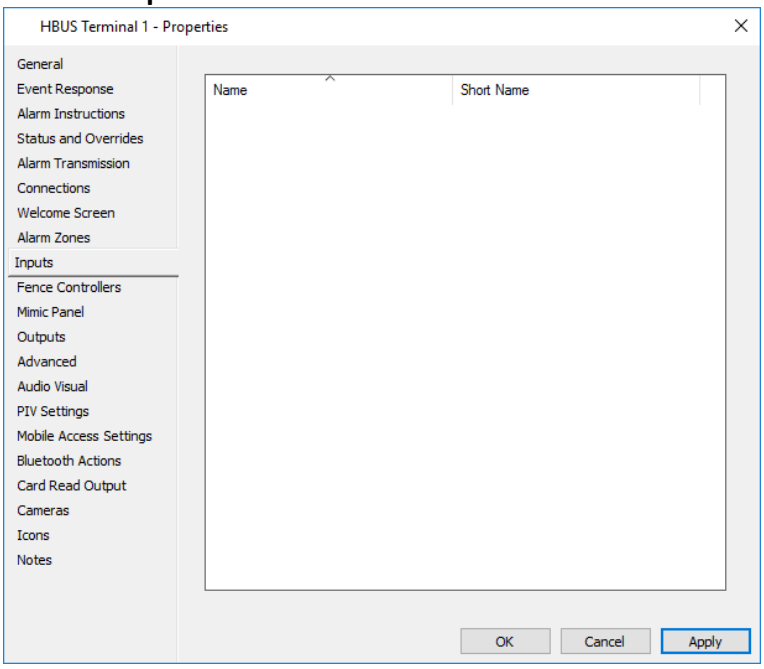
18. Once you have all the Alarms Zones you require in the window, you can re-order the Alarm Zones by using the **up** and **down** arrow buttons to the right of the window.
    Note: The order you sort the Alarm Zones in here will be the order they appear in the terminal user interface.
19. Configure as required.

Field	Description
Use site default Alarms List settings	When checked, the terminal will use the Alarms List Defaults, configured on the **HBUS Terminal Defaults** tab in the Server Properties. By default, the terminal will display all alarms at or above 'Very Low Priority' for the Alarm Zone(s) assigned to the terminal. **Note:** This functionality does not apply when disarming an Alarm Zone based on an access decision. To configure the Alarm List settings specific for this terminal, deselect the **Use site default Alarm List settings** checkbox. Configure the Alarm List settings for this terminal as required. **Note:** The alarms displayed and acknowledged are determined by the Alarm Zones assigned to the Cardholder's Access Group(s) and the Terminal Privileges configured within these Access Groups.
Use site default Arming settings	When checked, the terminal will use the Arming Defaults, configured on the **HBUS Terminal Defaults** tab in the Server Properties. By default, no arming/disarming failed message is displayed. To configure the Arming settings specific for this terminal, deselect the **Use site default Arming settings** checkbox. Enter the arming/disarming failed message to be displayed by this terminal. Maximum 60 characters.

20. Depending on the required configuration, you can prevent certain Access Groups from Controlling (arming or disarming) a specified Alarm Zone from this terminal.
    Do you want to configure this option?
    If **yes**, go to Step 20.
    If **no**, go to Step 23.



21. Click **Manage** from the menu bar, then **Access Groups**.
    The **Access Group** List Window opens.
    Select the Access Group(s) you wish to associate with this terminal, and drag and drop them into the bottom grid.
22. Click the Access Group to select it.
    The Alarm Zone drop-down list activates.
23. From the **Alarm Zone** drop-down list, select the Alarm Zone which you do not want the Access Group to Control (i.e. arm/disarm).
24. Click the **Inputs** tab.

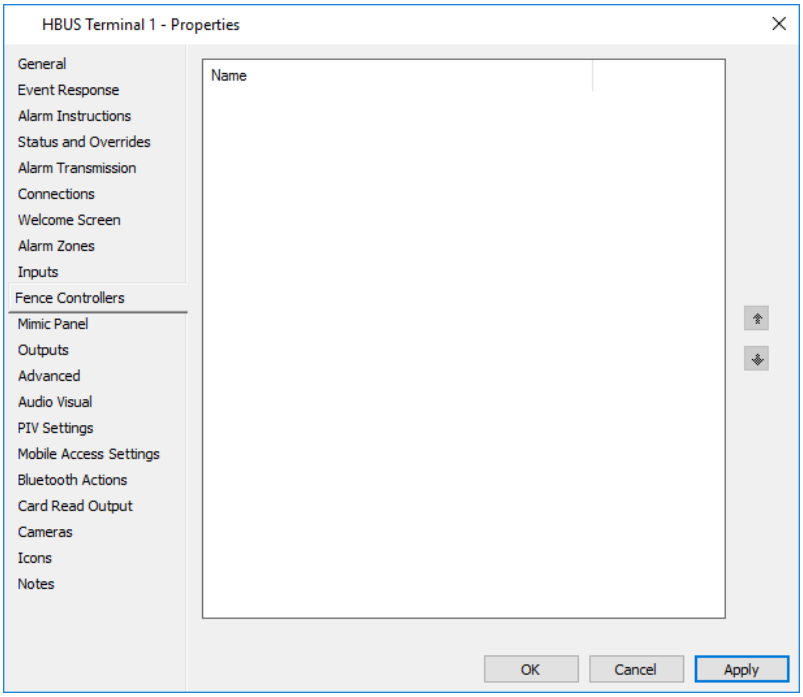


25. From the **Hardware** List Window, select the Inputs you wish to have

controlled by this terminal.
Drag and drop them into the **Inputs** tab window.
Notes:

- Up to 100 Inputs can be monitored by one terminal.
- If a Short Name has been entered for an Input, this will be displayed in the terminal user interface, instead of the Name.

26. Click the **Fence Controllers** tab.



This tab allows you to configure Fence Controllers so they can be monitored and controlled from this terminal.

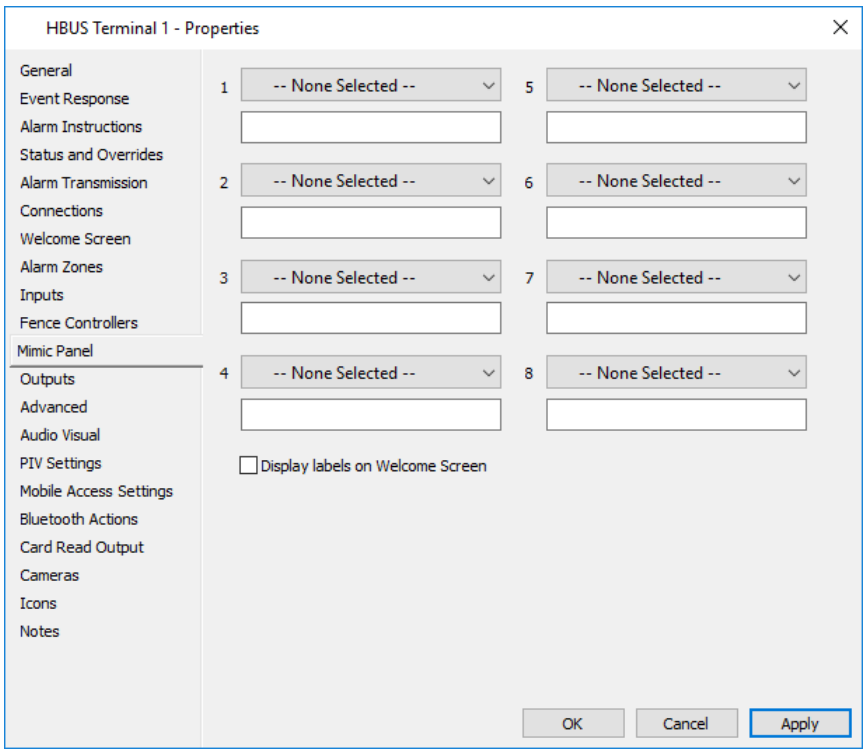
27. From the Hardware List Window, select the Fence Controllers you wish to associate with this terminal, and drag and drop them into the **Fence Controllers** tab window.
Notes:

- Up to 25 Fence Controllers, (e.g. 50 Fence Zones) can be associated with one terminal.
- Only F31, F32, F41, F42 and F22 Fence Controllers can be associated with this terminal.

28. Once you have all the Fence Controllers you require in the window, you can re-order the Fence Controllers by using the **up** and **down** arrow buttons to the right of the window.

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

29. Click the **Mimic Panel** tab.



This screen enables you to configure the 8 LEDs on either side of the terminal to show the status of Alarm Zones, Inputs or Outputs.

30. Select the drop-down arrow for the LED number (1-8) you wish to assign an Alarm Zone, Input or Output to. Select an Alarm Zone, Input or Output from the drop-down list.
    The item's name is automatically populated in the free text label field below.

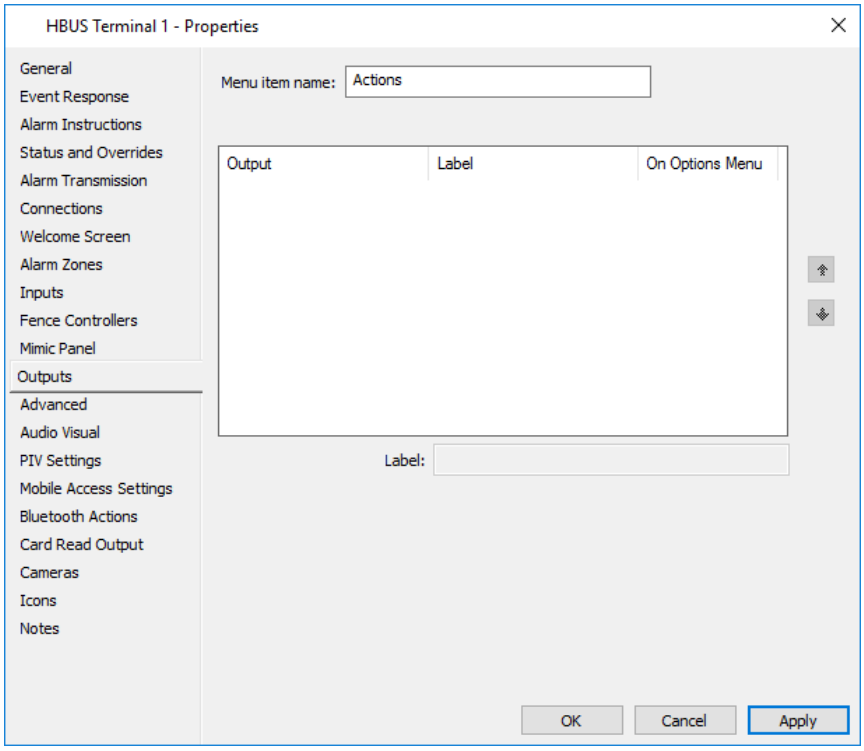
    To display the Alarm Zone, Input or Outputs name on the terminal, select the **Display labels on Welcome Screen** checkbox. The name shown in the free text label field will be displayed on the terminal beside the relevant LED, when the terminal is idle.

    If required, edit the free text label field for each item. Maximum 60 characters.

    Notes:

    - Press the ***** key on the terminal to display the free text labels at any time.
    - The colour of the LEDs and flash states can be configured on the **HBUS Terminal Defaults** tab in the Server Properties.

31. Click the **Outputs** tab.



32. From the **Hardware** List Window, select the Outputs you wish to trigger (On/Off) using this terminal.
    Drag and drop them into the **Outputs** tab window.

    The default **Menu item name** 'Actions' will be used within the terminal user interface. Change the **Menu item name**, if required. Maximum of 25 characters.

    The Output Name will be used within the terminal user interface. To use a different name within the terminal user interface, enter a **Label** for the Output. Maximum of 60 characters.

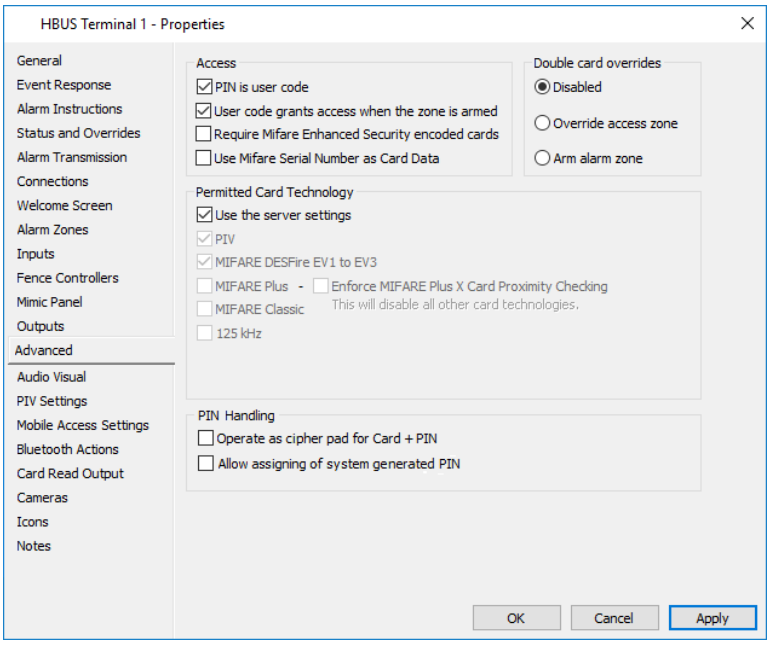
    If you require a non-authorised user, (i.e. terminal log on is not required) to be able to activate an Output, check the **On Options Menu** checkbox for the Output. The Output will appear on the Options Menu within the terminal user interface. A maximum of 5 Outputs can be added to the Options Menu. The Options softkey will only display if one or more Outputs have been configured to display on the Options Menu.

    Note: Up to 100 Outputs can be monitored by one terminal.

33. Once you have all the Outputs you require in the window, you can re-order the Outputs by using the **up** and **down** arrow buttons to the right of the window.

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

34. Click the **Advanced** tab.



35. Configure as required.

Field	Description
PIN is user code	When checked the Cardholder's user code will be required in place of a PIN for any access transactions at this terminal and the **User Code grants access when the zone is armed** option activates. **Note:** For Access Mode and Arming local overrides, the terminal uses the Log On Credentials configured on the **Welcome Screen** tab of the terminal.
User code grants access when the zone is armed	When checked, a Cardholder can gain access to an armed zone using User Code without disarming any Alarm Zone. However, if the Cardholder has the 'Change to Disarmed state' privilege, the Alarm Zone(s) will be disarmed upon access. **Note:** For be able to select this option, you need to select the **PIN is user code** checkbox first.
Require MIFARE Enhanced Security encoded cards	When checked, the terminal is instructed to only accept cards that have the enhanced security data when deciding whether to grant a Cardholder access. The MIFARE Enhanced security key is configured on the **Card Security** tab of the Server Properties. **IMPORTANT:** When this checkbox is unchecked, the terminal will be instructed not to send the enhanced security data to the Controller, even if present. Leave this checkbox unchecked in the following situations: 1. When not using the MIFARE Enhanced Security feature or when not using it for part of a site. 2. When some Cardholders requiring access using this terminal have not yet had their cards re-encoded. It is important to remember to enable the setting once all cards have been re-encoded. Disabling this setting will also allow cards encoded at sites using the MIFARE Enhanced Security feature to be used at sites who are not using this feature.

Field	Description
	In the event of this being enabled, all low security cards will be denied with an event saying *"Denied - MIFARE High Security Card Required at [Door]"*. To enable both high and low security cards to be used uncheck the checkbox for the Door Reader.
Use MIFARE Serial Number as Card Data	HBUS Terminals can be set to read the Card Serial Number (CSN) from a MIFARE Card and use it to identify a Cardholder in Command Centre. When enabled, this allows the terminal to send the CSN as Cardholder identification to the Controller if it does not detect any other form of Cardholder identification on the card. **Additional required configuration:** For the Controller to interpret the CSN as a Cardholder's card number, you also need to configure and assign a Universal Card Format. Once this is configured, you can assign cards to Card-holders using the CSN as the card 'Number'. See ***Universal Card Formats for 'Use MIFARE Serial Number as Card Data' (CSN mode)*** (on page 26-11) for the procedure.

36. If you want to configure **Double card overrides** for this terminal, see Configuring Local Overrides at Card Readers for further instructions.
37. In the Permitted Card Technology section, **Use the server settings** is selected by default.
    If you want to select other types of cards to be accepted at the reader, uncheck the **Use the server settings** checkbox and select the appropriate checkboxes.
38. If your site is using MIFARE Plus cards with the 'X' feature set and you wish to prevent relay attacks occurring over HBUS, check the **MIFARE Plus** checkbox to enable the **Enforce MIFARE Plus X Card Proximity Checking** checkbox.
39. Check the **Enforce MIFARE Plus X Card Proximity Checking** checkbox.
    The terminal will perform proximity checks when reading a MIFARE Plus X card. **Notes:**
    - Checking this option disables all other card technologies.
    - The MIFARE Plus X Card Proximity Checking feature will only work if the site that issued the card is using the same MIFARE Plus/DESFire key seed as your site.
    - Operators need the "Edit Site" privilege to be able to amend this setting.
    - For a MIFARE only HBUS Terminal, all 125 kHz cards will be denied.
40. The **Operate as cipher pad for Card + PIN** option allows sites to reduce the risk of cardholder PINs being discovered by someone looking over a cardholder's shoulder while they enter their PIN at the terminal.

    With this option enabled and the terminal in PINs mode, each time a user badges their card a randomised number keypad will display on the terminal screen. Users then need to follow the scrambled keys on the screen to enter their PIN correctly, (e.g. for the PIN 1234, the user would have to press 5170 on the keypad).



If your site requires this functionality, tick the **Operate as cipher pad for Card + PIN** checkbox.

Notes:

- This feature can be disabled for visually impaired cardholders. See ***Adding a card to a Cardholder*** (on page 32-9) for further detail.
- Cipher pad functionality is not supported with the Car Park Management feature.

41. The **Allow assigning of system generated PIN** checkbox is only visible when the **View new PIN on first use at configured HBUS Terminals** checkbox (on the **Standards** tab of the Server Properties) is ticked.

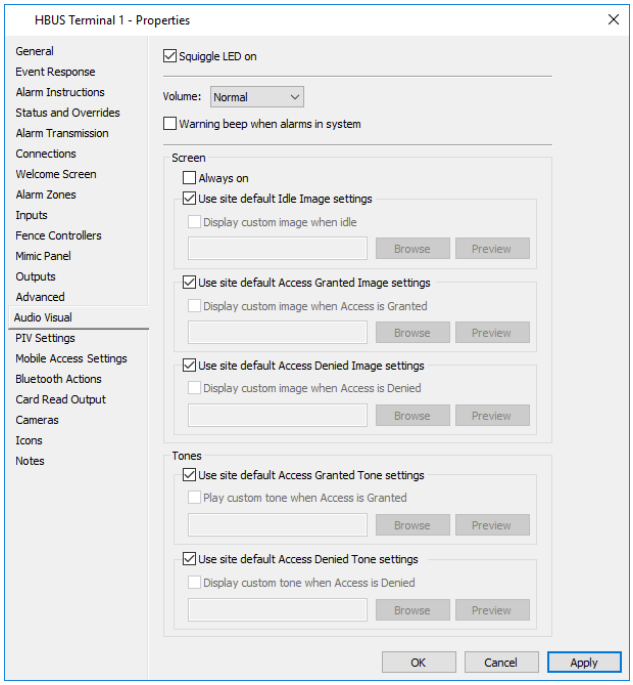
    Check this option if you want the system generated PINs to be displayed for 10 seconds on the HBUS Terminal on the first card badge, before moving onto the PIN entry (or scramble pad screen) for confirmation.



Notes:

- **Generate PIN** can be used to trigger re-issue of the PIN. The Controller must be online for the PIN to be re-issued.
- When a wrong PIN has been entered or when it has timed out, a new PIN will be generated and displayed on the terminal. A card access denied event appears if the wrong PIN is entered on the third attempt.
- Issuing of PIN fails when either:
  - Communication failure with the Server occurs while setting the PIN, or
  - When the PIN has already been assigned

42. Click the **Audio Visual** tab.



43. Configure the settings as required.

Field	Description
Squiggle LED on	The squiggle LED can be set to either OFF or ON. By default, this is checked so the squiggle LED will be ON. Unchecking it will turn the squiggle LED OFF.
Volume	This can be set to Off, Quiet, Normal or Loud. (Default = Normal)
Warning beep when alarms in system	When checked, the terminal will beep if an alarm is in the system. Configure the appropriate volume, as required. (Default = Unchecked)

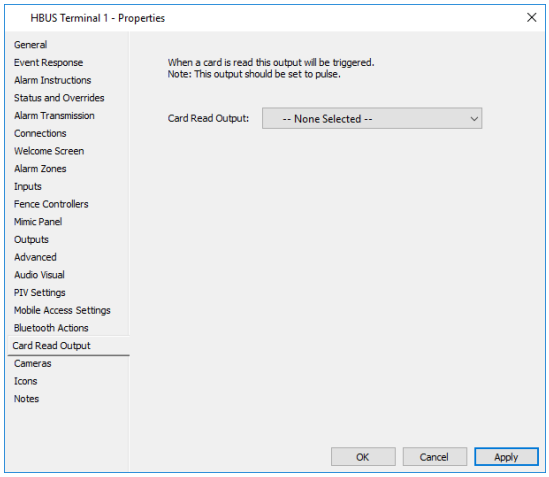
Screen	Check the **Always on** checkbox if you want the terminal screen to always be on. This option is useful when using the Mimic Panel functionality.
	The other options in this section allow you to display an Idle Image on the terminal, (e.g. company logo) instead of the Welcome screen, (i.e. when logged off), and/or a custom icon when access is granted or denied. The idle image will be displayed when the terminal has been idle for 10 seconds. Either:
	• leave the appropriate checkboxes checked, (i.e. **Use site default Idle Image settings**, **Use site default Access Granted Image settings** and/or **Use site default Access Denied Image settings**), to use the site wide image setting (configured on **HBUS Terminal Defaults 1** tab of the Server Properties), OR
	• uncheck the appropriate **Use site default...** check-box(es) and check the **Display custom image when...** checkbox below it instead to select an image for this terminal. Type in the name of the image file to be displayed or click the **Browse** button to locate the image file. **Notes:**
	  • When browsing for an image, only **.png**, **.jpg** and **.jpeg** files display.
	  • The image size should be 320x240 pixels.
	  • Select the **Preview** button, to preview how the image will look when displayed on the terminal.

Tones	These options allow you to play a tone on the terminal when access is granted and/or denied. Either:
	• leave the appropriate checkboxes checked, (i.e. **Use site default Access Granted Tone settings** and/or **Use site default Access Denied Tone settings**), to use the site wide tone setting (configured on the **HBUS Terminal Defaults 1** tab of the Server Properties), OR
	• uncheck the appropriate **Use site default…** check-box(es) and check the **Play custom tone when…** check-box below it instead to select a tone for this terminal. Type in the name of the sound file to be play-ed or click the **Browse** button to locate the sound file. **Notes:**
	  • When browsing for a sound file, only **.wav** and **.mp3** files display.
	  • The sound file will play for a maximum of 3 seconds, and will be no bigger than 100 kilobytes.
	  • Select the **Preview** button to review the selected tone.

Field	Description

- Tones can be distorted by the limited T20 speaker, therefore it is recommended custom tones are tested on T20 hardware.

44. Are you configuring an HBUS Reader or HBUS Terminal for Mobile Connect?
    If **yes**, refer to ***Configuring a reader for Mobile Connect*** (on page 31-11).
    If **no**, go to Step 44.
45. Do you want to associate a relay Output with this terminal, so that when a card is badged at the terminal, the relay will be triggered?
    If **yes**, go to Step 45. If **no**, go to Step 47.
46. Click the **Card Read Output** tab.



47. From the **Card Read Output** drop-down list (which includes virtual Outputs), select the Output to switch on when a card is badged at this terminal. **Note:** Badging a card at this terminal 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. **Recommendation:** 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 terminal at a time. Each terminal will cause the relay to pulse.
48. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this terminal. For further details, see ***Cameras*** (on page 3-24).
49. Click the **Icons** tab if you want to change the Icon Set for this terminal. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
50. Click the **Notes** tab if you want to add a note(s) about this terminal. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
51. 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 HBUS Terminal has been configured, assigned to a Controller 6000 or 7000, and is ready for use.

Configuring an HBUS Alarms Only Terminal

Introduction

This procedure describes how to configure an HBUS Alarms Only Terminal in Command Centre. Other procedures associated with configuring an HBUS Alarms Only Terminal are:

- ***Configuring Access Group Privileges for Terminal Access*** (on page 34-13)
- ***Configuring User Codes for Terminal Access*** (on page 32-23)
- ***HBUS Terminal Defaults*** (on page 6-67)

Notes:

- Operators require the "Edit Site" operator privilege to perform this procedure and must be in the same or parent Division of the HBUS Alarms Only Terminal.
- To change the date and time format, for all terminals, refer to the topic ***HBUS Terminal: Date and time format*** (on page 21-103).
- The language displayed on the terminal, is configured on the **Software** tab of the host Controller's properties. When configured for English text (the default), the terminal displays the month using abbreviations, (e.g. Jan, Feb, Mar). When configured for non-English text, the terminal displays the month as configured for the selected language. **Ensure you configure messages for terminals in the same language as is set on their host Controller's Software tab.**
- Command Centre data, (e.g. Event messages and item states) are sent to the terminal using the language selected on the Command Centre server. Command Centre editable fields, (e.g. Alarm Zone names and Input names) are sent to the terminal, as entered in Command Centre.

Minimum configuration requirements

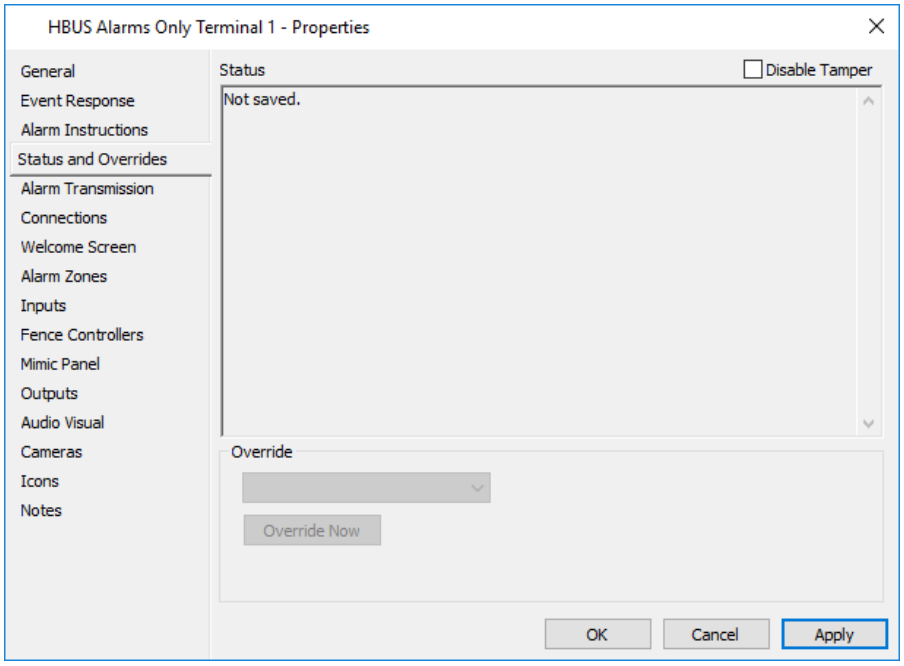
The terminal will display the message "Not Configured" unless the following configuration has been completed:

- On the **Connections** tab, assign the terminal to a Controller 6000 or 7000 and enter the terminal's HBUS serial number (10-character hexadecimal string).
- On the **Alarm Zones** tab, assign at least one Alarm Zone to the terminal.

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 **HBUS Alarms Only Terminal**.
   By default the **General** tab displays.
4. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).

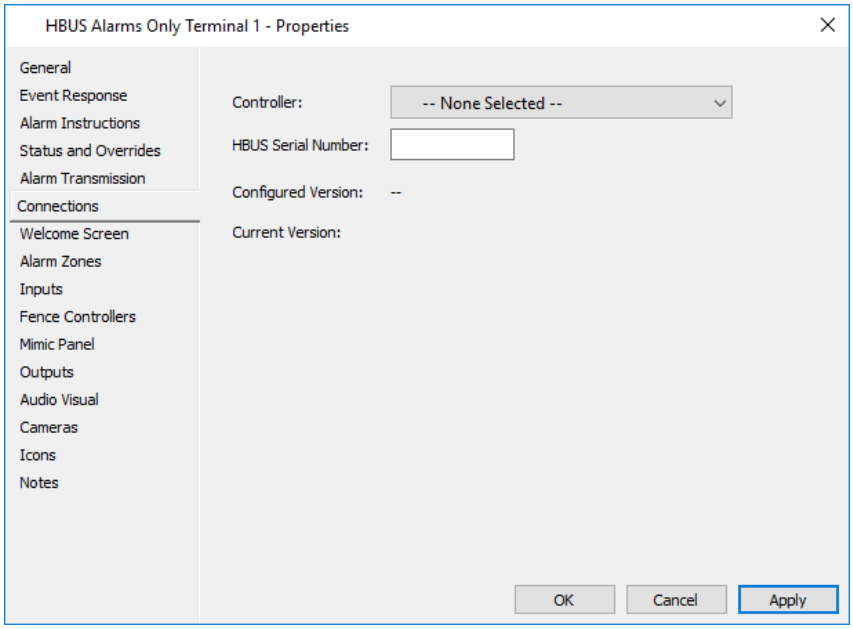
5. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
6. Click the **Alarm Instructions** tab, and configure as required.
   For further detail see ***Alarm Instructions tab*** (on page 3-22).
7. Click the **Status and Overrides** tab.



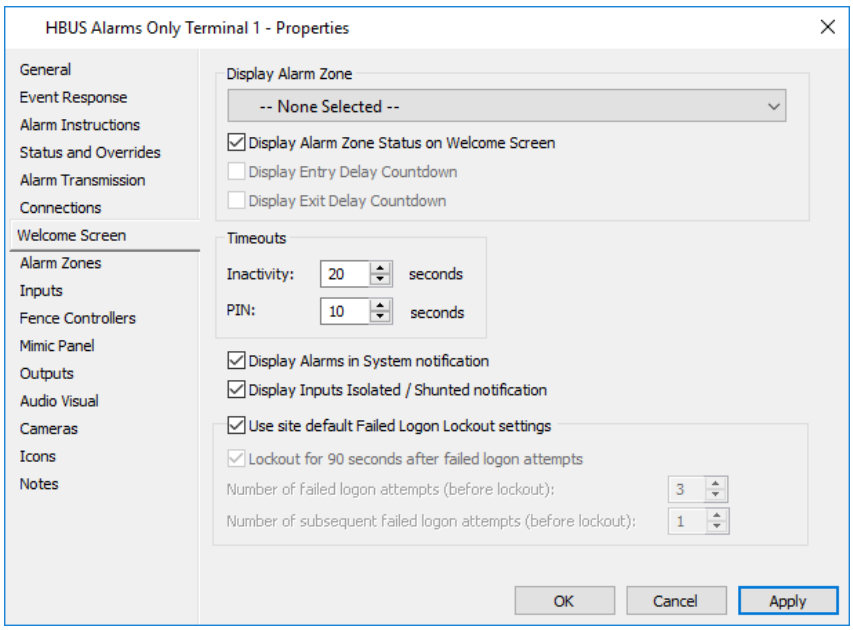
   If the terminal is removed (from the wall), a tamper alarm is generated. To prevent this from happening, tick the **Disable Tamper** checkbox.
8. To perform an override, click within the **Override** field and select the required override action from the drop-down list, then click the **Override Now** button.

   For a description on each of the override actions that can be performed for this device, see Performing Overrides.

   Note: This device does not support timed overrides. All overrides are immediate and persist until specifically cancelled by an operator.
9. Click the **Connections** tab.



10. Select the Controller 6000 or 7000 you want to assign this terminal to, from the **Controller** drop-down list.
    Notes:
    - HBUS Alarms Only Terminals can be created via the **HBUS Devices** tab of a Controller. In that case the **Controller** field would be pre-populated with that Controller name. Refer to the topic ***Configuring HBUS Devices*** (on page 21-65).
    - When a terminal is connected to a Controller 6000 or 7000 it will automatically be upgraded or downgraded to the version of T20 firmware held by the Controller. This will only happen if the terminal is correctly configured. A download bar displays on the **Connections** tab, showing the approximate progress of the download.
      If the download fails for whatever reason, the terminal will revert to the previous version of code. A Code Download Fail event is raised in Command Centre.
11. Enter the HBUS serial number (10-character hexadecimal string) into the **HBUS Serial Number** field. This serial number is located on the unit. **Note:** The HBUS serial number is optional, however the terminal will be considered as not properly configured unless one is entered.
12. If you click the **Apply** button, software version numbers display.
    The **Configured Version** is the version of the device software in the configured Controller FTS file, (i.e. **not** the version of the Controller software). The **Current Version** is the version of software as last reported by the terminal itself.
    Note: For the terminal to report its current version of software, an Alarm Zone must be assigned to the **Event Response** tab of the terminal's properties.
13. Click the **Welcome Screen** tab.



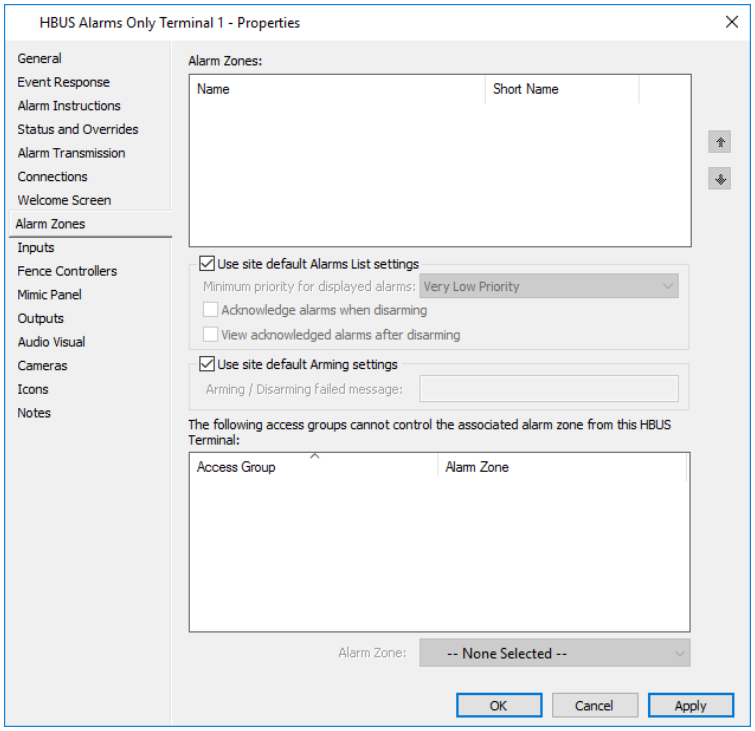
This screen enables you to display the status of a selected Alarm Zone and control the timeouts for this terminal, when a Cardholder attempts to log on using the function keys on this terminal.

14. Configure as required.

Field	Description
Display Alarm Zone	Select the Alarm Zone that will be displayed on the terminal, from the **Display Alarm Zone** drop-down list. When the Alarm Zone is armed, the armed icon displays. **Notes:** • The choice of Alarm Zone is restricted to only those associated with the terminal on the **Alarm Zones** tab. • Deselect the **Display Alarm Zone Status on Welcome Screen** checkbox, if you do not want to display the status of the Alarm Zone. • Check the **Display Entry Delay Countdown** and/or **Display Exit Delay Countdown** checkboxes if required. Displaying the Entry Delay Countdown informs a user of the time left before an alarm is triggered. Displaying the Exit Delay Countdown provides a user arming an Alarm Zone via the T20 an indication of how long they have left until exit delay expires. These checkboxes will be disabled if no Display Alarm Zone is selected.
Timeouts	In the **Inactivity** timeout field, enter the period of time (in seconds) of inactivity before a Cardholder will be logged off the terminal. Default 20 seconds. **Note:** If the terminal has not been used for 30 seconds, the screen and keypad backlight will dim. Hence if the inactivity period is greater than 30 seconds and the terminal has not

Field	Description
	been used, the screen and backlight will dim whilst the user is logged on. In the **PIN** timeout field, enter the period of time (in seconds) that a user has to enter their PIN or User Code at the terminal in order to log on. Default 10 seconds.
Display Alarms in System notifications	Deselect the **Display Alarms in System notification** checkbox, if you do not want to display the red alarm notification banner on the Welcome screen or Mimic Panel screen of the terminal.
Display Inputs Isolated / Shunted notification	Deselect the **Display Inputs Isolated / Shunted notification** checkbox, if you do not want to display the yellow isolated/shunted banner on the Welcome screen of the terminal, when one or more inputs in any of the Alarm Zones associated with the T20 is shunted or isolated. **Note:** If the Input is not assigned to the terminal, the banner will display without the ability for a user to address the issue directly from the terminal.
Use site default Failed Logon Lockout settings	Deselect the **Use site default Failed Logon Lockout settings** checkbox, if you want to configure the failed logon lockout settings specifically for this terminal. Select the **Lockout for 90 seconds after failed logon attempts** checkbox. The terminal will be locked out for a period of 90 seconds after the **Number of failed logon attempts** has been exceeded. Default 3. Range 3-10. If required, enter the **Number of subsequent failed logon attempts** to occur before the terminal is locked out again. Default 1. Range 1-10. **Notes:** • Failed Logon Lockout is configurable via the Server Properties. The default will be off for sites that already have T20s installed. For sites installing new T20s the default will be on. • The repeated use of the same user code or PIN will only count as a single attempt. • If the number of failed logon attempts reaches a certain number, then a tamper alarm is raised. This number is either the total of the two configurable amounts plus 1, or 7 attempts - whichever is reached first. The terminal will display the message "*Temporarily locked out*" with a red "X" on screen.

15. Click the **Alarm Zones** tab.



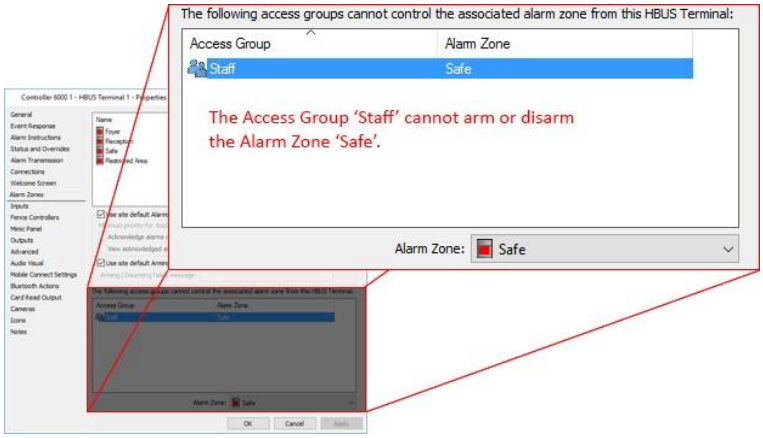
16. Click **Configure** from the menu bar, then **Alarm Zones**.
    The **Alarm Zone** List Window opens.
    Select the Alarm Zones you wish to associate with this terminal, and drag and drop them into the **Alarm Zones** grid.
    Notes:
    - In order to display Inputs, Outputs, Fence Controllers and Fence Zones within the terminal user interface, the Alarm Zones assigned to these items must be assigned to the terminal
    - Up to 50 Alarm Zones can be associated with one terminal. Assigning many Alarm Zones that are hosted by remote Controllers, may impact on the performance of the terminal.
    - All inactive/acknowledged alarms and all inactive/processed alarms older than 28 days are not displayed on the terminal.
    - Duress alarms are not displayed on the terminal.
    - A maximum of 200 alarms are displayed on the Current Alarms screen, listed in order of priority.
    - A maximum of 100 alarms are displayed on the Alarm History screen, listed in order of date/time occurrence.
    - The terminal cannot be assigned to an Elevator Car or Elevator Car HLI, if Alarm Zones have been assigned to the terminal.
    - If a Short Name has been entered for an Alarm Zone, this will be displayed in the terminal user interface, instead of the Name.
    - It is not possible to assign an HBUS Terminal with Alarm Zones to a Locker Bank.
17. Once you have all the Alarms Zones you require in the window, you can re-order the Alarm Zones by using the **up** and **down** arrow buttons to the right of the window.

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

18. Configure as required.

Field	Description
Use site default Alarms List settings	When checked, the terminal will use the Alarms List Defaults, configured on the **HBUS Terminal Defaults** tab in the Server Properties. By default, the terminal will display all alarms at or above 'Very Low Priority' for the Alarm Zone(s) assigned to the terminal. To configure the Alarm List settings specific for this terminal, deselect the **Use site default Alarm List settings** checkbox. Configure the Alarm List settings for this terminal as required. **Note:** The alarms displayed and acknowledged are determined by the Alarm Zones assigned to the Cardholder's Access Group(s) and the Terminal Privileges configured within these Access Groups.
Use site default Arming settings	When checked the terminal will use the Arming Defaults, configured on the **HBUS Terminal Defaults** tab in the Server Properties. By default, no arming/ disarming failed message is displayed. To configure the Arming settings specific for this terminal, deselect the **Use site default Arming settings** checkbox. Enter the arming/disarming failed message to be displayed by this terminal. Maximum 60 characters.

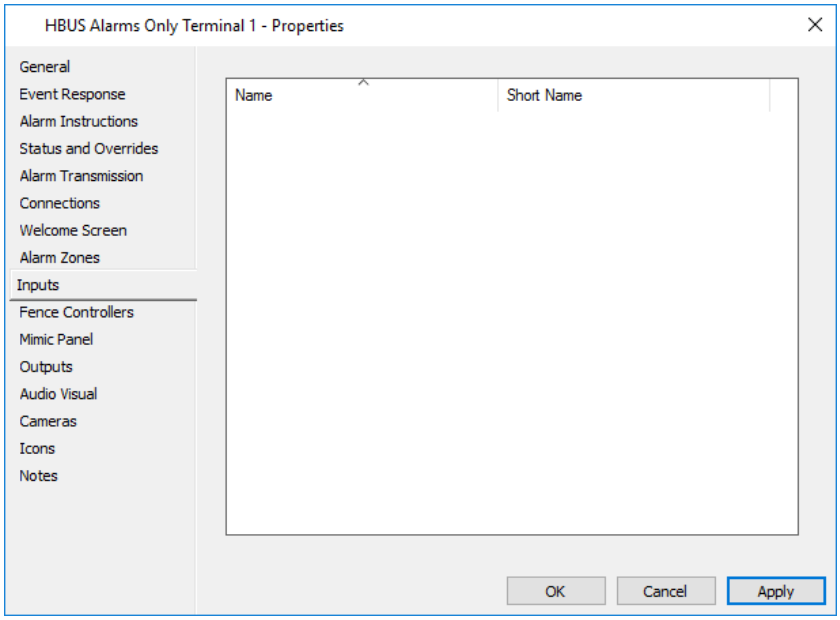
19. Depending on the required configuration, you can prevent certain Access Groups from Controlling (arming or disarming) a specified Alarm Zone from this terminal. Do you want to configure this option?
    If **yes**, go to Step 20.
    If **no**, go to Step 23.



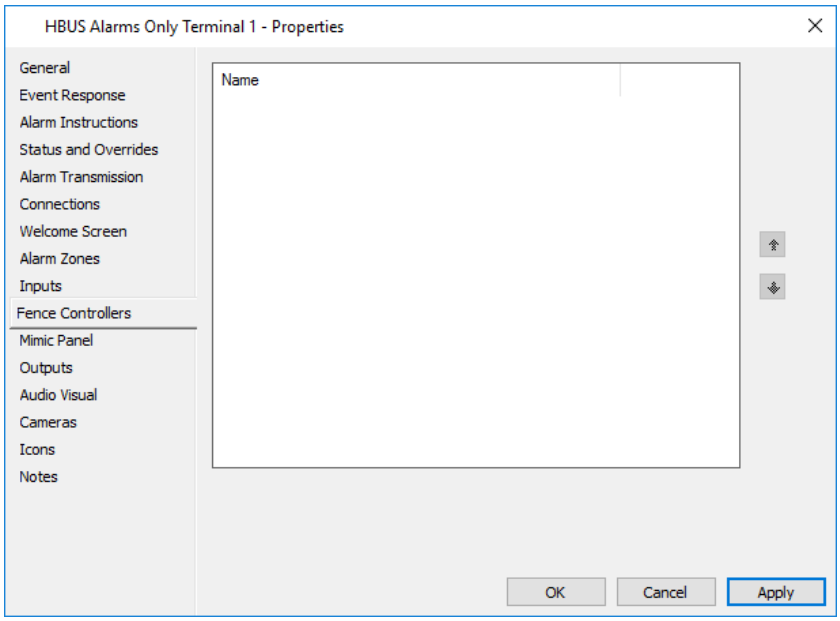
20. Click **Manage** from the menu bar, then **Access Groups**.
    The **Access Group** List Window opens.
    Select the Access Group(s) you wish to associate with this terminal, and drag and drop them into the bottom grid.

21. Click the Access Group to select it.
    The Alarm Zone drop-down list activates.

22. From the **Alarm Zone** drop-down list, select the Alarm Zone which you do not want the Access Group to Control (i.e. arm/disarm).
23. Click the **Inputs** tab.



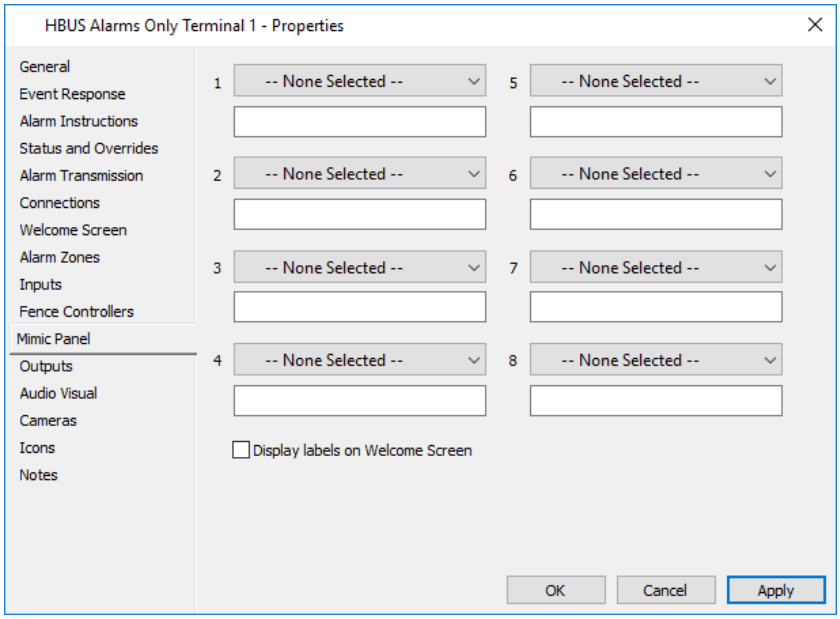
24. From the **Hardware** List Window, select the Inputs you wish to have controlled by this terminal, and drag and drop them into the **Inputs** tab.
    Notes:
    - Up to 100 Inputs can be monitored by one terminal.
    - If a Short Name has been entered for an Input, this will be displayed in the terminal user interface, instead of the Name.
25. Click the **Fence Controllers** tab.



This tab allows you to configure Fence Controllers so they can be monitored and controlled from this terminal.

26. From the Hardware List Window, select the Fence Controllers you wish to associate with this terminal, and drag and drop them into the **Fence Controllers** tab window.
    Notes:
    - Up to 25 Fence Controllers, (e.g. 50 Fence Zones) can be associated with one terminal.
    - Only F31, F32, F41, F42 and F22 Fence Controllers can be associated with this terminal.
27. Once you have all the Fence Controllers you require in the window, you can re-order the Fence Controllers by using the **up** and **down** arrow buttons to the right of the window.

    Note: The order you sort the Fence Controllers in here will be the order they appear in the terminal user interface.
28. Click the **Mimic Panel** tab



    This screen enables you to configure the 8 LEDs on either side of the terminal to show the status of Alarm Zones, Inputs or Outputs.
29. Select the drop-down arrow for the LED number (1-8) you wish to assign an Alarm Zone, Input or Output to. Select an Alarm Zone, Input or Output from the drop-down list.
    The item's name is automatically populated in the free text label field below.

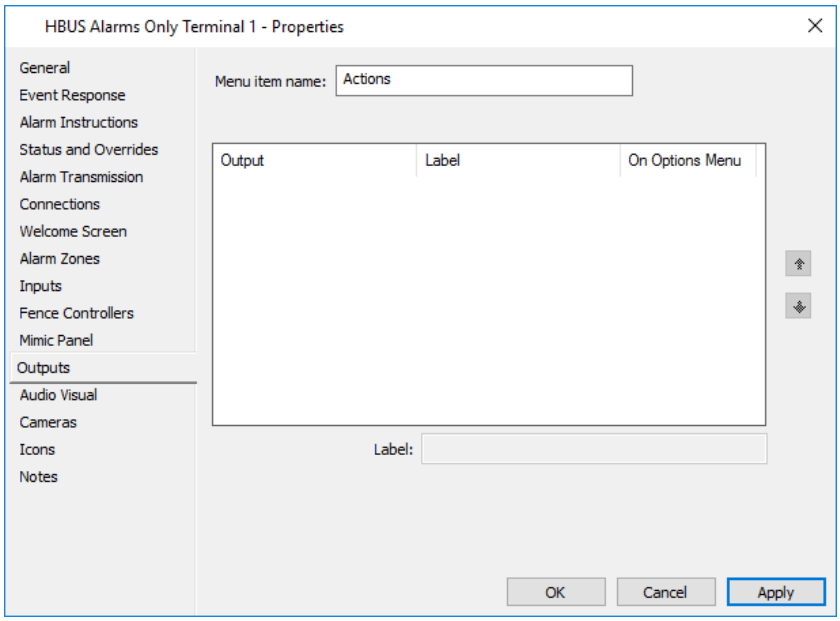
    To display the Alarm Zone, Input or Outputs name on the terminal, select the **Display labels on Welcome Screen** checkbox. The name shown in the free text label field will be displayed on the terminal beside the relevant LED, when the terminal is idle.

If required, edit the free text label field for each item. Maximum 60 characters.

Notes:

- Press the * key on the terminal to display the free text labels at any time.
- The colour of the LEDs and flash states can be configured on the **HBUS Terminal Defaults** tab in the Server Properties.

30. Click the **Outputs** tab.



31. From the **Hardware** List Window, select the Outputs you wish to trigger (On/Off) using this terminal.
    Drag and drop them into the **Outputs** tab window.

    The default **Menu item name** 'Actions' will be used within the terminal user interface. Change the **Menu item name**, if required. Maximum of 25 characters.

    The Output Name will be used within the terminal user interface. To use a different name within the terminal user interface, enter a **Label** for the Output. Maximum of 60 characters.

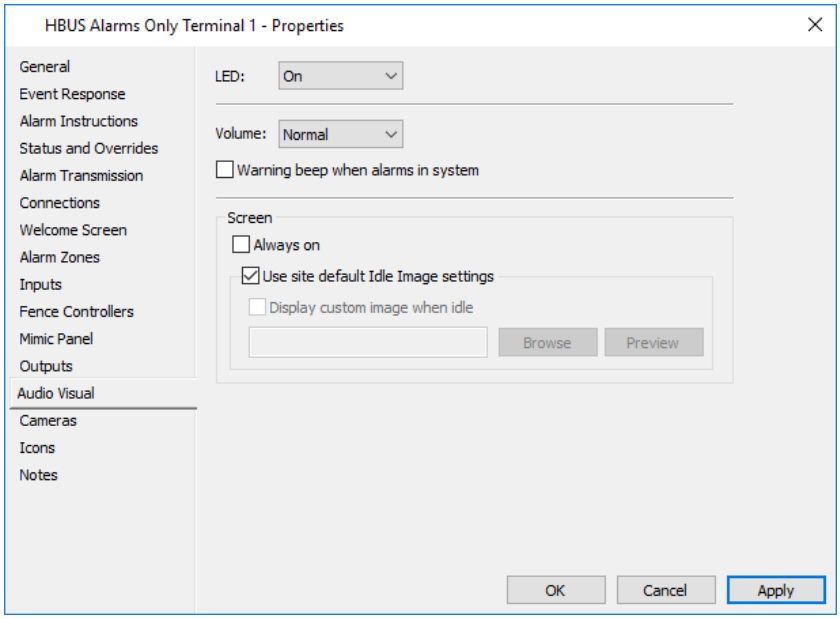
    If you require a non-authorised user, (i.e. terminal log on is not required) to be able to activate an Output, check the **On Options Menu** checkbox for the Output. The Output will appear on the Options Menu within the terminal user interface. A maximum of 5 Outputs can be added to the Options Menu. The Options softkey will only display if one or more Outputs have been configured to display on the Options Menu.

    Note: Up to 100 Outputs can be monitored by one terminal.

32. Once you have all the Outputs you require in the window, you can re-order the Outputs by using the **up** and **down** arrow buttons to the right of the window.

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

33. Click the **Audio Visual** tab.



34. Configure the settings as required.

Field	Description
LED	This can be set to either Off or On. (Default = On)
Volume	This can be set to Off, Quiet, Normal or Loud. (Default = Normal)
Warning beep when alarms in system	When checked, the terminal will beep if an alarm is in the system. Configure the appropriate volume, as required. Default = Unchecked
Screen	Check the **Always on** checkbox if you want the terminal screen to always be on. This option is useful when using the Mimic Panel functionality. You can display an Idle Image on the terminal, (e.g. company logo). This image will display instead of the Welcome screen, (i.e. when logged off) and the terminal has been idle for 10 seconds. Either: • leave the **Use site default Idle Image settings** checkbox checked to use the site wide image setting (on the **HBUS Terminal Defaults 1** tab of the Server Properties), OR • uncheck the **Use site default Idle Image settings** checkbox and check the **Display custom image when idle** checkbox instead to select an image for this terminal. Type in the name of the image file to be displayed or click the **Browse** button to locate the

Field	Description
	image file. **Notes:** • When browsing for an image, only **.png**, **.jpg** and **.jpeg** files display. • The image size should be 320x240 pixels. • Select the **Preview** button, to preview how the image will look when displayed on the terminal.

35. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this terminal. For further details regarding the **Cameras** tab, see ***Cameras*** (on page 3-24).
36. Click the **Icons** tab if you want to change the Icon Set for this terminal. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
37. Click the **Notes** tab if you want to add a note(s) about this terminal. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
38. 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 HBUS Alarms Only Terminal has been configured, assigned to a Controller 6000 or 7000, and is ready for use.

HBUS Terminal: Date and time format

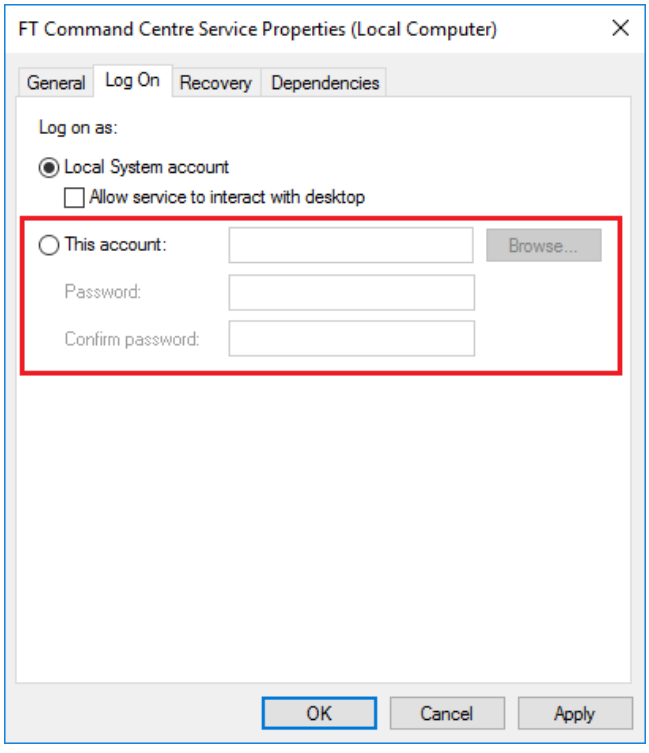
Date and time format

The date and time format displayed on HBUS Terminals, HBUS Alarms Only Terminals, and HBUS Contact Card Readers is determined by the "FT Command Centre Service" Local System account Region and Language setting. The default "FT Command Centre Service" logon account is Local System.

The Local System account Region and Language setting can be changed, as described here: *http://windows.microsoft.com/en-nz/windows7/apply-regional-and-language-settings-to-reserved-accounts*

Alternatively, the "FT Command Centre Service" can be configured to log on using a Local User or Domain User account. This account could have a different Region and Language setting to that of the Local System account.

To change the "FT Command Centre Service" logon account, open the properties of the "FT Command Centre Service". From the Windows **Start** menu, type *Services.msc* in the run field and press **Enter**. The Services window opens. Right click the service "FT Command Centre Service" and select **Properties**. Click the **Log On** tab and configure as required.



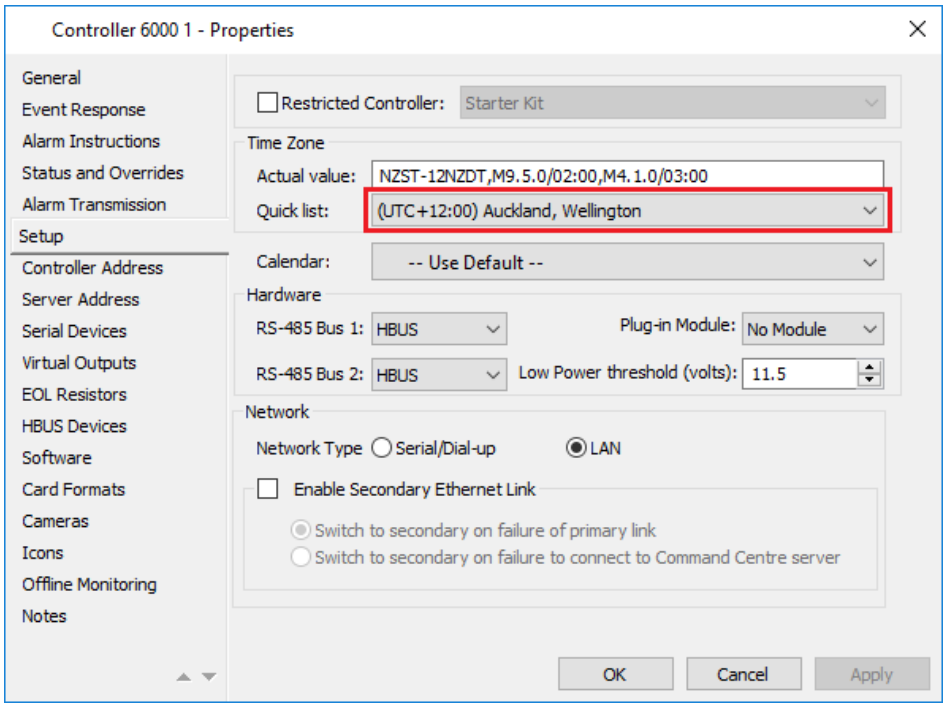
Notes:

- The Region and Language setting enables you to configure the date format, (e.g. day-month-year) and time format, (e.g. 24-hour time) to be displayed on all terminals.

- If there are any currently configured terminals in Command Centre when the Region and Language setting is changed, you will need to perform a 'Push Configuration' on each terminal (in order to display the date and time format change) or restart the "FT Command Centre Service".

Time zone

The time zone (date/time) displayed on a terminal is determined by the Time Zone configured on the host Controller's **Setup** property page.



HBUS Terminal: Overriding the Access Mode

Introduction

If the terminal or HBUS Contact Card Reader has been assigned as a Reader for a Door, the following procedure can be used to change the Access Mode for the Door's Access Zone, (e.g. from Secure to Free).

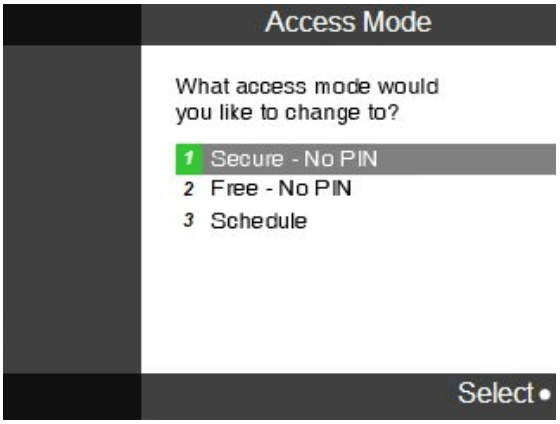
Notes:

- The Alarm Zone associated with the Door's Access Zone must be disarmed.
- You must have the 'Lock and unlock access zones' access privilege for the Door's Access Zone. Refer to Setting up Access Groups.

Method 1:

1. Press the **Mode** key.
2. Log on to the terminal.
   Notes:
   - The credentials required to log on to a terminal are configured on the **Welcome Screen** tab of the terminal item. By default, the first logon credential is 'Card'. By default, the second logon credential is 'PIN'.
   - If the terminal is assigned as the Reader for an Elevator Car, the **Mode** key is not displayed; hence it cannot be used to override the Access Mode for the Access Zones associated with the Elevator Car.

   If logon is successful, the Access Mode screen displays.



3. Press the key representing the Access Mode you require.

If you press...	then the Access Mode is...
1	overridden to Mode 1.
2	overridden to Mode 2.
3	overridden to the scheduled state.

Note: Mode 1 and Mode 2 are the Access Modes as configured on the **Access Mode** tab of the Access Zone properties. The scheduled state is the Access Mode currently defined in the Schedule associated with the Access Zone.

Method 2:

Present your card twice, (known as a 'double card override') at the terminal. This overrides the Access Mode of the Access Zone between Mode 2 and the scheduled state (as configured in Command Centre). If the override is successful, the Access Mode is changed and the message *"Override successful"* displays.

Notes:

- To use this feature, 'Double card overrides' must be set to 'Override access zone' on the **Advanced** tab of the terminal item.
- If the terminal is assigned as the Reader for an Elevator Car, it is recommended that double card overrides not be configured, because of the potential to accidentally override multiple Access Zones.
- Double card overrides are not supported when the Access Mode is set to Dual Auth.

HBUS Terminal: Overriding the Alarm Zone state to armed

Introduction

If the terminal or HBUS Contact Card Reader has been assigned as the Reader for a Door, the following procedure can be used to arm the Door's Access Zone Alarm Zone.

Note: You must have the 'Change to the Armed state' Alarm Zone privilege for the Alarm Zone. Refer to Setting up Access Groups.

Method 1:

1. Press the **Arm** key.

   Note: If the terminal is assigned as the Reader for an Elevator Car, the **Arm** key is not displayed; hence it cannot be used to override the Alarm Zones associated with the Elevator Car's Access Zones.

2. Log on to the terminal.

   Note: The credentials required to log on to a terminal are configured on the **Welcome Screen** tab of the terminal item. By default, the first logon credential is 'Card'. By default, the second logon credential is 'PIN'.

   If logon is successful, the message *"The system is armed"* and the Armed icon displays on the terminal.

Method 2:

Present your card twice, (known as a 'double card override') at the terminal. If arming is successful, the message *"The system is armed"* and the Armed icon displays.

Notes:

- To use this feature, 'Double card overrides' must be set to 'Arm alarm zone' on the **Advanced** tab of the terminal item.
- If the terminal is assigned as the Reader for an Elevator Car, it is recommended that double card overrides not be configured, because of the potential to accidentally override multiple Alarm Zones.

HBUS Terminal: Duress Code

Introduction

A duress code can be entered at a terminal or HBUS Contact Card Reader by a Cardholder to indicate that they are being threatened or forced to provide access under duress. Entering such a code generates a duress alarm. Duress alarms are raised in Command Centre but are not visible on the terminal/reader.

To raise a duress logon alarm:

1. Either:
   - Badge your card at the terminal/reader and enter your PIN, with the last digit incremented by one, OR
   - Enter your valid user code with the last digit incremented by one.

   For example:
   PIN / User code 1256 = Duress logon is 125**7**
   PIN / User code 1259 = Duress logon is 125**0**
2. Press the **Enter** key.

Configuring an HBUS Contact Card Reader

Introduction

This procedure describes how to configure an HBUS Contact Card Reader in Command Centre.

Other procedures associated with configuring an HBUS Contact Card Reader are:

- ***Configuring Access Group Privileges for Terminal Access*** (on page 34-13)
- ***Configuring User Codes for Terminal Access*** (on page 32-23)
- ***HBUS Terminal Defaults*** (on page 6-67)

Notes:

- Operators require the "Edit Site" operator privilege to perform this procedure and must be in the same or parent Division of the HBUS Contact Card Reader.
- To change the date and time format, for all HBUS Contact Card Readers, refer to the topic ***HBUS Terminal: Date and time format*** (on page 21-103).
- The language displayed on the HBUS Contact Card Reader, is configured on the **Software** tab of the host Controller's properties. When configured for English text (the default), the HBUS Contact Card Reader displays the month using abbreviations, (e.g. Jan, Feb, Mar). When configured for non-English text, the HBUS Contact Card Reader displays the month as configured for the selected language. **Ensure you configure messages for terminals in the same language as is set on their host Controller's Software tab.**
- Command Centre data, (e.g. Event messages and item states) are sent to the HBUS Contact Card Reader using the language selected on the Command Centre server. Command Centre editable fields, (e.g. Alarm Zone names and Input names) are sent to the HBUS Contact Card Reader, as entered in Command Centre.

PIV functionality

- Only PIV cards can be read by the reader's card slot.
- Global PINs are not supported. Application Pins only are supported.
- When using PIV cards, if the logon credentials are set to "Card" and "User Code", the reader will accept a card and PIV PIN only.
- When using PIV cards, duress logon and duress access are not supported.
- When using PIV cards, PIV PIN to PACS is not supported. When PIN entry is required, (e.g. the access mode is set to "Secure – PIN") you will need to insert your PIV card and enter your PIV PIN. Only the PIV PIN will be accepted.
- When using the Arm/Disarm/Mode soft keys and PIV cards, you will need to select the soft key prior to the card being inserted.

- When using two PIV cards for card entry, it is recommended that you increase the Door's **Second card (for two-card entry) must be swiped within** timeout to 10 seconds or greater; providing enough time to validate the first PIV card, then presentation or insertion of the second PIV card.
- When using PIV cards, the access decision is displayed when the card is removed from the reader. If a card is left in the reader longer than 40 seconds, the access decision will be cancelled.
- When using PIV cards, logon occurs when the card is removed from the reader, hence if the card is left in the reader accidentally, logon will occur when the card is removed.

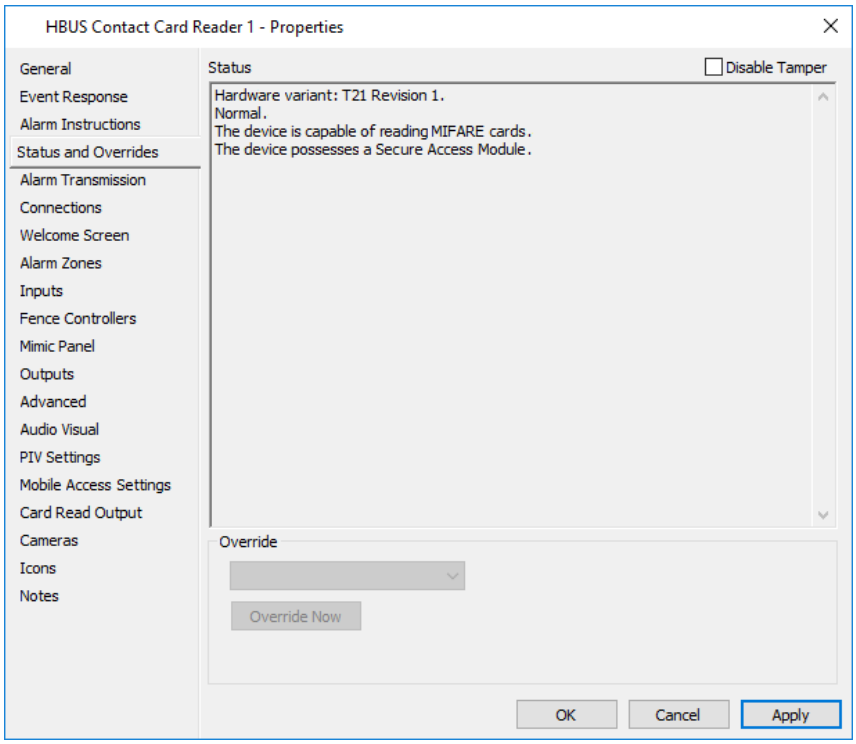
Minimum configuration requirements

The HBUS Contact Card Reader will display the message "Not Configured" unless the following configuration has been completed:

- On the **Connections** tab, assign the HBUS Contact Card Reader to a Controller 6000 or 7000, and enter the HBUS Contact Card Reader's HBUS serial number (10 character hexadecimal string).
- If using alarms management functionality, on the **Alarm Zones** tab, assign at least one Alarm Zone to the HBUS Contact Card Reader.
  Note: Alarms management functionality is not available when the HBUS Contact Card Reader is assigned as the Reader for an Elevator Car.
- If used for access control, assign the HBUS Contact Card Reader as the Reader for a Door or Elevator Car.

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 **HBUS Contact Card Reader**.
   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 **Status and Overrides** tab.

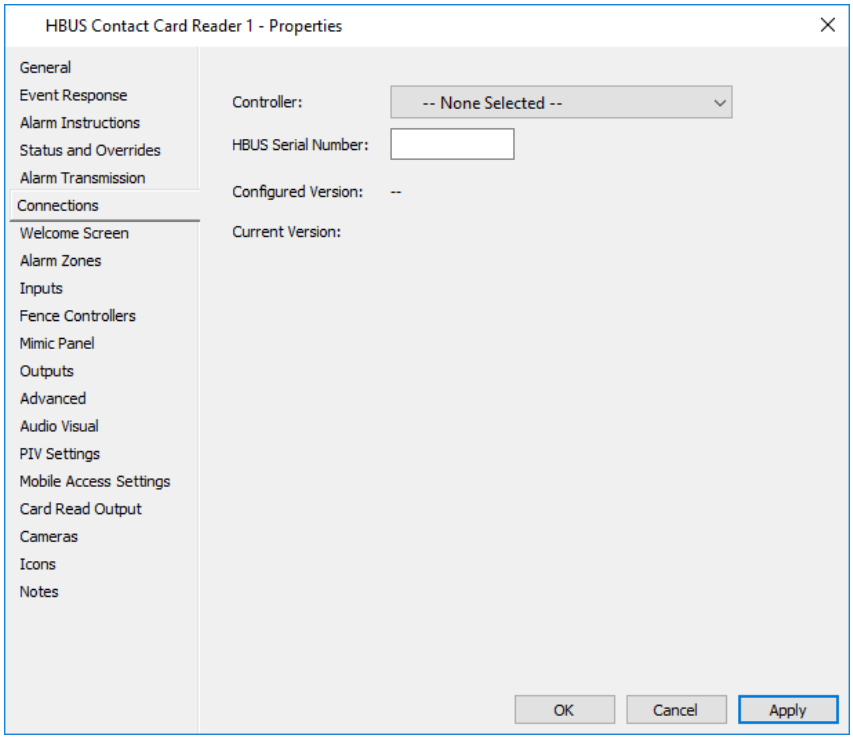


Information about the reader status, revision and supported card technologies display on this screen. For the T21 REV1 variant the status only updates when the reader goes offline.
Note: The T21 REV1 variant does not support 125 card technologies.

If the HBUS Contact Card Reader is removed (from the wall), a tamper alarm is generated. To disable the tamper, tick the **Disable Tamper** checkbox.

8. To perform an override, click within the **Override** field and select the required override action from the drop-down list, then click the **Override Now** button.

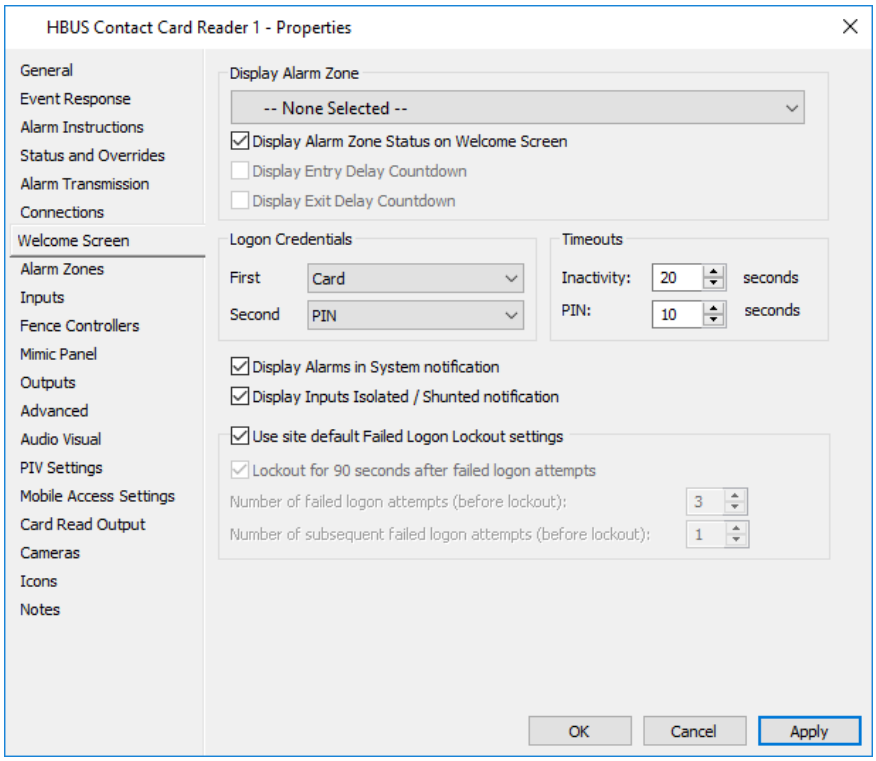
   For a description on each of the override actions that can be performed for this device, see ***Performing Overrides*** (on page 45-7).
   Note: This device does not support timed overrides. All overrides are immediate and persist until specifically cancelled by an operator.
9. Click the **Connections** tab.



10. Select the Controller 6000 or 7000 you want to assign this HBUS Contact Card Reader to, from the **Controller** drop-down list.
    Notes:
    - HBUS Contact Card Readers can be created via the **HBUS Devices** tab of a Controller. In that case the **Controller** field would be pre-populated with that Controller name. Refer to the topic ***Configuring HBUS Devices*** (on page 21-65).
    - When an HBUS Contact Card Reader is connected to a Controller 6000 or 7000 it will automatically be upgraded or downgraded to the version of T21 firmware held by the Controller. This will only happen if the HBUS Contact Card Reader is correctly configured. A download bar displays on the **Connections** tab, showing the approximate progress of the download.
      If the download fails for whatever reason, the HBUS Contact Card Reader will revert to the previous version of code. A Code Download Fail event is raised in Command Centre.
11. Enter the HBUS serial number (10-character hexadecimal string) into the **HBUS Serial Number** field. This serial number is located on the unit.
    Note: The HBUS serial number is optional, however the HBUS Contact Card Reader will be considered as not properly configured unless one is entered.
12. If you click the **Apply** button, software version numbers display.
    The **Configured Version** is the version of the device software in the configured Controller FTS file, (i.e. **not** the version of the Controller software). The **Current Version** is the version of software as last reported by the HBUS Contact Card Reader itself.

Note: For the HBUS Contact Card Reader to report its current version of software, an Alarm Zone must be assigned to the **Event Response** tab of the HBUS Contact Card Reader's properties.

13. Click the **Welcome Screen** tab.



This screen enables you to display the status of a selected Alarm Zone and control the logon credentials and timeouts for this HBUS Contact Card Reader, when a Cardholder attempts to log on or perform a local override using the function keys on this HBUS Contact Card Reader.

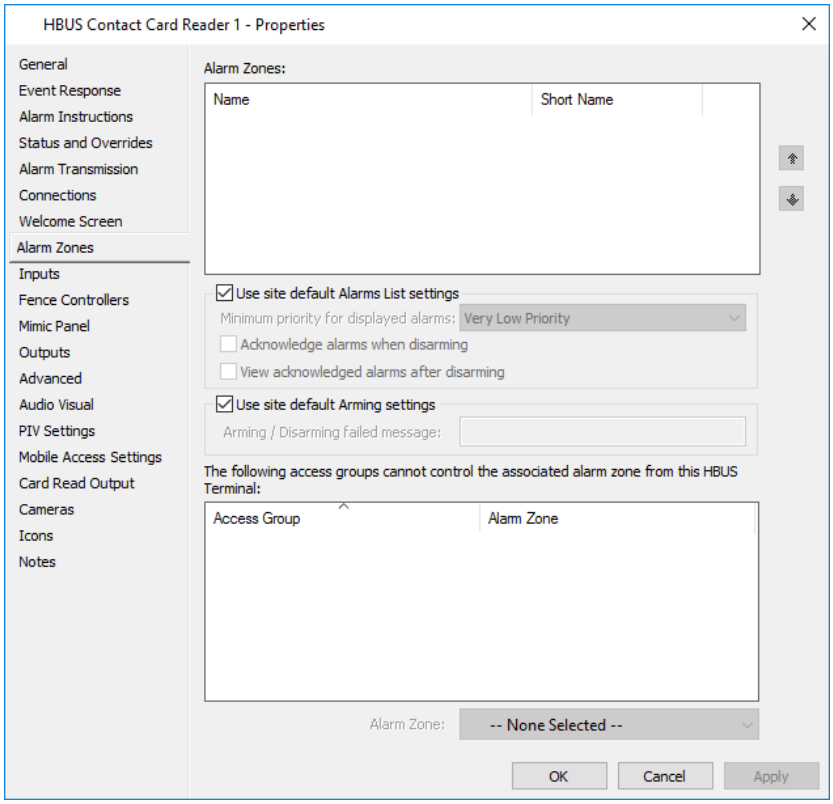
14. Configure as required.

Field	Description
Display Alarm Zone	Select the Alarm Zone that will be displayed on the HBUS Contact Card Reader, from the **Display Alarm Zone** drop-down list. When the Alarm Zone is armed, the armed icon displays. **Notes:** • When assigned as an entry reader, the **Display Alarm Zone** field is populated with the Alarm Zone assigned to the Door's entry Access Zone. When assigned as an exit reader, the **Display Alarm Zone** field is populated with the Alarm Zone assigned to the Door's exit Access Zone. • If not assigned as an entry or exit reader, the choice of Alarm Zone is restricted to only those associated with the HBUS Contact Card Reader on the **Alarm Zones** tab. • Deselect the **Display Alarm Zone Status on Welcome**

Field	Description
	Screen checkbox, if you do not want to display the status of the Alarm Zone. • Check the **Display Entry Delay Countdown** and/or **Display Exit Delay Countdown** checkboxes if required. Displaying the Entry Delay Countdown informs a user of the time left before an alarm is triggered. Displaying the Exit Delay Countdown provides a user arming an Alarm Zone via the HBUS Contact Card Reader an indication of how long they have left until exit delay expires. These checkboxes will be disabled if a Display Alarm Zone has not been selected or if the HBUS Contact Card Reader has been assigned as a reader.
Logon Credentials	Specify the first and second **Logon Credentials** required to log on to the HBUS Contact Card Reader. The default first logon credential required is "Card". The default second logon credential required is "PIN". **Note:** If you select "User Code" or "Card or User Code" as the **First** logon credential, then the **Second** credential field becomes disabled and displays "None".
Timeouts	In the **Inactivity** timeout field, enter the period of time (in seconds) of inactivity before a Cardholder will be logged off the HBUS Contact Card Reader. Default 20 seconds. **Note:** If the HBUS Contact Card Reader has not been used for 30 seconds, the screen and keypad backlight will dim. Hence if the inactivity period is greater than 30 seconds and the HBUS Contact Card Reader hasn't been used, the screen and backlight will dim whilst the user is logged on. In the **PIN** timeout field, enter the period of time (in seconds) that a user has to enter their PIN or User Code at the HBUS Contact Card Reader in order to log on. Default 10 seconds.
Display Alarms in System notifications	Deselect the **Display Alarms in System notification** checkbox, if you do not want to display the red alarm notification banner on the Welcome screen or Mimic Panel screen of the HBUS Contact Card Reader.
Display Inputs Isolated / Shunted notification	Deselect the **Display Inputs Isolated / Shunted notification** checkbox, if you do not want to display the yellow isolated/shunted banner on the Welcome screen of the HBUS Contact Card Reader, when one or more inputs in any of the Alarm Zones associated with the HBUS Contact Card Reader is shunted or isolated. **Note:** If the Input is not assigned to the HBUS Contact

Field	Description
	Card Reader, the banner will display without the ability for a user to address the issue directly from the HBUS Contact Card Reader.
Use site default Failed Logon Lockout settings	Deselect the **Use site default Failed Logon Lockout settings** checkbox, if you want to configure the failed logon lockout settings specifically for this HBUS Contact Card Reader. Select the **Lockout for 90 seconds after failed logon attempts** checkbox. The HBUS Contact Card Reader will be locked out for a period of 90 seconds after the **Number of failed logon attempts** has been exceeded. Default 3. Range 3-10. If required, enter the **Number of subsequent failed logon attempts** to occur before the HBUS Contact Card Reader is locked out again. Default 1. Range 1-10. **Notes:** • Failed Logon Lockout is configurable via the Server Properties. The default will be off for sites that already have HBUS Contact Card Readers installed. For sites installing new HBUS Contact Card Readers the default will be on. • The repeated use of the same user code or PIN will only count as a single attempt. • If the number of failed logon attempts reaches a certain number, then a tamper alarm is raised. This number is either the total of the two configurable amounts plus 1, or 7 attempts - whichever is reached first. The HBUS Contact Card Reader will display the message "*Temporarily locked out*" with a red "X" on screen. • The above settings are not applicable when using a PIV card. The PIV card will be locked after 5 consecutive failed PIN entries.

15. Click the **Alarm Zones** tab.



16. Click **Configure** from the menu bar, then **Alarm Zones**.
    The Alarm Zone List Window opens. Select the Alarm Zones you wish to associate with this HBUS Contact Card Reader, and drag and drop them into the **Alarm Zones** grid.
    Notes:
    - In order to display Inputs, Outputs, Fence Controllers and Fence Zones within the HBUS Contact Card Reader user interface, the Alarm Zones assigned to these items must be assigned to the HBUS Contact Card Reader.
    - Up to 50 Alarm Zones can be associated with one HBUS Contact Card Reader.
      Assigning many Alarm Zones that are hosted by remote Controllers, may impact on the performance of the HBUS Contact Card Reader.
    - All inactive/acknowledged alarms and all inactive/processed alarms older than 28 days are not displayed on the HBUS Contact Card Reader.
    - Duress alarms are not displayed on the HBUS Contact Card Reader.
    - A maximum of 200 alarms are displayed on the Current Alarms screen, listed in order of priority.
    - A maximum of 100 alarms are displayed on the Alarm History screen, listed in order of date/time occurrence.
    - The HBUS Contact Card Reader cannot be assigned to an Elevator Car or Elevator Car HLI, if Alarm Zones have been assigned to the HBUS Contact Card Reader.
    - If a Short Name has been entered for an Alarm Zone, this will be displayed in the HBUS Contact Card Reader user interface, instead of the Name.

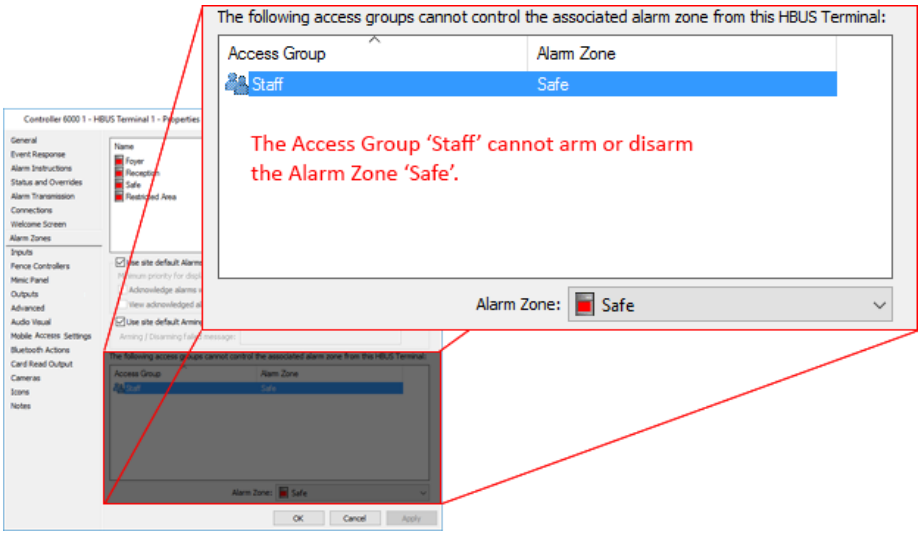
17. Once you have all the Alarms Zones you require in the window, you can re-order the Alarm Zones by using the **up** and **down** arrow buttons to the right of the window.

    Note: The order you sort the Alarm Zones in here will be the order they appear in the HBUS Contact Card Reader user interface.

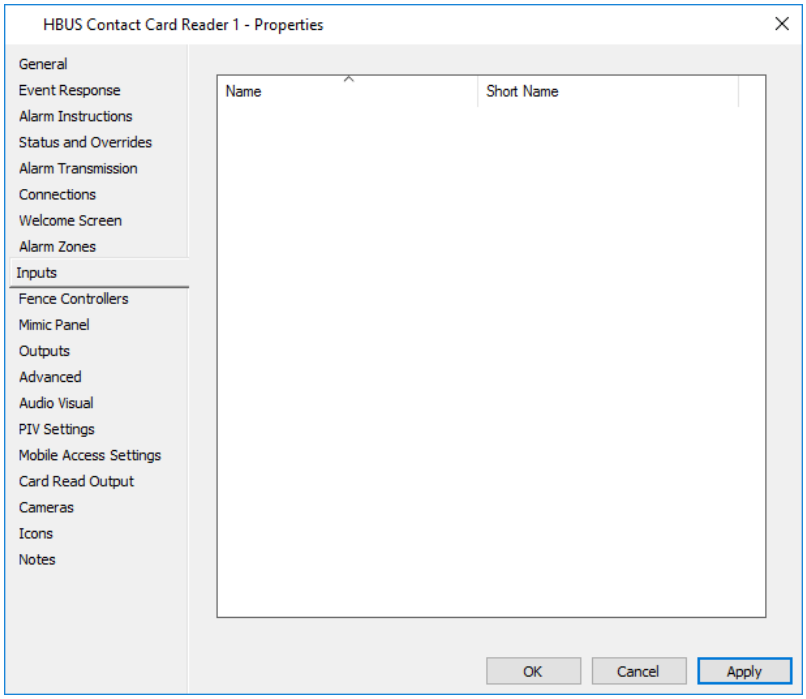
18. Configure as required.

Field	Description
Use site default Alarms List settings	When checked, the HBUS Contact Card Reader will use the Alarms List Defaults, configured on the **HBUS Terminal Defaults** tab in the Server Properties. By default the HBUS Contact Card Reader will display all alarms at or above 'Very Low Priority' for the Alarm Zone(s) assigned to the HBUS Contact Card Reader. **Note:** This functionality does not apply when disarming an Alarm Zone based on an access decision. To configure the Alarm List settings specific for this HBUS Contact Card Reader, deselect the **Use site default Alarm List settings** checkbox. Configure the Alarm List settings for this HBUS Contact Card Reader as required. **Note:** The alarms displayed and acknowledged are determined by the Alarm Zones assigned to the Cardholder's Access Group(s) and the Terminal Privileges configured within these Access Groups.
Use site default Arming settings	When checked, the HBUS Contact Card Reader will use the Arming Defaults, configured on the **HBUS Terminal Defaults** tab in the Server Properties. By default, no arming/disarming failed message is displayed. To configure the Arming settings specific for this HBUS Contact Card Reader, deselect the **Use site default Arming settings** checkbox. Enter the arming/disarming failed message to be displayed by this HBUS Contact Card Reader. Maximum 60 characters.

19. Depending on the required configuration, you can prevent certain Access Groups from Controlling (arming or disarming) a specified Alarm Zone from this terminal.
    Do you want to configure this option?
    If **yes**, go to Step 20.
    If **no**, go to Step 23.



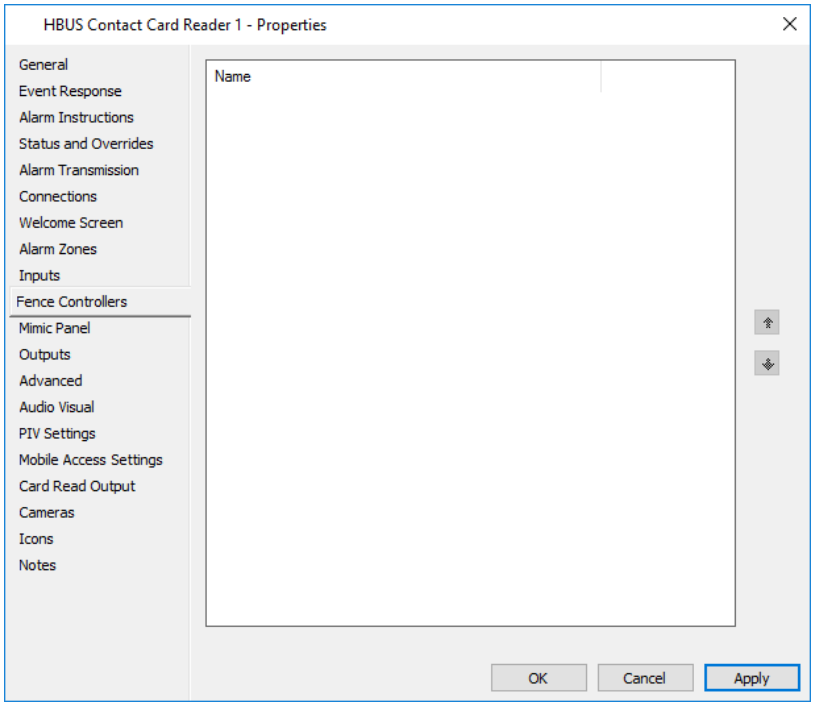
20. Click **Manage** from the menu bar, then **Access Groups**.
    The **Access Group** List Window opens.
    Select the Access Group(s) you wish to associate with this terminal, and drag and drop them into the bottom grid.
21. Click the Access Group to select it.
    The Alarm Zone drop-down list activates.
22. From the **Alarm Zone** drop-down list, select the Alarm Zone which you do not want the Access Group to Control (i.e. arm/disarm).
23. Click the **Inputs** tab.



24. From the **Hardware** List Window, select the Inputs you wish to have controlled by this HBUS Contact Card Reader.
    Drag and drop them into the **Inputs** tab window.
    Notes:
    - Up to 100 Inputs can be monitored by one HBUS Contact Card Reader.

- If a Short Name has been entered for an Input, this will be displayed in the HBUS Contact Card Reader user interface, instead of the Name.

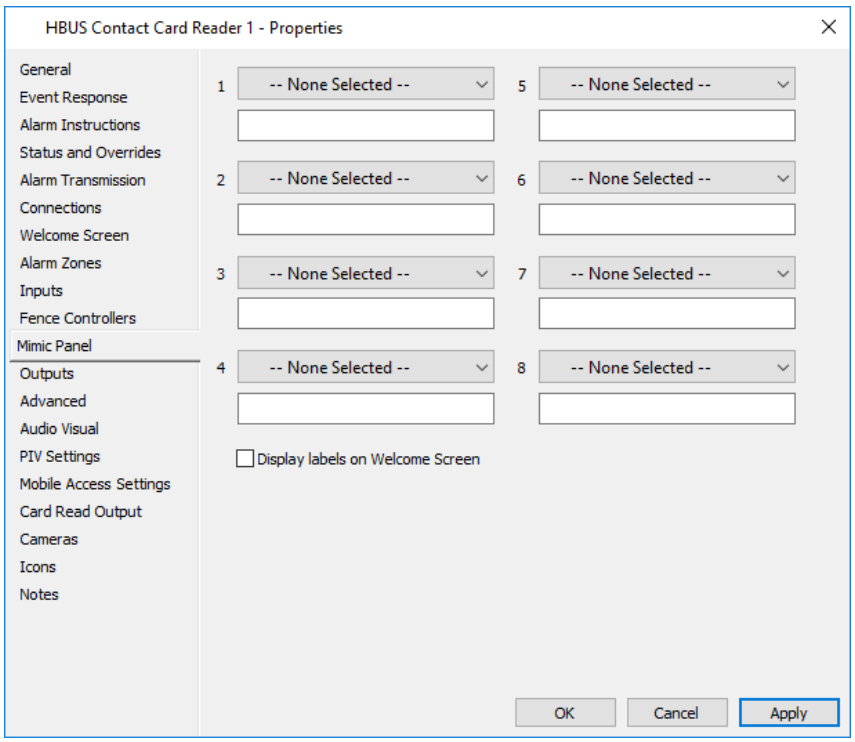
25. Click the **Fence Controllers** tab.



This tab allows you to configure Fence Controllers so they can be monitored and controlled from this HBUS Contact Card Reader.

26. From the Hardware List Window, select the Fence Controllers you wish to associate with this HBUS Contact Card Reader, and drag and drop them into the **Fence Controllers** tab window.
    Notes:
    - Up to 25 Fence Controllers, (e.g. 50 Fence Zones) can be associated with one HBUS Contact Card Reader.
    - Only F31, F32, F41, F42 and F22 Fence Controllers can be associated with this HBUS Contact Card Reader.
27. Once you have all the Fence Controllers you require in the window, you can re-order the Fence Controllers by using the **up** and **down** arrow buttons to the right of the window.

    Note: The order you sort the Fence Controllers in here will be the order they appear in the HBUS Contact Card Reader user interface.
28. Click the **Mimic Panel** tab.



This screen enables you to configure the 8 LEDs on either side of the HBUS Contact Card Reader to show the status of Alarm Zones, Inputs or Outputs.

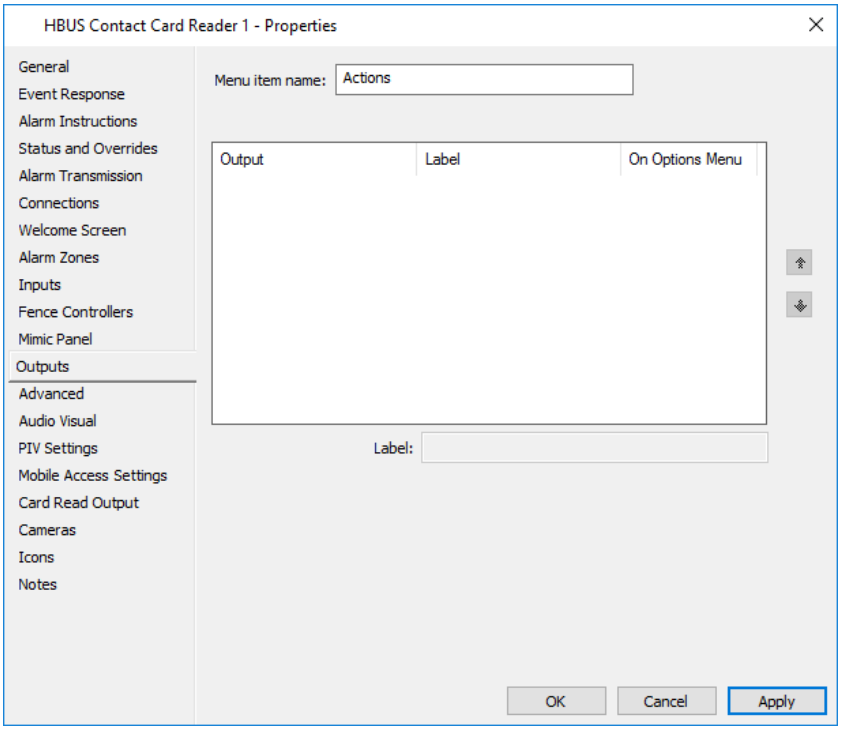
29. Select the drop-down arrow for the LED number (1-8) you wish to assign an Alarm Zone, Input or Output to. Select an Alarm Zone, Input or Output from the drop-down list.
    The item's name is automatically populated in the free text label field below.

    To display the Alarm Zone, Input or Outputs name on the HBUS Contact Card Reader, select the **Display labels on Welcome Screen** checkbox. The name shown in the free text label field will be displayed on the HBUS Contact Card Reader beside the relevant LED, when the HBUS Contact Card Reader is idle.

    If required, edit the free text label field for each item. Maximum 60 characters.
    Notes:

    - Press the ***** key on the HBUS Contact Card Reader to display the free text labels at any time.
    - The colour of the LEDs and flash states can be configured on the **HBUS Terminal Defaults** tab in the Server Properties.

30. Click the **Outputs** tab.



31. From the **Hardware** List Window, select the Outputs you wish to trigger (On/Off) using this HBUS Contact Card Reader.
    Drag and drop them into the **Outputs** tab window.

    The default **Menu item name** 'Actions' will be used within the HBUS Contact Card Reader user interface. Change the **Menu item name**, if required. Maximum of 25 characters.

    The Output Name will be used within the HBUS Contact Card Reader user interface. To use a different name within the HBUS Contact Card Reader user interface, enter a **Label** for the Output. Maximum of 60 characters.

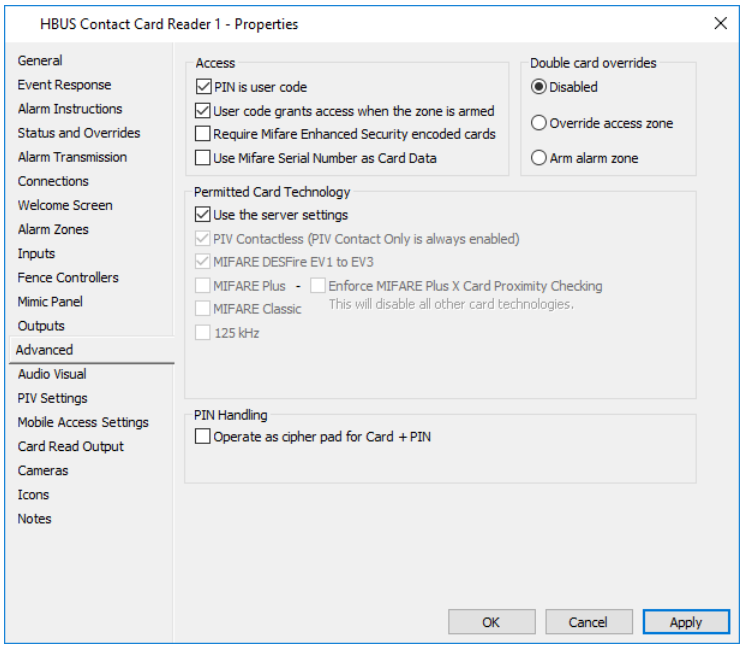
    If you require a non-authorised user, (i.e. HBUS Contact Card Reader log on is not required) to be able to activate an Output, check the **On Options Menu** checkbox for the Output. The Output will appear on the Options Menu within the HBUS Contact Card Reader user interface. A maximum of 5 Outputs can be added to the Options Menu. The Options softkey will only display if one or more Outputs have been configured to display on the Options Menu.

    Note: Up to 100 Outputs can be monitored by one HBUS Contact Card Reader.

32. Once you have all the Outputs you require in the window, you can re-order the Outputs by using the **up** and **down** arrow buttons to the right of the window.

    Note: The order you sort the Outputs in here will be the order they appear in the HBUS Contact Card Reader user interface.

33. Click the **Advanced** tab.



34. Configure as required.

Field	Description
PIN is user code	When checked the Cardholder's user code will be required in place of a PIN for any access transactions at this HBUS Contact Card Reader and the **User Code grants access when the zone is armed** option activates. **Notes:** • For Access Mode and Arming local overrides, the HBUS Contact Card Reader uses the Log On Credentials configured on the **Welcome Screen** tab of the HBUS Contact Card Reader. • PIN is user code is not supported when using PIV cards for access.
User code grants access when the zone is armed	When checked, a Cardholder can gain access to an armed zone using User Code without disarming any Alarm Zone. However, if the Cardholder has the 'Change to Disarmed state' privilege, the Alarm Zone(s) will be disarmed upon access. **Note:** To be able to select this option, you need to select the **PIN is user code** checkbox first.
Require MIFARE Enhanced Security encoded cards	When checked, the HBUS Contact Card Reader is instructed to only accept cards that have the enhanced security data when deciding whether to grant a Cardholder access. The MIFARE Enhanced security key is configured on the **Card Security** tab of the Server Properties. **IMPORTANT:** When this checkbox is unchecked, the HBUS Contact Card Reader will be instructed not to send the enhanced security data to the Controller, even if present. Leave this checkbox unchecked in the following situations:

Field	Description
	1. When not using the MIFARE Enhanced Security feature or when not using it for part of a site. 2. When some Cardholders requiring access using this HBUS Contact Card Reader have not yet had their cards re-encoded. It is important to remember to enable the setting once all cards have been re-encoded. Disabling this setting will also allow cards encoded at sites using the MIFARE Enhanced Security feature to be used at sites who are not using this feature. In the event of this being enabled, all low security cards will be denied with an event saying *"Denied - MIFARE High Security Card Required at [Door]"*. To enable both high and low security cards to be used uncheck the checkbox for the Door Reader.
Use MIFARE Serial Number as Card Data	HBUS Contact Card Readers can be set to read the Card Serial Number (CSN) from a MIFARE Card and use it to identify a Cardholder in Command Centre. When enabled, this allows the HBUS Contact Card Reader to send the CSN as Cardholder identification to the Controller if it does not detect any other form of Cardholder identification on the card. **Additional required configuration:** For the Controller to interpret the CSN as a Cardholder's card number, you also need to configure and assign a Universal Card Format. Once this is configured, you can assign cards to Cardholders using the CSN as the card 'Number'. See ***Universal Card Formats for 'Use MIFARE Serial Number as Card Data' (CSN mode)*** (on page 26-11) for the procedure.

35. If you want to configure **Double card overrides** for this HBUS Contact Card Reader, see Configuring Local Overrides at Card Readers for further instructions.
    Note: 'Double card overrides' are not supported when using PIV cards.
36. In the Permitted Card Technology section, **Use the server settings** is selected by default. If you want to select other types of cards to be accepted at the reader, uncheck the **Use the server settings** checkbox and select the appropriate checkboxes.
37. If your site is using MIFARE Plus cards with the 'X' feature set and you wish to prevent relay attacks occurring over HBUS, check the **MIFARE Plus** checkbox to enable the **Enforce MIFARE Plus X Card Proximity Checking** checkbox.
38. Check the **Enforce MIFARE Plus X Card Proximity Checking** checkbox.
    The HBUS Contact Card Reader will perform proximity checks when reading a MIFARE Plus X card. **Notes:**

- Checking this option disables all other card technologies.
- The **Enforce MIFARE Plus X Card Proximity Checking** feature will only work if the site that issued the card is using the same MIFARE Plus/DESFire key seed as your site.
- Operators need the "Edit Site" privilege to be able to amend this setting.
- For the HBUS Contact Card Reader to accept both contact and contactless PIV cards, check the **PIV Contactless** checkbox in the Card Technology Enforcement section.
- For the non Multi Tech variant, all 125 kHz cards will be denied.

39. The **Operate as cipher pad for Card + PIN** option allows sites to reduce the risk of cardholder PINs being discovered by someone looking over a cardholder's shoulder while they enter their PIN at the reader.



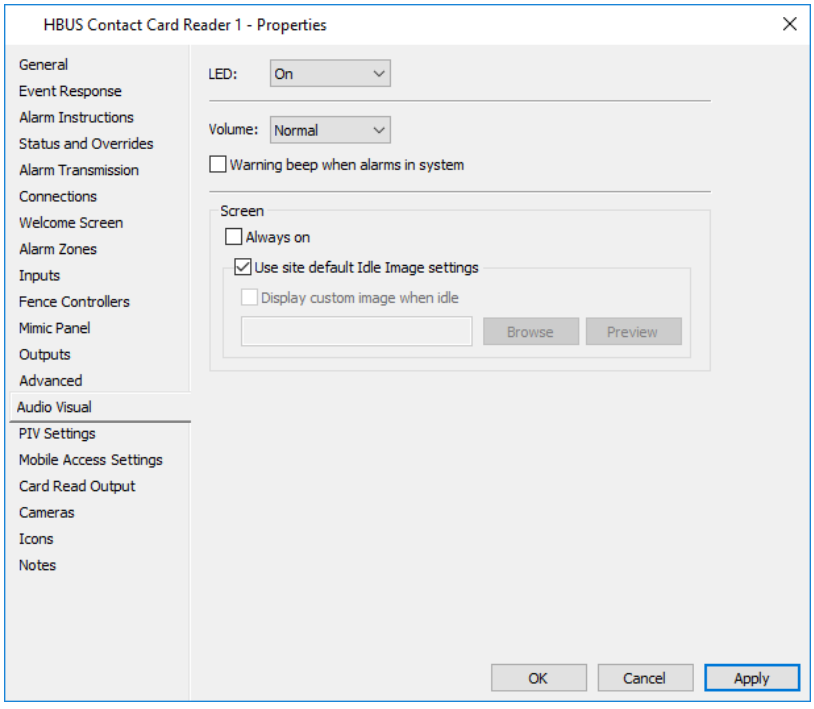
With this option enabled and the reader in PINs mode, each time a user badges their card a randomised number keypad will display on the reader screen. Users then need to follow the scrambled keys on the screen to enter their PIN correctly, (e.g. for the PIN 1234, the user would have to press 5170 on the keypad).

If your site requires this functionality, tick the **Operate as cipher pad for Card + PIN** checkbox.

Notes:

- This feature can be disabled for visually impaired cardholders. See ***Adding a card to a Cardholder*** (on page 32-9) for further detail.
- Cipher pad functionality is not supported with the Car Park Management feature.

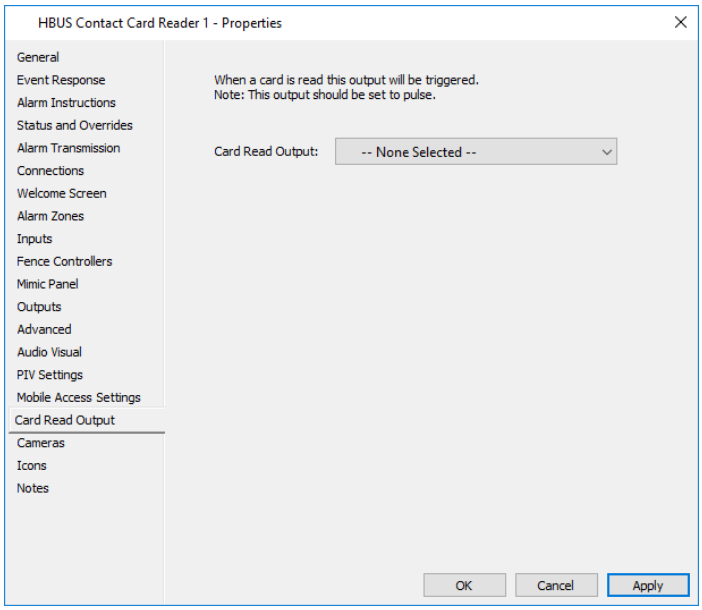
40. Click the **Audio Visual** tab.



41. Configure the settings as required.

Field	Description
LED	This can be set to either Off or On. (Default = On)
Volume	This can be set to Off, Quiet, Normal or Loud. (Default = Normal)
Warning beep when alarms in system	When checked, the HBUS Contact Card Reader will beep if an alarm is in the system. Configure the appropriate volume, as required. (Default = Unchecked)
Screen	Check the **Always on** checkbox if you want the HBUS Contact Card Reader screen to always be on. This option is useful when using the Mimic Panel functionality. You can display an Idle Image on the HBUS Contact Card Reader, (e.g. company logo). This image will display instead of the Welcome screen, (i.e. when logged off) and the HBUS Contact Card Reader has been idle for 10 seconds. Either: • leave the **Use site default Idle Image settings** checkbox checked to use the site wide image setting (configured on the **HBUS Terminal Defaults 1** tab of the Server Properties), OR • uncheck the **Use site default Idle Image settings** checkbox and check the **Display custom image when idle** checkbox instead to select an image for this HBUS Contact Card Reader. Type in the name of the image file to be displayed or click the **Browse** button to locate the image file. **Notes:** • When browsing for an image, only **.png**, **.jpg** and **.jpeg** files display. • The image size should be 320x240 pixels. • Select the **Preview** button, to preview how the image will look when displayed on the HBUS Contact Card Reader.

42. Do you want to associate a relay Output with this HBUS Contact Card Reader, so that when a card is badged at the HBUS Contact Card Reader, the relay will be triggered?
    If **yes**, then go to Step 43.
    If **no**, then go to Step 45.
43. Click the **Card Read Output** tab.



44. From the **Card Read Output** drop-down list (which includes virtual Outputs), select the Output to switch on when a card is badged at this HBUS Contact Card Reader.
    Note: Badging a card at this HBUS Contact Card 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.
    Recommendation: 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 HBUS Contact Card Reader at a time. Each HBUS Contact Card Reader will cause the relay to pulse.
45. 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).
46. Click the **Icons** tab if you want to change the Icon Set for this HBUS Contact Card Reader. For further details see ***Icons*** (on page 6-80).
47. Click the **Custom Fields** tab if you want to add and assign a custom field value to this HBUS Contact Card Reader.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
48. Click the **Notes** tab if you want to add a note(s) about this HBUS Contact Card Reader. For further details see ***Notes*** (on page 6-85).
49. 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 HBUS Contact Card Reader has been configured, assigned to a Controller 6000 or 70000, and is ready for use.

Configuring an HBUS I/O Interface

Introduction

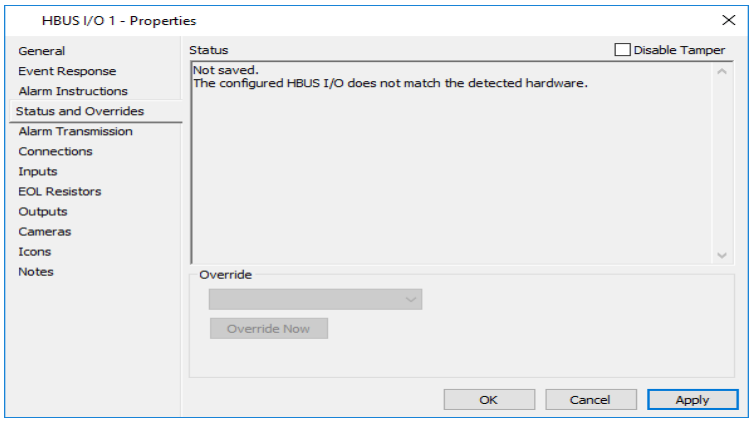
The HBUS I/O Interface enables you to configure an HBUS I/O expansion board, (i.e. 8-In Board, 8-In 2-Out Door Module, 8-In 4-Out Board, 16-In 16-Out Board, or 4-In 2-Out Door Module - Wiegand) in Command Centre.

Notes:

- By default, the 8-In 2-Out Door Module is selected when the HBUS I/O Interface is first created. You will need to select the correct hardware variant when configuring the HBUS I/O Interface.
- Operators require the "Edit Site" operator privilege to perform this procedure, and must be in the same or parent Division of the HBUS I/O Interface.

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 **HBUS I/O**. 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 **Status and Overrides** tab.



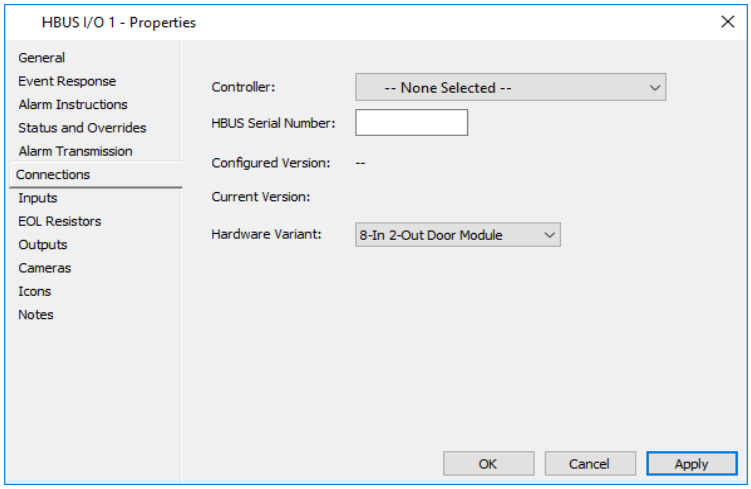
   To prevent continuous tamper alarms, tick the **Disable Tamper** checkbox.

   Notes:

   - The 16-In 16-Out Board has a Disable Front Tamper and a Disable Rear Tamper checkbox so that the Tampers can be enabled/disabled independently.
   - When correctly configured, the detected hardware variant is displayed in the Status field.
8. To perform an override, click within the **Override** field and select the required override action from the drop-down list, then click the **Override Now** button.

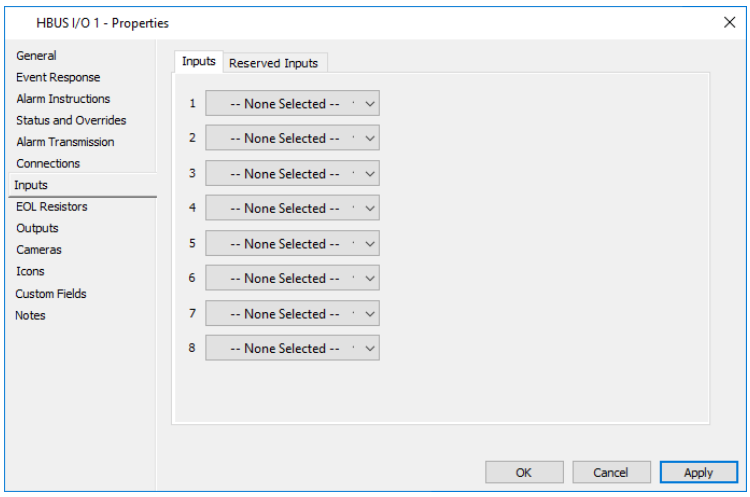
For a description on each of the override actions that can be performed refer to Performing Overrides.
Note: This device does not support timed overrides. All overrides are immediate and persist until specifically cancelled by an operator.

9. Click the **Connections** tab.

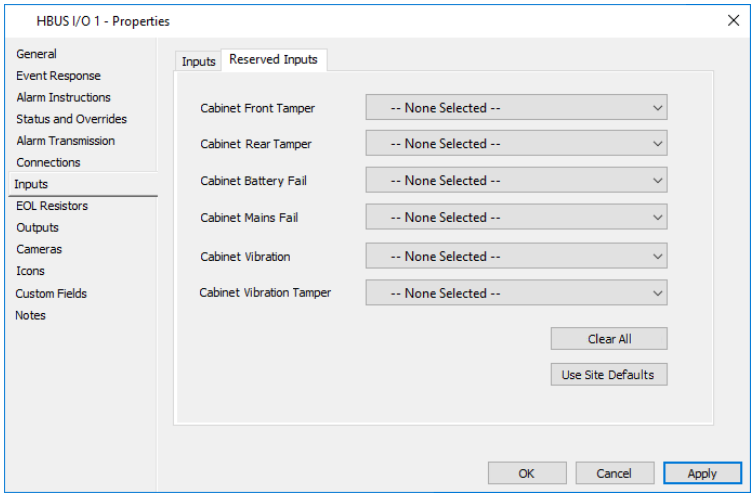


10. Select the Controller 6000 or 7000 you want to assign this HBUS I/O Interface to, from the **Controller** drop-down list. **Notes:**
    - HBUS I/O Interfaces can be created via the **HBUS Devices** tab of a Controller. In that case the **Controller** field would be pre-populated with that Controller name. Refer to ***Configuring HBUS Devices*** (on page 21-65).
    - When an HBUS I/O Interface is connected to a Controller 6000 or 7000 it will automatically be upgraded or downgraded to the version of I/O firmware (vHI firmware) held by the Controller. This will only happen if the HBUS I/O Interface is correctly configured. A download bar displays on the **Connections** tab, showing the approximate progress of the download. If the download fails for whatever reason, the HBUS I/O Interface will revert to the previous version of code. A Code Download Fail event is raised in Command Centre.
11. Enter the HBUS serial number (10 character hexadecimal string) into the **HBUS Serial Number** field. This serial number is located on the board sticker.
    Note: The HBUS serial number is optional, however the I/O Interface will be considered as not properly configured unless one is entered.
12. If you click the **Apply** button, software version numbers display. The **Configured Version** is the version of the device software in the configured Controller FTS file, (i.e. **not** the version of the Controller software).
    The **Current Version** is the version of software as last reported by the HBUS I/O Interface itself.
    Note: For the HBUS I/O Interface to report its current version of software, an Alarm Zone must be assigned to the **Event Response** tab of the HBUS I/O's properties.

13. Select the appropriate hardware variant, from the **Hardware Variant** drop-down list. **Notes:**
    - 'Bad Unit' type alarms may occur if the hardware variant attached to the Controller does not match to the hardware variant selected.
    - If "4-In 2-Out Door Module - Wiegand" was selected from the Hardware Variant drop-down list, an additional **Readers** tab will appear after the **Outputs** tab.
14. Click the **Inputs** tab.
    Note: The appearance of this screen may differ depending on the hardware variant selected, (e.g. If "4-In 2-Out Door Module - Wiegand" was selected, there will only be 4 Inputs available).
    Likewise, the **Reserved Inputs** sub-tab will not appear if either "8-In 2-Out Door Module" or "4-In 2-Out Door Module - Wiegand" were selected, as these variants do not support reserving inputs.
    The **Reserved Inputs** sub-tab provides a simple way of designating physical tampers and power supply monitoring inputs.



15. Assign each Input to the correct address. For details on how to create an Input, refer to ***Creating Inputs and Outputs*** (on page 21-50).
16. If applicable, click the **Reserved Inputs** sub-tab.
    Note: Operators require the "Edit Site" privilege to reserve inputs.

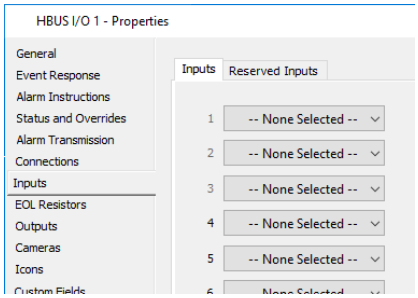


By default, all the Reserved Inputs will have "—None Selected --". They will however already be populated if the **Reserve inputs on creation of**

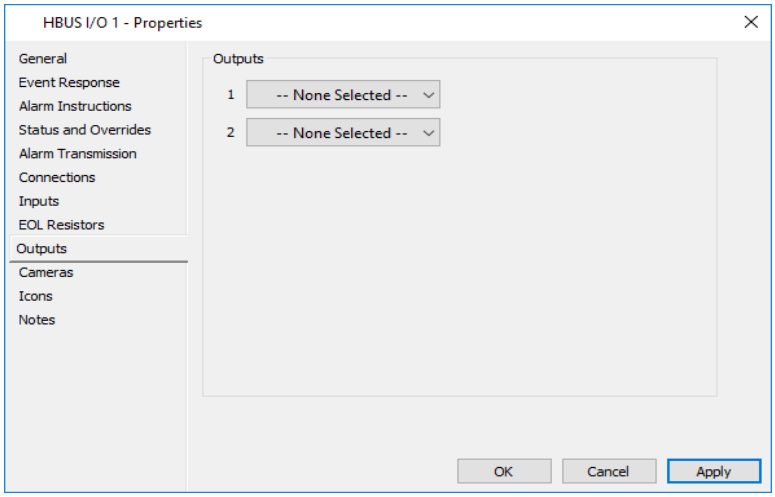
I/O module checkbox has been ticked on the Server Properties **Reserved Input Defaults** tab.

17. If the fields are not already populated or have been changed, and you want to set the site defaults from the Server Properties, click the **Use Site Defaults** button, otherwise select the required input for each field.
    Notes:
    - If Input 1 is already in use, ticking the **Use Input 1 for cabinet tamper** checkbox will generate the following message:
      "Input is assigned as a tamper input. Please remove the first input from this controller."
    - If you attempt to assign an input more than once, the following error message displays: *"Cannot reserve input, it is already allocated"*
    - When reserved inputs are configured for **Cabinet Front Tamper** and **Cabinet Rear Tamper**, the optical tampers on the **Status and Overrides** tab are disabled, (i.e. the **Disable Front Tamper** and **Disable Rear Tamper** checkboxes).
    - The **Clear All** button can be used to clear reserved inputs and return them to "—None Selected --".

    As inputs are reserved, they become disabled (greyed out) on the **Inputs** sub-tab.

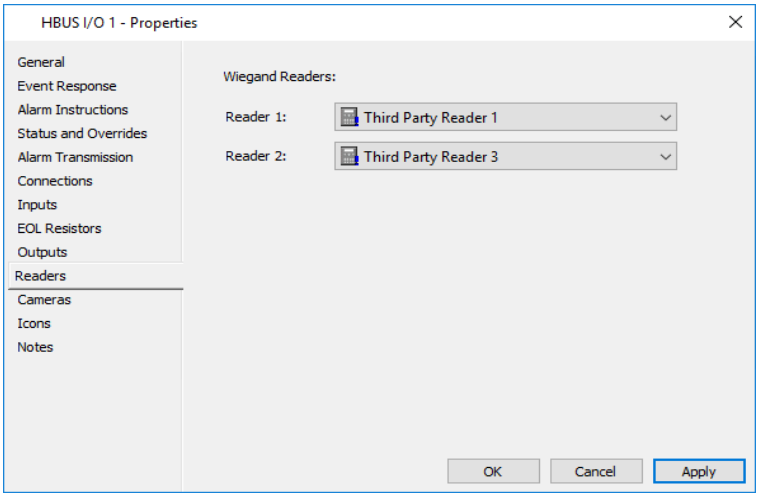


18. Click the **EOL Resistors** tab.
    This screen allows you to define the wiring and resistance values used on inputs that are connected to this device. Refer to ***Configuring EOL Resistors for devices*** (on page 21-46).
19. Click the **Outputs** tab.



Note: The appearance of this screen will differ depending on the hardware variant selected.

20. Assign each Output to the correct address. For details on how to create an Output, refer to ***Creating Inputs and Outputs*** (on page 21-50).
21. Is there a **Readers** tab present?
    If **yes**, that means "4-In 2-Out Door Module - Wiegand" was selected from the Hardware Variant drop-down on the **Connections** tab. Go to Step 20.
    If **no**, go to Step 22.
22. Click the **Readers** tab.



23. Select the appropriate readers from the **Reader 1** and **Reader 2** drop- down lists.
    Note: Only third party readers can be assigned to an "HBUS 4-In 2-Out Door Module - Wiegand".
24. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this HBUS I/O Interface.
    For further details see ***Cameras tab*** (on page 3-24).
25. Click the **Icons** tab if you want to change the Icon Set for this HBUS I/O Interface.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
26. Click the **Custom Fields** tab if you want to add and assign a custom field value to this HBUS I/O Interface.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
27. Click the **Notes** tab if you want to add a note(s) about this HBUS I/O Interface.
    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.

Result

An HBUS I/O Interface has been configured, assigned to a Controller 6000 or 7000, and is ready for use.

If you have configured an 8-In 2-Out Door Module, the HBUS devices connected to the module display in tree view. Refer to ***Configuring HBUS Devices*** (on page 21-65).

Configuring an HBUS Quickswitch Board

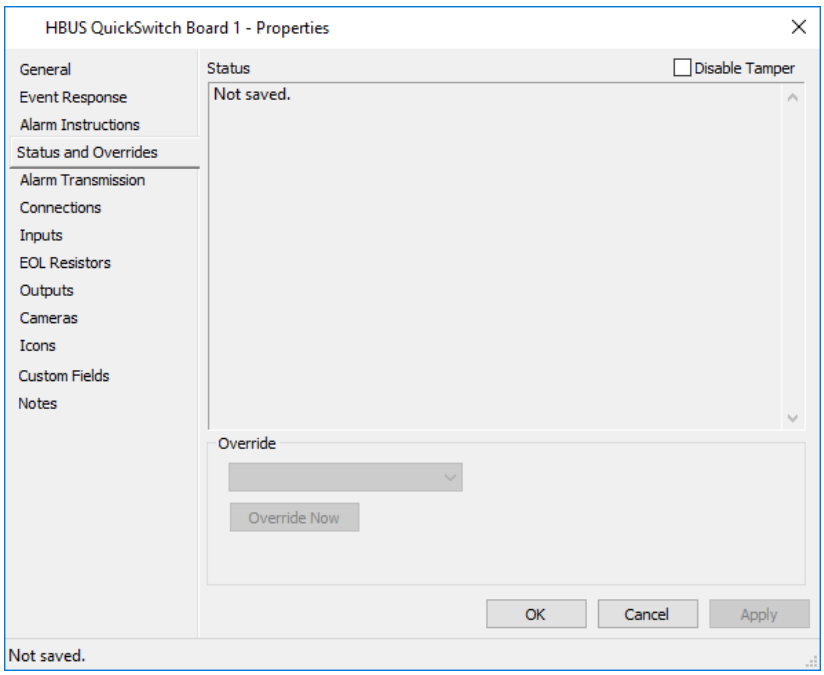
Introduction

The Gallagher QuickSwitch ME1502 extends the connectivity of the Gallagher Controller via the HBUS communications protocol. It enables connectivity for 8 inputs and 4 outputs, that match the footprint and terminal location of common third-party control panels.

Configuration

To configure an HBUS QuickSwitch ME1502 Board, perform the following procedures in Gallagher Configuration Client**:**

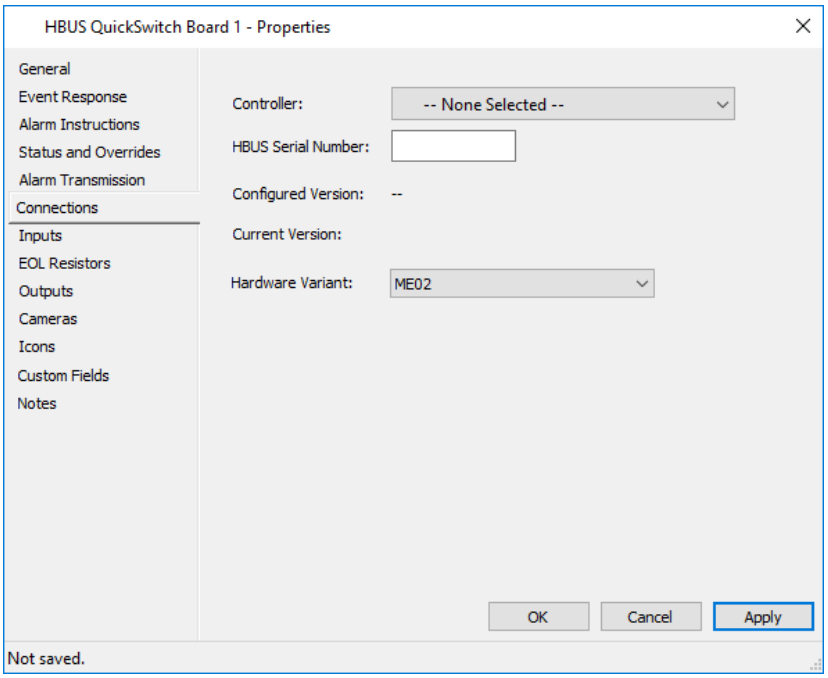
1. Click **Configure** from the menu bar, then **Hardware**.
   The Hardware List Window opens.
2. Right click and select **New...HBUS Devices**.
3. Select **HBUS QuickSwitch Board.**
   By default the **General** tab displays.
4. Complete the fields as required.
   For further detail see ***General 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 **Status and Overrides** tab.



To prevent continuous tamper alarms, tick the **Disable Tamper** checkbox.
Notes:

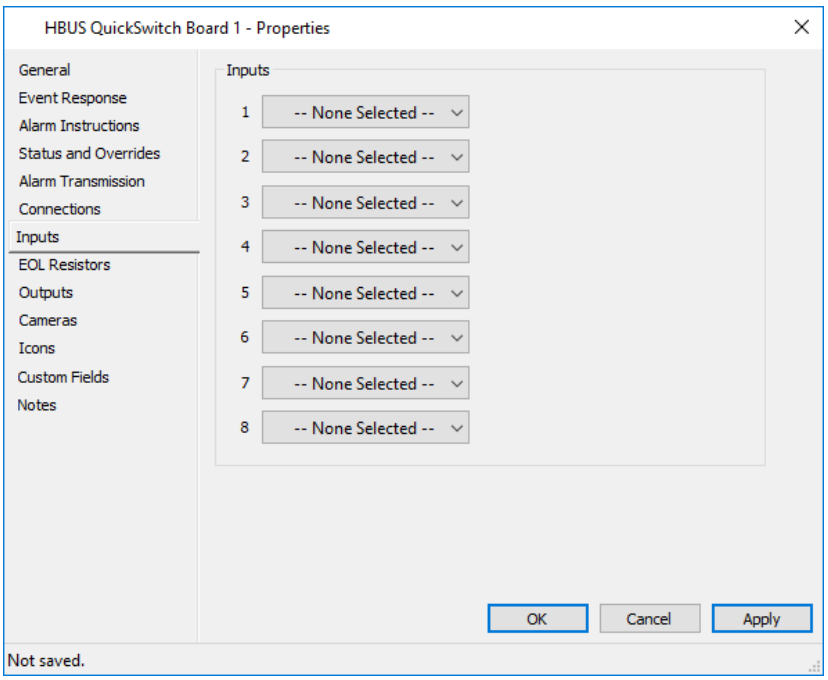
- The battery and power status does not display on this tab.
- This device does not support timed overrides. All overrides are immediate and persist until specifically cancelled by an operator.

8. To perform an override, click within the **Override** field and select the required override action from the drop-down list, then click the **Override Now** button.
   For a description on each of the override actions that can be performed refer to ***Performing Overrides*** (on page 45-7).
9. Click the **Connections** tab.

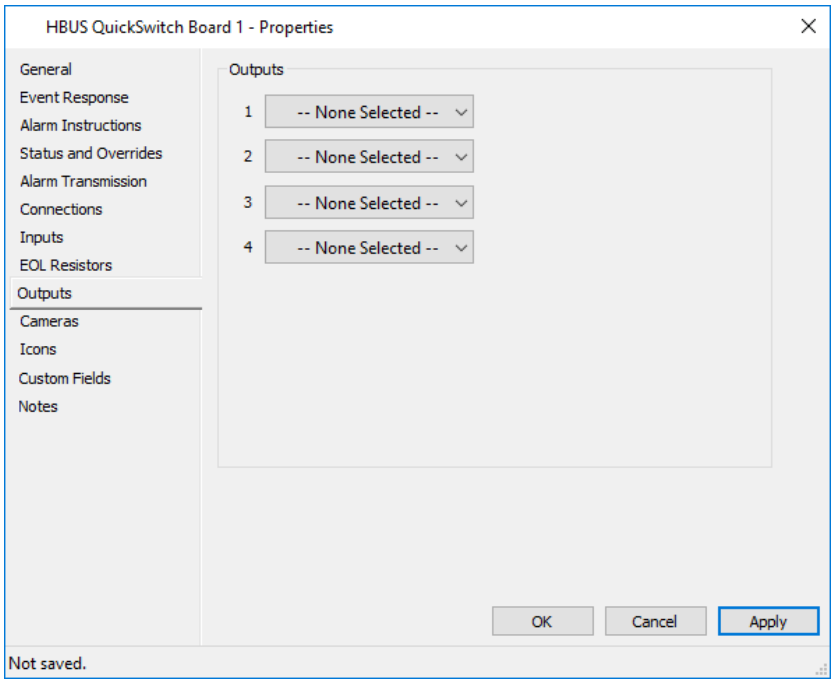


10. Select the Controller you want to assign this QuickSwitch Board to, from the **Controller** drop-down list.
    Note: QuickSwitch Boards can be created via the **HBUS Devices** tab of a Controller. In that case the **Controller** field would be pre-populated with that Controller name. Refer to the topic ***Configuring HBUS Devices*** (on page 21-65).
11. Enter the HBUS serial number (10 character hexadecimal string) into the **HBUS Serial Number** field. This serial number is located on the board sticker.
    Note: The HBUS serial number is optional, however the board will be considered as not properly configured unless one is entered.
12. If you click the **Apply** button, software version numbers display.
    The **Configured Version** is the version of the device software in the configured Controller FTS file, (i.e. **not** the version of the Controller software).
    The **Current Version** is the version of software as last reported by the board itself.

13. Select the appropriate hardware variant from the **Hardware Variant** drop-down list.
    Notes:
    - If you select either *ME16IN* or *LN-16 IN*, the **Outputs** tab will disappear. Likewise, if you select either *ME16OUT* or *LN-16 OUT*, the **Inputs** tab will disappear.
    - 'Bad Unit' type alarms may occur if the hardware variant attached to the Controller does not match to the hardware variant selected.
14. Click the **Inputs** tab if displayed.
    Note: The appearance of this screen may differ depending on the hardware variant selected on the **Connections** tab, (e.g. If "AMD50-2D" was selected, there will only be 4 Inputs available).



15. Assign each Input to the correct address. For details on how to create an Input, refer to ***Creating Inputs and Outputs*** (on page 21-50).
16. Click the **EOL Resistors** tab.
    This screen allows you to define the wiring and resistance values used on inputs that are connected to this device. Refer to ***Configuring EOL Resistors for devices*** (on page 21-46).
17. Click the **Outputs** tab if displayed.
    Note: The appearance of this screen will differ depending on the hardware variant selected on the **Connections** tab.



18. Assign each Output to the correct address. For details on how to create an Output, refer to ***Creating Inputs and Outputs*** (on page 21-50).
19. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this HBUS QuickSwitch Board. For further details regarding the **Cameras** tab, see ***Cameras tab*** (on page 3-24).
20. Click the **Icons** tab if you want to change the Icon Set for this HBUS QuickSwitch Board.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80)
21. Click the **Custom Fields** tab if you want to add and assign a custom field value to this HBUS QuickSwitch Board.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
22. Click the **Notes** tab if you want to add a note(s) about this HBUS QuickSwitch Board.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
23. 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 HBUS QuickSwitch ME1502 Board has been configured, assigned to a Controller, and is ready for use.

Chapter 22: Doors

A door is not a device; the readers that attach to the doors are the devices.

This chapter contains the following information:

- ***Creating Doors*** (on page 22-2)
- ***Configuring extended access time for a Door*** (on page 22-13)
- ***Interlocking Doors*** (on page 22-15)
- ***Challenge*** (on page 22-21)
- ***Action on Access*** (on page 22-33)

Creating Doors

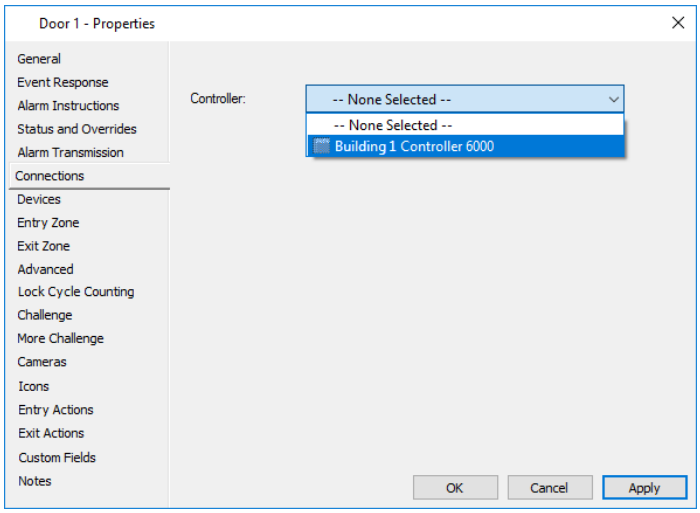
Introduction

Once Controllers have been configured you can then add "doors". This may seem odd at first, however by adding these logical doors, it makes it simple to attach the actual reader devices.

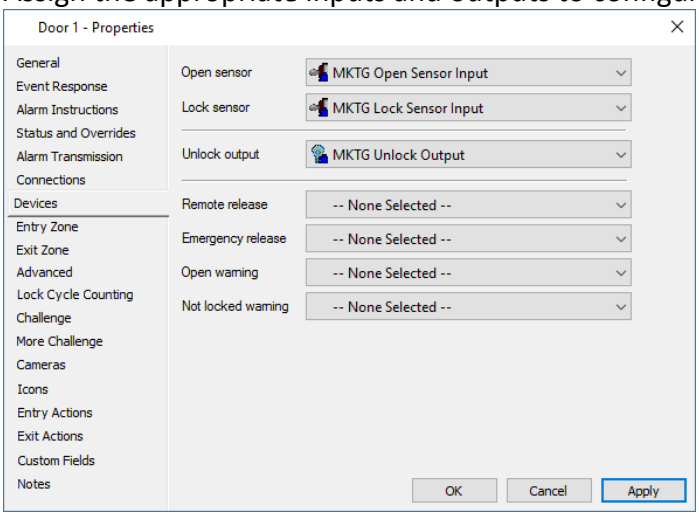
Note: We recommend that sites do not have sensors, outputs or readers for a single door spanning more than one Controller. This is recommended for performance reasons and so site security is not compromised, (e.g. components spanning Controllers can result in relays switching when they shouldn't, door access being provided when it shouldn't, and alarms being reported unnecessarily).

Procedure

1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens (in grid view).
2. **Right click** and select **New...Door**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab, and configure as required.
   For further detail see ***Event Response tab*** (on page 3-20).
   Note: The default Action Plan for the 'Unit on Door Tampered' Event Type (under the 'Tamper' Group) is **Log an event**. Command Centre will display a 'Unit on Door Tampered' event whose source is a door, when an associated reader or door sensor goes into a tamper state.
   This event can be configured as an alarm here instead so that these alarms will display elsewhere in Command Centre as being against the door, (e.g. if a site only has doors on their Site Plans they will show against the door. Note that if the associated reader or sensor is also on the Site Plan the alarm will show against them as well).
   If your site requires this functionality to be system-wide rather than against specific door(s), this can be configured on the **Event Default** tab of the Server Properties instead.
5. Click the **Connections** tab.



6. Assign the door to the Controller that will host this door. **Notes:**
   - Select the Controller with the majority of Door hardware assigned to it. It is preferable to have all Door hardware on the same Controller.
   - Doors are restricted to a maximum of 10 per controller by default. Additional door capacity can be added through licensing.
7. Click the **Devices** tab.
8. Assign the appropriate inputs and outputs to configure the Door.



Inputs should be wired depending on the type of input, as follows:

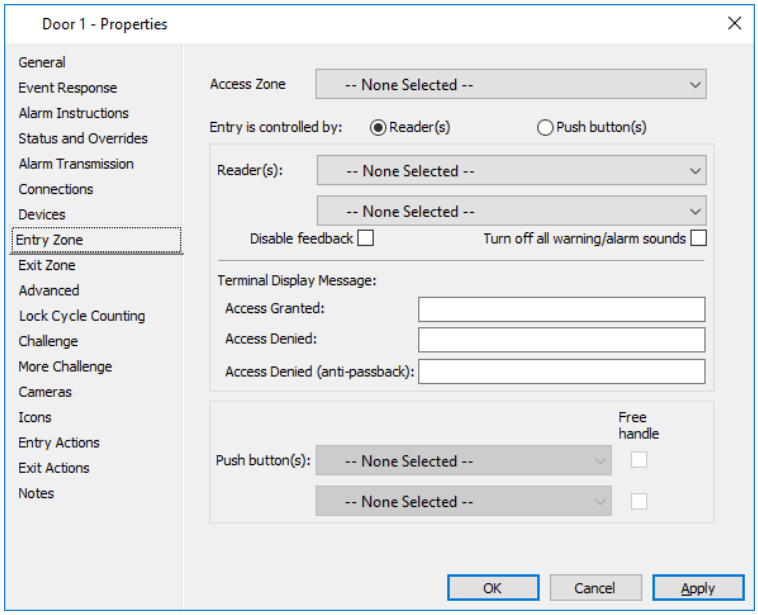
Input Type	Wired	Notes
Standard	Normally Closed	
Remote Release, Request to Exit (REX)	Normally Open	If wired Normally Closed, need to invert it

Field	Allows the selection of an . . .
Open Sensor	Input to act as the doors open sensor.
Lock Sensor	Input to act as the doors lock sensor.
Unlock output	Output to signal the door to unlock.
Remote release	Input connected to a push button that grants access to a door, (e.g. a button located behind a reception desk).

Field	Allows the selection of an . . .
Emergency release	Input that will be connected via a relay to the Free Access Input. Opening the Input results in the Door being manually overridden to Free Access (in the case of an emergency evacuation), and closing the Input results in Secure Access Mode.
Open warning	Output to activate when the door has been open too long (open sensor has failed to close).
Not locked warning	Output to activate when the door has been left unlocked (lock sensor has failed to close).

Note: Each site can have different door requirements, (e.g. some will require remote release door functionality, while others will require a warning mechanism when the door is open). The Input/Output requirements for the Door should have been determined during the site design process.

9. Click the **Entry Zone** tab.



10. Select the **Access Zone** that Cardholders access when entering through this Door.
11. Select whether **Entry is controlled by** Reader(s) or Push button(s).
12. Select the **Reader(s)** or **Push button(s)** that connect to this Door to control entry.
    Note: If you assign both a Third Party/OSDP Reader and an HBUS Terminal to this Door, the Readers behave like so:
    - The Third Party/OSDP Reader can be used for reading third-party cards.
    - The HBUS Terminal will display feedback from the Third Party/OSDP Reader on its screen. See page 22-10 for a full overview of what can be displayed.

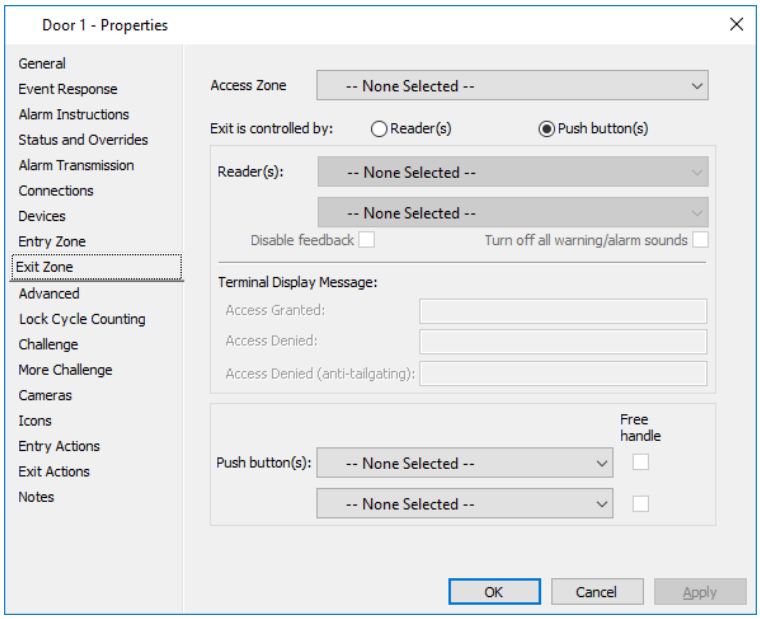
    However, note the following when using the HBUS Terminal to display feedback:

- The HBUS Terminal cannot be used to view or acknowledge alarms.
- The **Access mode** of the Access Zone of the Door must be set to **Secure**, and the **PINs mode** must be set to **No PIN**. Neither the Third Party/OSDP Reader or the HBUS Terminal will ever prompt for PIN.

Notes:

- If entry is controlled by a Reader, additional options are enabled:
  - **Disable feedback:** If this option is selected, the Door's Reader(s) will not display prompts, messages, icons, LEDs, or make access granted or access denied sounds when access attempts are made at the Reader.
  Note: Selecting this option has the effect of disabling any feature that requires Reader feedback, (e.g. PINs, dual-authorisation, Code or Card only mode, local overrides, etc.).
  - **Turn off all warning / alarm sounds:** This affects the "beeps" on Readers for "door not locked", "door open too long" and "forced door" statuses for all Readers configured on this tab.
  - **Terminal Display Message:** Optionally set custom messages for the HBUS Terminal **Reader(s)** selected on this tab to display when they grant access, deny access, and/or deny access for anti-passback to the Entry Zone. If you leave these fields blank, the selected HBUS Terminal **Reader(s)** display the default messages when granting/denying access to the Entry Zone.
  Notes:
    - To edit these, the **Disable feedback** check box must be unchecked.
    - HBUS Terminals can display a maximum of two full lines of text. If the message is too long, it is truncated when displayed on the Reader.
    - Several Doors' Terminal Display Messages can be modified at once with a Door Bulk Change. See ***Initiating a new Door Bulk Change*** (on page 38-37).
- If entry is controlled by a pushbutton, there is an additional **Free handle** option. This can be used for Doors where the lock does not need to be unlocked for exit. When this option is enabled, and a valid exit request is made, the Doors lock relay will not activate (Doors outside handle will remain locked).
  Pushbutton/Request to Exit should be wired as normally open, if the Pushbutton input is normally closed then the input can be inverted to provide correct operation.
- You can configure the Door to allow entry and exit via two Readers/pushbuttons. For example, vehicles of various heights use a building's vehicle Door. Therefore, two entry Readers can be mounted at different heights, one positioned for cars and the other for trucks and buses.

13. Click the **Exit Zone** tab.



14. Select the **Access Zone** that Cardholders access when they exit out this Door. There is no reason to configure an Exit Zone to a Door that has no exit Reader. Refer to ***Access Zones*** (on page 10-1) for further information.
15. Select whether **Exit is controlled by** Reader(s) or Push button(s).
16. Select the **Reader(s)** or **Push button(s)** that connect to this Door to control exit.

    Note: If you assign both a Third Party/OSDP Reader and an HBUS Terminal to this Door, the Readers behave like so:

    - The Third Party/OSDP Reader can be used for reading third-party cards.
    - The HBUS Terminal will display feedback from the Third Party/OSDP Reader on its screen. See page 22-10 for a full overview of what can be displayed.

    However, note the following when using the HBUS Terminal to display feedback:

    - The HBUS Terminal cannot be used to view or acknowledge alarms.
    - The **Access mode** of the Access Zone of the Door must be set to **Secure**, and the **PINs mode** must be set to **No PIN**. Neither the Third Party/OSDP Reader or the HBUS Terminal will ever prompt for PIN.

    Notes:

    - If exit is controlled by a Reader, additional options are enabled:
      - **Disable feedback:** If this option is selected, the Door's Reader(s) will not display prompts, messages, icons, LEDs, or make access granted or access denied sounds when access attempts are made at the Reader.
      Note: Selecting this option has the effect of disabling any feature that requires Reader feedback, (e.g. PINs, dual-authorisation, Code or Card only mode, local overrides, etc.).
      - **Turn off all warning / alarm sounds:** This affects the "beeps" on Readers for "door not locked", "door open too long" and "forced door" statuses for all Readers configured on this tab.
      - **Terminal Display Message:** Optionally set custom messages for the HBUS Terminal **Reader(s)** selected on this tab to display when they

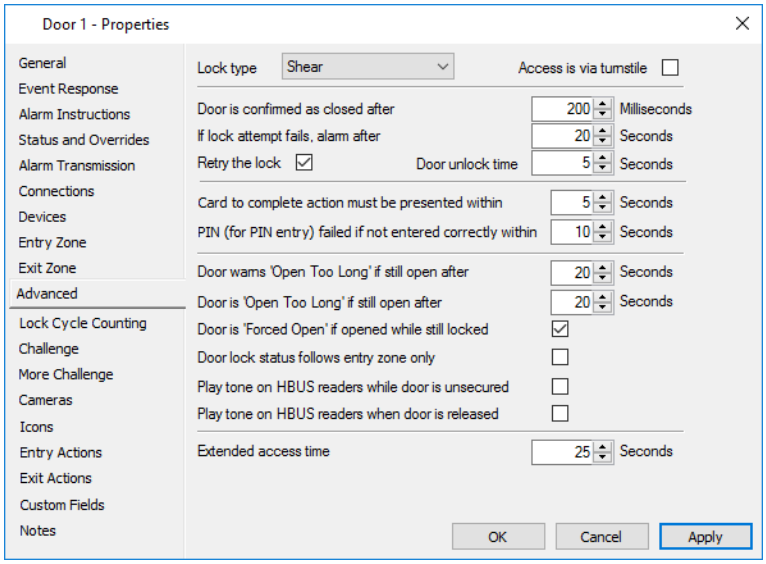
grant access, deny access, and/or deny access for anti-passback to the Exit Zone. If you leave these fields blank, the selected HBUS Terminal **Reader(s)** display the default messages when granting/denying access to the Exit Zone. **Notes:**

- To edit these, the **Disable feedback** check box must be unchecked.
- HBUS Terminals can display a maximum of two full lines of text. If the message is too long, it is truncated when displayed on the Reader.
- Several Doors' Terminal Display Messages can be modified at once with a Door Bulk Change. See ***Initiating a new Door Bulk Change*** (on page 38-37).

- If exit is controlled by a pushbutton, there is an additional **Free handle** option. This can be used for Doors where the lock does not need to be unlocked for exit. When this option is enabled and a valid exit request is made, the Door's lock relay will not activate (Door's outside handle will remain locked).

  Pushbutton/Request to Exit should be wired as normally open, if the Pushbutton input is normally closed then the input can be inverted to provide correct operation.
- Morpho Biometric Readers are not recommended for use on exit Doors. However, if you configure the exit at a Door to be controlled by a Morpho Reader, you must specify an Access Zone (even if you create one just for this purpose), otherwise no one will be able to exit through the Door.
- You can configure the Door to allow entry and exit via two Readers/ pushbuttons. For example, various height vehicles use a building's vehicle Door. Therefore, two entry Readers can be mounted at different heights, one positioned for cars and the other for trucks and buses.

17. Click the **Advanced** tab.



18. Select the appropriate **Lock Type** from the drop-down list:

Lock Type	Description
Shear Lock	When configured as a Shear Lock and a valid card is presented the door unlocks. If the door is not physically opened it will relock after the "Door unlock time" is exceeded. If the Door is opened, the lock relay remains active until the Door open sensor recloses, (i.e. the Door closes). **Uses:** Electronic bolts or double doors that do not have to rebate to prevent the inactive door locking prior to the active door.
Mortise Lock	When configured as a Mortise Lock and a valid card is presented the door unlocks. If the door is not physically opened it will relock after the "Door unlock time" is exceeded. If the Door is opened the lock relay resets immediately when the Door Open sensor switches open. When the Door physically closes the lock is in a state that immediately re-secures the Door. **Uses:** - Most standard lock situations - Magnetic clamp locks
Automatic Lock	When configured as an Automatic Lock the lock relay will always be activated for the user configured time. This time is set by the use of the **Door unlock time** option. All other settings will be as for the other lock types. **Uses:** Magnetic clamp door with only one Input.
Half-Cycle Lock	When configured configured as a Half-Cycle Lock and a valid card is presented, the Door will unlock and remain unlocked until opened and shut. Since one intended use-case is to leave doors closed after unlocking them, No Entry Taken ("access granted but not taken") events are not raised for Half-Cycle Doors. Reader's LEDs flash green on access granted and remain solid green while closed and unlocked; Terminals will flash green on access granted and continue flashing while closed and unlocked, unless they are configured as Cardax IV Readers, in which case their LEDs behave the same as Readers. When this lock type is selected, the **Door unlock time** and **Extended access time** settings are disabled, because the Door is unlocked indefinitely. And the 'Open Too Long' settings can optionally be disabled (see below table). If the Access Zone enters lockdown while a Half-Cycle Door is shut and unlocked, the unlocked state is restored once lockdown ends. Half-Cycle type Doors have the extra 'Lock Door' override available, to allow the Door to be locked by an operator with the 'Override - Lock Door' privilege. While a Door is shut and unlocked after access has been granted, the 'Lock Door' override can be used to lock it.

Notes:

- The system will energise the lock in accordance with the lock type selected.
- Ticking the **Access is via turnstile** checkbox means that when the door opens, only the last person who badged and was granted access is logged as having entered and if two people badge without the door opening, then the first person gets logged as having not entered. This is regardless of whether the person is a visitor or an escort. With a turnstile, if an escort has several visitors, then either the escort has to

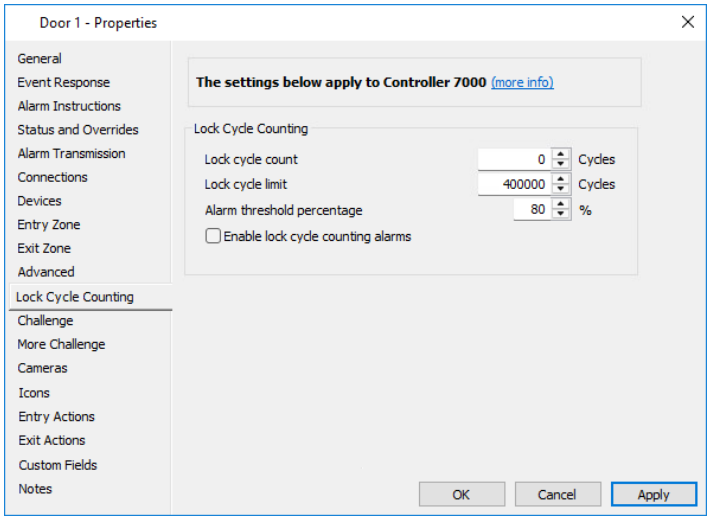
go through the door first, and then all the visitors (within a timeout), or else there will be a 'no entry' event for the escort.

19. Configure the Door timeouts as required.

Option	This setting . . .
Door is confirmed as closed after	is to stop door bounce causing a forced door alarm. (Valid range is 0 - 5000 milliseconds. Default = 200 milliseconds)
If lock attempt fails, alarm after	determines when a Door Not Locked alarm and beep is generated. (Valid range is 1 - 60 seconds. Default = 20 seconds)
Retry the lock	determines if the lock relay is pulsed when the door is not locked.
Door unlock time	determines the maximum time the Unlock relay is energised. (Valid range is 1 - 86400 seconds. Default = 5 seconds)
Card to complete action must be presented within	determines either: • the maximum time between card swipes for Dual Authorisation, **OR** • the time between pressing a function key on a keypad reader and badging the card for an Access Zone or Alarm Zone override. (Valid range is 1 - 99 seconds. Default = 5 seconds)
PIN (for PIN entry) failed if not entered correctly within	determines either: • the maximum time between badging a card and starting to enter a PIN at a keypad reader for access through a door in PINs mode, **OR** • overriding an Access Zone or Alarm Zone in PINs mode. (Valid range is 1 - 99 seconds. Default = 10 seconds)
Disable 'Open Too Long' alarms	is only available if the Lock type is 'Half-Cycle'. When checked, this setting disables the settings **Door warns 'Open Too Long' if still open after** and **Door is 'Open Too Long' if still open after**, so that no 'Open Too Long' warnings or alarms are raised for this Door. **Note:** 'Open Too Long' alarms are only raised if the door is physically open, not if it is unlocked and shut.
Door warns 'Open Too Long' if still open after	determines when the door reader starts beeping to warn the door has been open too long. (Valid range is 0 - 9999 seconds. Default = 20 seconds) **Note:** This cannot be set as greater than the alarm time, (i.e. the **Door is 'Open Too Long' time**). If it is, and you attempt to save the Door, the following error message will display: *"The 'Open Too Long' warning time must be less than or equal to the 'Open Too Long' alarm time."*
Door is 'Open Too Long' if still open after	determines when a Door Open Too Long alarm is generated. (Valid range is 5 - 9999 seconds. Default = 20 seconds)

Option	This setting . . .
Door is 'Forced Open' if opened while still locked	when checked, causes a Forced Door alarm to be generated if the open sensor detects the door is opened.
Door lock status follows entry zone only	when checked, the state of the door (locked or un-locked) will be based on the status of the Entry Zone only, (i.e. door is locked when Entry Zone is secure; door is unlocked when Entry Zone is set to free access).
Play tone on HBUS readers while door is unsecured	when checked, any T series readers operating over HBUS associated to the doors Entry and Exit Zone will play an extended access granted tone for the duration of the door being unsecured, (e.g. unlocked or open).
Play tone on HBUS readers when door is released	when checked, any T series readers operating over HBUS associated to the doors Entry and Exit Zone will play an extended tone when the door is opened via a remote release button, open door override, or an exit button on the secure side of the door.
Extended access time	determines an alternate unlock time, allowing the door to remain unlocked for longer than normal for those card-holders who require it, (e.g. disabled people, couriers, etc) (Valid range is 0 - 86400 seconds. Default = 25 seconds) Refer to ***Configuring alternate unlock time for a Door*** (on page 22-10) for further details.

20. Click the **Lock Cycle Counting** tab.
    This tab is visible regardless of whether the Door is configured on a Controller 6000 or 7000. However, Lock Cycle Counting functions only when the Door is connected to a Controller 7000 from v9.40 onwards.
    Lock Cycle Counting tracks how many times the door lock has been activated and optionally raises alarms when limits are reached.



21. Configure as required.

Field/Checkbox	Description
Lock cycle count	▪ When Command Centre is first upgraded from a version **prior to 9.40 to 9.40 or later**, this field **defaults to 0**. ▪ Displays the current number of lock cycles recorded for the door.

Field/Checkbox	Description
	▪ Can be manually modified to reflect the number of times the lock has been triggered, (e.g. after maintenance or lock replacement). ▪ Automatically increments when lock cycles occur (Door unlocked + locked = 1 cycle). ▪ **Valid range:** 0 to 100,000,000.
Lock cycle limit	▪ Defaults to **400,000**. ▪ Represents the maximum recommended number of lock cycles for the lock hardware. ▪ Can be modified based on the type and manufacturer's recommendations for the lock hardware used. ▪ **Valid range:** 0 to 100,000,000.
Alarm threshold percentage	▪ Defaults to **80%**. ▪ Specifies the percentage of the lock cycle limit at which the system raises an "approaching limit" alarm. ▪ The system raises a "limit reached "alarm when the lock cycle count reaches **100%** of the limit. ▪ **Valid range:** 0 to 100.
Enable lock cycle counting alarms	▪ Checkbox is disabled by default. ▪ When disabled, lock cycle count continues to increment when lock cycles occur with no alarm generated. ▪ When enabled, activates lock cycle alarms.

22. Clicking the **Apply** or **OK** button will confirm and save all changes made to the editable fields and checkbox.
23. The **Challenge** and **More Challenge** tabs are used for configuring the Challenge feature. For an explanation of this feature and further configuration details, refer to ***Configuring Challenge*** (on page 22-22).
24. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Door. For further details see ***Cameras tab*** (on page 3-24).
25. Click the **Icons** tab if you want to change the Icon Set for this Door. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
26. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Door. For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
27. Click the **Notes** tab if you want to add a note(s) about this Door. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-83).
28. Click **OK**. The door name now displays within the Door window.

Hint

Editing and Deleting Doors

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

Note: If you attempt to delete a Door that is linked to a macro or belongs to an Interlock Group, a message will display, for example:

"This item cannot be deleted as there is a macro that depends upon it for proper operation." OR

"This item cannot be deleted, as it is used in an Interlock Group."

What can be displayed on an HBUS Terminal on the same Door as a Third Party/OSDP Reader

This functionality is useful when you are using third-party cards that can only be read by a Third Party/OSDP Reader.
The HBUS Terminal can display feedback on its screen when cards are badged at the Third Party/OSDP Reader.

On a regular Door:

- Access granted/denied messages
- Missing Competency messages
- Arming/Disarming

On a Car Park Door:

- The allocated Car Park Space number.
- When the Car Park Space assignment will expire.

On a Random Selection Door:

- The Random Selection message (if Cardholder is selected).
- Option to acknowledge the message.

Configuring extended access time for a Door

Introduction

Extended access can be granted so that a door will remain unlocked for longer than normal, for those cardholders who require it, (e.g. disabled people, couriers, delivery vehicles, etc.).

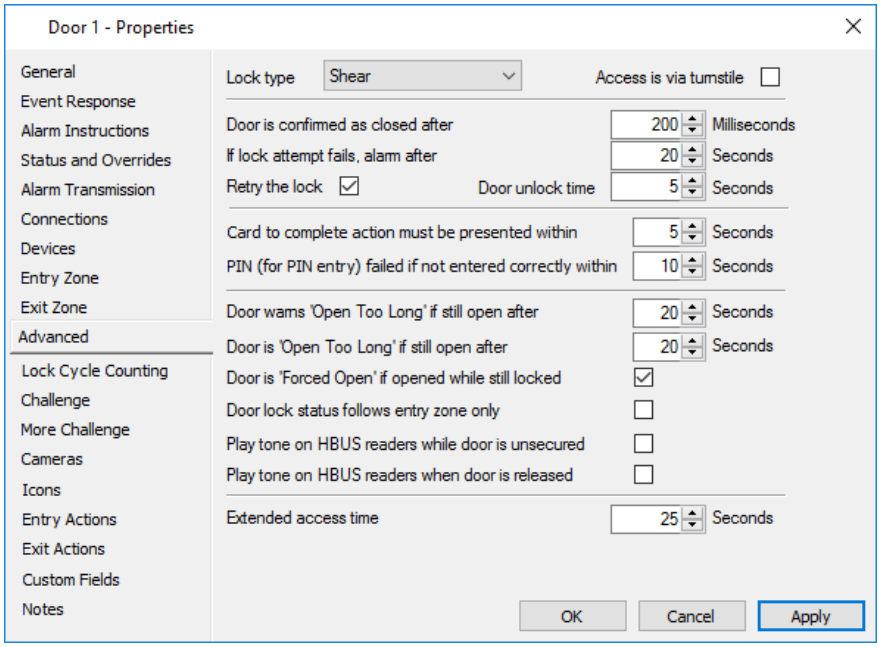
There are two parts to this procedure, (i.e. configuring the extended access time for a Door, and identifying those cardholders that require extended access time).

This procedure describes configuring the extended access time for a Door.
Note: Operators require the "Edit Site" operator privilege to perform this part of the procedure.

Identifying cardholders that require an extended access time is performed in Command Centre Client. Refer to ***Setting Accessibility options*** (under the "Cardholder Details Tile actions" topic), in the *Gallagher Command Centre Client User Guide* for detailed instructions.

Procedure

1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens.
2. Highlight the door the extended access time is to be configured for.
3. Right click and select **Properties**.
4. Click the **Advanced** tab.



5. Enter the maximum time you want the door to unlock for in the **Extended access time** field. (The range for this field is 0 - 86400 seconds, and by default is set at 25 seconds).

Note: The **Extended access time** affects the times used for all of the following:
- Door unlock time,
- Door Open Too Long Warning,
- Door Open Too Long Alarm

- When a cardholder identified as requiring extended access time badges their card at this door, the door will remain unlocked for a time equal to the **Door unlock time** PLUS the **Extended access time**, (e.g. if the door is configured with a Door unlock time of 5 seconds, and an Extended access time of 60 seconds, then the door will remain open for 65 seconds).
- Once a cardholder has opened the door, the Door Open Too Long Warning is activated if the door is still open after a period of time equal to the **Door Open Too Long Warning time** PLUS the **Extended access time**, (e.g. if the door is configured with a Door Open Too Long Warning time of 40 seconds, and an Extended access time of 60 seconds, then the Door Open Too Long Warning will activate after 100 seconds).
- Once a cardholder has opened the door, the Door Open Too Long Alarm is activated if the door is still open after a period of time equal to the **Door Open Too Long time** PLUS the **Extended access time**, (e.g. if the door is configured with a Door Open Too Long time of 50 seconds, and an Extended access time of 60 seconds, then the Door Open Too Long Alarm will activate after 110 seconds).

6. Click **OK**.

Result

An extended access time has been configured for a door.

Interlocking Doors

Introduction

Interlocking doors are defined as a means of ensuring that only specified doors can be opened at any one time for any set group of doors. Any pair of doors that form part of an Interlock Group will be allowed to be interlocked, meaning that one cannot be unlocked unless the other is secure and vice versa for all groups the doors, etc appear in. Interlock Groups can consist of doors, inputs, outputs, logic blocks, or a combination of these items, with a limit of a combined total of 20.

All tampers to doors, inputs, outputs or logic blocks that are part of an Interlock Group are treated as Open/Insecure by the Interlock Group, which then affects the activity of other items in the group.

Interlock Rules

The system enforces the Interlock rules when a cardholder badges their card at a reader, or a door is remote released. The only exceptions are:

- If a suitably authorised operator performed an Interlock Group override for the Interlock Group.
  Note:
  An operator requires the “Override – Open Door” operator privilege to perform this.
- If a door is excluded from the Interlock Group.
- If an Access Zone a door belongs to goes into free access.
- If an Emergency Release is triggered then all doors in an Interlock Group are released as any other door.
  Note: Overriding Interlock Groups, (e.g. "Disable Group" in the case of an emergency), can be run from a macro. See ***Creating a new Macro*** (on page 20-2) for further detail.

Interlock Breach

When the interlock rules are broken for at least one door/input in an Interlock Group, an Interlock Breach event is generated, which in turn generates an alarm by default. To help determine what has caused an interlock breach an operator can look in the following places:

- The **Status and Overrides** tab of the Interlock Groups properties will show which doors are in breach.

- The Event log or Alarm Viewer window. If there is a "Forced Door" or "Emergency Release of door" event/alarm immediately prior to the interlock breach then that is likely to be the cause of the breach.
- The Status Viewer or Site Plan with the interlocked doors and Access Zones displayed. This would show which door has been forced or emergency released, or which Access Zone has been overridden to free access, causing the interlock breach.

A Door that cannot be opened due to a breach will still give you an access granted indication but it will not let you through.

Note: For historical interlock breach information, an operator needs to run an Activity Report.

Recommendations

The following recommendations apply to interlocking doors:

- A door that is in an Interlock Group should not be put in any Access Zones with doors that are not part of that Interlock Group, and that may go in to free access.
- Where possible, all doors in an Interlock Group should be connected to the same Controller. This is recommended for system stability, (e.g. if the network failed and there are doors on more than one Controller in a single Interlock Group, and doors are forced, Breach Alarms will not be detected).
  If putting doors that are on different Controllers in a single Interlock Group cannot be avoided, it is recommended that you configure Inter-Controller offline monitoring for those Controllers. See ***Configuring Inter-Controller Offline Monitoring*** (on page 21-31) for further detail.
- Doors in Interlock Groups should not be set up with a free handle pushbutton exit, as this defeats the purpose of an Interlock Group and doesn't really work, (i.e. if a door is not in an Interlock Group and a free handle pushbutton is toggled, it does not fire any output. However, if it is in an Interlock Group it fires the unlock output).

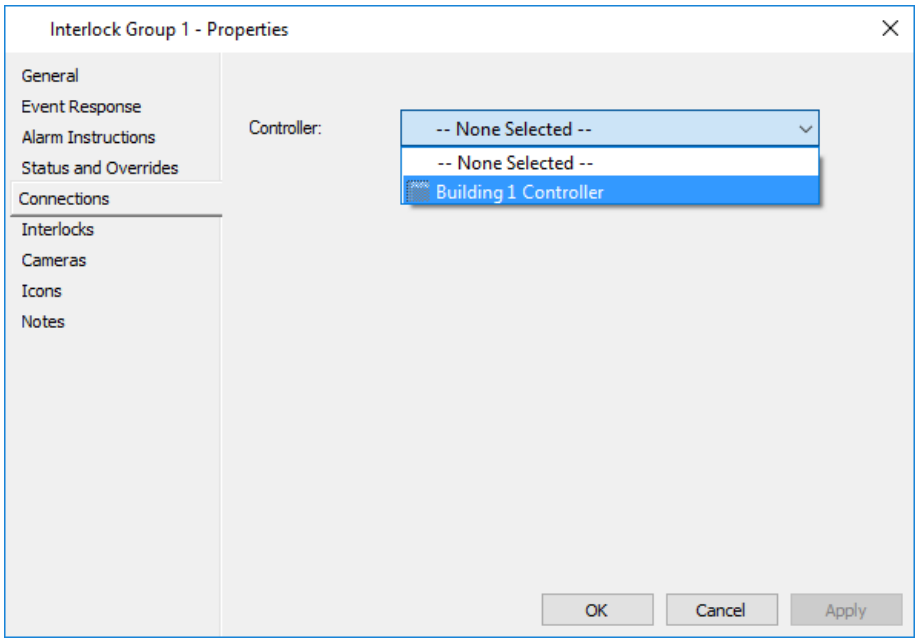
Adding a new Interlock Group

Introduction

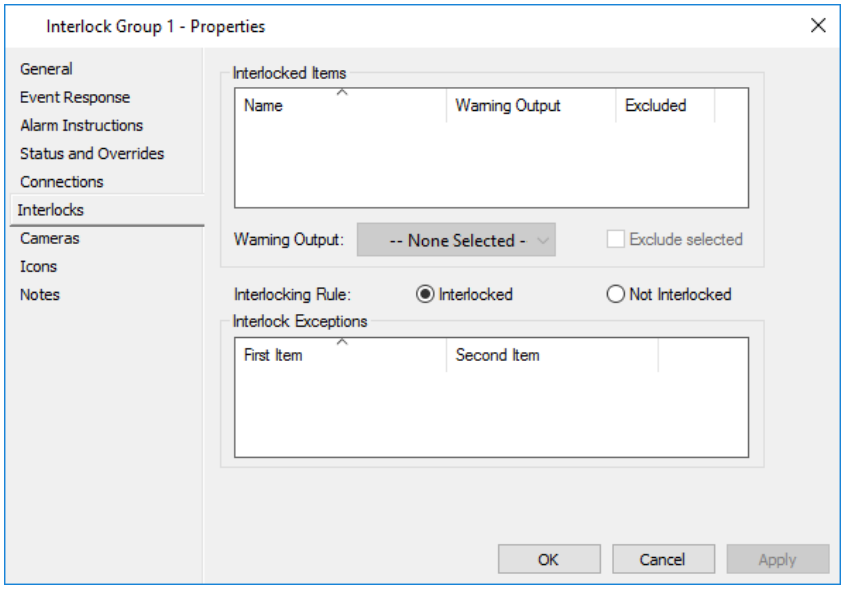
From the **Interlock Group** List Window, operators with the "Edit Site" operator privilege can add a new Interlock Group.

Procedure

1. Click **Configure** from the menu bar, then **Interlock Groups**. The **Interlock Group** List Window opens (in grid view).
2. **Right click** and select **New...Interlock 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 to host the Interlock Group. The Interlock Group will not function until a Controller is selected.
   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.
8. Click the **Interlocks** tab.



This screen allows you to create relationships between doors within the Interlock Group, and specify which doors in the group interlock with each other.

Note: Inputs, Outputs and/or Logic Blocks may also be used wherever doors are mentioned.

Complete the fields on this screen as appropriate.

Field	Description
Interlocked Items grid	Drag the doors into the **Interlocked Items** grid that you want to belong to this Interlock Group. **Notes:** • The list can consist of doors, inputs, outputs, logic blocks or a combination of these items, with a limit of a combined total of 20. If you attempt to add more than 20, an error message will display. • The icons in this grid reflect the current status of the doors/inputs/outputs/logic blocks.
Warning Output drop-down list	Each door can have an output assigned to it that is on when the door is prevented from being opened due to the interlocking rules. There are two ways of doing this. Either: • Drag the output into the **Interlocked Items** grid beside the appropriate door, OR • In the **Interlocked Items** grid, highlight the door you want to assign an output for, and select an output from the **Warning Output** drop-down list. The output displays in the **Interlocked Items** grid beside the door.

Field	Description
Exclude selected checkbox	Allows a door to be excluded from the Interlock Group (usually as a temporary measure). For situations where a door is damaged, or for some reason needs to be opened independently of the interlock, but will become part of the group again at a later date. To exclude a door, highlight it in the **Interlocked Items** grid and tick the **Exclude selected** checkbox. The door will still be listed in the **Interlocked Items** grid with "Yes" in the 'Excluded' column.
Interlocking rules radio buttons	Clicking the appropriate radio button allows you to change the interlocking rule depending on what you want to configure. When **Interlock** is selected, all doors listed as part of the group will be interlocked, (i.e. only one of the listed doors may be open/unlocked at any one time without causing a breach). When **Not Interlocked** is selected, none of the doors listed as part of the group shall be interlocked.
Interlock Exceptions grid	Drag the doors as pairs into the **Interlock Exceptions** grid that you want to be exceptions to the Interlock rule. If a door is dragged over an existing row with only one door, the dragged door is added to that row, unless it is the same as the first door. If the row dragged over already has two doors, then there will be no effect, (i.e. once an exception pair has two doors the pair cannot be modified, and to change it you need to delete the row and recreate it). **Notes:** • The list can consist of 40 exception pairs. If you attempt to add more than 40, an error message will display. • The icons in this grid never change state.

9. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Interlock Group.
   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 Interlock Group.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).

11. Click the **Notes** tab if you want to add a note(s) about this Interlock Group. 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 new Interlock Group has been created and displays in the **Interlock Group** List Window.

Hint

Editing and Deleting Interlock Groups
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Interlock Groups.
Note: If you attempt to delete an Interlock Group that is linked to a macro or appears on a Site Plan, a message will display, for example:
"This item cannot be deleted as there is a macro that depends upon it for proper operation."
OR
"This item cannot be deleted, as it currently appears on a site plan."

Challenge

The Command Centre Challenge feature allows an operator to contest Cardholders as they attempt to gain access through a Door. Operators may use the feature to visually confirm the identity of each Cardholder before manually granting access to a secure area. This means that an operator is notified at their Workstation, whenever a Cardholder presents their card at a Door that is being challenged. The operator then has the final determination as to whether a Cardholder is granted or denied access.

The Challenge feature is designed to be an extension of the Dual Authorisation feature, where an operator working remotely from their Workstation takes on the role of the second Cardholder.

Notes:

- Refer to Operator Privileges to check you have the correct operator privilege level for working with Challenge.
- Ensure the Workstation PC clocks are synchronised with the Command Centre Server to prevent potential timing issues. If the time between a workstation and the server is more than 30 seconds it will fail to work correctly. Also, both server and workstations need to be on the same time zone.

This section covers the following topics:

- ***Configuring Challenge*** (on page 22-22)
- ***Configuring Doors for Controlled Challenge mode*** (on page 22-26)
- ***Challenge Viewer - Controlled Challenge mode*** (on page 22-29)
- ***Challenge Viewer - View-Only mode*** (on page 22-31)

Configuring Challenge

Introduction

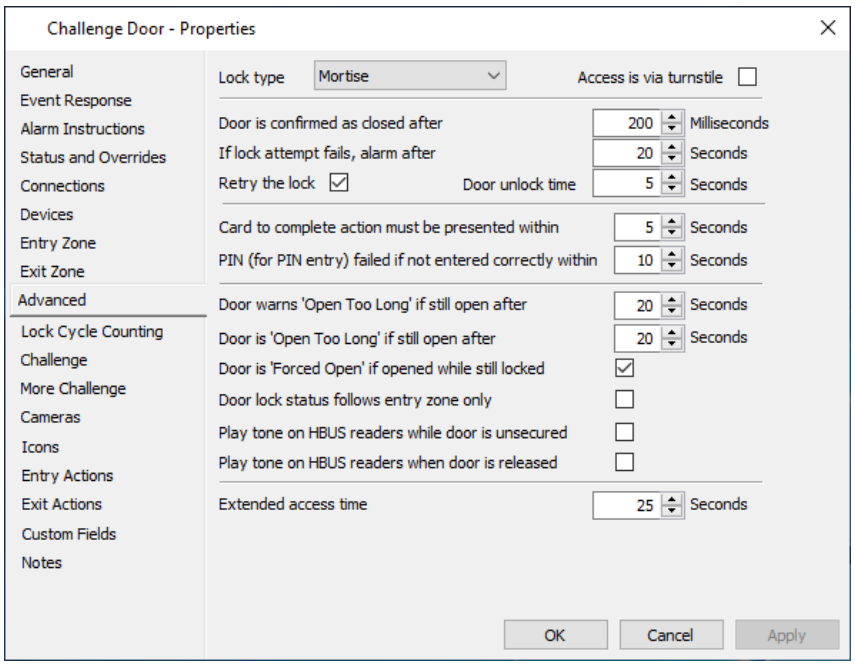
Configuration of Challenge is defined in several tabs on the Property pages of Controller Doors. This procedure describes how to configure Challenge for a Door that has already been configured.

Operators must have the "Site Edit" operator privilege to perform this procedure.

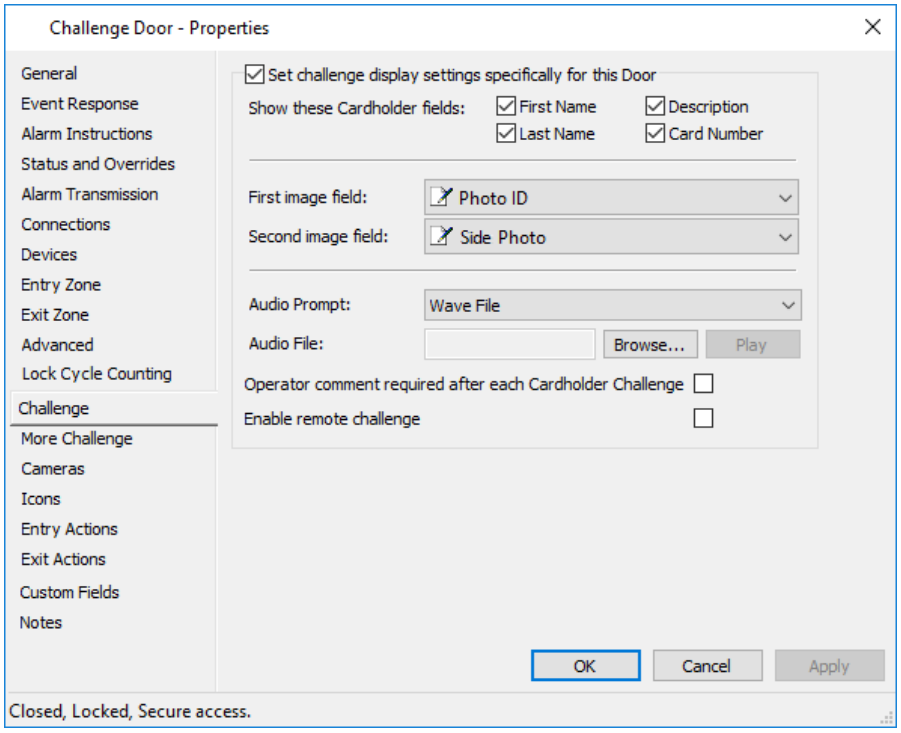
Note: Controlled Challenge mode means the Challenge Viewer will open automatically when a Challenge event occurs. There are a number of ways to configure Controlled Challenge for specific operators/workstations, depending on your site requirements. For further instructions, refer to ***Configuring Doors for Controlled Challenge mode*** (on page 22-29).

Procedure

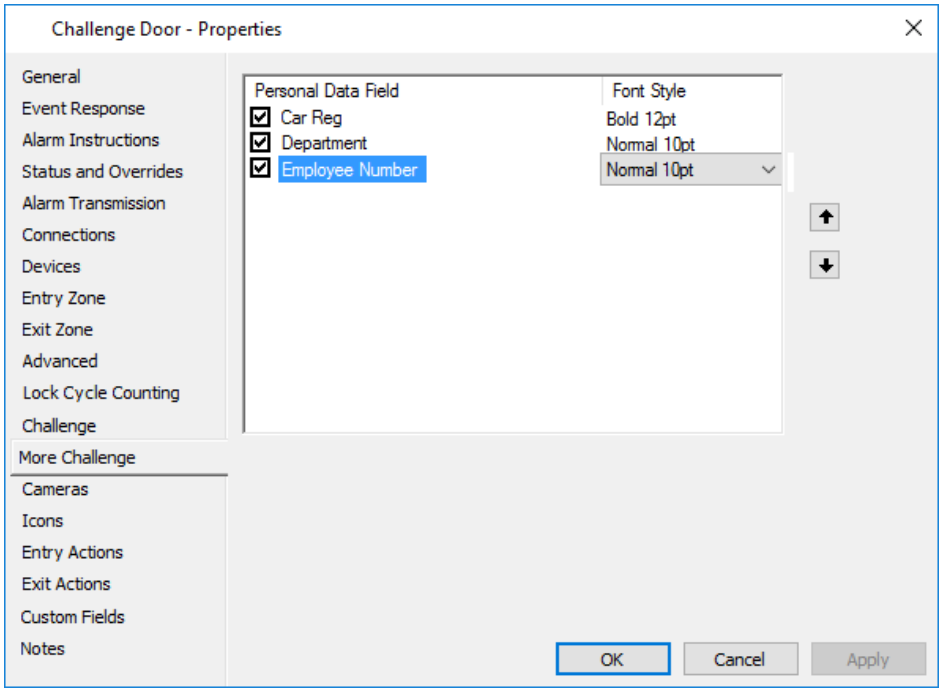
1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens (in grid view).
2. Highlight the door the Challenge feature is to be added to.
3. Right click and select **Properties**.
4. Click the **Advanced** tab.



5. Enter the number (in seconds) in the **Second card (for two-card entry) must be swiped within** field for the time limit an operator is given to grant or deny access. This time limit starts from the time a cardholder presents their card, and has a range of 1 to 99 seconds.
6. Click the **Challenge** tab.

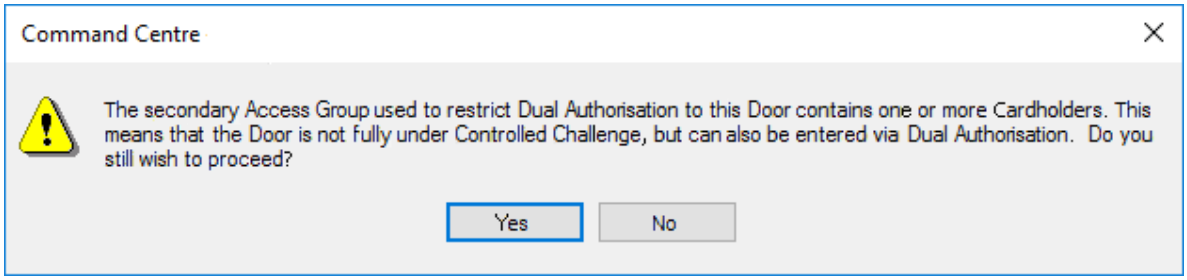


7. The default settings for all Doors in the system are configured in the Challenge and More Challenge tabs of the Server Properties. See ***Server Properties*** (on page 6-1) for further detail.
   If you want the default settings for this Door to be overridden, then tick the **Set challenge display settings specifically for this Door** checkbox.
8. Tick the checkboxes for the Cardholder fields you wish to be displayed in a Viewer window, (i.e. First Name, Last Name, Description and Card Number).
9. If you require Image based Personal Data Fields to be displayed in a Viewer window, select a **First image field** and a **Second image field** from the drop-down lists.
10. If you require an audio sound to be played whenever a Cardholder challenge occurs, select an **Audio Prompt** from the drop-down list.
    Note:
    Wave files used for audio prompts should be less than 5 seconds long.
11. If you require a short explanation from an operator after granting or denying access to each Cardholder, tick the **Operator comment required after each Cardholder Challenge** checkbox.
12. If you require this door to send Challenge events to remote servers, (i.e. in multi-server environments), select the **Enable remote challenge** checkbox. With this checkbox selected, Challenge viewers on remote servers will receive challenge events for this door, as well as Challenge viewers on the local server.
13. Click the **More Challenge** tab.



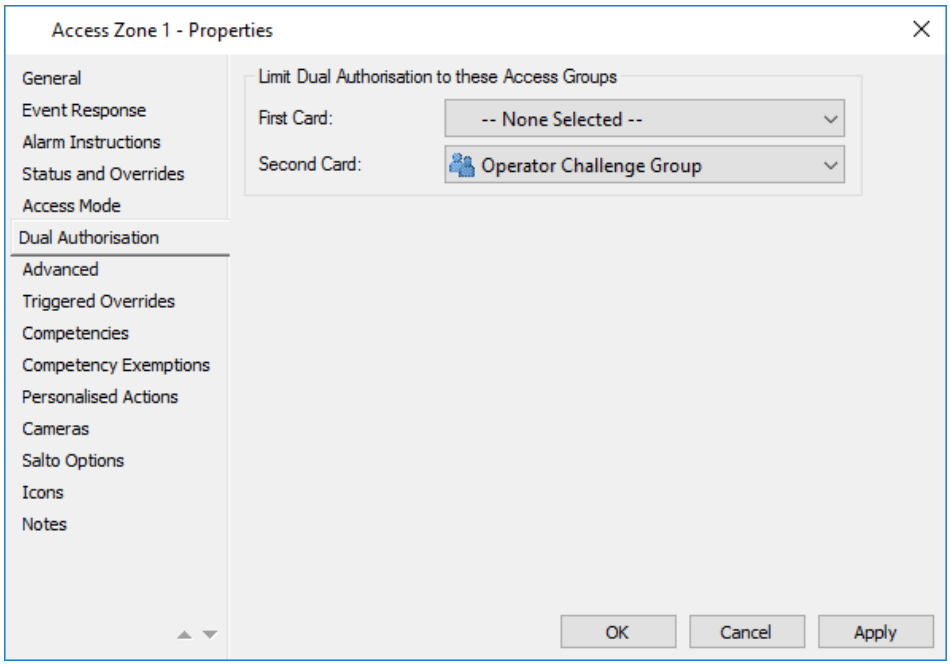
14. From the list the list of text and numeric Personal Data Fields (PDFs), select those that you wish to be displayed in a Viewer window by checking the ☑ tick-box beside the PDFs.
15. Configure a simple font style against each selected PDF.
16. Sort your selection of PDFs by using the **arrow** buttons to the right of the list box if required.
    The order you define will be retained when information is shown in the Challenge Viewer.
17. Click the **OK** button to save your changes to the Door.
18. Set up a new Access Group (see Setting up Access Groups on page 34-4 for the procedure).
    Note: Name the Access Group something meaningful, (e.g. Operator Challenge Group).

    This Access Group will be used for the Dual Authorisation Second Card in Step 24 and should not have any cardholder members. If there are cardholder members, the following message will display when an operator challenges a cardholder using the "Controlled Challenge" mode.



19. Click the **Entry Zone** tab of the Door to see the Door's entry Access Zone, and open the property pages for that Access Zone.

20. Click the **Access Mode** tab.
21. Select an appropriate **Schedule** that is in Dual-Authorisation mode, from the drop-down list.
22. Click the **Dual Authorisation** tab.



23. Select an Access Group from the drop-down list for the **First Card**, or leave blank if all cardholders are authorised to access the Door.
24. Select the new Access Group you configured at Step 18, from the drop-down list for the **Second Card**.
    Note:
    By setting the Access Group for the Second Card only, the cardholder of the first card presented can be from any Access Group, but the operator will be taking on the role of the second cardholder. This prevents a pair of cardholders from accessing a challenged Door as a normal Dual-Authorisation Door.
25. Click the **OK** button to save your changes to the Access Zone

Result

Challenge has been configured for a Door.
Refer to page 22-29 for the operation of Challenge.

Hint

Challenge mode cannot be used in conjunction with 'Double card override' and 'Visitor/Escort' modes.

Configuring Doors for Controlled Challenge mode

Introduction

There are a number of scenarios surrounding how Controlled Challenge can be configured for specific operators/workstations, depending on your site requirements. Below are some possible scenarios, each with configuration instructions to ensure Controlled Challenge works as required.

Scenario 1:

An operator is required to operate Controlled Challenge for a Door(s) and is NOT allowed to “turn it off”.

How to configure:
To do this, the administrator will need to ensure that EITHER:

- The operator is NOT privileged to change the System View, OR
- The operator does not belong to any Operator Group that does NOT have the Controlled Challenge privilege for that Door.

Scenario 2:

An operator is allowed to choose whether or not they will monitor/operate Controlled Challenge for a Door(s).

How to configure:
This is possible using System Views. To do this, the administrator will need to ensure that:

- The operator is privileged to change the System View, AND
- The operator belongs to an Operator Group that has the Controlled Challenge privilege for the Door(s), AND
- The operator also belongs to an Operator Group that does NOT have the Controlled Challenge privilege for that Door.

Scenario 3:

Two operators, working at separate workstations, are required to monitor and/or operate Controlled Challenge for the same Door(s) at the same time.

How to configure:
This is done by putting both operators into an Operator Group which has the Controlled Challenge privilege for the Door(s). In this scenario, for event Challenge Event, access is controlled by the first operator to grant or deny access.

Scenario 4:

One operator is required to operate Controlled Challenge for a Door(s) while another operator is required to operate Controlled Challenge for a different Door(s).

How to configure:
This is done by putting the operators into separate Operator Groups which each have the Controlled Challenge privilege for the appropriate Doors.

Scenario 5:

An operator is required to operate Controlled Challenge for a Door(s) when they are logged onto one workstation but not when they are logged onto another workstation.

How to configure:
To do this, an administrator would need to set up Workstation Operator Groups appropriately.

Scenario 6:

At one workstation, an operator is required to operate Controlled Challenge for a Door(s) and must NOT be allowed to “turn it off”. At another workstation the same operator is allowed to choose whether or not they will monitor/operate Controlled Challenge for that Door(s).

How to configure:
This is possible by using Workstation Operator Groups to prevent the System View from being changed on one workstation but not the other.

Scenario 7:

Morpho biometric readers are being used at doors that have been configured for Controlled Challenge, and are required to provide feedback in a challenge situation. However, Morpho biometric readers do not normally provide feedback in a challenge situation, (i.e. although the fingerprint/vein is accepted, there is no feedback that access has been granted through the door), therefore indicator lights are used to provide feedback.

How to configure:
Feedback using indicator lights at Morpho biometric readers can be achieved, as follows:

1. Create a new output for each indicator light, (i.e. *"Wait Sign"*, *"Access Granted"* and *"Access Denied"*).

2. Create a new virtual output, (i.e. *"Card Presented Event"*).

3. Create two new Macros, (i.e. "*Access Denied Sign Relay"* and *"Card Presented Event"*).

4. Create the following two new Action Plans", and ensure the **Alarm Priority** is set to "Message Only" for both:

   - *"Access Denied Card Event"*.
     On the **Disarmed** tab, drag and drop the "Access Denied Sign Relay" macro to run from this Action Plan into the **Cameras, Macros, and External System Items** grid.

   - *"First card presented event"*.
     On the **Disarmed** tab, drag and drop the "Card Presented Event" macro to run from this Action Plan into the **Cameras, Macros, and External System Items** grid.

5. Create the Challenge Controlled door. On the **Event Response** tab:
   a) Select the "Access Denied" Event Group and assign the "Access Denied Card Event" Action Plan.
   b) Select the "Card Event" Event Group and assign the "First card presented event" Action Plan.

6. Create the following two new Logic Blocks to control the indicator lights:

   - *"Reset Wait Sign"*.
     On the **Rules** tab, add the following **Logic items**; "Access Granted" output, "Access Denied" output and "Door Open Switch" input.
     On the **Timing** tab, set the **Delayed off time** to 3 seconds.

   - *"Wait Sign"*.
     On the **Rules** tab, add the following logic items; "Card Presented Event" virtual output and "Reset Wait Sign" logic block.
     On the **Timing** tab, set the logic block to be latched on until cleared by the "Reset Wait Sign" logic block.

Challenge Viewer - Controlled Challenge mode

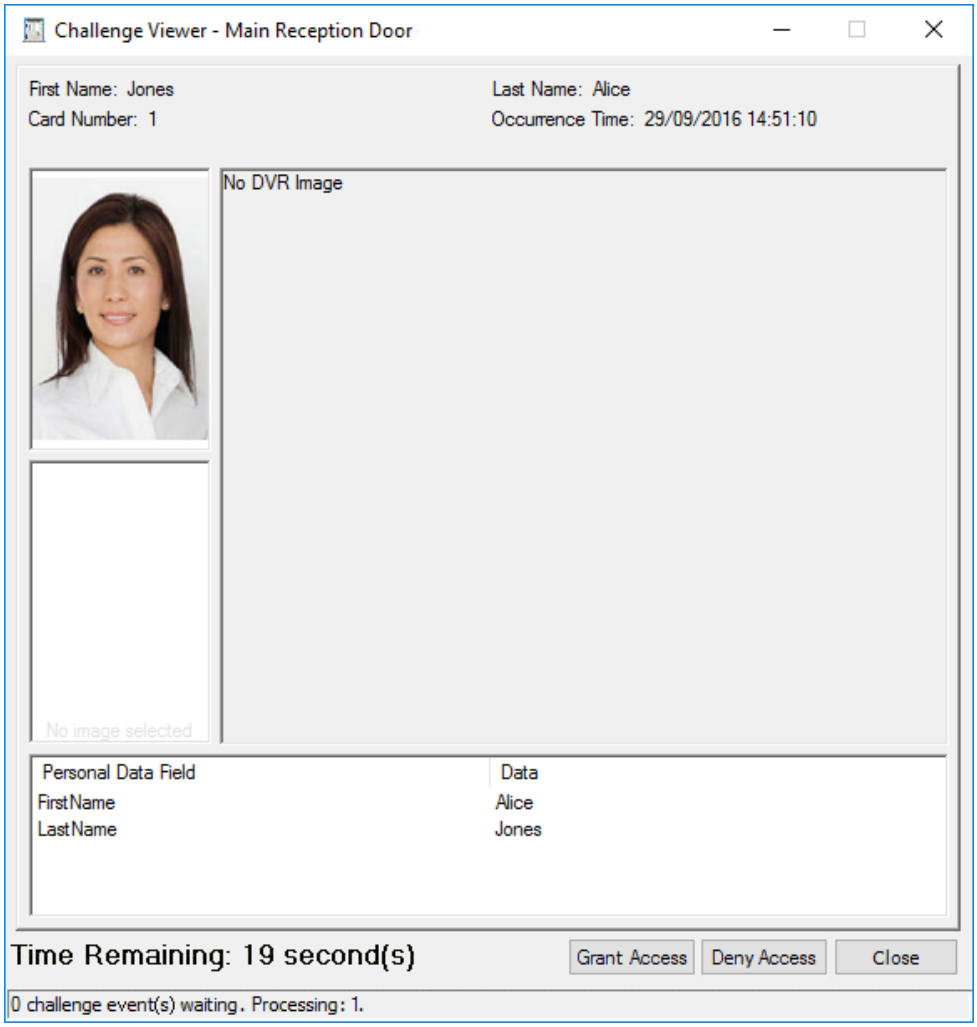
Introduction

When a Door is in Controlled Challenge mode the Challenge Viewer opens automatically for an operator when:

- One of the Door's Access Zones is configured for Controlled Challenge functionality using Dual Authorisation, AND
- The operator has the following operator privileges for the Door (which must be within the operators Division):
  - "View Events and Alarms", and
  - "Controlled Challenge"

The Challenge Viewer pops to the front whenever a Controlled Challenge Event requires processing at a workstation, and the operator makes the final decision as to whether access is granted or denied.

The Controlled Challenge Viewer opens automatically, as long as there are no other Challenge Viewers in Controlled Challenge mode open for this specific Door across all workstations.



This Viewer monitors the system for Card related events for the Door being challenged. When an event is received the Viewer determines what operator action is required based on the event type, the Viewer mode and the Schedule associated with the Door's entry or exit Access Zone.

The Controlled Challenge Viewer displays the following:

- Cardholders details and PDFs as defined in the Property pages of the Door being challenged.
- The 'Time Remaining', which is the number of seconds left before the current Challenge event will time out (at which point the cardholder will be denied access).
- At any one time, only the most outstanding event will be visible and available for processing. However, all Controlled Challenge Events will be queued in this Viewer in the order in which they were raised, and it provides an indication of how many other events are waiting in the queue. If a queued Challenge event times out, then this number will update to display the correct queue count.

Only one Challenge Viewer across all Workstations may be opened in **Controlled** mode per entry and exit side of each Door.

Procedure

1. Decide whether to grant or deny access to the Cardholder, and click the **Grant Access** or **Deny Access** button as appropriate.
   Note:
   If you fail to grant or deny access within the time specified on the **Advanced** property tab of the Door, the cardholder will be denied access. If the **Operator comment required after each Cardholder Challenge** checkbox is ticked in the Door Properties, then another window will display.
2. Enter a short comment.
   The comment is limited to 256 characters and is stored in an operator event in the system.
   Note: Even if an operator comment is not required, an event is still generated. The event includes the following:
   - Whether access was granted or denied
   - Date and time access was granted or denied
   - The Door at which the Challenge occurred
   - The names of the operator that challenged the cardholder, and the cardholder who was challenged
   - The card number presented at the Door.
3. Click the **OK** button.

Challenge Viewer - View-Only mode

Introduction

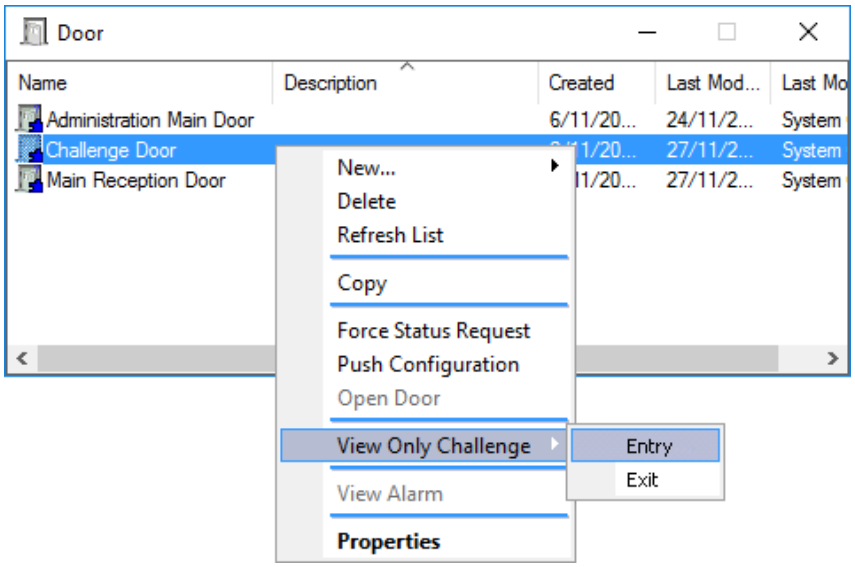
The View-Only Challenge mode allows operators with the “View Challenge” operator privilege to open the Challenge Viewer against the Door (which must be within the operators Division).

The Challenge Viewer opens in View-Only mode, therefore access is granted to the cardholder based on the standard Access Group and Schedule settings without operator intervention.

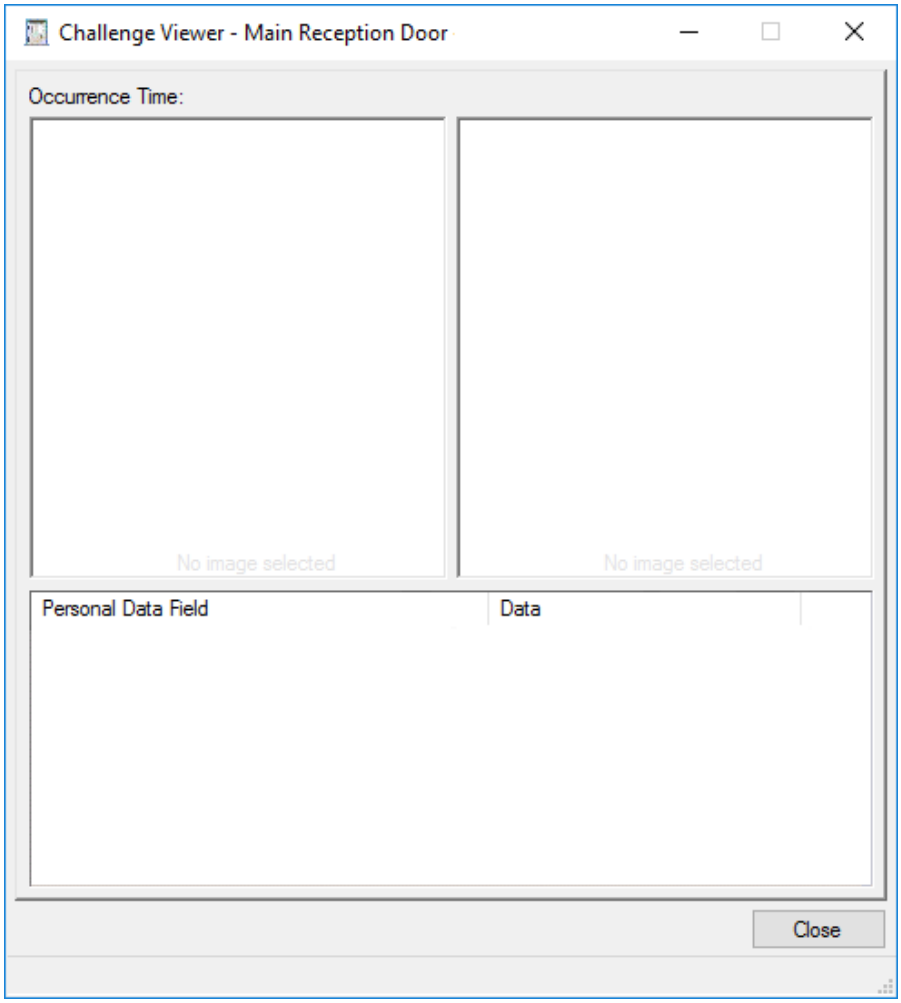
Any number of Challenge Viewers may be opened against a single Door in **View-Only** mode.

Procedure

1. Click **Configure** from the menu bar, then **Doors**.
2. **Right click** on the door you wish to challenge access to.



3. Select **View Only Challenge**, then **Entry** or **Exit** as appropriate.
   The Challenge Viewer opens:



The Challenge Viewer displays the Cardholders details and PDFs as defined in the Property pages of the Door being challenged.
The Challenge Viewer monitors the system for Card related events for the Door being challenged. When an event is received the Viewer determines that it is running in **View Only** mode, therefore there are no **Grant Access** or **Deny Access** buttons available.

4. Click the **Close** button to close the Challenge Viewer.

Action on Access

Introduction

Action on access feature can be used to configure a door to respond to entry and/or exit events.

Competency actions that can be configured to take place (per door) are:

- Disable, enable, expire, or reset the expiry for a Competency immediately
- Disable, enable, expire, or reset the expiry for a Competency after a specified period of time
- Disable or enable a Competency for a specified period

Access Group actions that can be configured to take place (per door) are:

- Assign Access Group membership for a specified time period
- Assign Access Group membership immediately until a specified time (at which time the Access Group membership will expire)
- Expire Access Group membership after a specified period of time.

Credential actions that can be configured to take place (per door) are:

- When a Cardholder presents a credential at a nominated reader, the credential is immediately disabled or enabled.
- When a Cardholder presents a credential at a nominated reader, the credential is disabled or enabled for a specified period of time.

Notes:

- For Competency and Access Group Field actions to take place, an entry granted and taken event, or a successful exit action event must occur for the Cardholder. For Credential actions to take place, present the credential at the appropriate reader.
- This feature has not been tested in a Command Centre multi-server environment.
- The Door FT item configuration options introduced by this feature are not supported in the Command Centre Configuration Client Site Configuration report.
- The ‘Require card to be disabled on creation’ option supported in customisation is not part of the Card Type properties in vEL7.90. Instead, Command Centre allows you to create a Card in any required state via ‘Card States.’ If the Action on Access feature is installed as customisation and you are upgrading to vEL7.90xxx, you can use ‘Disabled (manually)’ state to disable a Card upon creation. See creating a Card State Set and Cardholder Cards Tile actions topics in the Command Centre Client help file.

Consideration

Record locks and conflicts
This feature is unable to alter Competencies, Access Groups, Card Types, or write to Personal Data Fields for locked Cardholders. The workaround for this is to enforce the following conditions:

1. Only modify a Cardholder's record if that Cardholder is unlikely to enter or exit the site at the same time.
2. If (1) cannot be ensured, then it must be assumed that the operator's changes are of greater importance.

Note: The record is locked as soon as the operator starts modifying the Cardholder details and until the changes are applied.

Configuration

To configure this feature, perform the following procedures:

Configuring Competencies

If required, create the Competencies that will be modified when a Cardholder enters or exits through a Door. Ensure these Competencies are assigned to the relevant Cardholders.
Refer to the topics ***Configuring Competencies*** (on page 53-5) and ***Assigning Competencies to Cardholders*** (on page 53-9).

Configuring Access Groups

If required, create the Access Groups that the Cardholder will be assigned when the Cardholder enters or exits through a Door.
Refer to ***Setting up Access Groups*** topic (on page 34-4).
Notes:

- Do not add Cardholders when creating the Access Group. Cardholders will be added to the Access Group when entering or exiting through a Door.
- Ensure the **Automatically remove expired memberships** check box is ticked on the Access Group Membership Defaults tab.

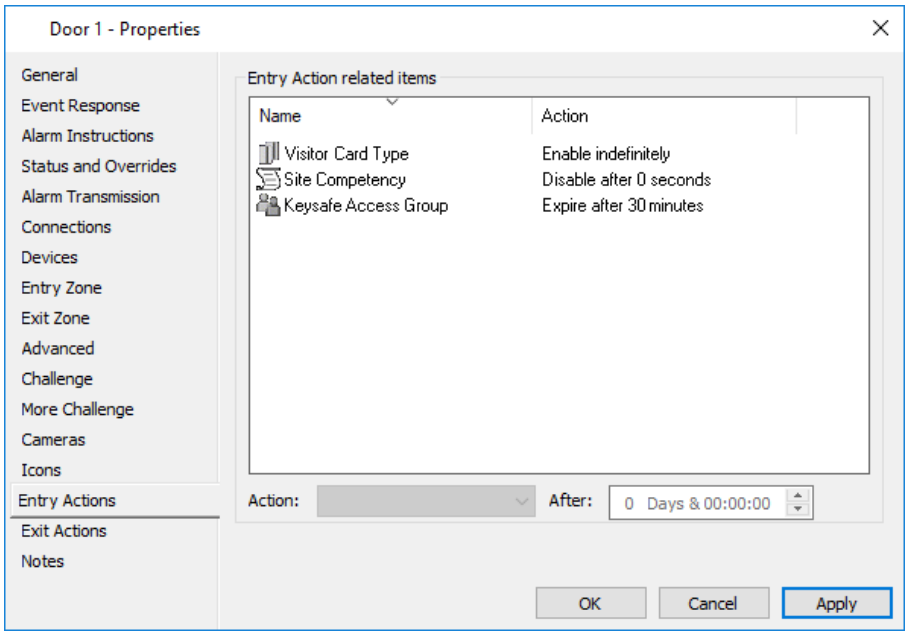
Configuring Entry and Exit Actions on a Door

Configuring a Door
If not already created, create the Door. Refer to the topic Creating Doors (on page 22-2).

Entry Actions

1. Open the properties for the Door (that will modify items upon entry).

2. Click the **Devices** tab. Select an input to act as the Door open sensor. This enables Command Centre to distinguish between "access granted" and "access granted but not taken" events.
3. If using a turnstile door, click the **Advanced** tab. Check the **Access is via turnstile** checkbox.
   This means that when the door opens, only the last person who badged and was granted access is logged as having entered and if two people badge without the door opening, then the first person gets logged as not having entered.
4. Click the **Entry Actions** tab.



5. Configure as required. Refer to the following table:

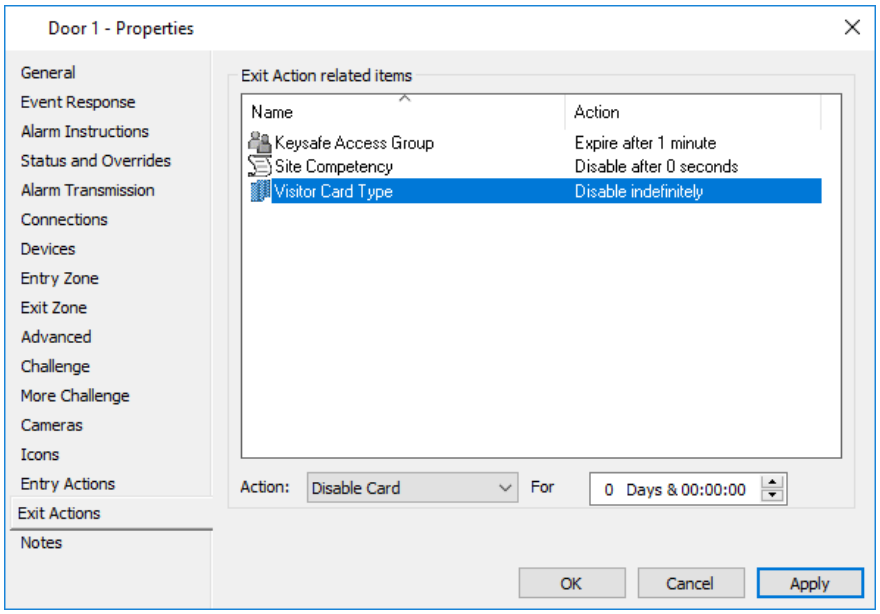
If you want to…	then…
disable, enable, expire, or reset the expiry for a Cardholder's Competency upon entry	**a)** Drag and drop the Competency that will be modified from the Competency list window to the Entry Action related items grid. **b)** Select the Competency, then select the action to be performed upon entry from the **Action** drop-down list and enter the period of time. Maximum 999 days, 23 hours, 59 minutes and 59 seconds. **Note:** If the Competency has already expired, the **Expire Competency** action will not adjust the expiry time. Use the **Reset item to expire** action to reset the expiry time.

If you want to…	then…
assign Access Group membership for a specified time period upon entry	**a)** Drag and drop the Access Group that the Cardholder will be assigned membership to upon entry, from the Access Group list window to the **Entry Action related items** grid. **b)** Select the Access Group then select the **Add Access** action from the **Action** drop-down list. Enter the period of time in the **From** and **Until** fields.
assign Access Group membership immediately until a specified time upon entry	**a)** Drag and drop the Access Group that the Cardholder will be assigned membership to upon entry, from the Access Group list window to the **Entry Action related items** grid. **b)** Select the Access Group then select the **Add Access to Expire** action from the **Action** drop-down list. Enter the period of time in the After field. Maximum 999 days, 23 hours, 59 minutes and 59 seconds.
expire Access Group membership after a specified period of time upon entry	**a)** Drag and drop the Access Group that the Cardholder will be assigned membership to upon entry, from the Access Group list window to the **Entry Action related items** grid. **b)** Select the Access Group then select the **Expire Access** from the **Action** drop-down list. Enter the period of time in the **After** field. Maximum 999 days, 23 hours, 59 minutes and 59 seconds.
disable or enable a credential upon entry	**a)** Drag and drop the Card Type that will be disabled or enabled upon entry, from the Card Type list window to the Entry Action related items grid. **b)** Select the Card Type then select the action to be performed upon entry, from the Action drop-down list and enter the period of time in the After field. Maximum 999 days, 23 hours, 59 minutes and 59 seconds. **c)** When a credential of this type is presented at the entry reader of this Door, the selected action will be performed for the credential.

6. Click the **OK** button.

Exit Actions

1. Open the properties for the Door (that will modify items upon exit).
2. Click the **Devices** tab. Select an input to act as the Door open sensor. This enables Command Centre to distinguish between "access granted" and "access granted but not taken" events.
3. If using a turnstile door, click the **Advanced** tab. Check the **Access is via turnstile** checkbox.
   This means that when the door opens, only the last person who badged and was granted access is logged as having entered and if two people badge without the door opening, then the first person gets logged as not having entered.
4. Click the **Exit Actions** tab.



5. Configure as required. Refer to the following table:

If you want to…	then…
disable, enable, expire, or reset the expiry for a Cardholder's Competency upon exit	**a)** Drag and drop the Competency that will be modified from the Competency list window to the **Exit Action related items** grid. **b)** Select the Competency then select the action to be performed upon exit, from the **Action** drop-down list and enter the period of time. Maximum 999 days, 23 hours, 59 minutes and 59 seconds. **Note**: If the Competency has already expired, the **Expire Competency** action will not adjust the expiry time. Use the **Reset item to expire** action to reset the Competency expiry time.

If you want to…	then…
assign Access Group membership for a specified time period upon exit	**a)** Drag and drop the Access Group that the Cardholder will be assigned membership to upon exit, from the Access Group list window to the **Exit Action related items** grid. **b)** Select the Access Group then select the **Add Access** action from the **Action** drop-down list. Enter the period of time in the **From** and **Until** fields.
assign Access Group membership immediately until a specified time upon exit	**a)** Drag and drop the Access Group that the Cardholder will be assigned membership to upon exit from the Access Group list window to the **Exit Action related items** grid. **b)** Select the Access Group then select the **Add Access to Expire** action from the **Action** drop-down list. Enter the period of time in the **After** field. Maximum 999 days, 23 hours, 59 minutes and 59 seconds.
expire Access Group membership after a specified period of time upon exit	**a)** Drag and drop the Access Group that the Cardholder will be assigned membership to upon exit, from the Access Group list window to the **Entry Action related items** grid. **b)** Select the Access Group then select the **Expire Access** from the **Action** drop-down list. Enter the period of time in the **After** field. Maximum 999 days, 23 hours, 59 minutes and 59 seconds.
disable or enable a credential upon exit	**a)** Drag and drop the Card Type that will be disabled or enabled upon exit, from the Card Type list window to the **Exit Action related items** grid. **b)** Select the Card Type then select the action to be performed upon exit, from the **Action** drop-down list and enter the period of time in the **After** field. Maximum 999 days, 23 hours, 59 minutes and 59 seconds. **c)** When a credential of this type is presented at the exit reader of this Door, the selected action will be performed for the credential.

6. Click the **OK** button.

Chapter 23: Elevator Cars

This chapter covers the following:

- ***Low Level Interface Elevator Cars*** (on page 23-2)
- ***High Level Interface Elevator Cars*** (on page 23-8)

Low Level Interface Elevator Cars

The Controller provides low level elevator access control using readers and input/output interfaces.

Readers may be installed in elevator cars to provide restricted access to floors with or without a PIN. Floors may be "unlocked", (i.e. the elevator floor select button enabled) on a time schedule.
Where entry to specific floors requires a PIN, the corresponding floor select buttons in the Elevator Car will not be enabled unless the Cardholder correctly enters their PIN. Access to other floors, that do not require PIN entry is allowed.

Note: See ***Configuring Local Overrides at Card Readers*** (on page 45-14) for further detail regarding card readers in elevators.

The flexible design of the Controller allows the Controller to be configured for almost any elevator control situation. The configuration is limited only by the following:

- Up to 75 levels per Controller
- Up to 4 elevator shafts per Controller 6000 or 7000

Typically, elevator control requires one card reader for each elevator car and one output for each floor select button in each elevator car. If destination reporting is required, then one input is required for each floor select button in each elevator car. If you are configuring elevator cars that are controlled via a high level interface refer to ***High Level Interface Elevator Cars*** (on page 23-8).

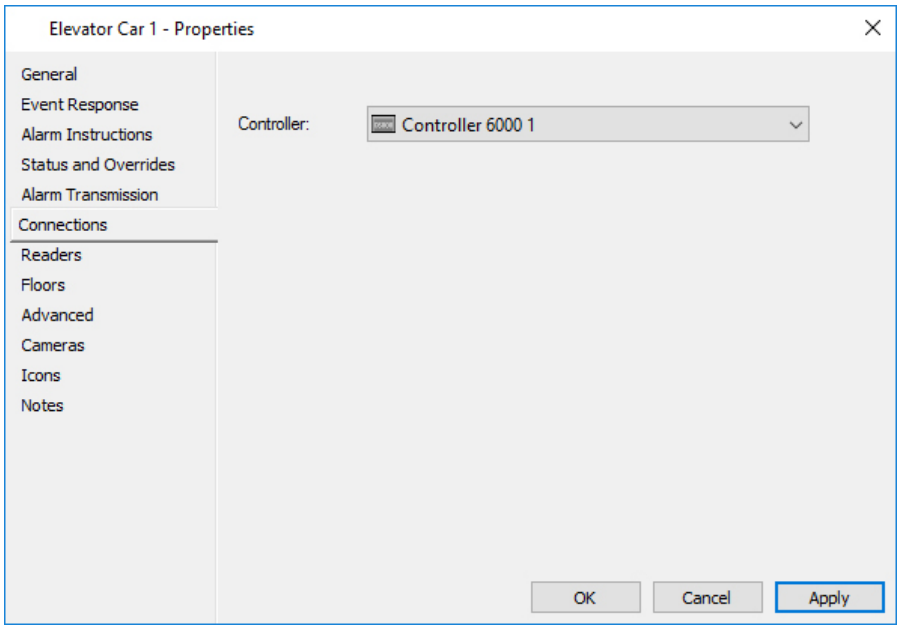
Configuring Elevator Cars

Introduction

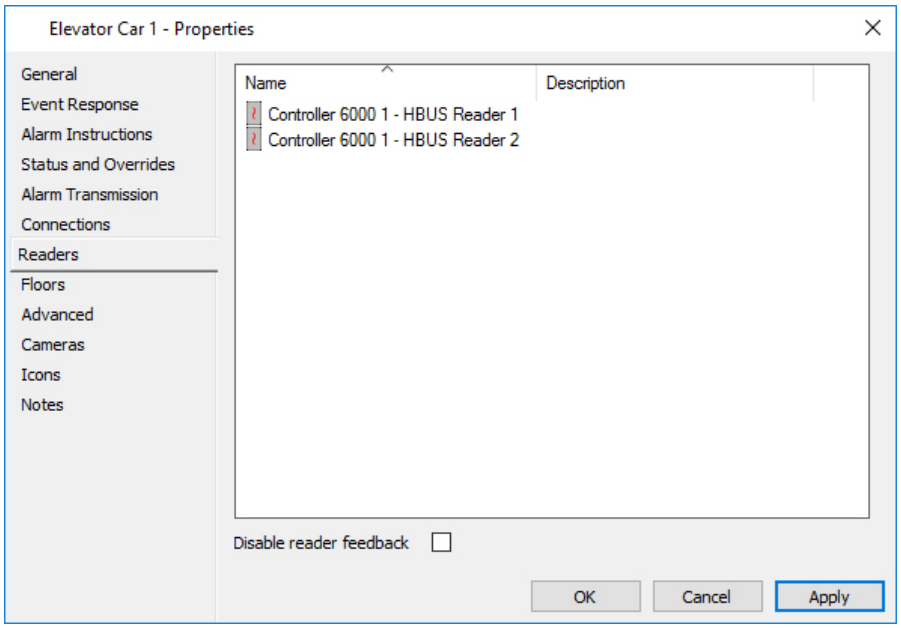
This procedure enables an operator with the "Edit Site" operator privilege to configure an Elevator Car.

Procedure

1. Click **Configure** from the menu bar, then **Elevator Cars**.
   The **Elevator Car** List Window opens (in grid view).
2. **Right click** and select **New...Elevator Car**.
   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 **Connections** tab.

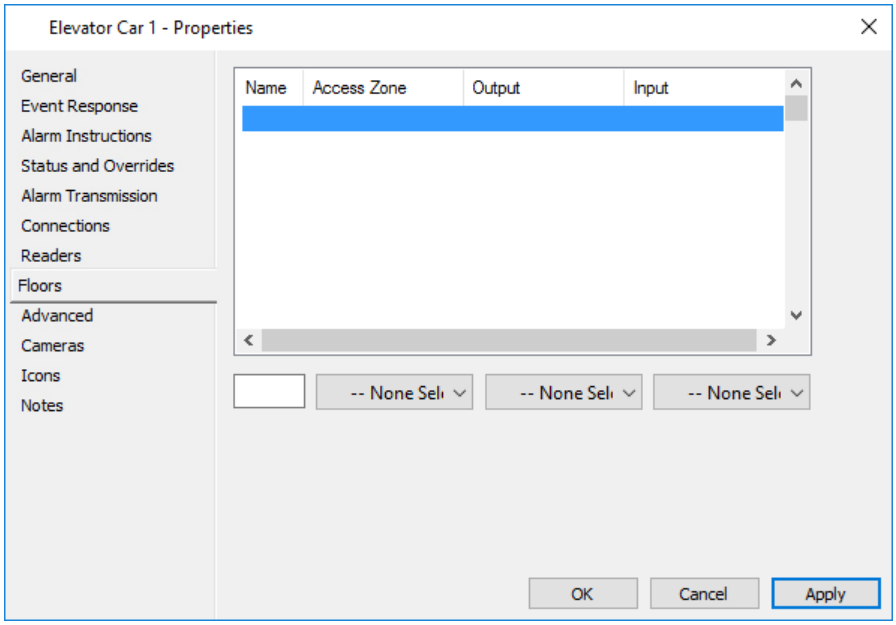


5. Enter the Controller for this Elevator Car.
6. Click the **Readers** tab.
7. Enter the Readers for this Elevator Car.

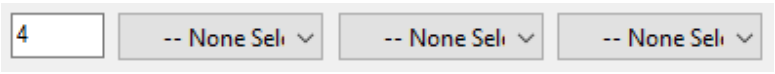


Note: All readers installed in the elevator car function the same. E.g. An elevator car has readers A and B. The Cardholder badges at reader A. If access is granted through reader A, reader B will also grant access simultaneously.

8. Check the **Disable reader feedback** checkbox if required.
   If this option is checked, then the elevator cars reader will not display prompts, icons, LEDs, or make access granted or access denied sounds when access attempts are made at the reader.
   Note: When checked, this option has the effect of disabling any feature that requires reader feedback, (e.g. PINs, Code or Card mode, local overrides).
9. Click the **Floors** tab.
   There are 75 slots available for floor data to be entered.
10. Start at the "top" slot on this screen by clicking the mouse button at the top of the white area.
    The first slot is highlighted and the fields across the bottom of the window are no longer greyed out.
    Note: Elevator Floors should be entered in descending order, (i.e. the top floor down to the lowest floor).



11. Enter the Name of the floor, (i.e. usually what is embossed on the elevator button in the elevator car, e.g. floor number, G for Ground, B for Basement, etc.) in the first field at the bottom of the screen.

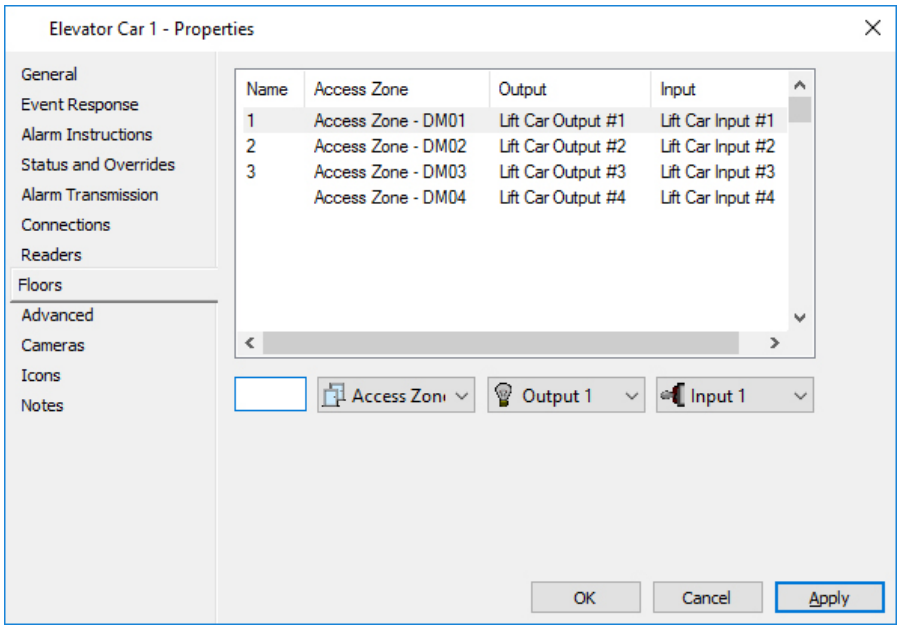


Note: Floor names are limited to four characters.

12. Click in the first field with an arrow box, and select the Access Zone that represents the area outside the elevator on this particular floor, from the drop-down list.
13. Click the next field and select the "Floor Select" output from the drop-down list. In Elevator Car configuration, outputs are used to activate the floor buttons, (i.e. enables the button to be used).
14. Click the last field and select an input to remove wait states, if required.

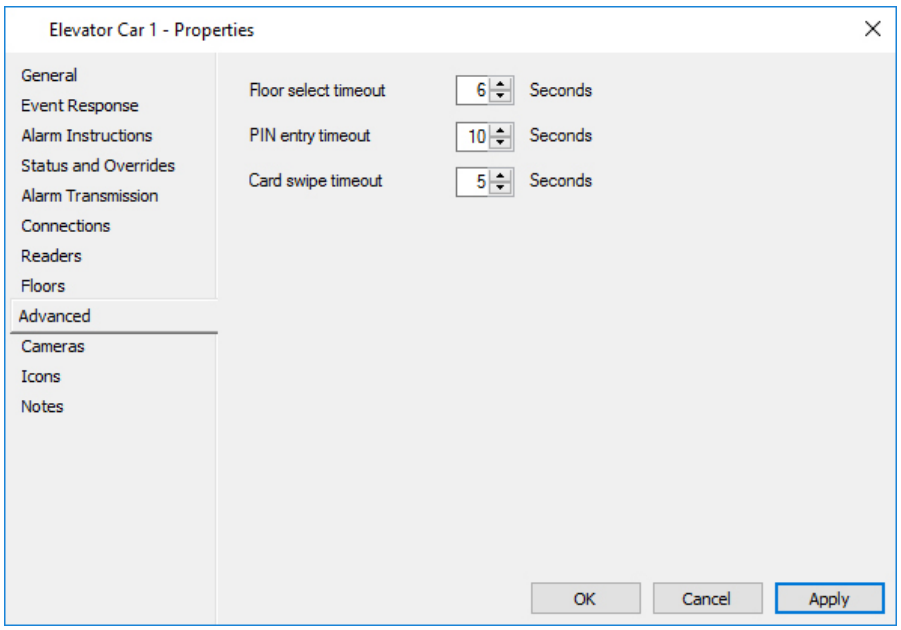
    This Input will cancel the wait state (as configured on the **Advanced** tab in the "Floor select timeout" field), for inputting or pressing a floor button. Once a cardholder badges their card there is normally an active wait state allowing time for the cardholder to select (push) the required floor button. The Inputs are used to deactivate all the floor buttons again, as soon as one has been pushed. This stops another person in the elevator-car pushing another floor button, that they should not have access to while the floor buttons are in an active state.

    Adding an Input to each floor button also provides a more precise audit trail of cardholder movement throughout a building. An Activity Report will show which button each cardholder pushed in the elevator car, indicating which floor (or access zone) they most likely entered.
15. Repeat Steps 10-14 for each floor you need to create.



Note: Should you need to delete a floor, highlight the floor, then clear the Name field at the bottom of the window and set all the other fields to --None Selected--. This may result in a gap in the list of 75 floors available. This does not matter however, as the choice of which slots are used does not affect the operation of the Elevator Car, nor does the order of the slots matter.

16. Click the **Advanced** tab.



17. Change the Advanced Settings as required.
18. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Elevator Car.
    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 Elevator Car.
    For further details regarding the **Icons** tab, see **Icons** (on page 6-80).

20. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Elevator Car.
    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 this Elevator Car.
    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.

Result

An Elevator Car is configured.

Hint

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

High Level Interface Elevator Cars

Introduction

Access from elevator cars can be controlled using a high level interface (Elevator HLI) between a Controller and the elevator control system. Alternatively, access from elevator cars is controlled using outputs from the Command Centre system to enable or disable specific elevator floor select buttons within an elevator car. Each method requires different configuration.

This section deals with configuring elevator cars that are controlled via a high level interface. If you are using outputs to control access to floors from within elevator cars refer to ***Elevator Cars*** (on page 23-1).

Licensing

The following license entries apply to the Command Centre Elevator HLI feature:

Licence	Description
[Limits] HLI Lift Cars=nnnn	Where nnnn is the maximum number of high level interface elevator cars (Elevator Car HLIs) that can be created. Once the maximum number has been reached the option to create additional Elevator Car HLIs will be disabled.
Kone – This integration is not licensed	Command Centre integrates with the Kone Protocol v2.5 communications protocol. This integration is a non-licensed feature of Command Centre. Communication is via the RS232 serial port on the Gallagher Controller.
Otis - This integration is not licensed	Command Centre supports the Otis E.M.S - Security/B.M.S Protocol, Otis Ref No. 51646B. This integration is a non-licensed feature of Command Centre. Communication is via the RS232 serial port on the Gallagher Controller.
[Features] ThyssenKruppHLI=1	Is required when integrating the ThyssenKrupp elevator system with Command Centre. Communication is via the RS232 serial port on the Gallagher Controller.
[Features] OtisCompassHLI=1	Is required when integrating the Otis Compass Destination Management System with Command Centre. Communication is via TCP/IP but the integration will use the RS232 serial port on the Controller. For information on how to install and configure this integration, refer to the document *"Release Note Otis Compass HLI (v7.60).pdf"* located in the **`Utilities\System Interfaces\OtisCompassHLI`** folder of the Command Centre installation files.

Licence	Description
[Features] OtisModbusHLI=1	Is required when integrating the Otis Modbus elevator system with Command Centre. Communication is via the RS232 serial port on the Gallagher Controller. This integration requires an RS232 to RS485 converter.
[Features] SchindlerHLI=1	Is required when integrating the Schindler elevator system with Command Centre. Communication is via the RS232 serial port on the Gallagher Controller. **Note:** This is a separate integration to that of the SchindlerID integration. The SchindlerID integration synchronises the Command Centre cardholder database with the SchindlerID user database via TCP/IP. Refer to External Systems for further details.
[Features] KoneELI=1 If the KoneRCGIF plugin is required, the following licence entries are also required: [Limits] Event Sources=n [Plugin] PluginX=KoneRCGIF	Is required when integrating the Kone ELI elevator system (Kone Socket Based Destination Call Giving Interface Specification Rev 1.5.1 829390) with Command Centre. Communication is via TCP/IP but the integration will consume the RS232 serial port. Optionally, the Kone Remote Call Giving Interface (RCGIF) plugin enables a tenant to direct an elevator car to the tenant's floor for a visitor. Please contact allagher echnical Support for obtaining the one RC IF plugin.
[Limits] SchindlerID Systems=n If using SchindlerID plugins the following licence entries are required: [Plugin] PluginX=SchindlerID-LifeReporting PluginX=SchindlerID-CallInterface	Is required when integrating Command Centre with SchindlerID v1.3.369.1 Where n is the maximum number of SchindlerID Systems that can be created. Once the maximum number has been reached the option to create additional SchindlerID Systems will be disabled. A SchindlerID System integrates the Command Centre cardholder database with the Schindler user database via TCP/IP. Optionally, the SchindlerID Life Reporting plugin enables Command Centre to build an audit trail for lift access events. Optionally, the SchindlerID Call Interface plugin is required if you are using Gallagher readers on elevator terminals and are controlling a floor's secure/free state from Command Centre.

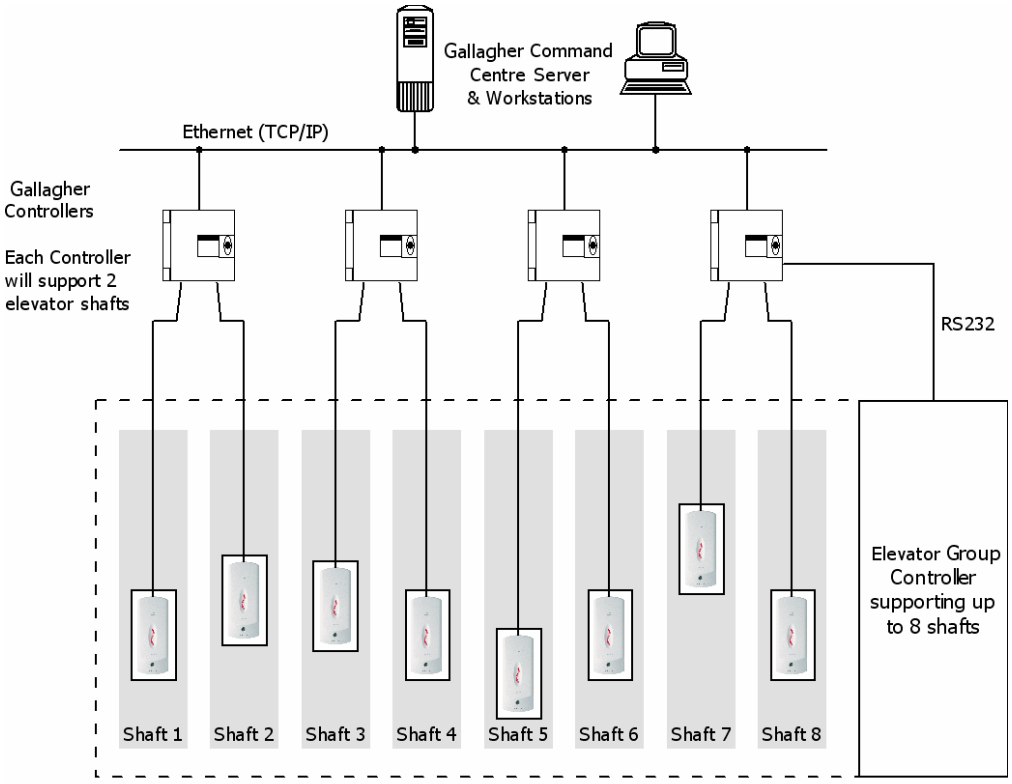
- ***Understanding the High Level Elevator Interface*** (on page 23-11)
- ***Performance*** (on page 23-14)
- ***Configuring High Level Elevator Interfaces*** (on page 23-15)
- ***Configuring a Floor Arrangement*** (on page 23-18)
- ***Configuring an Elevator Car HLI*** (on page 23-21)
- ***Copying an Elevator Car*** (on page 23-27)
- ***Performing executive overrides*** (on page 23-28)
- ***Supported elevator systems - Additional Configuration and Troubleshooting*** (on page 23-30)

Understanding the High Level Elevator Interface

Introduction

Communication with the elevator system is via an RS232 serial communications link between the Controller and the elevator system. The Elevator HLI item represents this link. When access to a floor changes, due to a time schedule or an access event at an elevator car reader, a message is sent from the Controller to the elevator system instructing it to enable or disable specific elevator floor select buttons. There is individual control by floor (or access zone) and by elevator car.

The following diagram shows the system configuration for interfacing to a Kone elevator system.



Conceptual Diagram Only
Specific hardware units and connections are not shown as each site requirement will differ

How it Works

An access zone is assigned to each floor that an elevator car travels to. The access zone represents the area immediately outside the elevator on that floor. By default, the floor select buttons in the elevator car are enabled if the corresponding access zone is in free access, or disabled if the corresponding access zone is secure. Every cardholder has access to floors that are not controlled by Gallagher.

When a cardholder makes a valid access attempt at the elevator car reader, the Controller sends a message to the elevator system instructing it to enable the floor select buttons for those floors (or zones) to which the cardholder has access. After the cardholder selects a floor, or a specified timeout period has expired, the floor select buttons in the elevator car return to the default state.

The Controller polls the elevator system at regular intervals, ensuring that if connection to the elevator system is lost, it is detected and an alarm is raised. Gallagher sends a message to the elevator system each time access to any floor changes. The elevator system replies to each poll.

Communication Interface

As the Controller has only one serial port, each serial connection to the elevator system requires a separate Controller. A Controller 6000 or 7000 can be used to provide the high level communications interface to the elevator system.

Lost Connection to the Elevator System

When the connection between the Controller and the elevator system is lost, the elevator system determines what access is allowed from elevator cars. Normally, this means all floors are set to free access until the connection is re-established. The Controller continues to poll the elevator system. Communication is re-established automatically and the floors re-secured as soon as the elevator system responds to a poll from the Controller.

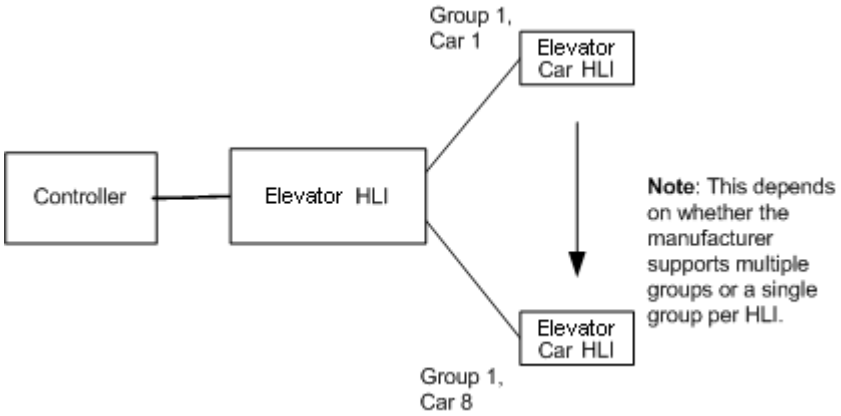
Supported elevator systems

Gallagher has been tested with and supports a number of elevator system protocols via the Elevator HLI. As the protocol that is used is specific to each manufacturer, variations may be required to support other elevator systems. Gallagher has been designed with the ability to customise manufacturer specific variables without requiring a new version of Controller. For information regarding the support of other manufacturers' elevator systems contact your local Gallagher dealer.

Note: Some of the supported elevator system protocols may have limitations. Refer to ***Supported elevator systems - Additional Configuration and Troubleshooting*** (on page 23-28) for further information.

Configuration

Each Elevator Car HLI must be associated with an Elevator HLI item. For further detail refer to ***Configuring High Level Elevator Interfaces*** (on page 23-15). The following diagram shows the items that must be configured for each high level elevator interface.



Readers and Access

Elevator control requires one card reader for each elevator car. Elevator car card readers can be connected to any Controller within the system. If a cardholder badges their card at an elevator car reader before the previous cardholder has completed their floor button selection, the second cardholder's access will supercede the first. This means the first cardholder will need to badge their card again to select the floor they require. This behaviour ensures that where a cardholder badges their card and then leaves the elevator car without selecting a floor, the access attempt of the next cardholder entering the elevator car isn't affected (or delayed).

Where entry to specific floors requires a PIN, the corresponding floor select buttons in the elevator car will not be enabled unless the cardholder correctly enters their PIN. Access to other floors, that do not require PIN entry, is allowed.

Floor Select Reporting

Where it is supported by the elevator system manufacturer Gallagher will report the floor that was selected following an access granted event at an elevator car.

System Limits

The Elevator HLI protocol determines the following system limits:

HLI	Controller 6000/7000
Levels per Elevator Car	256
Elevator Cars per Controller	8* This number describes the size of the configuration that is able to be hosted on the Controller.
Transactions per second	2* This is the number of cardholder access decisions that are able to be made with a high number of floors/ elevator cars.

Performance

Introduction

There are specific system configurations that will improve the response time between Command Centre and the elevator system.

Wherever possible you should conform to the following guidelines:

- The Elevator Car HLI and Reader should be hosted on the same Controller.
- Where cardholders require access to more than one level, it is better to create one access group that gives access to all the required levels, rather than creating multiple access groups that each provide access to only one level.
- The "Change to the Disarmed state" access group privilege (for Alarm Zones) should be used sparingly as it significantly impacts the response time. However, if this privilege is used the Alarm Zone should be on the same Controller as the Elevator Car.

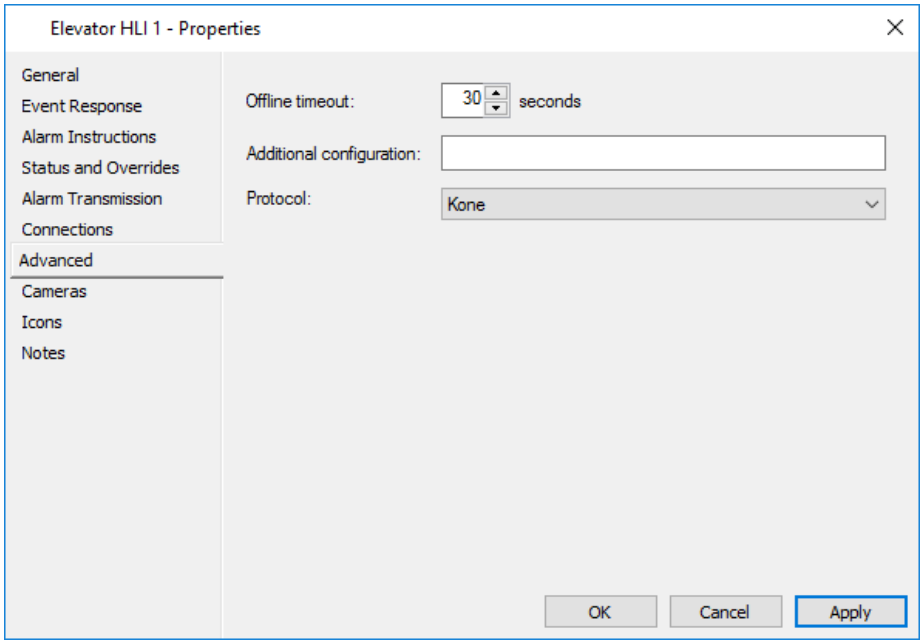
Configuring High Level Elevator Interfaces

Introduction

This procedure enables an operator with "Edit Site" privilege to configure an Elevator HLI. Before carrying out this procedure ensure you have created the Controller that hosts the high level elevator interface. Refer to ***Creating Controllers*** (on page 21-2).

Procedure

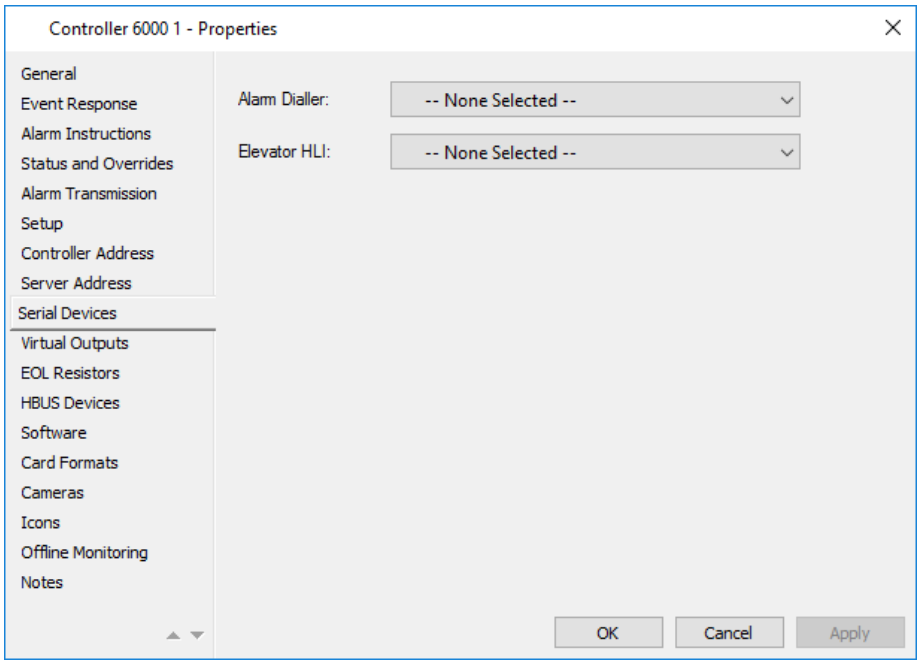
1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
2. **Right click** and select **New...RS232 Devices** > **Elevator HLI**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Advanced** tab.



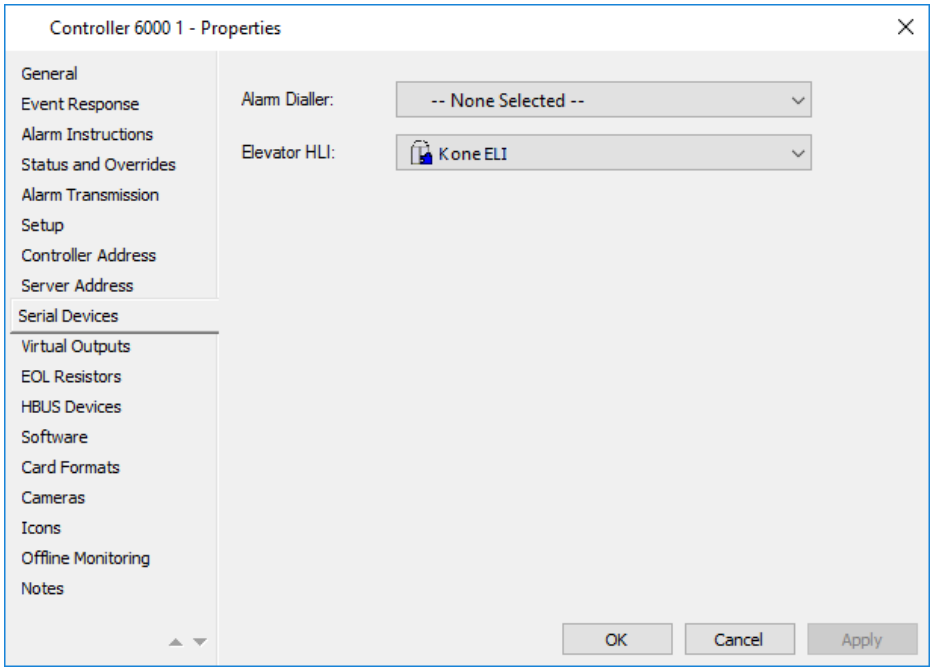
5. Enter the Offline timeout. A time between 30 and 120 seconds can be entered. After sending a command frame, Command Centre will wait for this period of time for a response from the elevator system. If no response is received it is assumed that communication with the elevator system has been lost and an alarm (or event) is generated. The status of the Elevator HLI changes to offline.
   Note: If you are configuring the Kone ELI Elevator HLI feature, set the **Offline timeout** to at least 60 seconds.
6. The **Additional configuration** field provides a means of altering manufacturer specific properties of the Elevator HLI that can vary between installations of an elevator system. It should only be configured on advice

from Gallagher Group Limited.
Refer to ***Supported elevator systems - Additional Configuration and Troubleshooting*** (on page 23-28) for further information on the parameters that can be entered for different elevator system protocols.

7. Select the elevator system **Protocol** you require from the drop-down list.
Note: The protocols that appear in the list will depend on what elevator system protocols your site is licensed for.
8. Click the **Icons** tab if you want to change the Icon Set for this Elevator HLI. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
9. Click the **Notes** tab if you want to add a note(s) about this Elevator HLI. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
10. Click **Apply**.
11. Return to the **Hardware** List Window, and **right click** on the Controller that will host this Elevator HLI and select **Properties**.
12. Click the **Serial Devices** tab.



13. Select the Elevator HLI you have just created from the drop-down list.



Notes:

- The Controller can communicate with either an Alarm Dialler or an Elevator HLI, but not both, using the Controller serial port connection.
- The link between the Elevator HLI and the Controller that hosts it is configured in the Controller properties, Serial Devices tab and is then displayed (but is not editable) on the Connections tab of the Elevator HLI.

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

An Elevator HLI is configured.

Hint

Editing and Deleting Elevator HLIs
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Elevator HLIs.
Note: The system will not allow you to delete an Elevator HLI if it is associated with an Elevator Car HLI.

Configuring a Floor Arrangement

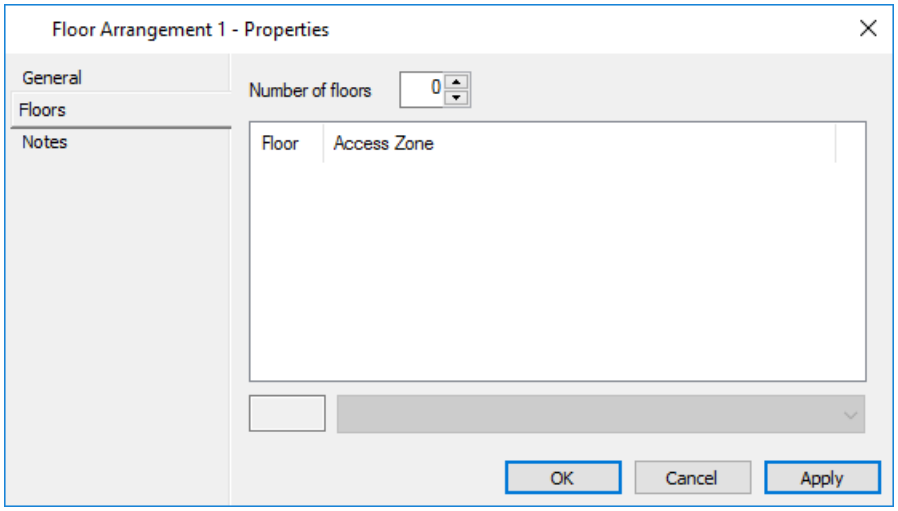
Introduction

A Floor Arrangement enables you to specify the number of floors and the Access Zone that represents the area outside the elevator on each particular floor.

Once configured, a Floor Arrangement can be assigned to multiple Elevator Car HLIs. While the configuration of a Floor Arrangement is optional (Access Zones for floors can be configured directly within each Elevator Car HLI), it is recommended that you do so.

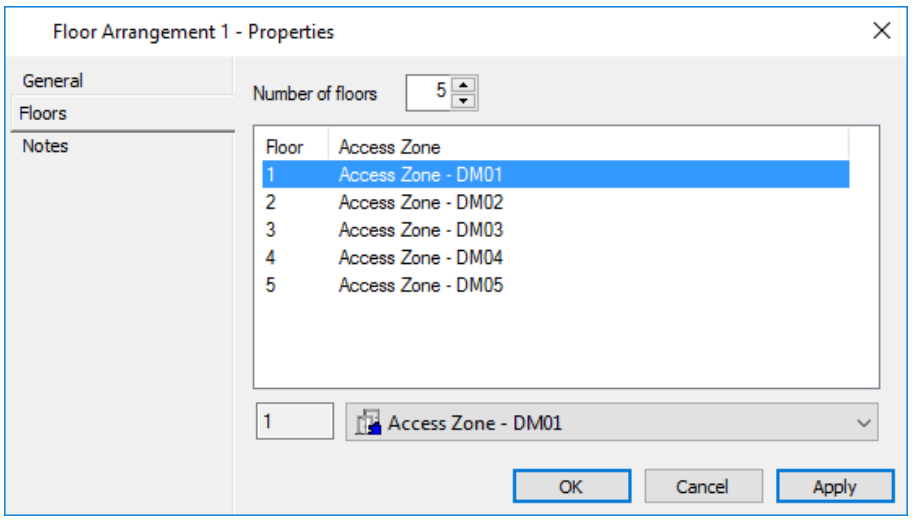
Procedure

1. Click **Configure** from the menu bar, then **Elevator Cars**.
   The **Elevator Car** List Window opens (in grid view).
2. **Right click** and select **New...Floor Arrangement**.
   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 **Floors** tab.



5. Enter or select the **Number of floors** accessed by the elevator group, (range 1-256). This automatically populates the table with the required number of Floors.
   Notes:
   - The Floor column refers to the number used by the elevator group controller (and within the HLI protocol) to refer to this floor. It is not the floor number by which the level is commonly known, (i.e. what is embossed on the elevator button in the elevator car). Floor numbers used within the HLI can also differ between elevator groups within the same elevator system.
   - The number of floors supported is protocol dependent.

6. Click on a row (or Floor) to select it. Select the Access Zone that represents the area outside the elevator on this particular floor, from the drop-down list immediately below the table.



7. Repeat Step 6 until an Access Zone has been selected for each Floor to which access is controlled by Command Centre.
   Notes:
   - If you do not select an Access Zone for a Floor, this means the associated floor is in free access mode.
   - To configure rear doors for elevator cars that have front and rear doors that lead to different Access Zones, refer to “Rear doors” later in this topic.
   - Whenever a change to a Cardholder’s access is made, all access for the Cardholder is sent to the Controller. If the access for a large number of Cardholders is changed at one time, (e.g. the Floor Arrangement item is modified), this will result in a large number of messages being sent to the Controller. The messages pending can be viewed on the **Status and Overrides** tab in the Controller properties. It is recommended that a large change to Cardholder access, be done at a time when the Controller is at its least busiest, (i.e. after hours).
8. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Floor Arrangement.
   For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
9. Click the **Notes** tab if you want to add a note(s) about this Floor Arrangement.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
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.

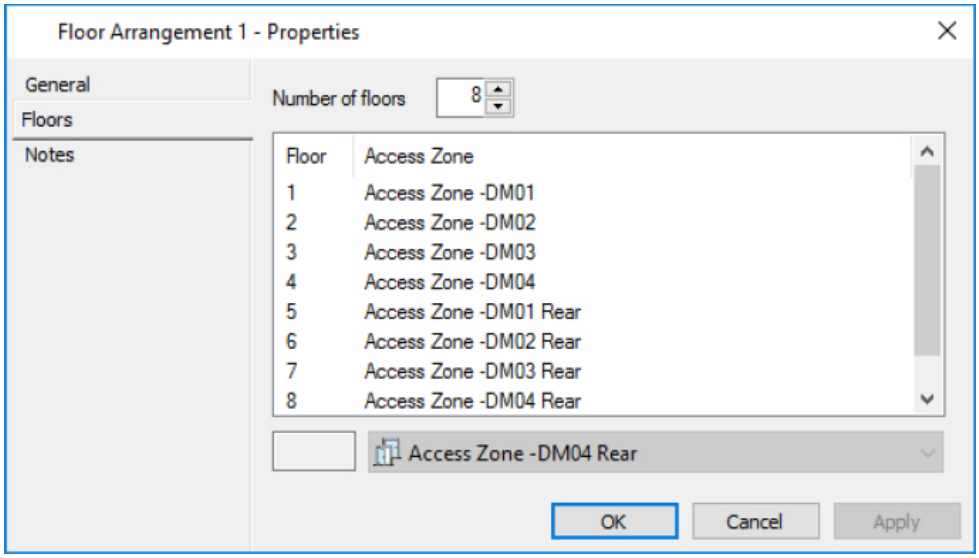
Result

A Floor Arrangement is configured and can be assigned to an Elevator Car HLI.

Rear doors

The Otis Compass and Kone ELI elevator system integrations currently support rear doors on elevator cars. If you are not using one of these integrations, ignore the following.

You can manage access to both front and rear elevator doors. In the Floor arrangement, you must create double the amount of floors specified in elevator HLI configuration. For instance, if you have 4 floors, in the Floor Arrangement, you would need to configure 8 floors (4 for front and 4 for rear). In the Floor Arrangement, the fifth floor represents the first floor's rear door and the sixth floor is the second floor's rear door and so on. If you have a floor that only has one door (either a front or rear door), you still need to configure two floors for it (one with access and the other without access). Ten Floors and Access Zones are configured below, to represent five physical floors with front and rear doors:



You also need to refer to ***Supported elevator systems - Additional Configuration and Troubleshooting*** (on page 23-30) for integration-specific rear door configuration (e.g. configuration specific to Otis Compass).

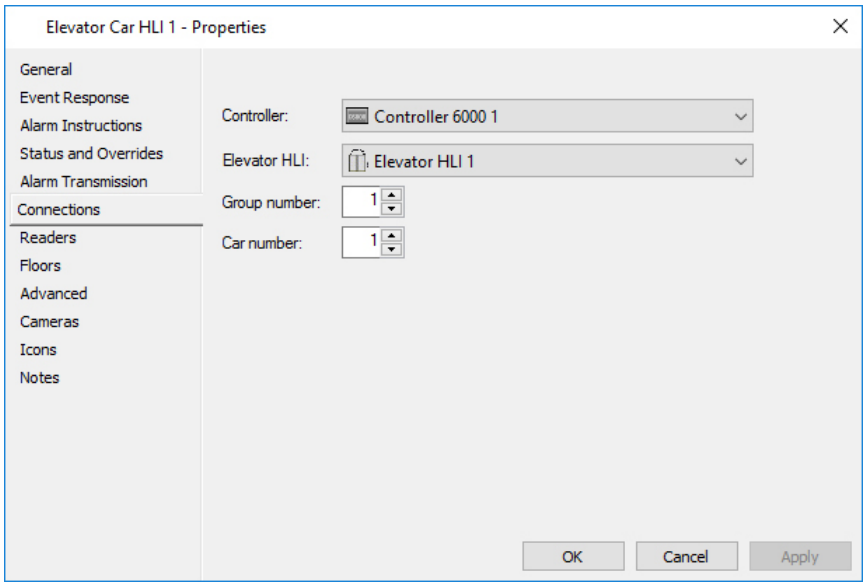
Configuring an Elevator Car HLI

Introduction

This procedure enables an operator with "Edit Site" privilege to configure an Elevator Car HLI. Use this procedure if the elevator system associated with this elevator car connects to Command Centre via a high level interface. Use the Configuring Elevator Cars procedure instead, if the elevator car floor select buttons will be controlled via outputs.

Procedure

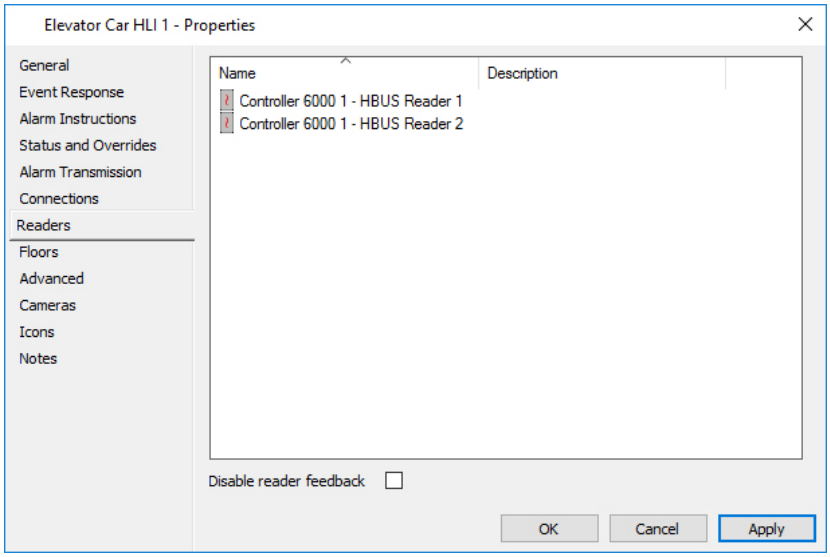
1. Click **Configure** from the menu bar, then **Elevator Cars**.
   The **Elevator Car** List Window opens (in grid view).
2. **Right click** and select **New...Elevator Car HLI**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Connections** tab.



5. Enter the following:
   - the Controller that will be making access decisions for this elevator car,
   - the Elevator HLI that will provide the communication interface to the elevator system,
   - the Group number that this elevator car belongs to, and
   - the Car number.

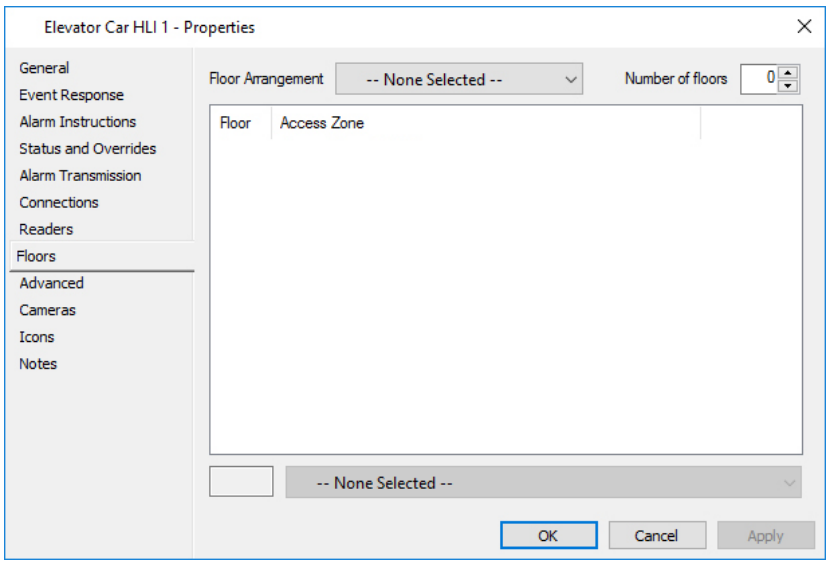
   Note: The Group number and Car number are the numbers defined within the elevator control system that together reference a specific elevator car. Refer to ***Troubleshooting - Supported elevator systems*** (on page 23-30) for details regarding the Group number and Car number configuration for your third party elevator system.

6. Click the **Readers** tab.
7. Enter the Reader installed in the elevator car.



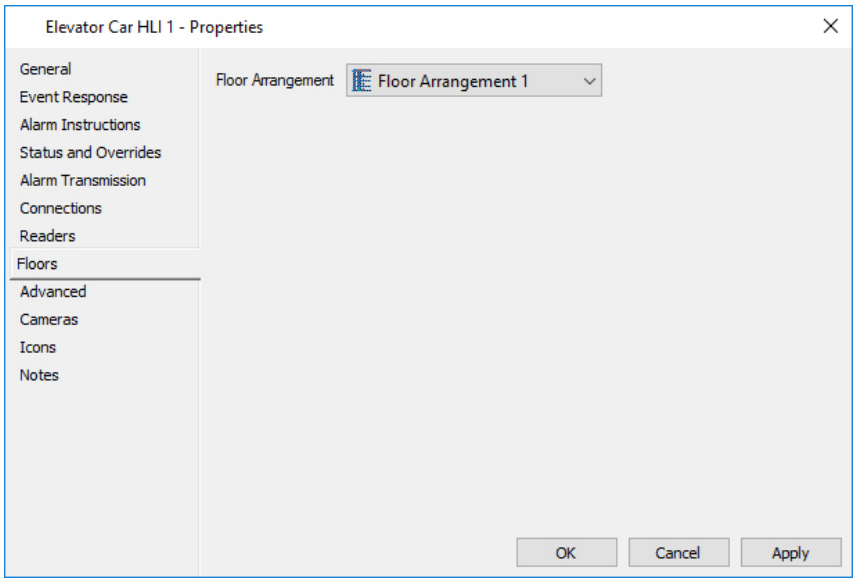
Note: All readers installed in the elevator car HLI function the same. E.g. An elevator car HLI has readers A and B. The Cardholder badges at reader A. If access is granted through reader A, reader B will also grant access simultaneously.

8. Check the **Disable reader feedback** checkbox if required.
   If this option is checked, then the elevator cars reader will not display prompts, icons, LEDs, or make access granted or access denied sounds when access attempts are made at the reader.
   Note: When checked, this option has the effect of disabling any feature that requires reader feedback, (e.g. PINs, Code or Card mode, local overrides).
9. Click the **Floors** tab.

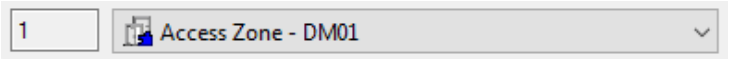


Note: All Elevator Car HLIs that are assigned to the same Elevator HLI must be assigned the same number of floors, whether this number be determined by **Floor Arrangement** or by **Number of floors**. If you have Elevator Car HLIs that need different numbers of floors from each other, they must be assigned to separate Elevator HLIs.

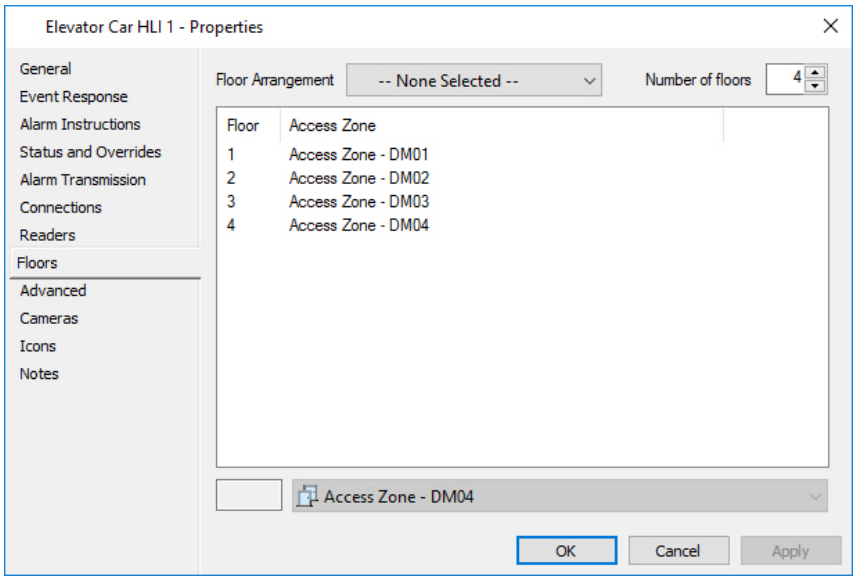
10. Has a Floor Arrangement been configured?
    If **yes**, go to Step 10.
    If **no**, go to Step 11.
11. Select the Floor Arrangement for this Elelvator Car HLI from the **Floor Arrangement** drop-down list. Go to the **Advanced** tab (Step 15).



12. Enter or select the Number of floors accessed by the elevator group.
    This automatically populates the table with the required number of Floors.
    Notes:
    - The Floor column refers to the number used by the elevator group controller (and within the HLI protocol) to refer to this floor. It is not the floor number by which the level is commonly known (i.e. what is embossed on the elevator button in the elevator car). Floor numbers used within the HLI can also differ between elevator groups within the same elevator system.
    - Whenever a change to a Cardholder's access is made, all access for the Cardholder is sent to the Controller. If the access for a large number of Cardholders is changed at one time, (e.g. the Floors within an Elevator Car HLI are changed), this will result in a large number of messages being sent to the Controller. The messages pending can be viewed on the **Status and Overrides** tab in the Controller properties. It is recommended that a large change to Cardholder access, be done at a time when the Controller is at its least busiest, (i.e. after hours).
13. Click on a row (or Floor) to select it. Select the Access Zone that represents the area outside the elevator on this particular floor, from the drop-down list immediately below the table.



14. Repeat Step 13 until an Access Zone has been selected for each Floor to which access is controlled by the Command Centre system.



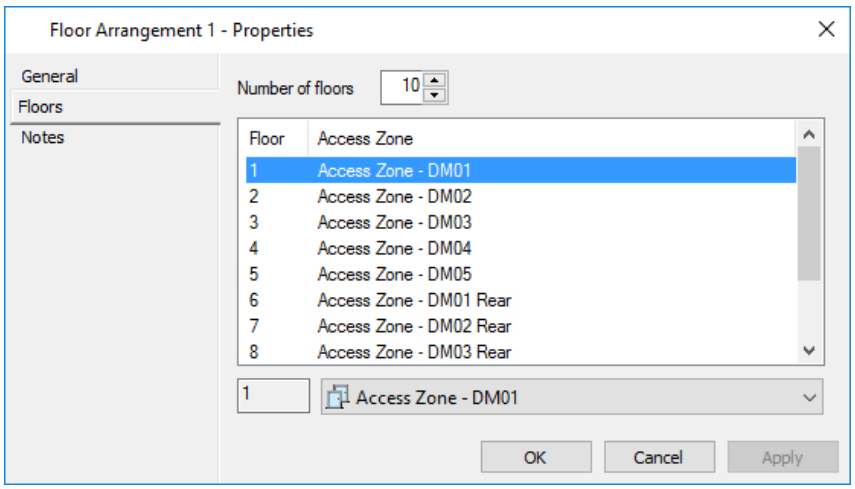
Notes:

- If you do not select an Access Zone for a Floor, this means the associated floor is in free access mode.
- To configure rear doors for elevator cars that have front and rear doors that lead to different Access Zones, refer to "Rear doors" below.

Rear doors

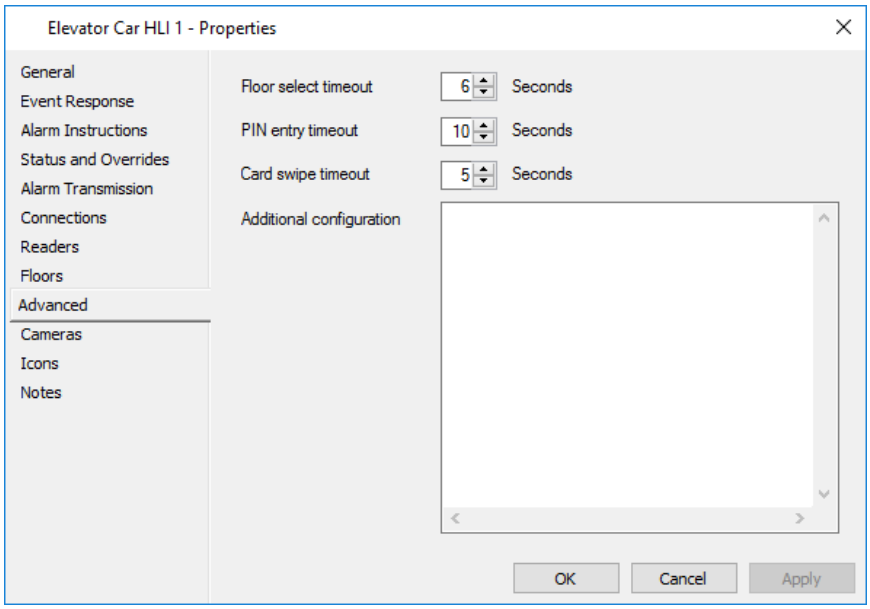
The Otis Compass and Kone ELI elevator system integrations currently support rear doors on elevator cars. If you are not using one of these integrations, ignore the following.

You can manage access to both front and rear elevator doors. In the floor arrangement, you must create double the amount of floors specified in elevator HLI configuration. For instance, if you have 4 floors, in the floor arrangement, you would need to configure 8 floors (4 for front and 4 for rear). In the floor arrangement, the fifth floor represents the first floor's rear door and the sixth floor is the second floor's rear door and so on. If you have a floor that only has one door (either a front or rear door), you still need to configure two floors for it (one with access and the other without access). Ten Floors and Access Zones are configured below, to represent five physical floors with front and rear doors:



You also need to refer to ***Troubleshooting - Supported elevator systems*** (on page 23-30) for integration-specific rear door configuration (e.g. configuration specific to Otis Compass).

15. Click the **Advanced** tab.



16. Change the Advanced Settings as required.

Option	Meaning
Floor select timeout	Time from when floor select buttons are enabled in an elevator car, following a cardholder being granted access at the elevator car reader, to when the floor select buttons are returned to the default access state.
PIN entry timeout	Maximum time allowed for a cardholder to enter their PIN. Measured from card badge. If PINs functionality is allowed in the elevator cars, this timeout should be set to as long as possible and preferably the same length of time as the “Floor select timeout” to avoid confusion.
Card swipe timeout	Maximum time allowed between card swipes when performing a double-card override or between pressing a function key on a keypad reader then swiping a card. Configure this timeout if the elevator car will support local overrides by either of these methods.
Additional configuration	An optional field used if you are configuring this Elevator Car HLI for a Kone DOP terminal (outside an elevator). When this field contains the string `SendDenial=1`, the Gallagher Controller will also inform Kone controllers when access is denied at this DOP's readers.

17. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Elevator Car HLI.
    For further details see ***Cameras tab*** (on page 3-24).
18. Click the **Icons** tab if you want to change the Icon Set for this Elevator Car HLI.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
19. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Elevator Car HLI.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
20. Click the **Notes** tab if you want to add a note(s) about this Elevator Car HLI.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
21. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

An Elevator Car HLI is configured and assigned to an Elevator HLI. The Controller that supports the Elevator HLI will begin polling the elevator system.

Hints

Each combination of an Elevator HLI, Group number and Car number must be unique. If they are not you will not be able to save the new Elevator Car HLI.

Editing and Deleting Elevator Car HLIs
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Elevator Car HLIs.

Copying an Elevator Car

Introduction

This procedure enables an operator with the "Edit Site" privileges to create a new elevator car that is a copy of an existing elevator car. Use this procedure when you are creating a new elevator car that provides the same access to floors as an existing elevator car. For example, you could use this procedure when creating an Elevator Car HLI that is part of the same group as an existing Elevator Car HLI.

Note: You can copy either standard elevator cars or high level interface elevator cars using this procedure.

Procedure

1. Click **Configure** from the menu bar, then **Elevator Cars**.
   The **Elevator Car** List Window opens (in grid view).
2. **Right click** on the elevator car you want to copy and select **Duplicate**.
3. A new elevator car is created.

If you copied	Refer to ....
a standard elevator c	***Configuring Elevator Cars*** (on page 23-2). All elevator car properties are copied except the Reade Inputs and Outputs, which will be different for each elevator car. Enter the Reader, and the Outputs and Inputs for each floor. Change the Name and amend other properties if necessary.
an Elevator Car HLI	***Configuring an Elevator Car HLI*** (on page 23-21). All elevator car properties are copied except the Reade which will be different for each elevator car. Enter the Reader and change the Name, Group number and Car number. Amend other properties if necessary.

4. 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 elevator car is created with selected properties copied from an existing elevator car. The Controller that supports the Elevator HLI will begin polling the elevator system.

Performing executive overrides

Introduction

This procedure enables an operator with the "Overrides" privilege to send individual lift cars to selected floors by performing an executive override.

Notes:

- This procedure can only be performed on **Schindler** and **Otis Modbus** lift systems.
- The operator is required to select an Access Zone (floor) to send the elevator car to. Ensure the operator is assigned the correct operator privileges in order to view all Access Zones.

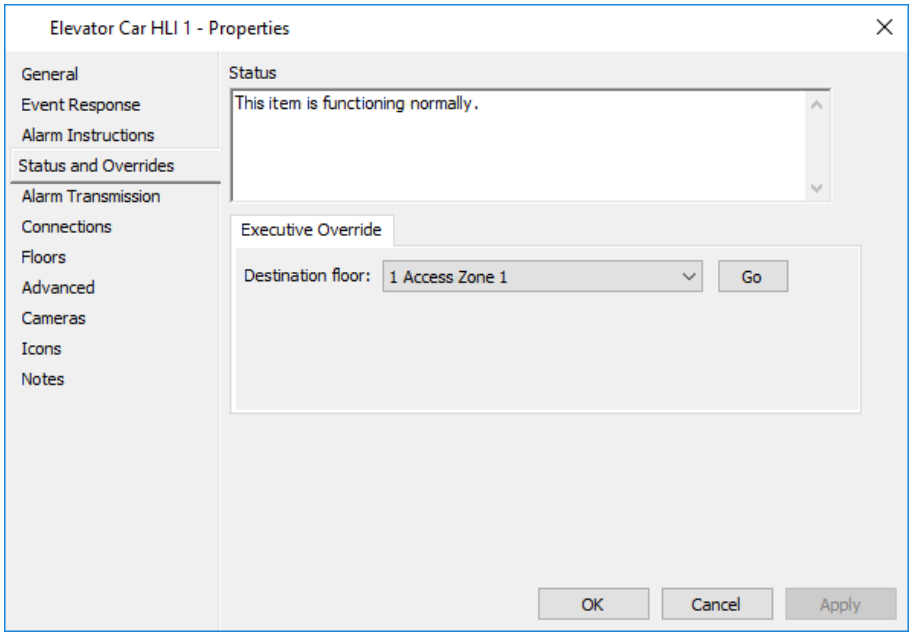
There are two methods for performing executive overrides:

- using the Properties window, or
- using the Context menu

Procedure

Using the Properties window

1. Click **Configure** from the menu bar, then **Elevator Cars**.
   The **Elevator Car** List Window opens (in grid view).
2. **Right click** on the required elevator car and select **Properties**.
3. Click the **Status and Overrides** tab.

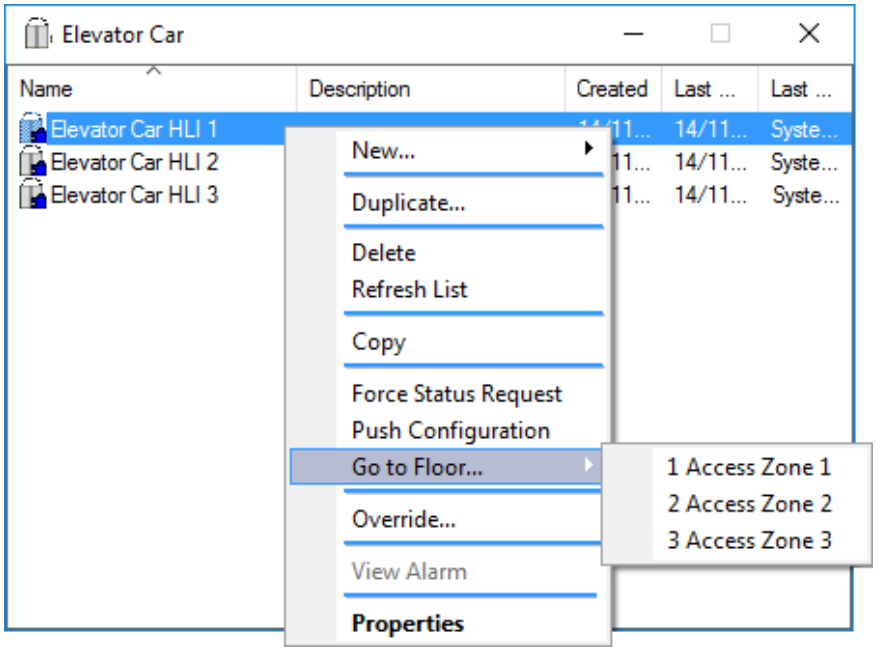


4. Select the appropriate **Destination floor** from the drop-down list.
   Note: If an Access Zone has not been assigned to a floor, this means the floor is free access, (i.e. anyone can access this floor). See ***Configuring an Elevator Car HLI*** (on page 23-21) for the procedure.

5. Click the **Go** button to send the Elevator Car HLI to the selected floor.
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.

Using the Context menu

1. Click **Configure** from the menu bar, then **Elevator Cars**.
   The **Elevator Car** List Window opens (in grid view).
2. **Right click** on the required Elevator Car HLI and select **Go to Floor...**



3. Select the appropriate **Destination floor** from the context menu.
   The Elevator Car HLI will be sent to the selected floor.

   Note: Alternatively, you can select **Override...** from the context menu to display the **Status and Overrides** tab of the selected Elevator Car HLIs property pages.

Result

When an override is requested, the elevator car will be sent to the requested floor, (e.g. Floor 5). This is dependent on the HLI protocol used, for example: If the car has already been sent to a floor, the car will travel there before travelling to the requested floor, (e.g. Floor 3 then on to Floor 5).

Supported elevator systems – Additional Configuration and Troubleshooting

This topic describes the additional configuration options and any limitations for the elevator systems supported by Command Centre.

Note: Additional elevator systems are provided as licensed customisations of Command Centre. For a list of all Elevator HLI customisations, contact Gallagher Security Technical Support.

Otis Compass

The Otis Compass Destination Management System integrates with Command Centre via the Otis Compass Plus protocol.

The following parameters can be entered in the **Additional configuration** field (on the **Advanced** tab of the Elevator HLI):

Parameter	Description
ip=nnn.nnn.nnn.nnn	This is the IP address of the 'FT Otis Compass HLI Service' PC **as seen from the Gallagher Controller**. The default is 192.168.50.250, but will be different if the Controller is not on the same subnet as the Otis hardware.
port=nnnn	Where *nnnn* is the destination TCP port the Elevator HLI sends data to (defaults to 9898). If this parameter is changed, you will need to ensure this parameter is also changed in the 'FT Otis Compass HLI Service' configuration 'OtisCompassHli.conf' file.
poll_due_timeout=nn	Where *nn* is the time interval between two default access mask polls or heartbeat during idle time (defaults to 15 seconds).
floor_offset=nn	Where *nn* is a number between -127 and 127 that will set the lowest floor of the Gallagher elevator cars to the lowest floor of the Otis Compass installation (defaults to 0). 127 negative floors, 1 ground floor, and 127 positive floors, which provides a sum of 255 floors.
reverse_csn=n	Where *n* is either 0 or 1. The default is 1 which reverses the CSN. Command Centre uses the reversed CSN for its card numbers. This value need only be set to 0 if using a 32 or 56 bit Wiegand format.
first_rear_floor=n	Where *n* is the first rear door floor configured in the Floor Arrangement/Elevator Car HLI. Valid range is 1 to 128 (for supporting up to 127 building floors with both front and rear doors). If n is valid, then floors before n are front door floors; floors at and above n are rear door floors.

Parameter	Description
enable_periodic_update=n	Where *n* is either 0 or 1. The default is 0, meaning a heartbeat poll is sent from the Gallagher Controller to the 'Otis Compass HLI Service' as specified by the poll_due_ timeout configuration parameter. If the value is set to 1, an access mask for all Elevator Car HLIs (DECs) is sent periodically from the Gallagher Controller to the 'Otis Compass HLI Service' as specified by the *poll_due_timeout* configuration parameter. The default heartbeat messaging method is multicast. You can change to unicast heartbeat messaging by editing the 'OtisCompassHli.conf' file***** stored in *C:\Program Files (x86)\Gallagher\Gallagher OTIS Compass High Level Integration\Otis Compass Service*, and changing the **<UseMulticastForHeartbeat>** number value. **1** = multicast, **0** = unicast.
max_session=nnnnnnn	Where *n* is the maximum TCP session time in seconds. Default is 31536000 seconds (365 days). When the session expires, messages from the 'FT Otis Compass HLI Service' will be rejected.
op_mode=*n*	Where *n* is the basic operational mode. Valid range 1-4. Default operational mode is 3. Only operational modes 1 or 4 support the Default Floor functionality. Individual Elevator Car HLIs can be configured with their own operational mode.

For example:
The following example shows the format to be used: *ip=192.168.50.250; port=9898; poll_due_timeout=15; floor_offset=0; reverse_csn=1; first_rear_floor=5; enable_periodic_update=0; max_session=31536000; op_mode=1*

*** Configuration file:** To create the 'OtisCompassHli.conf' file in *C:\Program Files (x86)\Gallagher\Gallagher OTIS Compass High Level Integration\Otis Compass Service*, copy and paste the 'OtisCompassHli.conf.sample' file and rename it to 'OtisCompassHli.conf'.

Notes:

- By default with no floor offset, (i.e. *floor_offset=0*) then Floor '1' in Command Centre refers to Floor '0' in Otis.
- If a floor offset has been configured, (i.e. *floor_offset=1*) then Floor '1' in Command Centre refers to Floor '1' in Otis.

Logging

The Otis Compass integration log files (OtisCompassHliService.log) are located in *C:\ProgramData\Gallagher\Command Centre\OtisCompass*.

To enable more detailed logging (e.g. when debugging an issue), edit the 'OtisCompassHliService.exe.config' file stored in *C:\Program Files (x86)\Gallagher\Gallagher OTIS Compass High Level Integration\Otis Compass Service*, and set the **minlevel** to **"Trace"**. For example:
<logger name="*" minlevel="Trace" writeTo="OtisCompassHliServiceLog" />
After changing the **minlevel**, you must restart the 'FT Otis Compass HLI Service' service for the change to take effect.

Kone

The Kone Elevator HLI integration supports the Kone Protocol v2.5

The following parameter can be entered in the **Additional configuration** field (on the **Advanced** tab of the Elevator HLI):

Parameter	Description
baud=9600	For Kone Protocol v2.5 to communicate at 9600 baud, enter the parameter as shown. Perform a 'Reset' override on the Controller used to host this Elevator HLI for the change to take effect. Appropriate values 1200 and 9600.
parity=n	Specify the parity to be used by entering "parity=n" where 'n' is one of: N = No parity O = Odd parity E = Even parity M = Mark parity S = Space parity
poll_due_timeout=nnn	This is the time (in seconds) between sending the default access masks for each floor. Default = 15. Appropriate values are between 15 and 900.
retry_timeout=nnn	This is the time (in milliseconds) between retrying a message that has not had a response from the Kone elevator system.
log_raw_data=1	This is used to log outgoing and incoming packets in hexadecimal format.
raise_debug_event=n	This is used to raise additional debugging alarms (where *n* is a number indicating the debugging level).

For example:
The following example shows the format to be used: *baud =9600; parity =O*

Notes:

- The Kone protocol requires that all Elevator Car HLIs in a group must be configured in Command Centre with the same number of floors as the Elevator Car HLI that has the most floors. The additional floors for each Elevator Car HLI should either be left with no Access Zone assigned, or with a default Access Zone that no one has access to, depending on the level of security.
- Should a Kone Group Controller be replaced or reset to factory defaults, the connection between the Gallagher and Kone systems must be re-initiated via a restart of the Controller hosting the Kone Elevator HLI.
- On a Kone Elevator Car HLI, groups are numbered 1-8 and the elevator cars associated with each group are numbered 1-8. Each unique group and car number combination identifies a particular elevator car

Otis

The following parameter can be entered in the **Additional configuration** field (on the **Advanced** tab of the Elevator HLI):

Parameter	Description
poll_due_timeout=nnn	This is the time (in seconds) between sending the default access masks for each floor. Default = 15. Appropriate values are between 15 and 900.
retry_timeout=nnn	This is the time (in milliseconds) between retrying a message that has not had a response from the Otis elevator system.
log_raw_data=1	This is used to log outgoing and incoming packets in hexadecimal format.
raise_debug_event=n	This is used to raise additional debugging alarms (where *n* is a number indicating the debugging level).

For example:
The following example shows the format to be used:
poll_due_timeout=15; log_raw_data=1

Note: The Otis protocol requires that all Elevator Car HLIs in a group must be configured in Command Centre with the same number of floors as the Elevator Car HLI that has the most floors. The additional floors for each Elevator Car HLI should either be left with no Access Zone assigned, or with a default Access Zone that no one has access to, depending on the level of security.

ThyssenKrupp

Note: The recommended method of configuring ThyssenKrupp is via the ThyssenKrupp integration. See ***ThyssenKrupp Elevator Systems*** (on page 77-1) for further detail.

A Gallagher reader is located near each ThyssenKrupp Destination Selection Control (DSC) terminal. When a Cardholder presents their card at the reader, Command Centre instructs the ThyssenKrupp elevator system which levels the Cardholder has access to. The Cardholder then selects a destination limited to those floors.

The following parameters can be entered in the **Additional configuration** field (on the **Advanced** tab of the Elevator HLI):

Parameter	Description
poll_due_timeout=nnn	This is the time (in seconds) between sending the default access masks for each floor. (Default = 15. Appropriate values are between 15 and 900.)

Parameter	Description
retry_timeout=nnn	This is the time (in milliseconds) between retrying a message that has not had a response from the ThyssenKrupp elevator system.
log_raw_data=1	This is used to log outgoing and incoming packets in hexadecimal format.
raise_debug_event=n	This is used to raise additional debugging alarms (where *n* is a number indicating the debugging level).
firmware_reports_dest =n	Disabled = 0. Enabled = 1. If you have the string 'ThyssenKruppHLI=1' in your licence file, floor destination reporting is enabled by default. If your ThyssenKrupp firmware does not support destination reporting and you have installed this feature, enter “firmware_reports_dest=0” to disable floor destination reporting. Command Centre will log an access granted event to the first floor regardless of which floor is selected, and whether a floor is selected or not.
Floor_offset=n	Default = 0. Range 0-32. By default the destination floor 0 reported by ThyssenKrupp will correspond to the first floor configured in Command Centre.
Broadcast_default_ masks=n	To turn on access masks to all terminals, add “broadcast_default_masks=1”. To leave this capability off, the parameter can have a value of 0 or be omitted from the string.

For example:
The following example shows the format to be used:
poll_due_timeout=15; log_raw_data=1

Limitations

- The ThyssenKrupp Elevator HLI integration supports up to 32 floors only.
- The ThyssenKrupp Elevator HLI integration does not support the use of a rear door in an elevator car.
- If an individual elevator car is offline, an offline message is not generated in Command Centre. Hence it is unknown which elevator car is currently offline. The operator will need to physically observe the status of the ThyssenKrupp elevator system to see which elevator car is currently offline.
- Destination Reporting is supported for up to 32 floors only.

Notes:

- A Command Centre operator will need to configure an Elevator Car HLI for each ThyssenKrupp DSC terminal.
- On a ThyssenKrupp Elevator Car HLI, the Group number is the ThyssenKrupp Destination Selection Control terminal number. The terminals are numbered from 1-94. The Car number is the associated ThyssenKrupp lift number. Lifts 1-63 are addressable.

Schindler

The following parameters can be entered in the **Additional configuration** field (on the **Advanced** tab of the Elevator HLI):

Parameter	Description
poll_due_timeout=nnn	This is the time (in seconds) between sending the default access masks for each floor. Default = 15. Appropriate values are between 15 and 900.
retry_timeout=nnn	This is the time (in milliseconds) between retrying a message that has not had a response from the Schindler elevator system.
log_raw_data=1	This is used to log outgoing and incoming packets in hexadecimal format.
raise_debug_event=n	This is used to raise additional debugging alarms (where *n* is a number indicating the debugging level).

For example:
The following example shows the format to be used:
poll_due_timeout=15; log_raw_data=1

Limitation: The Schindler lift control box supports up to 64 floors.

Note: The Elevator HLI only supports one Elevator Car HLI. The Car number must be 1, the Group number is ignored.

Otis Modbus

The following parameters can be entered in the **Additional configuration** field (on the **Advanced** tab of the Elevator HLI):

Parameter	Description
poll_due_timeout=nnn	This is the time (in seconds) between sending the default access masks for each floor. Default = 15. Appropriate values are between 15 and 900. This number should be set to: • less than the maximum temporary floor button enabled time the Otis lift control box can be configured. • more than the **Floor select timeout** (as configured on the **Advanced** tab of the Elevator Car HLI), otherwise Command Centre may have problems logging Cardholders floor selections.
retry_timeout=nnn	This is the time (in milliseconds) between retrying a message that has not had a response from the Otis Modbus elevator system.
cttl_start_addr=nnnnn	The first address of the CTTL discrete input is set to 10009.
log_raw_data=1	This is used to log outgoing and incoming packets in hexadecimal format.
raise_debug_event=n	This is used to raise additional debugging alarms (where *n* is a number indicating the debugging level).

For example:
The following example shows the format to be used:
poll_due_timeout=15; log_raw_data=1

Limitations

- The Otis Modbus lift control box supports up to 36 floors.
- If an individual elevator car is offline, an offline message is not generated in Command Centre. Hence it is unknown which elevator car is currently offline. The operator will need to physically observe the status of the Otis Modbus elevator system to see which elevator car is currently offline.
- If multiple Elevator Car HLIs are attached to the same Elevator HLI and some of the cars are offline, the other cars will still function as expected, (e.g. Cardholders can badge cards and select floors, and operators can perform overrides). However, there is no guarantee that the override will reach the Otis Modbus lift control box. If this occurs, re-send the override.

- On an Otis Modbus Elevator Car HLI, Group number and Car number must be configured as the same number as the child device ID of the Otis Modbus lift control box. Valid numbers are from 1-247.

Kone ELI

The Kone ELI Elevator HLI feature has been implemented according to "Group Controller Access Control Interface Specification" document, Rev 1.8, provided by Kone.

The Kone ELI Elevator HLI feature supports Kone DOPs (Destination Operation Panels) on some floors as well as COPs (Car Operation Panels inside the elevators), with a Gallagher reader positioned at each DOP or COP. When a Cardholder presents their card at the reader, Command Centre instructs the Kone system which levels the Cardholder has access to. The Cardholder can then select a destination limited to those floors. If the Cardholder is using a DOP, the DOP then instructs the Cardholder on which elevator car to use, alleviating the need for floor selection within the elevator car itself.

Warning: If a Cardholder presents a card at a reader associated to a Kone terminal (DOP or COP) and then walks away without selecting a floor, another user may select a floor based upon that Cardholder's access privileges until the configured floor selection timeout is reached. If any Cardholder attempts to present another card during this time, their card read will be ignored. Any floor selection made will be subject to the first Cardholder's access privileges. The floor selection will be reported as belonging to the first Cardholder.

The following parameters can be entered in the **Additional configuration** field (on the **Advanced** tab of the Elevator HLI):

Parameter	Description
Ip	Provide the IP address of the Kone Group Controller. **Note:** This parameter is overridden if any controllers are specified as [KCEGC] parameters.
Port	Provide the IP port of the Kone Group Controller. **Note:** This parameter is overridden if any controllers are specified as [KCEGC] parameters.
BackupIp	Provide the IP address of the backup Kone Group Controller. **Note:** This parameter is overridden if any controllers are specified as [KCEGC] parameters.
BackupPort	Provide the port of the backup Kone Group Controller. **Note:** This parameter is overridden if any controllers are specified as [KCEGC] parameters.

Parameter	Description
Floors	Provide the number of floors configured for the building. (This will be used to create global default access masks.)
Poll	Provide the time between sending the default access masks (in seconds). If the value is not included then the default of 20 seconds will be used.
PollLimit	Provide the number of default access masks that this Gallagher Controller will have in transit with the Kone Group Controller.
FloorSelectTimeout	Used to notify Kone of the amount of time that a DOP will be open for a Cardholder to select a floor (in seconds). If the value is not included then the Kone Group Controller value will be used. If this value is set, then the Floor select timeout on the **Advanced** tab of each Elevator Car HLI should be set to this value plus a bit extra to allow for network delay.
DisconnectedState	Used to notify Kone of what it should do if the connection between the Gallagher Controller and the Kone Group Controller is lost. Options are: Same, Free or Secure. **Same:** The current free floors remain free, other floors will be inaccessible. **Free:** Anyone can travel from any floor to any floor using an elevator. **Secure:** All floors will be inaccessible. If the value is not included then the default "Same" will be used. If this setting is changed the Controller must be re-started for the new Disconnected State to take effect.
poll_due_timeout=nnn	This is the time (in seconds) between sending the default access masks for each floor. Default = 15. Appropriate values are between 15 and 900.
retry_timeout=nnn	This is the time (in milliseconds) between retrying a message that has not had a response from the Kone elevator system.
log_raw_data=1	This is used to log outgoing and incoming packets in hexadecimal format.
raise_debug_event=n	This is used to raise additional debugging alarms (where *n* is a number indicating the debugging level).

Parameter	Description
GlobalDefaultAccessMaskOption=<operating panels>	This is used to set the default access mask. Options are COPsOnly, DOPsOnly, or both. If it is set to COPsOnly, only COP_GLOBAL_DEFAULT_MASK messages will be sent. If it is set to DOPsOnly, only DOP_GLOBAL_DEFAULT_MASK messages will be sent. If it is set to both (or if it is not included or set), both COP_GLOBAL_DEFAULT_MASK and DOP_GLOBAL_DEFAULT_MASK messages will be sent.
Kone Control & Electrification Group Controller parameters	
Address	Provide the IP address and port number of each Kone Control & Electrification Group Controller (KCEGC). You do not need to specify which are primary and which are backup controllers. Type an IP address, followed by a colon (:), then the port number. Separate listed controllers with a line break (no semicolon). A maximum of five KCEGCs can be listed. **Note:** Controllers specified here override any controllers specified by the Ip, Port, BackupIp, and BackupPort parameters mentioned above. If controllers are listed as [KCEGC] paramters, those other specified controllers are ignored.
Call Type parameters	
[CALL_nnn]	Used to specify the call type number. The call type number can be between 0-200. The word 'CALL' must be capitalized.
Name	Used to specify the name of the Call Type. The names provided here will be displayed under the Call Type column in the Cardholder Kone ELI properties tile.
Lifts	Used to specify the lifts that will be used for a Call Type. **Notes:** • Any lifts specified here that do not exist in the Kone ELI system, the lifts will be ignored and the available lifts will be used for the Call Type. • The maximum number of lifts you can specify for Call Type is eight. • Each value entered for a lift must be >=1.

Parameter	Description
Gallagher Advanced Global Default Mask parameters	
DOP_GDM_C	DOP Global Default Mask (Connected)
DOP_GDM_D	DOP Global Default Mask (Disconnected)
COP_GDM_C	COP Global Default Mask (Connected)
COP_GDM_D	COP Global Default Mask (Disconnected)
DOP_SDM_C	DOP Specific Default Mask (Connected)
DOP_SDM_D	DOP Specific Default Mask (Disconnected)
COP_SDM_C	COP Specific Default Mask (Connected)
COP_SDM_D	COP Specific Default Mask (Disconnected)
DOP_GDM_DEL	DOP Global Default Mask delete
COP_GDM_DEL	COP Global Default Mask delete
DOP_SDM_DEL	DOP Specific Default Mask delete
COP_SDM_DEL	COP Specific Default Mask delete
GDM_ONLY_OPS	Specifies Operation Panels (OPs) that only use GDM.
DD	Destination Default (Secure or Free). By default, it is set to 'Secure or Locked' (S).
DE	Destination Exceptions (destination floors that are configured differently compared to the DD mask configuration).
GN	Group Number. Numbers 1-100 represent a COP, numbers higher than 100 represent a DOP.
CN	Car Number
SD	Source Default (open or locked)
SE	Source Exceptions (source floors that are configured differently compared to the SD configuration).
S	Secure or Locked. 'S' is the default for DD.
F	Free or Open. 'F' is the default for SD.
n,m,…	Floor numbers. Index starts from 1 and corresponds to the floor in your Floor Arrangement in the Command Centre. If you have rear floor(s), in the Floor arrangement, you need to create double the number of floors specified in elevator HLI configuration. For instance, if you have 4 floors, in the Floor Arrangement, you need to configure 8 floors (front and rear). In the Floor Arrangement, the

Parameter	Description
	fifth floor represents the first floor's rear door and the sixth floor is the second floor's rear door and so on.
SendMessage	Sends a single specific mask message to Kone Group Controller

For example:

- The following example shows the format to be used:
```
Ip=192.168.1.1; Port=2005; BackupIp=192.168.1.2;
BackupPort=2005; Floors=40; Poll=36000; PollLimit=10;
FloorSelectTimeout=5; DisconnectedState=Free
```
- The following example shows the parameters used to specify one primary and two backup Kone Control & Electrification Group Controllers (KCEGCs):
```
[KCEGC]
Address=192.168.1.1:2005
Address=192.168.1.2:2005
Address=192.168.1.3:2005
```
- The following example shows the parameters used to create a Call Type:
```
[CALL_0]
name= Priority
lifts=1,2,3,4
```
- The Following example shows some of the Gallagher Advanced Global Default Mask parameters used for configuration:
```
[Gallagher]
DOP_GDM_C=DD=S; DE=5,25; SD=S;
DOP_GDM_D=DD=F; SD=F;
COP_GDM_C=DD=S; DE=5,25;
```

Configuration	Explanation
DOP_GDM_C=DD=S; DE=5,25; SD=S;	DOP Global Default Mask connected state is set to Destination Default (secure or locked). Destination Exception mask applies to floors 5 and 25. Source Default floors are set to secure or Locked.
DOP_GDM_D=DD=F; SD=F;	DOP Global Default Mask disconnected state is to Destination Default (free). Source Default floors are set to free or open.
COP_GDM_C=DD=S; DE=5,25;	COP Global Default Mask connected state is set to Destination Default (secure or locked), Destination Exception mask applies to floors 5 and 25.
COP_GDM_D=DD=F;	COP Global Default Mask disconnected state is set to Destination Default (free or open).
COP_SDM_D=DD=F;	COP Specific Default Mask disconnected state is set to Destination Default (free or open).

Configuration	Explanation
DOP_SDM_D=DD=F;	DOP Specific Default Mask disconnected state is set to Destination Default (free or open).
GDM_ONLY_OPS= (101,1),(105,1), (111,1),(1,1)	Operation Panels that are using only Global Default Mask are DOP1, DOP 2, DOP 3 and COP 1. The second value following a comma is the Car number (i.e. (101,1) means: DOP 1, Car 1).

Configuration example

```
Floors=20; Ip=192.89.159.2; Port=2005;
BackupIp=192.89.159.3; BackupPort=2005;
Poll=36000;FloorSelectTimeout=5;
DisconnectedState=Free;

[KCEGC]
Address=192.168.1.1:2005
Address=192.168.1.2:2005
Address=192.168.1.3:2005

[CALL_0]
name = Normal Call
lifts = 1,2,3

[CALL_1]
name = Handicapped call
lifts = 1,2

[CALL_2]
name = Priority call
lifts = 1,5,7

[CALL_3]
name = Empty car call
lifts = 1,2

[CALL_4]
name = Space allocation call
lifts = 3,4,5

[Gallagher]
DOP_GDM_C=DD=S; DE=5,25; SD=S;
DOP_GDM_D=DD=F; SD=F;
COP_GDM_C=DD=S; DE=5,25;
COP_GDM_D=DD=F;
COP_SDM_D=DD=F;
DOP_SDM_D=DD=F;
GDM_ONLY_OPS=(101,1),(105,1),(111,1),(1,1)
```

Notes:

- The Ip, Port, BackupIp, and BackupPort parameters would not be specified as well as [KCEGC] parameters in a real configuration. The [KCEGC] parameters override the Ip, Port, BackupIP, and BackupPort parameters.
- One Elevator Car HLI needs to be created per DOP or COP.
- If using a KIC leave the *BackupIp* field as 0.0.0.0 Kone default port is 2005.

- When configuring multiple Elevator Car HLIs, the configured (hosting) Elevator HLI should be removed from the Controller as each update of an Elevator Car HLI will queue multiple messages for the Elevator HLI. Once all Elevator Car HLIs are configured then the ELI can be reattached to the Controller and a smaller subset of configuration will be sent.
- When configuring the Group number, make sure that all the terminals belonging to one group are of the same type, (i.e. either they are all DOPs, or they are all COPs. Mixed groups are not currently possible).

If configuring...	then...
COPs	configure the Group number to match the Kone Grou ID, and the Car number to match the Kone Elevator ID
DOPs	• configure the Group number to match the Kone DOP floor ID, plus an offset of 100. Make sure it matches the actual DOP configuration. See Example next. All DOPs on the same floor are in the same group. • configure the Car number to match the Kone DOP ID. Each DOP on a floor has a unique identifier.

Example:

	COPs	DOPs
Kone	Elevator ID 1	DOP ID 1
	Group ID 1	DOP Floor ID 1
Gallagher	Car number 1	Car number 1
	Group number 1	Group number 101

- When configuring a DOP, you can configure access denied messages to be sent to the Kone system, by entering the following string in the **Additional configuration** field on the **Advanced** tab of that DOP's Elevator Car HLI:
  `SendDenial= 1`

Initialisation

To initialise the connection between each Elevator HLI and Kone, perform the following procedure:

1. Change the poll value in the Additional configuration string, located within the Advanced tab of each Elevator HLI to '300', (e.g. Poll=300).
2. Wait for the Elevator HLI's to show that they are online.

3. Change the poll value in the Additional configuration string, located within the Advanced tab of each Elevator HLI to '36000', (e.g. Poll=36000) or an appropriate figure for your site.

Troubleshooting

- There may be a period during schedule changes and polling where there may be a delay in Cardholder badging messages being passed to Kone and the floor selections being returned to Command Centre. This usually has no effect on a Cardholders usage of the system but can affect the destination reporting during that time.
- After the first badge, any bad replies from terminals may indicate poor configuration of the panel (on Kone side) or poor Gallagher reader hardware installation.
- In a Polaris hybrid configuration (that implements both DOPs and COPs) COPs will not be active when the elevator reaches a floor that uses DOPs for destination control.
- If a DOP does not receive a Specific Mask (the default access for the DOP) during a schedule change, then the only way to send this message is going to be:
  - the next schedule change,
  - a poll, or
  - by an operator performing an Access Zone Override, for one of the floors serviced by the DOP in question.
- If you are experiencing problems during schedule change or during polling then the Poll Limit can be altered:

  A large number means the mask messages will be sent faster, however this places more load on the HLI Controller and Cardholder Mask messages may be lost.

  A small number means that it will take longer to send all mask messages, however there will be more bandwidth available for the Cardholder Mask messages. An unwelcome side effect is that if the configured amount of mask messages are waiting for replies that are not returning then no other mask messages will be sent until those messages expire (Specific Mask messages only - Cardholder messages are still sent).
- Should a Kone Group Controller be replaced or reset to factory defaults, the connection between the Gallagher and Kone systems must be re-initiated via a restart of the Controller hosting the HLI/ELI.
- This feature was not designed for multi-server. Although it may work, it will leave pending changes for the Floor Arrangement item.

Chapter 24: External Systems

Introduction

Gallagher Command Centre uses the bi-directional Gallagher FTCAPI Middleware Framework to communicate with multiple third party systems concurrently. Third party system examples are: DVR systems, intercom systems, security sub-systems, alarm monitoring systems, key cabinets and elevator systems.

Such integrations require an FTCAPI middleware plug-in to be developed in order to conduct the protocol conversions between Command Centre and the third party system.

Integrations

Gallagher has developed an FTCAPI middleware plug-in for each of the following third party systems:

- ASCII Text Interface
- Incoming ASCII Interface
- Senstar Stellar Interface
- SNMP v1 Interface
- Bosch Security Escort Interface
- DVR DigiOp HLI Interface
- KeySecure System Interface
- Kone RCGIF plug-in
- SchindlerID Interface
- Ademco 685 FTCAPI plug-in

For details on a particular interface and configuration instructions, refer to the appropriate release note in the `'Utilities\System Interfaces'` folder of the Gallagher Installation files.

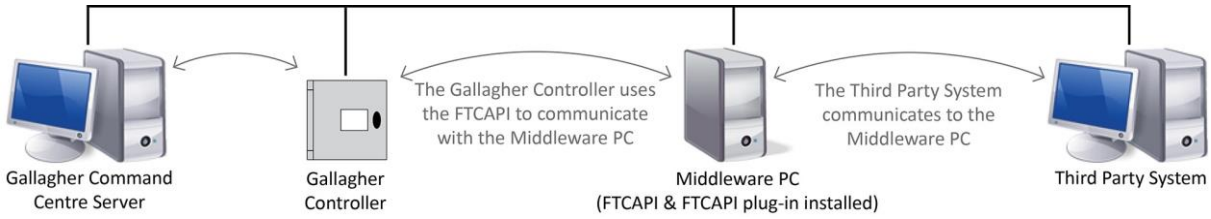
Note: Each third party system (integration) requires an entry in the [Plugin] section of your Command Centre license file (Command Centre.lic).

Gallagher has also developed FTCAPI middleware plug-ins for other third party systems, (e.g. DVR integrations). These integrations are provided as licensed customisations of Command Centre. For a list of customisations that use FTCAPI middleware plug-ins, contact Gallagher Security Technical Support.

The FTCAPI Middleware Framework

The FTCAPI allows for the following functionality:

- communication of events and status from external systems to Command Centre;
- command strings triggered by internal or external events to be transmitted from Command Centre to an external system; and
- status change messages from external systems to change the state of outputs.



Notes:

- The FTCAPI has the ability for card events (those submitted via logCardEvent API method) to be used for the purpose of access in Command Centre.
- An External System Item or DVR Camera can be assigned anywhere in Command Centre where a reader may be assigned (other than in the **Delay** and **Alarm Warnings** tabs for an Alarm Zone), i.e. on a Door or an Elevator Car. Thus, the ESI/DVR Camera takes on the general function of a reader in the system.
- The FTCAPI will not function using Gallagher UltraSec Controllers.

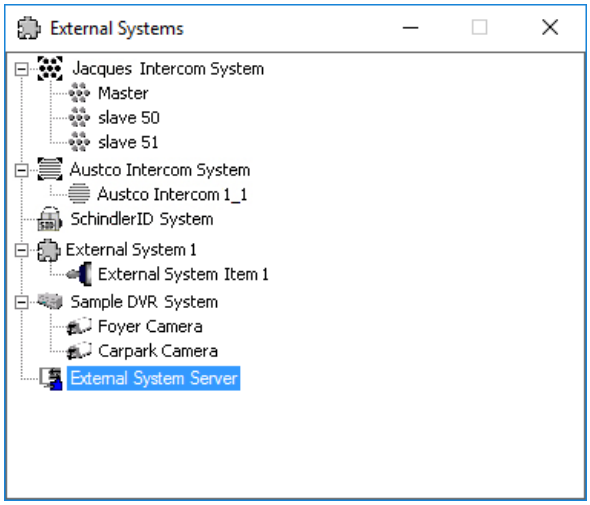
The External System List Window

Introduction

The **External Systems** List Window allows the following external systems, and associated children to be created.

System type	Child	Purpose
DVR System	DVR Camera	DVR Interface
Intercom System	Intercom	Jacques Intercom Interface
External System	External System Item	FTCAPI functionality
Austco Intercom System	Austco Intercom	Austco Intercom Interface
SchindlerID System		Schindler Cardholder Management Interface
Commend Intercom System	Commend Intercom Item	Commend Intercom Interface

The **External Systems** List Window displays in tree view showing all external system(s), set up in your system.
By expanding the tree, the children of each system can also be displayed and edited, and in the case of DVR, 'live footage' viewed.



In this example, there are two DVR Cameras that belong to the 'Sample DVR System', three Intercoms that belong to the 'Jacques Intercom System', one External System Item that belongs to the 'Sample External System', one Austco Intercom that belongs to the 'Austco Intercom System' and a 'SchindlerID System'.

Note: At most, 100 External System Items can be assigned to an External System. However, you can configure multiple External Systems that are the same. To configure an External System that is the "same as" another External System, refer to Step 8 in the topic ***Configuring an External System*** (on page 24-8).

Configuration

To configure your external system, refer to the appropriate procedure below:

- ***Configuring an External System Server*** (on page 24-5)
- ***Configuring an External System*** (on page 24-8)
- ***Configuring a DVR System*** (on page 24-14)
- ***Configuring FTCAPI Trigger Strings and Reflected Outputs*** (on page24-22)
- ***Configuring a SchindlerID System*** (on page 24-26)
- ***Adding external systems to a Site Plan*** (on page 24-69)

Configuring an External System Server

Introduction

The normal setup procedure of an External System Server is to:

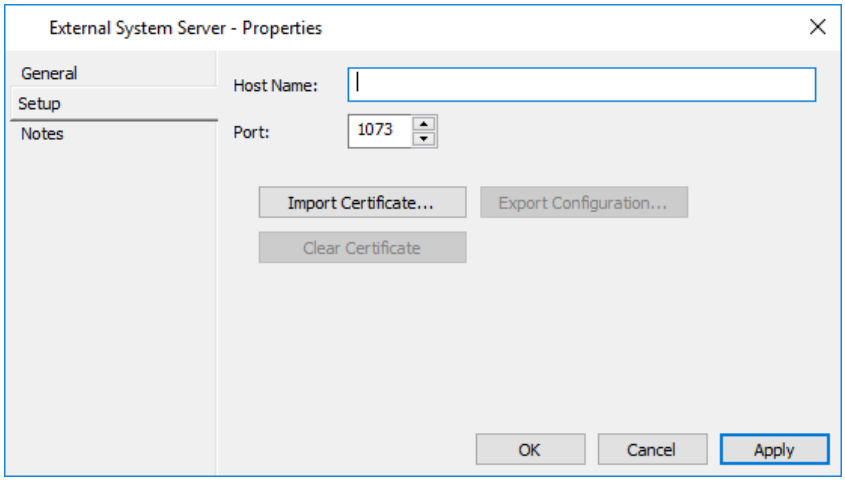
1. Install FTCAPI Middleware Framework to create keys. See ***Installing the FTCAPI Middleware Framework (FMF)*** (on page 24-7) for detailed instructions.
2. Import the **GallagherFTCAPI.pem** certificate into Command Centre via the External System Server's **Setup** tab.
3. Export the **GallagherFTCAPI.ini** configuration file from Command Centre via the External System Server's **Setup** tab.
4. Copy the configuration file to FTCAPI install folder.

Note: The External/DVR System is assigned to the External System Server item via the **API Setup** property page on the External System or DVR System items.

- It is possible to configure multiple External Systems and/or DVR Systems on each External System Server.
- The External System Server must be configured for all pre-7.80 Controller 6000s.
- Each External System and DVR System must have an External System Server configured in the **API Setup** property page from v7.80 onwards, or the external interface will not function.

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...External System 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 **Setup** tab.



5. Enter the Middleware PCs name or IP Address in the **Host Name** field. This field is limited to 255 alpha-numeric characters.
6. Enter the FTCAPI listening Port that the External System (or DVR System) is configured on in the **Port** field.
7. The **Import Certificate** button allows you to import the FTCAPI certificate (**GallagherFTCAPI.pem**) from the PC containing the FTCAPI.
   This is so the FTCAPI will be allowed to send messages through to Command Centre via the Controller.
   Notes:
   - Once you import the FTCAPI certificate, the **Export Configuration...** button is enabled.
   - If you select an invalid certificate, the **Clear Certificate** button becomes enabled. Clicking it allows you to click on **OK** or **Apply** without the invalid certificate being imported.
   - If you are using a pre-v7.80 version of FTCAPI, then you copy the server's licence file onto the FTCAPI machine instead of importing keys and exporting configuration.
     You only do Steps 7 and 8 for a 7.80 FTCAPI (or later).
8. You can export the **GallagherFTCAPI.ini** configuration file that can then be copied into the **`GallagherFTCAPI`** folder of your FTCAPI machine. This allows the FTCAPI to be used and you can then send events to Command Centre. Without this **.ini** file, the API will not work.
   Note: The private key (**GallagherFTCAPI.key**) and configuration file (**GallagherFTCAPI.ini**) can be placed in the middleware application folder instead of the FTCAPI folder if you want to have more than one middleware application installed on the same machine.
9. Click the **Custom Fields** tab if you want to add and assign a custom field value to this External System Server.
   For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
10. Click the **Notes** tab if you want to add a note(s) about this External System Server.
    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 new External System Server has been created and displays at the root level of the External Systems window.

Installing the FTCAPI Middleware Framework (FMF)

Introduction

This topic describes how to install the FTCAPI Middleware Framework.

If your site is licensed for FTCAPI middleware plug-ins, each middleware PC must have the FTCAPI Middleware Framework installed. Perform the following procedure on each middleware PC:

Note: Microsoft .NET Framework 4.7.2 is required on the middleware PC.

Procedure

1. Run the executable **FMFSetup_8.xx.xx.msi** located in the **`Utilities\System Interfaces\Middleware Framework vMF8.xx.xx`** folder of the Gallagher Command Centre installation files.
   The FTCAPI Middleware Framework Installer wizard displays.
2. Click the **Next** button on each wizard screen, and then the **Finish** button on the final screen.
   The following are installed on the middleware PC:
   - The Gallagher FTCAPI Middleware Framework.
   - A new service named FTCAPI Router Service. It will need to be manually started first time. This service needs to remain running to enable FTCAPI functionality.
3. The directory **`C:\ProgramData\Gallagher\Command Centre`** will be created as soon as you start the service. You need to enable "Show hidden files, folders and drives" in **Control Panel** > **Folder Options** to see it. Copy your Command Centre license file (**Command Centre.lic**) into that folder.
4. Ensure the middleware PC's Firewall is configured to allow the FTCAPI to listen on port 1073.

Configuring an External System

Introduction

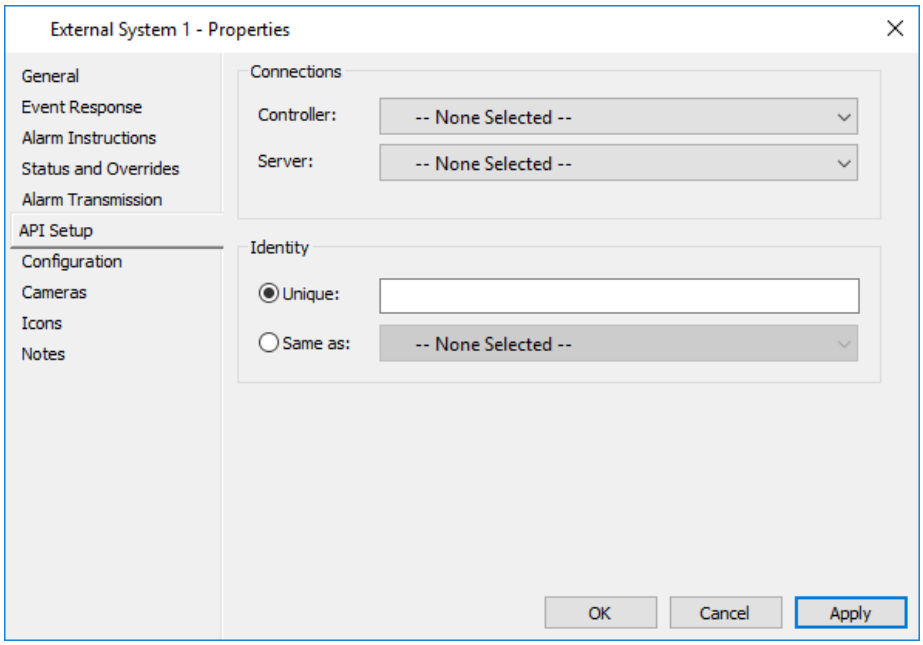
This topic describes how to configure an External System in Command Centre.

An External System in Command Centre represents a connection to middleware, (i.e. a third-party developed application or service running on a Windows PC that interfaces to an external system).

Note: Operators require the "Edit Site" operator privilege to be able to add, modify and delete External Systems.

Procedure

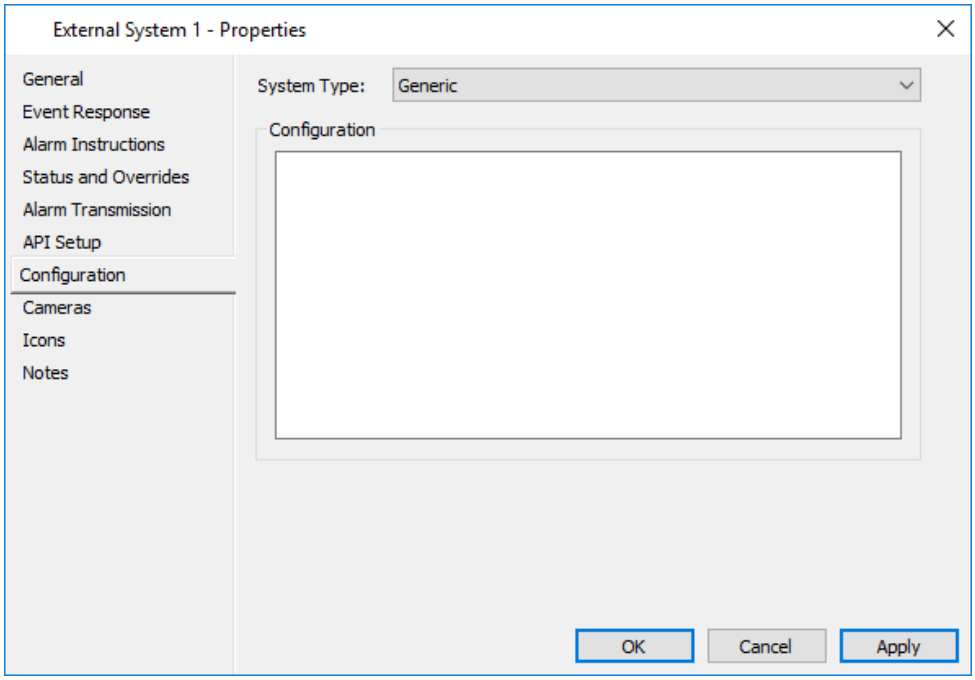
1. Click **Configure** from the menu bar, then **External Systems**.
   The **External Systems** List Window opens (in tree view).
2. **Right click** and select **New...External System**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General 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 **API Setup** tab.



7. Select the appropriate **Controller** from the drop-down list.
   Note: If a Controller is selected, the **Server** field becomes compulsory.
8. Select the appropriate External System Server from the **Server** drop-down list.
9. Click the appropriate radio buttons in the "Identity" section of this screen.

Radio Button	Description
Unique	This radio button allows you to assign an identity string to this External System such that all FTCAPI communication related to this item will be tagged with the assigned identity. This field is limited to a maximum of 64 characters.
Same as	This radio button allows you to link the identity of this External System to be the same as another. **Note:** If "Same as" is selected, the **Configuration** tab disappears, therefore go to Step 15.

10. Click the **Configuration** tab.



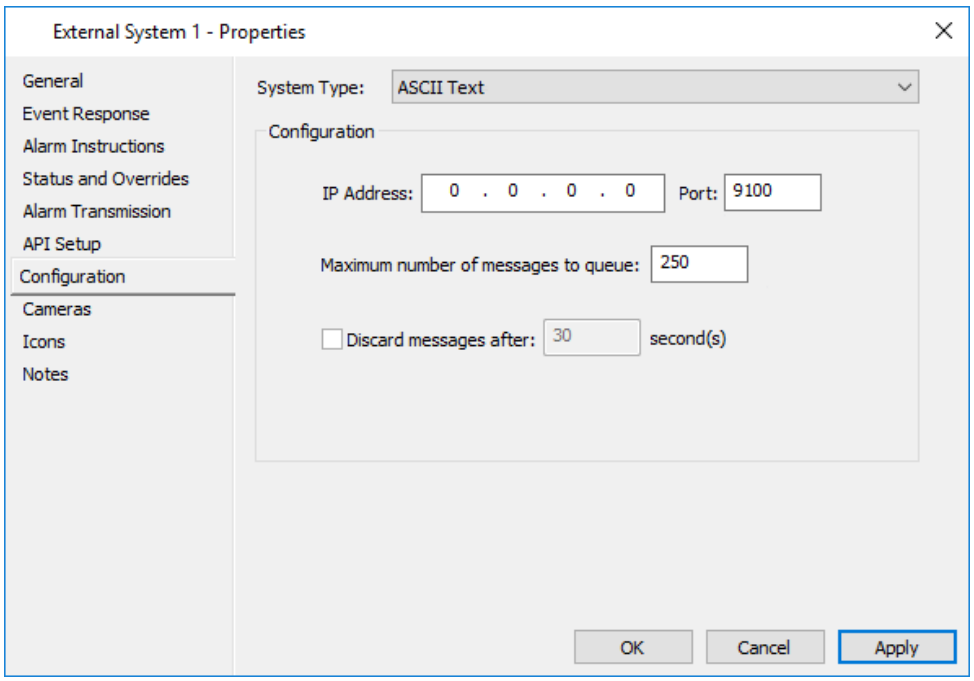
This screen allows you to assign a system type and a configuration string to the External System. The **System Type** drop-down list defaults to "Generic", and will only be populated with the supported middleware 'plug-in' system types it finds in your Command Centre license file.

11. Is your site licensed for middleware plug-ins?

If...	and you...	then go to...
yes	want to use a plug-in for this External System,	Step 12.
yes	do **not** want to use a plug-in for this External System,	Step 15.
no		Step 15.

12. Select the middleware plug-in to be used, from the **System Type** drop-down list.

    Note: The "Configuration" section of this screen becomes populated according to the plug-in selected, (e.g. the following screen example demonstrates how the screen will look when the **ASCII Text** plug-in is selected). For instructions on how to configure your selected plug-in, refer to the appropriate release note, located in the `'Utilities\System Interfaces'` folder of the Gallagher Installation files.



13. For the ASCII Text plug-in, enter the **IP Address** and **Port** of the terminal server that acts as a Serial-TCP/IP protocol converter for the plug-in.

    Note: You must use a terminal server that allows multiple concurrent connections. This is required as the plug-in creates a new separate connection for each message and some terminal servers take a long time to close them. This has been tested using a 'Moxa Nport 5150 serial device server'.

14. For the ASCII Text plug-in, complete any other "Configuration" details as required:

Field	Description
Maximum number of messages to queue	This field determines the maximum number of messages that the ASCII Text plug-in will hold in a queue while the connection between the FTCAPI Middleware Framework (FMF) and the Terminal Server is down. When the queue is full the oldest message is discarded when a new message arrives. Limited to a maximum of 500 messages.
Discard messages after	Checking this field allows you to enter the length of time that messages will be held in the ASCII Text plug-ins queue. Limited to 1-9999 seconds.

15. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this External System.
    For further details see ***Cameras tab*** (on page 3-24).
16. Click the **Icons** tab if you want to change the Icon Set for this external system.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
17. Click the **Custom Fields** tab if you want to add and assign a custom field value to this external system.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
18. Click the **Notes** tab if you want to add a note(s) about this external system.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
19. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

A new External System has been created and displays at the root level of the External Systems window, with no children.
Note: A new External System can be saved even if some of the properties are not entered, however it will not function correctly until all the properties are entered.

Hint

Editing and Deleting external systems
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete external systems.
Notes about deleting external systems:

- The External System will only allow the deletion if it does not have any children, (i.e. no External System Items 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 an External System Item

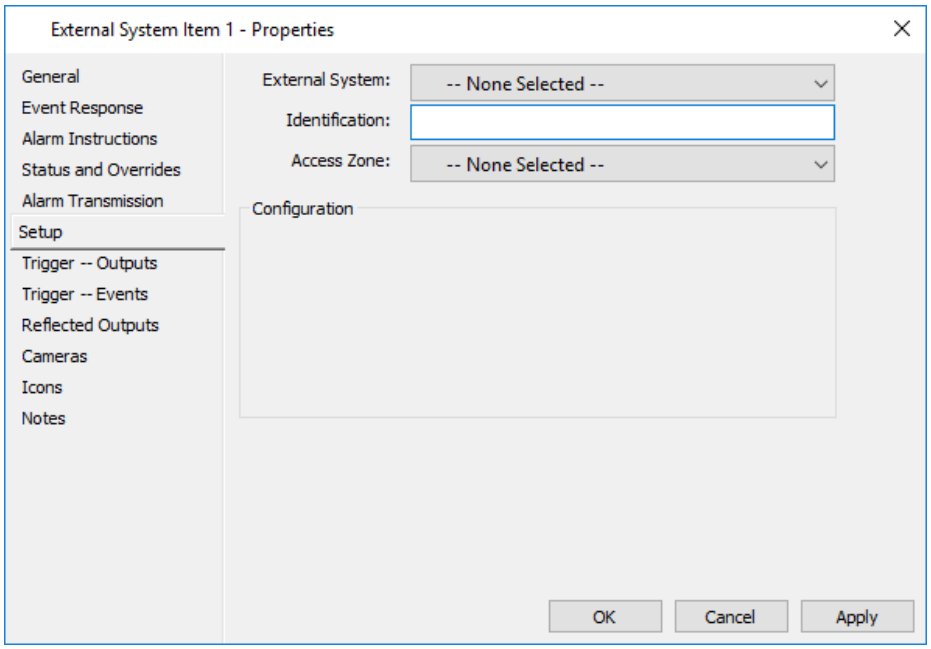
Introduction

This topic describes how to create an External System Item in Command Centre.

Note: Operators require the "Edit Site" operator privilege to be able to add, modify and delete External System Items.

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...External System Item**.
   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 **API Setup** tab.



7. Select the appropriate **External System** from the drop-down list that this External System Item belongs to, (e.g. an "ASCII Text" External System Item must have an "ASCII Text" External System Type).
   Notes:

- The "Configuration" section is dependent on the plug-in selected on the parent External System's **Configuration** tab. Most plug-in's will not require further configuration for individual External System Items therefore the "Configuration" section will be disabled.
- If you do not select an External System, this External System Item will display at the root level of the **External Systems** List Window tree until it is assigned an External System as a parent.
- Although there is no hard limit to the number of External System Items per External System, it is recommended that this number does not exceed 2000.

8. Enter a string value in the **Identification** field.
   This identifier is intended to allow the API to map external system items in the external system to the Command Centre items that represent them.
   Note: The Identification string entered is checked for uniqueness within the same External System. It is limited to 64 characters.
9. Select an **Access Zone** from the drop-down list, if required for card events.
   Note: This is a deprecated setting that was used by FTC clients before External System Items were able to be used as Readers. External System Items should now be assigned to Doors on the **Entry Zone** and **Exit Zone** tabs of their properties in Configuration Client.
10. If you want to configure trigger strings and/or reflected outputs for this External System Item, go to ***Configuring FTCAPI Trigger Strings and Reflected Outputs*** (on page 24-25) for the procedure.
11. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this external system item.
    For further details see ***Cameras tab*** (on page 3-24).
12. Click the **Icons** tab if you want to change the Icon Set for this external system item.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
13. Click the **Custom Fields** tab if you want to add and assign a custom field value to this external system 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 external system item.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
15. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

A new item has been created and displays as a child of the selected External System in the **External Systems** List Window.

Hint

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

Configuring a DVR System

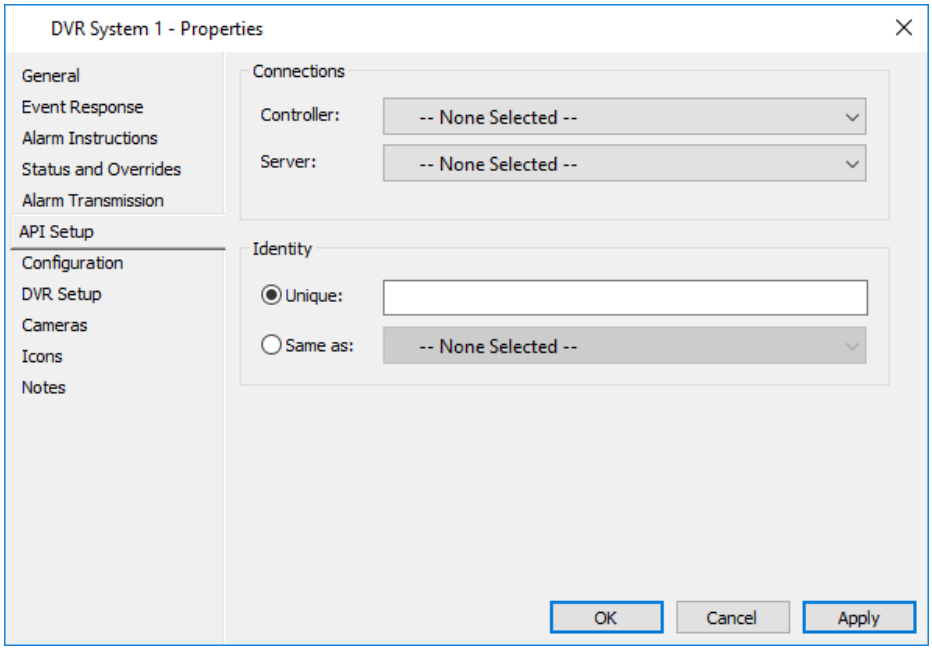
Introduction

Command Centre can be integrated with Digital Video Recording (DVR) equipment and software from a range of manufacturers. For a list of all DVR Integrations currently supported by Command Centre, contact Gallagher Security Technical Support.
Note: The DVR Server PC must maintain synchronisation with the Command Centre Server at least once a day to ensure the stored image sequences can be accurately requested through Command Centre from the DVR Server. Synchronisation can either be of each other, (i.e. Command Centre Server and the DVR Server), or it can be configured to synchronise off a common source, (e.g. the Domain Controller or a known reliable time-clock source off the Internet).

To configure a DVR System, complete the following procedure:
Note: Operators require the "Edit Site" operator privilege to be able to add, modify and delete DVR Systems.

Procedure

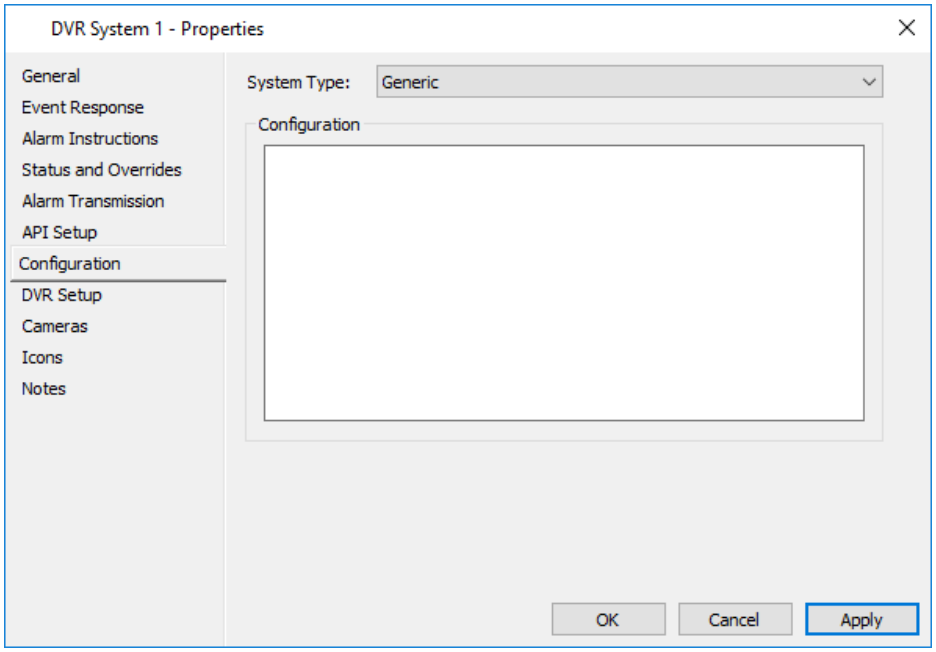
1. Click **Configure** from the menu bar, then **External Systems**.
   The **External Systems** List Window opens (in tree view).
2. **Right click** and select **New...DVR System**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (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 **API Setup** tab.



7. Select the appropriate **Controller** from the drop-down list.
   Notes:
   - Only standard Gallagher Controllers will work, (i.e. Gallagher UltraSec Controllers will not work).
   - If a Controller is selected, the **Middleware PC Name/IP Address** field becomes compulsory.
8. Enter the Middleware PCs name or IP Address in the **Middleware PC Name/IP Address** field. This field is limited to 255 alpha-numeric characters.
9. Click the appropriate radio buttons in the "Identity" section of this screen.

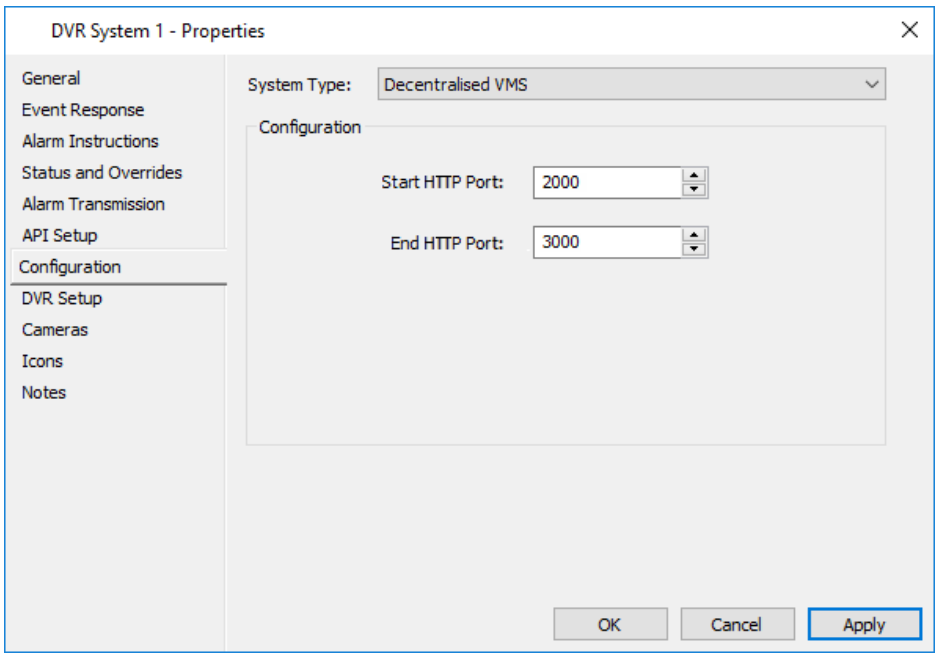
Radio Button	Description
Unique	This radio button allows you to assign an identity string to this DVR System such that all FTCAPI communication related to this item will be tagged with the assigned identity. This field is limited to a maximum of 64 characters.
Same as	This radio button allows you to link the identity of this DVR System to be the same as another. **Notes:** • At most, 100 External System Items can be assigned to an External System. By configuring multiple External Systems that are the same, you can negate this limitation. • If "Same as" is selected, the **Configuration** tab disappears, therefore go to Step 17.

10. Click the **Configuration** tab.

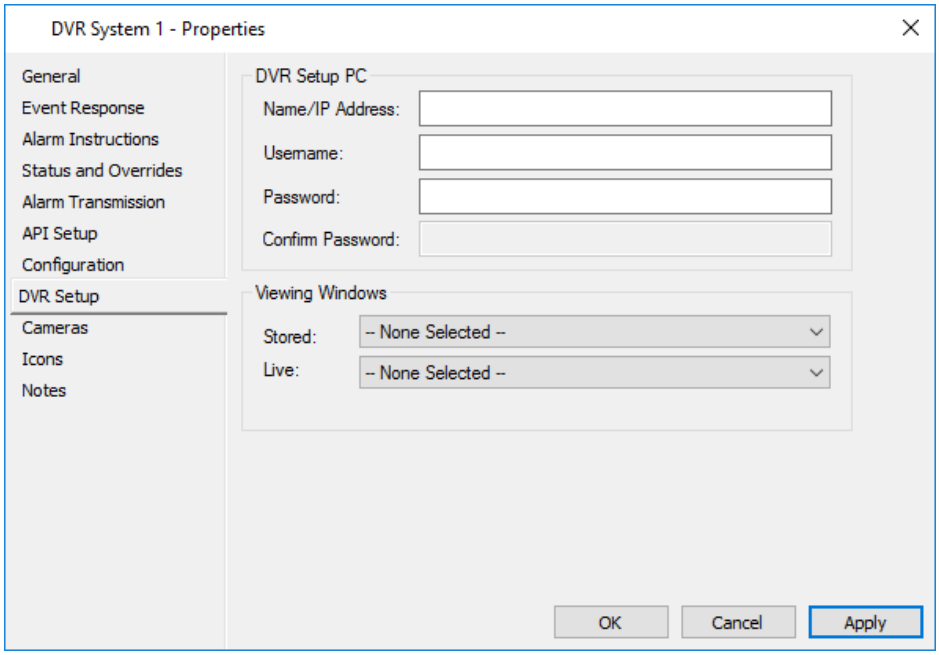


This screen allows you to assign a system type to this DVR System. The **System Type** drop-down list defaults to "Generic", and will only be populated with the supported middleware 'plug-in' system types it finds in your Command Centre license file.

11. Select the DVR middleware plug-in to be used, from the **System Type** drop-down list.
Note: The "Configuration" section of this screen becomes populated according to the plug-in selected, (e.g. the next screen example shows how the screen will look when the **Decentralised VMS** plug-in is selected). For instructions on how to configure your selected plug-in, refer to your DVR Integration release note, provided with your DVR plug-in files.



12. For the Decentralised VMS plug-in, specify the port range that Command Centre can use to listen for events generated by the Decentralised VMS cameras assigned as DVR Camera Items. Command Centre will pick the first available free port within this range. Range 1000 to 9999.
13. Click the **DVR Setup** tab.



14. Enter the IP Address or DNS name of the DVR Server PC.
15. Enter the DVR Username and Password to log on to the DVR Server PC.
16. In the 'Viewing Windows' section select the preferred **Stored** and **Live** Video Viewer controls from the drop-down lists.
    These lists will only contain entries if the DVR System Integrator supplied software has been copied onto this workstation PC and registered with the operating system if necessary.
    The supplied software should be installed on all Command Centre workstations that will view DVR images.
17. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this DVR System.
    For further details see ***Cameras tab*** (on page 3-24).
18. Click the **Icons** tab if you want to change the Icon Set for this DVR System.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
19. Click the **Notes** tab if you want to add a note(s) about this DVR system.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
20. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

A new DVR System has been created and displays at the root level of the External Systems window, with no children.

Note: A new DVR System can be saved even if some of the properties are not entered however it will not function correctly until all the properties are entered.

Hint

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

Notes about deleting DVR Systems:

- The DVR System will only allow deletion if it does not have any children, (i.e. no DVR Cameras 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.
- You will still be able to view old stored image sequences for a deleted DVR Camera from within Command Centre, by locating the sequence in the Find Tool. If you also delete the DVR System the camera was associated with, then you will no longer be able to view the old stored image sequence from within Command Centre. You will need to use the DVR manufacturer's tool instead.

Configuring a DVR Camera

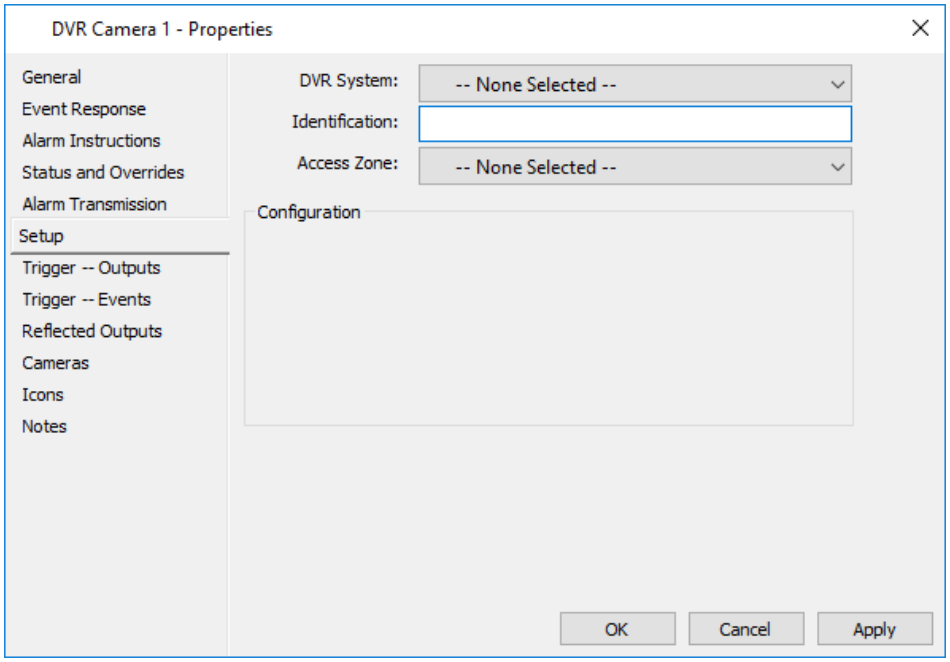
Introduction

This topic describes how to create a DVR Camera in Command Centre.

Note: Operators require the "Edit Site" operator privilege to be able to add, modify and delete DVR Cameras.

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...DVR Camera**.
   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. Select the appropriate **DVR System** from the drop-down list that this DVR Camera belongs to, (e.g. a "Mobotix" DVR Camera must have a "Decentralised VMS" DVR System type).
   Notes:

- The "Configuration" section is dependent on the plug-in selected on the parent DVR System's **Configuration** tab.
- If you do not select a DVR System, this DVR Camera will display at the root level of the **External Systems** List Window tree until it is assigned a DVR System as a parent.

8. Enter a string value in the **Identification** field.
   This identifier is intended to allow the API to map cameras in the DVR System, to the Command Centre items that represent them.
   Notes:
   - The Identification string entered is checked for uniqueness within the same DVR System. It is limited to 110 characters, however only 64 are used for middleware.
   - The identification string does not have to be unique across the entire set of DVR Cameras, as cameras belonging to different DVR Systems may share the same identifier, but the Identifier cannot be left blank.
9. Select an **Access Zone** from the drop-down list, if required for card events.
10. If you want to configure trigger strings and/or reflected outputs for this DVR Camera, go to ***Configuring FTCAPI Trigger Strings and Reflected Outputs*** (on page 24-22) for the procedure.
11. Click the Cameras tab if you want to associate other DVR Camera(s) with this DVR Camera.
    For further details regarding the **Cameras** tab (on page 3-24).
12. Click the **Icons** tab if you want to change the Icon Set for this DVR Camera.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
13. Click the **Notes** tab if you want to add a note(s) about this DVR Camera.
    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 DVR Camera has been created and displays as a child of the selected DVR System in the **External Systems** List Window.

Editing Action Plans with DVR Cameras

Introduction

Operators with the “Edit Alarm Configuration” operator privilege can modify Action Plans.

Procedure

Refer to the procedure for ***Creating a new Action Plan*** (on page 15-4) for full details on how to add a DVR Camera to an Action Plan.

Note though for every trigger DVR Camera you will need a dedicated relay (output) also to communicate the trigger to the external DVR recording device.

Each dedicated relay (output) should also have a pulse time set, via the Advanced tab of the Output Property page. The pulse time may control the number of seconds of video stored after the alarm, depending on the DVR manufacturer. Alternatively, the number of seconds of pre-alarm imaging and post-alarm imaging may be configured through the DVR manufacturers software, and the Command Centre relay pulse time should be set to one second.

Configuring FTCAPI Trigger Strings and Reflected Outputs

Introduction

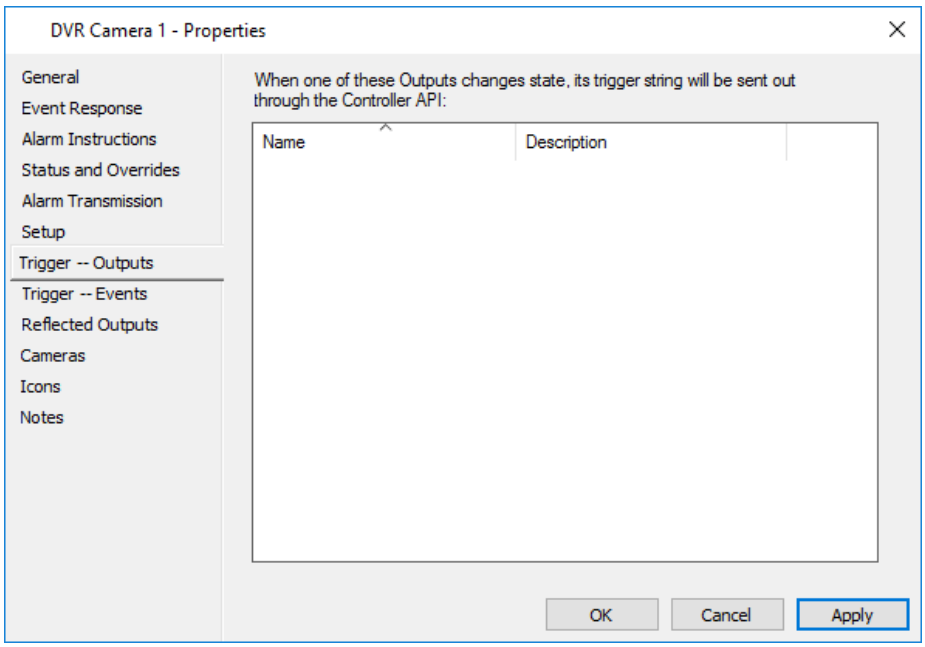
The dispatch of trigger strings through the Gallagher Controller API (FTCAPI) can be configured for External System Items and DVR Cameras, and can be based on:

- Output state changes, and/or
- event and alarm occurrences

This procedure provides instructions on how to configure trigger strings and/or reflected outputs for an External System Item or DVR Camera. The example used here is for a DVR Camera.

Procedure

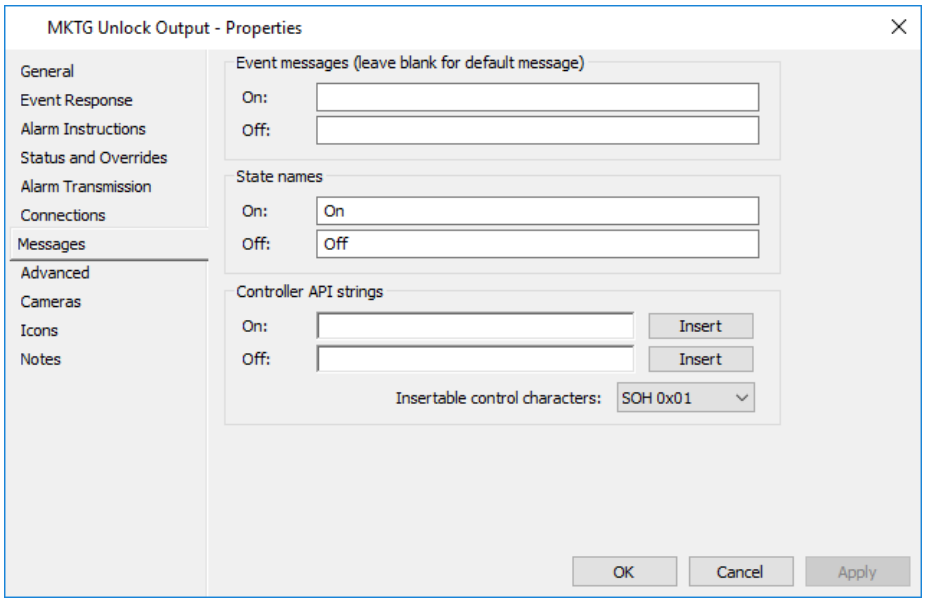
1. Click **Configure** from the menu bar, then **External Systems**.
   The **External Systems** List Window opens (in tree view).
2. **Right click** on the appropriate External System Item or DVR Camera.
3. Do you want to configure FTCAPI strings that will be triggered by Output switching?
   If **yes**, go to Step 4.
   If **no**, go to Step 12.
4. Click the **Trigger -- Outputs** tab.



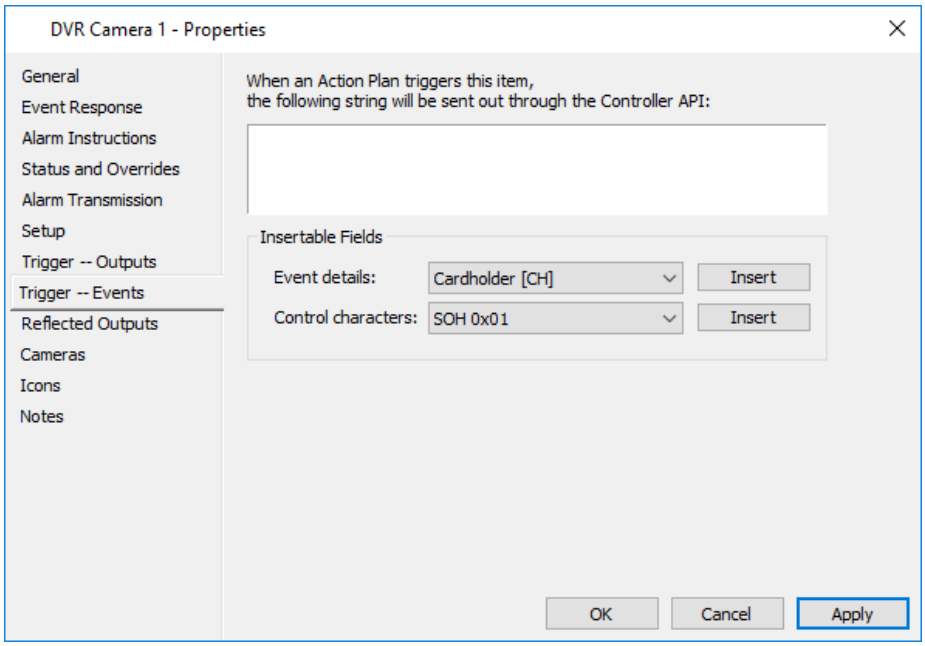
This screen allows Outputs to be associated with the External System Item or DVR Camera, used to group and identify the outbound strings.

5. Open the **Hardware** List Window, and drag and drop the Output(s) required onto this screen, and click **Apply**.
6. Open the property pages for the Output(s) from the previous step.

7. Click the **Messages** tab.

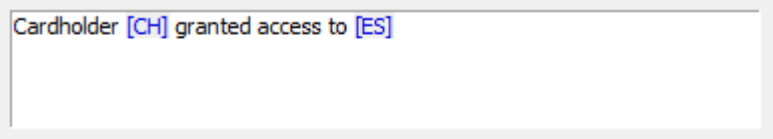


8. In the **Controller API strings** section of this screen, enter the definition of one API Output string for each state, (i.e. **On** and **Off**) of the Output.
   Note: The On and Off strings can include control characters to support ASCII text plug-ins.
9. Click **Apply**.
10. Repeat Steps 7 - 9 for each Output associated with the External System Item or DVR Camera.
11. Do you want to configure FTCAPI Strings that will be triggered by Events also?
    If **yes**, go to Step 12.
    If **no**, go to Step 19.
12. Click the **Trigger -- Events** tab.



This screen allows you to define a trigger string for the External System Item or DVR Camera, that is dispatched out of the API on the activation of an Action Plan.

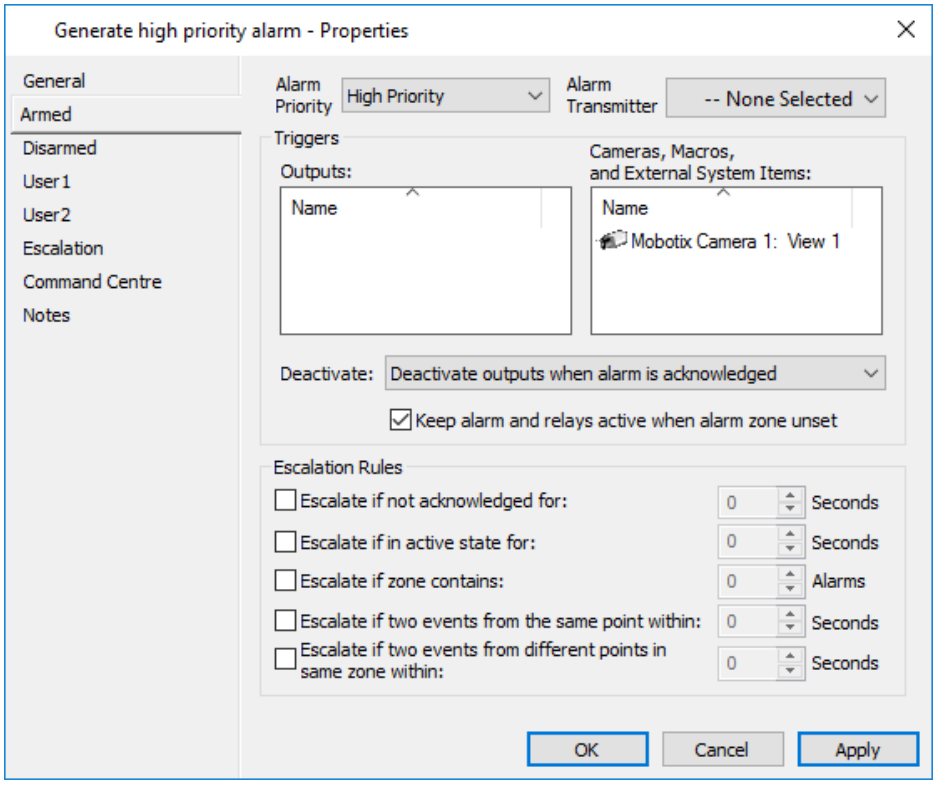
13. Enter a string into the grid.
    This is achieved by typing in text and selecting the appropriate 'Insertable Fields', (i.e. **Event details** and **Control characters**), from the drop-down lists where necessary, and clicking the applicable **Insert** button.



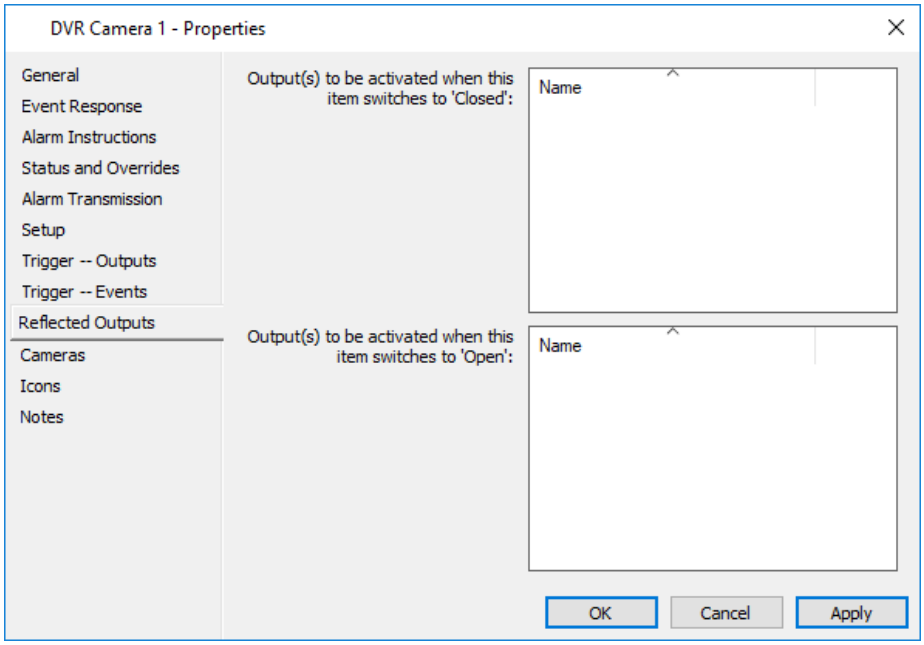
Notes:

- The string is limited to 100 characters.
- The Insertable fields represent entities that can be named within Command Centre, (e.g. [CH] represents a cardholders name, and [ES] represents a Door), and control characters, (e.g. carriage return, line feed, etc.).

14. Click **Apply**.
15. Open the Action Plan you want assign the External System Item or DVR Camera to as a trigger.
16. Click the appropriate State tab, (i.e. **Armed**, **Disarmed**, **User 1** or **User 2**).



17. Drag and drop the External System Item or DVR Camera into the **Cameras, Macros, and External System Items** grid.
    When this Action Plan is activated, the trigger string will be dispatched.
18. Click **OK**.
    The Action Plan screen closes.
19. The FTCAPI is able to reflect the state of Outputs (with the support of inversion), based on the External System Item's or DVR Camera's status values submitted through the API to Command Centre.
    Do you want to configure reflected outputs for this External System Item or DVR Camera?
    If **yes**, go to Step 20.
    If **no**, go to Step 22.
20. Click the **Reflected Outputs** tab of the External System Item or DVR Camera.



21. Drag and drop the Outputs required into the appropriate grids on this screen.
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.

Result

Trigger strings have been configured for the External System Item or DVR Camera.

SchindlerID

The SchindlerID System integrates Command Centre and the SchindlerID individualization and access control system v1.3.369.1.

This integration is comprised of three parts:

1. The Schindler Cardholder Management Interface

- Synchronises the Schindler user database with the Command Centre Cardholder database.
- Allows one access card to be used for building doors and the lift system.
- Can convert Badge Numbers from decimal to hexadecimal format.
- Allows Cardholder cards to be automatically formatted as hexadecimal Badge Numbers according to their Card Type specification.
- Assigns a Cardholder's MIFARE Card Serial Number (MIFARE CSN) to the Badge Number field of the corresponding Schindler user.
- Reports on access events at a turnstile/barrier.

2. The Life Reporting Interface (plugin)

- Builds an audit trail of Schindler access events in Command Centre.
- Enables Command Centre to receive non-badge card events from Schindler.

3. The Call Interface (plugin)

- Enables a Gallagher reader to be used at a Schindler terminal to identify the Cardholder to the Schindler system.
- Enables Command Centre to set the status of a floor to 'Secure' or 'Free' via a schedule or operator override.

Notes:

- This integration is compatible with the SchindlerID Call Interface protocol as specified in the document J 41900402.
- Card numbers greater than 16,777,215 are not supported.

Licensing

The following licence entries are required:

Licence	Description
[Limits] SchindlerID Systems=n If using SchindlerID plugins the following licence entries are required: [Plugin] PluginX=SchindlerID-LifeReporting PluginX=SchindlerID-CallInterface	Where n is the maximum number of SchindlerID Systems that can be created. Once the maximum number has been reached the option to create additional SchindlerID Systems will be disabled.

Command Centre multi-server support

The following Command Centre multi-server functionality has been tested:

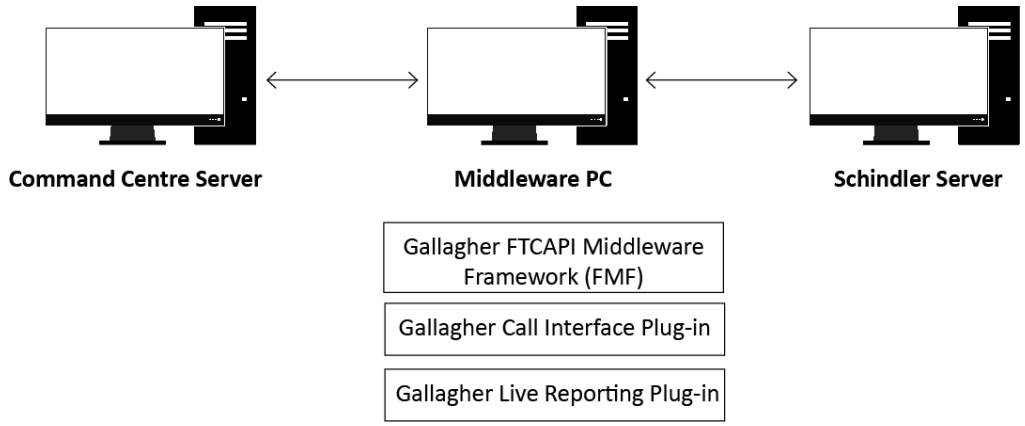
- All Gallagher-Schindler communications (including Cardholder Sync and Life Reporting) occur from server 1.
- Life Reporting events are replicated to server 2.
- Cardholders can be created on either server (assuming Card Types exist on server 1) and are replicated.
- Floor overrides can occur from both servers.

Compatibility

The following components are compatible with the Schindler interface:

- Third-Party Database Online Interface J41900401:153324 (11-09-01)
- Call Interface to External Security Systems J41900402: 153324 (11-09-01)
- Third Party Life Reporting Interface v2.8: (12-03-26)
- Schindler ID v1.3.369.1

Deployment architecture



The Schindler Cardholder Management Interface

Introduction

The Cardholder Management Interface enables the Schindler user database to be synchronised with the Command Centre Cardholder database.

If a change is made in the Command Centre Cardholder database the Schindler user database will be updated to match. If a user has been manually added to the Schindler user database and not the Command Centre Cardholder database, the user will not be removed when an update occurs.

Command Centre should be used to add, change and delete all Cardholders.

When syncing Card Types, a Command Centre Cardholder's **Card Number** and **Facility Code** is encoded into the Schindler **Personal Number**; when syncing Mobile Credentials, a Command Centre Cardholder's Mobile Credential ID (number) followed by '_MOBILE' is encoded into the Schindler Personal Number. This Personal Number is what identifies a user in the Schindler user database. The user is then granted lift access depending on their allowed access profile configured within Schindler.

Cardholders must be assigned at least one card or Mobile Credential in Command Centre in order to be synchronised to the Schindler user database.

Configuration

To configure the Schindler Cardholder Management Interface, perform the following procedures:

- ***Configuring a Schindler Access Zone Schedule*** (on page 24-29)
- ***Configuring a Schindler Cardholder Access Schedule*** (on page 24-29)
- ***Configuring a Schindler Access Zone*** (on page 24-29)
- ***Configuring Schindler Personal Data Fields*** (on page 24-30)
- ***Configuring a Schindler Access Group*** (on page 24-31)
- ***Configuring Schindler Cardholders*** (on page 24-32)
- ***Configuring a Schindler Card Type*** (on page 24-36)
- ***Configuring a SchindlerID System*** (on page 24-38)
- ***Synchronising databases*** (on page 24-42)

Configuring a Schindler Access Zone Schedule

Create an Access Zone Schedule. Refer to the topic Creating a new Schedule. Name the Schedule 'Schindler Access Zone Schedule'. Set the State/Action to **Secure - No PIN** at all times.

Configuring a Schindler Cardholder Access Schedule

Create a Cardholder Access Schedule. Refer to the topic Creating a new Schedule. Name the Schedule 'Schindler Cardholder Access Schedule'. Set the State to **Grant Access** at all times.

Configuring a Schindler Access Zone

Create an Access Zone. Refer to the topic Adding a new Access Zone. Name the Access Zone 'Schindler Access Zone'. Assign the 'Schindler Access Zone Schedule' to this zone.

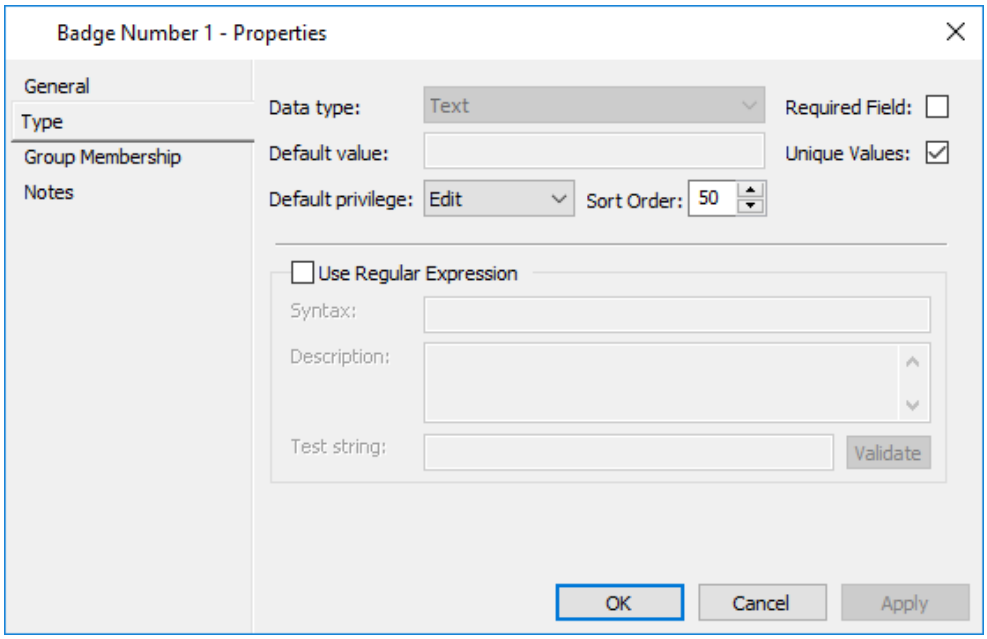
Configuring Schindler Personal Data Fields

Create a Personal Data Field for each of the Schindler fields listed below.

Schindler field	PDF data type
User Template	Text - List
Parent Group	Text - List
Department	Text - List
Badge Number 1	Text - Only required if Direct PDF option is used
Badge Number 2	Text - Only required if Direct PDF option is used
Badge Number 3	Text - Only required if Direct PDF option is used

Notes:

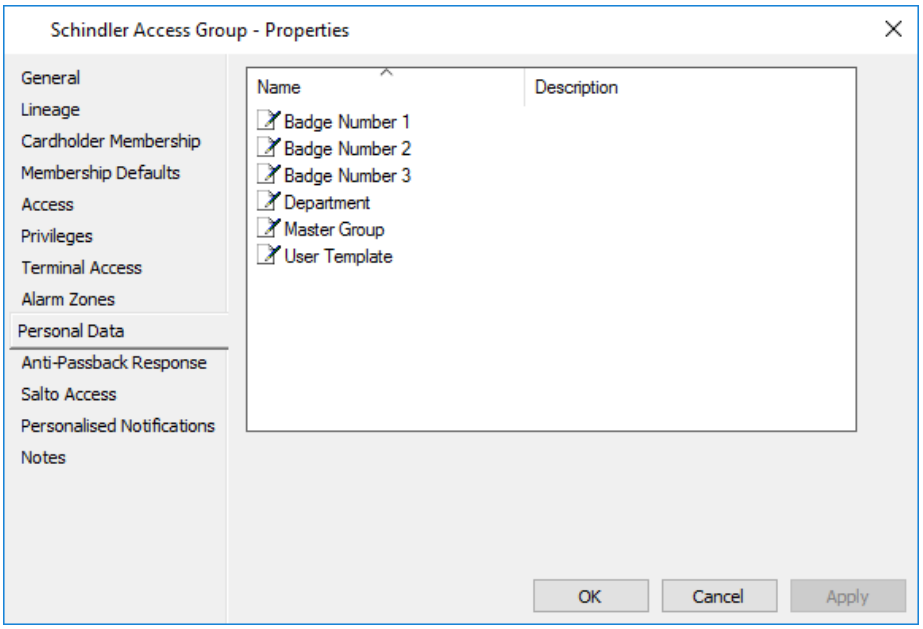
- The PDF name is arbitrary, but the data type must correspond (match) the Schindler field for which the PDF is created for.
- Configure the Text - List data type PDFs with each of the Text - List data type Schindler fields.
- Ensure the Badge Number 1, Badge Number 2, and Badge Number 3 PDFs are configured as unique values, as shown below.



Configuring a Schindler Access Group

Create a Schindler Access Group. Refer to the topic Setting up Access Groups.
Name the Access Group 'Schindler Access Group'.
Assign to this Access Group:

- Cardholders (Cardholders that require access to Schindler readers, terminals and lifts).
- The Schindler Access Zone previously configured. Cardholders belonging to this Access Group will inherit access to the Schindler Access Zone.
- The Schindler Cardholder Access Schedule previously configured (for the Schindler Access Zone).
- Schindler Personal Data Fields. Cardholders belonging to this Access Group will inherit the Schindler Personal Data Fields.



Notes:

- If a Cardholder is removed from the Schindler Access Group (thus the Cardholder no longer has the Schindler PDFs assigned), then an update will occur and the Cardholder will be removed from the Schindler user database.
- The Cardholder's last name must not be left empty, as this is a mandatory field in Schindler. If the Cardholder's last name is empty, the corresponding Schindler user will be deleted.
- If a Cardholder is removed from an Access Group that does not have the Schindler PDFs assigned, then an update will not occur.
- If a Cardholder has been assigned to a Temporary Access Group that has the Schindler PDFs assigned, then the Cardholder will be removed from the Schindler user database, once the temporary access has expired.

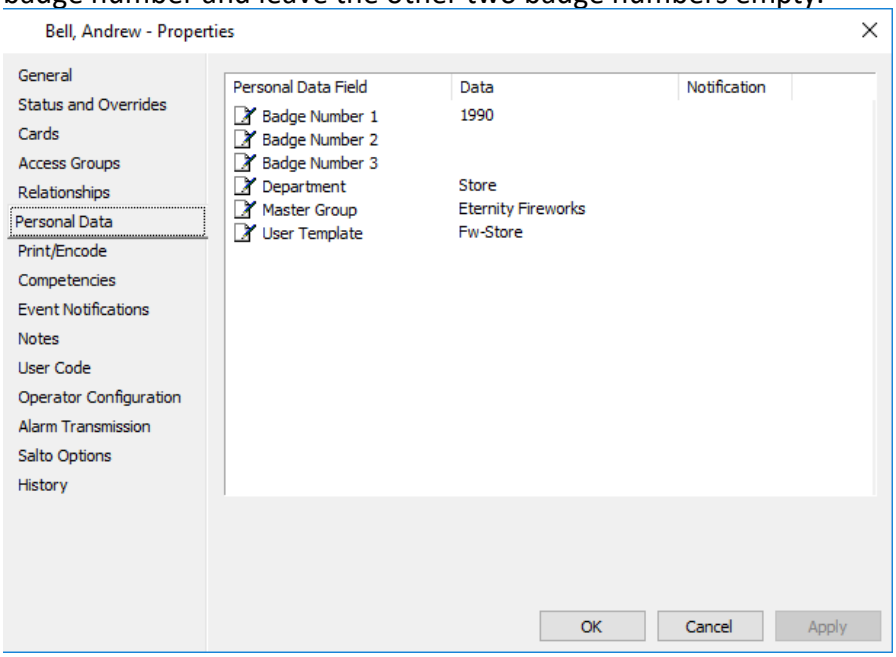
Configuring Schindler Cardholders

Create the Cardholders that require access to Schindler readers, terminals, and lifts. Configure the Schindler Personal Data Field values for each Cardholder.
To map the Schindler Personal Data Field values, refer to the following topics:

- ***Mapping the Schindler User Template*** (on page 24-33)
- ***Mapping the Schindler Parent Group*** (on page 24-33)
- ***Mapping Schindler Badge Numbers*** (on page 24-33)

Notes:

- The Schindler 'User Template' and 'Parent Group' PDFs must be assigned to each Cardholder, otherwise the Cardholder will **not** be imported into the Schindler user database.
- If a Cardholder has the Schindler 'User Template' and 'Parent Group' PDFs assigned and has **two cards or more** assigned, then the Cardholder will be imported as two or more users into the Schindler user database.
- If a Cardholder has the Schindler 'User Template', 'Parent Group' and 'Badge Number' PDFs assigned and two cards assigned, then only one user will be imported into the Schindler user database. This user will have the badge numbers assigned. The second user will not be imported because the badge numbers are already assigned to the first user.
- If a Cardholder does not have the PDF Badge Numbers assigned, when an update occurs, Badge Numbers already configured for this user in the Schindler user database will be removed. To avoid this, assign the PDF Badge Numbers to the Cardholder and type '**ignore**' as the data value for the first badge number and leave the other two badge numbers empty.



Mapping the Schindler User Template

The User Template PDF value must match exactly the User Template in Schindler. User Templates are used, among other things to configure the access rights. A User Template is applied when the user is transferred to Schindler.

The access rights can be configured in two different ways. Either you can configure it directly on the User Template tab, or you configure an Access Profile and assign it to the User Template. Access Profiles are configured on another button located near the User Templates button.

Mapping the Schindler Parent Group

The Parent Group PDF value must match exactly the Parent Group in Schindler.

The Parent Group in Schindler typically refers to a company whose operator, a 'parent' manages the company's employees in Schindler.

Mapping Schindler Badge Numbers

Schindler allows three **Badge Numbers** (card credentials) to be populated for one user. The **Badge Numbers** are used by Schindler for matching card data read by Schindler controlled readers.

The basic format of a Badge Number is a hexadecimal number string. Its length and interpretation are dependent on Schindler configuration.

Command Centre can populate a **Badge Number** in one of the following ways:

- A Cardholder's Mifare Card Serial Number (Mifare CSN) is automatically formatted as a hexadecimal number string upon updating. This option corresponds to the 'Mifare CSN' **Badge Number Preference** selectable on the SchindlerID External System item.
- A Cardholder's card can be automatically formatted as a hexadecimal number string. This option corresponds to the 'Card Type Specified' **Badge Number Preference** selectable on the SchindlerID External System item. Card formats 'Wiegand 26/8 bit', 'Wiegand 35/12 bit (HID Corporate 1000)', and 'Wiegand 37/16 bit (HID H10304)' are supported. Multiple Card Types (thus multiple Facility Codes) can be used.
- A Command Centre operator can enter a decimal number as a value of a Text data type Personal Data Field (PDF) for a Cardholder. This value is automatically converted to a hexadecimal string upon updating. This option requires some Windows hexadecimal conversion registry values to be set up on the Command Centre server. This option corresponds to the 'Direct PDF' Badge Number Preference selectable on the SchindlerID External System item.

- A Command Centre operator can enter a hexadecimal number string as a value of a Text data type Personal Data Field (PDF) for a Cardholder. This option corresponds to the 'Direct PDF' **Badge Number Preference** selectable on the SchindlerID External System item.

Schindler Badge Number Conversion

The Badge Number PDF value entered will be imported into Schindler as the Schindler Badge Number.

Badge numbers can be converted from decimal format to hexadecimal format when imported into Schindler. In order to perform the conversion you will need to create the following registry entries and define the appropriate values for each:

Registry Entry Name	Type	Value	Meaning
BadgeNumberConvert	REG_DWORD	1	The conversion is performed and the BadgeNumberConstant is added to the front of the converted value of the Badge Number PDF value.
		2	The conversion is performed and the BadgeNumberConstant is added to the end of the converted value of the Badge Number PDF value.
		0/Other/Not present	The conversion is not performed.
BadgeNumberLength	REG_DWORD	The length of the whole Badge Number once converted. The length cannot be more than the sum of 'HI' and 'LO' number of digits configured in Schindler, as configured in Schindler at **Network, Elevators, Tools > 3rd party database interface**.	
BadgeNumberConstant	REG_SZ	A constant in hexadecimal notation that is added to the front or end of every converted Badge Number.	

Creating a registry entry

Perform the following procedure to create a registry entry:
Note: The registry entries will need to be created on each Command Centre workstation. If a registry value is changed, ensure all other workstation registry values are updated.

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 FT.
   Note: If using a 64 bit system, path you way to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GALLAGHER\Command Centre FT.

4. Right click, then click **New** from the drop-down menu. Another drop-down menu displays. Click **DWORD Value**. Your new DWORD Value is populated at the bottom of the registry values list.
5. Enter the DWORD Value name, (e.g. BadgeNumberConvert).
6. Double-click your newly created DWORD Value. The **Edit DWORD Value** window displays.
7. Select **Decimal** as the Base then enter your new value, (e.g. 1) and click **OK**.
8. Repeat this procedure to create the other registries.

Conversion conditions

To perform a successful conversion, ensure the following is correct:

- All three registry entries mentioned are present
- The 'BadgeNumberConvert' value is 1 or 2
- The Badge Number PDF value is a decimal number (0 - 4294967294)
- The length of the converted value plus the length of the 'BadgeNumberConstant' is less than or equal to the 'BadgeNumberLength'

When the number is converted into hexadecimal notation, leading zeros are added to the converted value so its length equals 'BadgeNumberLength'.

Badge Numbers that are successfully imported into Schindler can be found in Schindler at **Users/Building > Users** (select a user) **> Assigned ID media**.
Note: If the conversion is unsuccessful the card number is imported as is.

Conversion examples:

Registry Entries			Badge Number PDF value	Badge Number as is sent to SID	Comment
BadgeNumberConvert	BadgeNumberLength	BadgeNumberConstant			
-	-	-	4568	4568	No registry entry, no conversion
1	16	01000000ABC1	1990	01000000ABC107C6	1990(dec)=7C6(hex) 0 - leading zero added (to match the length 16) Convert is 1 > Constant was prepended
2	16	01000000ABC1	1990	07C601000000ABC1	Convert is 2 > Constant was appended
1	16	01000000ABC1	0B000000AAFF07C6	0B000000AAFF07C6	Conversion not performed
1	16	01000000ABC1	-12	-12	Conversion not performed
1	16	01000000ABC1	1990 hello	1990 hello	Conversion not performed
1	14	01000000ABC1	1990	1990	Conversion not performed (01000000ABC17C6 is **longer** then 14)

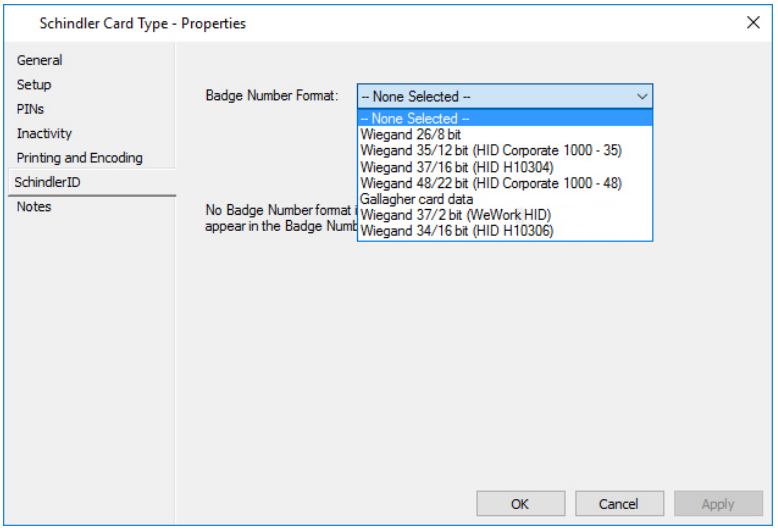
Configuring a Schindler Card Type

Note: This topic is only applicable for Card Types, not Mobile Credentials. Mobile Credential types do not have a **SchindlerID** tab.

If using a Cardholder's card to populate a Schindler **Badge Number**, you will need to specify the option 'Card Type Specified' as the **Badge Number Preference** on the SchindlerID System. You will then need to specify the expected **Badge Number Format**, (e.g. Wiegand 26/8 bit) for the Card Type of the Cardholder's card.

Notes:

- Multiple Card Types, each with a different Badge Number Format can be used (thus multiple Facility Codes are supported).
- The Badge Number Format selected is for the one Command Centre server only and applies to all SchindlerID Systems on that server.



Option	Description
-- None Selected --	This is the default. Combined with the 'Card Type Specified' **Badge Number Preference** option (mentioned later) indicates that there will be no conversion/population for the cards of this Card Type.
Wiegand 26/8 bit	Specifies a Wiegand 26/8 bit card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Wiegand 35/12 bit (HID Corporate 1000 - 35)	Specifies a Wiegand 35/12 bit (HID Corporate 1000) card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]

Option	Description
Wiegand 37/16 bit (HID 10304)	Specifies a Wiegand 37/16 bit (HID H10304) card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Wiegand 48/22 bit (HID Coprorate 1000 - 48)	Specifies a Wiegand 48/22 bit (HIS Corporate 1000-48) card format, including 22 bits of Facility Code, 23 bits of Card Number and 3 parity bits. Applicable cards are formatted accordingly and populated in the Badge Number field in the update message. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Gallagher card data	Specifies a 64-bit Gallagher encoded data. Can only be saved if the Card Type has a ‘Decimal’ Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - MIFARE DESFire [23] **Note:** The Schindler terminals need to have SAM cards deployed that have been provisioned to read Gallagher-encoded data. For more information, contact your local Gallagher representatives.
Wiegand 37/2 bit (WeWork HID)	Specifies a Wiegand 37/2 bit card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Wiegand 34/16 bit (HID H10306)	Specifies a Wiegand 34/16 bit (HID H10306) card format, including 16 bits of Facility Code, 16 bits of Card Number and 2 parity bits. Applicable cards are formatted accordingly and populated in the Badge Number field in the update message. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]

Configuring a SchindlerID System

Introduction

This topic describes how to create a SchindlerID System. The SchindlerID System interfaces with the Schindler Third Party Database Interface.

Notes:

- Operators require the "Edit Site" operator privilege to be able to add, modify, and delete SchindlerID Systems.
- The total number of SchindlerID Systems you can create is determined by your licence file.

Before you begin

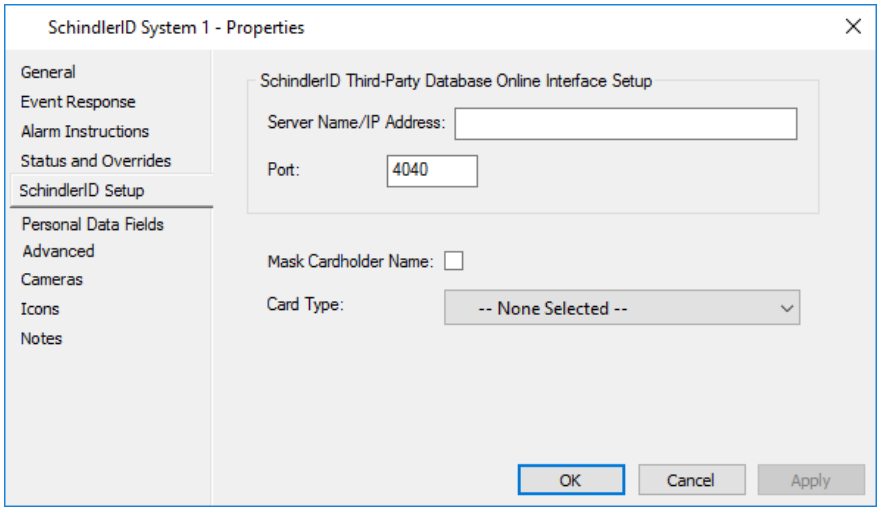
Create the Schindler Third Party Database in Schindler.

Request Schindler integrators to create a Schindler Third Party Database, and provide the following database information:

- The Schindler server name or IP Address of the computer used to create the Schindler Third Party Database.
- The TCP/IP Port Number of the Schindler Third Party Database.

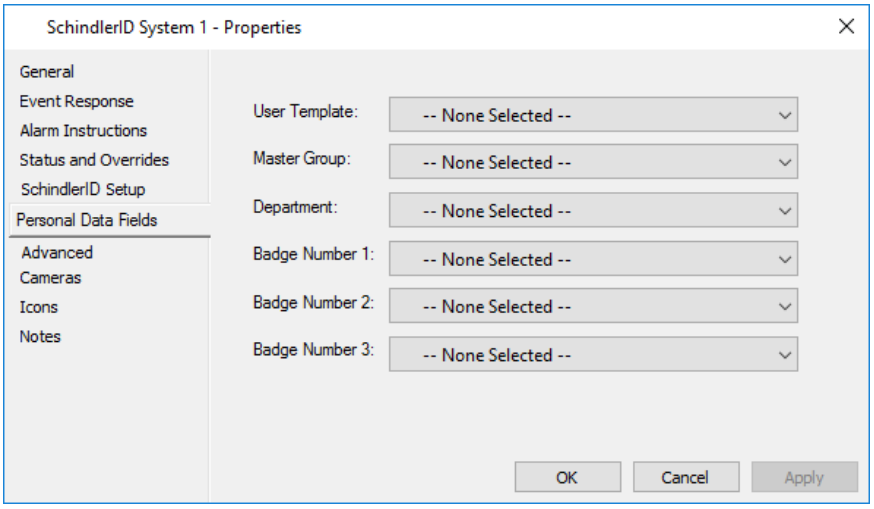
Procedure

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...SchindlerID 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 **SchindlerID Setup** tab.



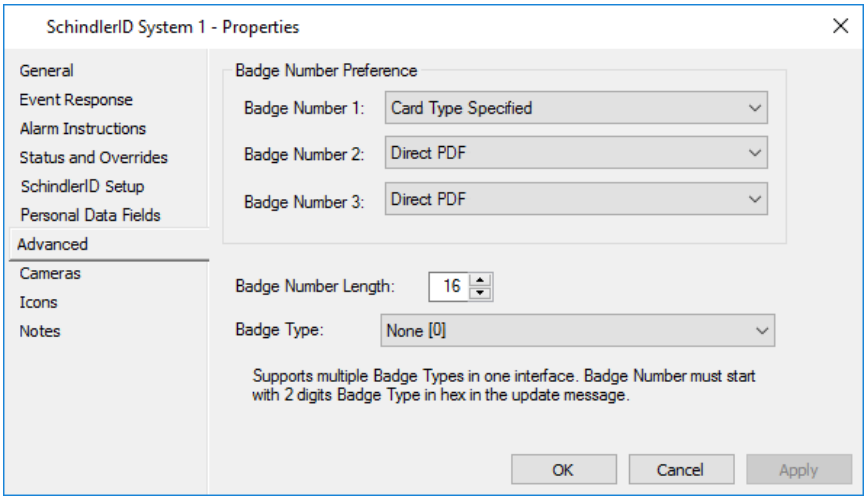
7. Enter the Schindler server PC's IP Address in the **Server PC Name/IP Address** field. This field is limited to 255 alpha-numeric characters.
8. Enter the TCP/IP Port Number of the Schindler Third Party Database Interface in the **Port** field. This value is located in the Schindler Third Party Database Interface. Valid range 1 – 65535.
9. Select the **Mask Cardholder Names** checkbox to hide Cardholders' names within this Schindler system (e.g. to ensure Cardholder privacy). Since Cardholders require a first and last name in the Schindler system, selecting this checkbox replaces Cardholder names in the Schindler system rather than removing them. If this checkbox is checked, each Cardholder entry in the Schindler system has both the first and last names replaced by the Cardholder's card number and facility code, in the format [card number]_[facility code].

   This checkbox does not hide or change any Cardholder names within Command Centre. If you select this checkbox, all existing Cardholder names in the Schindler system are masked. Likewise, if you deselect this checkbox, all existing Cardholder entries in the Schindler system are updated with their real names.
10. If required, select a Card Type or Mobile Credential type from the **Card Type** drop-down list. If selected, only Cardholders configured with this Card Type or Mobile Credential will be imported into the Schindler user database. If left as '-- None Selected --', all Cardholders that have any Card Type card or Mobile Credential will be imported into the Schindler user database.
11. Click the **Personal Data Fields** tab.



12. Select the PDF that corresponds to the Schindler **User Template** field.
13. Select the PDF that corresponds to the Schindler **Master Group** field.
14. Select the PDF that corresponds to the Schindler **Department** field, (optional).
15. Select the PDFs that correspond to each of the Schindler **Badge Number** fields, (optional).
    Note: If using Schindler readers the Badge Number PDFs are required.

16. Click the **Advanced** tab.
    Note: If you selected a Mobile Credential type for the **Card Type** on the **SchindlerID Setup** tab, the **Advanced** tab is not applicable. Only configure this tab if you selected a 'Card Type' type.



17. Select the appropriate **Badge Number Preference** for each Badge Number. Badge Number options are:
    - **Direct PDF**
      This option will use the Badge Number PDF (previously selected) as the Badge Number field in Schindler
    - **MIFARE CSN**
      This option will use the Cardholder's MIFARE CSN as the Badge Number field in Schindler. This option is allowed for one Badge Number field only. This option supports 4-byte and 7-byte CSN only.
      Cardholder cards may need to be (re)captured in Command Centre in order to store each card's CSN in the Command Centre database. A Cardholder's CSN can be captured by presenting the card to a USB MIFARE Encoder in a Cards tile in the Command Centre Client, or in the Configuration Client -> Monitor -> Read MIFARE Card.
      Important: If a Badge Type of **-- None Selected --** has been configured in the SchindlerID System, it assumes that the Badge Type **MIFARE [1]** is configured in Schindler, otherwise the Badge Type configured in the SchindlerID System must correspond to the Badge Type configured in Schindler.
      Command Centre will construct the hexadecimal string using the card's MIFARE CSN and prepend the string with the leading zeros to extend the string length to the configured Badge Number Length.
      For example: 000000000A436AC1 (16 hexadecimal digits).
      The relevant Badge Number field can be verified in Schindler as:
    - **Card Type Specified**
      If this option is selected, the Badge Number hexadecimal number string will be constructed according to the specification of the **Badge Number Format** configured for the relevant Card Type. This option is allowed for one Badge Number field only.

Note: After a 'Badge Number Preference' is changed on a SchindlerID System item, an automatic resync of the item is performed in order to update the Cardholders' relevant Badge Number field.

18. To specify the Badge Number Length, enter the required length in the **Badge Number Length** field. Zeros will be prepended to the hexadecimal string to extend the string length to this number of characters. Default = 16.
19. If the 'Card Type Specified' option has been specified as a Badge Number Preference, select the required Schindler **Badge Type** from the **Badge Type** drop-down list.
    Important: The Badge Type configured here must correspond to the Badge Type configured in Schindler.

Option	Description
-- None Selected --	This is the default and is backward compatible with the existing 'Mifare CSN' Badge Number Preference option. This option only supports 4-byte MIFARE CSN when the 'Mifare CSN' Badge Number Preference has been selected.
None [0]	For supporting multiple Badge Types. Each Badge Number hexadecimal number string in the update message must explicitly specify a two-digit Badge Type at the start. If 'Mifare CSN' is selected as a Badge Number field, this option supports both 4-byte and 7-byte CSN.
MIFARE [1]	Only for 4-byte CSN.
InterISO14443A [21]	Only for 7-byte CSN.
Pure Wiegand [37]	For Wiegand formats with parity bits.
MIFARE DESFire [23]	Supports MIFARE® DESFire® card data including Gallagher encoded card data.

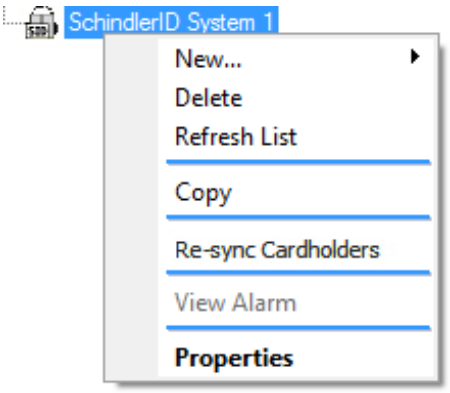
20. Click the **Icons** tab if you want to change the Icon Set for this SchindlerID System.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
21. Click the **Notes** tab if you want to add a note(s) about this SchindlerID System.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-81).
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.

Synchronising databases

It may be necessary to perform a manual cardholder re-sync from time to time.

To perform a manual re-sync, select the SchindlerID System created, right click and select **Re-sync Cardholders**.

A re-sync occurs and the Schindler user database is updated to match the Command Centre database.



The Live Reporting Interface (plugin)

Introduction

The Live Reporting Interface builds an audit trail of Schindler access events in Command Centre, and enables Command Centre to receive non-badge card events from Schindler.

The Live Reporting Interface is an optional licensed plugin of Command Centre. This plugin must be installed on the middleware PC (PC hosting the FTCAPI Middleware Framework).

Installation

To install the Live Reporting Interface plugin, perform the following procedure:

1. Install the FTCAPI Middleware Framework on the middleware PC (if not already installed). Refer to the topic ***Installing the FTCAPI Middleware Framework*** (on page 24-7) for instructions.
2. Ensure your Command Centre licence file (CommandCentre.lic) contains the following entry:
   [Plugin]
   PluginX=SchindlerID-LifeReporting (where X is a number)
3. Run the installation executable **Gallagher Schindler Live Reporting Plugin-Setup 8.xx.xx.msi** on the middleware PC.
   This file can be found with the Command Centre installation files in the folder: Utilities\System Interfaces\Schindler\SchindlerLiveReportingPlugin
   Note: The FTCAPI Router Service restarts as part of the install.
4. To ensure that the Live Reporting plugin has installed correctly, select the Windows **Programs and Features** utility from the Windows/Control Panel. The program 'Gallagher Schindler Live Reporting Plug-in' should be listed as currently installed.

Configuration

To configure the Live Reporting Interface, perform the following procedures:

- ***Configuring an External System Server*** (on page 24-5)
- ***Configuring a Live Reporting External System*** (on page 24-44)
- ***Configuring External System Items (Floors)*** (on page 24-47)

Configuring a Live Reporting External System

Introduction

This topic describes how to create an External System (Live Reporting Interface) that will enable Command Centre to build an audit trail for lift access events. This External System is used to interface with the Logging Task Interface in Schindler.

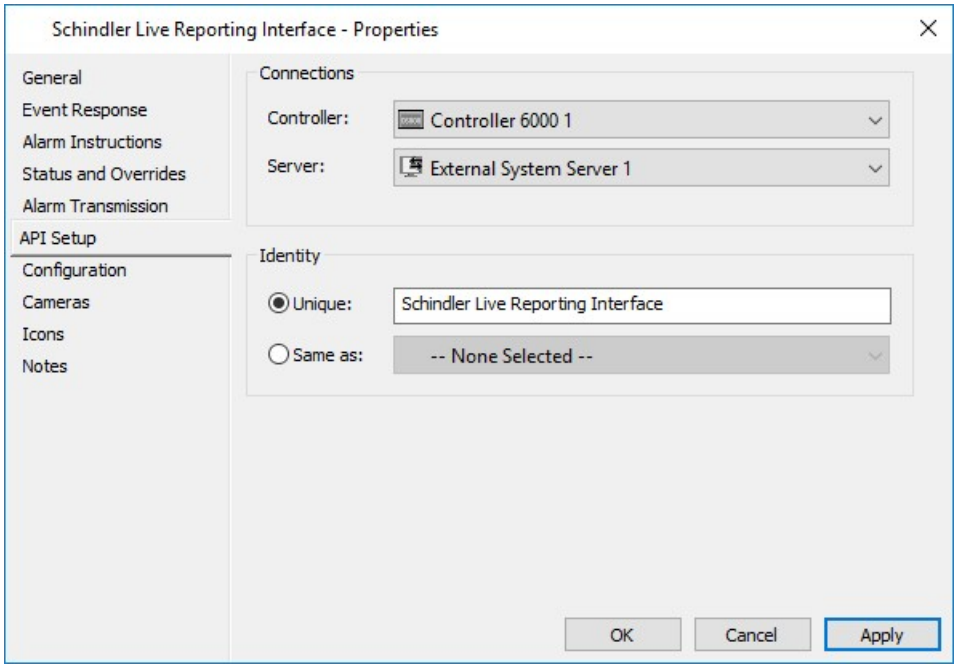
Note: Operators require the "Edit Site" operator privilege to be able to add, modify, and delete External Systems.

Before you begin

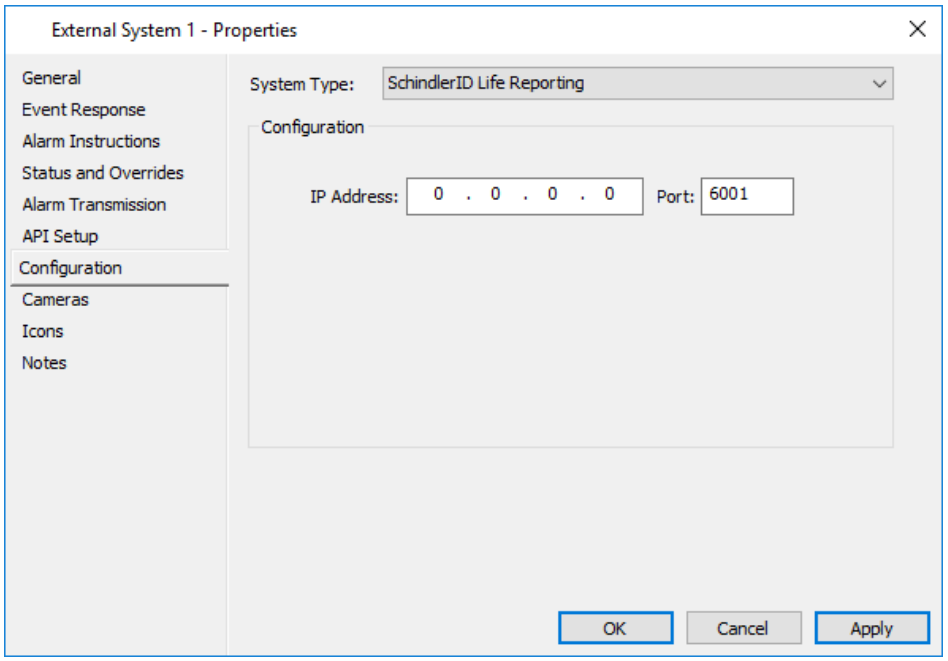
- Create the Logging Task Interface in Schindler.
- Request Schindler integrators to create a Logging Task Interface in Schindler, and provide the TCP/IP Port Number shown on the Logging Task Interface. This TCP/IP Port is required later in this procedure.

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...External 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 **API Setup** tab.



7. Select the appropriate **Controller** from the drop-down list.
   Note: Only standard Gallagher Controllers will work, (i.e. Gallagher UltraSec Controllers will not work).
8. Select the appropriate External System server from the **Server** drop-down list.
9. Click the **Unique** radio button in the 'Identity' section of this screen and type in a unique identity string. This field is limited to a maximum of 64 characters.
10. Click the **Configuration** tab.



11. Select the **SchindlerID Life Reporting** middleware plug-in from the **System Type** drop-down list.
    The 'Configuration' section this tab becomes populated accordingly.
12. Enter the Schindler server IP address in the **IP Address** field.
13. Enter the TCP/IP Port Number of the Schindler Logging Task Interface in the **Port** field. Range 0-65535.
    To enable Live reporting ensure the Logging of Personal Data is set to **Always** and the Live Reporting **Active** checkbox is ticked.
    Note: Schindler advises that storing the personal data may violate local laws. However, if the local laws are fulfilled and you want to log the personal data using the Live Reporting Interface, you need to select the option **Always** for Logging of Personal Data in the Logging Task Interface.
14. Click the **Icons** tab if you want to change the Icon Set for this external system.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
15. Click the **Notes** tab if you want to add a note(s) about this external system.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
16. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Configuring External System Items (floors)

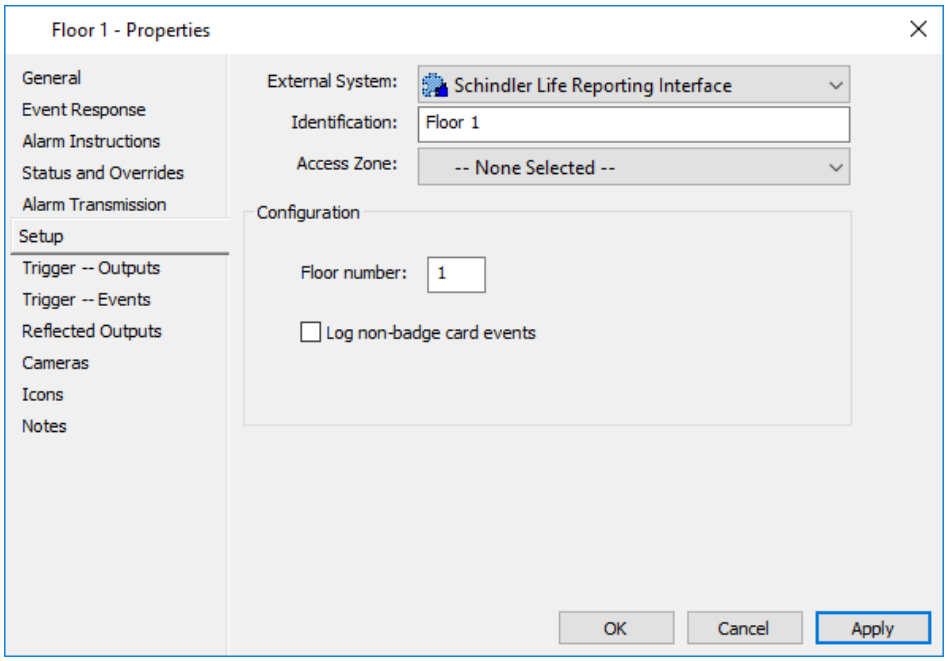
Introduction

An External System Item is required for each floor in the building. The External System Items represent Schindler floors in Command Centre. Live reporting events are logged against these floors.

Note: Operators require the "Edit Site" operator privilege to be able to add, modify, and delete External System Items.

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...External System Item**.
   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. Select the Schindler Life Reporting Interface **External System** from the drop-down list.

Note: If you do not select an External System, this External System Item will display at the root level of the **External Systems** List Window tree until it is assigned an External System as a parent.

8. Enter a string value in the **Identification** field, for example "Floor 1". **Note:** The Identification string entered is checked for uniqueness within the same External System. It is limited to 64 characters.
9. Enter the floor number in the **Floor number** field. This number must correspond to a floor in Schindler.
10. If required, check the **Log non-badge card events** checkbox. Selecting this option will enable Command Centre to receive 'non-badge card events' from Schindler.
    Note: A 'non-badge card event' is a Schindler allocation event that doesn't have an ID or person number, but has a destination floor.
11. Click the **Icons** tab if you want to change the Icon Set for this external system item.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
12. Click the **Notes** tab if you want to add a note(s) about this external system item.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
13. Click **OK** to exit and save your changes.
14. Repeat this procedure to configure an External System Item for each floor.

The Call Manager Interface (plugin)

Introduction

The Call Manager Interface enables Gallagher readers to be used at Schindler terminals to identify Cardholders in Schindler. The interface also enables Command Centre to set the status of a floor to 'Secure' or 'Free' via a schedule or operator override.

If you do not require this functionality, you don't need to create the Call Manager Interface, hence the information in this chapter is not applicable.

The Call Manager Interface is an optional licensed plugin of Command Centre. This plugin must be installed on the middleware PC (PC hosting the FTCAPI Middleware Framework).

Installation

To install the Call Manager Interface plugin, perform the following procedure:

1. Install the FTCAPI Middleware Framework on the middleware PC (if not already installed). Refer to the topic ***Installing the FTCAPI Middleware Framework*** (on page 24-7) for instructions.
2. Ensure your Command Centre licence file (CommandCentre.lic) contains the following entry:
   [Plugin]
   PluginX=SchindlerID-CallInterfac (where X is a number)
3. Run the installation executable **Schindler Call Interface Plug-in Setup 8.xx.xx.msi** on the middleware PC.
   This file can be found with the Command Centre installation files in the folder: Utilities\System Interfaces\Schindler\SchindlerCallInterfacePlugin
   Note: The FTCAPI Router Service restarts as part of the install.
4. To ensure that the Call Interface plugin has installed correctly, select the Windows **Programs and Features** utility from the Windows/Control Panel. The program 'Gallagher Schindler Call Interface Plug-in' should be listed as currently installed.

Configuration

To configure the Call Manager Interface, perform the following procedures:

- ***Configuring a Call Manager External System*** (on page 24-50)
- ***Configuring External System Items (Terminals)*** (on page 24-53)
- ***Configuring a Schindler Alarm Zone*** (on page 24-55)
- ***Configuring Schindler Action Plans*** (on page 24-55)
- ***Configuring Schindler Readers*** (on page 24-56)
- ***Configuring Schindler Dummy Doors*** (on page 24-56)

Configuring a Call Manager External System

Introduction

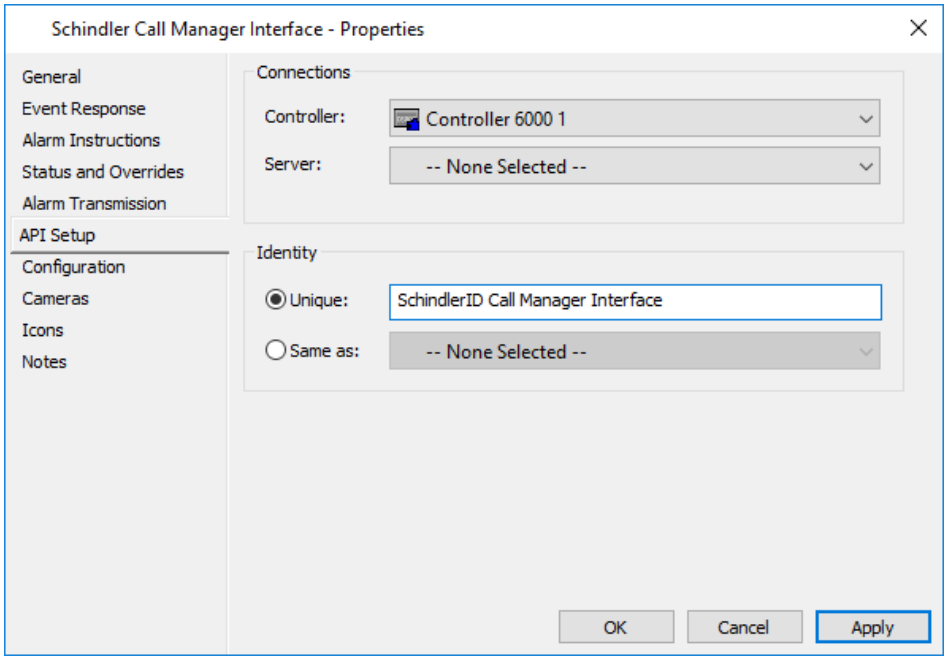
This topic describes how to create a Schindler Call Manager External System.
Note: Operators require the "Edit Site" operator privilege to be able to add, modify, and delete External Systems.

Before you begin

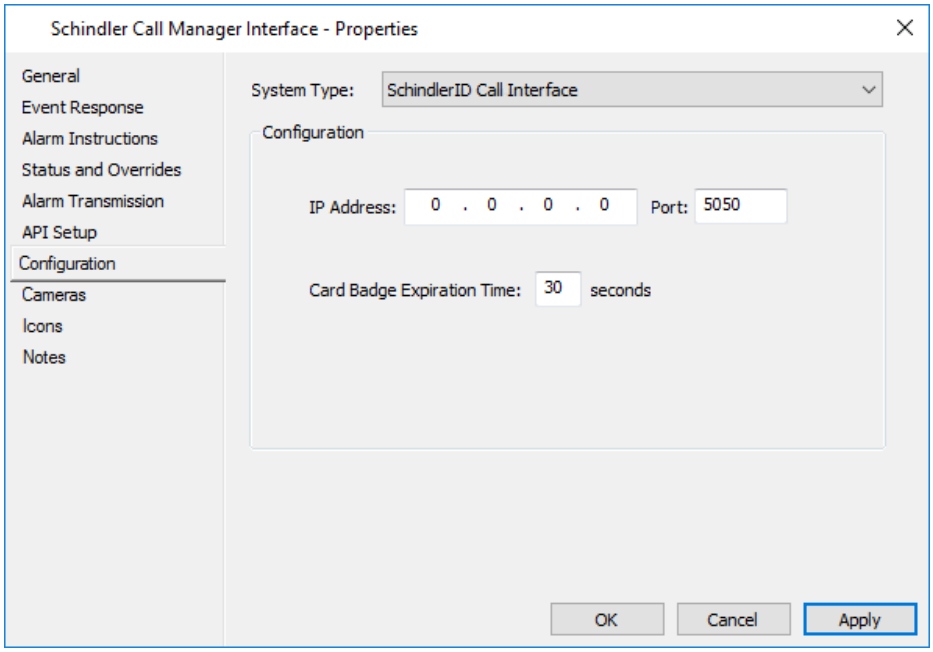
Request Schindler integrators to create the Call Manager Interface in Schindler, and provide the TCP/IP Port Number of the Schindler Call Manager Interface shown in the Port field.

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...External 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 **API Setup** tab.



7. Select the appropriate **Controller** from the drop-down list.
   Note: Only standard Gallagher Controllers will work, (i.e. Gallagher UltraSec Controllers will not work).
8. Select the appropriate External System server from the **Server** drop-down list.
9. Click the **Unique** radio button in the 'Identity' section of this screen and type in a unique identity string. This field is limited to a maximum of 64 characters.
   Note: Should you have more than 100 terminals, click the **Same as** radio button and link the identity of this terminal to be the same as another by selecting a terminal from the drop-down list.
10. Click the **Configuration** tab.
    Note: This tab only appears if the 'Identity' on the **API Setup** tab is set to 'Unique'.



11. Select the **SchindlerID Call Interface** middleware plug-in from the **System Type** drop-down list.
    The 'Configuration' section this tab becomes populated accordingly.
12. Enter the Schindler server IP address in the **IP Address** field.
13. Enter the TCP/IP Port Number of the Schindler Logging Task Interface in the **Port** field. Range 0-65535.
14. If required, enter a **Card Badge Expiration Time**. Range 1-600 seconds.

    If a user badges his/her card, this information is sent from the Controller to the Middleware Framework. The time between the information being sent, is checked by the Middleware Framework. If this time exceeds the Card Badge Expiration Time, the terminal is not enabled and an event is logged, as it assumes a network delay has occurred and the person may no longer be at the terminal.

15. Click the **Icons** tab if you want to change the Icon Set for this external system.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
16. Click the **Notes** tab if you want to add a note(s) about this external system.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
17. 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 External System Items (terminals)

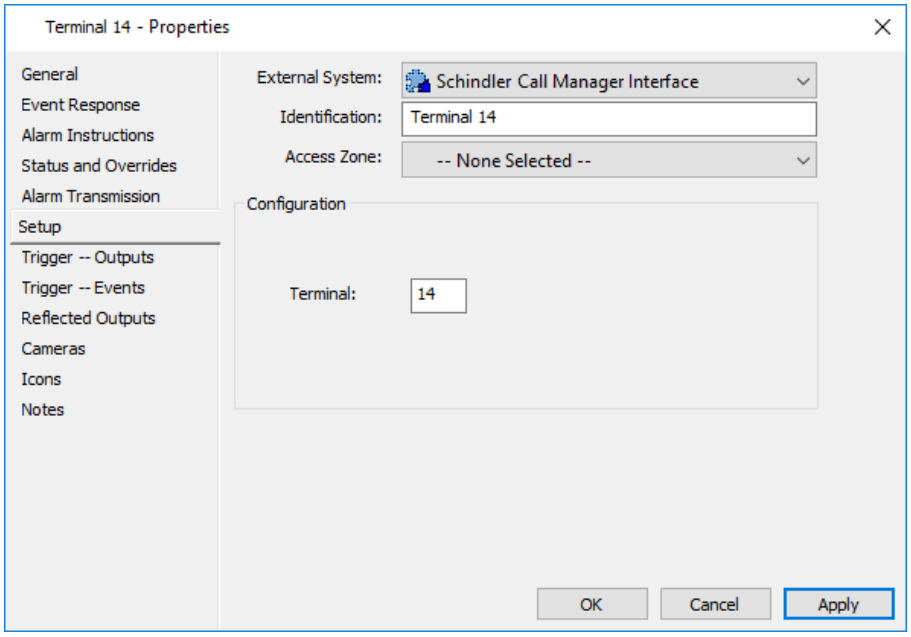
Introduction

An External System Item is required for each terminal in the building. The External System Items represent Schindler terminals in Command Centre. A building may have more than one terminal per floor.
IMPORTANT: Contact Schindler integrator to obtain the Terminal IDs in Schindler.

Note: Operators require the "Edit Site" operator privilege to be able to add, modify, and delete External System Items.

Procedure

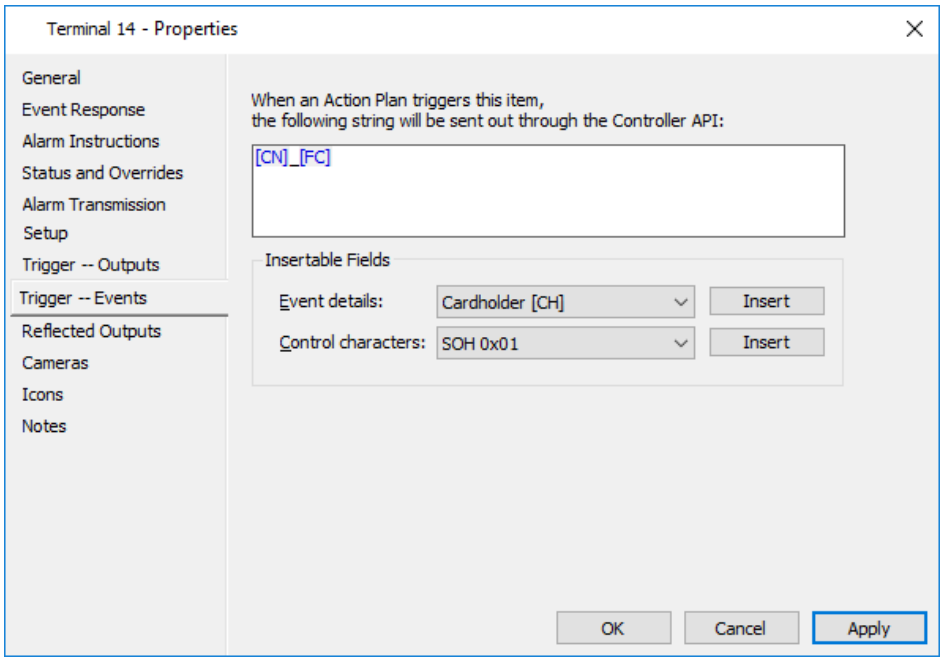
1. Click **Configure** from the menu bar, then **External Systems**.
   The **External Systems** List Window opens (in tree view).
2. **Right click** and select **New...External System Item**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General 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. Select the Schindler Call Manager Interface **External System** from the drop-down list.

Note: If you do not select an External System, this External System Item will display at the root level of the **External Systems** List Window tree until it is assigned an External System as a parent.

8. Enter a string value in the **Identification** field, for example "Terminal 14".
   Note: The Identification string entered is checked for uniqueness within the same External System. It is limited to 64 characters.
9. Enter a Terminal ID in the **Terminal** field. This Terminal ID must match a Terminal ID in Schindler. Range 0-255. The origin of this range limit is in the Schindler External Call Manager Settings.
10. Click the **Trigger -- Events** tab.



11. Select **Card Number [CN]** from the Event Details drop-down list and click **Insert**.
12. Type an underscore then select **Facility Code [FC]** from the Event Details drop-down list and click **Insert**.
    Note: Manually typing in [CN] and [FC] will result in a error message, later on.
13. Click the **Icons** tab if you want to change the Icon Set for this external system item.
    For further details regarding the **Icons** tab, see Icons.
14. Click the **Notes** tab if you want to add a note(s) about this external system item.
    For further details regarding the **Notes** tab, see Notes.
15. Click **OK** to exit and save your changes.
16. Repeat this procedure to configure an External System Item for each terminal in the building.

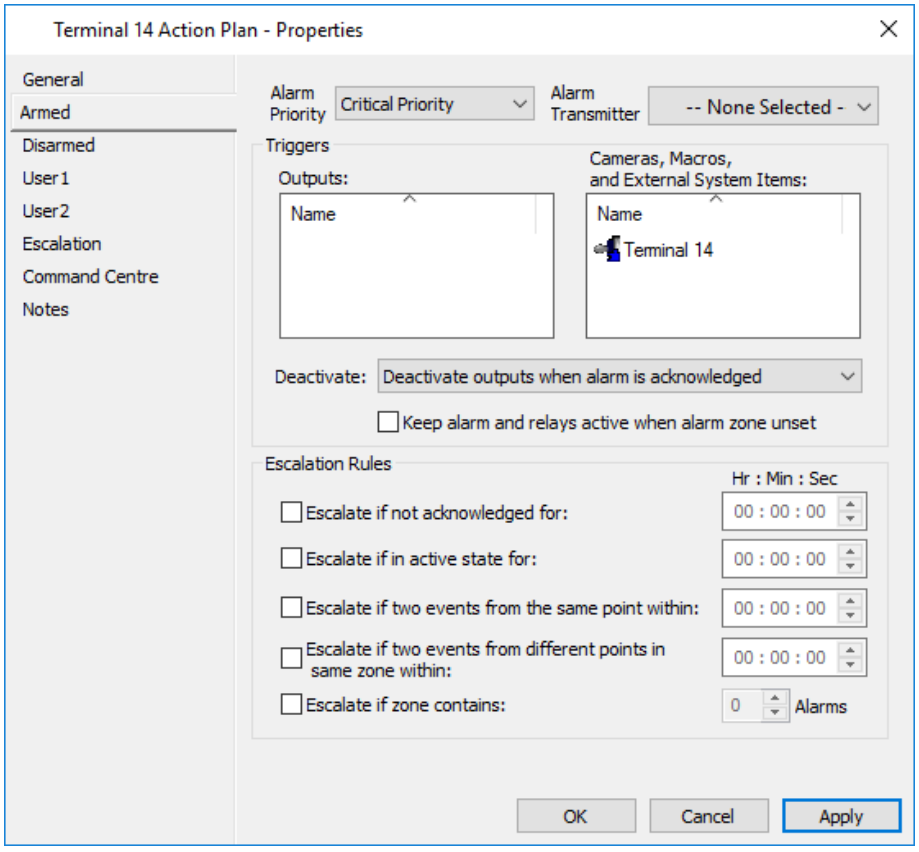
Configuring a Schindler Alarm Zone

Create an Alarm Zone. Refer to the topic ***Setting up Alarm Zones*** (on page 14-3). Name the Alarm Zone 'Schindler Alarm Zone'. Assign the 'Schindler Alarm Zone' to all Schindler items.

Configuring Schindler Action Plans

A Schindler Action Plan is required to associate the dummy door (yet to be created) with the External System Item (terminal). An Action Plan is required for each terminal in the building.

1. Click **Configure** from the menu bar, then **Action Plans**.
   The **Action Plan** List Window opens (in grid view).
2. **Right click** and select **New...Action Plan**.
   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 **Armed** (or **Set**) tab.
   These settings define the responses when the item is linked with the Armed Alarm Zone.



5. Select **Not an Event** from the Alarm Priority drop-down list.
   Note: Ensure the Action Plan has an Alarm Priority that is set to 'Not an Event' otherwise you will get a lot of unnecessary events about access through the door. For debugging during the installation it may be useful to configure the priority to 'Message Only'.
6. Drag and drop the External System Item (terminal) to be triggered into the **Cameras, Macros and External System Items** grid, (e.g. Terminal 14).
7. Click the **Disarmed** tab and repeat steps 5-6. These settings define the responses when the item triggering the Action Plan is in the disarmed state.
8. Repeat steps 5-6 for the next two tabs also, (i.e. **User 1** and **User 2** tabs).
9. Click the **Notes** tab if you want to add a note(s) about this Action Plan. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
10. Click **OK** to exit and save your changes.
11. Repeat this procedure to create an Action Plan for each terminal in the building.

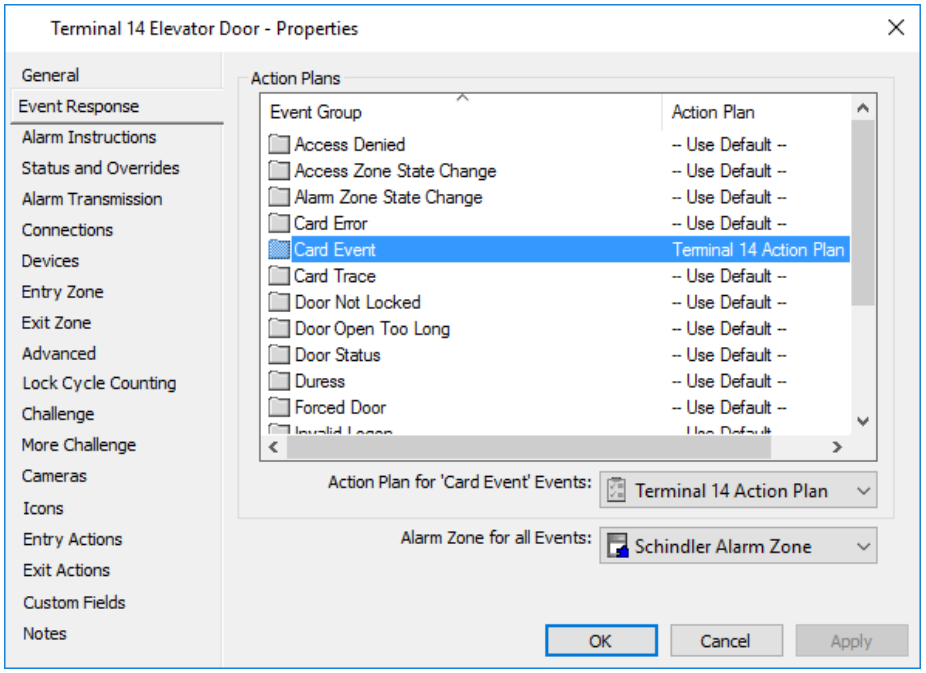
Configuring Schindler Readers

Create the readers required for this integration. Refer to the topic ***Creating Readers*** (on page 21-57)

Configuring Schindler Dummy Doors

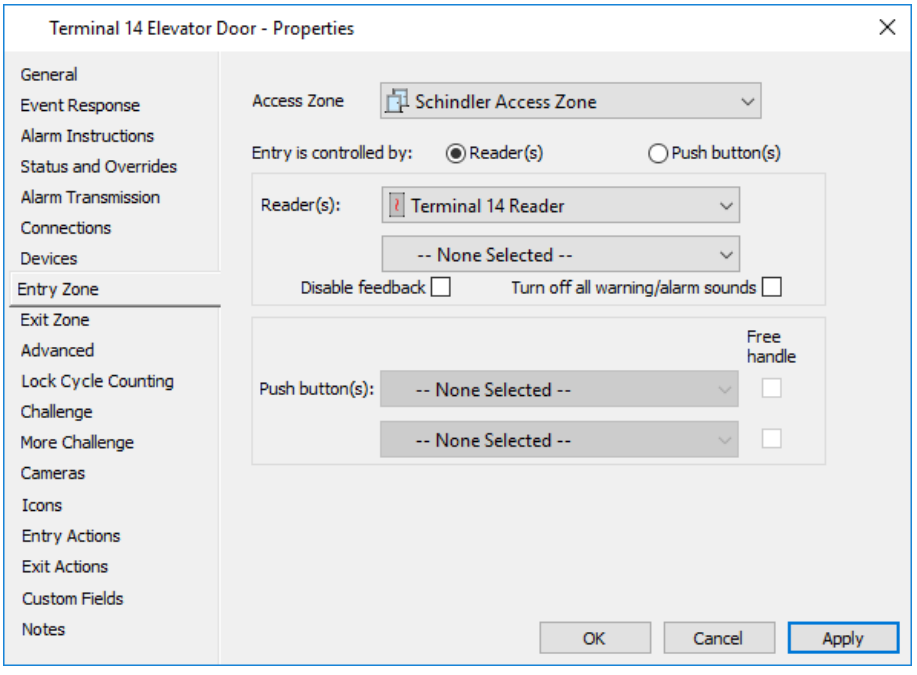
A dummy Door is required for each terminal in the building.
Note: You do not need to create a dummy door for simulated terminals, used to control the secure/free state of floors.

1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens (in grid view).
2. **Right click** and select **New...Door**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Event Response** tab.



5. Select the **Card Event** Event Group and assign the Action Plan created for the terminal corresponding to this dummy door.
6. Select an **Alarm Zone** from the drop-down list that is common to all terminals in the Schindler system.

   Note: Doors must be placed into an Alarm Zone before you will receive Door Events.
7. Click the **Connections** tab and assign the door to the Controller that will host this door. This should be the same Controller assigned to the External System Item representing each terminal.
8. Click the **Entry Zone** tab.



9. Select an **Access Zone** from the drop-down list. Ensure the Schindler Access Zone Schedule (previously created) is assigned to the zone, and that Cardholder Access to this zone is 'Secure - No PIN' at all times.
10. From the **Reader(s)** drop-down list, select the appropriate reader that provides entry for this terminal.
11. Click the **Icons** tab if you want to change the Icon Set for this Door.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
12. Click the **Notes** tab if you want to add a note(s) about this Door.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
13. Click **OK** to exit and save your changes.
14. Repeat this procedure to configure a dummy door for each terminal in the building.

Configuring Secure/Free Floors

The secure/free floor component of the Call Manager Interface enables an operator to either secure or free a floor.

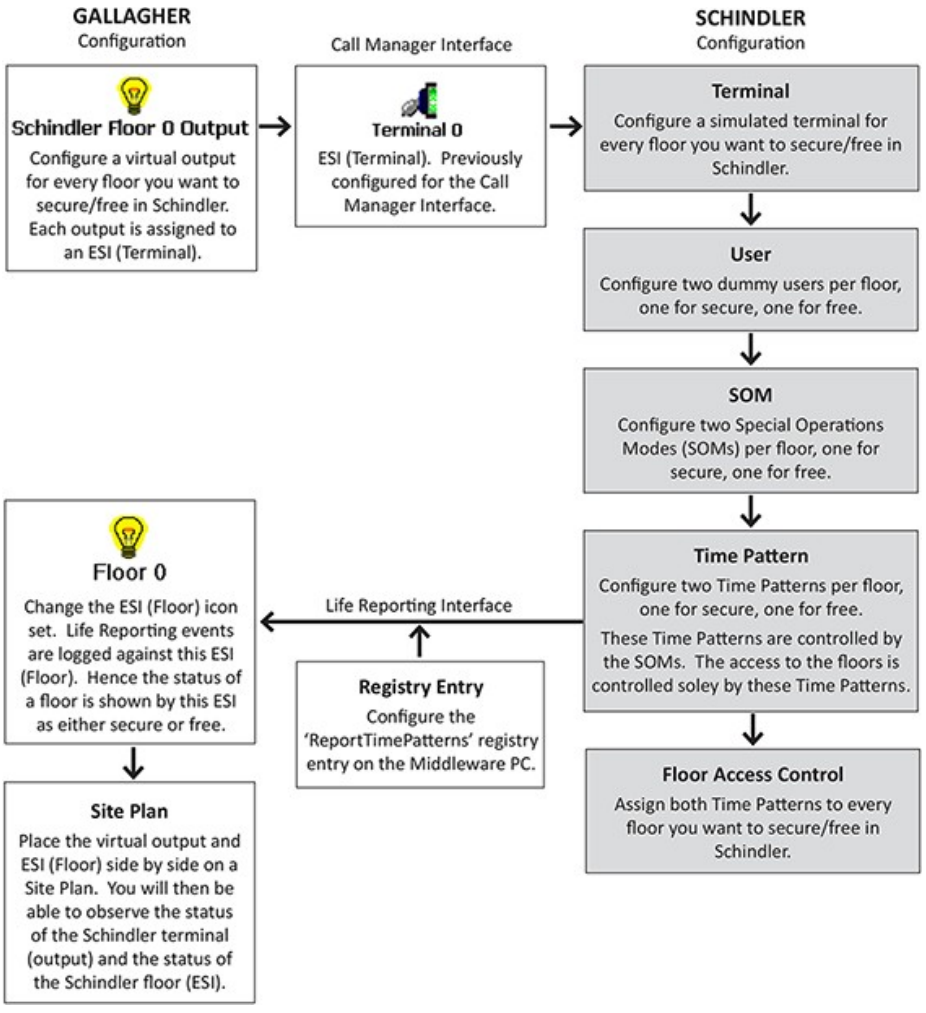
Secure: A valid access card is required in order to gain access to the floor.

Free: An access card is not required.

Configuration Process

Command Centre doesn't control the state of the floors directly. Instead Command Centre uses Schindler Special Operation Modes (SOMs) that control the Time Patterns assigned to the floors in Schindler. Therefore, the proper functionality depends on the correct configuration of these Schindler items.

The following diagram provides an overview of the configuration process you will need to follow in order to secure/free floors. This process identifies the various items you will need to configure in both Command Centre and Schindler.



Notes:

- This configuration process has been tested and is a suggestion as to how Schindler can be configured to secure/free floors. Your configuration of Schindler may vary, depending on your requirements.
- Schindler integrators should configure the Special Operations Modes, provide their names to Gallagher integrators.
- An additional configuration option (schindler_zone_status_delay_ milliseconds) exists in the Schindler plugin configuration file 'SchindlerPlugin.config'. This option adds a delay between each zone change message/command sent from Command Centre to Schindler, to help mitigate queue overload. For details about the configuration file, refer to the document *"Release Note Schindler Call by Profile (v8.xx)"* located on the Command Centre installation media.

Configuration Procedures

To configure secure/free floors, perform the following procedures in the order listed below.

In Schindler:

- ***Configuring Time Patterns*** (on page 24-61)
- ***Configuring Floor Access Requirements*** (on page 24-61)
- ***Configuring Special Operation Modes (SOMs)*** (on page 24-61)
- ***Configuring Dummy Users*** (on page 24-61)
- ***Configuring Simulated Terminals*** (on page 24-61)

On the Middleware PC:

- ***Configuring the 'ReportTimePatterns' Registry*** (on page 24-62)

In Command Centre:

- ***Configuring a Virtual Output for each Floor*** (on page 24-63)
- ***Assigning each Virtual Output to an ESI (terminal)*** (on page 24-65)
- ***Configuring a Site Plan for Secure/Free Floors*** (on page 24-65)

Configuring Time Patterns

Contact Schindler integrator to configure time patterns as required.

Configuring Floor Access Requirements

Contact Schindler integrator to configure floor access requirements.

Configuring Special Operation Modes (SOMs)

Contact Schindler integrator to configure Special Operation Modes as required.

Configuring Dummy Users

Note: Before creating dummy users, Schindler integrators need to create an Access Profile (Allow All). This profile will allow access to all zones in the building. Contact Schindler integrator to configure dummy users.

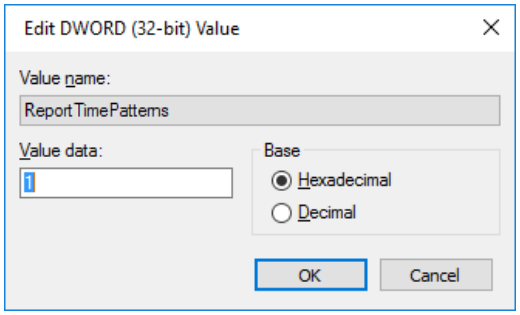
Configuring Simulated Terminals

For every floor you want to Secure/Free in Schindler, you will need to create a simulated terminal. Contact Schindler integrators to create simulated terminals as required.

Configuring the 'ReportTimePatterns' Registry

To enable Time Pattern status reporting you will need to create the registry entry 'ReportTimePatterns' on the middleware PC.
To create the 'ReportTimePatterns' registry, perform 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
   Note: If using a 64 bit system, browse to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GALLAGHER\Command Centre
4. Right click, and then click **New** from the drop-down menu. Another drop-down menu displays. Click **DWORD Value**. Your new DWORD Value is populated at the bottom of the registry values list.
5. Enter the DWORD Value name 'ReportTimePatterns'.
6. Double-click your newly created DWORD Value.
   The **Edit DWORD Value** window displays.

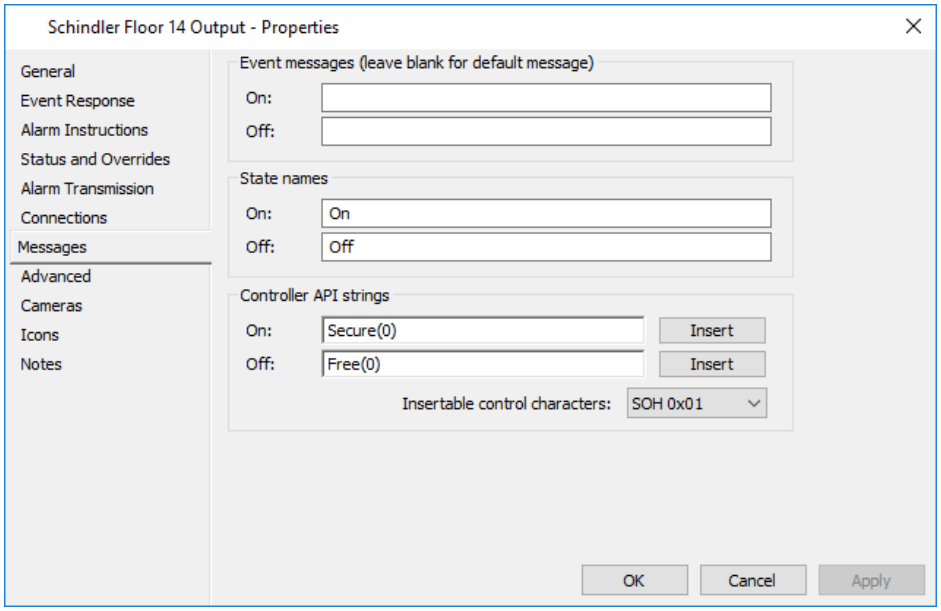


7. Select **Decimal** as the Base then enter a value, (e.g. 1) and click **OK**.
   Note: If a value is not entered or the 'ReportTimePatterns' entry is not defined, Time Pattern status reporting will not be supported.

Configuring a Virtual Output for each Floor

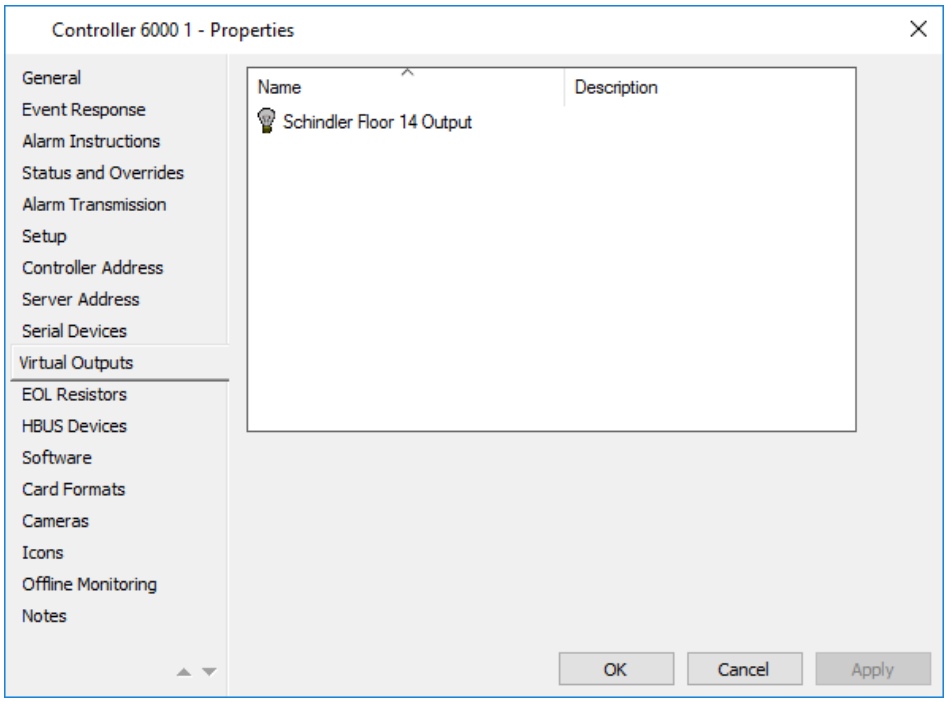
You will need to create a Virtual Output for each floor you wish to secure/free.
To create a Virtual Output, perform the following procedure:

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** and select **New...Output**.
   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 **Messages** tab.



6. To configure the Output to on:
   Enter the **Personal Number** of the dummy user (to **Secure** the corresponding floor) configured in Schindler into the FT Controller API String 'On' field, e.g. Secure(0).
7. To configure the Output to off:
   Enter the **Personal Number** of the dummy user (to **Free** the corresponding floor) configured in Schindler into the FT Controller API String 'Off' field, e.g. Free(0).
8. Click **OK** to exit and save your changes.
9. From the **Hardware** List Window, open the Controller that the Virtual Output is to be assigned to.

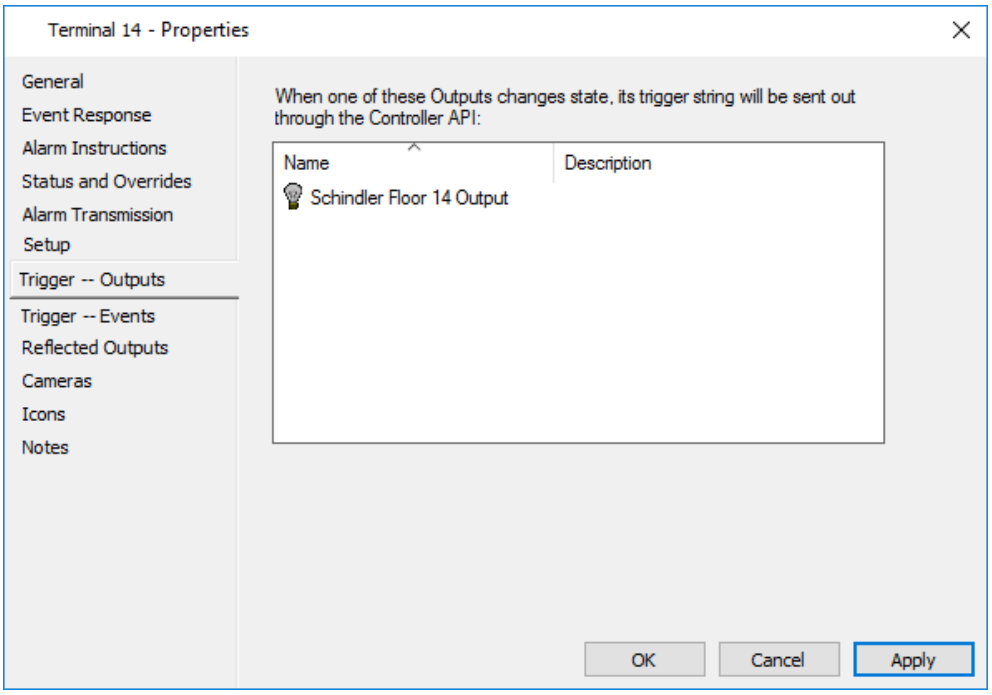
10. Click the **Virtual Outputs** tab.



11. Drag and drop the Virtual Output you have just created into the grid on this screen.
12. Click **Apply**.
13. Repeat this procedure to configure a Virtual Output for each floor you wish to secure/free.

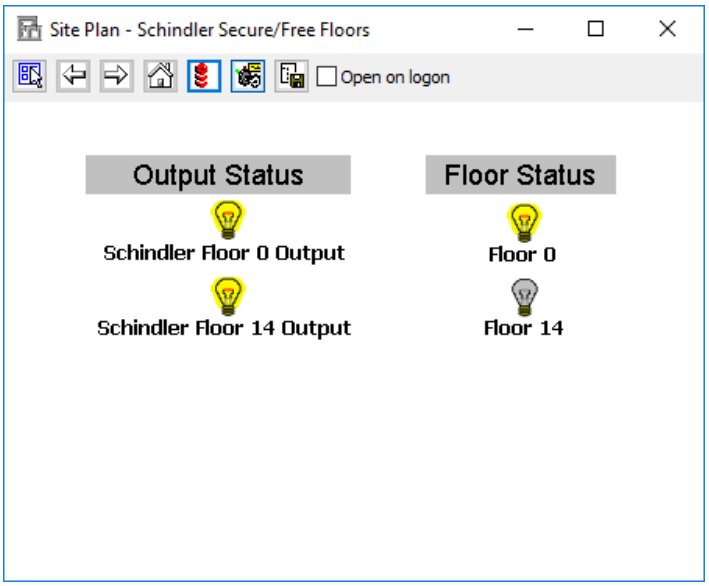
Assigning a Virtual Output to an ESI (terminal)

You would have already configured the External Systems Items (terminals). Assign each Virtual Output (previously configured) to the **Trigger -- Outputs** tab of the External System Item (terminal) for the corresponding floor.



Configuring a Site Plan for Secure/Free Floors

Drag the External System Item (floor) onto a Site Plan beside the Virtual Output. When placed on the Site Plan side by side, it is easily seen whether the Free/Secure action succeeded or whether it needs to be repeated.



If all goes fine, the status of the virtual output will match the status of the External System Item (floor).

If a user overrides a Virtual Output at the moment when the Schindler simulated terminal is still processing the previous request (and therefore the latter one is thrown away), the status of the External System Item (floor) reflects the last successful change, therefore differs from the External System Item (terminal) status, and this way informs the operator that he/she should repeat the action.

Note: In the example above, the Output Icon Set has been applied to the External System Items (floors). This enables you to view the status of a floor easily, when the External System Item (floor) is added to the Site Plan. Refer to the topic Creating a new Icon Set for further details.

Schindler Event Reporting

Select the appropriate Schindler reporting option.

- If the 'Report an error' option is selected, and a Cardholder has two cards assigned, then only one user will be imported into the Schindler database. This user will have the badge numbers assigned. The second user will not be imported because the badge numbers are already assigned to the first user. The event 'Card already assigned' is logged in Command Centre.
- If the 'Leave the card assigned to the existing user' option is selected and a Command Centre Cardholder has badge numbers assigned that match the badge numbers of an existing Schindler user, then the Command Centre Cardholder's badge numbers will not be imported. No event is logged in Command Centre.
- If the 'Assign the card to the new user' option is selected and a Command Centre Cardholder has badge numbers assigned that match the badge numbers of a Schindler user, then the badge numbers are removed from the Schindler user and assigned to the Command Centre Cardholder. No event is logged in Command Centre.

Troubleshooting

- Where Gallagher readers on a Controller are connected to the elevator terminals it is recommended that the maximum Controller loading is no more than 2 card events per second. This is the sum of the card events for all connected readers.
- A Schindler Call Manager can handle only one connection. Several Call Managers can be created in Schindler. Command Centre is able to connect to several Schindler systems. In such a case several External Systems (Call Interfaces) are created in Command Centre. Command Centre is not supposed to connect to several Call Managers of the one Schindler system. Another Call Manager in the Schindler system would be needed, if there is yet another system besides Command Centre that is going to call the lifts.
- When a terminal is processing a request, the terminal will not accept any other requests until such time as the original request is processed.
- If a Time Pattern is deleted you will also need to delete the SOM related to it. When creating the Time Pattern again, you will need to create a new SOM. If you don't do this, you may find that the behaviour of the SOM is inconsistent.
- If a Time Pattern is deleted, an alarm is raised advising the operator that one of the Time Patterns is not defined. If the alarm is acknowledged it will not be raised again, (e.g. When an override is performed on the Output the alarm is not raised again).
- If the middleware services or the Schindler system are disconnected from the network and both Time Patterns are deleted from a floor, then Command Centre will not report the Time Pattern deletion.

Adding external systems to a Site Plan

Introduction

External systems, like other site items, can be displayed on Site Plans.
Operators require the “Edit Site” operator privilege to perform this procedure.

Procedure

1. Open the Site Plan you wish to add the external system to.
   Note: The Site Plan needs to be in “Edit” mode, (i.e. have a red line border around it), to add an item to it.
2. Click the  Site Plan editing icon to change to “Edit” mode if necessary.
3. Click **Configure** from the menu bar, then **External Systems**.
   The **External Systems** List Window opens (in tree view).
4. Select the item you want to add to the Site Plan, and drag and drop it onto the Site Plan.
5. **Close** the Site Plan.
6. A confirmation window displays.
   Click **Yes** to save your changes.

Result

The external system has been added to a Site Plan.

Hint

External systems can also be added to Site Plans from the Find Tool.

Chapter 25: Logic Blocks and Virtual Outputs

Introduction

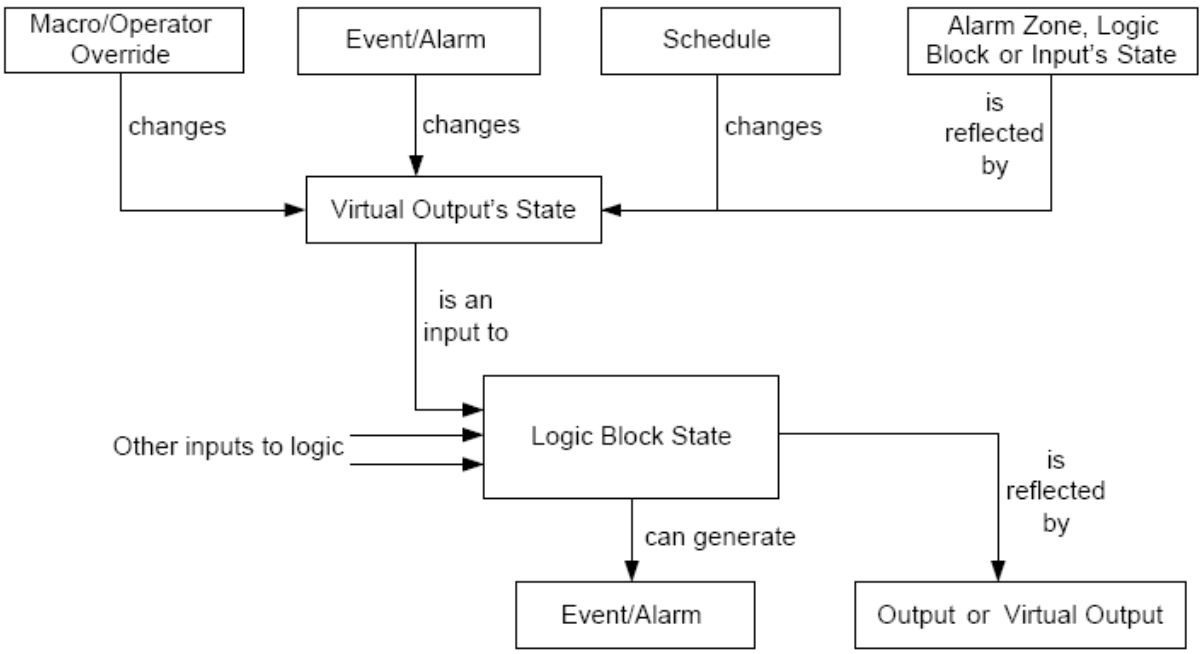
Logic Blocks and Virtual Outputs provide building blocks that can be used to provide custom functionality not otherwise supported by Command Centre, or which is difficult to achieve using existing higher-level features.

Virtual Outputs

Virtual Outputs are one of the items on which logic blocks can be based.
A Virtual Output provides a means to base logic on the following, without the cost of using real outputs:

- the state of an alarm (active or inactive), by using the virtual output as an alarm output, or
- the time of day, by scheduling the virtual output's state, or
- an operator override, by allowing an operator to override the state of the virtual output, or
- the state of an Alarm Zone, by configuring the virtual output as a reflect output for an Alarm Zone state

The Virtual Output's purpose is summarised in the following diagram:



Logic Blocks

A Logic Block's state is either "on" or "off". Logic Blocks contain a set of rules and a timing option. When a rule is met, (meaning all the items in the rule are

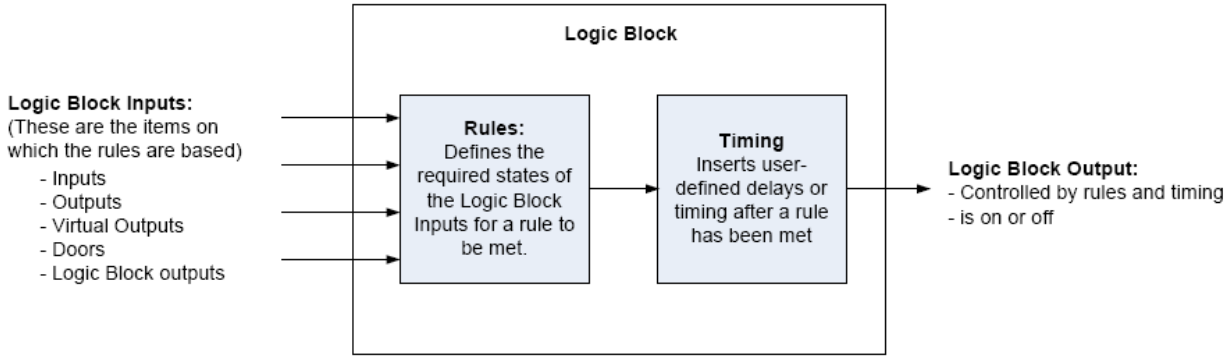
in the state defined in the rule), the Logic Block can indicate this by turning on. Exactly when the Logic Block turns on is also controlled by the timing option. The timing options available are:

- Logic Block follows the rules explicitly
- Logic Block follows rules, with a maximum on time
- Logic Block is pulsed when the rules are met
- Logic Block output has a delayed off time
- Logic Block output has a delayed on time
- Logic Block is latched until cleared by an input

The Logic Block's state can generate events or alarms, and can drive outputs, (e.g. controlling lights or sirens).

A Logic Block can be used in place of an input anywhere with Command Centre that an input can currently be selected, with the exception of where inputs are associated with the hardware on which they reside, or where they are associated with a Terminal, or as a camera motion detection input.

The Logic Block is turned on when a set of system conditions that are defined by the user, are met. In overview, the Logic Block is as follows:



Logic Block rules

1. A Logic Block rule specifies:
   - the set of items on which the rule is based, and
   - the required state of each item, for the rule to be met.
2. The items and states on which a rule can be based are:

Item	States
Input	Open, Closed
Output	On, Off
Logic Block Output	On, Off
Door	Free, Secure
Virtual Output	On, Off

A Door's state is **free** if it remains unlocked in between authorised entries and exits.

A Door's state is **secure** if it is locked in between authorised entries and exits.

Note: An Output's **Mapping to an Input state** setting is not applicable when the Output is used as a Logic Block rule item.

3. Each Logic Block can have up to 10 items on which the rules are based.
4. A Logic Block can have multiple rules. Up to 10 rules are allowed within a single logic block. Any rule can be based on a subset of the items which are inputs to the Logic Block (and hence to other rules).
5. The state of the Logic Block is controlled by the combination of the rules and the timing options that have been defined, unless its state is overridden (to disable the logic).
6. A Logic Block's state is either on or off.
7. A Logic Block operates as follows:
   The Logic Block's state is **on** when one or more rules are met, (i.e. all the inputs to a rule are in the states defined in the rule), and the timing options have been applied. At all other times, the Logic Block output is **off**.

Select the item below that you require further detail on:

- ***Scenarios using Logic and Virtual Outputs*** (on page 25-4)
- ***Creating a new Logic Block*** (on page 25-15)
- ***Creating a new Virtual Output*** (on page 25-21)

Scenarios using Logic and Virtual Outputs

The following scenarios provide worked examples of possible uses for logic blocks:

- ***Scenario 1: Disabling Access Zone pushbuttons during lockdown*** (on page 25-5)
- ***Scenario 2: Perform 'Open Door Override' during lockdown*** (on page 25-6)
- ***Scenario 3: Restricting access at multi-tenanted car-parks*** (on page 25-7)

Scenario 1: Disabling Access Zone pushbuttons during lockdown

Scenario

Disabling push-button entry and exit, or remote release push-buttons while an Access Zone is locked down. This assumes either a keyswitch or operator overrides can be used for initiating and cancelling a lockdown.

Solution

This can be achieved with the following set up:

a) Operators place an Access Zone into lockdown by running a 'Lockdown' macro. The macro is configured to override a virtual output to on when the Access Zone is locked down, as well as performing the Access Zone lockdown override.

b) Operators cancel a lockdown on an Access Zone by running a 'Cancel lockdown' macro. The macro is configured to override the virtual output (as in **a.**) to off, as well as cancelling the Access Zone lockdown.

c) If the Access Zone is locked down using an input, then the 'input closed' event is configured to run the 'Lockdown' macro, via an action plan, and the 'input open' event is configured to run the 'Cancel lockdown' macro, via a different action plan. This means, the virtual output in **a.** and **b.** provides lockdown status - it is on when the Access Zone is locked down and off when the Access Zone is not locked down.

d) Configure each of the push-button entry, exit or remote release inputs in Command Centre as a logic block (rather than the real inputs). The logic is configured to be on when the real push button entry/exit or remote release input is closed and the Access Zone is not locked down (i.e. the virtual output in **a.** is off). The logic block 'on' is mapped to 'input closed', and used as the entry/exit button or remote release input.

This configuration means that pushing the push-button entry/exit or remote release inputs will have no effect when the Access Zone is locked down, but will open the door at all other times. Note this is just one configuration using logic and virtual outputs that would provide this functionality - there are other similar configurations which would achieve the same effect.

Scenario 2: Perform 'Open Door Override' during lockdown

Scenario

Any operator can perform an open door override when the Access Zone is not locked down. A subset of these operators (the 'higher privileged operators') can perform an open door override whether or not the Access Zone is locked down.

Solution

This can be achieved with the following set up:

a) The 'Open Door Override' privilege is given only to the higher privileged operators - those who can perform open door overrides whether or not the Access Zone is locked down.

b) For lower privileged operators, an 'Open Door' macro is placed on a Site Plan (or in Status Viewer). All operators are given the privilege to run this macro. The macro is configured to override a virtual output to on for 4 seconds (I'll call this 'Output A'). The same virtual output as used in Scenario 1, is also set up so that it is on when the Access Zone is locked down, and off at all other times (I'll call this 'Output B').

c) The remote release input on the door is set up as a logic block. The logic block is configured so that it is on when Output A is on and Output B is off, (i.e. when an operator has run the 'Open Door' macro and the Access Zone is not locked down). The logic block 'on' is mapped to 'input closed'.

This configuration means when the 'Open Door' macro is run it will unlock the door, via the use of logic and the remote release input, only if the Access Zone isn't locked down. Note that this solution doesn't use an open door override for the lower privileged operators, so the event log will only show the macro being run and in some cases the logic block changing state, and hence the door opening.

Scenario 3: Restricting access at multi-tenanted car-parks

Scenario

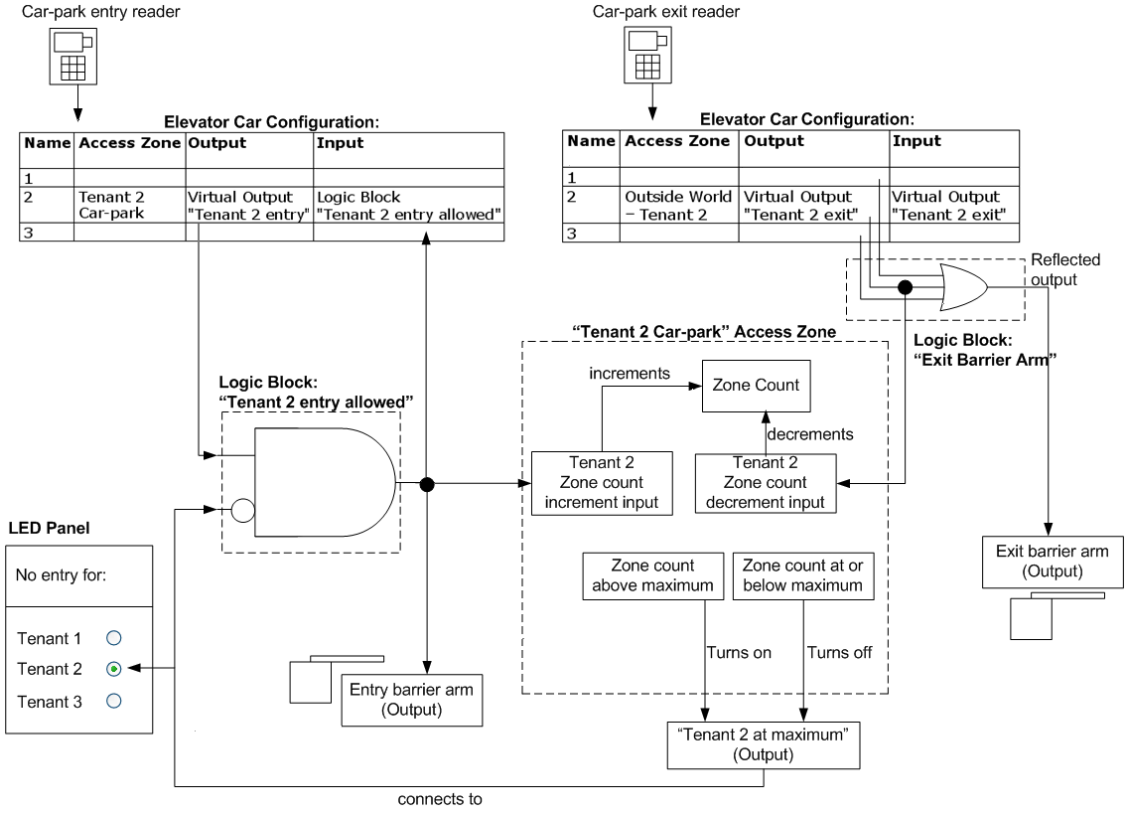
A car-park caters for a multi-tenanted building. Each tenant has a maximum number of car-parks allocated for their use. When the maximum number of car-parks allowed for a particular tenant is reached, other cardholder access attempts (by that tenant) are denied. Once a cardholder leaves, access to the car-park is re-enabled for that tenant (until such time as the maximum allowed car-parks is again reached). For this example it is assumed there are three tenants, although the proposed solution can cater for up to 75 tenants.

When a particular tenant has reached the maximum allowed car-parks, an LED is lit on a mimic panel. This provides an indication to other tenants that they will be unable to gain access. Once a person leaves, and a car-park for that tenant is then available, the LED turns off, and access to the car-park (for that tenant) is re-enabled. There is a separate LED for each tenant.

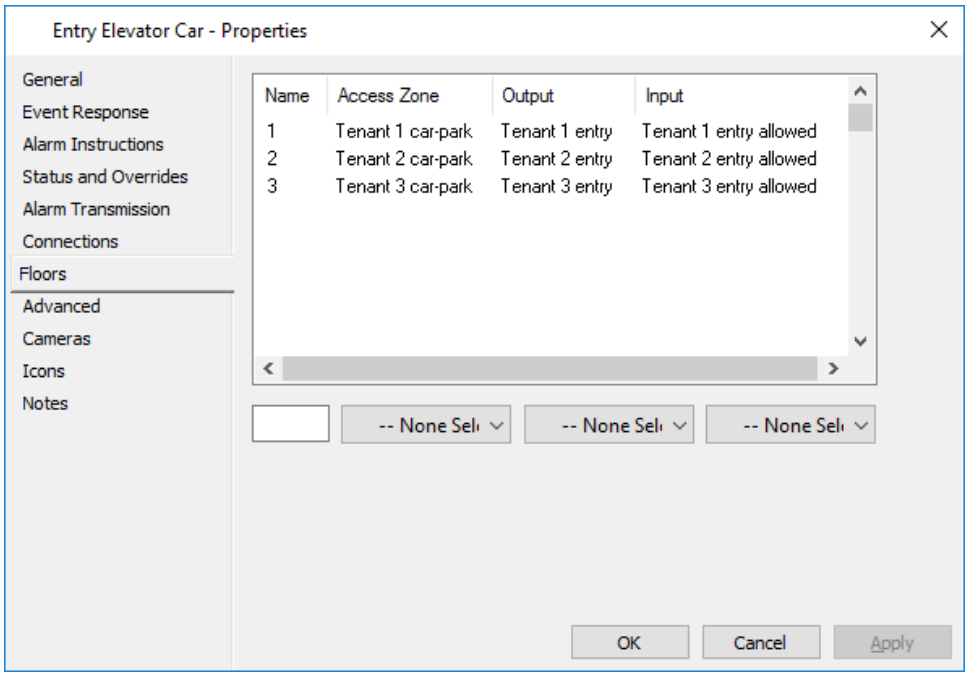
Solution: Using Elevator Cars, Virtual Outputs, Logic Blocks and Zone counting

The purpose of this configuration is to use zone counting on Tenant 1, Tenant 2 and Tenant 3 car-park Access Zones to count the number of cardholders currently in the car-park, for each tenant, and to deny further entry to that tenant once the maximum allowed car-parks have been used.

The following diagram gives an overview of the configuration described below:



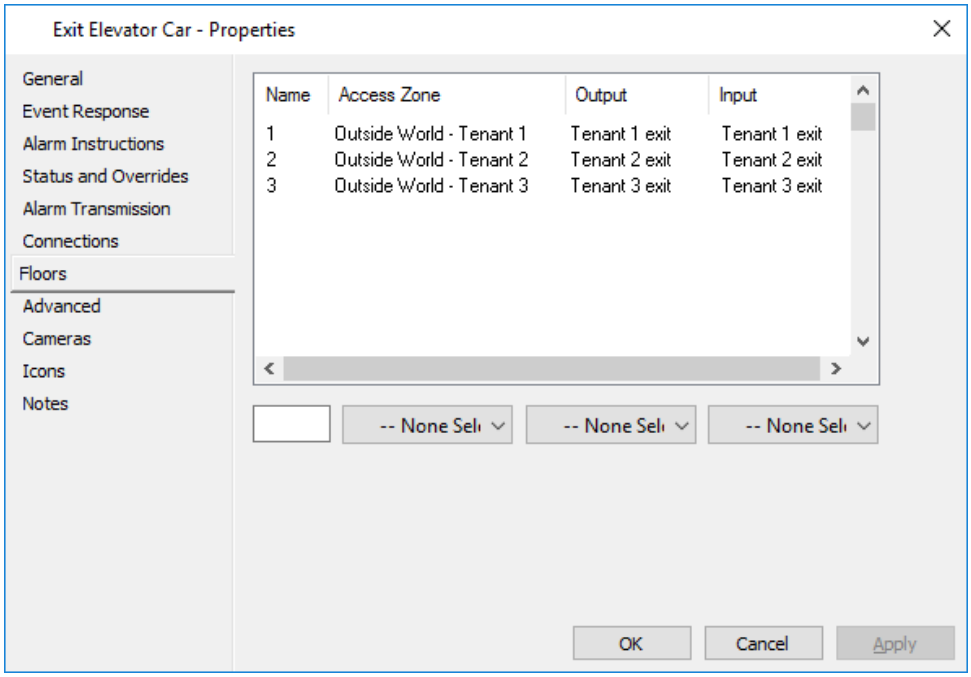
1. The entry to the car-park is controlled by a reader, which is configured as an elevator car reader. Exit from the car-park is also controlled by a reader, which is configured as a (different) elevator car reader.
2. The entry elevator car controls entry to three "levels". Each tenant's cardholders are given access to only one of the three "levels" (i.e. a different level for each tenant). Each level is configured to trigger a specific virtual output when a cardholder who has access to that level badges their card at the car-park entry reader. Hence, the lift car is configured as follows:



Notes:

- Each tenant has access to one level.
- The items in the **Output** column are virtual outputs and are turned on when the tenant attempts to enter the car-park.
- The items in the **Input** column are Logic Block outputs that trigger the barrier arm when the tenant is allowed to enter.

The exit elevator car controls exit from the car-park to outside world. It triggers different virtual outputs and is configured as follows:



Notes:

- The items in the **Output** column are virtual outputs and turn on when the tenant exits the car-park.
- The items in the **Input** column are the same as the outputs.

Exit from the car-park is always allowed, however each tenant is configured as exiting into a different zone, and only has access to that zone, so that the zone count can be decremented for the correct tenant, when a cardholder leaves the car-park.

3. Three Zone Count increment inputs are configured - one for each tenant. The Access Zones "Tenant 1 Car-park", "Tenant 2 Car-park" and "Tenant 3 Car-park", are each configured for zone counting.

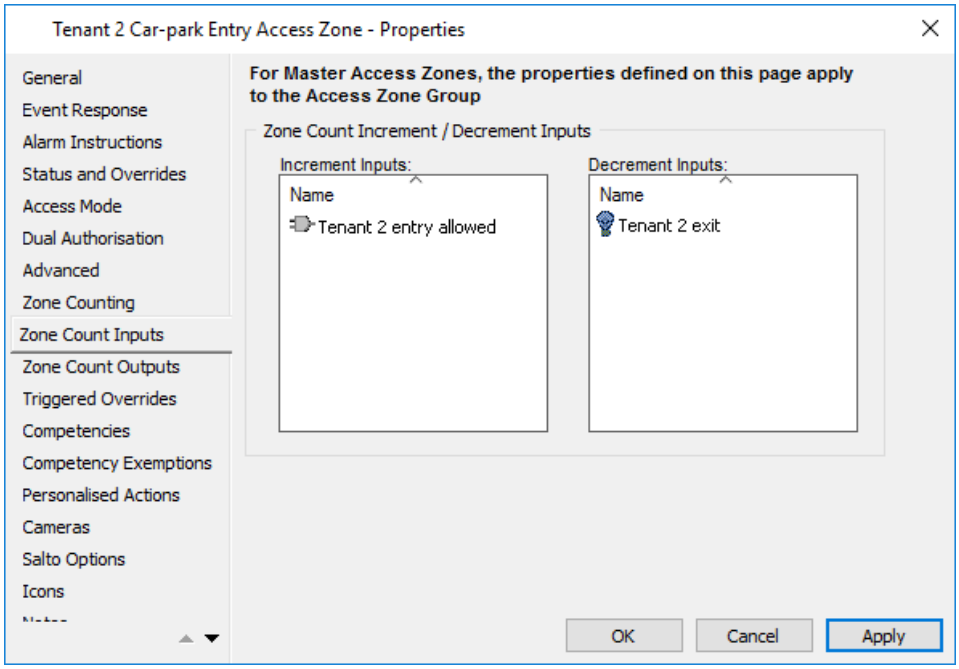
The Logic Block..	**is configured as Zone Count increment input for the Access Zone…**
"Tenant 1 entry allowed"	"Tenant 1 Car-park"
"Tenant 2 entry allowed"	"Tenant 2 Car-park"
"Tenant 3 entry allowed"	"Tenant 3 Car-park"

See No.5 for a description of the logic. The Zone Count increment input ensures that the zone count for the tenant is incremented when the tenant is granted entry to the car-park. The zone count represents the number of car-parks in use for that tenant.

Three Zone Count decrement inputs are configured - one for each tenant.

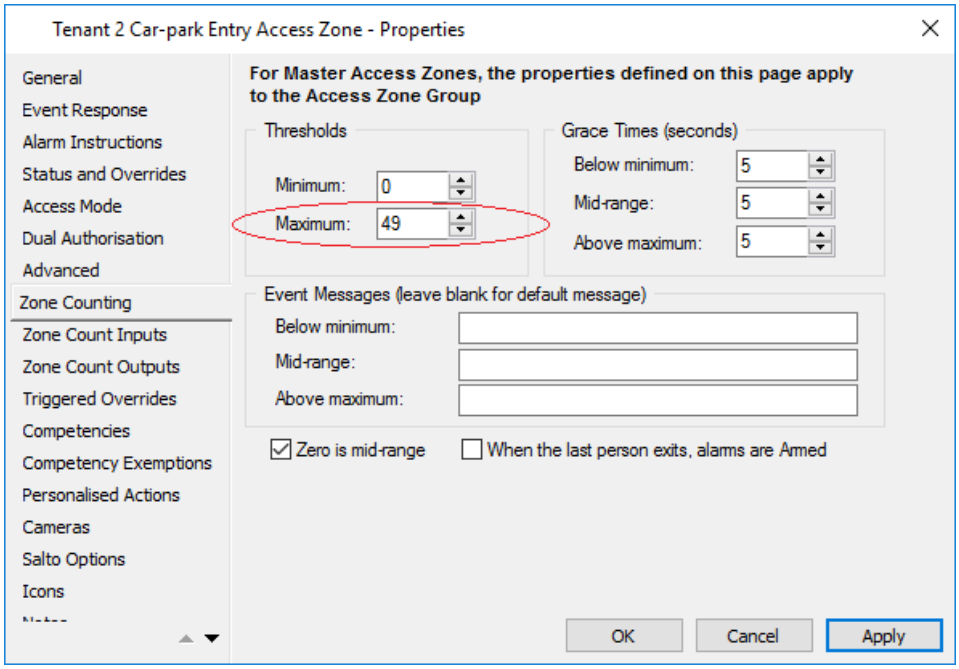
The Virtual Output..	is configured as Zone Count decrement input for the Access Zone…
"Tenant 1 exit"	"Tenant 1 Car-park"
"Tenant 2 exit"	"Tenant 2 Car-park"
"Tenant 3 exit"	"Tenant 3 Car-park"

The Zone Count decrement input ensures that the zone count for the tenant is decremented when the tenant exits from the car-park.



4. The Zone Count threshold is set to one below the maximum number of car-parks allowed for that tenant. That is:

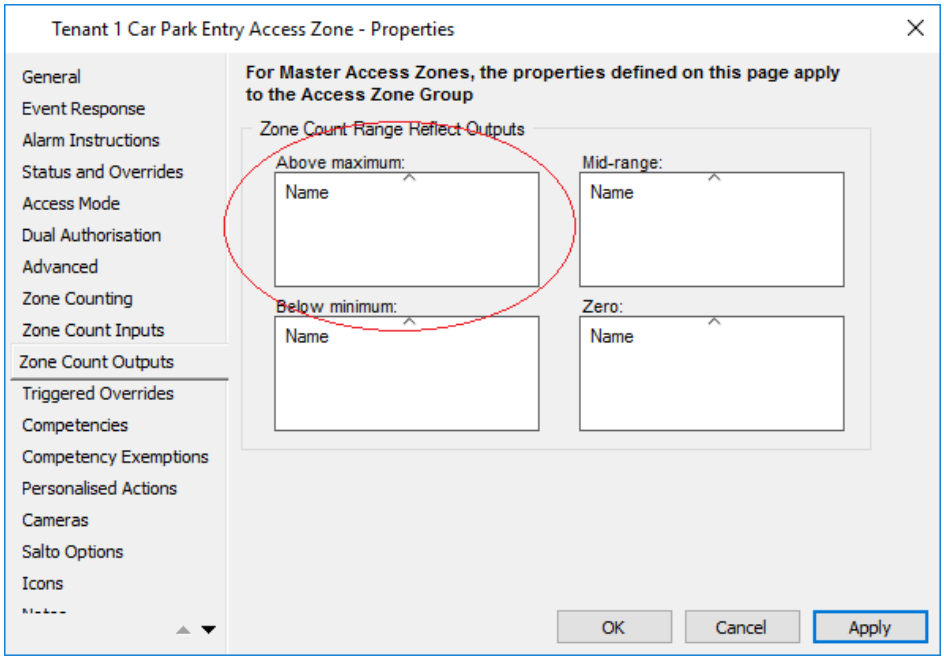
   - Access Zone "Tenant 1 Car-park" maximum zone count threshold is set to 29 (the maximum number of car-parks allocated to Tenant 1 is 30).
   - Access Zone "Tenant 2 Car-park" maximum zone count threshold is set to 49 (the maximum number of car-parks allocated to Tenant 2 is 50).
   - Access Zone "Tenant 3 Car-park" maximum zone count threshold is set to 99 (the maximum number of car-parks allocated to Tenant 3 is 100).



For each Access Zone, an output is switched on when the zone count exceeds the maximum threshold, using the zone counting "above maximum" reflect outputs. That is:

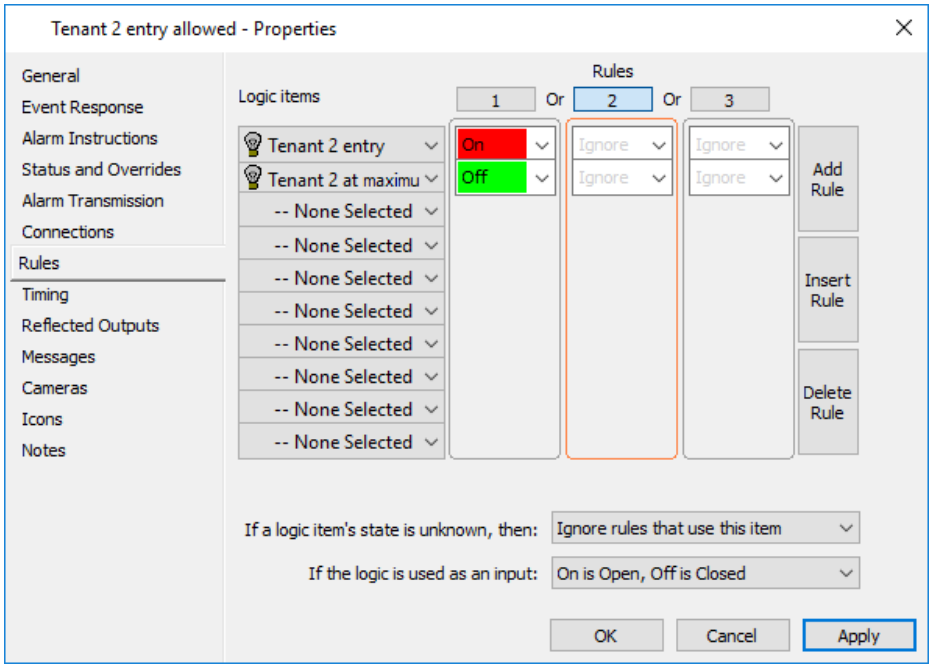
- when Access Zone "Tenant 1 Car-park" zone count exceeds the maximum threshold (reaches 30), output "Tenant 1 at maximum" is turned on.
- when Access Zone "Tenant 2 Car-park" zone count exceeds the maximum threshold (reaches 50), output "Tenant 2 at maximum" is turned on.
- when Access Zone "Tenant 3 Car-park" zone count exceeds the maximum threshold (reaches 100), output "Tenant 3 at maximum" is turned on.

The zone count for each access zone ("Tenant 1 Car-park" etc) holds the number of car-parks in use for that tenant.



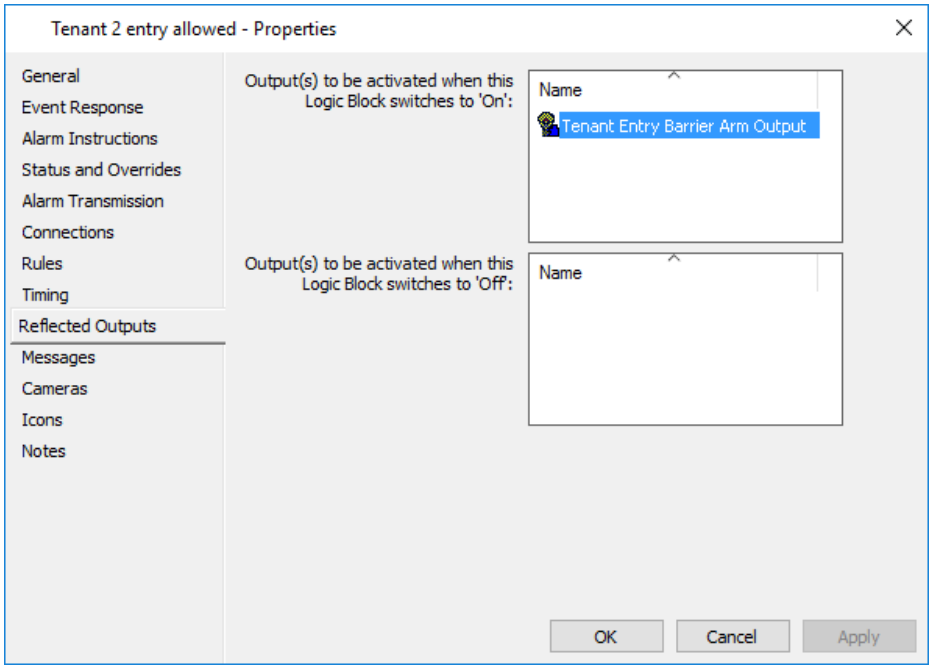
The "Tenant 1 at maximum", "Tenant 2 at maximum" and "Tenant 3 at maximum" outputs each control a separate LED on a mimic panel. Hence, the "Tenant 2 at maximum" LED is on when Tenant 2 has reached the maximum number of car-parks allowed (similarly for other tenants). Once the zone count for the "Tenant 2 Car-park" is no longer above the maximum the "Tenant 2 maximum" output turns off, and hence so does the LED (similarly for other tenants). For each tenant, the LED is therefore on when access to the car-park will be denied because the maximum allowed car-parks for that tenant has been reached. With this configuration, the zone count for the "Tenant 2 Car-park" Access Zone will reflect the number of entries to, less exits from, the car-park for Tenant 2 (similarly for other tenants).

5. A Logic Block is set up as shown below, for each tenant to determine whether access is allowed (the barrier arm is raised) when that tenant badges their card at the entry reader.



If the "Tenant 2 entry" virtual output is on (meaning Tenant 2 has badged their card at the entry reader), and "Tenant 2 at maximum" is off (meaning Tenant 2 still has car-parks available), then the Logic Block is pulsed on for a few seconds.

The car-park entry barrier arm is configured as a reflected output for the Logic Block.



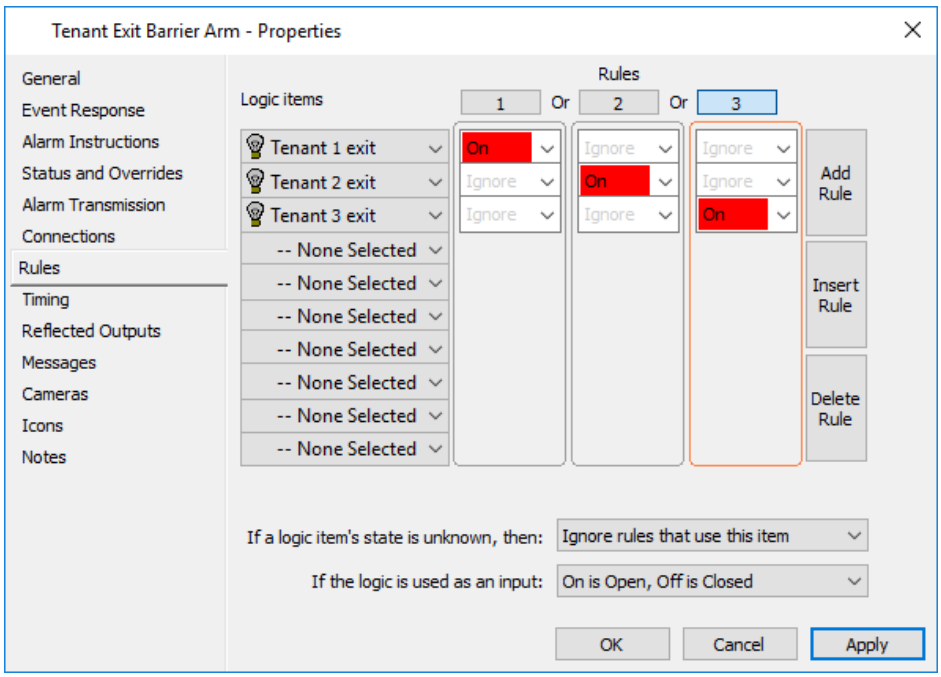
This logic means the barrier arm at the car-park entry is opened, when a valid access attempt is made, only if the number of car-parks in use for the tenancy to which this cardholder belongs, is below the maximum.

The Logic Block is also used to increment the "car-parks in use" zone count for the tenant, so that the zone count is only incremented if the

cardholder is actually allowed to enter the car-park (as shown in Step 3).

6. Exit from the car-park is always allowed, however we need to detect which tenant is exiting, so that the correct "car-parks in use" zone count for that tenant can be decremented. Virtual outputs are set up on the exit elevator car, one for each level/tenant, to detect which tenant has badged their card to exit. The virtual output is configured as a Zone Count decrement input, on the appropriate access zone.

   At the same time, any tenant exiting must open the exit barrier arm. Logic is set up to do this. The logic uses the virtual outputs, one of which is triggered by each tenant when they exit the car-park, in an 'OR' configuration. The output controlling the exit barrier arm is then configured as a reflected output for the logic block output's "on" state.



   With this configuration, a cardholder's exit from the car-park will decrement the "car-parks in use" zone count for that tenant, and always opens the barrier arm for the car-park exit.

7. The "access taken" inputs configured on the entry elevator car, mean that the following event will be logged **only when** the cardholder is actually allowed to enter the car-park:

   [Cardholder] was granted entry into [Tenant 1 Car-park] through [Car-park Barrier Arm - Entry]

   When the cardholder exits from the car-park, the following event will be logged:

   [Cardholder] was granted entry into [Outside World - Tenant 1] through [Car-park Barrier Arm - Exit]

   Note: The names in brackets will vary depending on the actual names used for these items.

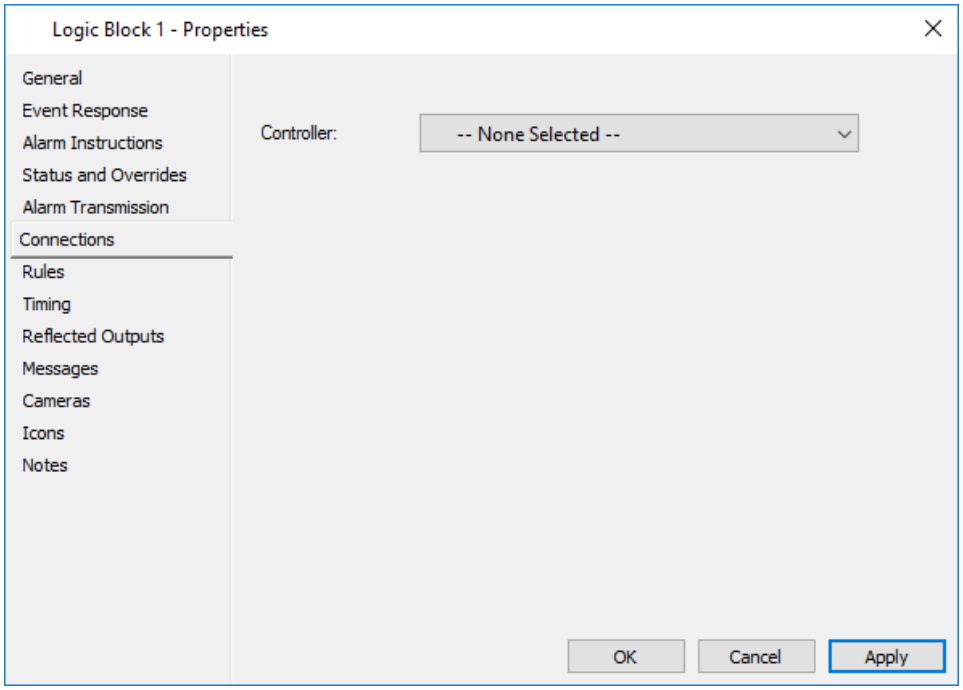
Creating a new Logic Block

Introduction

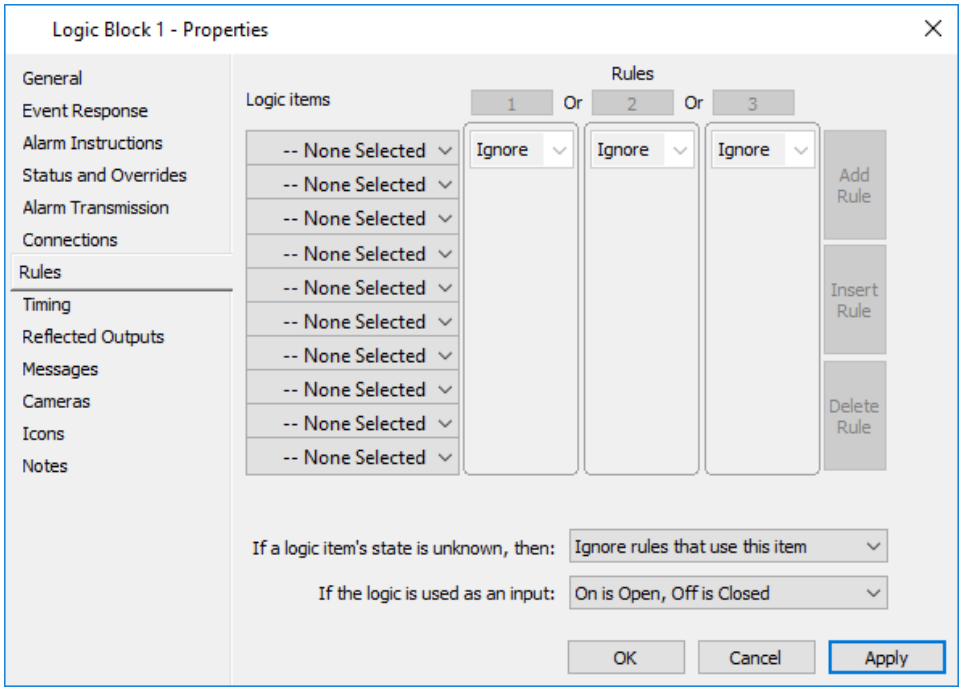
This procedure details how to create a new Logic Block.

Procedure

1. Click **Configure** from the menu bar, then **Logic Blocks**.
   The **Logic Block** List Window opens (in grid view).
2. **Right click** and select **New…Logic Block**.
   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.

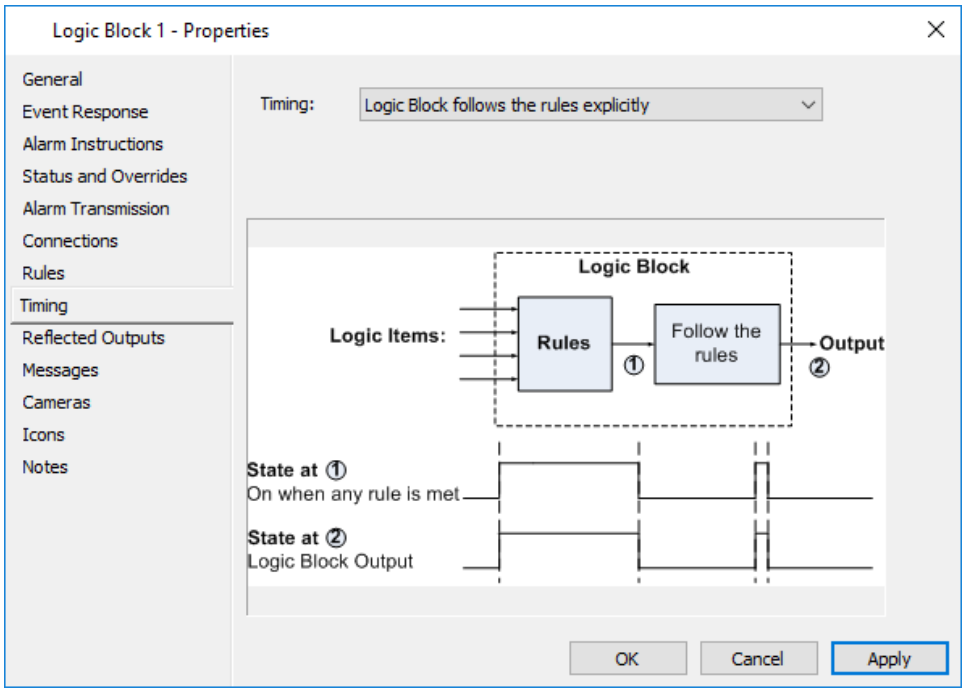


7. Select the appropriate **Controller** from the drop-down list.
8. Click the **Rules** tab.



The centre of the grid contains 10 rows of up to 10 columns, (i.e. 3 columns display, but more can be added, up to a total of 10). Each row has an item of a type that a logic block rule can be based on (see ***Logic Block rules*** on page 25-2). Each column represents a rule (numbered 1 to 10). The cells of the grid allow states to be selected from drop-down lists that include “Ignore” and the states relevant to the item, (e.g. for a Door, “Free” and “Secure”).

9. Logic items will only be saved if one or more rules are set to something other than "Ignore".
10. Select the appropriate options from the drop-down lists for **If a logic item's state is unknown** and **If the logic is used as an input**.
    Note:
    The drop-down list for **If a logic item's state is unknown** includes the options 'Turn Logic Block on' and 'Turn Logic Block off'. If either of these are selected, the output is forced "on" or "off" as applicable, (i.e. it isn't the logic that gets turned on or off).
11. Click the **Timing** tab.

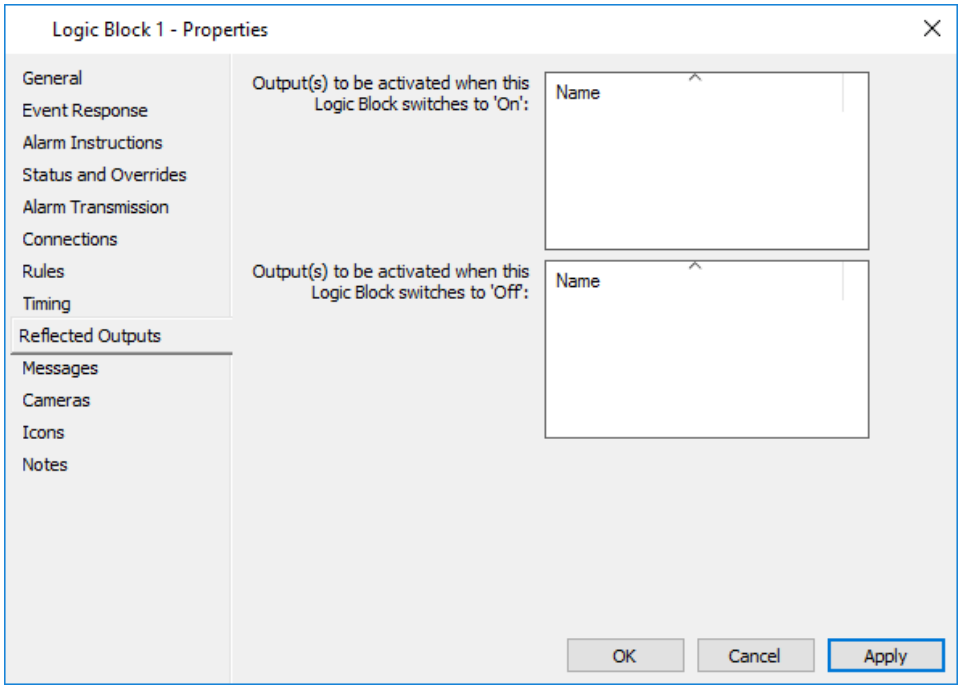


There are six different timing modes available from the **Timing** drop-down list. The default mode is "Logic Block follows the rules explicitly".
If you require another timing mode from the default one, select the appropriate option as indicated:

Mode	Description
Logic Block follows the rules explicitly	The Logic Block will follow the rules explicitly, (i.e. it will be ON while one or more rules are met, and will be OFF while none of the rules are met).
Logic Block follows rules, with a maximum on time	The Logic Block will follow the rules, but with a maximum time for which it is turned on, (i.e. it will turn ON when one or more of the rules are met, and OFF when none of the rules are met, but with a maximum on time). When selected, a **Maximum on time** edit box displays, allowing a time in seconds between 1 (default) and 86400 (24 hours) to be selected.
Logic Block is pulsed when the rules are met	The Logic Block will pulse when a rule is met for the configured pulse time and then switch off for the configured stay off time, (i.e. the pulse and off time occurs when one or more of the rules are met. Then it remains off until the next time the Logic Block transitions from 'no rules met' to 'one or more rules met'). When selected, two edit boxes display, allowing a **Pulse on time** (between 1 second and 24 hours) to be selected, and a **Stay off time** (between 0 seconds and

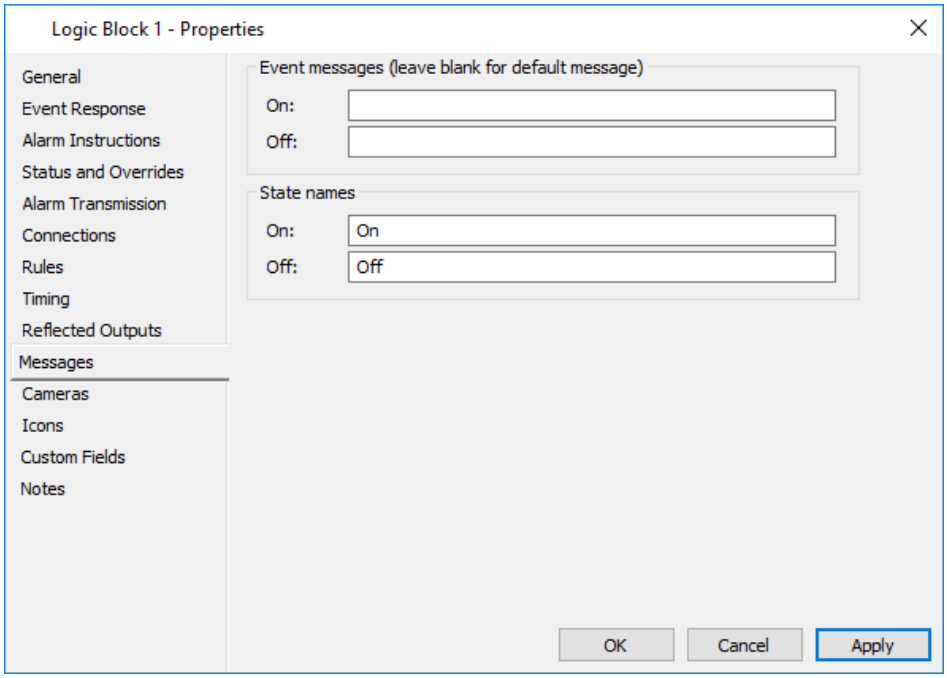
Mode	Description
	24 hours) to be selected after the pulse completes.
Logic Block output has a delayed off time	The Logic Block's output will stay ON for the time specified after the rules are no longer met, (i.e. it will turn ON when one or more of the rules are met, and OFF at the specified time, after none of the rules are met). When selected, a **Delayed off time** edit box displays, allowing a delay time in seconds between 1 (default) and 86400 (24 hours) to be selected.
Logic Block output has a delayed on time	The Logic Block's output will be delayed by the time specified, (i.e. it will turn ON at the specified time after one or more of the rules have been met, but only if at least one rule remains met for the entire delay time. It will be OFF when none of the rules are met, and the delay time restarts each time there is a transition from 'no rules met' to 'one or more rules met'. When selected, a **Delayed on time** edit box displays, allowing a time in seconds between 1 (default) and 86400 (24 hours) to be selected.
Logic Block is latched until cleared by input	The Logic Block's output will latch until cleared by an input, Logic Block or output (virtual or real). This means it will turn ON when one or more of the rules are met, and OFF when either: - an input transitions from closed to open, or - a Logic Block or output transitions to the state that is mapped to "open". The input, Logic Block or output (virtual or real) that resets the Logic Block's state can be any item defined in Command Centre, subject only to operator privileges. Only one item resets the Logic Block. When selected, a **Cleared by input** edit box displays, allowing an input, Logic Block or output to be selected.

12. Click the **Reflected Outputs** tab.



Reflected outputs can be configured on this tab to carry out actions required in response to a rule being met and the Logic Block's state changing as a result.

13. From the **Hardware** List Window, select the output(s) to reflect the Logic Block's "On" state.
14. Drag and drop them into the top grid on the **Reflected Outputs** tab. These output(s) will turn on when the Logic Block turns on, and off when the Logic Block turns off.
15. From the **Hardware** List Window, select the output(s) to reflect the Logic Block's "Off" state.
16. Drag and drop them into the bottom grid on the **Reflected Outputs** tab. These output(s) will turn on when the Logic Block turns off, and off when the Logic Block turns on.
    Note:
    The Find Tool can be used to locate outputs instead of opening the **Hardware** List Window. By selecting **Outputs** (in the "Look in" field) on the **General** tab, you then get some additional search options on the **Advanced** tab to help define your search further.
17. Click the **Messages** tab.



18. Enter the **Event messages** and **State names** (if you require them to be different from the site-wide defaults), that will display in Command Centre when the Logic Block transitions to "on" and "off".
19. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Logic Block.
    For further details see ***Cameras tab*** (on page 3-24).
20. Click the **Icons** tab if you want to change the Icon Set for this Logic Block.
    For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
21. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Logic Block.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
22. Click the **Notes** tab if you want to add a note(s) about this Logic Block. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
23. 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 Logic Block has been created.

Hint

Duplicating Logic Blocks
Logic Blocks can be duplicated as long as an operator has the edit privilege to the existing Logic Block being duplicated. Any Command Centre items that the operator does not have the view privilege for, that are part of the existing Logic Block's configuration, will not be copied to the new Logic Block.

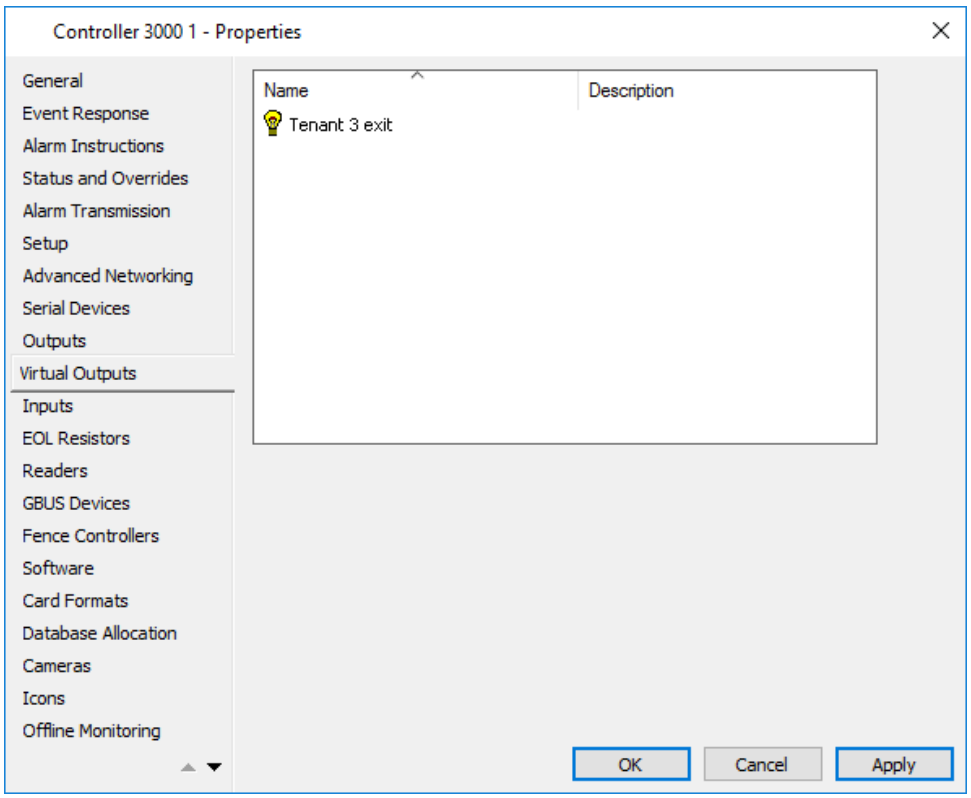
Creating a new Virtual Output

Introduction

Normal (or 'real') outputs are relays that activate any number of things, (e.g. alarms, light switching, doors unlocking, etc.). Virtual Outputs are used as an input to a Logic Block without going to the expense of creating a real output. When a real output goes to a Controller, a device is activated. With a Virtual Output, the Controller is aware that the output is not to trigger a physical action.

Procedure

1. The procedure for creating a Virtual Output is basically the same as creating a real output. Therefore, refer to ***Creating Inputs and Outputs*** (on page 21-39) for the steps required.
   Note: On the **Advanced** tab of the Output properties there is an 'Output is inverted' option. This feature does not apply to Virtual Outputs, as it reverses the behaviour of a physical relay.
2. From the **Hardware** List Window, open the Controller that the Virtual Output is to be assigned to.
3. Click the **Virtual Outputs** tab.



4. Drag and drop the Virtual Output you have just created into the grid on this screen.

Note: Outputs assigned to this grid are automatically removed from any other Controller's Virtual Outputs grid, or from its physical slot on a Controller or device.

5. Click **Apply**.

Result

A Virtual Output has been created.

Chapter 26: Universal Card Format

The Universal Card Format item allows users to define their own card formats and transfer them to Controller(s). This is in addition to the manufacturer's Gallagher card formats and certain Wiegand formats that have been pre-defined in Command Centre.

The Universal Card Format item can be defined as Wiegand or ABA (American Banking Association) compatible. It can be used with either Gallagher 125 readers or Wiegand compatible readers connected to Universal Reader Interfaces or Reader I/O Interfaces.

Operators define Universal Card Formats by specifying significant parameters, (i.e. bit position, card number length, facility code, issue level and parity check bits for Wiegand formats, or digit positions and lengths for ABA formats). The Universal Card Format is passed to the Controller as properties of a Reader Part in the Controller, which uses the format when interpreting card data.

Note:
The process of defining and configuring Universal Card Formats requires a technical knowledge of ID Card systems, and will normally be configured by your dealer. It is recommended that you contact your dealer prior to modifying or creating Universal Card Formats.

Adding a new Universal Card Format

Introduction

An operator wishing to add a new Universal Card Format must have the "Configure Site" privilege and be in the same Division (or parent Division) as the Controller.
The following procedure describes how to create a new Universal Card Format and add it to the list of active formats.

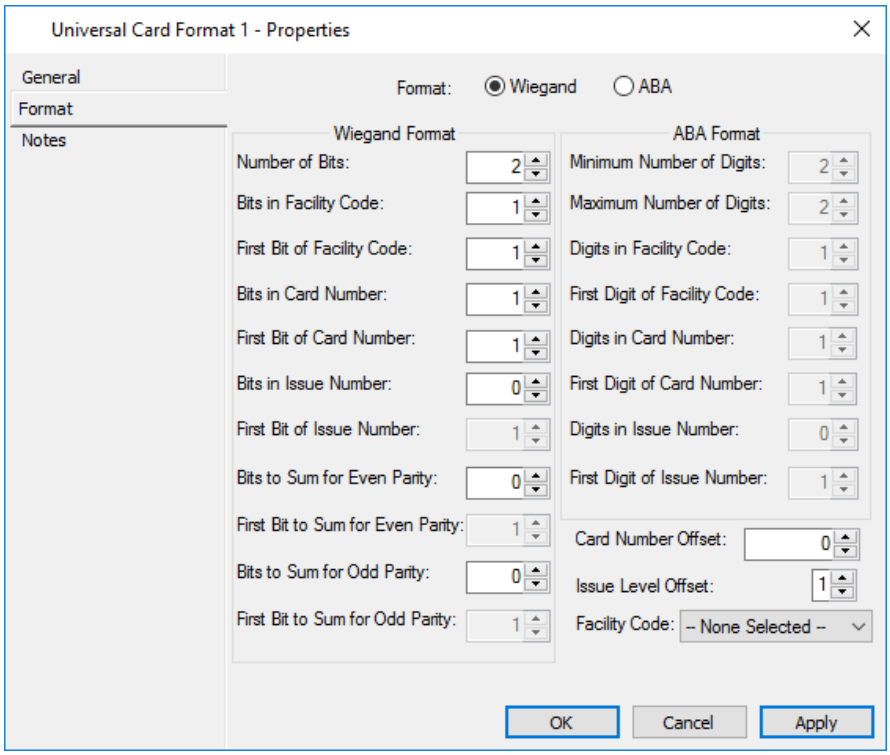
Before you begin

The structure and format of any Wiegand or ABA (American Banking Association) cards will need to be known before a Universal Card Format can be configured. If this is not known then it is recommended that Gallagher Group Limited is contacted. A variety of cards will be required with card numbers having as wide a range as possible. The facility codes, card numbers and issue numbers (if used) for the cards supplied, must be known.

Note:
Some card formats do not have Facility codes. The following procedure describes what action to take in this situation.

Procedure

1. Click **Configure** from the menu bar, then **Universal Card Format**.
   The **Universal Card Format** List Window opens (in grid view).
2. **Right click** and select **New...Universal Card Format**.
   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 **Format** tab.



5. Click the appropriate radio button for the format you require, (i.e. Wiegand or ABA).
   See the note at the end of this topic for examples.

Format	Description
Wiegand	Wiegand card data is stored on the card as a binary representation of the card details. The size and position of these fields, (e.g. Facility code, Issue Number, etc.) can vary from one card to another. **Important:** The Least Significant Bit (LSB) is referred to as bit 1, not bit 0.
ABA	American Banking Association (ABA) cards are handled quite differently to Wiegand format cards. Rather than a binary representation, ABA card data is handled as a series of decimal digits. The various fields are extracted from the card data string as real numbers and are handled normally from then onwards. All fields read will have any leading 0's stripped, (e.g. Facility code "0000730" will become "730").

6. Complete the parameters to describe the data on the cards to be supported.

WIEGAND FORMAT FIELDS:

Field	Description
Number of Bits	(2 - 65535) This must be the exact number of data bits contained on the card (including parity bits)

Field	Description
Bits in Facility Code	(1 - 20) The number of bits comprising the Facility code. **Note:** Not all card formats have Facility codes. If this is the case, enter 0. You should then select a valid Facility code to be assigned to this format from the **Facility Code** drop-down list at the bottom of the tab. If you do not, the first Facility code for the site will be used.

First Bit of Facility Code	Start reading bits from this position for the Facility code.
	Important: The structure of Facility codes in Command Centre is in the following format:
	Region Code: <A - P><upper 4 bits>
	Fac Code: <1 - 50,000> <lower 16 bits>
	Any card data exceeding these values will generate an unrecognised card event. If 16 or less bits are used then the region code will always be 'A', e.g.
	`1011011010 (10 bits) => A 00730`
	`1100001101010000 (16 bits) => A 50000`
	`1 1100001101010000 (17 bits) => B 50000`
	`1011 1011011011100001 (20 bits) => L 46817`

Bits in Card Number	(1 - 2000) The number of bits comprising the Card number.
First Bit of Card Number	Start reading bits from this position for the Card number.
Bits in Issue Number	(0 - 4) The number of bits comprising the Issue number.
First Bit of Issue Number	Start reading bits from this position for the Issue number.
Bits to Sum for Even Parity	(1 - 65535) The number of bits (including the parity bit) to add up for the Even parity check.
First Bit to Sum for Even Parity	Start reading bits for the Even parity check from this bit position.
Bits to Sum for Odd Parity	(1 - 65535) The number of bits (including the parity bit) to add up for the Odd parity check.
First Bit to Sum for Odd Parity	Start reading bits for the Odd parity check from this bit position.

ABA FORMAT FIELDS:

Field	Description
Minimum Number of Digits	(2 - 107) The minimum number of digits a card may have for it to be a candidate for this Universal Card Format.

Field	Description
Maximum Number of Digits	(2 - 107) The maximum number of digits that a card may have for it to be a candidate for this Universal Card Format.
Digits in Facility Code	(1 -7) The number of digits comprising the Facility code. **Note:** Not all card formats have Facility codes. If this is the case, enter 0. You should then select a valid Facility code to be assigned to this format from the **Facility Code** drop-down list at the bottom of the tab. If you do not, the first Facility code for the site will be used.
First Digit of Facility Code	The position of the first digit in the Facility code. **Important:** The major difference is that the ABA Facility Code digit 'string' will be converted to binary first and then handled in exactly the same manner as described for Wiegand format cards. If, when converted to a binary representation, the number of bits exceeds 20, then the card will automatically be passed through as an 'unrecognised card' and no further match attempts will take place, e.g. "730" => 1011011010 (10 bits) => A 00730 "50000" => 1100001101010000 (16 bits) => A 50000 "115536" => 1 1100001101010000 (17 bits) => B 50000 "767713" => 1011 10110110111100001 (20 bits) => M 46817 , etc.
Digits in Card Number	(0 - 107) The number of digits comprising the Card Number.
First Digit of Card Number	The position of the first digit in the Card Number.
Digits in Issue Number	(0 - 2) The number of digits comprising the Issue Number.
First Digit of Issue Number	The position of the first digit in the Issue Number.

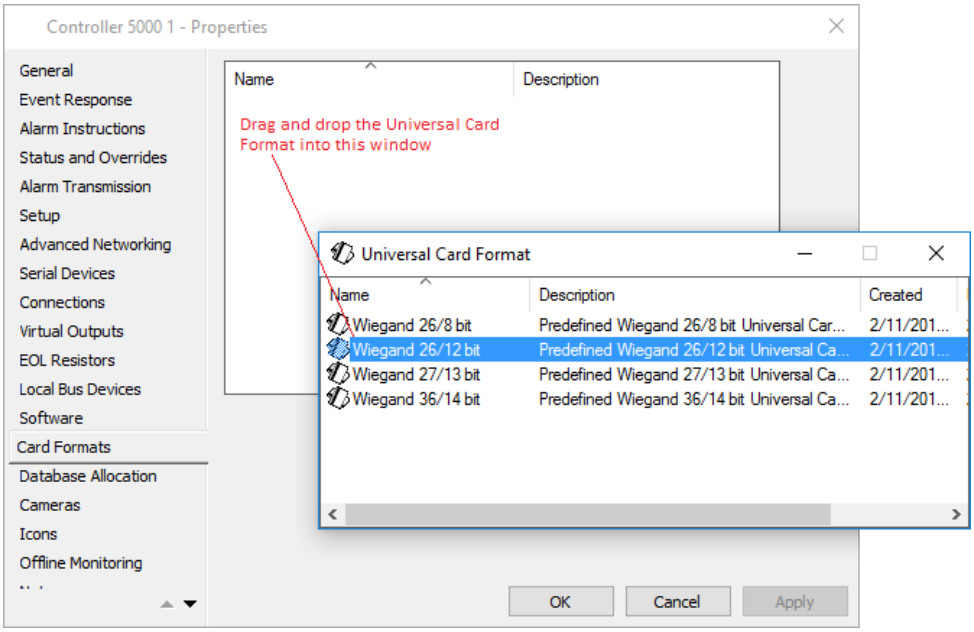
COMMON FIELDS:

Field	Description
Card Number Offset	(0 - 16777216) This is to be used when combining multiple existing card bases into one system would cause duplicate card numbers. The system administrator will choose to offset one set of cards by a fixed amount to stop clashes. This applies to both Wiegand and ABA card formats. This offset is added to the card number of any valid cards matching this Universal Card Format, e.g.

Field	Description
	A card is badged/swiped and is matched to a Universal Card Format. The card number is 24377 with the offset set to 420000. These are added together to give a card number of 444377. This new value is the card number that will be used for transaction attempts made by this card. To the rest of the system, this modified value is the actual card number and must be treated as such, (e.g. when assigning cards to a cardholder the value 444377 would be used, not 24377). **Important:** By changing the Card Number Offset of a Universal Card Format after cards (matching this Universal Card Format) have been assigned to various users, then the card configuration for each user will also have to change to reflect the new Card Number Offset.
Issue Level Offset	Some cards with issue levels encode the first level as 0, while others encode the first level as 1. Command Centre issue levels always start at 1.
Facility Code	When a Wiegand or ABA card is badged the facility code is the first field to be extracted from the card data. If a facility code has been specified and the facility code read from the card is different to that found in the Universal Card Format, then the Controller will attempt to match the card data with the next Universal Card Format in the list until a matching facility code is found. This will continue until a match has been attempted with all available Universal Card Formats. If no matches are made then the card is passed on as an 'unrecognised card format'. If a facility code has not been specified in a Universal Card Format, then the Controller will attempt to match the cards facility code with any valid facility code used anywhere in the system. Specifying a facility code severely limits the chances of an incorrect Universal Card Format match. There may be cases where this is desirable though, so this feature has been left optional.

7. Click **OK** to exit and save your changes.
   The new Universal Card Format displays in the **Universal Card Format** List Window.
8. From the **Hardware** List Window, open the properties for the Controller you wish to transfer the Universal Card Format to.

9. Click the **Card Formats** tab.
10. Highlight the Universal Card Format and drag and drop it into the **Card Formats** tab of the Controller.

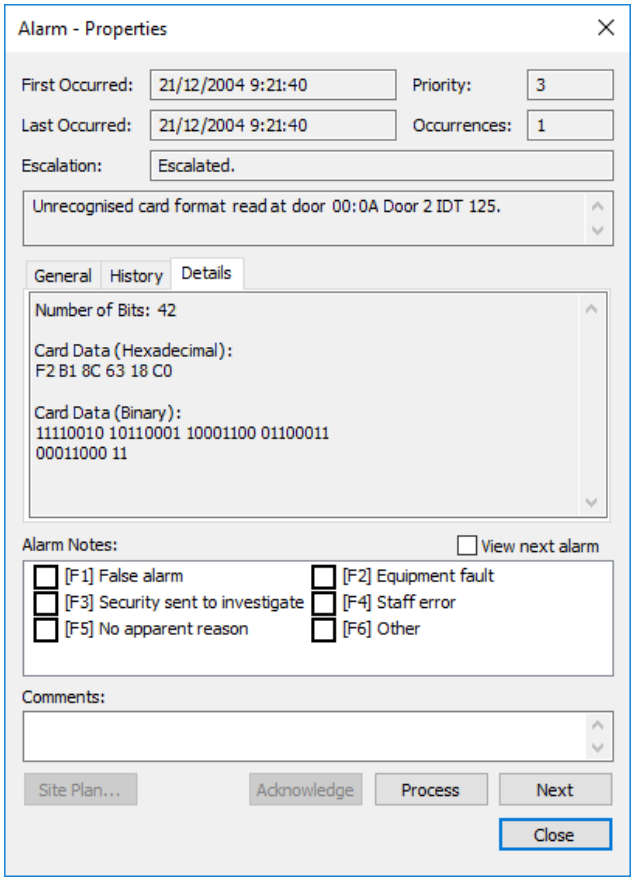


11. Click the **Custom Fields** tab if you want to add and assign a custom field value to the Universal Card Format.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
12. Click the **Notes** tab if you want to add a note(s) about this Universal Card Format.
    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.

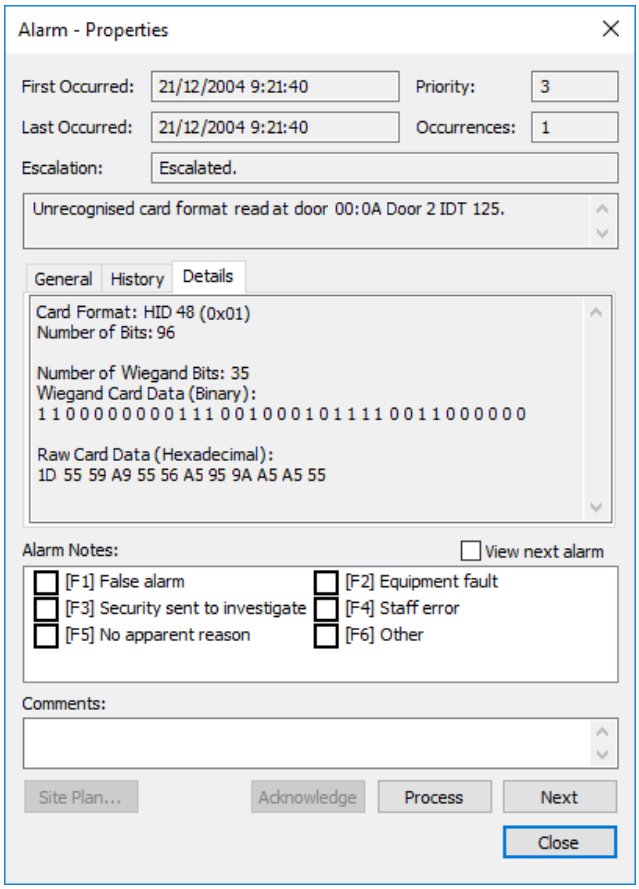
Result

A new Universal Card Format has been created and the Controller has been configured to recognise the new format.

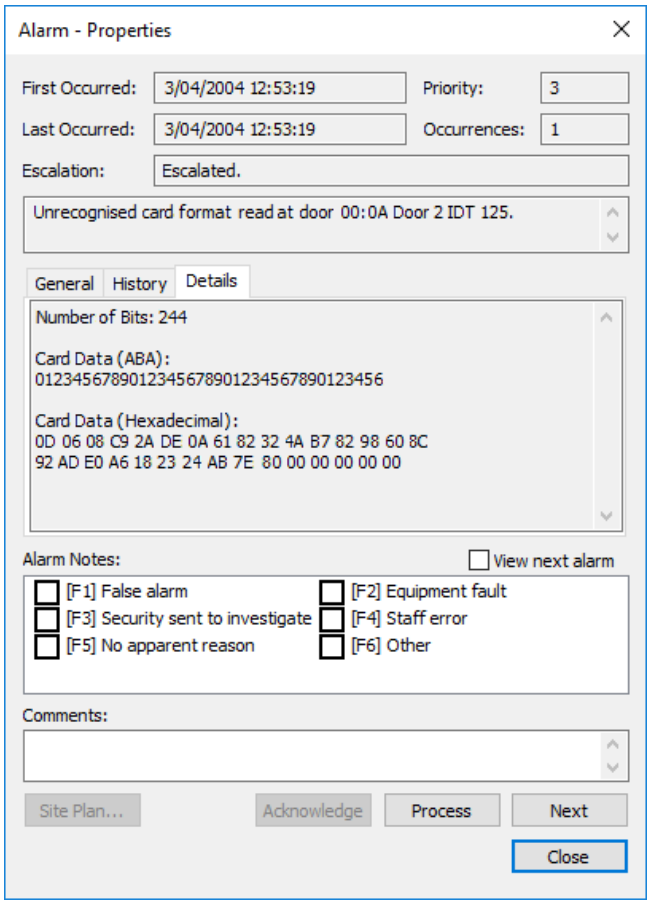
Note: The following screen shows an example of the Alarm/Event Properties page when an unknown format card is badged:



The following screen shows an example of the Alarm/Event Properties page when an unknown Wiegand format card is badged:



The following screen shows an example of the Alarm/Event Properties page when an unknown ABA format card is badged:



Hint

Editing Universal Card Formats
Refer to ***Editing items*** (on page 3-26) for the procedure on how to edit a Universal Card Format.

Deleting a Universal Card Format

Introduction

An operator wishing to delete a Universal Card Format must have the "Configure Site" privilege and be in the same Division (or a parent Division) as the Controller. The Universal Card Format needs to be removed from any Controllers it is associated with prior to deleting it. The following procedure describes how to delete a Universal Card Format from Command Centre.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Open the properties for the Controller that the Universal Card Format is associated with.
3. Click the **Card Formats** tab.
4. **Right click** on the Universal Card Format and select **Remove from List**.
5. Click **OK** to exit and save your changes.
6. Repeat Steps 2-5 for any other associated Controllers.
7. Click **Configure** from the menu bar, then **Universal Card Format**.
   The **Universal Card Format** List Window opens (in grid view).
8. Highlight the Universal Card Format you want to delete.
9. **Right click** and select **Delete**.
   A confirmation window displays.
10. Click **Yes** to delete the Universal Card Format.

Result

The Universal Card Format disappears.

Hint

Locating linked Controllers
If you attempt to delete a Universal Card Format that is linked to a Controller the following message will display:
"This Universal Card Format cannot be deleted, as it is assigned to a Controller."

The message however does not indicate which particular Controller(s) it is linked to, of which there could be many. Therefore a quick method of locating the Controller(s) is to use the Find Tool.
See ***Example 2: Searching using Related To details*** (on page 41-8) for the procedure.

Universal Card Formats for 'Use MIFARE Serial Number as Card Data' (CSN mode)

Introduction

All MIFARE cards have a unique Card Serial Number (CSN) also known as a Unique ID (UID). A MIFARE card's CSN will usually be either be 4 bytes (32 bits) or 7 bytes (56 bits) in length.

Gallagher HBUS Readers and MIFARE Cardax IV Readers can be set to read the Card Serial Number (CSN) from a MIFARE Card and use it to identify a Cardholder in Command Centre. When the 'Use MIFARE Serial Number as Card Data' option is enabled on a reader, this allows the reader to send the card's CSN as Cardholder identification to the Controller if it does not detect any other form of Cardholder identification on the card. See Creating Readers for further detail.

In order to interpret the CSN as a card number, the Controller hosting the reader needs to be assigned a Universal Card Format (UCF) that matches the length of the CSN of the MIFARE cards being used.

Configuring a Universal Card Format for CSN mode

Use the following procedure to create a UCF for either 4 byte (32 bit) or 7 byte (56 bit) length CSNs:

1. Click **Configure** from the menu bar, then **Universal Card Format**. The **Universal Card Format** List Window opens (in grid view).
2. Open the Universal Card Format you want to configure for CSN mode, or create a new Universal Card Format (see ***Adding a new Universal Card Format*** on page 26-2 for the procedure).
3. Click the **Format** tab.
4. Click the **Wiegand** radio button to indicate the required Format.
5. Complete the parameters to describe the data on the cards to be supported, as indicated in the following table:

Wiegand Format fields	32 bits (4 byte)	56 bits (7 byte)
Number of Bits:	32	56
Bits in Facility Code:	0	0
First Bit of Facility Code:	n/a	n/a
Bits in Card Number:	32	56
First Bit of Card Number:	1	1

Wiegand Format fields	32 bits (4 byte)	56 bits (7 byte)
Bits in Issue Number:	0	0
First Bit of Issue Number:	n/a	n/a
Bits to Sum for Even Parity:	0	0
First Bit to Sum for Even Parity:	n/a	n/a
Bits to Sum for Odd Parity:	0	0
First Bit to Sum for Odd Parity:	n/a	n/a

Facility Code: <select the appropriate facility code from the list>

Note: No bits are set for the **Facility Code** as this data is not sent when retrieving the CSN only. You will need to create a card type with the appropriate facility code that you want to use. On the Card Types **Setup** property page, you also need to increase the card number range to 72057594037927935 for 56 bit cards or 4294967295 for 32 bit cards. See Setting up Card Types for further detail.

6. Select this Card Type's facility code from the **Facility Code** drop-down list.
7. Assign the UCF to the Controller's **Card Formats** property page.

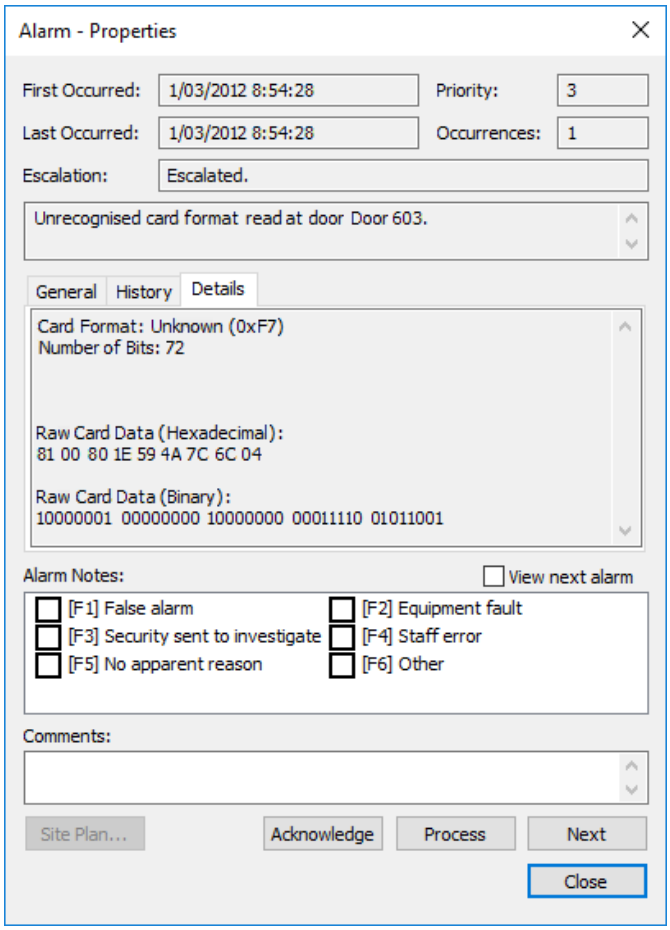
Result

- Now when a MIFARE card, that has no Gallagher data, is presented to a reader configured for CSN mode, an 'Unauthorised Card' event is generated with details of the card's CSN displayed. You can copy this CSN number when you add the card to a cardholder.
- The **Read MIFARE Card** utility will also display MIFARE cards CSN (in decimal format). See ***Reading MIFARE Cards using a MIFARE USB Encoder*** (on page 32-31) for further detail.

Unrecognised Card Format events

If a MIFARE card without Gallagher data is presented to a reader in CSN mode and the Controller does not have the appropriate UCF assigned, then a 'Foreign Card - Unrecognised card format' event will be generated.

The details of this Foreign Card event will display the bit pattern of the MIFARE cards CSN. For example:



Note: T series readers will display an additional 2 bytes (16 bits) before the bit pattern that represents the cards CSN. For example:

Card Format: Unknown (0xF7)
Number of Bits: 72

Raw Card Data (Hexadecimal):
81 00 **80 1E 59 4A 7C 6C 04**

Raw Card Data (Binary):
10000001 00000000 **10000000 00011110 01011001 01001010 01111100 01101100 00000100**

The bits that represent the cards CSN (7 bytes) are highlighted in bold above.

Chapter 27: Device Software

Device Software items represent what versions of Controller or other device software you have on your system.

The Device Software feature provides a method of storing versions of device software in the database and retrieving it for transfer to a Controller or device.

During installation the most current device software would have been loaded off the Command Centre Installation files.

Device Software items are subject to full system division. Therefore, an operator will only be able to view or edit Device Software items that are in their division.

Adding a new version of Device Software

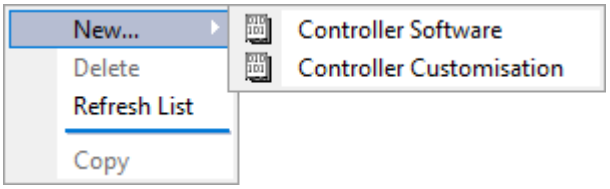
Introduction

This procedure enables an operator with the "Configure Site" privilege, to add a new version of software to Controller 6000s or Controller Customisations.

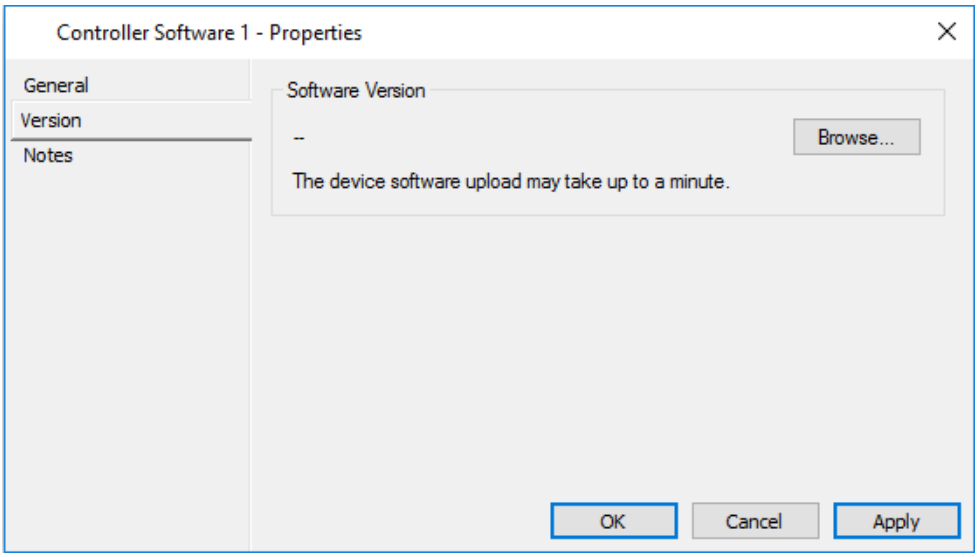
Note: Controller Device Software upgrades should be performed when there is no card activity occurring, (i.e. card badging). This will reduce the chance of alarms occurring while the Controller is being upgraded.

Procedure

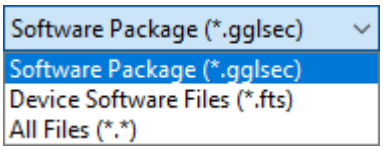
1. Click **Configure** from the menu bar, then **Device Software**.
   The **Device Software** List Window opens (in grid view).
2. **Right click** and select **New...**, and then the appropriate software option.
   By default the **General** tab displays.



3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Version** tab.
   Note: This screen example shown is that of the Controller Software, however this tab looks the same for Controller Customisation.

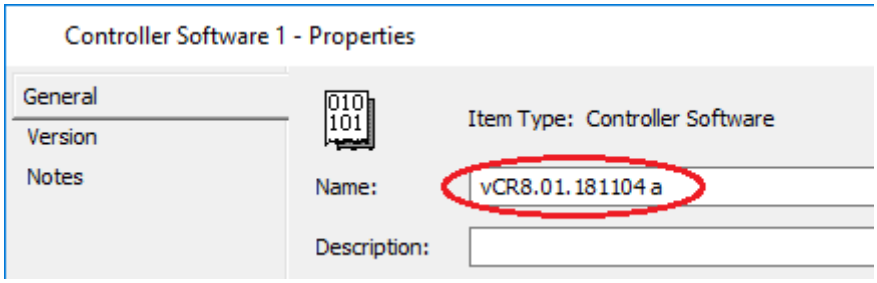


5. Click the **Browse** button and path your way to either:
   - the Device Software File, (***.fts**), containing the correct version of code for this device, OR
   - the Software Package (***.gglsec**).

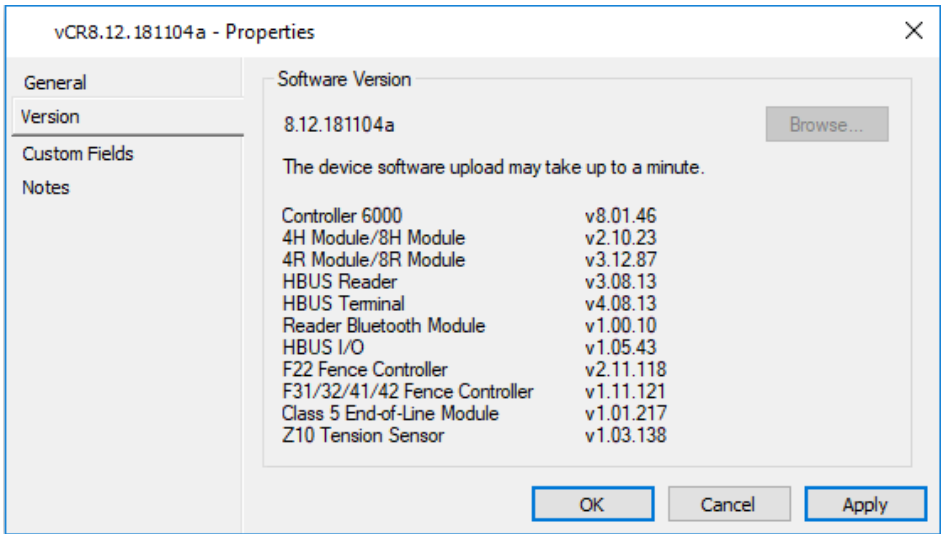


6. Highlight the file once located and click the **Open** button.
   The version of software displays in the **Software Version** field.

   The name of any software selected will automatically populate the **Name** field on the **General** tab.



   When a Software Package (***.gglsec**) is selected, once the software has downloaded the individual device files that are included in the vCR file package display on the **Version** tab.



7. Click the **Custom Fields** tab if you want to add and assign a custom field value to this device.
   For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).

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

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 new version of software has been added for the device.

Hint

Deleting obsolete Device Software items
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete an obsolete Device Software Item.

Assigning Device Software to Controllers

Introduction

The following procedure enables you to assign device software to Controllers.

Note: To simplify the process of upgrading firmware on multiple Controllers, the Controller Upgrade feature can be used instead. Refer to ***Upgrading Multiple Controllers*** (on page 27-11) for further detail.

Before you begin

Before you begin this procedure:

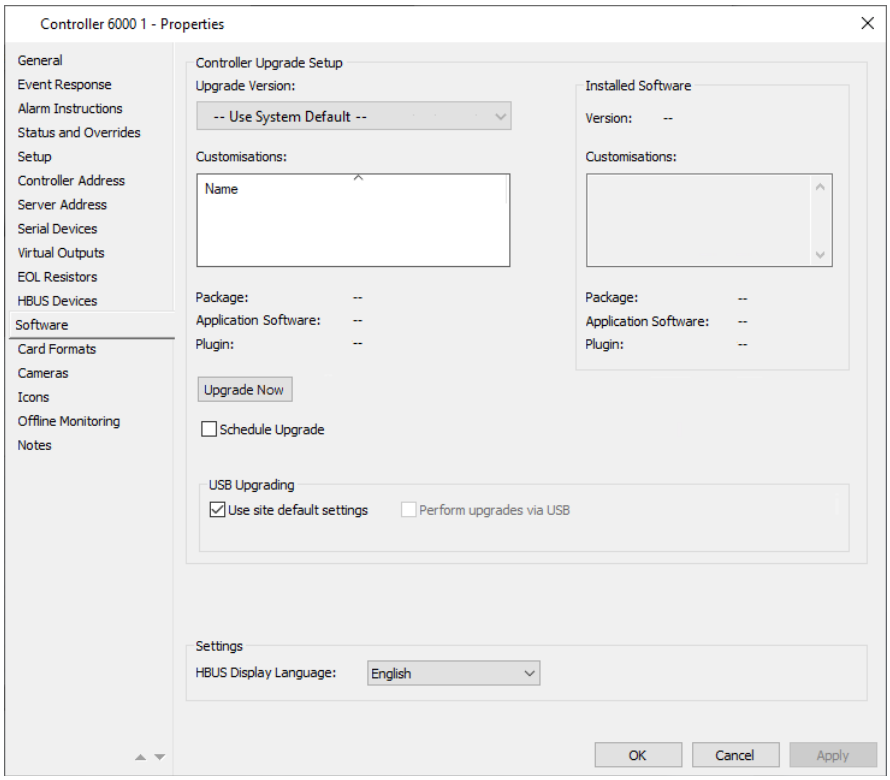
- You need to create the Controller you wish to assign the device software to. Refer to ***Creating Controllers*** (on page 21-2) for the procedure.
- It is recommended you link the Controller to an Alarm Zone before assigning device software to it. Otherwise, the software version number will not display in the **Software** tab of the Controller's properties.

Notes:

- Software can be upgraded on Controller 6000s and 7000s from a USB memory stick. If you require the procedure for this, refer to ***Loading Device Software to a Controller 6000 or 7000 using a USB stick*** (on page 27-9).
- If downgrading a Controller 6000 to a version before v7.80, you will need to perform a "revalidate certificate" override in order for the Controller to come back online. If this is not done, you will see "invalid certificate" alarms for this Controller.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Highlight the required Controller, (i.e. the one you wish to assign the device software to).
3. **Right click** and select **Properties**.
4. Click the **Software** tab.
   Note: The fields on this tab vary slightly for the different devices.



5. Click the **Upgrade Version** drop-down list and select the required Controller version.

   Notes:

   - If you click the **Apply** button, the version of software displays on the screen once the download has completed. If it doesn't complete successfully, the version number that displays will be the version that the Controller "thinks" it has, which may not match what the device software is labelled as.
   - Other versions of software display as well as the **Controller Version**, (i.e. **Package**, **Application Software** and **Plug-in Versions**).

6. The **Installed Software** section allows for downloading DLLs and assigning a customisation to a Controller.
   To assign a customisation, drag it from the **Device Software** List Window into the Customisations grid and click **Apply**.

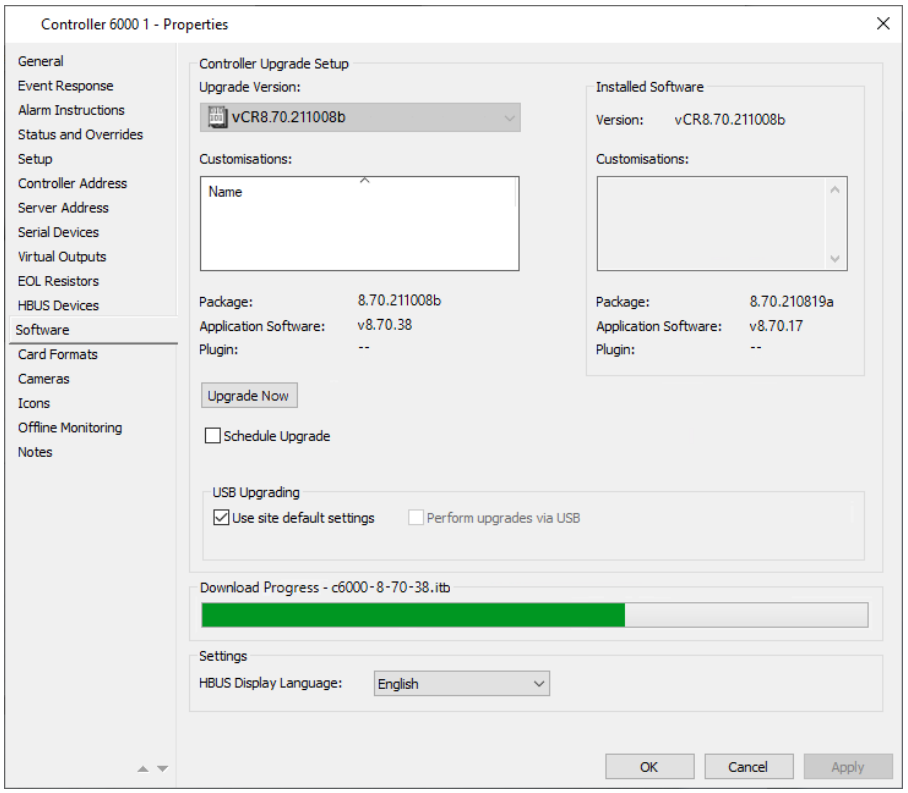
   Note: Only one customer card customisation at a time can be deployed on any one Controller.

7. Do you want to upgrade the Controller now or schedule it for later?
   If **now**, go to Step 8.
   If **later**, go to Step 9.

   Note: Upgrades require Controllers to be online and Dipswitch 2 to be OFF. A warning message will display below the Upgrade Now button if the Controllers are offline OR Dipswitch 2 is ON:

   DIP Switch 2 is set to ON. The controller will fail to come online when restarting if it cannot determine its IP address

8. Click the **Upgrade Now** button.
   The Controller starts downloading the software, and a progress bar shows the progress of the download. Once the upgrade is complete the Controller restarts and comes back online.
   Go to Step 11.



9. Tick the **Schedule Upgrade** checkbox.
   A Date and Time drop-down displays.
10. Specify a suitable time for the Controller upgrade to occur by entering the required **Date** and **Time**, and click **Apply**.
11. The **USB Upgrading** section allows the software installed on the Controller to be upgraded with FTS files from a USB memory stick plugged into the USB port of the Controller 6000.
    To enable this option, uncheck the **Use site default settings** checkbox, and check the **Perform upgrades via USB** checkbox.
    Notes:
    - When selected, upgrades can be performed via USB for this Controller only. To change the site default settings for all Controller 6000s, refer to ***Controller Defaults*** (on page 6-59) in Server Properties.
    - When an upgrade has been initiated but can only be performed via USB, the following message is displayed at the bottom of this page:

      The current settings require the selected software to be installed manually via a USB Upgrade.

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

The device software is assigned to the appropriate device.
Notes:

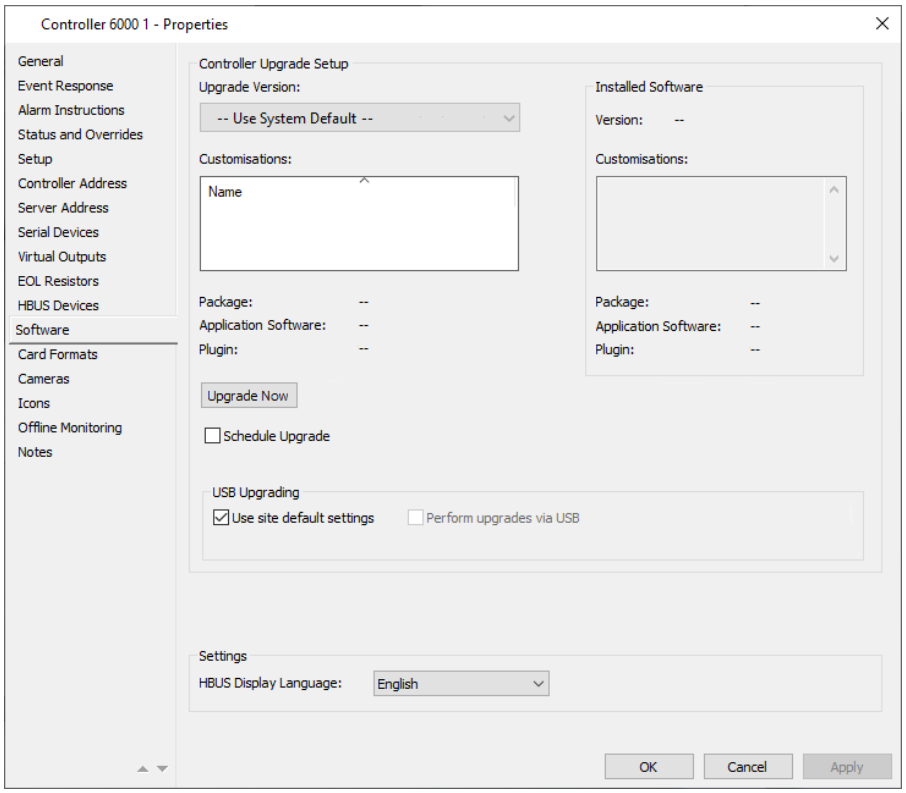
- If you were assigning software to a Controller, the Controller will be automatically restarted after the download.
  If the Controller software is upgraded and the Controller has custom DLLs installed, the Controller will delete the custom DLLs prior to downloading the upgraded Controller software, and then the Controller automatically restarts. The DLLs are then downloaded again to the Controller, and the Controller will restart a second time.
- For Controller 6000s that have HBUS devices configured, these devices will be automatically upgraded after the Controller has completed it's upgrade if the Controllers Device Software contains a newer version of the HBUS Devices firmware.

Loading Device Software to a Controller 6000 or 7000 using a USB stick

Note: The Controller 6000 and 7000 use Linux as their operating system, and not all USB memory sticks are compatible with Linux. It is strongly advised that you ensure your USB memory stick functions properly when loading Controller software, by setting it up on a workbench prior to going to site.

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** on the required Controller, and select **Properties**.
3. Click the **Software** tab.



4. In the **USB Upgrading** section, uncheck the **Use site default settings** checkbox, and check the **Perform upgrades via USB** checkbox.
5. Select the latest version of Controller software from the **Upgrade Version** drop-down list, and click the **Apply** button.
6. Click the **Upgrade Now** button.
7. Insert your USB memory stick into a port on a PC.
8. Browse to the `'Setup\Program Files\Gallagher\Command Centre\Device Software'` folder of the Command Centre Installation files, and copy the Controller software to your USB memory stick, (e.g. vCRx.xx.xxxxxxx.gglsec).

9. Insert the USB memory stick into the USB slot on the Controller. The Controller will go into a slow 1-flash state for up to 3 minutes, and then a 7-flash state to indicate that is has finished downloading the software.
   Note: Compared with C6000, the C7000 USB update speed is much faster, (i.e. the C7000 takes up to 5-10 seconds, whereas the C6000 takes up to 3 minutes).
10. Remove the USB memory stick.
    The Controller will restart.

How to know if the download has failed

The Controller will return to a normal 1-flash state, and the following alarm will be generated in Command Centre:
"[Controller] - USB Upgrade Aborted".

If this happens, the USB memory stick that you are using is more than likely incompatible. You will need to use a different USB memory stick, formatted using FAT, and containing only the Controller gglsec file.

Upgrading Multiple Controllers

Introduction

Using the Controller Upgrade feature to upgrade firmware on multiple Controllers simplifies the upgrade process and reduces the risk of errors.

The upgrade process involves downloading the software to the Controller, replacing the software on the Controller, and then rebooting the Controller.

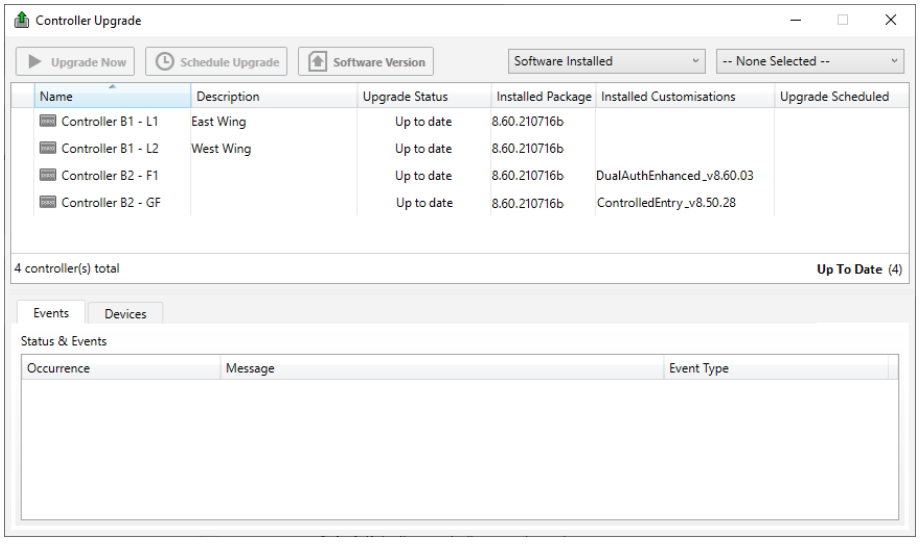
Prerequisites

Before performing this procedure, ensure:

- A Command Centre version upgrade has already been completed, and the workstation performing this Controller upgrade has already had a workstation Click-Once client upgrade.
- The Controller's new software version and customisations (if any) have been created in the Device Software List Window. Refer to ***Adding a new version of Device Software*** (on page 27-2) for the procedure.
  Note: Customisations do NOT need to be uninstalled before an upgrade.

Procedure

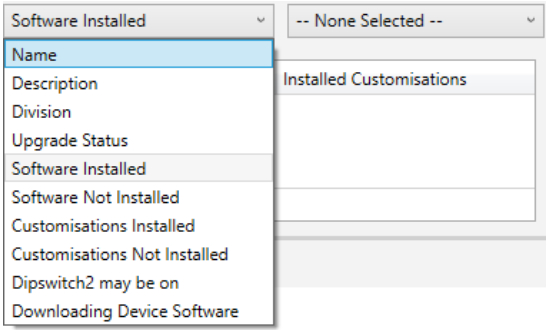
1. Click **Manage** from the menu bar, then **Controller Upgrade**.
   The **Controller Upgrade** Window opens (in grid view).
   All Controllers in the system are listed, and by default are sorted by 'Name'.



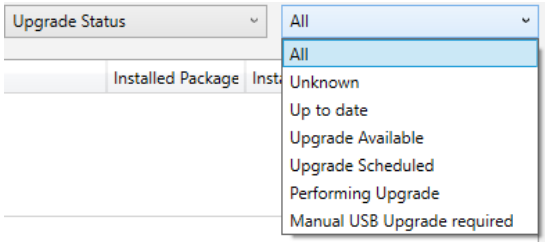
Notes:

- The Column Headers can be resized and/or repositioned, and the information in the columns can be resorted. See ***Grid View*** (on page 3-4) for further detail.
- The properties of a Controller in the list can be opened by either double-clicking on it, or right-clicking and selecting **Properties**. The Controller properties open on the **Status and Overrides** tab.

2. The filtering options at the top of this window allow you to sort and group Controllers, and determine which versions of firmware they are currently running.

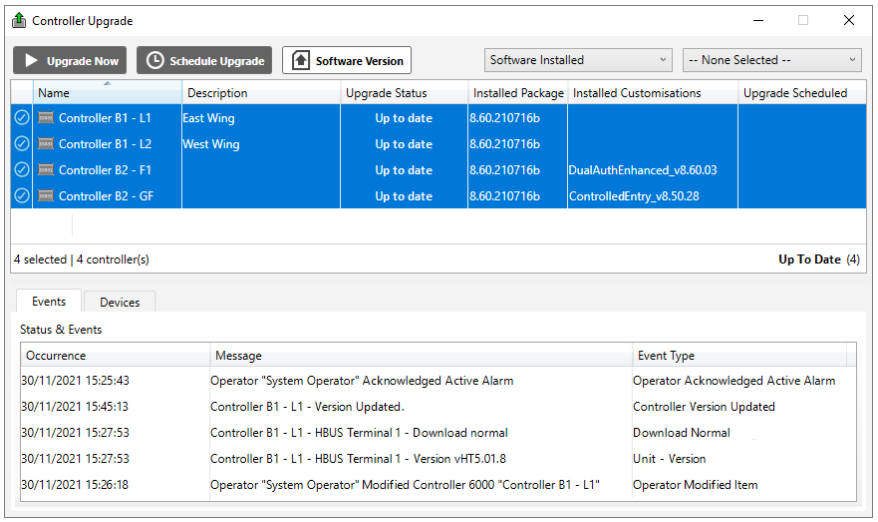


Set the appropriate search criteria from the filtering options, as follows:

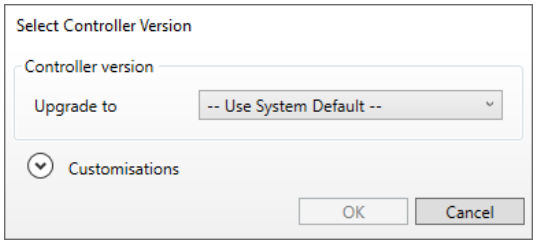
Filtering Option	Description
Name	This option allows you to type a name in the Search field. This may be useful if your site has implemented a naming convention for Controllers.
Description	This option allows you to type in the Search field. This may be useful if your site includes descriptions for Controllers, (e.g. notes about what the Controller is connected to or where it is located).
Division	Upgrades are typically done by building or area. If your site has specified Divisions for building or areas, this may be the preferred method of sorting and grouping the Controllers.
Upgrade Status	This option allows you to filter based on the current upgrade status of the controller. The status options are shown below:
Software Installed	This option allows you to select a software version from a drop-down list, which will then display the Controllers that are currently running that software.
Software Not Installed	This option allows you to select a software version from a drop-down list, which will then display the Controllers that are NOT running that software.
Customisations Installed	This option allows you to select a customisation from a drop-down list, which will then display the Controllers that are currently running that customisation.
Customisations Not Installed	This option allows you to select a customisation from a drop-down list, which will then display the Controllers that are NOT running that customisation.
Dipswitch2 may be on	Selecting this option will list any Controllers with Dipswitch2 on, and any other Controllers that are not online at the moment, (e.g. offline or not fully configured Controllers).

Filtering Option	Description
Downloading Device Software	Selecting this option will list any Controllers with any connected HBUS devices that currently have software downloading to them.

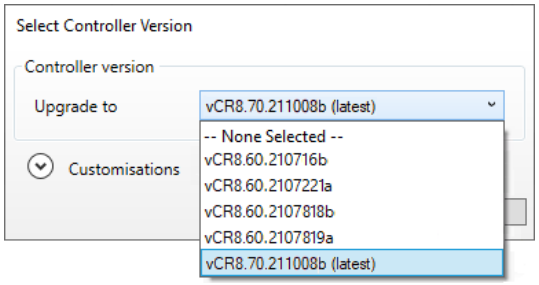
3. Select the Controller(s) you want to upgrade the firmware for, (i.e. click on an individual Controller, or for multiple Controllers hold the <**Ctrl**> key down while clicking on each Controller).
   The buttons across the top of the window become enabled.



4. Click the **Software Version** button.
   The Select Controller Version dialog displays.

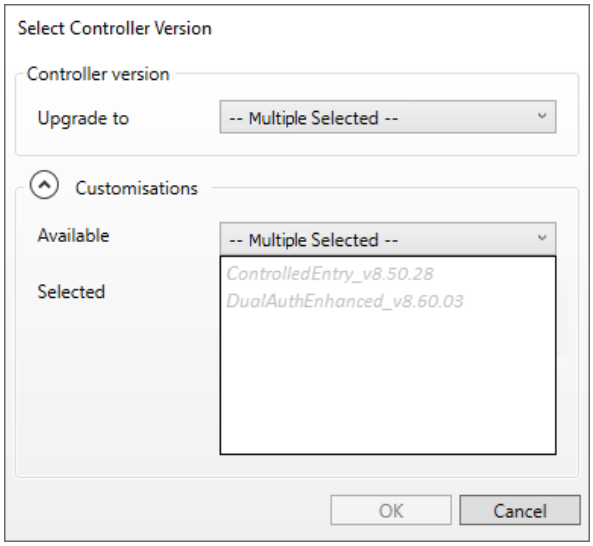


5. Click on the **Upgrade to** drop-down list and select the required Controller version.

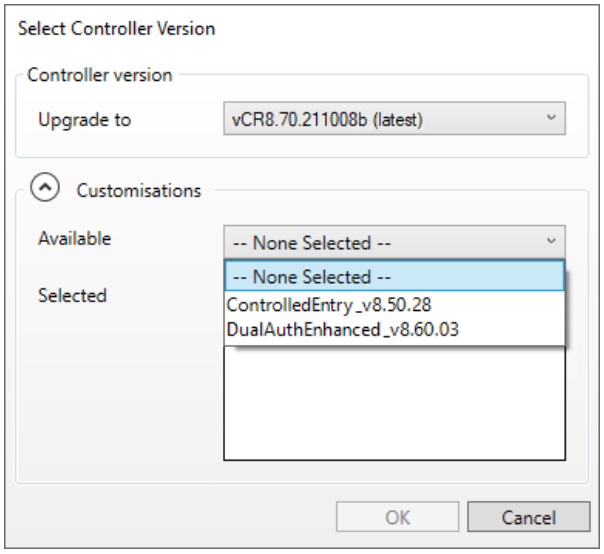


Notes:

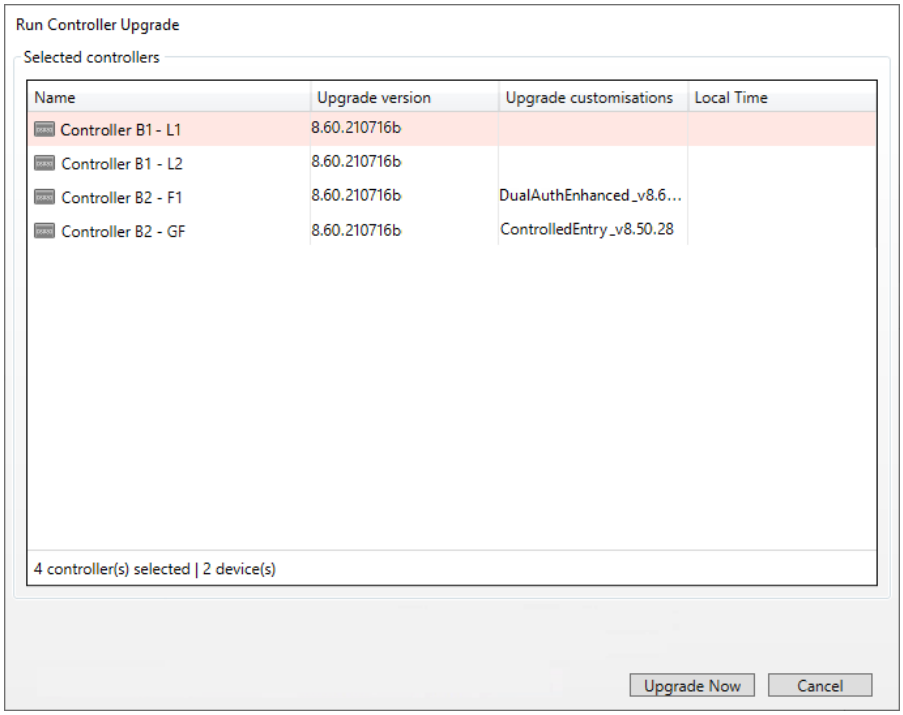
- The drop-down list shows the latest controller device software created in system with the label '(latest)'.
- If you selected multiple Controllers with different software or customisations configured, the software version fields will display **-- Multiple Selected --**.
  Any changes are then applied to all selected Controllers.



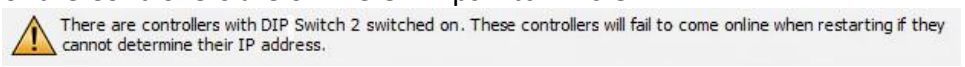
6. Expand the **Customisations** pane by clicking on the button.
7. Click on the **Available** drop-down list and select the required customisation.
   Note: The drop-down will be empty if there are no Controller customisations in the system.



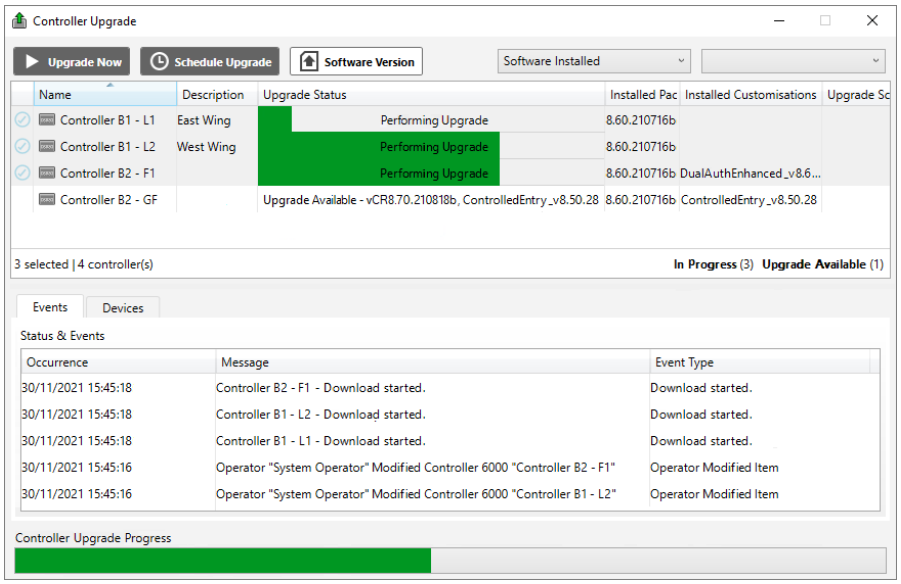
   The selected customisation will display in the **Selected** grid.
   Note: If you wish to remove a customisation from the **Selected** grid, highlight the customisation, right-click and select **Remove from List**.
8. Click the **OK** button.
   The Select Controller Version dialog closes.
9. Do you want to upgrade the Controllers now or schedule the upgrade for later?
   If **now**, go to Step 10.
   If **later**, go to Step 12.
10. Click the **Upgrade Now** button.
    The Run Controller Upgrade dialog displays.



Note: Upgrades require Controllers to be online and Dipswitch 2 to be OFF. A warning message will display in the lower part of this dialog if any of the Controllers are offline OR Dipswitch 2 is ON:



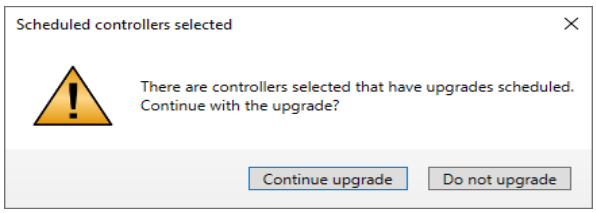
11. Click the **Upgrade Now** button.
    The Run Controller Upgrade dialog closes and the upgrade begins.



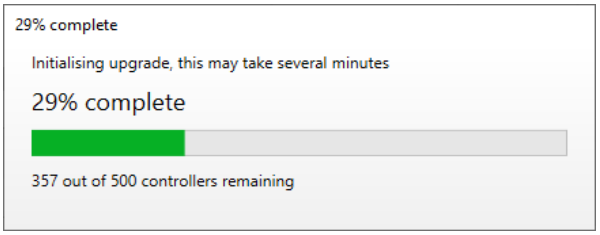
You can view the progress of the upgrade for each Controller in the **Upgrade Status** column, and the global progress bar at the bottom of the window displays the aggregated progress of all current upgrade activity.

Notes:

- If a user attempts to upgrade a Controller that already has an upgrade scheduled, the following message displays:



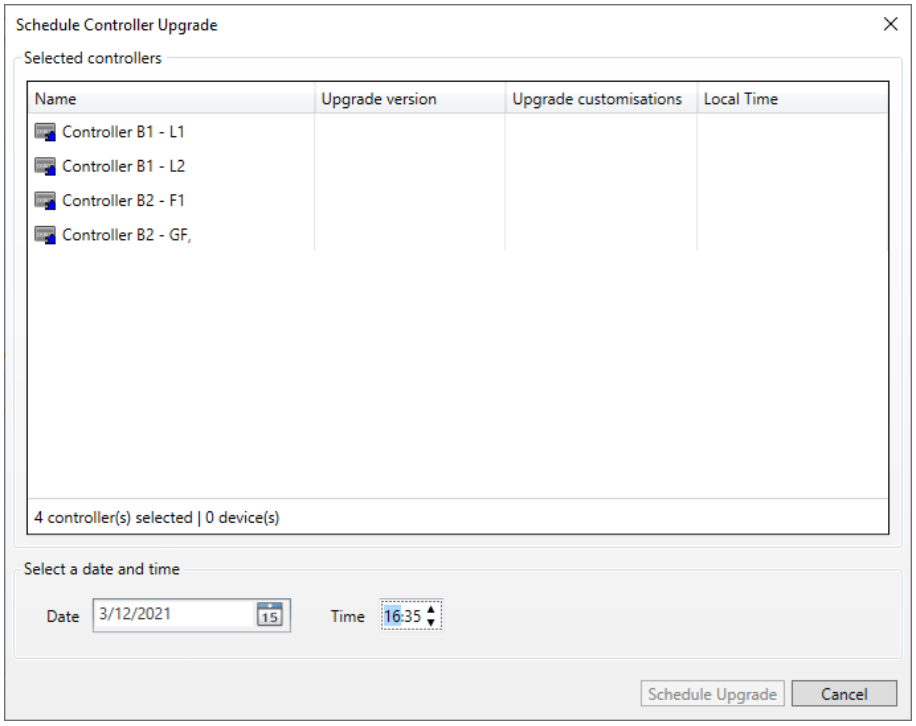
- With a large number of Controllers selected it can take a while for the upgrade to be initiated. In this case, a progress dialog will display:



The various states reflect what point the upgrade is at, as follows:

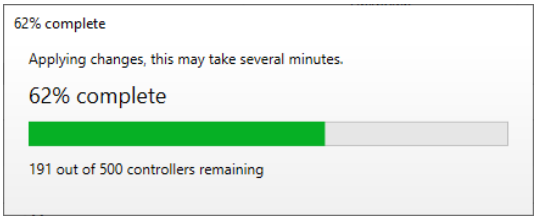
Upgrade State	Description
Error	There is a problem with the upgrade.
Manual upgrade with USB required	The Controller is running the installed software but not running the download software. A manual upgrade with USB is required because the Controller has the **Perform upgrades via USB** option selected (on the **Software** tab of the Controller properties).
Performing Upgrade	The Controller is currently downloading software or will start downloading as soon as possible.
Unknown	The Controller has not reported the software version to Command Centre yet. This can happen if the Controller has not come online even once or in some cases, the Controller has come online but the package version cannot be verified (in this case upgrading or re-applying the latest version of the Controller software onto the Controller may rectify this issue).
Upgrade Available <version>	There is new Controller software available. The Controller is running the installed software but not running the download software.
Upgrade Scheduled <date/time> <version>	The upgrade is scheduled for a future date/time, (i.e. the Controller is running the installed software but not running the download software. The Controller will start downloading software at the scheduled time).
Up to date	The Controller is up to date. There is no new Controller software, (i.e. the download software is the same as the installed software).

12. Click the **Schedule Upgrade** button.
    The Schedule Controller Upgrade dialog displays.

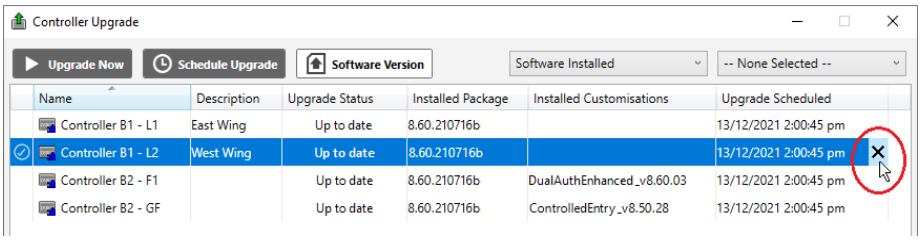


13. Specify a suitable time for the Controller upgrade to occur by entering the required **Date** and **Time**.
    Note: The Date and Time display according to the time zone of the operator. The **Local Time** column will be updated with the Controller's local time according to it's configured time zone, (i.e. where it is physically located).

14. Click the **Schedule Upgrade** button.
    The Schedule Controller Upgrade dialog closes and the date and time that the upgrade is scheduled for displays against each of the Controllers in the **Upgrade Scheduled** column.
    Notes:
    - With a large number of Controllers selected it can take a while for the upgrade to be scheduled. In this case, a progress dialog will display:



    - If for some reason you want to cancel the scheduled upgrade for a Controller, select the Controller and click on the ✕ that displays beside the date and time in the **Upgrade Scheduled** column.



Chapter 28: Services and Workstations

Services and Workstations are basically an "at a glance" way of determining which workstations and servers are using the Central Server as a host.

It mainly provides system status and configuration information, (e.g. does a Controller Server have a connection to the Central Server).

Services cannot be created manually. Instead, Command Centre creates them automatically whenever a new Service is detected. However, new Workstations can be created.

This chapter contains the following topics:

- ***Creating a new Workstation Item*** (on page 28-2)
- ***Editing a Service or Workstation Item*** (on page 28-5)
- ***Deleting a Service or Workstation Item*** (on page 28-6)
- ***Connecting to the Cloud*** (on page 28-7)
- ***Creating a REST API Client Item*** (on page 28-13)

Additional Services and Workstation items

In addition to Workstations, there are other items that can be created from the Services and Workstations List Window. These items are covered elsewhere in this manual, as follows:

Item	Description
Remote Server	Remote Servers are only required, and can only be created, if your site is licensed for Multi-server functionality. Refer to ***Multi-Server systems*** (on page 49-1) for further detail, and the procedure for creating a remote server.
Command Centre Cloud	A Command Centre Cloud item is only required if your site uses Mobile Connect. Refer to ***Mobile Connect*** (on page 31-1) for further detail, and the procedure for creating a Command Centre Cloud item.

Controller Service

The Controller Service is automatically created when the Controller Service first connects to Command Centre. The log level of this service can be changed on the **Configuration** tab of the Controller Service property page, with a value ranging from **Off**, (i.e. least verbose) to **Trace**, (i.e. most verbose). This setting will only filter log messages going into the Command Centre log file created by the Controller Service and not Controllers connected to the service.

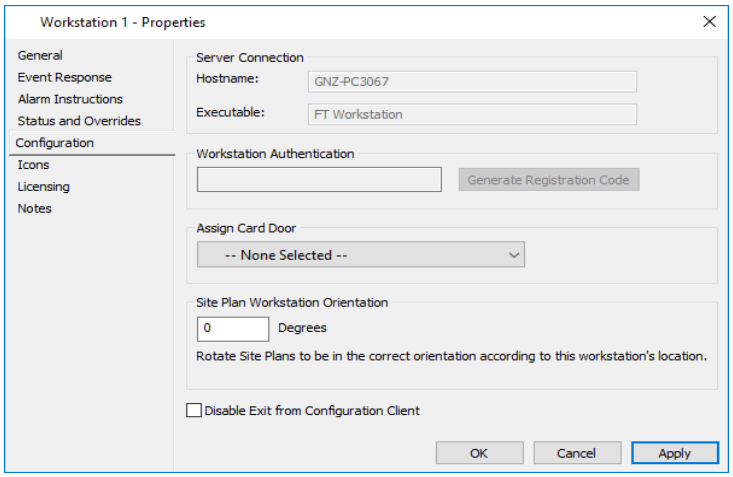
Creating a new Workstation Item

Introduction

This procedure enables you to create a new Workstation Item.
Note: Only Workstations can be created manually, (i.e. Services cannot be created manually. Instead, Command Centre creates them automatically whenever a new Service is detected).

Procedure

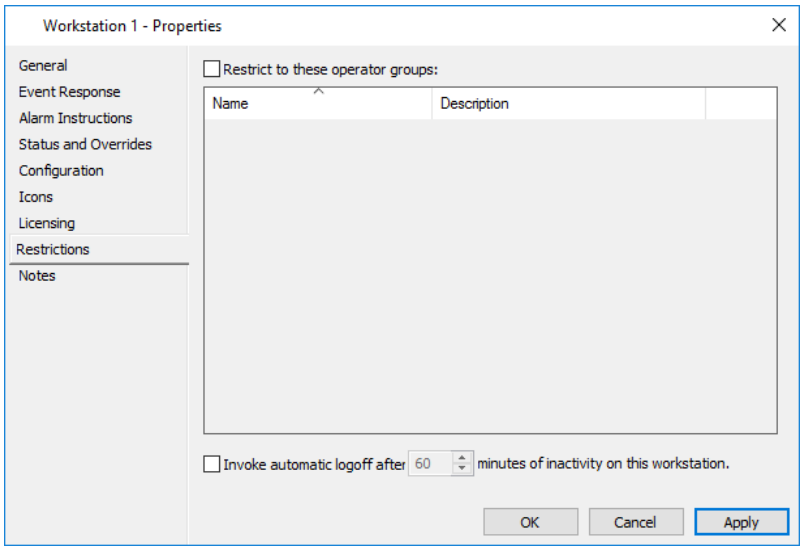
1. Click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens (in grid view).
2. **Right click** and select **New...Workstation**.
   By default, the **General** tab displays.
3. Complete the fields as required.
   For further detail 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 **Configuration** tab.



7. Enter the host PC name in the **Hostname** field.
8. If required, a Door's Reader(s) can be used for card reading and assignment by operators of this Workstation. To allow this, select a Door from the **Assign Card Door** drop-down list. You should choose a Door that is physically located near this Workstation.
   Note: There are no checks made to ensure there are valid Readers attached to the Door you select; you should make sure of this before selecting the Door.
9. The **Generate Registration Code** button is for Client Authentication purposes. Client Authentication verifies that a Workstation is what it claims to be, using a Client Certificate installed on the Workstation machine. If your site uses Workstation Restrictions the workstation needs to be registered with a registration code.

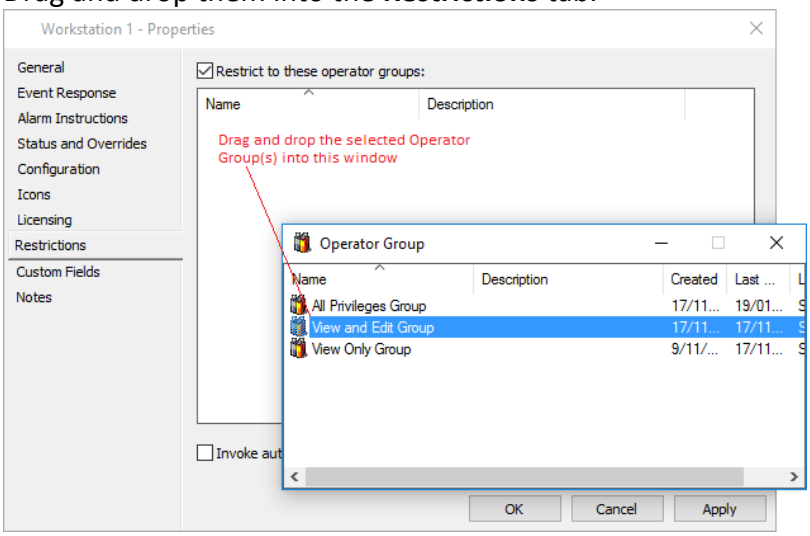
Refer to the "Client Authentication Appendix" in the *Command Centre Release Note* for further detail.

10. The **Site Plan Workstation Orientation** option allows site plans to be orientated to the workstation operator's seated position.
    If you want to rotate the site plan, enter the appropriate number between 0 and 359 degrees.
    Notes:
    - Site Plans rotate anti-clockwise.
    - Site Plan rotation cannot be configured for legacy Site Plans (Site Plans created in Configuration Client).
11. Check the **Disable Exit from Configuration Client** checkbox if you want operators to be unable to exit from this Workstation, to avoid accidental closure of it.
    Note: This feature only applies to the Configuration Client and NOT Command Centre Client.
    Checking the **Disable Exit from Configuration Client** checkbox disables:
    - the **Exit** button on the **File** menu bar,
    - the  button in the top right-hand corner, and
    - Close <**Alt**+**F4**>
12. Click the **Icons** tab if you want to change the Icon Set for this Workstation. For further details regarding the **Icons** tab, see ***Icons*** (on page 6-80).
13. Click the **Restrictions** tab.
    Note: This tab will only appear if configured to do so via the Server Properties (on the **Operator Defaults** tab).



14. Do you want to specify which Operator Groups this workstation is restricted to?
    - If **no**, go to Step 16.
    - If **yes**, tick the **Restrict this workstation to these operator groups** checkbox. The main grid becomes enabled.
15. Click **Manage** from the menu bar, then **Operator Groups**.
    The **Operator Group** List Window opens.

16. Select those Operator Groups you want the Workstation to be restricted to. Drag and drop them into the **Restrictions** tab.



Notes:

- There must be at least one Operator Group assigned when restricting privileges to a workstation. If you try to save the workstation without assigning any Operator Group(s) an error message will display.
- If you want to remove an Operator Group from the grid, the **Restrict this workstation to these operator groups** checkbox must remain checked.

17. Close the **Operator Groups** List Window.
18. Do you want this workstation to automatically log off after a specified period of inactivity?

If...	then...
yes	tick the **Invoke automatic logoff** checkbox and indicate the period of inactivity in the Time Box. **Note:** An automatic logoff time specified here for this workstation will override any automatic logoff time configured for the entire system, via the Server Properties (on the **Operator Defaults** tab).
no	go to Step 18. **Note:** By leaving the automatic logoff time as disabled, the workstation's automatic logoff time will be the same as the Server's value, (i.e. on the **Operator Defaults** tab of the Server Properties).

19. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Workstation Item.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
20. Click the **Notes** tab if you want to add a note(s) about this Workstation Item. For further details, see ***Notes*** (on page 6-85).
21. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Result

A new Workstation Item has been created.

Editing a Service or Workstation Item

Introduction

This procedure enables you to edit a Service or Workstation Item. You may wish to rename a Service or Workstation to a more user-friendly name.

Note: Editing may involve removing Operator Groups from the **Workstation Restriction** tab. To do this the "Restrict this workstation to these operator groups" checkbox (on the **Workstation Restriction** tab) must remain checked.

Procedure

1. Click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens (in grid view).
2. Highlight the Service or Workstation Item you wish to edit.
3. **Right click** and select **Properties**.
4. Edit the relevant information, (e.g. name).
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

The Service or Workstation Item details are changed.

Deleting a Service or Workstation Item

Introduction

The following procedure enables you to delete an obsolete Service or Workstation Item.

Notes:

- Services or Workstations assigned to a Site Plan can not be deleted.
- The Import/Export Services cannot be deleted. Even though they do initially disappear from your list when deleted, they will reappear within approximately five minutes.

Procedure

1. Click **Configure** from the menu bar, then **Services & Workstations**. The **Services and Workstations** List Window opens (in grid view).
2. Highlight the Service or Workstation Item you wish to delete.
3. **Right click** and select **Delete**.
4. A confirmation window displays.
   Click **Yes** to delete the Service or Workstation Item.

Result

The selected Service or Workstation Item is deleted from the system.

Connecting to the Cloud

Introduction

This procedure describes how to create a Command Centre Cloud item. This item connects your Command Centre system to the Cloud. This item represents the status of the Cloud. Only one Command Centre Cloud item can be created per Command Centre server. **Notes:**

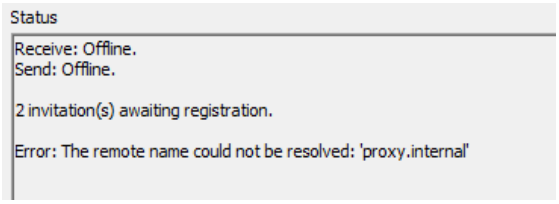
- The Command Centre server authenticates against the Cloud using a private certificate which is stored in Command Centre's database. If you wish to move your Command Centre installation from one server to another, refer to ***Server Migration*** (on page 28-12) for further detail.
- In a Command Centre multi-server environment, credentials issued on one server will replicate out to other servers. If you wish to issue credentials from multiple servers, you will need to create a Command Centre Cloud item on each Command Centre server used to issue credentials; the Command Centre Cloud item is not replicated across servers. If you wish to merge Command Centre servers that have been using this feature, please contact Gallagher Technical Support.
- If you attempt to issue credentials from a Command Centre server that does not have a Command Centre Cloud item, the credentials will sit in the "sending" state, until the mobile credential expires; no invitation email is sent.

Before you begin

Ensure you are logged on as an operator with the "Advanced User" privilege. **Note:** While the "Advanced User" privilege is required to create the Command Centre Cloud item, to edit the properties of the Command Centre Cloud item you only need the "Edit Site" privilege.

Procedure

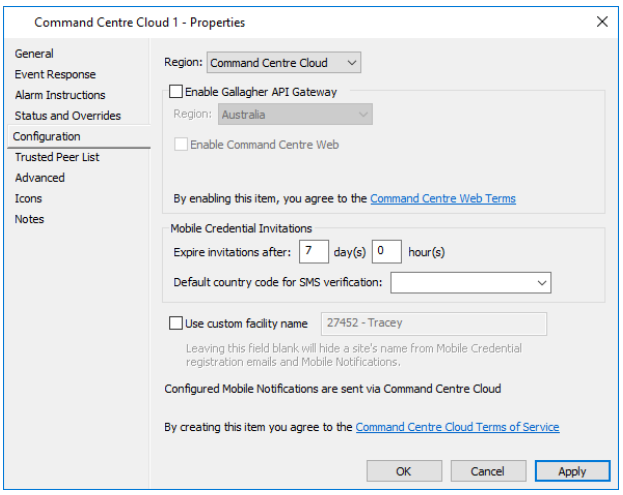
1. Click **Configure** from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens (in grid view).
2. **Right click** and select **New...Command Centre Cloud.**
   By default the **General** tab displays.
3. Complete the fields as required.
   For further 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 **Status and Overrides** tab. **Notes:**
   - When talking to the Cloud there are two communication channels; an inbound (Receive) channel and an outbound (Send) channel, either of which can be active independently of the other. Both the send and receive channels can be online, offline or idle independently of one another, and if there is a network error, it will now show some text related to that error. *For example:*



If...	then...
Idle	The channel has no work to do and has not attempted to connect to the Cloud.
Online	The channel has successfully connected to the Cloud.
Offline	The channel has attempted to connect to the Cloud, but has failed due to an error.

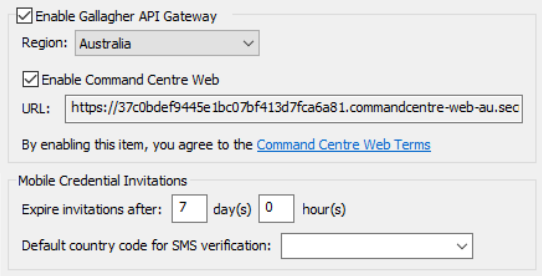
- If the Cloud is offline it is highly likely that the individual network configuration of the site (Firewalls, network connections, etc.) is preventing the connection. It is likely the IT staff on site will need to be involved to unblock the connection. More detailed error information may be available in the Command Centre log file.

7. Click the **Configuration** tab.



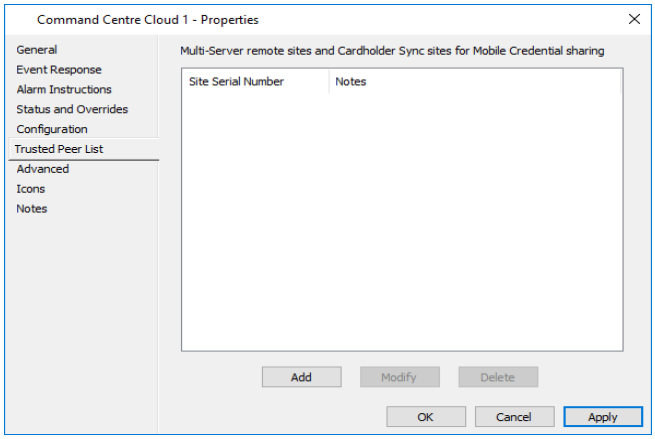
8. Configure as required.

Field	Description
Region	The 'Command Centre Cloud' resides in Sydney, Australia.
URL	This field only appears and is enabled when 'Custom' is selected as the **Region**. 'Custom' should only be selected upon advisement from Gallagher Technical Support. The URL is: ***Command Centre Cloud*:** DNS address: **commandcentre-ap-southeast-2.security.gallagher.cloud** It has two static IP addresses: **52.62.211.7** and **54.79.91.203**
Enable Gallagher API Gateway	The Gallagher API Gateway allows Command Centre Mobile, Rest API, Web Client, Apple Wallet and OneLink Clients to connect securely from anywhere without the need for complex reverse proxy solution or VPNs. If your site wants the ability to access Command Centre from any internet connected device, (including desktop and mobile), configure as follows:

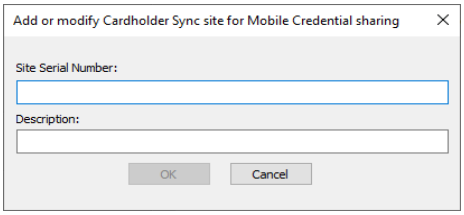
Field	Description
	a) Tick the **Enable Gallagher API Gateway** checkbox. The **Region** selector below it is enabled. b) Select the appropriate **Region** from the drop-down, (i.e. Australia, United States or Custom). **Note:** If you select 'Custom' a **URL** field will appear. Custom should only be selected upon advisement from Gallagher Technical Support. c) Tick the **Enable Command Centre Web** checkbox. A **URL** field displays populated with a system generated URL address. **Tip:** Clicking once in the **URL** field will highlight the entire URL to allow you to copy it.  d) Enter the appropriate country code in the **Default country for SMS verification** field by either typing it in or selecting from the drop-down list. e) Click the **OK** or **Apply** button to save your changes. **Note:** This step is necessary for the system to generate the correct URL address.
Region	This is the region that the Gallagher API Gateway resides in.
URL	This field only appears and is enabled when 'Custom' is selected as the Gallagher API Gateway **Region**. Custom should only be selected upon advisement from Gallagher Technical Support. The AU/US URLs are: ***Australian Gateway Region:*** DNS address: **commandcentre-api-au.security.gallagher.cloud** It has two static IP addresses: **3.106.1.6** and **3.106.100.112** ***United States Gateway Region:*** DNS address: **commandcentre-api-us.security.gallagher.cloud** It has two static IP addresses: **44.193.42.111** and **3.209.194.103**
Expire invitations after	This field allows you to configure the invitation expiry time period, (i.e. the invitation will be valid for 7 days from when it was registered to a user in Command Centre). The default invitation expiry period is 7 days. Minimum expiry period is 1 hour. Maximum expiry period is 100 days. When the invitation has expired, the invitation is removed from the Command Centre Cloud.
Default country code for SMS verification	Select or **type** the default country code for SMS verification of the mobile credential. **Notes:** • The country code specified here will automatically prepend the cardholder's mobile number when the SMS verification is sent. • If a cardholder's mobile number already specifies a country code, then the country code here will not be used. This enables

Field	Description
	cardholders within different regions to receive SMS verification, for mobile credential registration. • Typing a country code will display the option 'Custom' with your country code entered.
Use custom facility name	If the **Use custom facility name** checkbox is unchecked, the default facility name (taken from the Command Centre licence file) will be used in the invitation email subject line, (i.e. You have received a new mobile credential for [facility name]). To use a custom facility name in the invitation email subject line, check the **Use custom facility name** checkbox and enter a custom name in the text field. If you do not wish to use a facility name in the invitation email subject line, check the **Use custom facility name** checkbox and leave the text field blank.

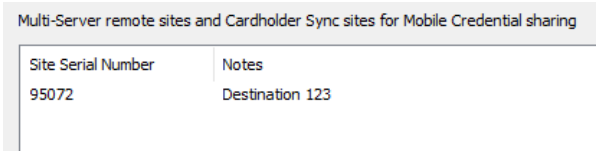
9. Click the **Trusted Peer List** tab.
   Note: Only sites using the Cardholder Sync Utility need to modify this tab.
   Source servers, (i.e. a server that shares cardholder information and mobile credentials with other servers) can define the Command Centre systems they want to share credentials with on this tab. The Gallagher Cloud will ensure mobile credentials are only shared with these trusted sites.
   For example: In a multi-tenanted building where a tenant needs to access both their own areas (controlled by one Command Centre system) as well as shared areas such as a lobby (controlled by another Command Centre system).



10. Click the **Add** button. The Add or modify Cardholder Sync site for Mobile Credential sharing dialog displays.

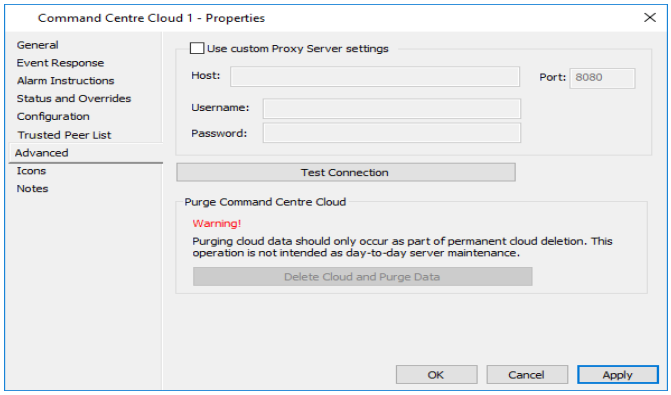


11. Add the **Site Serial Number** of the site you want to share credentials with and an appropriate **Description**.
12. Click the **OK** button. The dialog closes and the details you entered populate the grid on the **Trusted Peer List** tab. The Description you entered appears in the 'Notes' column. **Notes:**



- Highlighting a Cardholder Sync site in the grid and clicking the **Modify** button allows you to modify the Description. The Site Serial Number cannot be changed.
- A Cardholder Sync sites can be removed by highlighting it in the grid and clicking the **Delete** button.

13. Click the **Advanced** tab. This screen allows you to:
    - configure an outbound **Proxy Server** for Command Centre to use when talking to the Cloud.
      Note: Only HTTP(s) proxies are supported, (i.e. SOCKS and other proxy protocols are not supported).
    - purge Command Centre Cloud.
      WARNING: This feature should not be used in isolation, (i.e. purging the Cloud deletes all data in the Cloud as well as deleting the Cloud item itself). If a site wishes to create a new cloud item, mobile credentials will require reissuance. For further details refer to **Mobile Connect Cloud and App Security TIP.pdf** located in the `'Documentation'` directory of the Command Centre installation files.



14. Configure an outbound proxy server if needed, as follows:
    a) Tick the **Use custom Proxy Server settings** checkbox.
       The other fields become enabled.
    b) Enter the **Host** and **Port** for your proxy server.
    c) Enter logon credentials, (i.e. **Username** and **Password**).
15. Click the **Test Connection** button to check your connection to the Cloud. The message *"Successfully Connected to the Cloud"* will display if the connection is successful, otherwise the remote server will return an error message.
16. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Note: The Command Centre Cloud is now available for use by Mobile Notifications to send alarm notifications to Mobile Client users. Refer to ***Mobile/SMS Notifications*** (on page 6-54) for details on how to enable Mobile Notifications to be sent to Mobile Client users.

Server Migration

The TLS Client Certificate used to authenticate a Command Centre server against the Cloud is unique per server. It is stored in Command Centre's database.

If you move your Command Centre installation to a new server – typically by restoring a Command Centre backup onto a new machine – both the old and new servers will have a copy of the certificate and the cloud will treat them as a single instance. If the old server remains online this may lead to failure to issue Mobile Credentials or other connectivity problems.

If you wish to move your Command Centre installation from one server to another, and the old server is still online and connected to the internet, you must perform the **Disable Communication** override on the Cloud Item on the old server to prevent it from interfering with the new server.

You should not delete the Cloud Item from the old server. Simply disable communications and ideally power off the old server after migration.

Creating a REST API Client Item

Introduction

The REST Client item represents a credential that clients (other computers) can use to connect to the REST API Client. The properties hold a secure token which is used to authenticate the client.
Note: Operators require the "Advanced User" privilege to save a REST Client item.

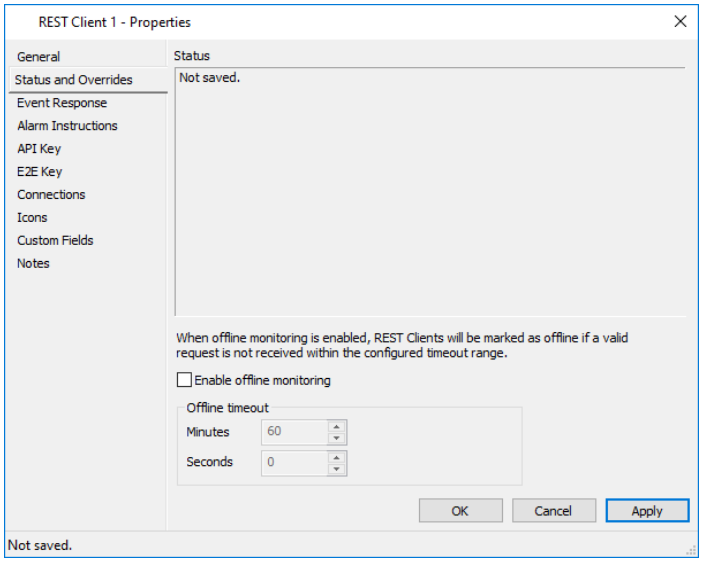
Before you begin

Before you begin this procedure, ensure the Client Certificate Thumbprint is created on the host machine that will be running the REST client. Refer to ***Creating the Client Certificate*** (on page 28-18) for instructions.

Using a client certificate increases security by limiting incoming REST connections to the Command Centre Server. REST connections will only be able to come from machines with a client certificate whose thumbprint matches the Server's Client Certificate Thumbprint.

Procedure

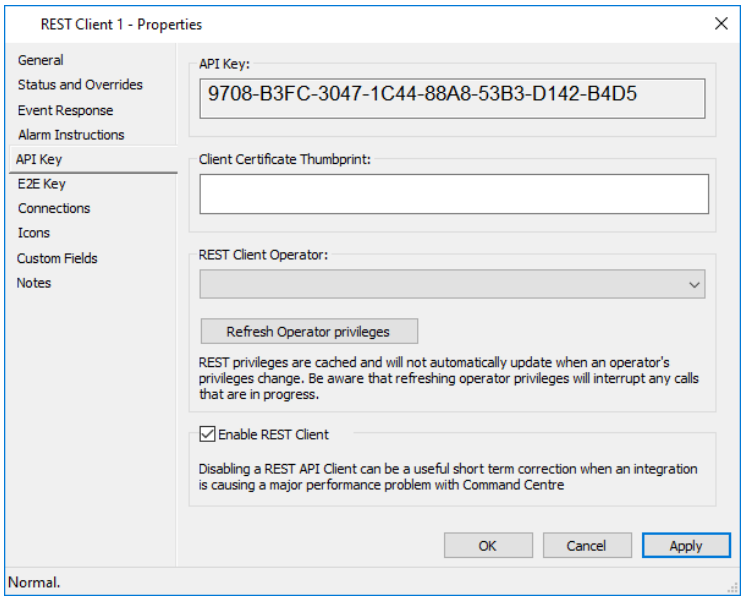
1. Click Configure from the menu bar, then **Services & Workstations**.
   The **Services and Workstations** List Window opens (in grid view).
2. Right click and select **New...REST Client**.
   By default, the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Status and Overrides** tab.



   REST Clients that use this REST Client item's API Key can push status updates that will appear on this tab.

5. The Enable offline monitoring check box (disabled by default) allows the REST Client item to enter the 'Offline' state if no REST request is received using this REST Client item's API Key within the configured timeout range.

6. If you selected the Enable offline monitoring check box, enter an Offline timeout. If no request is received for this duration, the REST Client item displays as 'Offline'. (Valid range is 30 seconds - 26 hours)
7. Click the **API Key** tab.
   Note: The **API Key** field is only visible if the Configuration Client operator has the 'Advanced User' privilege. REST Clients need this key in order to connect to the REST API.



   The **API Key** field is populated with an automatically generated secure token for the Rest Client.
8. Populate the **Client Certificate Thumbprint** field with the certificate thumbprint (found in the 'Details' tab of the Certificate file). Spaces are allowed, but remove any colons.
   Note: You can either enter the certificate thumbprint you have been provided or create one using the ***Creating the Client Certificate*** procedure (on page 28-18). Using a client certificate increases security by limiting incoming REST connections to the Command Centre Server. REST connections will only be able to come from machines with a client certificate whose thumbprint matches the Server's Client Certificate Thumbprint.
9. Click **Manage** from the menu bar, then **Cardholders**.
   From the Cardholder List Window drag and drop a Cardholder into the **Rest Client Operator** field. **Notes:**
   - The selected Cardholder must be assigned to an Operator Group, (i.e. the Cardholder must be an Operator).
   - Only one Operator can be added in this field.
   - The REST Client cannot be saved until an Operator is assigned.
   - The permissions assigned to this Operator's group will be applied to the REST session. To maximise security, we recommend giving this Operator's group the minimum privileges required, including denying the group privileges to use the Command Centre and Configuration clients.

- To ensure proper auditing, we recommend that each REST client uses a different operator.
- Ensure that the REST Operator for the remote Command Centre server does NOT have the 'View Alarm' privilege. Otherwise, "operatorRelogon" and "relogon" errors will be logged to the Command Centre log file.

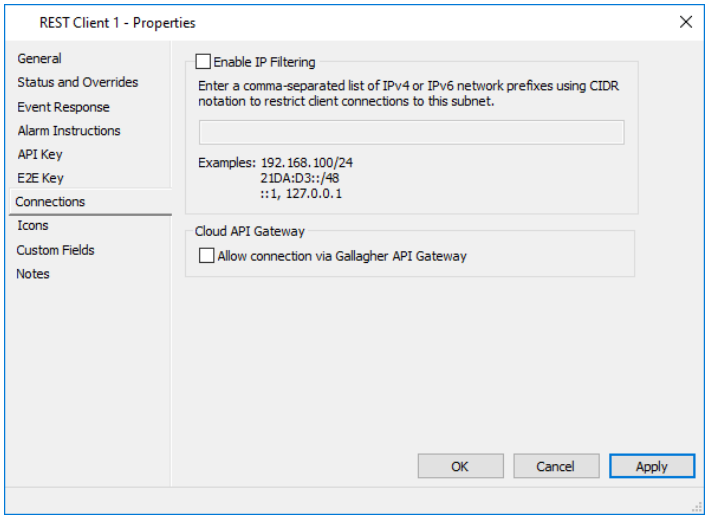
IMPORTANT: If the **Enable REST Clients with no client certificate** checkbox (in the ***Web Services tab*** (on page 6-30) of the Server Properties) is left unchecked as recommended, the Client Certificate Thumbprint must be copied from the certificate used by the REST API client and pasted into the **Client Certificate Thumbprint** field. If the **Enable REST Clients with no client certificate** checkbox is checked, the Client Certificate Thumbprint does not need to be entered; but it may be entered. If a Client Certificate Thumbprint is entered, it must match the client certificate (must be valid).

10. The **Refresh Operator privileges** button makes the REST Client aware of the REST Client Operator's current Operator Privileges. You need to click this button every time you change the REST Client Operator's privileges, or the REST Client will not know about the changes, (i.e. the changes will not take effect).
    Note: The logged-on Command Centre operator must have the 'Terminate Operator Sessions' Operator Privilege, or clicking this button will have no effect.
11. The **Enable REST Client** checkbox (enabled by default) allows a client to be disabled for diagnostic purposes.
    When disabled (unchecked) the REST client will stop working, and when enabled (checked) again the REST client will resume working.
    Operator events will be recorded when it is changed.

Set an IP address range (optional)

This allows sites to set a range of IP addresses using CIDR notation. Only clients that connect using machines within this IP range will be allowed access.

12. Click the **Connections** tab.



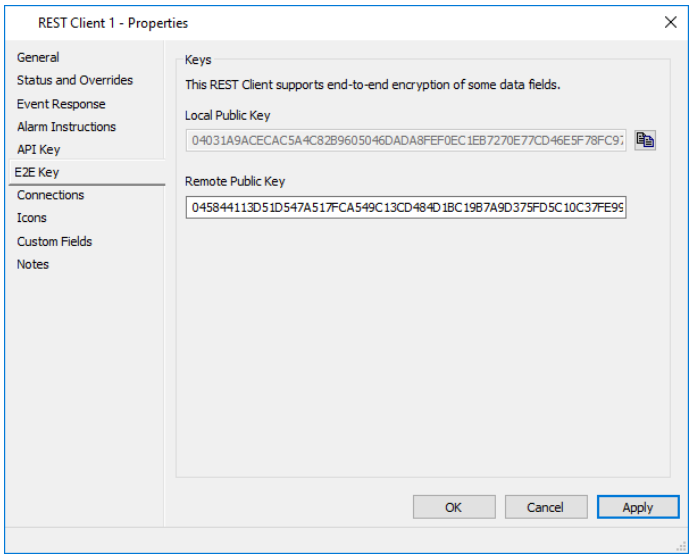
13. Check the **Enable IP Filtering** checkbox. The field below becomes enabled.
14. Enter the IP address range that you want to allow access, using the format

given in the example on screen.

15. Tick the **Allow connection via Gallagher API Gateway** checkbox if the site has configured the API Gateway and this REST Client is allowed to connect via the API gateway.
    Before using this feature you need to create a Command Centre Cloud item. See ***Connecting to the Cloud*** (on page 28-7) for the procedure.

Set up End to End Encryption for REST User Codes (optional)

16. Click the **E2E Key** tab.



17. Copy the local public key using the Local Public Key copy button  and paste it into your remote server.
18. Paste the equivalent key from your remote server into the **Remote Public Key** field. You are now set up for remote User Codes.
19. You need the "View Encrypted Cardholder User Codes" privilege (not part of "Advanced User") to see the resulting encrypted user code via the REST API.

Set up the E2E for API encoding (optional)

For the encoding API, E2E must be configured in order for the API response to contain the encoding payload (API will return a misconfiguration message if not configured).

20. Click the **E2E Key** tab.
21. Paste the equivalent key from your remote server into the **Remote Public Key** field. You are now set up for API encoding.
    Note: The **Local Public Key** isn't required for the encoding API.
22. You need one of the following privileges to see the resulting encrypted encoding data via the REST API:
    - "Advanced User"
    - "Print/Preview & Encode Card"
    - "Allow Re-Printing and Re-Encoding"
23. 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.

Test REST API connectivity with third party system (Chrome)

Before you begin

Before you begin these procedures:

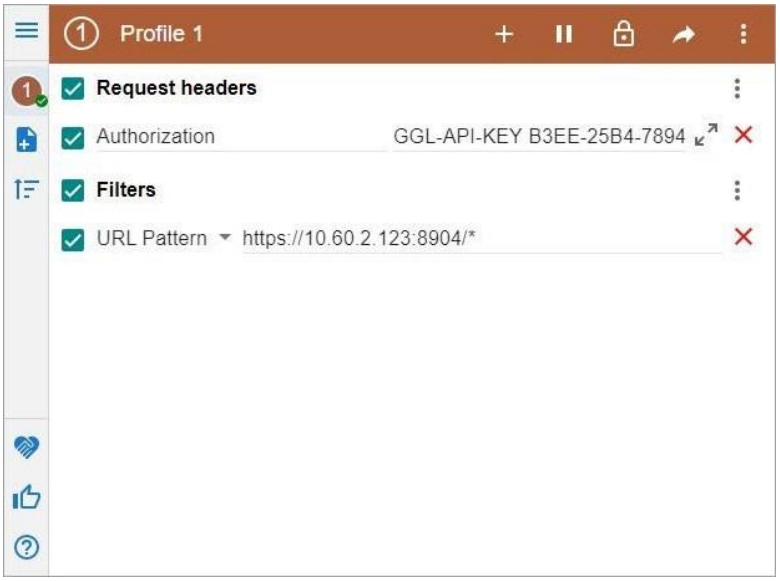
- Download and install a browser, we recommend Chrome.
- Add an extension (ModHeader) to Chrome to modify outgoing HTTP headers.
- Add an extension (JSON VIEWER) to Chrome to make the JSON response more readable.

Modify HTTP header

Perform the following procedure to add the Authorization HTTP header with the Client API key as its value.

Procedure

1. From the taskbar click **Start** > **Google Chrome**.
   Ensure the ModHeader extension is added to Chrome.
2. Click on the ModHeader icon showing on the top right-hand corner of Chrome. The ModHeader window displays.
3. Under the Request Headers section, enter Authorization.
4. Under the value section, enter: GGL-API-KEY [API key].



Note: This HTTP header modification may also apply to other outgoing HTTP headers, to prevent this, create a filter.

5. Click on the Add icon on the ModHeader window.
   The Menu option opens.
6. Select **Filter**. URL Pattern displays.

7. Create a filter using this syntax: https://[Your-IP address]:[Server Base Port]/*.

   For example: https://10.60.2.123:8904/*

View REST API events

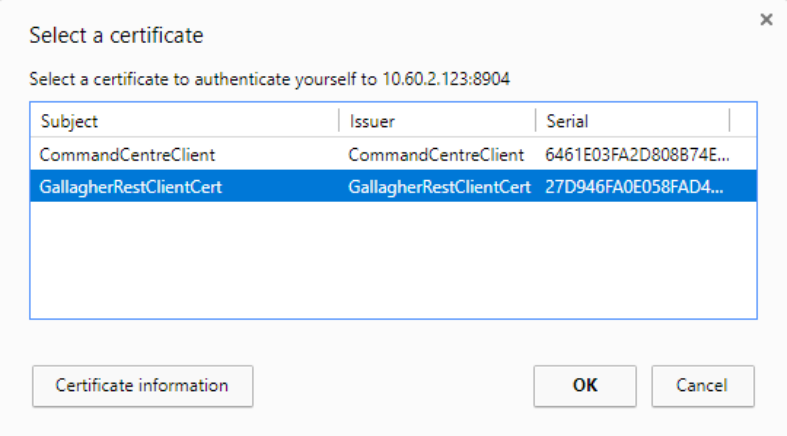
Perform this procedure to view events provided by REST.

Procedure

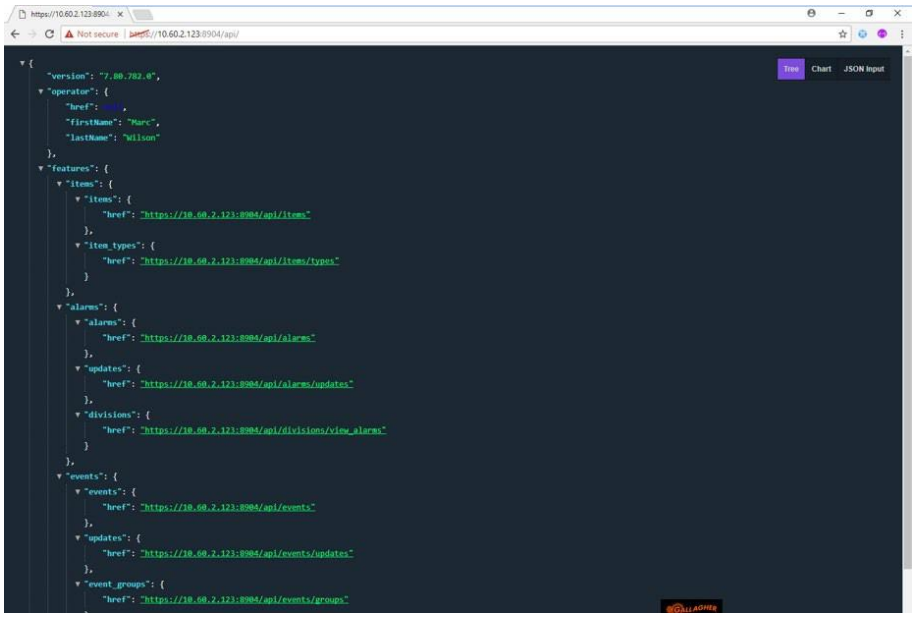
1. From the taskbar click **Start** > **Google Chrome**.
   Note: Ensure that JSON VIEWER is added as an extension to Chrome.
2. Enter the following URL: https://[Your-IP address]: [Rest API Port]/api/.

   For example: https://10.60.12.10:8904/api/

   Google prompts a certificate window.



3. Select the appropriate certificate, and click **OK**.
   The Operator's details, features, alarms and events display on the screen.



Creating the Client Certificate

When using a Windows operating system, PowerShell can be used to create the client certificate.

Perform the following procedure to create the client certificate thumbprint, and then add Network Service permission to the certificate.

Why use a Client Certificate?

Using a client certificate for REST connections to the Command Centre Server increases security. It means the Command Centre Server will only accept incoming REST connections that can provide a client certificate whose thumbprint matches the Client Certificate Thumbprint assigned to a configured REST Client item.

A client certificate is stored on a client machine. After creating the client certificate, you get its unique thumbprint and assign it to a REST Client item on the Command Centre Server. Now, that REST Client item will only accept incoming connections from the machine(s) that can provide its matching API Key and also have the client certificate that matches its assigned thumbprint.

Creating the certificate

1. Open the Run command by pressing <⊞+**R**> on the computer that will be connecting to the REST API.
   The Run command window displays.
2. Type 'PowerShell' and press <**Enter**>.
   The Windows PowerShell displays.
   Note: You may need to run PowerShell as an Administrator.
3. Enter the following command:

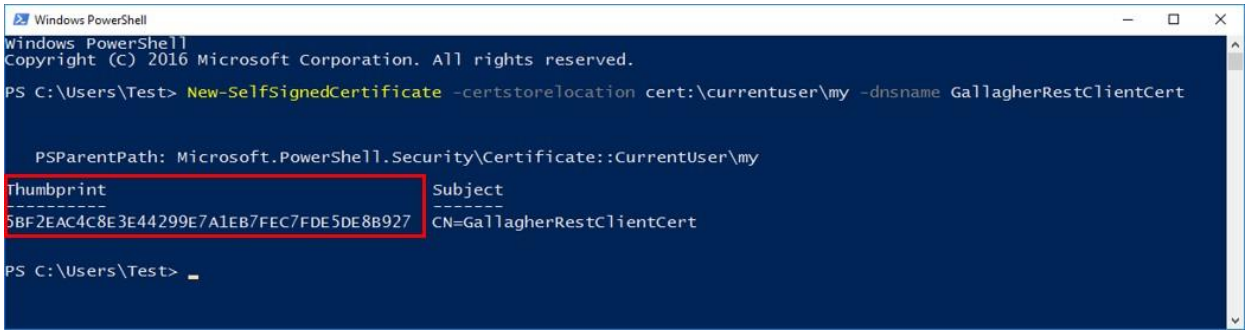
   ```
   New-SelfSignedCertificate -certstorelocation
   cert:\currentuser\my -dnsname [Certificate-Name]
   ```

   Example:

   ```
   New-SelfSignedCertificate -certstorelocation
   cert:\currentuser\my -dnsname GallagherRestClientCert
   ```

   Certificate name: Give your certificate a recognisable yet unique name (dnsname) so that it can easily be found later, while its purpose is also distinguishable from other REST Client Certificates potentially installed on the same machine. For example, if a site required a REST Client item for the Gallagher Cardholder Sync feature, the certificate could be named 'GallagherRESTClientCert_CardholderSync'.

Note: This script creates the certificate in the **Current User** > **Personal** > **Certificates** store. If the service making a REST connection will not be able to access the certificate there (e.g. the service is run as 'LocalSystem'), you should create the certificate in the **Local Computer** > **Personal** > **Certificates** store. Replace `'cert:\currentuser\my'` with `'cert:\localmachine\my'` and run PowerShell as the same user that the service runs as.



The above example creates the certificate “GallagherRestClientCert” in the **Current User** > **Personal** > **Certificate store**.

4. Copy the Thumbprint.
   The Thumbprint will be used in the ***Creating a REST API Client Item procedure*** (on page 28-7).
   Note: The certificate’s thumbprint can be viewed in the ‘Details’ tab of the Certificate file.

Chapter 29: External Alarm Monitoring

Contact ID

Contact ID is a DTMF (Dual Tone Multi-Frequency) protocol for transmitting event/alarm occurrences to remote alarm monitoring stations over telecommunications.

Contact ID requires a suitable modem device and uses an analog phone line. It requires exclusive use of the phone line when it is transmitting data.
Note: Contact ID is not currently supported on digital phone systems or over a GSM network.

The form of the message sent to the alarm monitoring station is as follows:

ACCT MT QXYZ GG CCC

ACCT Four digit Account number (0-9, B-F)

MT Two digit Message Type used to identify the Contact ID message to the receiver.

Q Event Qualifier which gives specific event information as follows:
1 = New Event or Opening
3 = New Restore or Closing
6 = Previously reported condition still present

XYZ Event Code (3 Hex digits 0-9, B-F), which is mapped to an existing Event group in Command Centre.

GG Group or Partition number (2 Hex digits 0-9, B-F).
00 can be used to indicate that no specific group or partition information applies

CCC Zone number (Event reports) or User number (Open/Close reports).
3 Hex digits 0-9, B-F.
000 can be used to indicate that no specific zone or user information applies.

For every alarm that is sent off site using Contact ID, a restoral event will also be sent to the monitoring station to indicate that the alarm condition has been attended to. See Events with Restorals for a list.
IMPORTANT:
There are a number of events that are exclusive to Command Centre and play no part in the Controller based Contact ID, and therefore will never provide Contact ID alarms.

Sites can choose to send multiple transmissions of the same alarm occurrence, (i.e. alarm floods) via Contact ID, or to send just one and then wait for an Alarm Zone Set/Unset before sending another. The multi-breaks option (see Alarm Flooding for details) determines how repeated alarm messages will be sent via Contact ID to a remote alarm monitoring company.

IP Alarm Monitoring

IP Alarm Monitoring uses another means of transmitting the alarms between the Controller and alarm receiving centre, (i.e. an IP Alarm Transmitter). The IP Alarm Transmitter uses TCP/IP to transmit messages to an alarm monitoring centre.

Messages are transmitted using the Offsite Alarm Transmission Protocol. This protocol uses the Contact ID ANSI\SIA DC-09 message format. Encryption can be enabled or disabled.

Messages are received by the IP Alarms Receiver Software. The IP Alarms Receiver Software forwards the messages via a serial port, using the Ademco 685 protocol, to the alarm monitoring system in the alarm monitoring centre.
Notes:

- While you can have digital cameras and Contact ID on the same Controller, the transmission error rates increase if you are doing rapid image triggering. Therefore, if you require rapid image triggering on a Controller, you should not have Contact ID on the same Controller.
- An online help file listing all the event/alarm messages in the system can be accessed via the Help menu bar in Command Centre, and will provide you with explanations of what each of the Contact ID messages mean.
- A Contact ID Assignment Report is available, which provides a list of all the possible Contact ID strings that can be sent from a Dialler to a remote monitoring station. See Contact ID Assignment Report for further detail.
- The "Edit Site" and "View Site" operator privileges are required for working with the Contact ID functionality.
- When using the Find Tool to locate items, those with Alarm Dialling configuration will have additional search criteria available on the **Alarm Transmission** tab, determined by what you select in the "Look in" field on the **General** tab, as follows:

Selection in the "Look in" field on the General tab	Field that appears on the Alarm Transmission tab
All items	**User or Zone Identifier (CCC)** field *
Cardholder	**User Identifier (CCC)** field *
any hardware item or site item (excluding Alarm Zone)	**Zone Identifier (CCC)** field *

Selection in the "Look in" field on the General tab	Field that appears on the Alarm Transmission tab
Alarm Zone	**Group Identifier (GG)** field. If a GG code is entered in this field, the search results will display the Alarm Zones that have been assigned that GG. If the GG value is left blank, then it will not be used as a search criterion.

* If a CCC code is entered in this field, the search results will display the cardholders or items that have been assigned that CCC. If the CCC value is left blank, then it will not be used as a search criterion.

Setting up Contact ID

Introduction

This topic is separated into four individual procedures that make up the process for setting up Contact ID, as follows:

1. Setting the Country Code

Setting the Country Code for an Alarm Transmitter/Dialler is done once you have physically connected the Alarm Transmitter/Dialler to the Controller. There are two methods for setting the country code, therefore use the method applicable to your situation. Either:

- via the Controller Diagnostics web page, or
- if circumstances do not permit for you to use the web page, the modem can be connected via a serial cable.

Refer to ***Setting the Country Code*** (on page 29-6) for both procedures.

2. Creating an Alarm Transmitter/Dialler Output (optional)

If you want to receive visual or audible acknowledgements when Alarm Zone armed messages are received by the monitoring company, an output(s) needs to be created for the Alarm Transmitter/Dialler.
Notes:

- More than one output can be configured for the Alarm Transmitter/ Dialler, (e.g. an audio output and a visual output).
- Ensure you set the output to pulse when activated.

Refer to ***Creating Inputs and Outputs*** (on page 21-50) for the procedure.

3. Configuring an Alarm Transmitter/Dialler

An Alarm Transmitter/Dialler gets configured in Command Centre, and is required to dial the monitoring company in three basic situations:

- When an alarm occurs or restores.
- When an Alarm Zone changes state between armed and any other state.
- Periodically to indicate that the Transmitter/Dialler is still functioning.

Refer to ***Configuring an Alarm Transmitter/Dialler*** (on page 29-10) for the procedure.

4. Assigning the Alarm Dialler to a Controller

Once an Alarm Transmitter/Dialler is configured, it needs to be assigned to a Controller in Command Centre.
(**Note:** Contact ID messages will be lost if a Controller is restarted for any reason.)

Refer to ***Assigning the Alarm Transmitter/Dialler to a Controller*** (on page 29-25) for the procedure.

5. Configuring Items for Contact ID

The items that are required to report Contact ID events need to be configured to do so by assigning CCC codes to them, and if you wish, CCC codes to card users who set and unset alarms.

The Alarm Zones that will be used for Contact ID also need to have GG codes assigned to them.
Note: Each Alarm Transmitter/Dialler must have a separate Alarm Zone for its reporting.

Lastly, you need to select which Action Plan will have an Alarm Transmitter/Dialler assigned. This action will start alarm dial out to the Monitoring Company.
Note: When setting the Action Plan to use an Alarm Transmitter/Dialler, ensure that the corresponding XYZ value is appropriate, as some of the Command Centre defaults may not be appropriate to your Monitoring Company.

Refer to ***Configuring Items for Contact ID*** (on page 29-27) for the procedure.

Setting the Country Code

Introduction

The Country Code needs to be set for an Alarm Dialler. This is done once the Alarm Dialler has been physically connected to the Controller, (the Installation Note provided with the Alarm Dialler has instructions on how this is done), and preferably before you configure the Alarm Dialler in Command Centre.

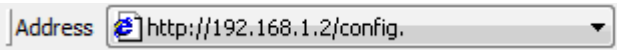
There are two methods for setting the country code, therefore use the procedure applicable to your situation:

- via the Controller Diagnostics web page, or
- the modem can be connected via a serial cable

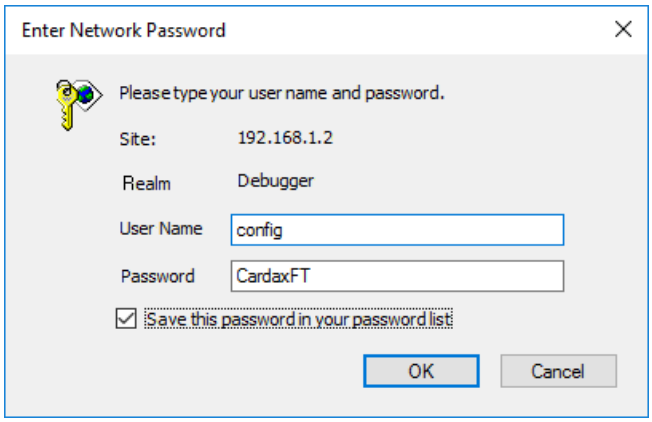
Procedure

Setting the Country Code via the Web Page

1. Ensure DIP Switches 1 and 2 are set on the Controller.
   Note: The Controller 6000 will need to be power cycled with DIP Switch 2 on to allow access to the Controller Diagnostics web page.
2. Open the Internet Browser.
3. In the **Address** field enter the IP Address of the Controller followed by a forward slash, then **config** followed by a full stop. See the example below for the correct format.

   Press the **Enter** key on your keyboard.
   The Enter Network Password screen displays.

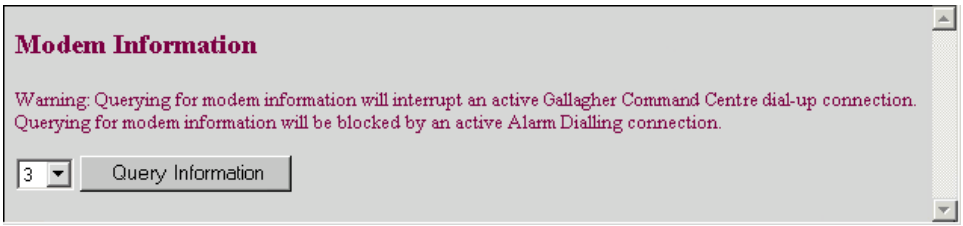
4. Enter **config** for the 'User Name' (all in lower case), and **CardaxFT** for the 'Password'. You also have the option to 'Save this password in your password list'.
5. Click the **OK** button.
   The Gallagher Controller Configuration screen displays.



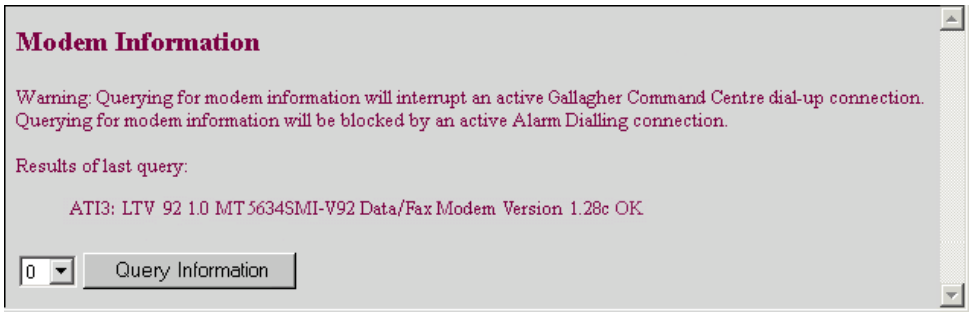
6. Select **Dial-up Configuration**.
   The Dial-up Modem Configuration screen displays.



7. Scroll down the web page to the **Modem Information** section.



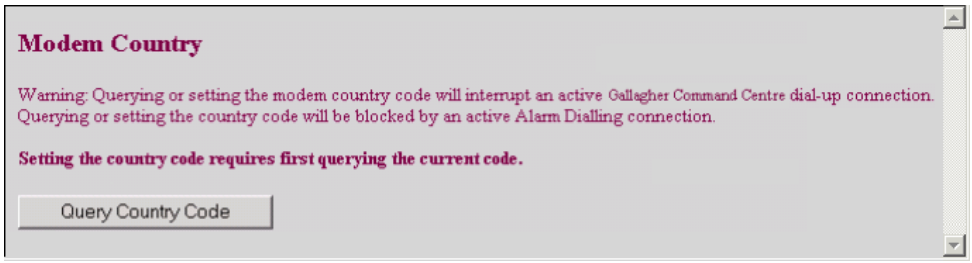
8. Specify the modem information string you wish to query, by clicking the drop-down menu list box and selecting the appropriate string.
9. Click the **Query Information** button.
   The following screen shot shows an example of the query results that display:



The results of this query show the level of the firmware on the socket modem. This query is used mostly for diagnostic purposes, therefore it is not essential that you perform this step.

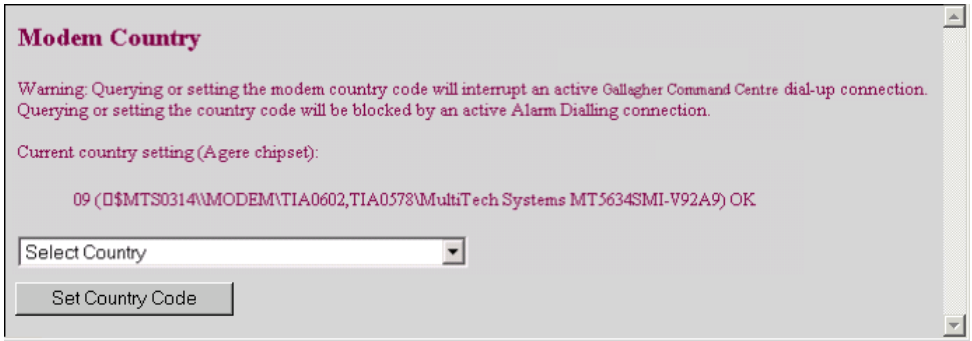
If however the Modem has not been connected to the Controller correctly, *"No Response"* displays in the query results.
If you query the Modem when the Alarm Dialler is using it, *"Alarm Dialler is using modem. Try again later"* displays in the query results.

10. Scroll down the web page to the **Modem Country** section.



This section of the web page displays all the countries that the modem supports.

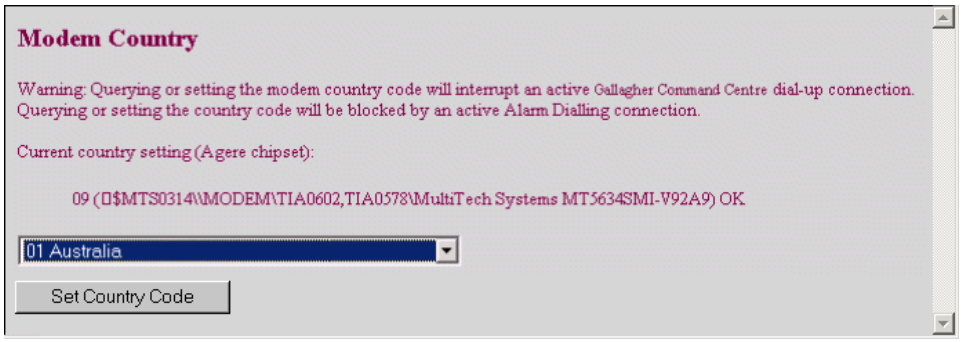
11. Click the **Query Country Code** button.
The current country setting displays.



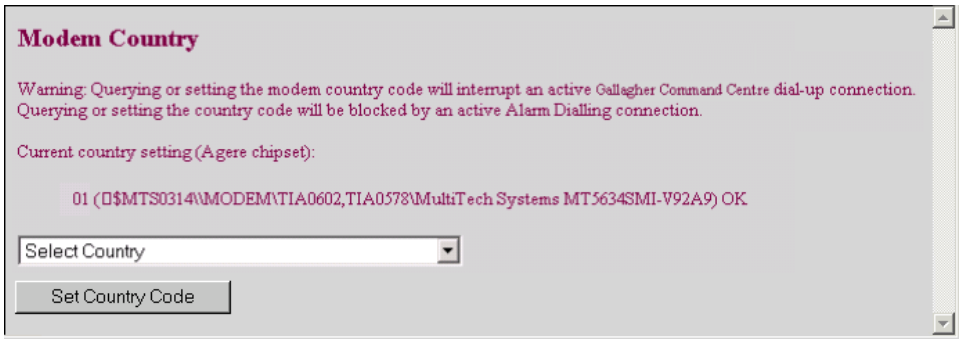
Note: In the example above the Country Code currently set is 09 New Zealand, therefore you would not need to re-set the Country Code if in New Zealand.

12. If you do require a different country setting from the one currently set, click the drop-down menu list box to display all the Country Codes, and select the Country Code you require. See Country Codes for details of all country codes supplied.

For example:
The following screen shot shows 01 Australia selected in the drop-down menu list list box.



When the **Set Country Code** button is clicked, the Country Code changes (in the following screen example it changes from 09 to 01) and the message in the drop-down menu list box reverts back to "Select Country".



13. Click the **Set Country Code** button.

Result

The Country Code has been set for the Alarm Dialler.

Next

Configuring an Alarm Transmitter/Dialler (on page 29-10)

Configuring an Alarm Transmitter/Dialler

Introduction

This procedure enables you to create an Alarm Transmitter/Dialler in Gallagher Command Centre.

Before you begin

Before you begin this procedure ensure you have:

performed ***Setting the Country Code*** (on page 29-6).

created an output(s) for the Alarm Transmitter/Dialler (using the ***Creating Inputs and Outputs*** procedure on page 21-50), if you want to receive visual or audible acknowledgements when Alarm Zone armed messages are received by the monitoring company.
Notes:

- More than one output can be configured for the Alarm Transmitter/Dialler, (e.g. an audio output and a visual output).
- Ensure you set the output to pulse when activated.

Procedure

In Command Centre, click **Configure** from the menu bar, then **Hardware**.
The **Hardware** List Window opens (in tree view).

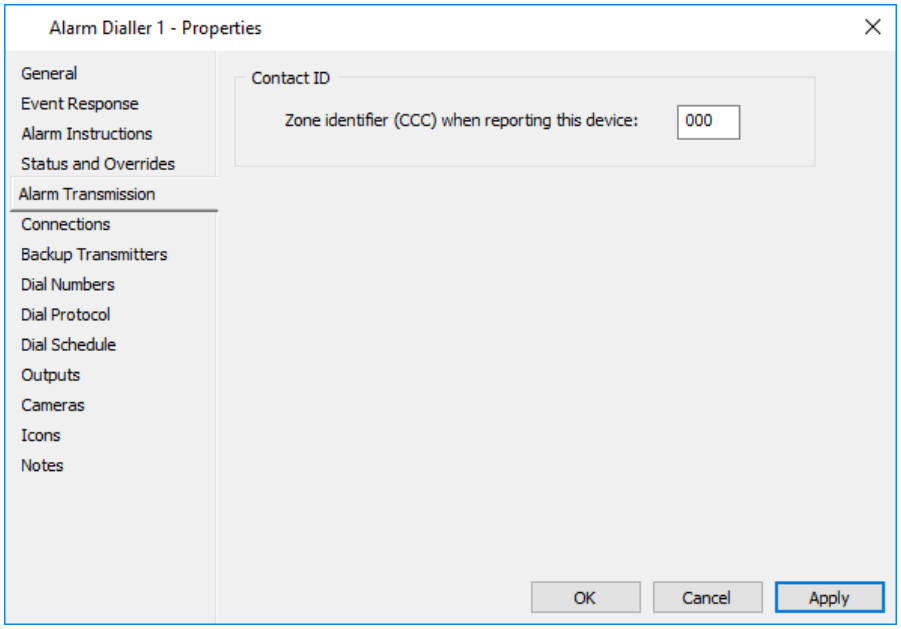
Right click and select either:
New...RS232 Devices > **Alarm Dialler**, or
New...IP Alarm Transmitter.
By default the **General** tab displays.

Complete the fields as required.
For further detail see ***General tab*** (on page 3-18).

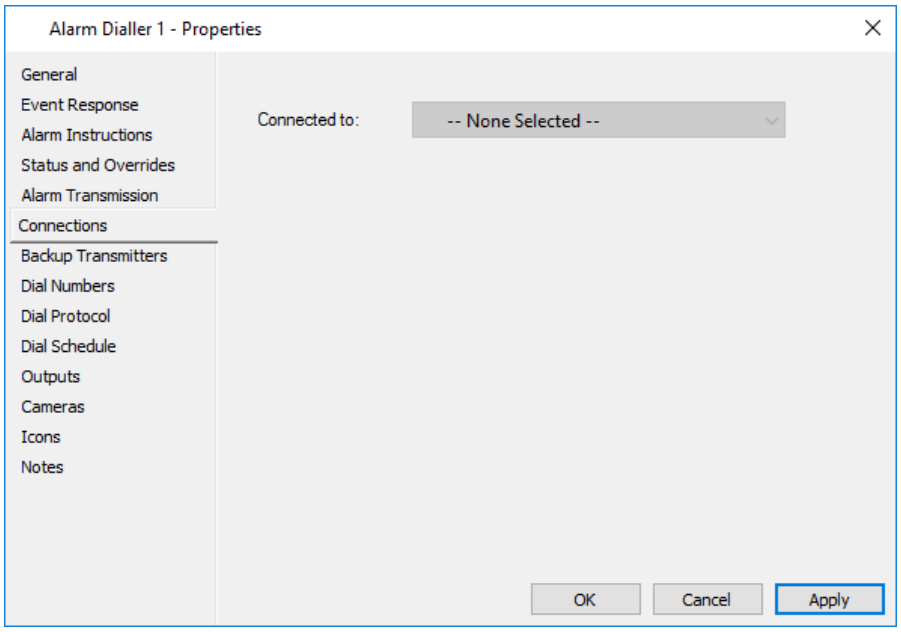
Click the **Event Response** tab, and configure as required.
For further detail see ***Event Response tab*** (on page 3-20).

Click the **Alarm Instructions** tab, and configure as required.
For further detail see ***Alarm Instructions tab*** (on page 3-22).

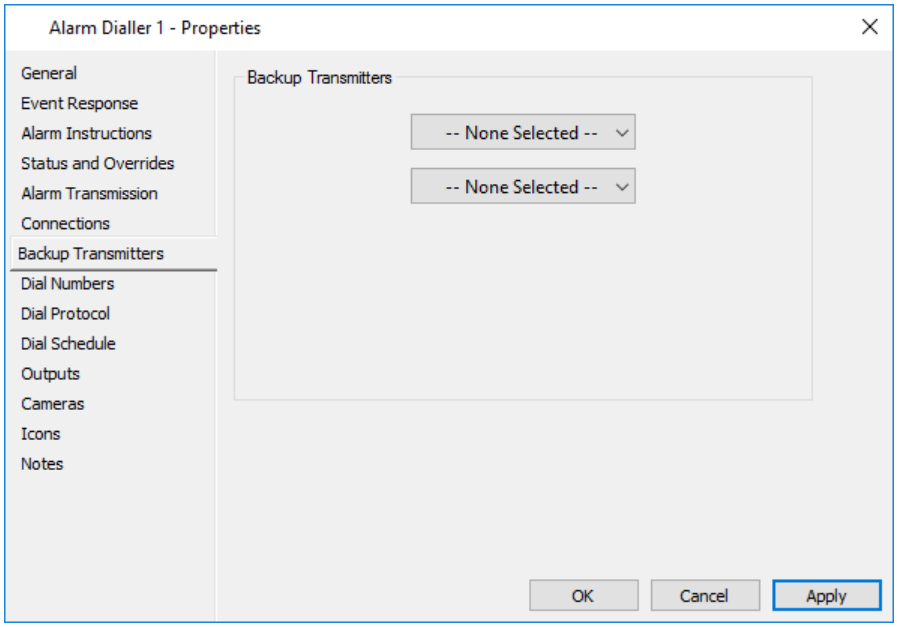
Click the **Alarm Transmission** tab.



7. Enter the zone identifier for Contact ID.
   Notes:
   - This field will accept 3 Hex digits 0-9, B-F.
   - The default of 000 can be left if you do not wish to indicate a specific zone or user information.
8. Click the **Connections** tab.



   This tab shows the Controller that this Alarm Transmitter/Dialler is connected to. This has to be configured from the **Alarm Transmission** tab of the Controller properties. Refer to ***Assigning the Alarm Transmitter/Dialler to a Controller*** (on page 29-25) for the procedure.
9. Click the **Backup Transmitters** tab.

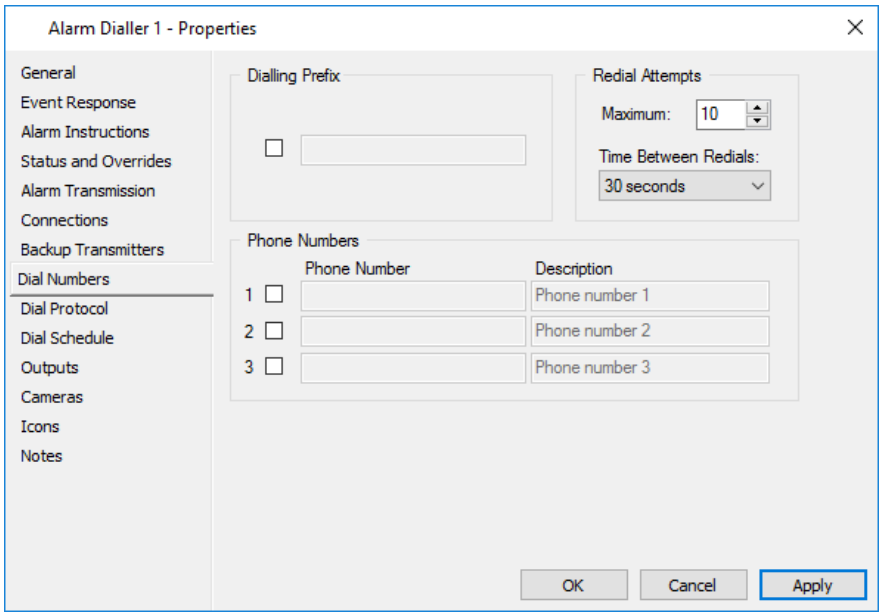


A Backup Transmitter/Dialler can take over from an Alarm Transmitter/Dialler that is having trouble communicating due to any number of problems. Each Alarm Transmitter/Dialler can have up to two backup transmitters/diallers.

Notes:

- Backup Transmitters/Diallers can only be nominated for LAN connected Controllers.
- A Transmitter/Dialler on a Dial-up Controller can not act as a backup for a LAN based Controller.

10. Click the drop-down menu box(es) and select the appropriate Alarm Transmitter/Dialler to be used as a backup transmitter/dialler.
11. Are you configuring an Alarm Dialler or an IP Alarm Transmitter?
    If an **Alarm Dialler**, go to Step 12.
    If an **IP Alarm Transmitter**, go to Step 21.
12. Click the **Dial Numbers** tab.



13. Tick the checkbox under **Dialling Prefix** and enter the number required to dial out of the internal phone system.
    A maximum of eight digits can be entered.
    Each Dialler can be configured to dial up to three numbers in an attempt to communicate with an alarm monitoring station, as follows:

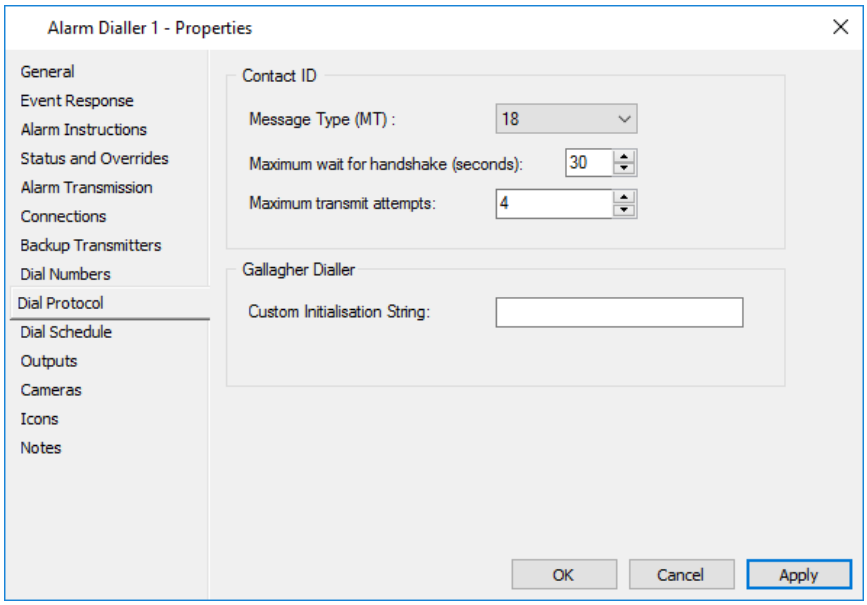
Field	Description
Phone Number 1	This is the first phone number that the Dialler will call when a Contact ID message needs to be sent. (Maximum 32 digits)
Phone Number 2	This is the second phone number that the Dialler will call once all attempts on Phone Number 1 have expired. (Maximum 32 digits)
Phone Number 3	This is the third phone number that the Dialler will call once all attempts on Phone Number 2 have expired. (Maximum 32 digits)
Description	The Description fields for the phone numbers allow a text description of each number to be entered so the numbers can be easily recognised. These descriptions will also appear in an audit trail rather than disclosing the actual called numbers.

14. Complete the **Redial Attempts** as required:

Field	Description
Maximum	(Range is 1-99, and default is 10 attempts) This is the number of redials that the Dialler will attempt before moving onto the next phone number. If this number is set to 10, then a total of 11 calls will be made to the first phone number, (i.e. the first attempt and then 10 more attempts). Once the redial attempts have expired then the Dialler will move to the next number on the list and the same rules will apply to that number, being that the first attempt will be followed by the number of redial attempts. Once all redial attempts have expired an alarm can be generated by an Action Plan. Events are held for 15 minutes, then the sequence starts again. If you assigned a Backup Dialler(s) at Step 16, then once all attempts have been made with this Dialler, the messages will be passed to the backup Dialler(s) for transmissions. **Notes:** • Each Dialler supports 255 events being held in the buffer, so if there are more than 255 events to be sent via Contact ID, the oldest events will be discarded. A message is generated however in the Event Log to advise the Date, Time and details of the discarded event(s) to provide a full audit trail. • A 15 minute wait period is started after all attempts at

Field	Description
	connecting to the security company's Contact ID receiver have failed. During this period, if further Contact ID alarms occur, no Contact ID events appear in Command Centres event viewer window and no further dialler activity is initiated. Take this functionality into account when you have no backup dialler, assign only one telephone number, and set the Redial Attempts Maximum to 0. If the dialler tries to report a Contact ID event and encounters say a busy line, subsequent Contact ID transmission attempts will be inhibited for 15 minutes.
Time Between Redials	This is the time value between calls that are made to the designated phone numbers. **Note:** This should be set according to your local telecommunications company specifications. (Range is 1 second to 1 hour. The default is 30 seconds)

15. Click the **Dial Protocol** tab.

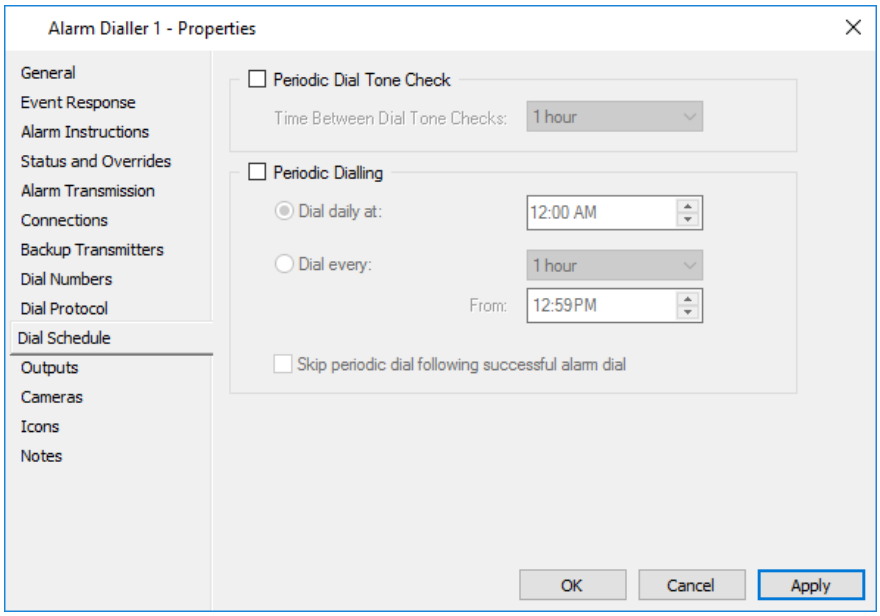


16. Complete the fields on this tab as required.

Field	Description
Message Type (MT):	This two digit sequence is used to identify the Contact ID message to the receiver. It may be transmitted as either 18 (which is the default and the preferred option), or 98 (optional). **Note:** New receivers will accept either an 18 or a 98, however some older receivers may not accept a 98.
Maximum wait for handshake (seconds):	This value determines how long the modem will wait for a connection and "handshake" from the alarm monitoring receiver. If no valid handshake is detected by the end of the wait time, (this could happen because of busy receiver telephone lines, or there was no answer at the called

Field	Description
	number), then an Alarm Dialling failure alarm can be generated and the system will retry again after the time between redials has elapsed. (Range is 1 to 255 seconds. The default is 30 seconds.)
Maximum transmit attempts:	The number of transmit attempts to send the same Contact ID string to the receiver during the same call, before hanging up and redialling. The attempts counter is reset each time a valid kiss-off signal is received. (Range is 1-4 attempts. Default is 4 attempts.)
Custom Initialisation String:	It is unlikely your site will need to enter an intialisation string, therefore it is important you leave this field BLANK. However there are cases where you may need to add an initialisation string, as follows: • If your Contact ID receiver (normally located at the alarm monitoring company) happens to be on the same PABX as the Dialler, or • If you are experiencing problems with reliably receiving Contact ID messages at the receiver. In these situations, contact Gallagher Group Limited (Tech Support) for further instructions on entering an initialisation string.

17. Click the **Dial Schedule** tab.



18. If you want to check for dial tone on the line on a regular basis, tick the **Periodic Dial Tone Check** checkbox and select the time from the drop-down list for the frequency of the check.
Notes:
    - The checks can be as frequent as 1 minute or as intermittent as 24 hours. (The default is 1 hour)

- If an Alarm Dialler fails a “Periodic Dial Tone Check”, an alarm will be generated.
- The line is not broken during these dial tone checks, and an alarm is raised if there is no dial tone on the line when it is checked. You can use an Action Plan to annunciate these alarms to Command Centre, and optionally send them out from another Dialler on the system.
- It is recommended that Diallers are connected to a dedicated phone line, or at least a line that is used infrequently by other devices on that line. In the case of a shared line, the Contact ID Dialler must be the first device that can break or use that line.
- If there is more than one Alarm Dialler on your system, unique periodic tests must be sent from each Dialler. The periodic dial test works as follows:
  - **ACCT:** If an Alarm Zone is assigned to the Dialler **and** the Alarm Zone overrides the site ACCT code, **then** the periodic test dial will use the Alarm Zone's ACCT code, **otherwise** the periodic test dial will use the site's ACCT code.
  - **GG:** If an Alarm Zone is assigned to the Dialler, **then** the periodic test dial will use the Alarm Zone's GG code, **otherwise** the periodic test dial will have a GG code of "00".
  - **CCC:** The periodic test dial will use the zone identifier (CCC) that has been assigned to the Alarm Dialler.

19. The timer test can also be configured on this tab by ticking the **Periodic Dialling** checkbox and then setting the frequency of the tests by clicking the appropriate radio button.

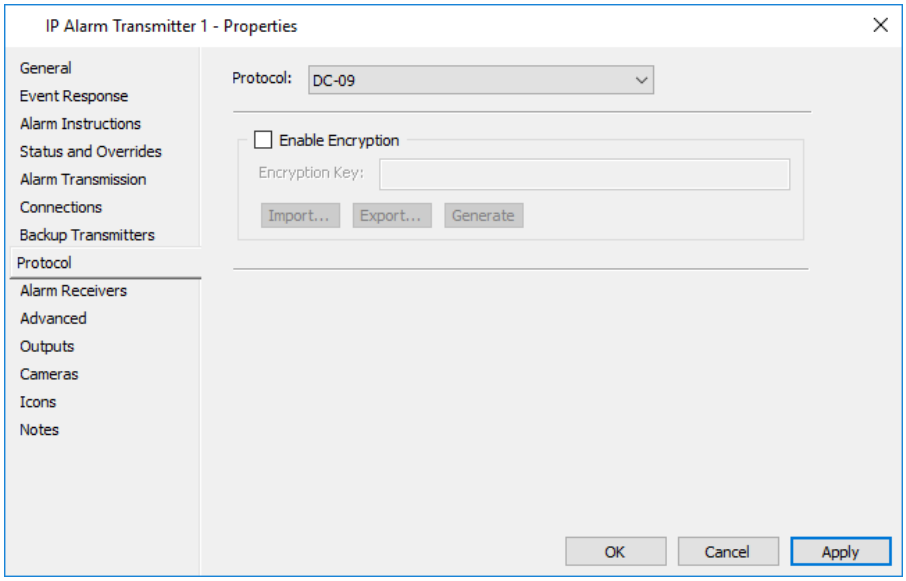
Option	Description
Dial daily at:	Selecting this option will mean that a Periodic dial will occur at the same time each day. Always set it for a time of the hour or half hour to avoid overloading the monitoring station at these times. If you change the periodic dial time, notify the monitoring station of the new test time. The time will automatically adjust for daylight savings. **Note:** Remember that this is based on the time at the Controller, not at Command Centre.
Dial every:	Select this option if you require more frequent periodic test dials. This means that a periodic dial will occur at the interval specified, starting at the time that has been specified. Time intervals allowed = 30 minutes, 1, 2, 3, 4, 6, 8 or 12 hours. Anytime can be entered in the start time. Daylight savings corrections will be applied when the Controllers clock is updated.

The timer test (also known as the ‘periodic test’ or ‘24 hour’ test), is an indication to the monitoring station that the alarm system is capable of sending Contact ID. Most systems send one test per day. The signal is fixed in its format and will be sent with a XYZ (contact id event code) of 602 and it will be sent in the (GG) partition or Alarm Zone 00. Only one

periodic test can be enabled per account number for accurate reporting of line status (this is a consideration when using multiple Diallers using single client code reporting). It may be necessary to configure periodic tests from different diallers into different account numbers. It will also be reported as a new event and will have a CCC of 000, (e.g. 123418160200000, where 1234 is your account number).

If a test is not received action is taken by the monitoring station staff, which may include phoning the site to check that the phones are working.

20. Tick the **Skip periodic dial following successful alarm dial** checkbox if required.
    By enabling this feature, the periodic dial will get skipped when there has been a successful alarm dial since the last periodic dial test.
    If the periodic dial is skipped, the next time you can expect a periodic dial is after the periodic dial interval (or at the same time of day tomorrow), depending on how it is configured.
21. Click the **Protocol** tab.

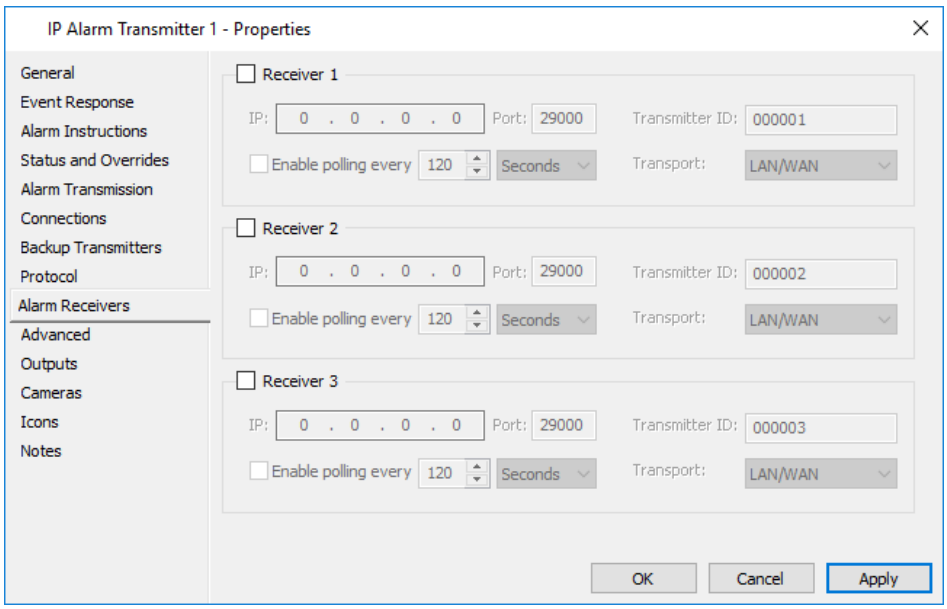


22. Select the appropriate **Protocol** from the drop-down list, i.e. either DC-09 (default) or CSV.
    Notes:
    - The CSV protocol extends the existing 4-digit Account Codes to 6-digit Account Codes, which are supported on Controller 6000s only.
    - The protocol cannot be changed once the item has been saved.
23. Which protocol did you select?

If...	then...
DC-09,	the **Enable encryption** section displays. If you want to use an encryption key, check the **Enable Encryption** checkbox and populate the **Encryption Key** field with a 64 character hexadecimal string.

If...	then...
	Notes: • 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 and enable the **Apply** button. If the **Apply** button is clicked now, the 64 characters are converted to 64 X's. • When an encryption key is entered, this is sent across DCOM to the server. As it would be possible for someone on the network to capture the packet as it passes along the network, it is recommended that this only be done on the workstation that runs directly on the server PC. • Keys exported by earlier versions than vEL8.00 of Command Centre cannot be imported.
CSV,	the **Enable Authentication** section displays. If you want to enable authentication, check the **Enable Authentication** checkbox and enter the **Username** and **Password** that will be used by the third party to authenticate the data received.

24. Click the **Alarm Receivers** tab.
    Note: If you are configuring an Alarm Dialler rather than an IP Alarm Transmitter, go to Step 30.



25. Tick the checkbox beside the **Receiver** you wish to use. Each IP Alarm Transmitter can be configured to transmit to three receivers in an attempt to communicate with an alarm monitoring centre, as follows:

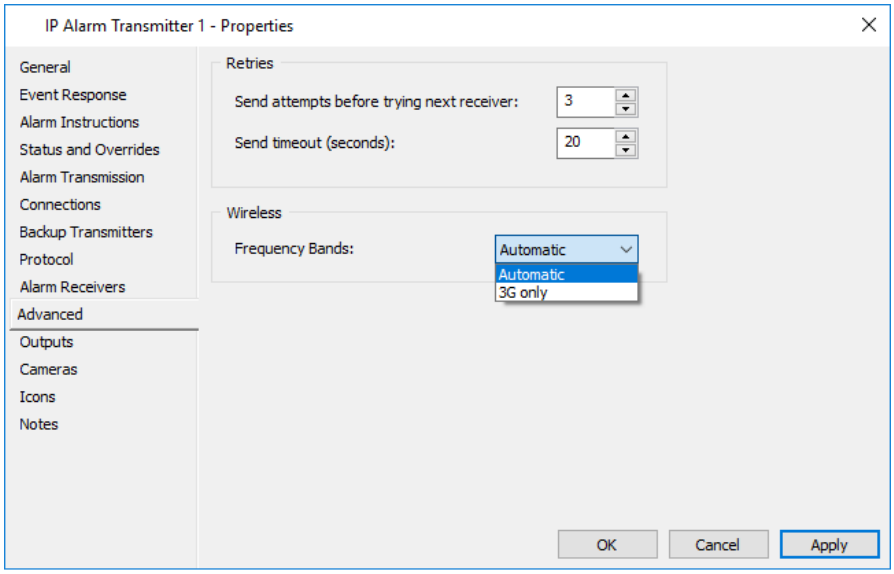
Field	Description
Receiver 1	The first receiver that the IP Alarm Transmitter will transmit to when a message needs to be sent.
Receiver 2	The second receiver that the IP Alarm Transmitter will transmit to once all attempts on the Primary Receiver have expired.

Field	Description
Receiver 3	The third receiver that the IP Alarm Transmitter will transmit to once all attempts on Receiver 2 have expired.

26. Complete the **Receiver** fields as required:

Field	Description
IP	This is the IP address of the receiver. This will be provided by the alarm monitoring centre.
Port	This is the port number of the receiver. This will be provided by the alarm monitoring centre.
Enable polling	This is the heartbeat time used to poll the receiver.
Transmitter ID	If required, you can configure a transmitter ID, so that the receiver can monitor and identify the channels separately. This field is pre-populated with a unique suggestion, formed from the site wide ACCT code plus a unique 2 digit identifier. **Note:** If you selected CSV protocol on the **Protocol** tab, the **Transmitter ID** fields will not appear, as they are redundant when configuring Alarm Receivers with CSV protocol.
Transport	The available transport options are WAN/LAN or Wireless. For the Wireless transport option, the IP Address/Port combination will need to be allowed through any firewall that is configured between Command Centre and the Alarm Receiver via the cellular provider. **Note:** If you use the Wireless option and need to update the Intercel Sam3G+ module to use a different connection profile that the 3 preloaded profiles, refer to ***Changing the Connection profile on the Intercel Sam3G+ module*** (on page 29-22) for the procedure.

27. Click the **Advanced** tab.



28. Enter the number of attempts before trying the next receiver.
    This is the number of retries that the IP Alarm Transmitter will attempt before moving onto the next IP address. If this number is set to 10, then a total of 11 transmissions will be made to the first IP address, (i.e. the first attempt and then 10 more attempts).

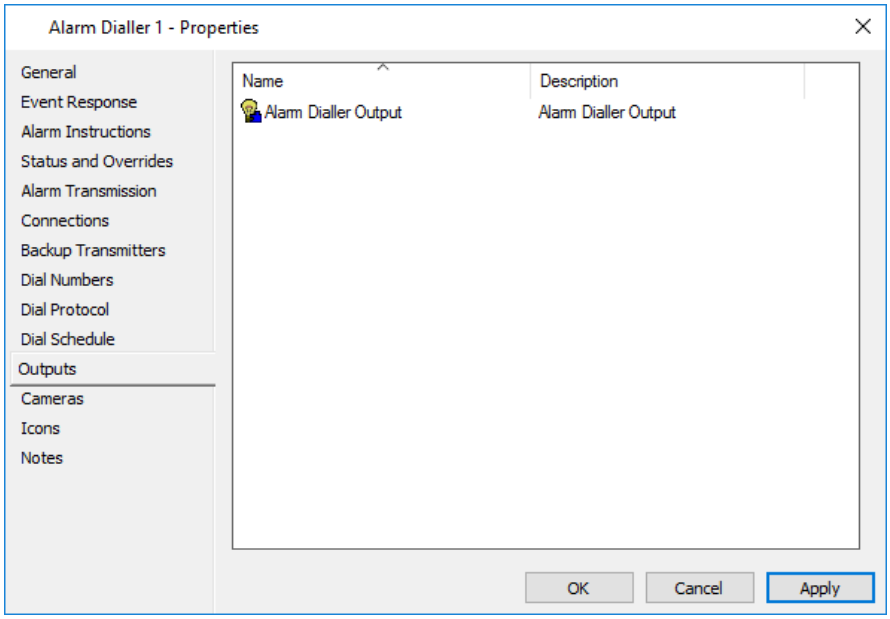
    Once the retry attempts have expired then the IP Alarm Transmitter will move to the next IP address on the list and the same rules will apply to that IP address, being that the first attempt will be followed by the number of retry attempts. Once all retry attempts have expired an alarm can be generated by an Action Plan. Events are held for 15 minutes, and then the sequence starts again.

    If you assigned a backup transmitter(s) at Step 10, then once all attempts have been made with this IP Alarm Transmitter, the messages will be passed to the backup transmitter(s) for transmissions.
    Notes:

    - Each IP Alarm Transmitter supports 255 events being held in the buffer, so if there are more than 255 events to be sent via Contact ID, the oldest events will be discarded. A message is generated however in the Event Log to advise the Date, Time and details of the discarded event(s) to provide a full audit trail.
    - A 15 minute wait period is started after all attempts at connecting to the offsite alarm receiver have failed. During this period, if further Contact ID alarms occur, no Contact ID events appear in Gallagher Command Centre's event viewer window and no further transmission activity is initiated.
      Take this functionality into account when you have no backup transmitter, assign only one IP address, and set the Retry Attempts Maximum to 0. If the IP Alarm Transmitter tries to report a Contact ID event and cannot, subsequent Contact ID transmission attempts will be inhibited for 15 minutes.

29. If you selected the Wireless transport option on the previous tab, (i.e. the **Alarm Receivers** tab), you can select a Wireless **Frequency Band** incase the reception on one band is very low, but the modem will not select a higher strength band. The options are 'Automatic' or '3G only'.
    Note: When the Frequency Band is changed, the band may not change until the next update (approximately 2 minutes).

30. Did you create an output for the Alarm Transmitter/Dialler so you will receive visual or audible acknowledgements when Alarm Zone armed messages are received by the monitoring company?
    If **yes**, then click the **Outputs** tab.
    If **no**, go to Step 32.



31. Open the **Hardware** List Window, and drag and drop the Alarm Transmitter/Dialler output(s) previously created into the grid.
    Note: If backup Alarm Transmitters/Diallers are used they must have their own outputs configured.
32. Click the **Cameras** tab if you want to associate a DVR Camera(s) with this Alarm Transmitter/Dialler.
    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 Alarm Transmitter/Dialler.
    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 Alarm Transmitter/Dialler.
    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 Alarm Transmitter/Dialler.
    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 Alarm Transmitter/Dialler has been created in Command Centre.

Next

Assigning the Alarm Transmitter/Dialler to a Controller (on page 29-25)

Changing the Connection profile on the Intercel Sam3G+ module

Introduction

This procedure describes how to configure the Intercel Sam3G+ module with a connection profile that is not one of the 3 default profiles.

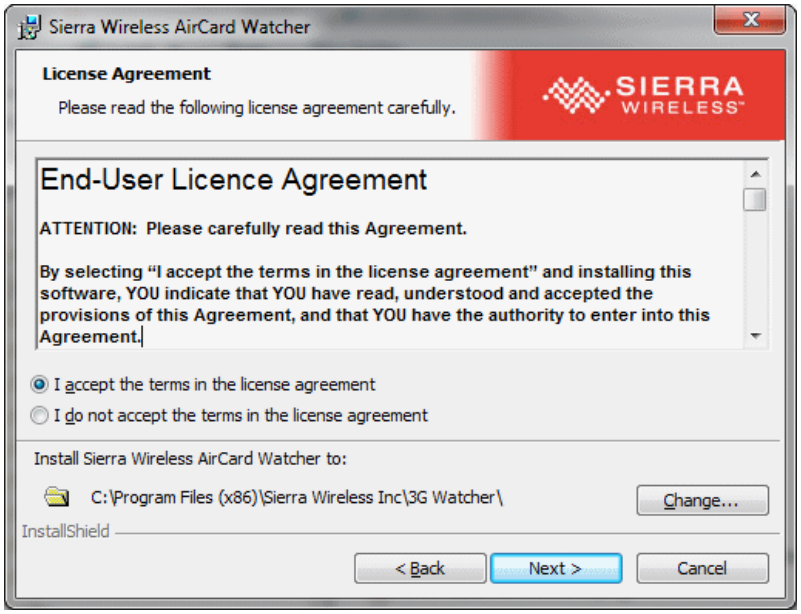
This may be necessary if default connection profiles supplied with the Intercel Sam3G+ module are not suitable and you selected the Wireless transport option when creating an Alarm Transmitter/Dialler in Gallagher Command Centre (on the **Alarm Receivers** tab).

Procedure

1. Run the **Watcher_Generic.msi** file, located in the **`'Utilities\IP Alarm Receiver\External alarm monitoring'`** directory of the Command Centre installation files.
   The Welcome screen of the Sierra Wireless AirCard Watcher Installer wizard displays.



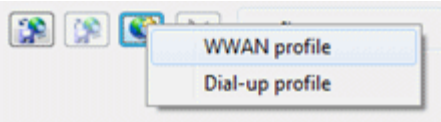
2. Click the **Next** button.
   The License Agreement screen of the wizard displays.



3. Click the radio button to accept the terms and conditions listed in the End-User License Agreement, and click the **Next** button.
4. Plug in the wireless module (via USB) and open the AirCard Watcher User Interface.

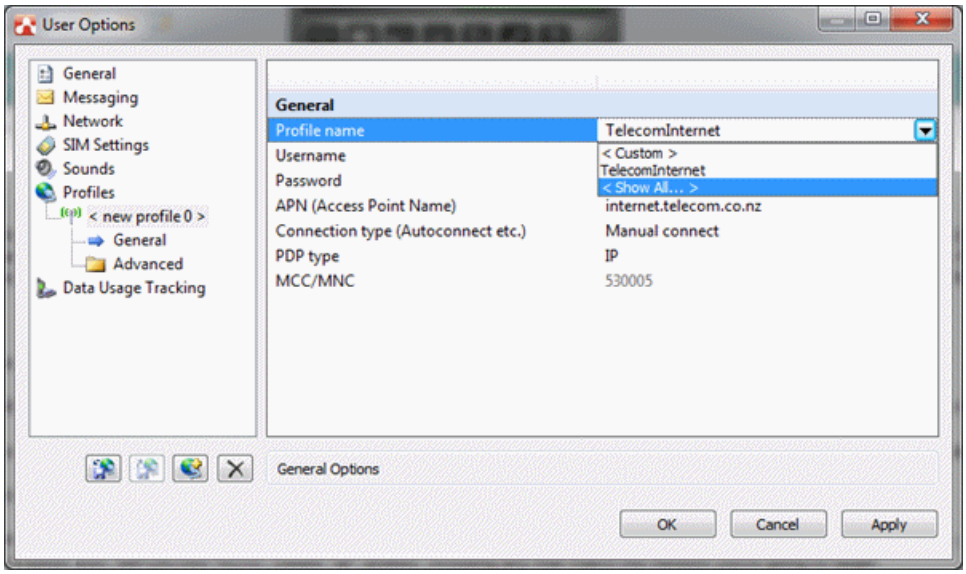


5. Click on the Spanner icon, (i.e. **Options**).
   A User Options screen displays.
6. Select **Profiles** in the list at the left.
7. One at a time, click on any existing profile and click the  button to delete it.
   IMPORTANT: Delete ALL profiles, including any that match the network you are going to target.
8. Click the **Apply** button.
9. Click the  **Add New Profile** button to create a new profile, and select the **WWAN profile** option.



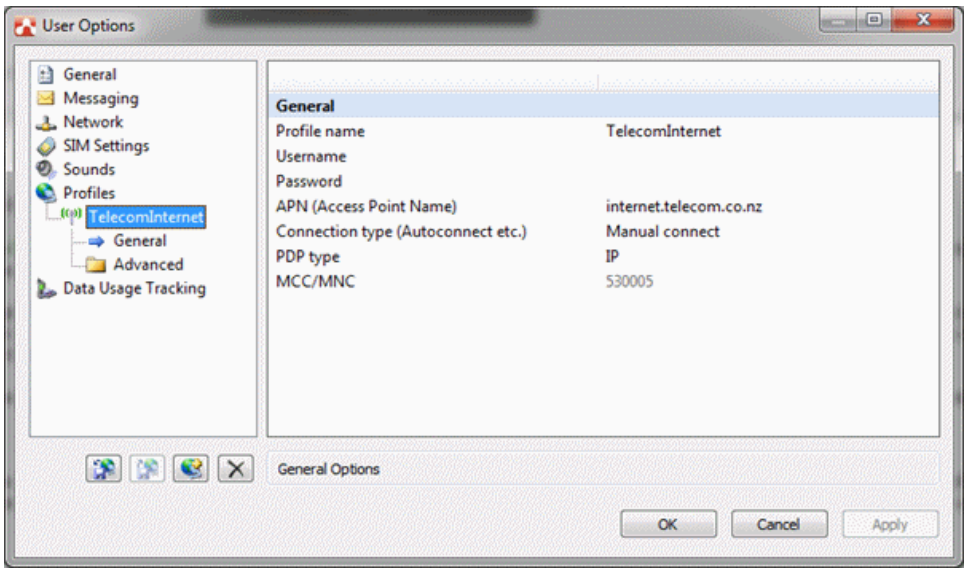
A **< new profile >** entry appears under the **Profiles** in the list at the left, and **General** information displays at the right.

10. The application automatically selects the most appropriate new profile based on the SIM card that is in the module.
    If this is not the target profile you want, select < Show All... > from the **Profile name** drop-down list to re-populate the list with ALL profiles.



11. Select the mobile operator from the list of all profiles.

12. Leave all other profile settings as default and click the **Apply** button.
    The module is now customised with the target network in profile position 1, replacing the **< new profile >** entry. It may be disconnected from the PC and connected to the Controller 6000.



Assigning the Alarm Transmitter/Dialler to a Controller

Introduction

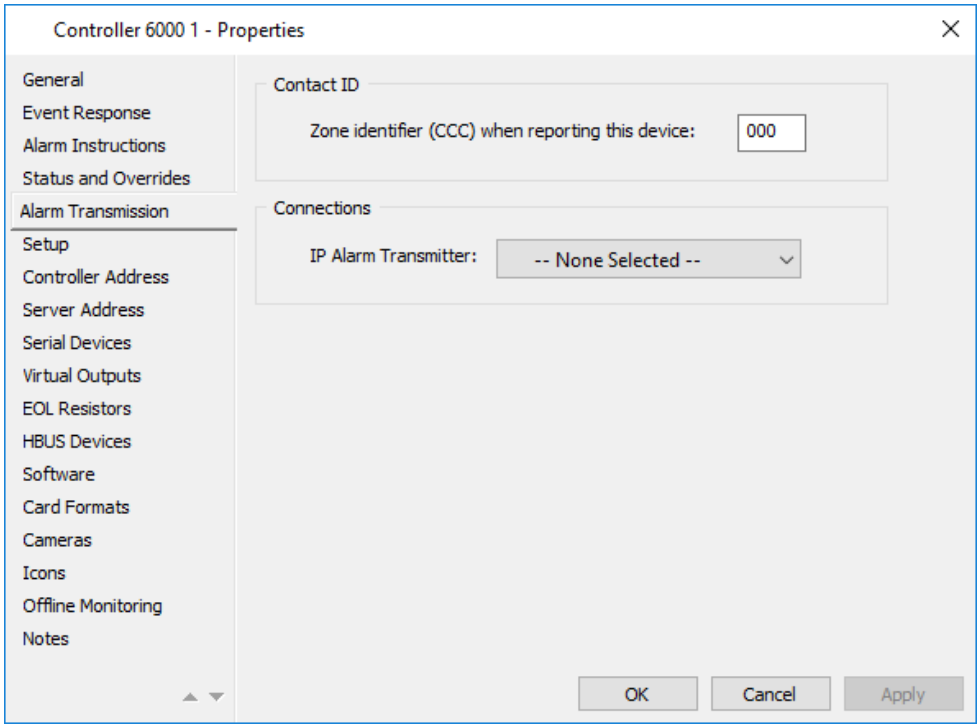
Once an Alarm Transmitter/Dialler has been created in Command Centre, it must then be assigned to a Controller.

Before you begin

Before you begin this procedure ensure you have performed ***Configuring an Alarm Transmitter/Dialler*** (on page 29-10).

Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. Select the Controller you wish to assign the Alarm Transmitter/Dialler to.
3. Click the **Alarm Transmission** tab.



4. Enter a Zone identifier (CCC) to be used for Contact ID reporting.
   Notes:
   - This field will accept 3 Hex digits 0-9, B-F.
   - The default of 000 can be left if you do not wish to indicate a specific zone or user information.
5. Are you assigning an IP Alarm Transmitter or an Alarm Dialler to this Controller?

If an...	then...
IP Alarm Transmitter,	from the drop-down list select the **IP Alarm Transmitter** you want to connect to this Controller.
Alarm Dialler,	**a)** Click the **Serial Devices** tab. **b)** From the drop-down list, select the **Alarm Dialler** you want to connect to this Controller. **Note:** The Controller can communicate with either an Alarm Dialler or an Elevator HLI, but not both, using the Controller serial port connection.

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.

   Note: If a 'Push Configuration' is performed on an IP Alarm Transmitter, then all Controllers that have an Alarm Transmitter configured will have their Alarm Transmission configuration resent. Performance on all these Controllers will be reduced for a short period of time. This should be less than a minute. Access to doors will be affected at this time. It is recommended that this is only performed at the appropriate time for the site concerned.

Result

An Alarm Transmitter/Dialler has been assigned to a Controller.

Next

Configuring Items for Contact ID (on page 29-27)

Configuring Items for Contact ID

Introduction

This procedure describes how to configure an item that needs a Contact ID message sent. The following items can be configured to report Contact ID events, via the **Alarm Transmission** tab in their property pages:

Item	Refer to...
Outputs Interface Boards Controller Devices Readers Doors Elevator Cars Cardholders External Systems DVR Systems	***Configuring Items for Contact ID*** (on page 29-28) for this procedure.
Inputs	***Configuring Inputs for Contact ID*** (on page 29-29) for the procedure.
Alarm Zones	***Configuring Alarm Zones for Contact ID*** (on page 29-29) for the procedure.
External System Items DVR Cameras	***Configuring external system children for Contact ID*** (on page 29-31) for the procedure.
Action Plans	***Configuring Action Plans for Contact ID*** (on page 29-31) for the procedure.

Notes:

- Additional Contact ID configuration can also be done from the Server Properties (see Alarm Transmission).
- The Contact ID message obtains the CCC from the item, the GG from the item's Alarm Zone and the XYZ from the Event for the item.

Before you begin

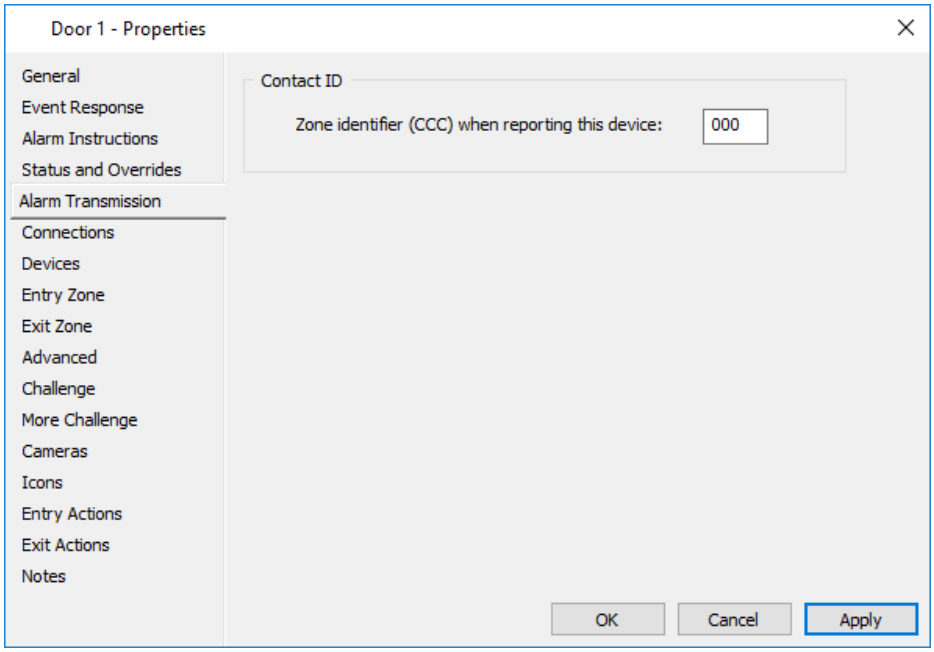
Before you begin this procedure ensure you have performed ***Assigning the Alarm Transmitter/Dialler to a Controller*** (on page 29-25).

Configuring Items for Contact ID

Although the following procedure describes how to configure Contact ID for a Door, this same procedure is used for most other items. The only difference is how you select the item at Step 1.

Important: When the doors on your site were set up, they may have been configured with a common Alarm Zone associated with the Controller. However, for use with Contact ID they may need to use different Alarm Zones based on the area or location of the door. It may not be appropriate to use the same Alarm Zone as the "Intruder" alarms, as "Door" alarms are mostly 24 hour, whereas "Intruder" alarms use Set and Unset at different times of the day.

1. Click **Configure** from the menu bar, then **Doors** (as an example).
2. **Right click** on the Door and select **Properties**.
3. Click the **Alarm Transmission** tab.



4. Enter a Zone identifier (for Hardware items), or user number (for Cardholders) to be used for Contact ID reporting, (i.e. the CCC value).

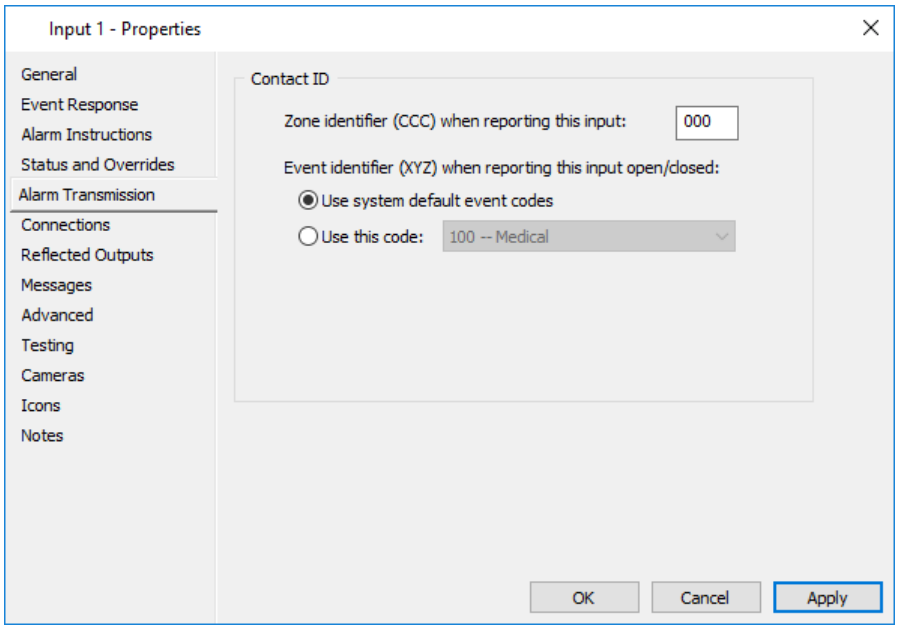
   Notes:

   - This field will accept 3 Hex digits 0-9, B-F.
   - The default of 000 can be left if you do not wish to indicate a specific zone or user information.

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.

Configuring Inputs for Contact ID

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** on the Input and select **Properties**.
3. Click the **Alarm Transmission** tab.



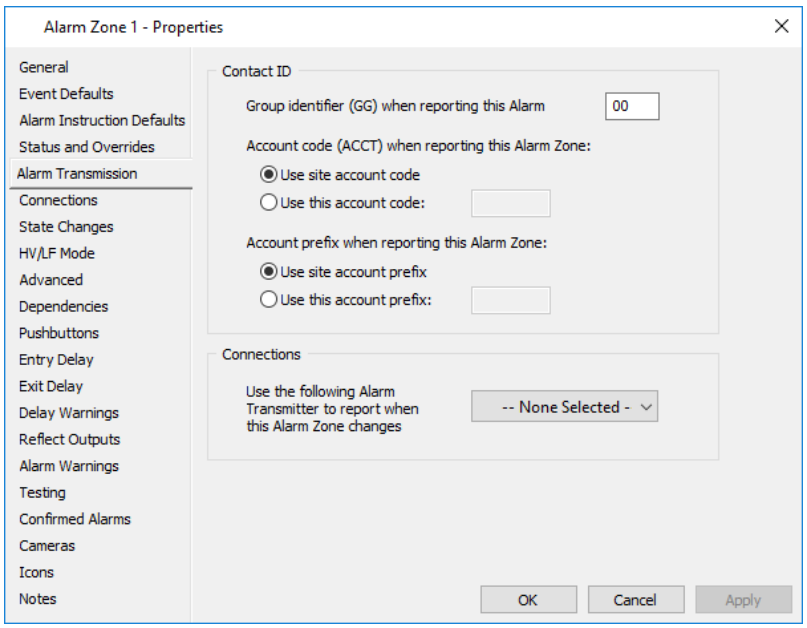
4. Select the Event Identifier (the XYZ value) to be used for Contact ID reporting.

   You can choose to either use system default event codes or select a specific code from the drop-down list. See ***XYZ Event Mappings*** (on page Appx B-1) for further detail.

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.

Configuring Alarm Zones for Contact ID

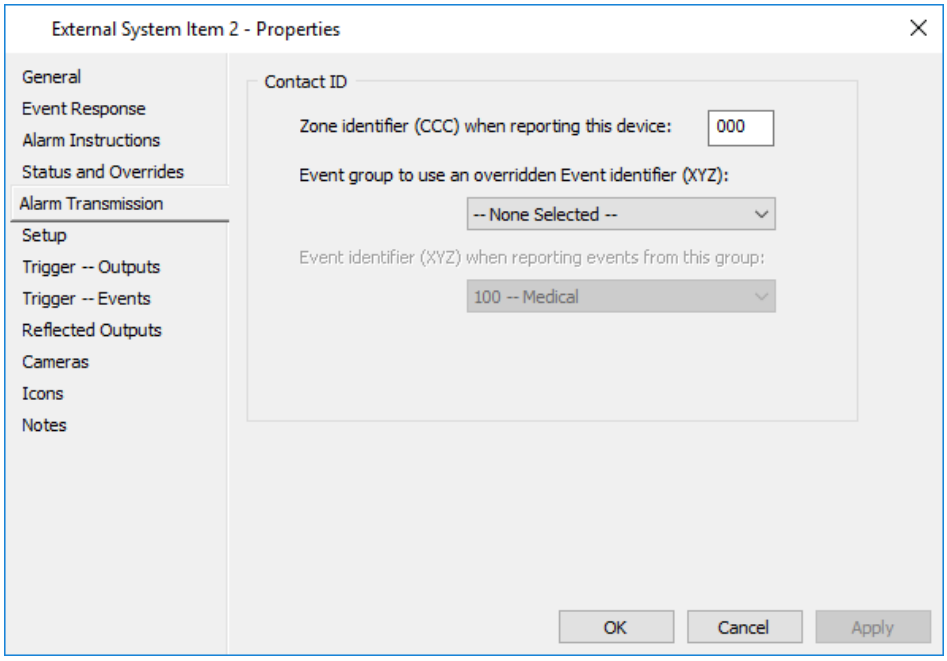
1. Click **Configure** from the menu bar, then **Alarm Zones**.
   The **Alarm Zone** List Window opens (in grid view).
2. **Right click** on the Alarm Zone and select **Properties**.
3. Click the **Alarm Transmission** tab.



4. Enter a Group identifier (the GG value) to be used for Contact ID reporting.
5. If you require an individual Account code for each Alarm Zone, click the **Use this account code** radio button, and enter a four-digit Account code depending on the protocol, (i.e. DC-09 protocol requires a 4 digit Account Code and CSV protocol requires a 4 OR 6 digit Account Code).
   Notes:
   - 0-9 and B-F are acceptable entries for the Account code, and leading zeros are acceptable.
   - The Account code you enter on this property page overrides the site wide Account code.
   - If the Account code is left blank, when a save is attempted, the default setting will revert back to the site wide value.
6. If you require an individual Account prefix for each Alarm Zone, click the **Use this account prefix** radio button, and enter a hexadecimal Account prefix. **Notes:**
   - The Account prefix you enter on this property page overrides the site wide Account prefix.
   - If the Account prefix is left blank, when a save is attempted, the default setting will revert back to the site wide value.
   - CSV protocol does not use an Account prefix.
7. From the drop-down list in the Connections section, select the Alarm Transmitter/Dialler you wish to use for reporting when this Alarm Zone changes state.
   Note: With an Alarm Transmitter/Dialler selected, when the Alarm Zone state changes from armed to disarmed, Contact ID will transmit an event message, and when it changes from disarmed to armed Contact ID will transmit a restore message providing it is an event that has a 'Return to Normal' event.
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.

Configuring external system children for Contact ID

1. Click **Configure** from the menu bar, then **External Systems**.
   The **External Systems** List Window opens (in tree view).
2. **Right click** on the External System Item or DVR Camera, and select **Properties**.
3. Click the **Alarm Transmission** tab.



4. Enter a zone identifier (CCC) to be used for Contact ID reporting, (i.e. the CCC value).
5. Select an **Event Group** from the drop-down list of possible Event Groups that will use an overridden XYZ code for this External System Item or DVR Camera.
6. Select the appropriate Contact ID XYZ code for the Event Group from the Event Identifier drop-down list. See ***XYZ Event Mappings*** (on page Appx B-1) for further detail.
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.

Configuring Action Plans for Contact ID

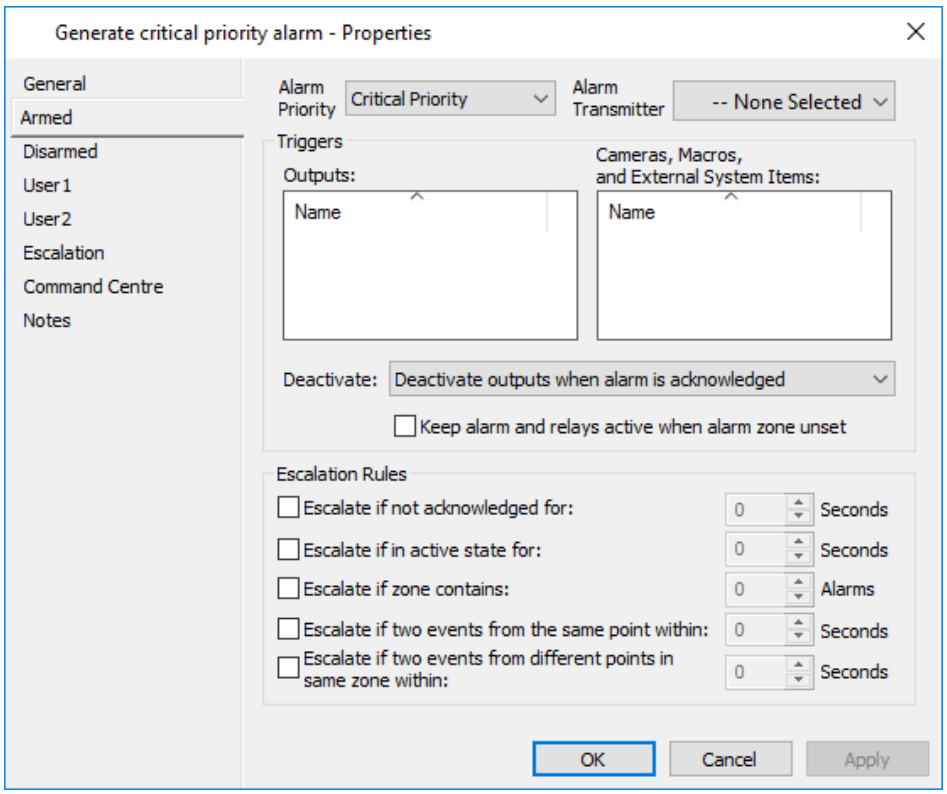
Before an event can be sent to an Alarm Monitoring Company, the Action Plan associated with the event(s) must be set up with an Alarm Transmitter/Dialler.

Important: It may not be appropriate to use the default Action Plans. If these are set up to use an Alarm Transmitter/Dialler, then all alarms will be sent.

However, it may not be desirable to send some alarm types to an Alarm Monitoring Company.
All items using an Action Plan with an Alarm Transmitter/Dialler configured will send Contact ID messages. If the Alarm Zone or item has not been configured for Contact ID, then a GG or CCC of zero may be sent.

Note: Alarms will be sent as many times as an Alarm Transmitter/Dialler appears on an Action Plan for the various priorities involved in an escalation.
For example:
If a "Forced Door" alarm uses a very high priority Action Plan with an Alarm Transmitter/Dialler attached, it will escalate to a critical priority that also has the Alarm Transmitter/Dialler attached. The "Forced Door" alarm Contact ID message will then be sent twice, (i.e. once for each priority).

1. Click **Configure** from the menu bar, then **Action Plans**.
   The **Action Plan** List Window opens (in grid view).
2. **Right click** on the Action Plan and select **Properties**.
3. Click the **Armed** (or **Set**) tab.



4. Click within the **Alarm Transmitter** field to display the available options, and from the list select the appropriate Alarm Transmitter/Dialler for Contact ID.
5. Click each of the remaining tabs and repeat Step 4 for each one.
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.

Sample Messages

Example 1: Alarm Message

Account 1234 is reporting a Perimeter Burglary Alarm on Zone 15 of Partition 1.

The message will be sent as:

1234 18 1131 01 015

where:

1234 = The account number (1234)

18 = The message type used to identify the message as Contact ID

1131 = The Event Qualifier (1) for a new event, followed by the Event Code for Perimeter Burglary (131)

01 = The partition number (01)

015 = The zone number (015)

Note: The checksum has been removed from this example.

Example 2: Restoral Message

Account 1234 is reporting a Restore of a Perimeter Burglary Alarm on Zone 15 of Partition 1.

The message will be sent as:

1234 18 3131 01 015

where:

1234 = The account number (1234)

18 = The message type used to identify the message as Contact ID

3131 = The Event Qualifier (3) for a restoral, followed by the Event Code for Perimeter Burglary (131)

01 = The partition number (01)

015 = The zone number (015)

Note: The checksum has been removed from this example.

IP Alarms Receiver Software

Introduction

The IP Alarms Receiver Software runs on a Windows PC in a remote alarm monitoring centre. The IP Alarms Receiver Software performs the following tasks:

- Listens on a socket for incoming socket connections.
- Accepts a connection from a Gallagher Controller.
- Reads data from an open socket connection to a Gallagher Controller.
- Decrypts and decodes the received message.
- Forwards the message to the alarm monitoring system (via the serial port).
- Waits for a reply from the alarm monitoring system acknowledging receipt of the message.
- Sends an acknowledge message to the Gallagher Controller if the message was successfully sent to the alarm monitoring system and acknowledged by the alarm monitoring system.
- Closes the socket, if not already closed by the Gallagher Controller
- Regularly checks to see if any remote station has not been heard from for too long and generates heartbeat alarms as required.

For further detail on installing and using the IP Alarms Receiver Software, refer to the current **IP Alarms Receiver Software Release Note** located in the `'Utilities\IP Alarm Receiver'` directory of the Gallagher Command Centre installation files.

Chapter 30: Licensing Groups

Licensing Groups allow for reserved Workstation and Visitor Management Kiosk licenses, guaranteeing access, especially in multi-tenanted or multi-divisional sites. Workstation license reservation can be guaranteed by workstation and/or by operator ensuring that access to the security software is always available for important users or stations.
When an operator logs on, the system will first check if there is a reserved license for that licensing group member. If there is, it will use this reservation. If not, then the system will check if any unreserved floating licenses are available. If there is an available floating license, the operator will logon successfully. If no floating licenses remain the operator will not be able to logon.
Note: An operator or a workstation cannot be a member of more than one Licensing Group.

Operator Privileges

Operator Privilege	is required to...
"View Site" in the division of the Licensing Group	view a Licensing Group.
"Edit Site" in the division of the Licensing Group	edit a Licensing Group.
"Edit Site" in the division of the workstation	change the Licensing Group assigned to a workstation.

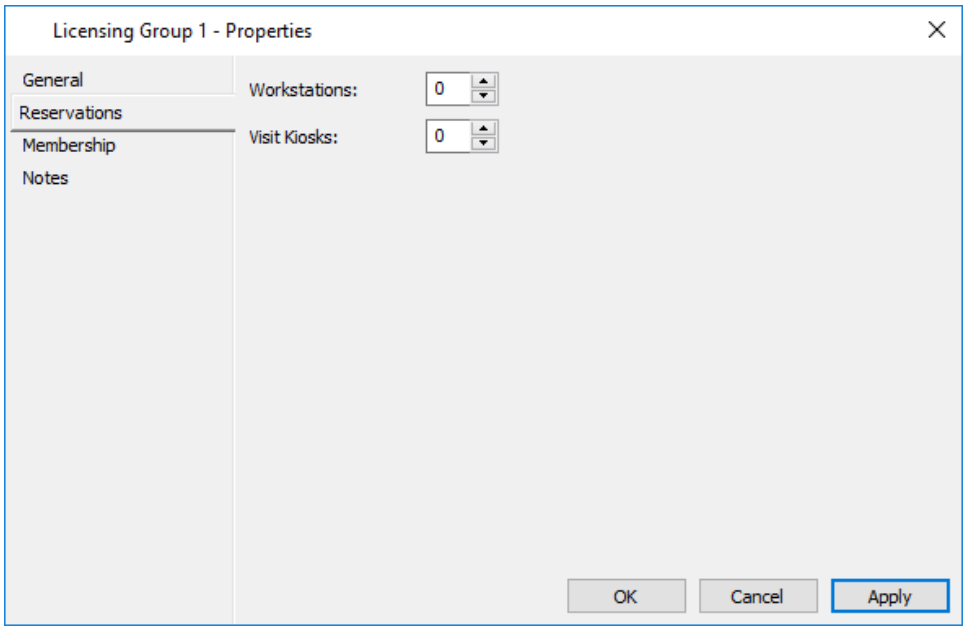
Creating a new Licensing Group

Introduction

This procedure describes how to create a Licensing Group.

Procedure

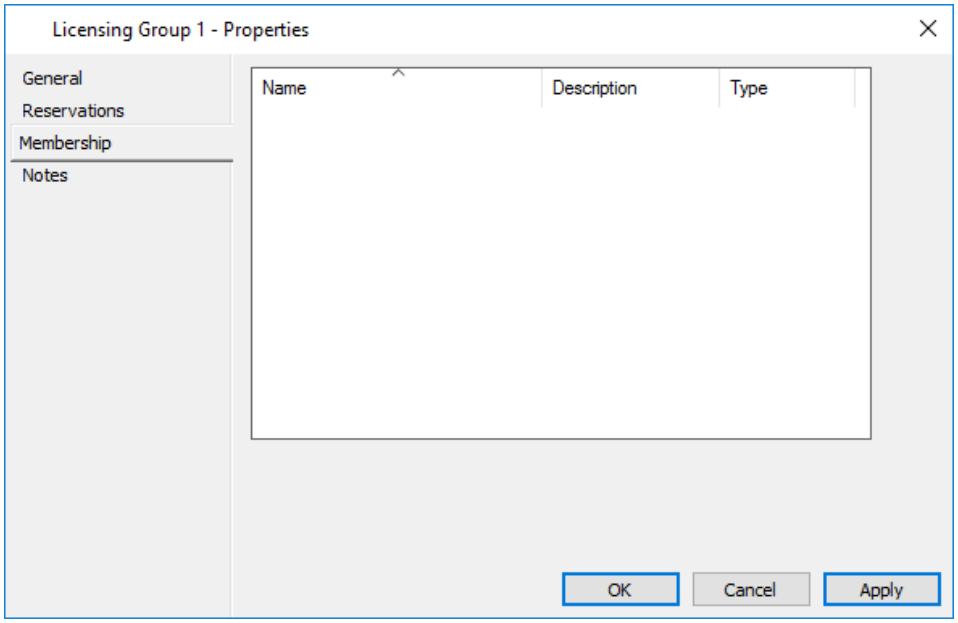
1. Click **Configure** from the menu bar, then **Licensing Groups**.
   The Licensing Group List Window opens.
2. **Right click** and select **New...Licensing Group**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see General tab (on page 3-18).
4. Click the **Reservations** tab.



   This tab allows you to set the number of dedicated licenses.
5. Configure as appropriate.

Field	Description
Workstations	This is the total number of dedicated Workstations across all license groups. It must be less than or equal to the total Workstation license limit.
Visit Kiosks	This is the total number of dedicated Visit Kiosks across all license groups. It must be less than or equal to the total Visit Kiosk license limit.

6. Click the **Membership** tab.



Note: If you set the Workstation or Kiosk reservations to be more than zero on the **Reservations** tab, there must be a minimum of one Workstation or Operator membership on this tab. Otherwise, when you attempt to save the Licensing Group, the following message will display: *"Unable to save configuration as it will cause one or more Licensing Groups to have no memberships."*

7. Drag and drop items from the Services and Workstations List Window, from other Licensing Group grids, or from any other grid that the item exists in.
   Notes:
   - Each item can only belong to one Licensing Group.
   - An item can be removed from the grid by right mouse clicking on the item and selecting **Remove from List**.
8. Click the **Notes** tab if you want to add a note(s) about this Door.
   For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
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 new Licensing Group is added to the Command Centre system. On the **Licensing** tab of each of the item(s) added to this group (via the **Membership** tab), the Licensing Group name will appear in the **Licensing Group** field.

Hint

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

Chapter 31: Mobile Connect

Introduction

The Gallagher Mobile Connect App allows a user to request access using their mobile device in place of a traditional access card. Access can be requested at a Gallagher HBUS Reader or Gallagher HBUS Terminal.

The App uses Bluetooth® wireless technology, or Near Field Communication (NFC) to communicate with the reader or terminal. A Command Centre operator can specify the reader's or terminal's communication method (either Bluetooth®, NFC, or both).
Note: Only Android devices can use NFC.

A Mobile Credential, stored by the App, is used to identify the mobile device. Second factor authentication (PIN or fingerprint) can be used to identify the device's user. Mobile credentials are registered to users in Command Centre, and use the FIDO (Fast IDentity Online) Universal Authentication Framework (UAF) protocol. This is a globally recognised method of authentication that is proven safe and secure.

In addition to requesting access, a suitably privileged user can use the App to perform an action at a Bluetooth® enabled reader or terminal. Actions that can be performed are listed here.

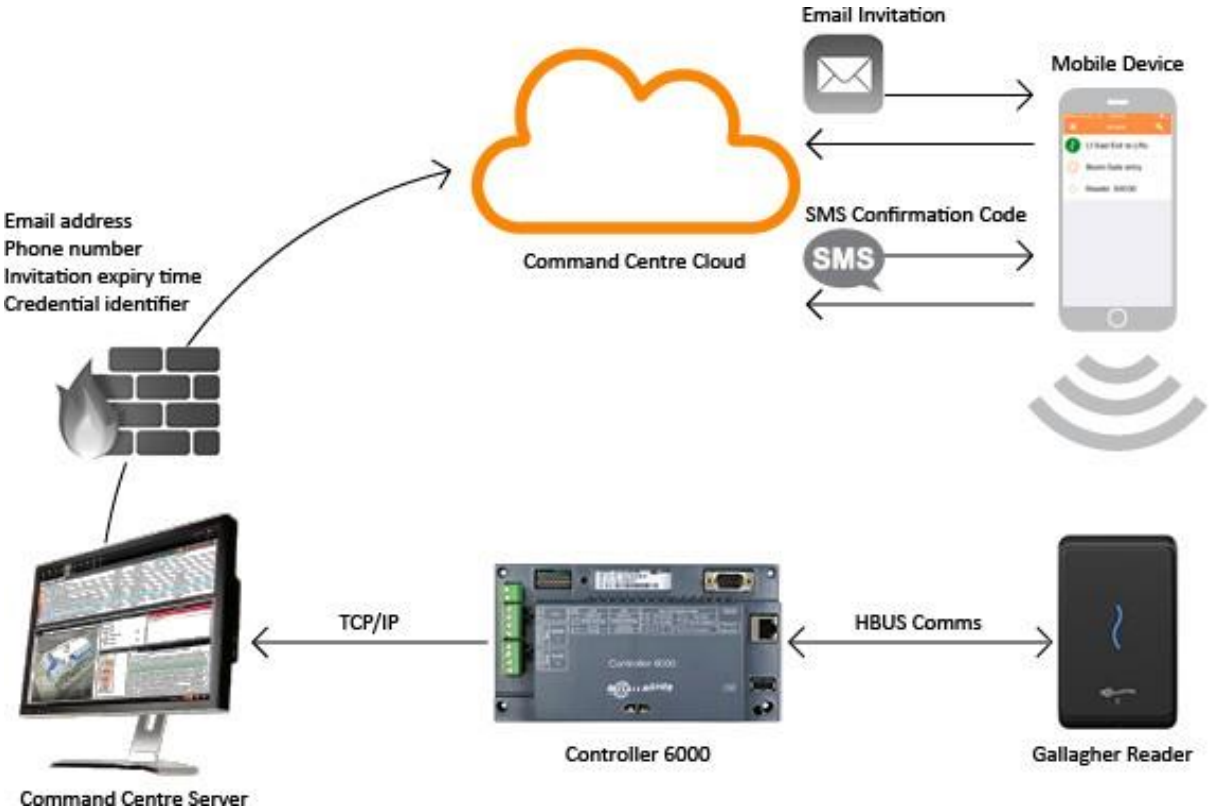
A Digital ID is also held on the Mobile Connect App, and appears as a digital 'Card' on a Cardholder's Mobile Device to provide visual identification of the Cardholder. It's layout can be configured in the same manner a Card's can be, and can contain text, images, and barcodes.

Digital IDs must be registered in Command Centre Client. Cardholders must have a Mobile Credential in order to receive the Digital ID.

Registration process

Stage	Description
1	An operator uses the Cardholder Cards tile in Command Centre to register a mobile credential with a user. When registered, a request is sent from Command Centre to the Command Centre Cloud. Command Centre sends the user's: email address, phone number, invitation expiry time, and mobile credential identifier.

Stage	Description
2	The Command Centre Cloud sends an invitation email to the user's email address. This email contains a link to the Gallagher Mobile Connect App. The user must download and install the App on their device. The email also contains an **Accept Credential** button. The user must accept the credential.
3	The Command Centre Cloud sends an SMS containing a six-digit confirmation code to the user's phone number. The user must enter the six-digit code into the App in order to authorise their device.
4	The user must specify their second authentication factor, either PIN or fingerprint. If the door requires a second authentication factor, this must be entered using the device, not the keypad on a reader.
5	The user can now request access at a Gallagher reader. Note: The credential identifier is stored on the Gallagher Controller. Internet connectivity is not required for a user to request access at a Gallagher reader.



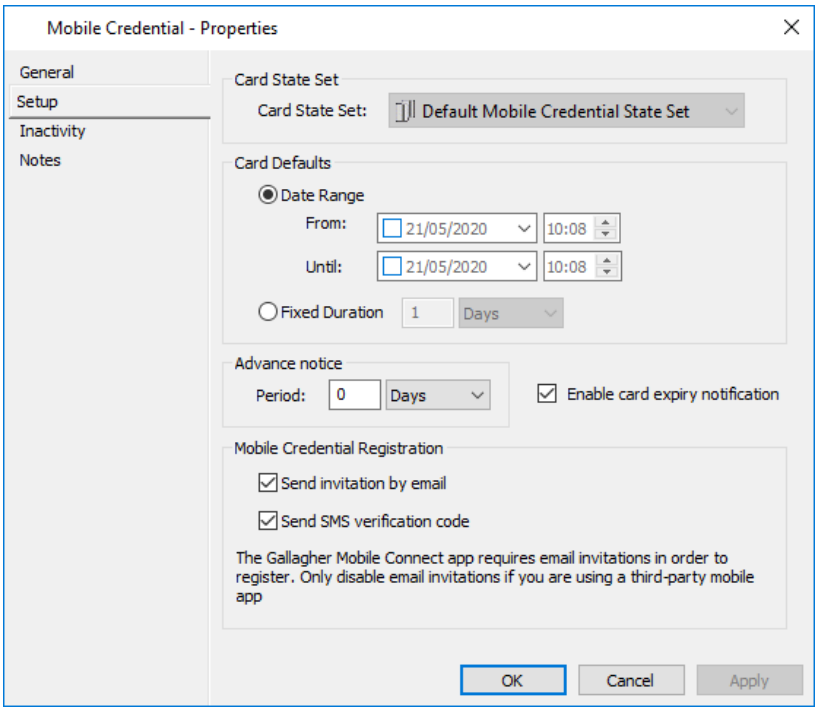
Setting up Mobile Credential Types

Introduction

The Mobile Credential Type "Mobile Credential" is created by default when Command Centre is installed or upgraded. The following procedure describes how to create a new Mobile Credential Type, should an additional Mobile Credential Type be required.
Note: The "Configure Site" operator privilege is required to perform this procedure.

Procedure

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...Mobile Credential 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 Mobile Credential Type, from the drop-down box.
   Note: Once the Card State Set is assigned to the Mobile Credential Type and saved, it cannot be changed. Bulk changes can be used to change the Mobile Credential Type if an alternative set of Card States is required.
6. In the **Card Defaults** section you can activate the mobile credential 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 mobile credentials of this type will be activated and expire in the **From** and **Until** fields. **Notes:** • If you do not enter a date in the **From** field, when a mobile credential of this type is registered to a user and the mobile credential is enabled, activation will be immediate. • If you do not enter a date in the **Until** field, the mobile credential 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 will be determined from the assignment date with the configured offset / duration.

When a Cardholder is registered to a mobile credential of this type, (i.e. on the **Cardholder Cards** tile in Command Centre Client), the **Until** Date will reflect the expiry date configured here.

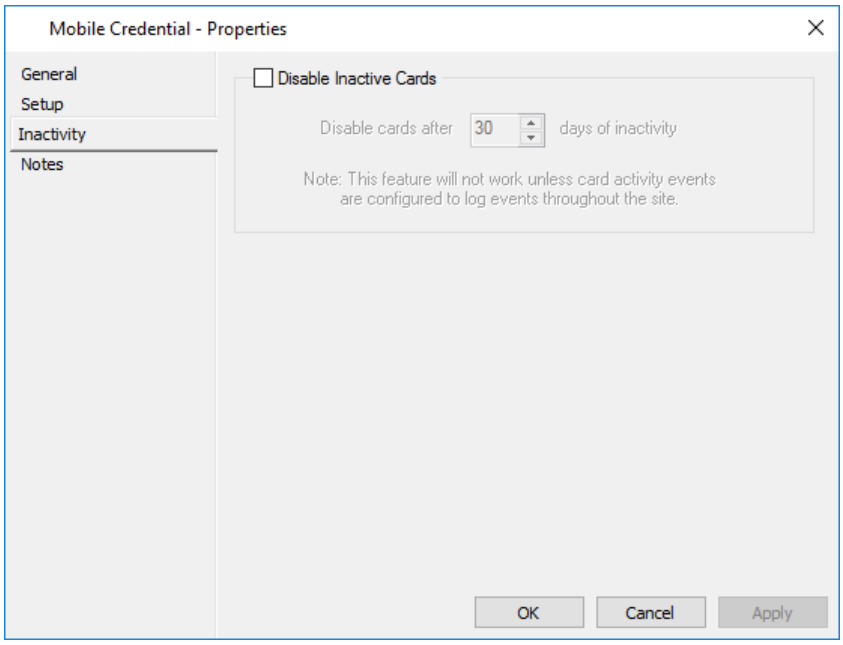
7. The **Advance notice** section of this screen allows you to configure warning notifications of pending mobile credential expiry to be sent when the specified period is reached, for all mobile credentials regardless of status.
8. Do you want to enable card expiry notification?

If...	then...
yes	Set the **Period** to the value that is required to represent the number of days, weeks, months or years prior to mobile credential expiry to initiate the warning notification. Ensure the **Enable card expiry notification** checkbox remains checked.
no	leave the **Period** as 0 days, and uncheck the **Enable card expiry notification** checkbox.

9. Configure the Mobile Credential Registration as required:

Checkbox	Description
Send invitation by email	Tick this option so cardholders can receive an invitation email from the Registration Server. This makes an **Email** field appear on the Assign Card pop-up in the Command Centre Client when registering mobile credentials for a cardholder.
Send SMS verification code	Tick this option so the Registration Server can authorise cardholders' mobile phones. **Note:** This makes a **Mobile** field appear on the Assign Card pop-up in the Command Centre Client when registering mobile credentials for cardholders.

10. Click the **Inactivity** tab.



11. Do you wish to enable the Inactive Card Expiry feature?
    Note: All mobile credentials of this type shall share a common inactivity timeout if enabled.

If...	then...
yes	Check the **Disable Inactive Cards** checkbox. Go to Step 12.
no	Leave the **Disable Inactive Cards** checkbox unchecked. Go to Step 13.

12. Enter a figure to represent the number of days of inactivity that will disable a mobile credential.
    Notes:
    - When this feature is first enabled the default timeout = 30 days. The range is 1-999 days.
    - Users will be expired regardless of activity if mobile credential activity events are not configured to log events throughout the site. (Refer to ***Event Defaults*** on page 6-12 for further detail.)
13. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Mobile Credential Type.
    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 Mobile Credential Type.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
15. Click **OK** to save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.
    Note: After you register your phone against the Cloud, there may be a delay of up to 90 seconds before it reaches the Command Centre Server. Badging at the reader before the credential status changes to "Active" will result in "Access Denied".

Setting up Digital ID Types

Introduction

This procedure describes how to create a Digital ID Type. Digital ID Types are required for you to register new Digital IDs for Cardholders. When registering a Digital ID, you select one of your configured Digital ID Types.

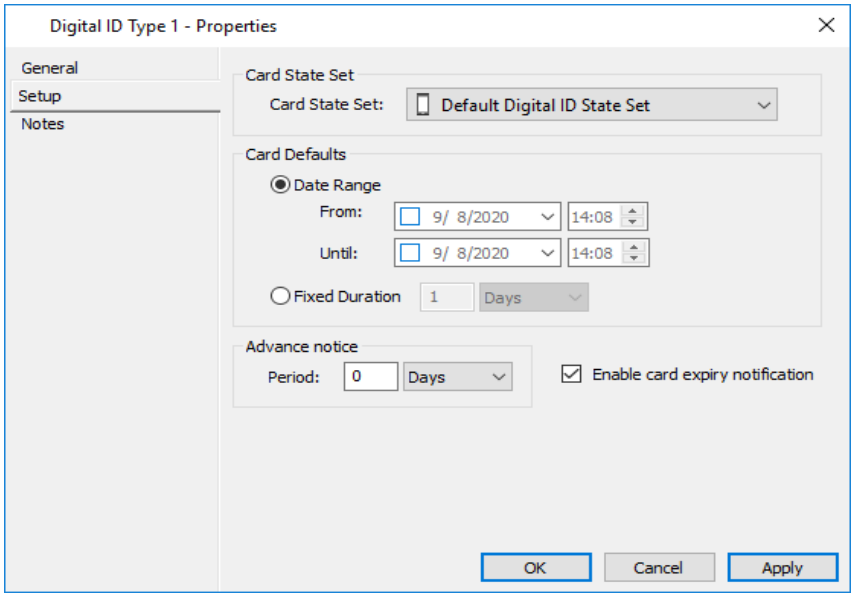
The 'card expiry' feature allows the life of a Digital ID to be specified by defining a 'From' time and date and an 'Until' time and date. Digital IDs with these times defined are enabled between those times and are referred to as Scheduled Card Expiry.

Note: The "Configure Site" operator privilege is required to perform this procedure.

Configuration

To set up an additional Digital ID 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...Digital ID 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. From the **Card State Set** drop-down box, select the appropriate Card State Set to be associated with this Digital ID Type.
   Note: Once the Card State Set is assigned to the Digital ID Type and saved, it cannot be changed. Bulk changes can be used to change the Digital ID Type if an alternative set of Card States is required.

6. In the **Card Defaults** section, you can activate the Digital ID for either a specific Date Range or a Fixed Duration.
   Click the appropriate radio button:

If you select…	then…
Date range,	in the **From** and **Until** fields, set the dates and times that Digital IDs of this type will be activated and will expire. **Notes:** • If you do not enter a date in the **From** field, when a Digital ID of this type is registered to a user and the Digital ID is enabled, activation will be immediate. • If you do not enter a date in the **Until** field, the Digital ID 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 will be determined from the assignment date with the configured offset / duration.

   When a Cardholder is registered to a Digital ID of this type, (i.e. on the **Cardholder Cards** tile in Command Centre Client), the default **Until** date will reflect the expiry date configured here.
7. The **Advance notice** section of this screen allows you to configure notifications of upcoming Digital ID expiries to be sent when the specified period is reached. Warning notifications are given via the Gallagher Mobile Connect app, and are sent for all Digital IDs regardless of status.
8. Do you want to enable Digital ID expiry notifications?

If…	then…
yes	• Set the **Period** to the value that represents the number of days, weeks, months or years before Digital ID expiry when warning notifications will be sent. • Select the unit of time (Days, Weeks, Months, or Years) from the drop-down list. • Ensure the **Enable card expiry notification** check box is checked.
no	leave the **Period** as 0 days, and deselect the **Enable card expiry notification** checkbox.

9. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Digital ID Type. For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
10. Click the **Notes** tab if you want to add a note(s) about this Digital ID Type. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
11. Click **OK** to save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Configuring a reader for Mobile Connect

Introduction

This procedure describes how to configure a reader for Mobile Connect.

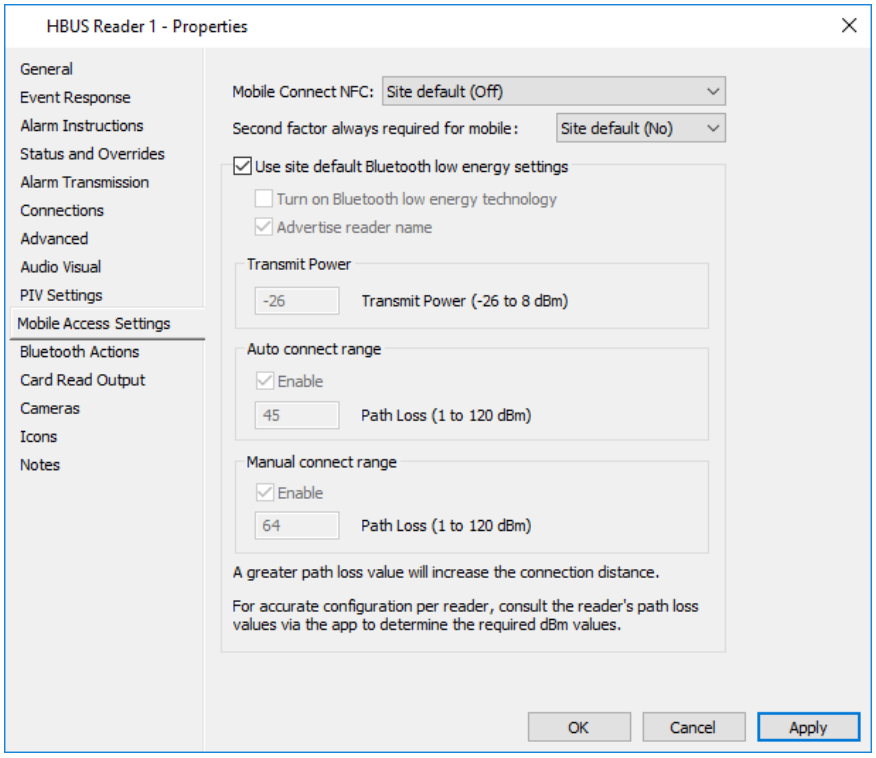
Before you begin

- HBUS Readers that support Bluetooth® have the icon printed on the reader fascia. HBUS Terminals that support Bluetooth® have Bluetooth® listed on the Information screen. To display the Information screen, press and hold the '#' key for 3 seconds.
- The HBUS Reader or HBUS Terminal must be connected to a Controller 6000 or 7000. Both the reader or terminal and the door must be assigned to the Controller. If a mobile credential is used to request access at a door not assigned to a Controller, the alarm "*Mobile access unsupported - Door requires Controller*" will be generated.
- Assigning more than one Bluetooth® enabled reader to the same side of the Door is not supported.
- Assigning the same Bluetooth® enabled reader to multiple Doors is not supported; multiple Outputs will not be triggered. Use a Logic Block to trigger multiple Outputs from a Door.

Operators require the "Edit Site" privilege in the appropriate division to be able to create, edit and delete Bluetooth® enabled readers.
Note: The "View Site" privilege in the appropriate division will allow an operator to view (but not edit) Bluetooth® enabled readers.

Procedure

1. Complete the HBUS Reader configuration as per the procedure for ***Creating Readers*** (on page 21-57), and then go to Step 2 of this procedure.
   Note: If configuring an HBUS Terminal, refer to the procedure ***Configuring an HBUS Terminal*** (on page 21-68), and then go to Step 2 of this procedure.
2. Click the **Mobile Access Settings** tab.

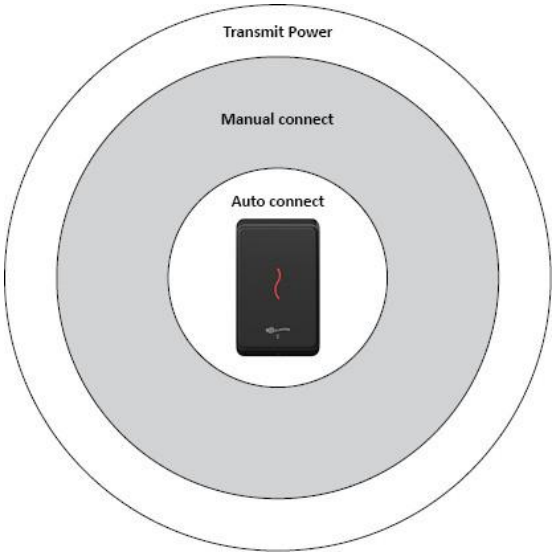


3. Configure as required.

Field	Description
Mobile Connect NFC	Select an option from the drop-down list. When ON, Android devices will use NFC to request access at the reader. NFC applies to Auto Connect only. If the user has NFC disabled on their device, their device will revert to Bluetooth® to make the access request. The default uses the ***Server Properties settings*** (on page 6-63), which is OFF by default.
Second factor always required for mobile	Select an option from the drop-down list. When ON, presentation of a second authentication factor is required at the reader at all times, unless the access mode is set to 'Free-No PIN'. The default uses the ***Server Properties settings*** (on page 6-63), which is OFF by default. Second factor authentication is enforced for mobile credentials only. **Note:** If the access mode is set to 'Free-No PIN' and a personalised action has been assigned to the user, a second authentication factor will be required. Refer to ***Configuring Personalised Actions for Access Zones*** (on page 10-34) for details on how personalised actions work. NFC works over a short range, hence a user may take their device out of range to provide their second factor. When this happens, the App displays an icon encouraging the user to re-enter the field.

Field	Description
Use site default Bluetooth low energy settings	When checked, the reader will use the Bluetooth low energy settings, configured on the **Mobile Access Settings** tab in the Server Properties. Default is ON.
Turn on Bluetooth low energy technology	When checked, Bluetooth® comms are enabled for the reader. Default is OFF.
Advertise reader name	When checked, the reader's name will be displayed in the Gallagher Mobile Connect App. Default is ON. If the reader has been configured with a Short Name, the Short Name will be used. Names longer than 26 characters will be truncated. If set to OFF, a generic identifier incorporating part of the reader's HBUS serial number will be shown in the Gallagher Mobile Connect app, (e.g. Reader: 12345).
Transmit Power	Controls the Bluetooth® signal strength. Default is -26 dBm. **Notes:** • Increasing the transmit power will increase the Bluetooth® connection distance. • Reducing the transmit power can be used to prevent closely located readers from interfering with each other Bluetooth® communications.
Auto connect range	When checked, all mobile devices will automatically initiate an access request when they sense a signal stronger than this value. Lower values indicate a stronger signal, and thus higher values will allow access from farther away. Default is 45 dBm. Auto connect will be disabled when: the Door that this reader is assigned to has no Access Zone assigned to it, or the Door that this reader is assigned to has one Access Zone that is in access mode 'Free-No PIN', or the reader is assigned to an Elevator with all floors in access mode 'Free-No PIN'. the Door's Emergency Release has been triggered. **Note:** Auto connect may not be suitable for all reader installations, (e.g. if a user is situated close to the reader, continual connection attempts from the reader will reduce the device's battery).

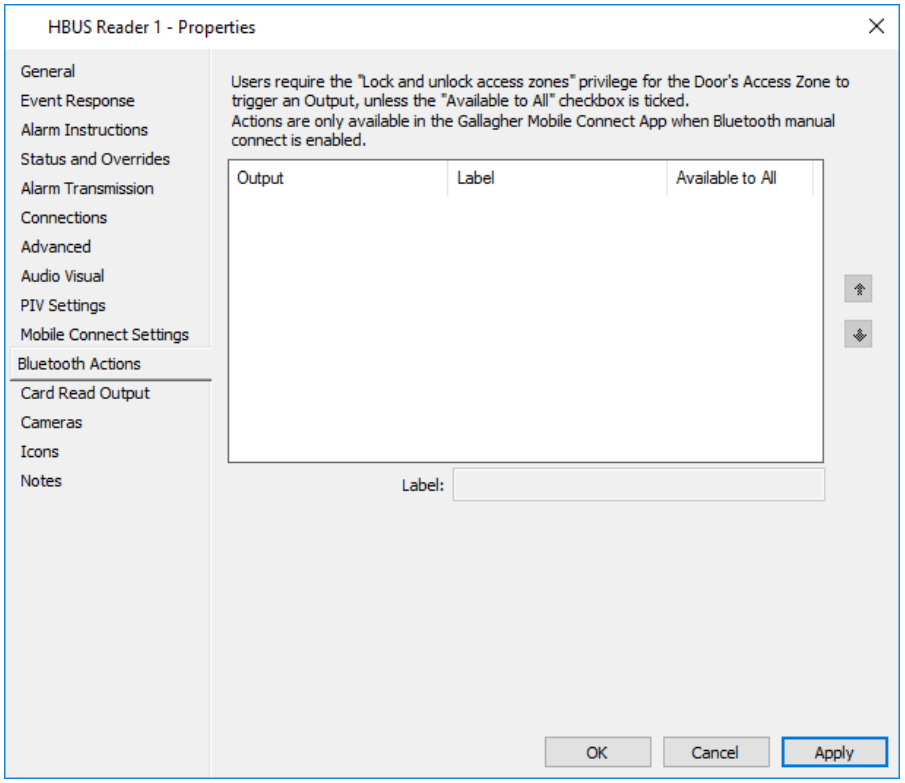
Field	Description
Manual connect range	When checked, the user will be able to manually initiate an access request from this range (which must be a longer range than the auto-connect range), using the Gallagher Mobile Connect App. Default is 64 dBm.



Notes:

- Increasing the path loss value will increase the reader's Bluetooth® read range.
- Consideration should be given to the installation environment, as environmental factors may reduce the reader's Bluetooth® read range. It is advised that each readers transmit power and connection ranges are individually calibrated. The Gallagher Mobile Client App can be used to calibrate the signal strength for each reader.
- Consideration should be given to the signal strength of readers that are installed back-to-back. For example, a reader installed at the front door is set to 'Secure-PIN' and the exit reader on the other side of the wall is set to 'Secure', a user could connect to the exit reader and gain entry without entering a PIN.
- If the reader is assigned to an Elevator, the user will be required to enter a second authentication factor, if any of the Elevator's floors require a PIN.

4. Click the **Bluetooth Actions** tab.



5. From the Hardware List Window, select the Outputs you wish to trigger (On/Off) using the Mobile Connect App.
   Drag and drop them into the **Bluetooth Actions** tab window.

   The Output Name will be used within the Mobile Connect App. To use a different name within the Mobile Connect App, enter a **Label** for the Output. Maximum of 20 characters.

   If you require a non-authorised user, (i.e. a user who has not been assigned the "Lock and unlock access zones" privilege for the Door's Access Zone) to be able to trigger an Output, check the **Available to All** checkbox for the Output. The Output will appear in the Mobile Connect App.

   Notes:

   - In order to perform actions at the reader, the reader must be configured for Manual Connect.
   - NFC cannot be used to perform an action at a reader, only Bluetooth® comms.
   - When a second authentication factor is required, the second factor must be presented before the action can be requested. The user will have up to 30 seconds to perform the action without needing to re-enter their second factor.
   - Actions are not available when the reader is assigned to an Elevator. Entry to the Access Zone will be the only action available.

- Other users can continue to request access at the reader while a user decides which action to perform. Bluetooth® comms are only used to perform the privilege check and the action.
- A maximum of 10 Outputs can be assigned to a reader.
- An Output whose state should be changed by a Command Centre operator only, should not be assigned here.
- An Output can be configured to perform various functions in Command Centre when triggered, (i.e. an Action Plan assigned to the Output contains a Macro that when triggered perform various actions in Command Centre).

6. Once you have all the Outputs you require in the window, you can re-order the Outputs by using the **up** and **down** arrow buttons to the right of the window. The order you sort the Outputs in here will be the order they appear in the Mobile Connect App.
7. Click **OK** to save your changes.
   Click **Cancel** to exit without saving your changes.
   Click **Apply** to save your changes and stay in this window.

Performing Bluetooth® Actions

Introduction

Actions that can be performed by a suitably privileged user at a Gallagher Bluetooth® enabled reader using the Mobile Connect App are:
- Gain entry to an Access Zone
- Arm or disarm the Door's Access Zone
- Change the access mode for the Door's Access Zone
- Change the state of Outputs

Notes:

- In order to perform actions at a reader, the reader must be configured for Bluetooth® and Manual Connect.
- When a second authentication factor is required, the second factor must be presented before the action can be requested. The user will have up to 30 seconds to perform the action without needing to re-enter their second factor.
- Actions are not available when the reader is assigned to an Elevator. If allowed, entry to the Access Zone will be the only action available.
- Other users can continue to request access at the reader while a user decides which action to perform. Bluetooth® comms are only used to perform the privilege check and the action.

Procedures

Refer to the appropriate procedure:

- ***Gaining entry to an Access Zone*** (on page 31-15)
- ***Arming or disarming the Door's Access Zone*** (on page 31-16)
- ***Changing the Door's access mode*** (on page 31-17)
- ***Changing the state of Outputs*** (on page 31-18)

Gaining entry to an Access Zone

Introduction

The Actions menu within the Mobile Connect App can be used to gain entry to an Access Zone.

Notes:

- The Alarm Zone associated with the Door's Access Zone must be disarmed. If the user has the "Change to the Disarmed state" privilege, then the Actions menu will display the option to disarm.
- The user must belong to an Access Group that provides access to the Access Zone.

Procedure

1. In the Mobile Connect App, press the **Action** button located to the right of the reader's name on the Access screen.
   A list of available actions is displayed.
2. Select the **Access** option.
   If access is allowed, the reader will beep and the door will unlock.

Arming or disarming the Door's Access Zone

Introduction

The Actions menu within the Mobile Connect App can be used to arm or disarm the Alarm Zone associated with the Door's Access Zone.
Notes:

- To disarm the Alarm Zone, the user must belong to an Access Group that has the "Change to the Disarmed state" privilege for the Alarm Zone.
- To arm the Alarm Zone, the user must belong to an Access Group that has the "Change to the Armed state" privilege for the Alarm Zone.
- If no Alarm Zone has been assigned to the Access Zone, no option to arm or disarm will be provided in the Actions menu.
- The reader will beep if the arm/disarm action is successful.

Procedure

1. In the Mobile Connect App, press the **Action** button located to the right of the reader's name on the Access screen.
   A list of available actions is displayed.
2. Select either **Arm** or **Disarm**.

Changing the Door's access mode

Introduction

The Actions menu within the Mobile Connect App can be used to change the access mode of the Access Zone associated with the Door.
Notes:

- The Alarm Zone associated with the Door's Access Zone must be disarmed. If a user has been assigned the "Change to the Disarmed state" privilege for the Alarm Zone, the user can disarm and change the access mode in one action.
- The user must belong to an Access Group that has the "Lock and unlock access zones" privilege for the Access Zone associated with the Door.
- The reader will beep if the access mode change is successful.

Procedure

1. In the Mobile Connect App, press the **Action** button located to the right of the reader's name on the Access screen.
   A list of available actions is displayed.
2. Select the access mode you require: Mode 1, Mode 2, or the scheduled state.
   Note: The access modes for an Access Zone are configured on the **Access Mode** tab in the Access Zone's properties. A Display Name can be configured for each access mode here.

Changing the state of Outputs

Introduction

The Actions menu within the Mobile Connect App can be used to change the state of Outputs, (e.g. turn on or off building lights and air conditioning).
Notes:

- A maximum of 10 Outputs can be assigned to a reader.
- An Output can be configured to perform various functions in Command Centre when triggered, (i.e. an Action Plan assigned to the Output contains a Macro that when triggered perform various actions in Command Centre).

Procedure

1. In the Mobile Connect App, press the **Action** button located to the right of the reader's name on the Access screen.
   A list of available actions is displayed.
2. Select the Output whose state you wish to change.

SALTO Mobile Access Integration

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

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

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

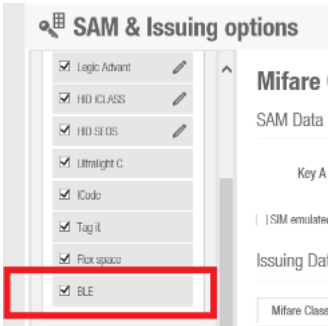
For further detail refer to the ***Mobile Connect Cloud and App Security TIP.pdf*** (located in the 'Mobile Client' directory of the Command Centre installation files). **Notes:**

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

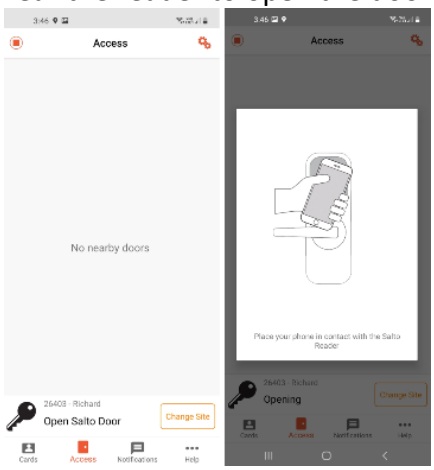
Prerequisites

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

- Command Centre mobile connect,
- Command Centre,
- Cloud Server,
- Salto Server,
- Salto BLE licenses,
- Salto Ethernet Encoder (Dongle), and
- SALTO Bluetooth-capable wired or wireless online locks
- Bluetooth settings defined in SALTO, as follows:
  a) Select **System** > **SAM & Issuing options**, and tick **BLE**.



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



Licensing

Salto SPACE licensing required:

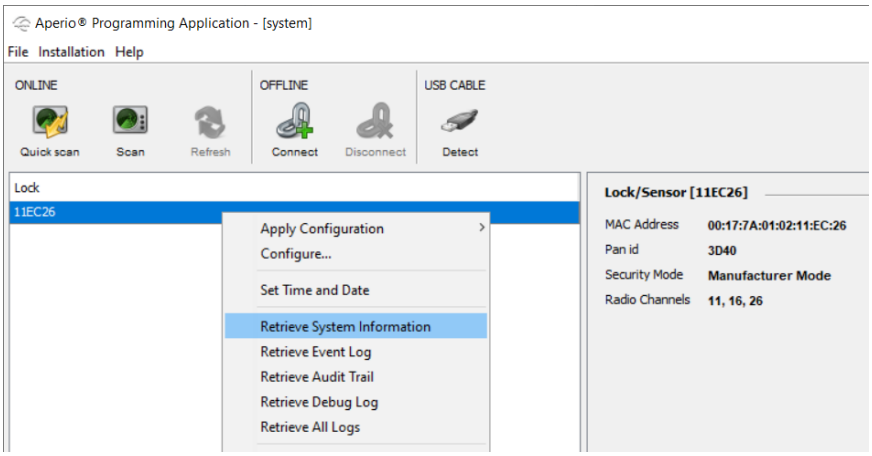
- C866020 - SALTO BLE SITE LICENSE (SPACE OPT 0028-2 - ANNUAL)
- C866023 - SALTO BLE WIRELESS DOOR LICENSE (SPACE OPT 0033) Converts BLE Offline readers to Online. Requires one per wireless door.

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

Aperio Mobile Access Integration

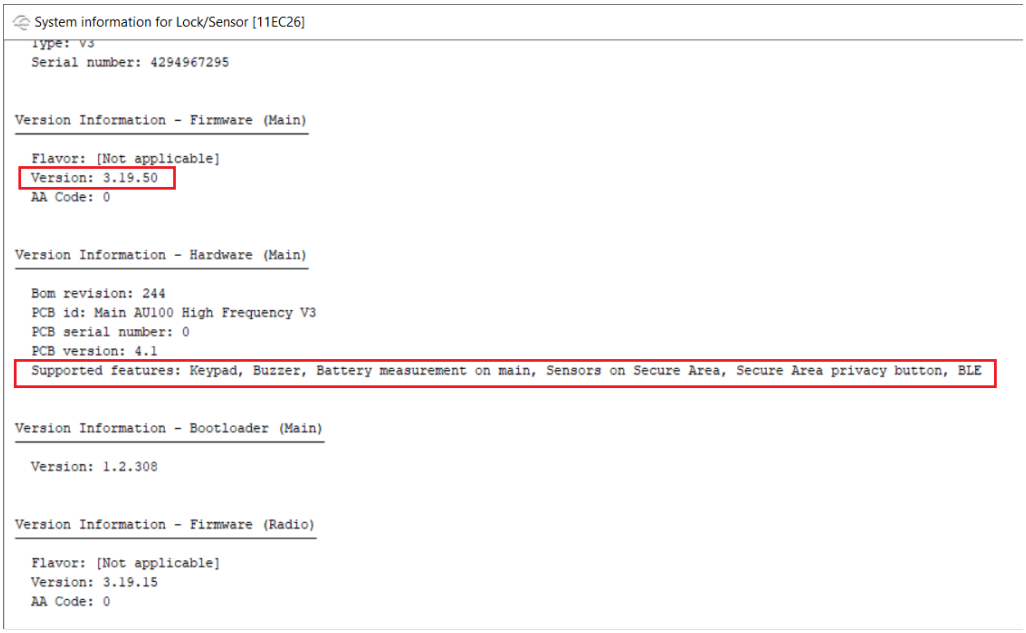
If your site has Aperio BLE capable locks connected to Command Centre, then the Gallagher Mobile Connect app can be used to open such locks. This requires Gallagher Command Centre version vEL9.00 or newer.

Aperio mobile access will be available for all users with mobile credentials provided that the prerequisites are fulfilled. However, Aperio locks must be BLE compatible and updated with firmware that provides Gallagher mobile credential support. This can be verified with the Aperio Programming Application Protocol (PAP) by **right-clicking** on the lock/ reader and selecting **Retrieve System Information**.



The System information for Lock/Sensor screen displays showing the BLE item under supported items.

Note: Aperio firmware version needs to be 3.19.50 or higher for Gallagher Mobile Credential support.



Aperio BLE locks do not advertise access unlike Gallagher readers. Cardholders must contact the Aperio lock with their phone similar to a card to activate the reader. The lock will then appear on the Mobile Connect app if they are a member of the lock's facility. No feedback is given on access inside the app itself. Cardholders are encouraged to check the lock itself for the access result.

For Aperio lock configuration with the PAP tool, refer to ***Aperio Integration*** (on page 72-1).

Prerequisites

For an Aperio BLE credential to be provided to mobile credential cardholders:

- Gallagher Mobile Connect app (for each cardholder)
- Mobile credentials assigned (for each cardholder)
- Command Centre Cloud connected
- Aperio site key generated

For an Aperio lock to recognise Gallagher mobile credentials:

- Aperio BLE compatible lock (with firmware 3.19.50 or higher)
- Aperio Hub connected to Gallagher controller
- Aperio PAP configuration with Gallagher mobile credentials

Licensing

Aperio licensing required:

- 2A8995 APERIO DOOR LICENCE WITH HARDWARE

Access

To access an Aperio BLE lock:

1. Open the Mobile Connect app.
2. Hold the phone up to the reader where a card would normally be read, typically there is a wireless symbol to indicate the badge point.
   The lock will show up on the Mobile Connect app and auto-connection will initiate.
3. If 2FA is enabled, you must authenticate with your screen lock.
   Access is granted or denied.
4. If in the 2FA scenario, you may be denied access if you have not set an Android or iOS screen lock. Your phone must be secured for credentials to be available.
   Set a screen lock by following the manufacturer instructions for the appropriate device.