Gallagher Command Centre

# Configuration Client User Guide

Volume 2

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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

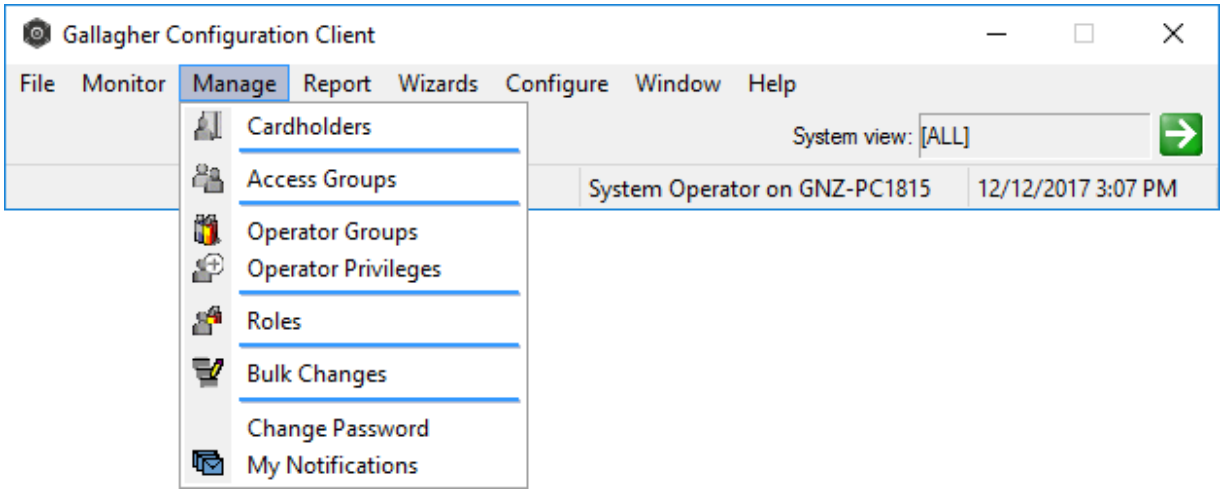
**Index I-1**

# Part 3: Site Management

It is the role of the Command Centre System Administrator to monitor and maintain the Command Centre software and hardware.

This part of the User Guide provides details on how to perform the functions required for managing 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 **Manage** option on the Command Centre main menu bar.




The only exceptions are:

- Chapter 33 - Personal Data Fields, which is accessible via the **Configure** option of the menu bar.
- Chapter 39 - Reports, which is accessible via the **Report** option on the menu bar, and
- Chapter 40 - Archives, Backups and Restores. 'Backup' and 'Archiver' are both accessible via the **File** option on the menu bar, and the 'Restore' function displays as an icon on your desktop (Server only, not presently on Workstations).

**Note:**
Depending on your operator privileges or your current system view, some menu items referred to may not be visible to you.

# Chapter 32: Cardholders

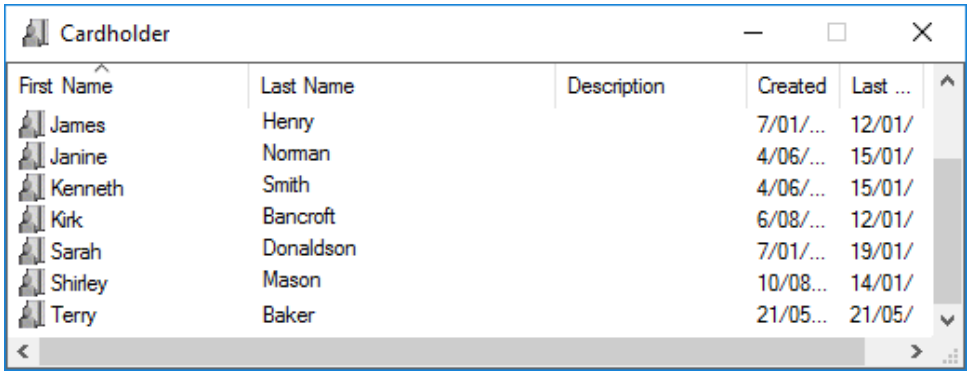
## Introduction

The **Cardholder** List Window enables you to manage all cardholders that have access to your site.
You can view, edit, add and delete cardholders.

Your site license will determine the number of Cardholders you can have.

## The Cardholder List Window

The **Cardholder** List Window opens in grid view.




**Note:**
Operators can be configured so they will be able to view cardholders from any Division in the system. Although all cardholders will display in the **Cardholder** List Window, the properties for all will not be viewable, as follows:

- For cardholders in your own Division everything will be viewable and editable.
- For cardholders in another Division only the **Access Groups** tab will be viewable. (The Access Groups this operator is assigned to will not display if they are 'out-of-division'.)

For further detail see ***Cardholder Management across Divisions*** (on page 9-5).

## Adding a New Cardholder

### Introduction

Details for every person requiring access to Command Centre sites must be set up within Command Centre.

This procedure is split into two parts, as follows:

- Creating Cardholders,
  (i.e. providing the minimum information required to create a new Cardholder)
- Configuring a Cardholder,
  (i.e. linking the various components to it - Card Types, Access Groups, Operator Groups and Personal Data Fields are the components of a Cardholder).

You can create a new Cardholder, then configure it at a later stage, once you have set up the necessary components for it.
**Note:** Your site license will determine the number of Cardholders you can have, therefore once you have added all you are allowed, the option to create more will be disabled.

### Procedure

#### *Create the Cardholder*

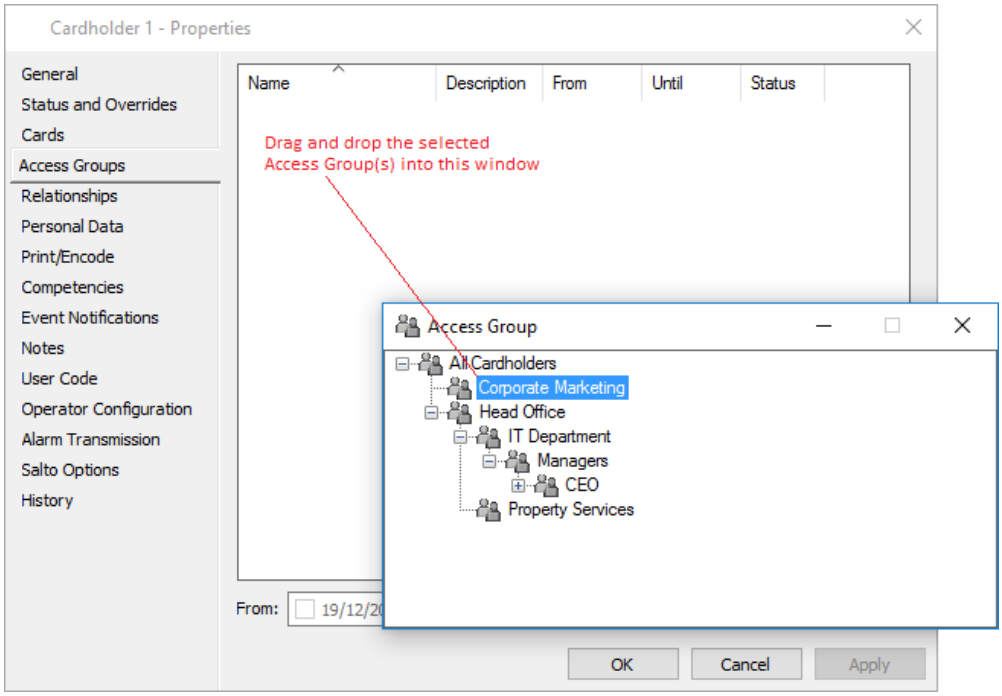
1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. **Right click** and select **New...Cardholder**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Apply** button, and the Cardholder is created. The rest of this procedure allows you to fully configure the Cardholder.

#### Configure the Cardholder

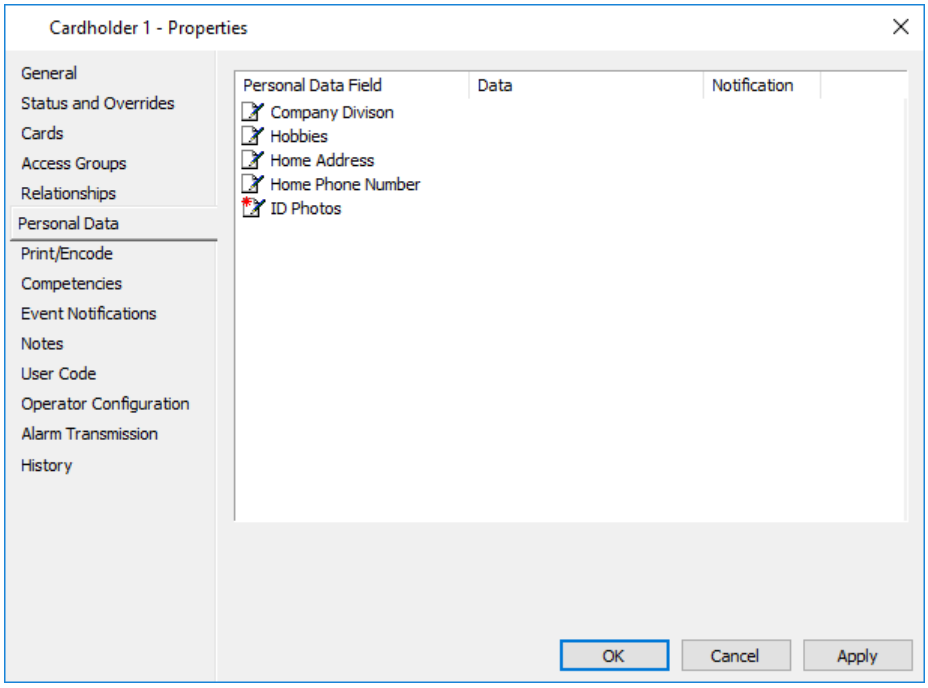
5. Ensure the following information has already been set up:
   *Divisions*
   Refer to ***Setting up System Division*** (on page 9-3).
   *Card Types*
   Refer to ***Setting up Card Types*** (on page 7-2).
   *Access Groups*
   Refer to ***Setting up Access Groups*** (on page 34-4).
   *Operator Groups*
   Refer to ***Setting up Operator Groups*** (on page 36-5).

*Personal Data Fields*
Refer to ***Creating a new Personal Data Field*** (on page 33-2).

6. Click the **Cards** tab. (See ***Adding a card to a Cardholder*** on page 32-9 for procedure)
7. Click the **Access Groups** tab.
8. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens.
   Select the Access Group(s) that the cardholder will belong to.
   Drag and drop them into the **Access Groups** tab.
   **Notes:**
   - It is recommended that you do not assign a cardholder to any more than ten Access Groups, as too many Access Groups per cardholder will result in slow access responses. See ***Setting up Access Groups*** (on page 34-4) for further detail.
   - A cardholder can be granted temporary access to an Access Group. See Temporary Access for further details.



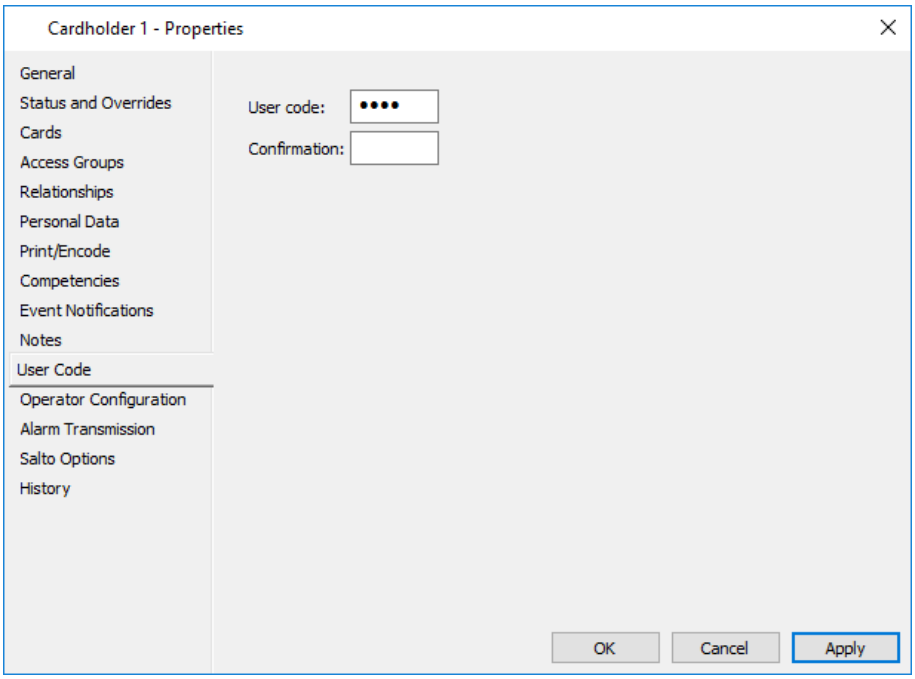

9. Close the **Access Group** List Window.
10. Click the **Personal Data** tab.




See ***Editing a Cardholders PDF data*** (on page 32-20) for the procedure.

11. Click the **Notes** tab if you want to add a note(s) about this cardholder.
    **Note:** Depending on your operator privileges, the **Notes** tab may or may not display.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).

12. If your site has HBUS Terminals installed, and this cardholder will be required to access these Terminals, click the **User Code** tab.
    If not, go to Step 15.
    **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.



13. Enter a 4-8 digit User Code that will be used to identify this cardholder at a HBUS Terminal.
    **Note:** You can find out which Cardholders have user codes by running a summary Cardholder Report and selecting the User Code field. While the report will indicate who has a user code, the actual codes will not be disclosed.
14. Is this Cardholder an Operator?
    If **no**, go to Step 15.
    If **yes**, click the **Operator Configuration** tab and see ***Configuring Operators*** (on page 36-14) for the procedure.
    **Note:** The **Operator Configuration** tab only displays if you have "Edit Cardholders" and "Edit Operators" privileges.
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 cardholder is added.

**Hints**

*Editing and Deleting Cardholders*
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Cardholders.
**Note:** Although deleted, a Cardholder's actions may still appear in an Activity Report. Refer to ***Activity Report*** (on page 39-15).

*Copy and paste*
An alternative to the drag and drop method is to use the copy and paste method.

*Copying cardholder details*
To speed up the process of adding new cardholders, details for the new Cardholder can be copied from an existing cardholder. See ***Copying Cardholder details*** (on page 32-7).

*Operator Configuration details*
When a system administrator sets up a cardholder as 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. See ***Changing Operator Passwords*** (on page 2-16).

*Advanced drag and drop feature*

Cardholders can be dragged and dropped directly from their own List Window into another List Window. See ***Using the advanced drag and drop feature*** (on page 2-24) for further detail.

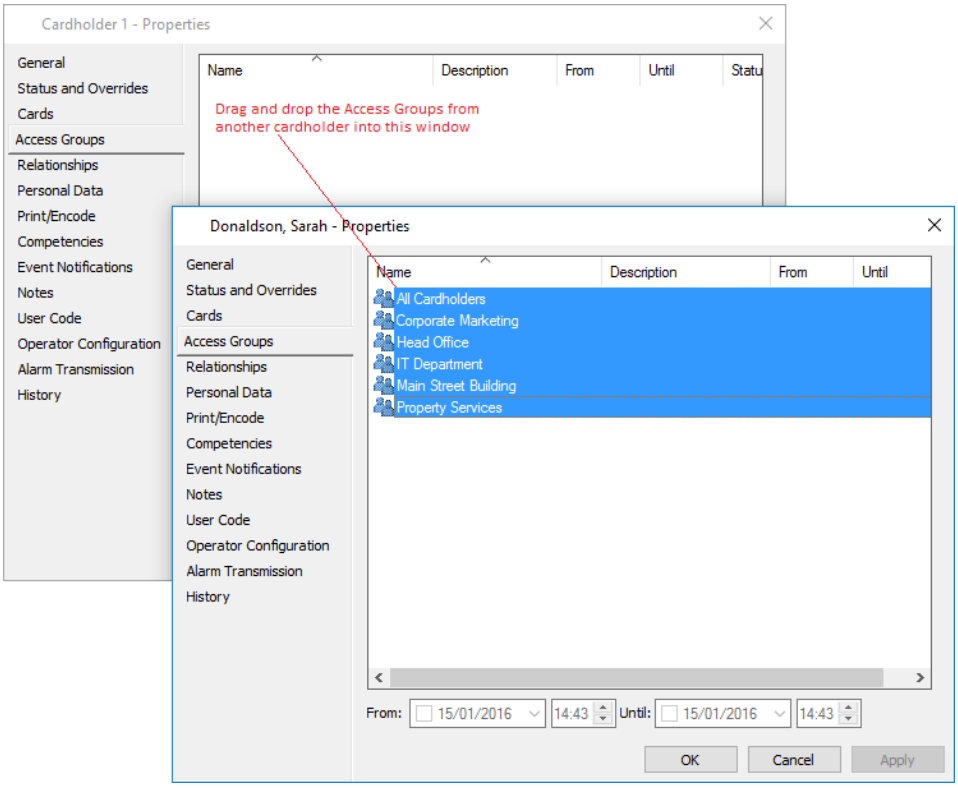
# Copying Cardholder details

## Introduction

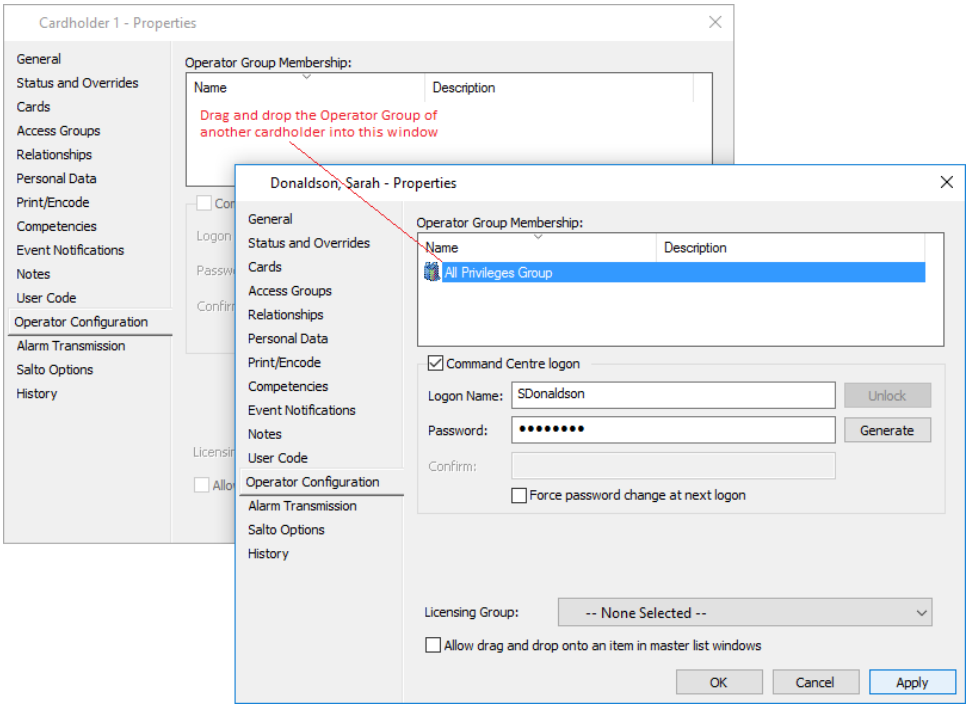
Details for new cardholders can be copied from an existing cardholder. Likewise, if a cardholder is given more than one card, the data needs to be duplicated.
Copying cardholder details speeds up the process of adding new cardholders.

## Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. **Right click** and select **New...Cardholder**.
   By default the **General** tab displays.
3. Type in the new cardholders name, an appropriate description and division.
4. Click the **Cards** tab.
   See ***Adding a card to a Cardholder*** (on page 32-9) for procedure.
5. Click the **Access Groups** tab.
6. From the **Cardholder** List Window, open the **Properties** window of the existing Cardholder whose details you wish to copy.
7. Click the **Access Groups** tab of the "existing" cardholder and select the access groups.
   Drag and drop them into the **Access Groups** tab of the new cardholder.



8. If the Cardholder is an Operator, click the **Operator Configuration** tab. If not, go to Step 10.
9. In the **Properties** window of the "existing" cardholder, click the **Operator Configuration** tab and select the operator group.
   Drag and drop it into the **Operator Configuration** tab of the new cardholder.




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 new cardholder, with details copied from an existing cardholder, is added.

# Adding a Card to a Cardholder

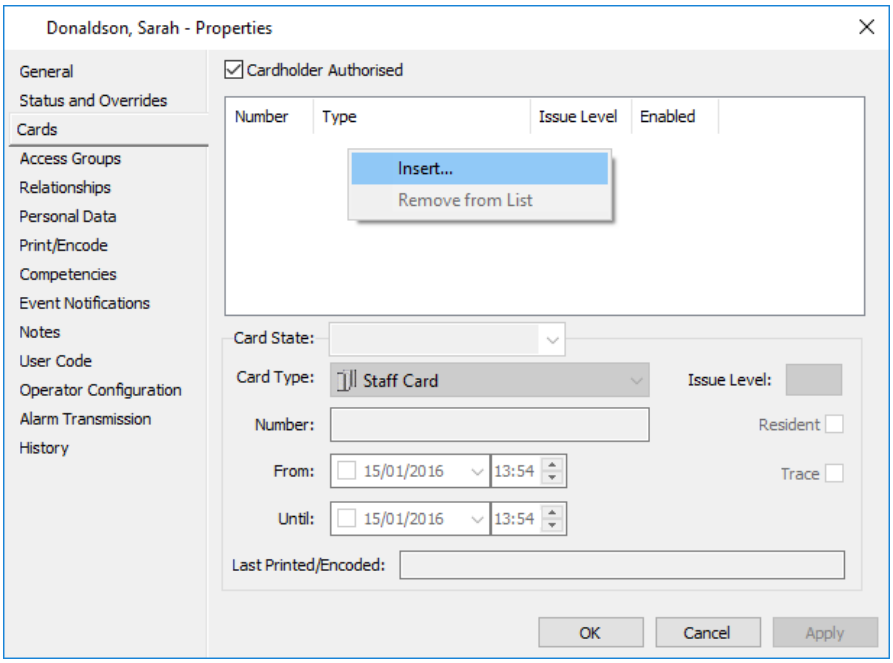
## Introduction

A card is an access token. The cardholder presents the card to a reader to gain access to a zone or elevator level.

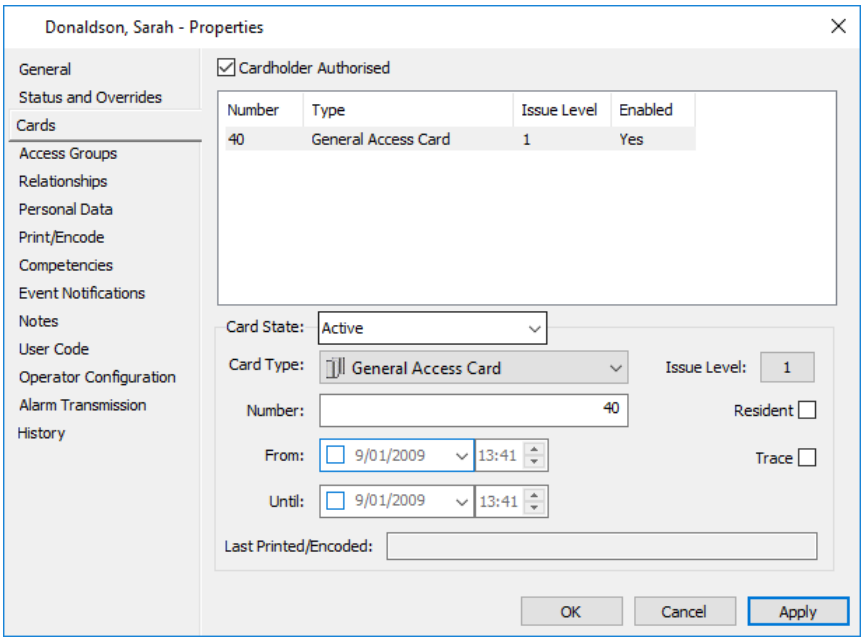
One cardholder may be issued with more than one card; for example, they require access to different sites.
**Note:** The default limit is 500 cards per cardholder.

## Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the Cardholder to edit.
3. **Right click** and select **Properties**.
4. Click the **Cards** tab.
   The **Cardholder Authorised** checkbox is ticked by default. This authorises the cardholder so they can use their cards. This is not specific to one card -it authorises the use of all cards listed.
5. **Right click** anywhere within the upper grid, (i.e. on a column header, on the scroll bar, in the blank area or on a card if there is one), and select **Insert**.




A "new card" is added to the upper grid and highlighted. This new card is enabled and if it has had card defaults already configured, (see ***Setting up Card Types*** on page 7-2), the 'From', 'Until' and/or 'Issue Level' fields will be populated with those defaults. The card will also be allocated the next available 'Number'.




6. Is the "new card" the required Card Type?

| If... | then... |
|---|---|
| yes | go to Step 7. |
| no | click the **Card Type** drop-down menu box and select the correct Card Type. For example, proximity card, mag-stripe card, etc.<br>**Note:** The default settings will change to that of the card type selected. |

7. Set the remaining card details.
   **Note:** If the 'From', 'Until' and/or 'Issue Level' fields are populated with default settings, they can be overwritten if required. The card number can also be overwritten prior to saving changes on this screen.

   **Card State**
   Each card requires a current state. The state selected initially is configured from the Card Type's Card State Set, and the drop-down will be populated with all the card states that are available for use.

   **Number**
   Each card requires an encoded number to uniquely identify it. Once you click Apply the card number becomes greyed out and can not be altered. The card number range that can be assigned to a card type is set in the Card Type properties. The card number format of the selected card type will determine what characters can be used, as follows:

| If the card type is... | then... |
|---|---|
| **Decimal** format, | a decimal card range is supported. The system "auto-allocates" a card number, however this can be overwritten if required by typing another number over the one allocated prior to saving changes on this screen. |

| If the card type is... | then... |
|---|---|
| **Text** format, | if a regular expression syntax string has been configured in the Card Type properties, you will be forced to enter a card number that fits that definition.<br>**Notes:**<br>• a maximum of 251 alphanumeric characters are supported. However, with some languages this may be less as some characters use more than one byte.<br>• If you enter an invalid card number, an error message will display indicating it is invalid, and show what the syntax string pattern is. |

**From**
Set the date and time the card will be activated - the Command Centre system will accept the card details when presented.
*Note:* 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.

**Until**
Set the date and time the card will expire - the Command Centre system will not accept the card after this date.
*Note:* If you do not enter a date in this field, the card will not expire.

**Issue level** (1 to 15)
If a card is replaced, you do not need to go through the process of creating a new card; you can simply increment the issue number.
A card may need to be replaced if the cardholder has lost their card, for example.

**Resident**
Check this box if you require the details of this cardholder to be stored (resident) at the Controller.
The Controller stores a 'resident' cardholder and security parameters database to enable it to carry out access control and security functions. The cardholder database stores access data for cardholders who will regularly use the devices attached to that Controller. It enables the Controller to make access control decisions instantaneously.

For cardholders that are not included in the resident cardholder database, when they present their card, the Controller requests access information from Command Centre. Their information is then stored on the resident database, but may get discarded if the Controller Cardholder database becomes full and another unknown user presents their card. If communications fail and the cardholder information is not in the Controller, that cardholder will not be able to gain access.

**Trace**
A message and/or alarm is generated each time the card is presented to a reader, including readers that are associated with Remote Arming Terminals.

**Last Printed/Encoded**
A read-only field displaying the "Last Printed/Encoded" information, (i.e. the date last printed and/or encoded, and the Issue Level used), for the currently selected card.

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.

   **Notes:**
   - When you save changes at this stage, depending on the expiry date set for the card, a "card activated" or "card expired" event may be logged in the **Event** window.
   - Once you save your changes the Card Type and Number fields become greyed out and can not be changed.

**Result**

The new card details are updated to reflect the changes you have made.

**Hint**

There cannot be two cards in the system with the same card number *and* the same card type.

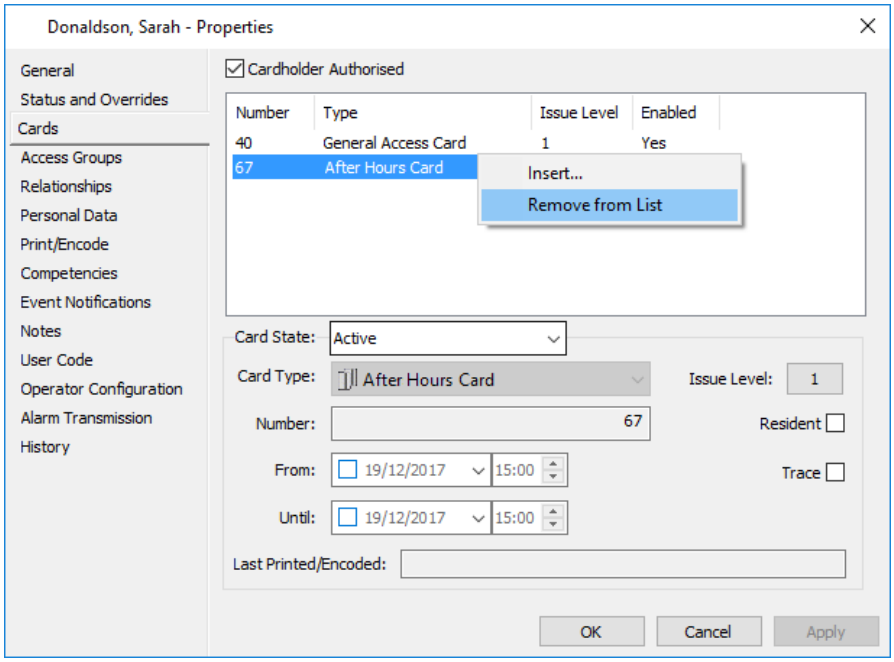
# Removing a Card from a Cardholder

## Introduction

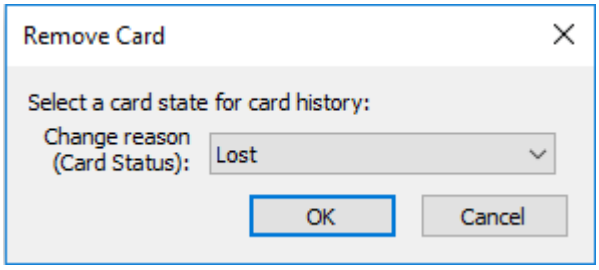
When a card is no longer required, it can be removed from the cardholders list of cards.

## Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the cardholder to edit.
3. **Right click** and select **Properties**.
4. Click the **Cards** tab.
5. Click on the card you want to remove.
6. **Right click** and select **Remove from List**.




A Remove Card pop-up displays.



7. Select the appropriate card state for card history, (e.g. Lost, Damaged, etc.) from the **Change Reason (Card Status)** drop-down of available card states.
8. Click the **OK** button.
   The Remove Card pop-up closes and the card disappears from the list of cards in the upper 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.

**Result**

The card details are removed from the card list.

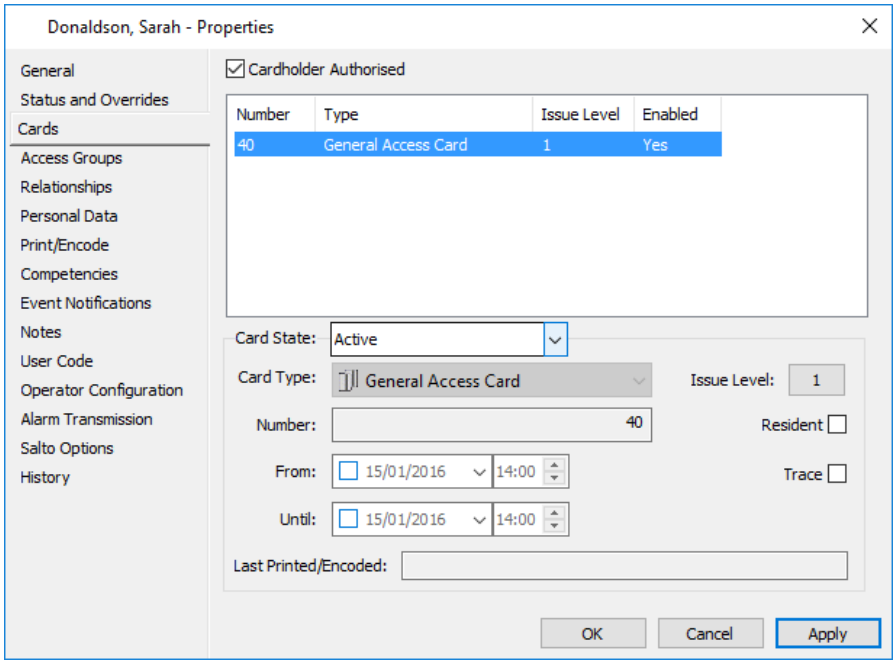
# Editing Card details

## Introduction

You may need to change card details for a particular cardholder. For example, a replacement card is given to a cardholder and you are required to alter the card's issue number.

## Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the cardholder to edit.
3. **Right click** and select **Properties**.
4. Click the **Cards** tab.




5. Select the card that requires editing.
6. Edit the card information as appropriate for this cardholder.
   For details on the fields, refer to ***Adding a Card to a Cardholder*** (on page 32-9).
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 card details are updated to reflect the changes you made.

## Enabling Card Trace

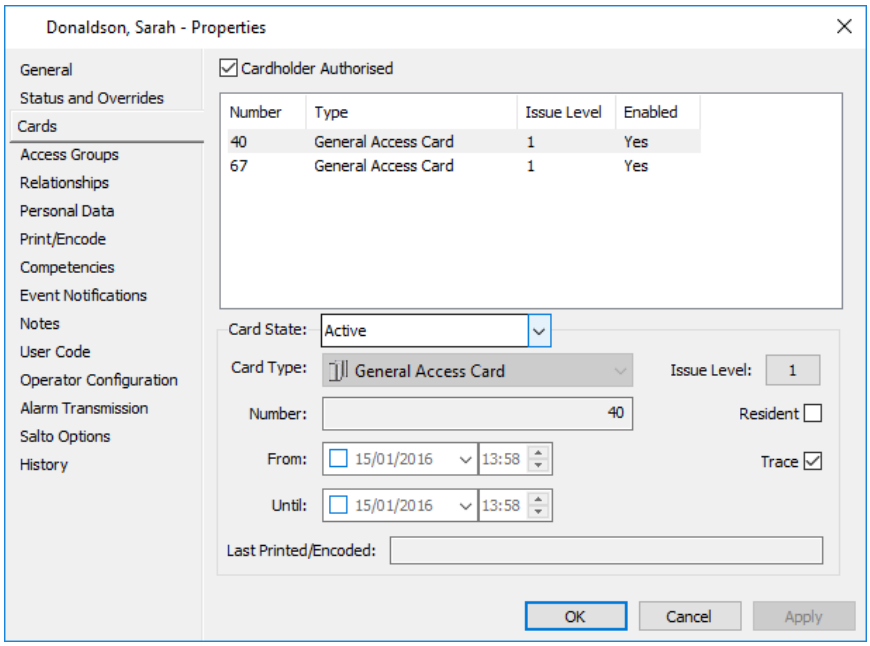
### Introduction

When adding a new cardholder or editing cardholder data in Command Centre, you can specify that a "card trace" be put against the cardholder. This will cause an alarm to be generated everytime the cardholder presents their access card or token.

**Note:** The event default setting for Card Trace alarms can be changed via the **Event Defaults** tab of the Command Centre Server Properties (see ***Event Defaults*** on page 6-12.)

### Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the cardholder you wish to trace.
3. **Right click** and select **Properties**.
4. Click the **Cards** tab.




5. Highlight the appropriate card by clicking on it.
6. Check the **Trace** checkbox.
7. Repeat Steps 5-6 to apply card trace to other access cards belonging to this cardholder, if necessary.
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

Card Trace has been applied to the cardholder's card(s).

# Reactivating Expired or Disabled cards

## Introduction

When a card has expired, an appropriate message displays in red text on the **Cards** tab of the Cardholder, according to what caused the expiry, as follows:

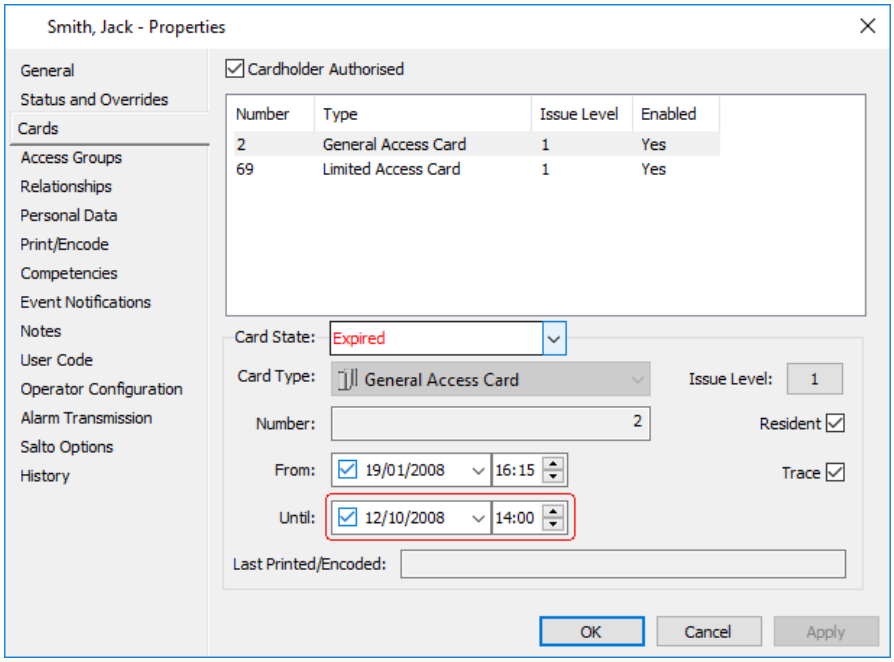
- **Scheduled Card Expiry**
  The life of a card has been specified by defining a "From" time and date and an "Until" time and date.
- **Inactive Card Expiry**
  A card is disabled after a specified period of card inactivity.

The following procedure describes how to reactivate expired cards.

## Procedure

### *Scheduled Card Expiry*

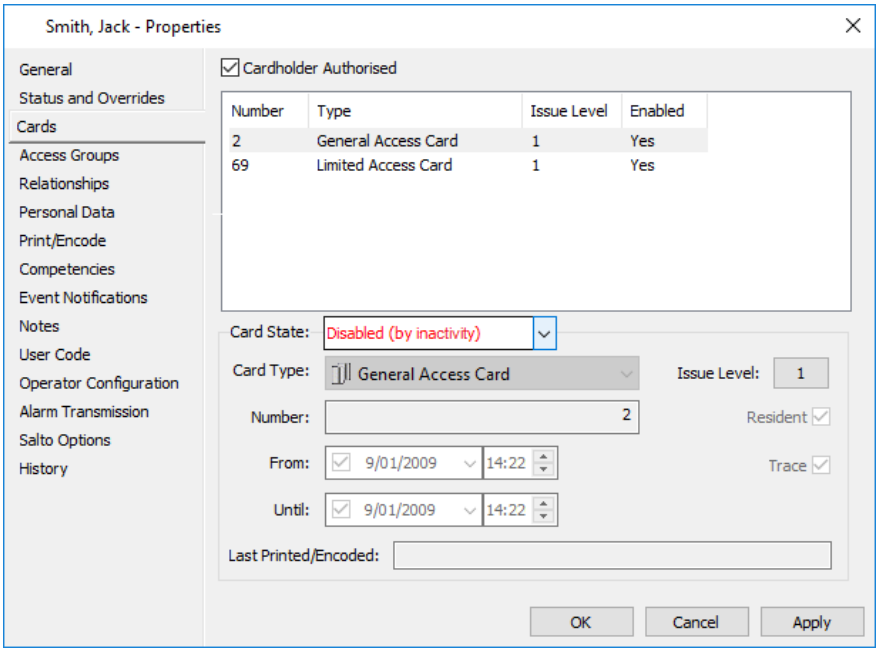
1. Open the **Cards** tab of the Cardholder.
2. Highlight the card that has expired, (i.e. the date in the "Until" column has passed).
   The message **Expired** (in red text) populates the **Card State** field.




3. Extend the "From" and/or "Until" dates and/or times as required.
4. Click **Apply**.
   The message in the **Card State** field changes from **Expired** (in red text) to **Active** (in black text). The card is now reactivated.
   **Note:** If you extend the "From" date and/or time to something in the future, the **Expired** message will change to **Not Yet Activated** (in blue text) once **Apply** is clicked.

### *Inactive Card Expiry*

1. Open the **Cards** tab of the Cardholder.
2. Highlight the card that is not enabled, (i.e. the card with No in the "Enabled" column).
   The message **Disabled (by inactivity)** (in red text) populates the **Card State** field.




3. Select the **Active** state from the **Card State** drop-down list.
4. Click **Apply**.
   The message in the **Card State** field changes from **Disabled (by inactivity)** (in red text) to **Active** (in black text). The card is now reactivated.

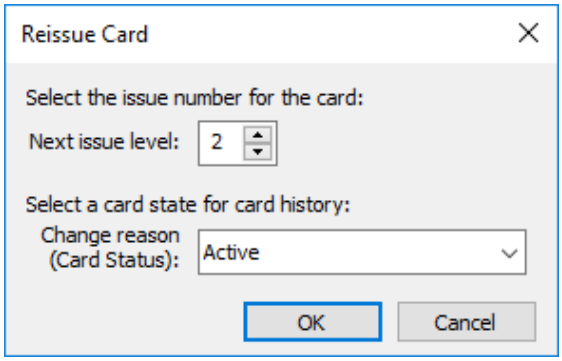
## Re-issuing a Card for a Cardholder

### Introduction

If a card is replaced, you do not need to go through the process of creating a new card; you can simply increment the issue number from the Cardholder properties.
A card may need to be replaced if the cardholder has lost their card, for example.

### Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the cardholder to edit.
3. **Right click** and select **Properties**.
4. Click the **Cards** tab.
5. Click on the card you want to re-issue.
6. Click the **Issue Level** button.
   The Reissue Card pop-up displays.




7. The Issue Level of the card needs to increment by one.
   Ensure the number that defaults into the **Next issue level** field is correct.
8. Select the appropriate reason for why you are re-issuing the card, (e.g. Lost, Damaged, etc.) from the **Change reason (Card Status)** drop-down of available card states.
9. Click the **OK** button.
   The Reissue Card pop-up closes and the number of the **Issue Level** button has incremented by one.
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

The card has been re-issued.

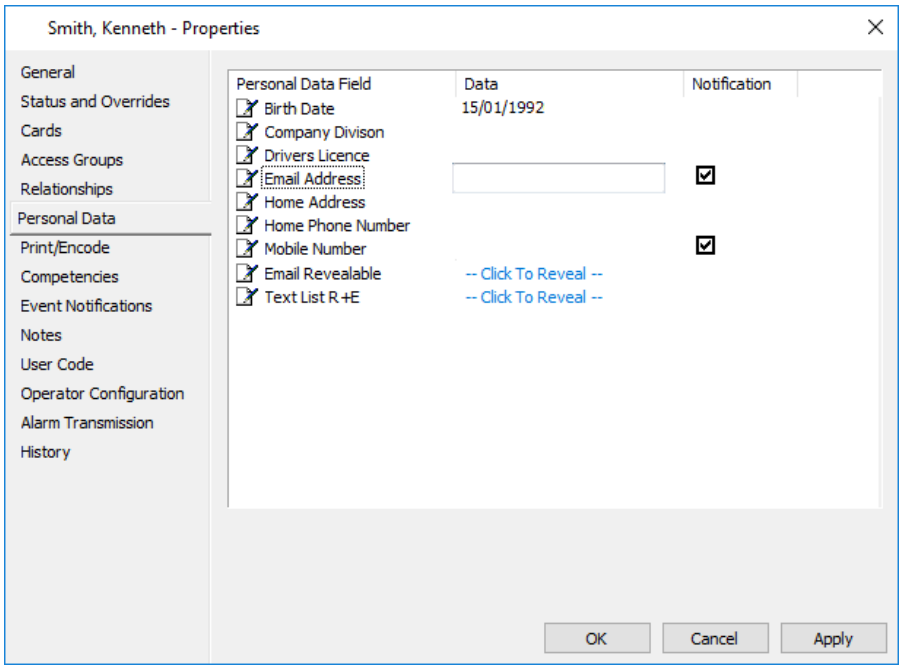
## Editing a Cardholders PDF data

### Introduction

This procedure enables you to enter a cardholder's personal data into the Personal Data Fields (PDFs).

### Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the cardholder to edit.
3. **Right click** and select **Properties**.
4. Click the **Personal Data** tab.
   **Note:** If an Access Group containing PDFs has been assigned to this Cardholder, then the PDFs associated with the Access Group will display here. Otherwise, the grid will be empty.
5. **Right click** over the data section of the PDF that you want to enter cardholder data against.
   The Data Entry field for that PDF is enabled.




**Note:** Personal Data Fields with either "Revealable" or "Revealable and Editable" accessibility display -- Click To Reveal -- in the Data Entry field. This accessibility is set on the **Type** tab of the Personal Data Field properties.



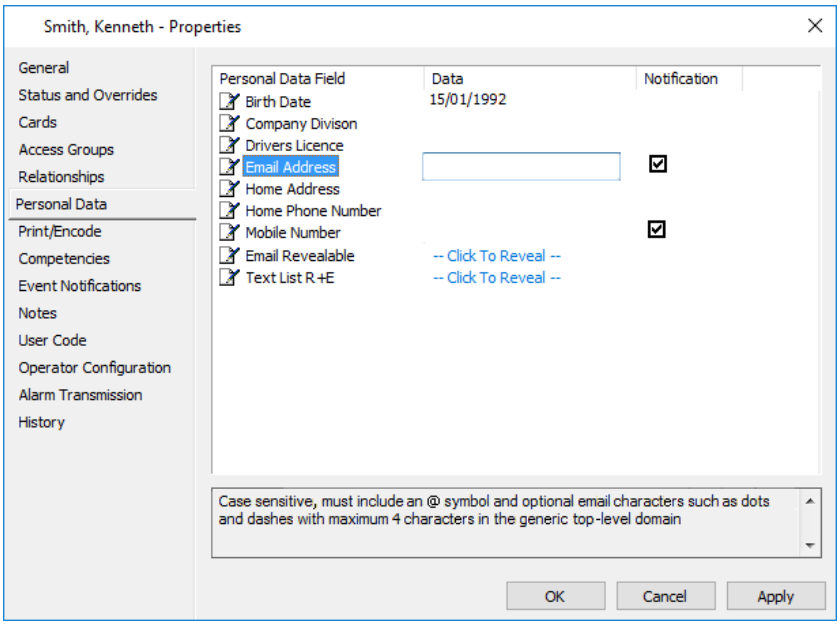

With the appropriate privileges, operators can either view or create and edit the value of a Personal Data Field by clicking on -- Click To Reveal --,

and then clicking the **Reveal** button that displays.
The **Default Notifications** checkbox will be revealed when the **Reveal** button is pressed, (i.e. it is a blank space until that happens).



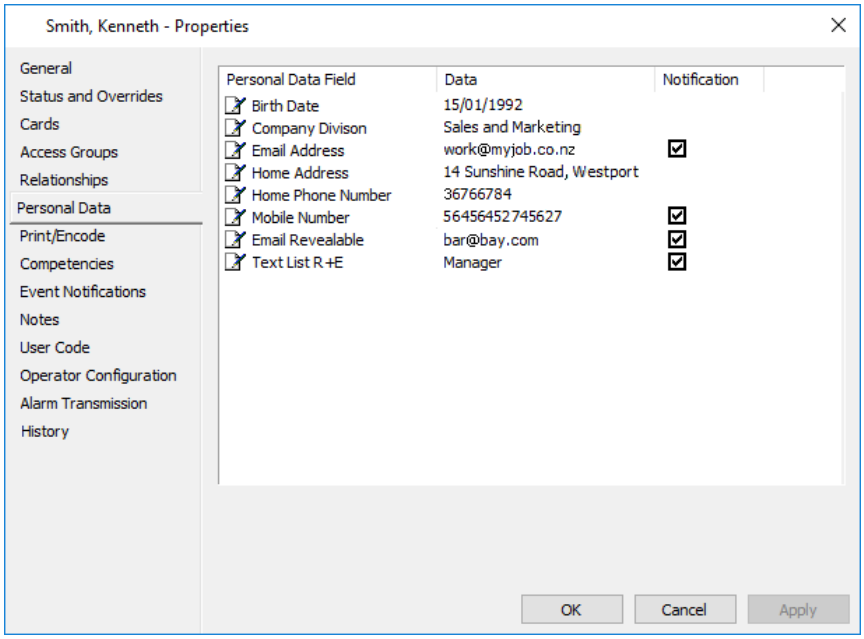

For further detail regarding "Revealable" and "Revealable and Editable" accessibility, and the operator privileges required, see ***Creating a new Personal Data Field*** (on page 33-2).

6. Enter the appropriate personal data.
   **Notes:**
   - Images, (e.g. corporate logos, cardholder photographs, etc.), can be captured and used for "Image" PDFs. Refer to Capturing an Image for the procedure.
   - By clicking on a "Date" PDF, a Date control appears. No date value is assigned if the checkbox is unchecked.
     A date must be supplied for required PDFs.
   - By clicking on a "Text - List" PDF, a pre-defined drop-down list appears. If it is a **Restricted** "Text - List" PDF, a cardholder can only have values populated from the pre-defined list, or a blank value. However, if it is **Unrestricted**, free text entry is allowed.
   - The **Notification** column contains a checkbox only for "Mobile" and "Email" type PDFs. When these checkboxes are ticked, it indicates that the PDF value is used in the Notifications feature for sending and receiving notifications, (i.e. "Mobile" for SMS and "Email" for Email notifications).
   - By clicking on a "Text" type PDF, or any of the contact type PDFs, (i.e. "Address", "Phone", "Email" or "Mobile"), a text box appears at the bottom to describe the regular expression syntax if the **Use Regular Expression** feature was enabled and defined on the PDF's **Type** tab.



**Note:** On applying the changes, an error message box will display of the PDF data entered does not meet the regular expression syntax.

7. Repeat Steps 5-6 for each PDF.




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

**Result**

The cardholder now has personal data recorded against the PDFs.

# Configuring a User Code for Terminal Access

## Introduction

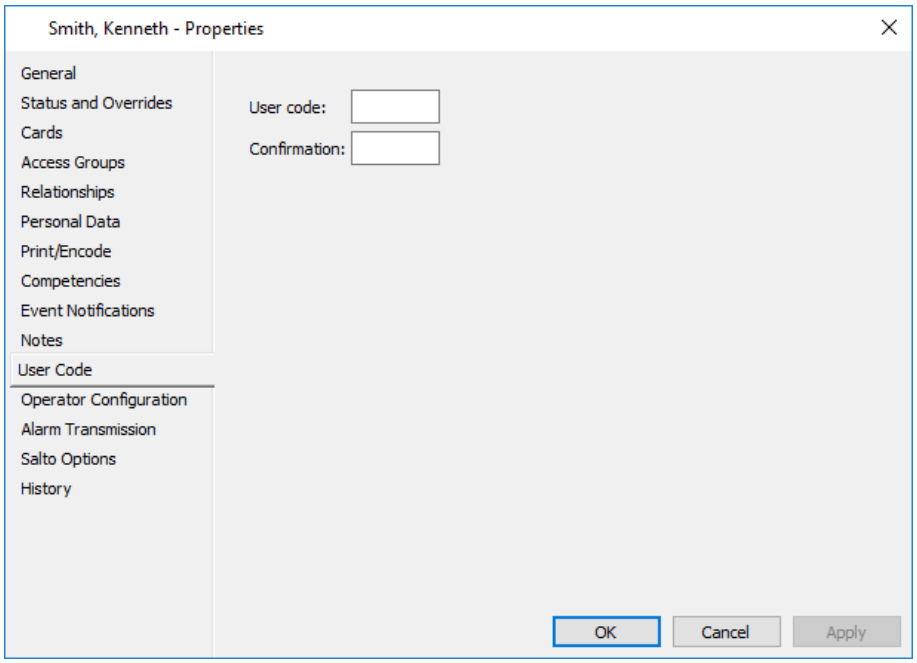
This procedure describes how to specify a user code for a Cardholder, in order to identify the Cardholder at an HBUS Terminal or HBUS Alarms Only Terminal.

Operators require the "Edit Cardholders" operator privilege, and must be in the same or a parent Division of the Cardholder. Without this operator privilege the fields on this tab will not be enabled.

**Note:** User Codes can also be used as PINs for any reader with a keypad. This is set via a checkbox on the **Advanced** tab of the reader properties.

## Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Highlight the **Cardholder** you wish to give a user code to.
3. **Double-click** the mouse button.
4. Click the **User Code** tab.




**Note:** This code will be hidden from all operators, regardless of privilege.

5. Enter a 4-8 digit user code in the **User code** field.
   **Notes:**
   - As you enter the user code, asterisks display in place of each digit.

- Command Centre enforces a user code range of 1 to 99999999. Therefore, the code must contain at least one non-zero digit, (i.e. 0000 or 00000000 are invalid and an error will be generated).

6. Confirm the user code by re-typing it in the **Confirmation** field.
7. Click **Apply**.

**Result**

A user code has been specified to identify a Cardholder at an HBUS Terminal or HBUS Alarms Only Terminal.

## Configuring User Codes for access at Card Readers with keypads

### Introduction

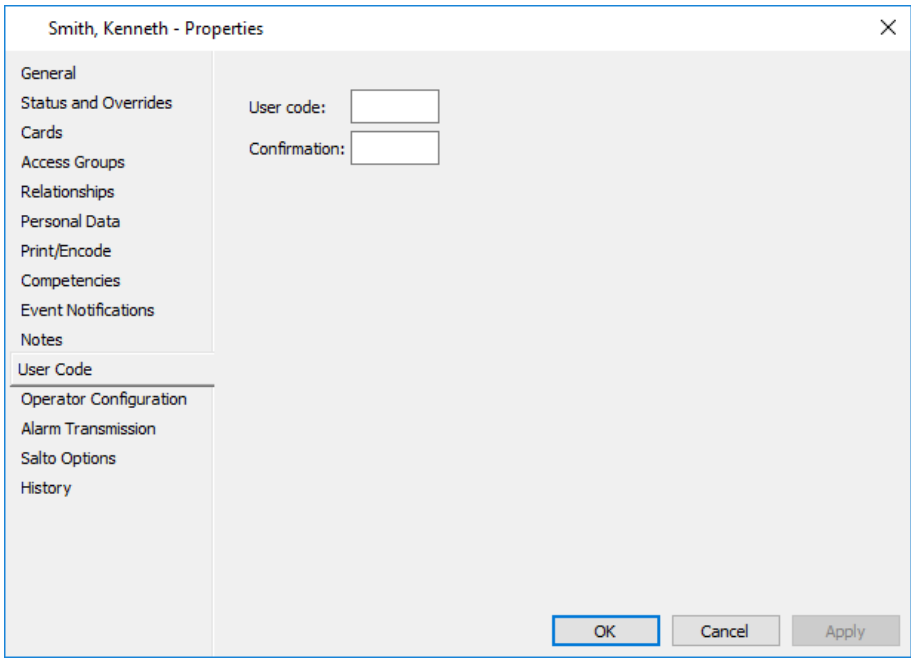
User codes can be configured, in place of PINs, for gaining access at card readers with keypads, (i.e. Gallagher readers and third-party readers that are supported by Command Centre).

### Restrictions

- "Code or Card - PIN" mode does not work for User Code only mode. The Access Zone's mode must be "Code or Card - No PIN" for this feature to work correctly.
- This feature does not support duress functionality.
- The Access Zones Code Only code will not allow access when the reader is configured with "PIN is user code" enabled. Access can only be granted by User Code entry or a valid Card.
- The maximum length User Code accepted is 6 digits.
- Double card overrides are not supported.

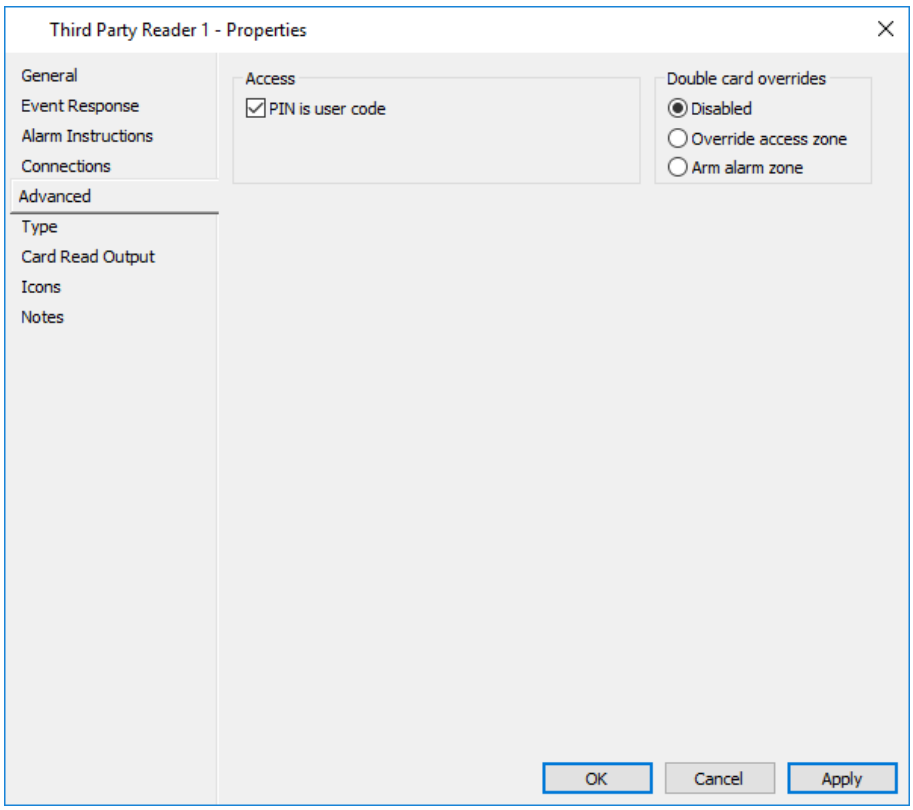
### Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Highlight a Cardholder that requires access via the Reader.
3. **Right-click** and select **Properties**.
4. Click the **User Code** tab.




**Note:** This code will be hidden from all operators, regardless of privilege.

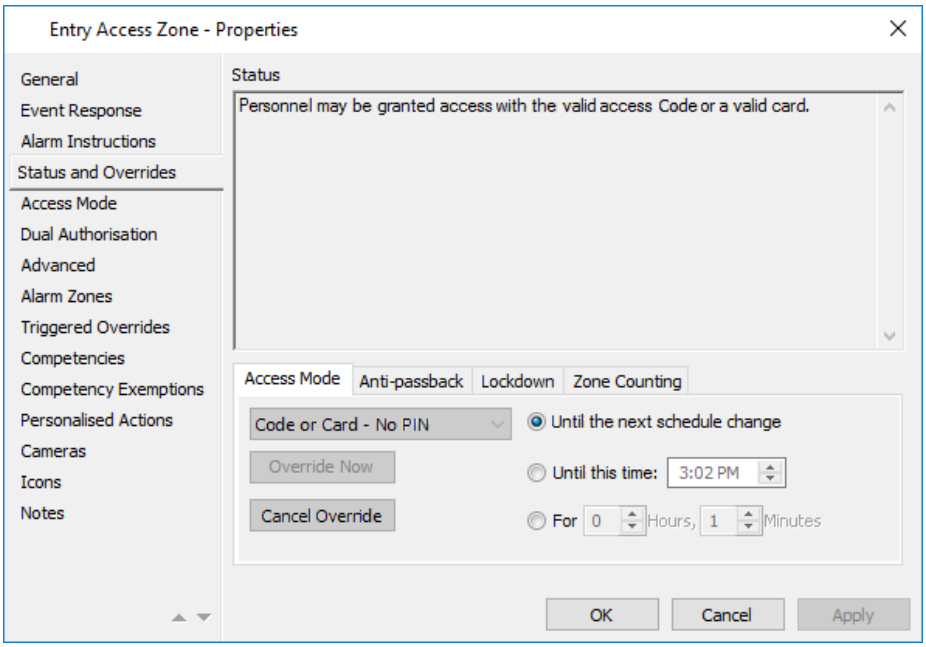
5. Enter a 4-6 digit user code in the **User code** field.
   **Notes:**
   - As you enter the user code, asterisks display in place of each digit.
   - The code must contain at least one non-zero digit, (e.g. 0000 is invalid and an error will be generated).
6. Confirm the user code by re-typing it in the **Confirmation** field.
7. Click the **OK** button.
8. Repeat Steps 2 - 7 for each Cardholder that requires access at the Reader.
   **Note:** You can find out which Cardholders have user codes by running a summary Cardholder Report and selecting the User Code field. While the report will indicate who has a user code, the actual codes will not be disclosed.
9. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
10. **Right click** on the reader and select **Properties**.
11. Click the **Advanced** tab.




12. Check the **PIN is user code** checkbox.
    With **PIN is user code** checked, the user code will be required in place of a PIN for any transactions at the reader which would normally require a PIN. This includes door access and overrides.

    **Note:** Double-card overrides do not work in this mode, therefore leave the Double card overrides as **Disabled**.

13. Click the **OK** button.
14. Set the access mode of the reader's Access Zone to "Code or Card - No PIN". This can be done from either the:
    - **Schedule**. See ***Creating a new Schedule*** (on page 12-2) for further detail.
      The Schedule is then applied to the Access Zone via the **Access Mode** tab of the Access Zone properties.
    - **Access Zone**, as follows:




a) On the **Status and Overrides** tab, select the **Access Mode** tab.
b) Select the "Code or Card - No PIN" mode from the drop-down list.
c) Click the **Override Now** button, and then the **OK** button.

**Result**

User codes have been specified to identify cardholders at a Reader for PIN only access.

When cardholders enter their user code correctly at the Reader, the following Door Access Granted event will be generated in Command Centre:

*"[Cardholder] was granted entry into [Access Zone] through [Door]"*

## Audit Trail of Cardholder changes

### Introduction

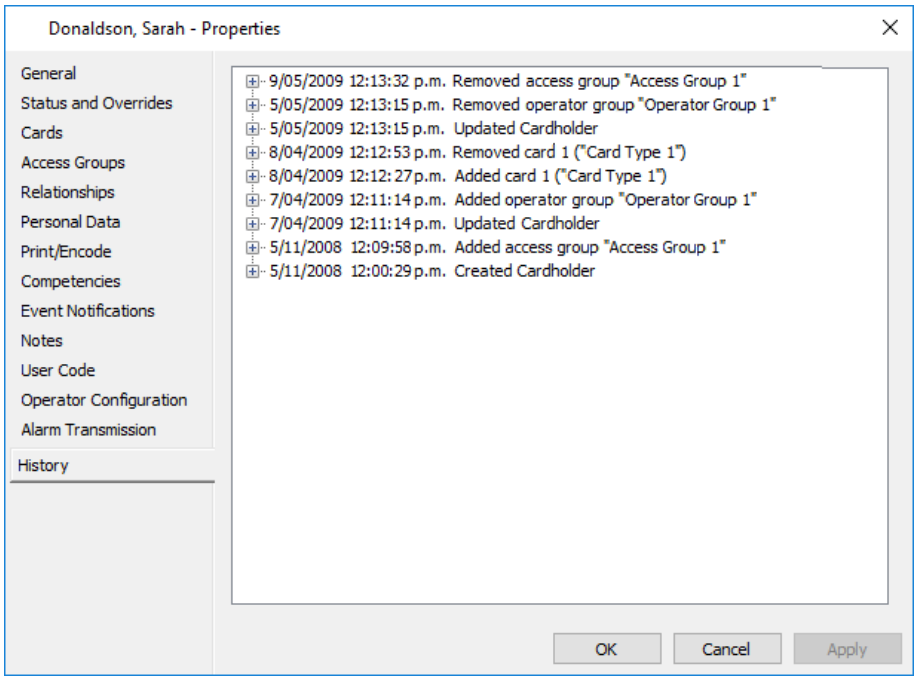
This procedure allows you to view an audit trail of changes made to a cardholder. The following privileges are required:

- "View Cardholders,
- "View Cardholder Notes" (to see changes to notes), and
- "View Operators" (to see changes to operator configuration).

**Note:** This feature was new in version vEL6.01 of Command Centre. Therefore, if your site has upgraded from a pre-vEL6.01 version of Command Centre, cardholders created in earlier versions will show their status of the time when they were being upgraded, (e.g. the cards they had, the Access Groups they were added to). Some audit history details before upgrading will be lost, (e.g. the time a card was added, a card was added to the cardholder and deleted later).

### Procedure

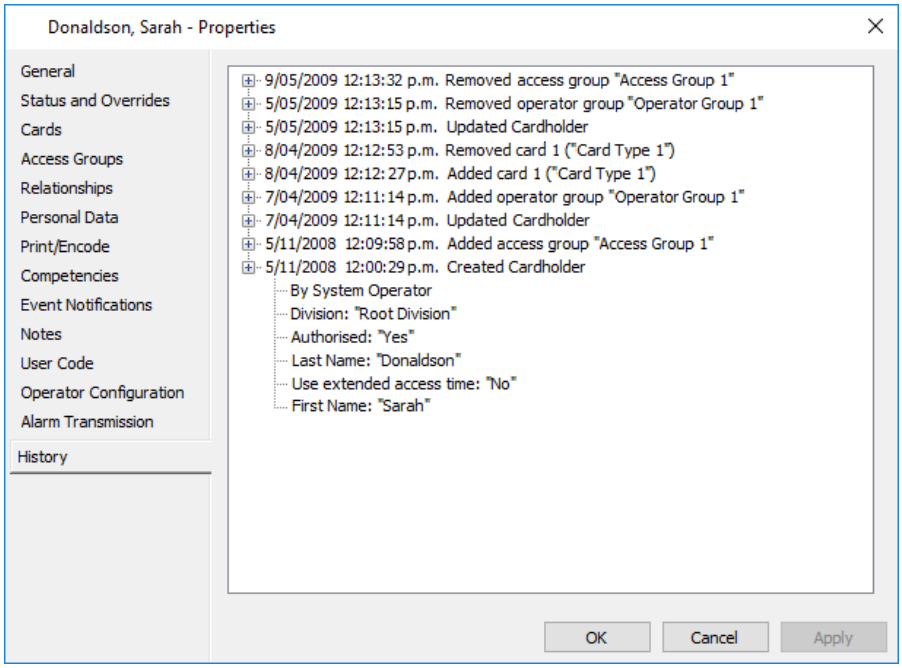
1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the Cardholder you want to view changes for.
3. **Right click** and select **Properties**.
4. Click the **History** tab.




The entries on this page display in tree view, and each entry represents one change made to the cardholder. They are sorted by time, in

descending order, with the latest change at the top. The titles of the entries show when the change was made and what the change was. Extra information is sometimes included in the titles to make a change identified easily, (e.g. when a card was created, the card number and card type are included in the title, as shown in the above screen shot).

5. Click the ⊞ beside one of the entries to expand the list of items below it.




The first item under the entry shows the operator who made the change, and the workstation where the change was made. All the other items that follow show the details of the change.

## Notes

- While the information on this page is "read-only", the text can be copied and pasted into any other application as per common Microsoft Windows functionality. To do this, **right click** anywhere in the grid and select **Copy**. A copy of all the text within the **History** tab (including the lines normally only visible after expanding an entry) will be placed on the clipboard, preceded by the title: *Cardholder "<name>" History*.
- Editing existing Access Groups can produce an "Added" and then "Removed" entry, (e.g. changing a Cardholder Membership date).
- The following activities do not appear in the Cardholder History:
  - Changes to Morpho finger selection
  - Card expiring (on the **Cards** tab)
  - Contact ID changes
  - Salto changes
  - Access Groups expiring
  - Re-enabling of a Competency

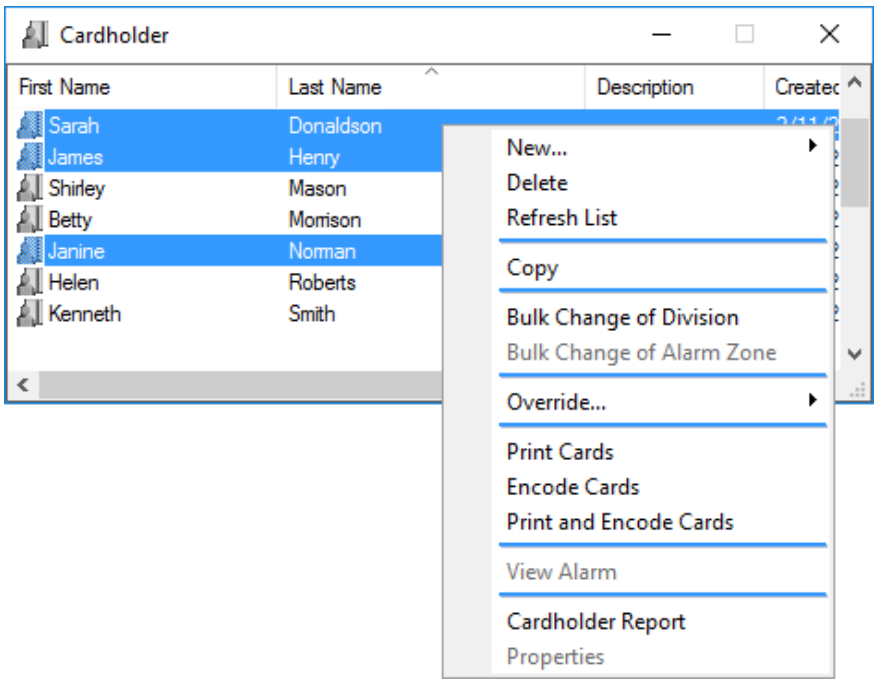
## Running a Cardholder Report from a Cardholder

### Introduction

This procedure allows you to run a Cardholder Report from the Cardholder List Window.

### Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Select the Cardholder(s) you want to run a report on, and **right click** the mouse.




3. Click **Cardholder Report** from the context menu.
   The Cardholder Report Wizard automatically advances to the **Report Generation Progress** page and a Detailed Cardholder Report starts running. The report will include only the selected cardholder(s).
   Once the report has been generated, you can close and discard the report, or use the **Back** button in the report wizard to reconfigure or save the report.

# Reading MIFARE Cards using a MIFARE USB Encoder

## Introduction

When lost, unnamed cards are handed in, this feature allows you to identify the cardholder that has lost their card. The Cardholders data is displayed when the system is prompted by the user and an active card is swiped against either an *ACR1252*, a *SDI010* or *SDI011G Contactless MIFARE Reader and Encoder*.

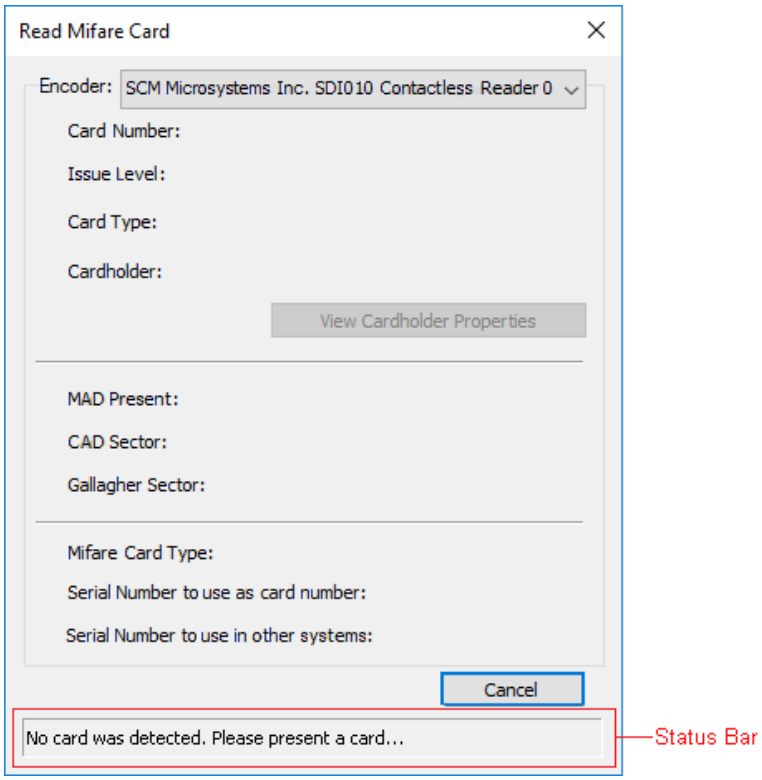
**Notes:**

- This feature is **not** a licensed feature, and only works with the following encoders:
  - *ACS ACR1252 1S CL Reader PICC 0*
  - *SCM Microsystems Inc. SDI010 Contactless Reader 0*
  - *SCM Microsystems Inc. SDI011G Contactless Reader 0*
- Operators require the "View Cardholder" operator privilege to use this feature.

This procedure describes how to read a MIFARE card using an ACS or SCM MIFARE USB Encoder in Gallagher Command Centre.

## Procedure

1. Click **Monitor** from the menu bar, then **Read MIFARE Card**.
   The **Read MIFARE Card** dialog displays.

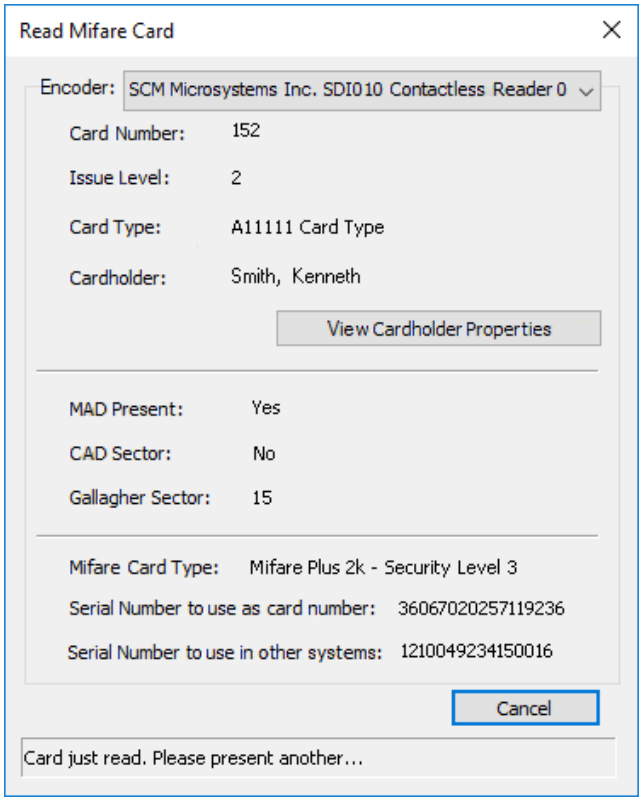


By default, the first available USB encoder is used for reading and populates the **Encoder** field. If there are other USB encoders connected to the workstation they will also appear in the drop-down list.

2. Select the required **Encoder** from the drop-down list.

| If... | then... |
|---|---|
| no USB Encoder is detected | the message *"No USB Encoder was detected"* appears in the Status bar. |
| the workstation is enabled for SmartCard logon | • the 'Read MIFARE Card' feature will be disabled on the workstation,<br>• the **Encoder** field will be empty, and<br>• the message *"Disabled on workstations enabled for Smartcard log-on"* will appear in the Status bar. |

3. Place the card on the encoder.
The details of the card display in the **Read MIFARE Card** dialog if the card contains Gallagher data and the corresponding cardholder can be found in the system.




**Notes:**

- If the Card Type and Cardholder are found in Gallagher Command Centre but the issue level is different, (e.g. a new card was issued to the cardholder with the same card number but different issue level), then the message *"*Issue level differs"* will display to the left of the **Cancel** button.

- If no Gallagher data is found on the card, then the card details will be greyed out and the message *"No Gallagher data was found"* will appear in the Status bar.
- If Gallagher data is found on the card, but the card does not belong to the system, then:
  - the **Card Type** field will show as "Unknown Card Type",
  - the **Cardholder** field will show as "Unknown Cardholder", and
  - the **View Cardholder Properties** button will be disabled.
- Possible **MIFARE Card Types** that could display are:
  MIFARE Classic 1k
  MIFARE Classic 4k
  MIFARE Plus S - Security Level 0
  MIFARE Plus X - Security Level 0
  MIFARE Plus S 2k - Security Level 3
  MIFARE Plus X 2k - Security Level 3
  MIFARE Plus S 4k - Security Level 3
  MIFARE Plus X 4k - Security Level 3
  MIFARE DESFire 2k
  MIFARE DESFire 4k
  MIFARE DESFire 8k
- The **Serial Number to use as card number** field shows the unique Card Serial Number (CSN) of the card in decimal format and reverse byte order. The **Serial number to use in other systems** field shows the unique serial number of the card (UID).
  **Note:** If the card is assigned to a Cardholder, is of a type where re-encoding is prevented, and it has a different CSN from one recorded in the past for that identifier, a 'Potential Duplicate Card' alarm will be generated. If this occurs, we recommend the safest course of action for your site is to issue the Cardholder who is currently assigned a Card with that identifier, a new card.
- If the card is unknown, the **MIFARE Card Type** field may display "Unknown ISO1444-3". Likewise, the message *"The card selected is an unsupported ISO14443-3 card"* may display in the Status bar if the card is detected as one of the known unsupported types.

4. Click the **View Cardholder Properties** button.
   The properties of the Cardholder that the card belongs to opens.
5. Present the next card if there are more to read.

**Notes**

- The encoder beeps the first time a card is placed on it and the **Read MIFARE Card** utility in Command Centre is used, and then goes quiet.
- The encoder beeps when a card is placed on it, before Command Centre is opened and the **Read MIFARE Card** utility is used.

# Disabling the System Operator

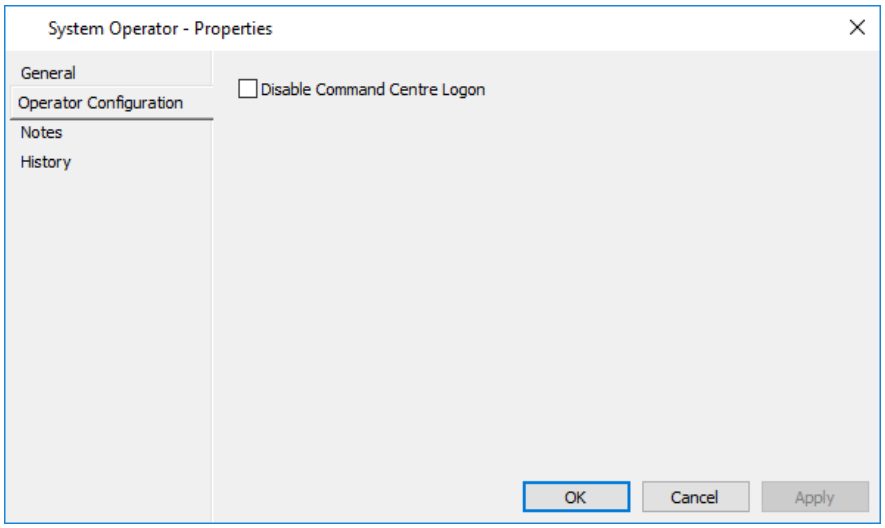
## Introduction

The System Operator account is initially used to set up Command Centre. Once separate operators have been created, the System Operator is not entirely necessary and should be disabled by another operator for security purposes.

Operators require either the "View/Edit Operators" privilege to perform this procedure.

## Procedure

1. Click **Monitor** from the menu bar, then **Find..**.
   The **Find** Tool opens.
2. Click within the **Look in** field and select the "System Operator" option.
3. Click the **Start Search** button.
   The System Operator displays in the Search window.
4. **Right click** on the System Operator and select **Properties**.
   By default the **General** tab displays.
5. Click the **Operator Configuration** tab.




6. Tick the **Disable Command Centre Logon** checkbox.
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 System Operator account is disabled.
**Note:** If an operator attempts to logon using the System Operator name and password, the message "Invalid logon name or password" will display on the Logon screen.

# Chapter 33: Personal Data Fields

Personal Data is information that is stored for an individual cardholder. This information can include items such as car license plate, date of birth, signature, photographs, company division, etc.

Personal Data Fields (PDFs) are created as separate entities and are attached to Access Groups. Cardholders inherit the Personal Data Fields from the Access Group(s) they belong to.

When viewing a cardholder's record, it will contain all the Personal Data Fields specified in the Access Group(s) the Cardholder belongs to.

There are nine different types of Personal Data Fields, as follows:

- Text (an operator may enter any free hand text)
- Text - List (if "Restrict to List" is enabled, an operator may select from a list of pre-defined entries or leave it blank. If "Restrict to List" is not enabled, free text entry is allowed)
- Numeric
- Date
- Image (an operator may capture an image, e.g. signatures, cardholder photographs, etc.)
- Address
- Phone
- Mobile
- Email

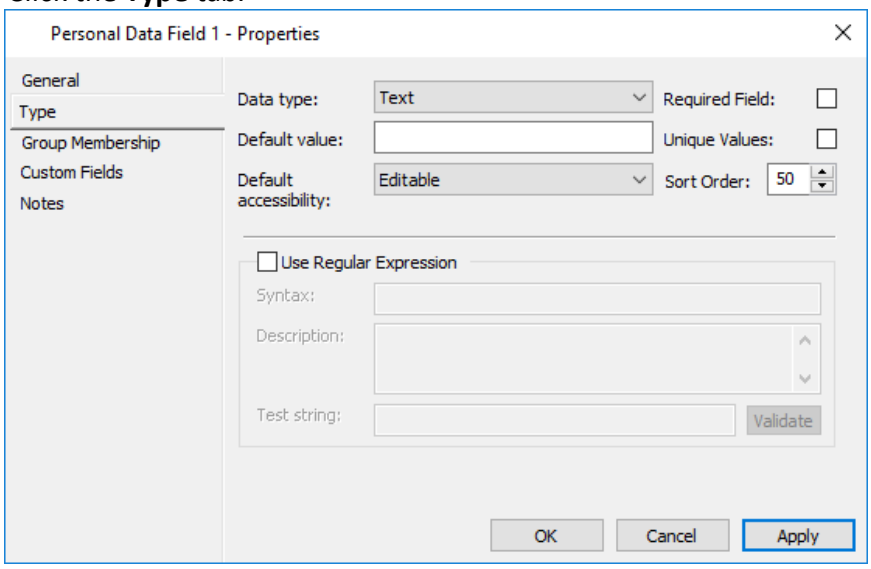
## Creating a new Personal Data Field

### Introduction

This procedure details how to create a Personal Data Field.

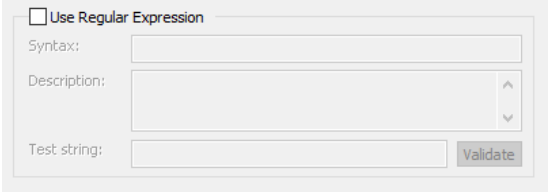
### Procedure

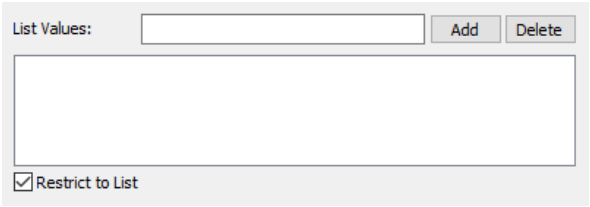
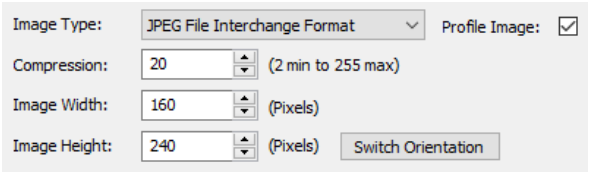
1. Click **Configure** from the menu bar, then **Personal Data Fields**.
   The **Personal Data Field** List Window opens (in grid view).
2. **Right click** and select **New...Personal Data Field**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
4. Click the **Type** tab.

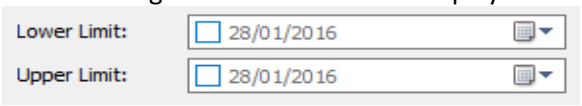



This tab determines the type of data to be entered against the PDF.
By default, "Text" populates the **Data Type** field.

5. Click within the **Data type** field and select the appropriate type from the drop-down list.
   **Note:** With the exception of the **Numeric** type, each type has additional information that must be entered, some of which is common to all types, while other information is specific to individual types, as follows:

| If you select... | the... |
|---|---|
| Text, or any contact PDF types, (i.e. Address, Phone, Email or Mobile) | following additional fields display:<br><br><br>The **Use Regular Expression** feature is for text and contact type PDF data validation to allow the enforcement of text values. It allows you to write a regular expression that will force PDF entered values to obey the rules of the |

| If you select... | the... |
|---|---|
| | expression. If values are entered that break the expression, then an error message displays detailing the expression requirements. See ***Regular Expression Settings*** (on page 33-6) for further detail on entering information into this section.<br>**Note:** If the **Data type** is either 'Mobile' or 'Email', there is an additional **Default Notifications** checkbox which is used by the Visitor Management application. If you want hosts to be able to send invitations to visitors this checkbox must be ticked. When checked, it also determines whether or not the **Notifications** checkbox is checked when an Access Group with that PDF is added to a Cardholder, or the Cardholder added to the Access Group. |
| Text - List | following additional fields display:<br><br>These fields allow you to define a set of entries that may be selected from, when entering data against a cardholder. To do this, enter a value in the 'List Values' field, then click the **Add** button.<br>When the 'Restrict to List' option is enabled the **Default value** must be one of the list values or blank. If 'Restrict to List' is not enabled, free text entries can be entered against a cardholder. |
| Image | following additional fields display:<br><br>These fields allow you to specify details about the image that is saved to the database.<br>The **Image Type** can be JPEG, Bitmap or PNG.<br>Check the **Profile Image** checkbox if you want this Image PDF (containing the cardholder photo) to be shown on the Mobile Client Details screen.<br>**Note:** Only one Image PDF will be used for each cardholder. If a cardholder has more than one Image PDF captured and they all have the **Profile Image** checkbox enabled, the image with the lowest sort order will display.<br>Refer to ***Capturing an Image*** (on page 33-10) for the procedure on how to capture images for an Image Personal Data Field. |

| If you select... | the... |
|---|---|
| Date | **Default value** field changes to a Date control:<br><br><br>Leave the checkbox unchecked if you do not want a default.<br>The following additional fields also display:<br><br><br>A lower and/or upper date range may be specified to control the dates entered into the PDF.<br>**Note:** The dates will display on-screen and in reports in the date format specified in the workstation settings. |

6. Check the following boxes as necessary:

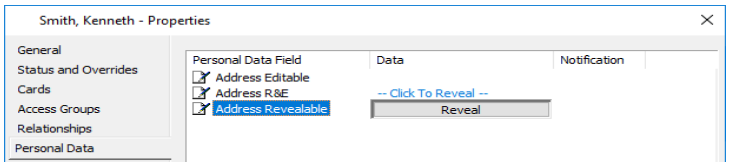
| If... | is checked, then... |
|---|---|
| Required Field: | Data for the Personal Data Field will be mandatory when editing a cardholder. |
| Unique Values: | an operator will be prevented from entering the same value across multiple cardholders (although the system will allow a "no data" value to be entered multiple times). The **Default Value** field is disabled. |

**Note:** "Unique Values" is disabled for **Text - List** type, **Image** type and **Date** type.

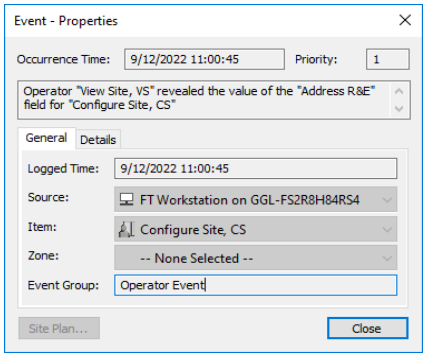
7. Click within the **Default accessibility** field and select the appropriate privilege (i.e. type of access), from the drop-down list.
This determines the base operator rights for this Personal Data Field.

| If you select... | then... |
|---|---|
| Edit (default) | operators with the "View Cardholders" privilege in a division can view the Personal Data Field value but not create or edit it.<br>Operators with the "Edit Cardholder Personal Data" privilege in a division can create or edit the Personal Data Field values of a cardholder in that division. |
| Hidden | operators who do not have the "Advanced User" privilege will not see the cardholder information recorded for this Personal Data Field for cardholders in this group's Divisions, or even see that it exists. |
| Revealable | operators with the "View Cardholders" privilege in a division can view the Personal Data Field value (from the **Personal Data** tab of the Cardholders properties), by clicking on the **Reveal** button.<br>Operators with the "Edit Cardholder Personal Data" privilege can view the Personal Data Field value by clicking on the **Reveal** button, but not create or edit it. |
| View Only | operators with the "View Cardholders" privilege in a division can view the Personal Data Field value.<br>Operators with the "Edit Cardholder Personal Data" privilege can view the Personal Data Field value, but not create or edit it. |
| Revealable and Editable | operators with the "View Cardholders" privilege in a division can view the Personal Data Field value (from the **Personal Data** tab of the Cardholders properties), by clicking on the **Reveal** button, but not create or edit it. |

| If you select... | then... |
|---|---|
| | Operators with the "Edit Cardholder Personal Data" privilege in a division by clicking on the **Reveal** button can create or edit the Personal Data Field value of a cardholder in that division.<br>**Notes:**<br>• Revealable and Editable PDFs are not available in REST or Mobile Client.<br>• Personal Data Fields with either "Revealable" or "Revealable and Editable" accessibility display a **Reveal** button on the Personal Data tab of the Cardholder properties.<br>• Revealable or revealable/editable PDFs that are included will not log the new access event when a report is run, a search via REST is made, or there has been an operator event. |



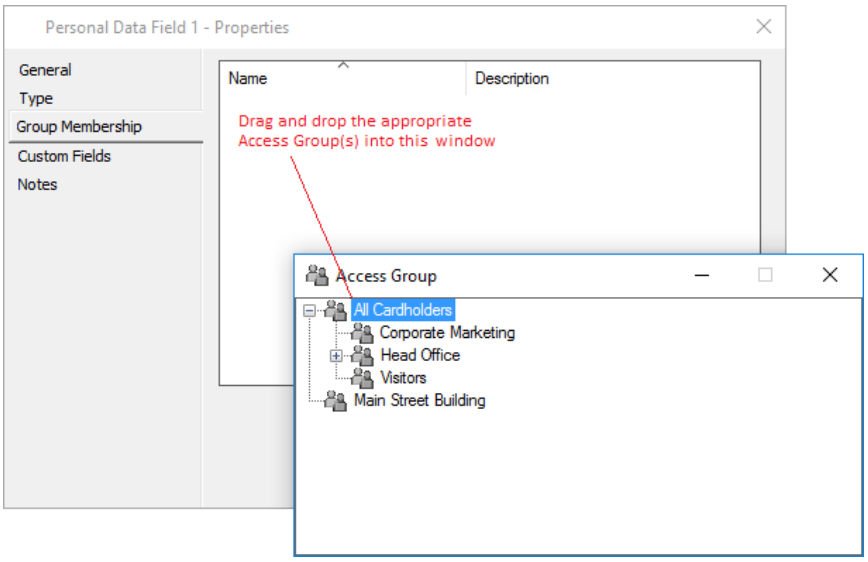

Every time a **Reveal** button is pressed, there is an Operator Event in the form of *Operator "View Site, VS" revealed the value of the "Address R&E" field for "Configure Site, CS"*, from the "Source" of the Workstation that the operator was logged into.




**Notes:**

- The **Default Notifications** checkbox will be revealed when the **Reveal** button is pressed, (i.e. it is a blank space until that happens).
- The system operator does not have the reveal option visible, as they can see everything anyway.
- A field which is not editable will have its title rendered in grey.

8. Alter the **Sort Order** field if necessary. This controls the order in which PDF records are shown in the cardholder property page.
   **Note:** The lower the number, the higher up the list it will display, (e.g. 1 will display the PDF at the top of the screen, 100 will put it at the bottom, and if all are set to the same number they will display in alphabetical order).
9. Click the **Group Membership** tab.
10. Click **Manage** from the menu bar, then **Access Groups**.
    The **Access Group** List Window opens.
    Select those Access Group(s) appropriate for this Personal Data Field.
    Drag and drop them into the **Group Membership** tab.




11. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Personal Data Field.
    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 Personal Data Field.
    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 Personal Data Field is created.
**Note:** Once a Personal Data Field has been created and data has been recorded against it, the ability to alter its Data Type will not be available.
For recording cardholders personal data against PDFs, see ***Editing a Cardholders PDF data*** (on page 32-20) for the procedure.

## Hints

*Editing and Deleting Personal Data Fields*
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Personal Data Fields.
**Note:** Deletion of a Personal Data Field is only allowed if it is not currently assigned to be used anywhere in the system, except if it is saved against a report.

*Copy and Paste*

An alternative to the drag and drop method is to use the copy and paste method.

*Group Membership details*

The Access Group(s) you added to this Personal Data Field (in Step 11) will now have this PDF displayed in the **Personal Data** tab of their Properties screen.

## Regular Expression Settings

### Introduction

Regular expressions can be used to define what data is valid and may be entered in a Personal Data Field. For example, a regular expression can be used to ensure Employee IDs always contain two letters followed by up to six digits.

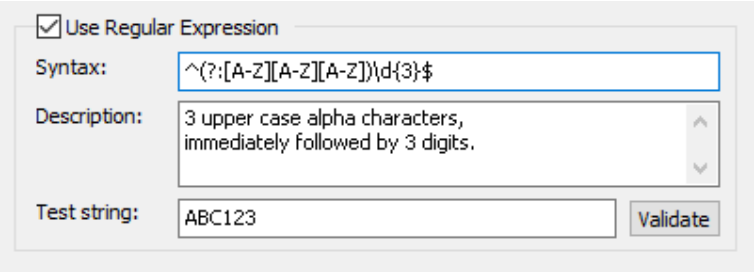
### Procedure

Checking the **Use Regular Expression** checkbox (on the **Type** tab of Personal Data Field properties), enables all the fields in that section.

Configure as appropriate:
**Note:** Refer to ***Common Regular Expressions*** (on page 33-8) for a list of example regular expressions.

| Field | Description |
|---|---|
| Syntax | This field allows a regular expression syntax, of up to 2048 characters, which is used to validate cardholder PDF data. It allows multiple lines and carriage returns. |
| Description | This field allows up to 2048 characters to describe regular expression syntax. It allows multiple lines and carriage returns.<br>**Note:** This is the message which will be displayed to an operator if the value entered cannot be saved because it doesn't meet the regular expression validation. |
| Test string | This field allows a sample string, of up to 2048 characters, which helps technicians to write/test regular expression syntax.<br>**Note:** This field is not saved into the Command Centre database. |
| **Validate** button | This button validates the test string against the regular expression syntax when clicked. The returned messages could be one of the following:<br>• *"The Syntax field cannot be empty.",*<br>• *"The Test String field cannot be empty.",*<br>• *"Validation succeeded.",* or<br>• *"Validation failed as the value does not match the regular expression."* |

**Note:** "Mobile" and "Email" type PDFs have an additional Default Notifications checkbox on this tab. If checked, this provides a default value for cardholder contacts.




When the **Use Regular Expression** checkbox is checked:

- The **Syntax** field must not be empty.
- If the **Default Value** field is not empty, its value must meet the regular expression syntax.
- For an existing PDF, if the **Syntax** field is modified and this PDF is being used by one or more Access Groups, the system will validate all related cardholder PDF data against the new regular expression syntax. If validation fails, an error message box pops up saying: *"Cardholder has one or more invalid PDF data values."*
- The regular expression cannot be saved until all existing data is validated against this expression.

## Common Regular Expressions

The following table provides a number of regular expression examples that have been tested and can be used to validate text-type PDF data.

| Category | Regular Expression | Description |
|---|---|---|
| Email Address | ^[A-Za-z0-9._%+-]+@(?:[A-Za-z0-9-]+\.)+[A-Za-z]{2,4}$ | Case insensitive, must include an @ symbol and optional email characters such as dots and dashes with maximum 4 characters in the generic top-level domain. |
| Phone Number (example) | ^0[1-9]\s\d{3,4}\s\d{4}$ | Requires an STD prefix 01.09 followed by a compulsory space then seven or eight digits with a compulsory space separating the last four digits,<br><br>(e.g. 07 3482 7520 or 07 386 4902) |
| Phone Number, international format (example) | ^[+]\d{7,18}$ | Forces a '+' character at the start of the string followed by 7 to 18 integers (no spaces). |
| License Number/ID (example) | ^(?:CNS\|BNE\|TNS)\d{4,6}(?:-(:?[1-9]\|1[0-5]))?$ | Three upper case letters CNS, BNE, or TNS, immediately followed by 4-6 integers, optionally followed by a dash and an integer of 1-15, (e.g. CNS15425-13 or BNE928362). |
| Numeric ID (example) | ^\d{4,8}$ | Only integers but must consist of a minimum of 4 digits and a maximum of 8. |
| Car Registration (example) | ^[A-Z]{3}\d{3}$ | Three upper case letters immediately followed by three integers, (e.g. KMO512). |
| Single limited numeric value (example) | ^[0-4]$ | Numeric value 0, 1, 2, 3 or 4 |
| Alpha characters only | ^[A-Za-z]+$ | Any uppercase or lowercase characters only, no spaces. |

| Category | Regular Expression | | Description |
|---|---|---|---|
| Upper case | ^[A-Z]+$ | (continuous string) | All upper case characters. |
| | ^(?:[A-Z]\s?)+$ | (single spaces allowed, e.g. ASD BD GHJ) | |
| Lower case | ^[a-z]+$ | (continuous string) | All lower case characters. |
| | ^(?:[A-Z]\s?)+$ | (single spaces allowed, e.g.rgag dhgdh afg) | |
| Proper case | ^(?:[A-Z]\w*\s?)+$ | | First Letter Of Each Word Must Be Upper Case. |
| Boolean | ^0\|1$ | | A simple on/off by using only the values 0 or 1. |

## Capturing an Image

### Introduction

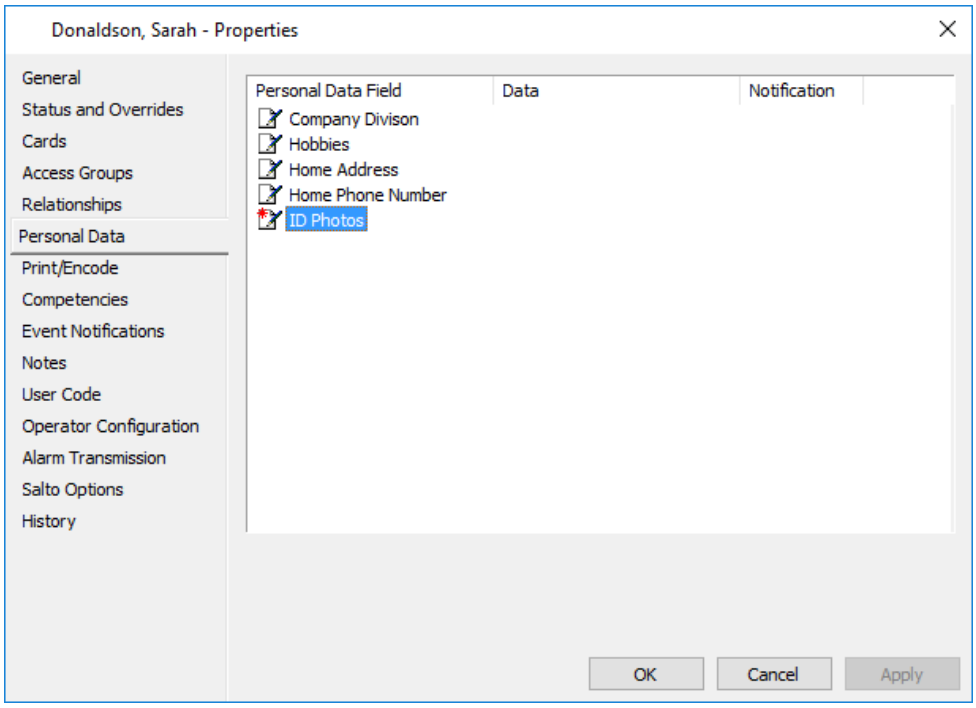
This procedure enables an operator to capture an image, (e.g. corporate logos, cardholder photographs, etc.), for an "Image" Personal Data Field (PDF) of a cardholder.

**Notes:**

- Cardholder photograph images can be used for Photo ID cards. See Photo ID for more detail.
- Sites wanting to capture images for PDFs on a Microsoft Windows Server 2008 operating system need to install the Desktop Experience feature, as follows:
  1. From the **Start** menu, click **Control Panel** > **Administrative Tools** > **Server Manager**.
  2. In the **Details** pane, locate the Features Summary area, and then click **Add Features**.
  3. In the 'Add Features' wizard, check the **Desktop Experience** checkbox, then click **Next** and then click **Install**.
  4. Once the Desktop experience feature is installed, click **Close** to exit the 'Add Features' wizard, and then click **Yes** to restart the computer.

### Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. **Right click** on the required cardholder, and select **Properties**.
3. Click the **Personal Data** tab.

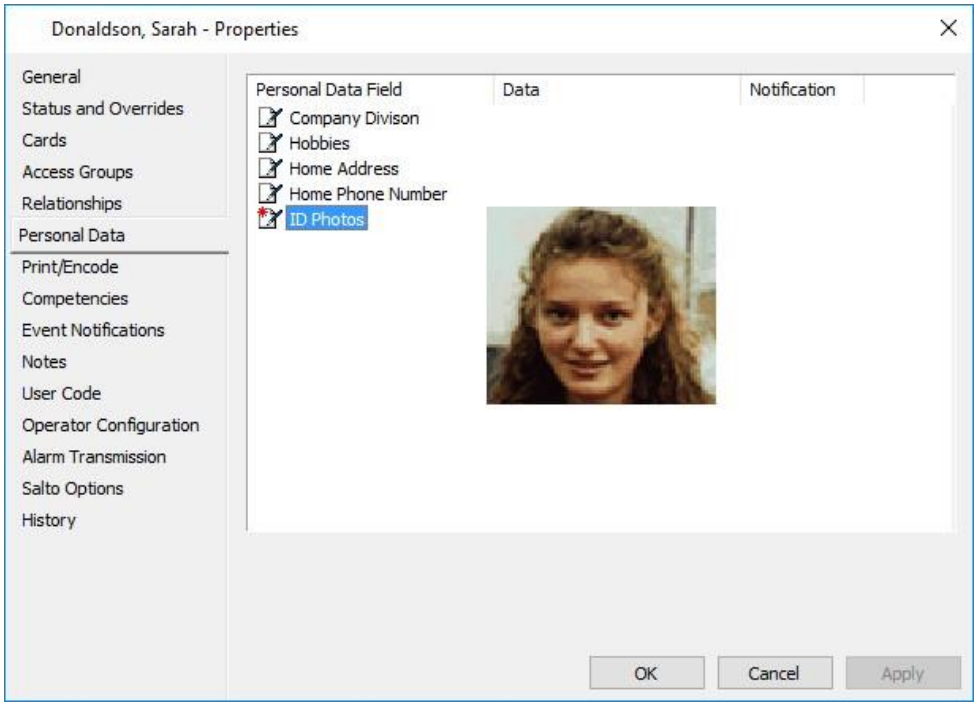



4. **Right click** over the data section of the "Image" PDF, then click **Capture Image**.
   The **Capture Image** window displays. It will be blank if it is the first time you have captured or loaded an image on this workstation, otherwise it will default to the last method of capturing you used.
5. 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.
6. Click the **Capture...** button.
7. 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.<br>• Path your way to the location of the image you require, and click the **Open** button. The image displays in the **Capture Image** window.<br>**Note:**<br><br>To adjust the contrast and/or brightness of a saved image, right click and move the indicator as necessary. |

| If you want to... | then... |
|---|---|
| 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.<br><br>**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.) |

8. Reposition the cropping frame.
9. Click the **OK** button.
   The **Capture Image** window closes.
   The captured image now displays in the Personal Data tab and the **Apply** button is enabled.




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**

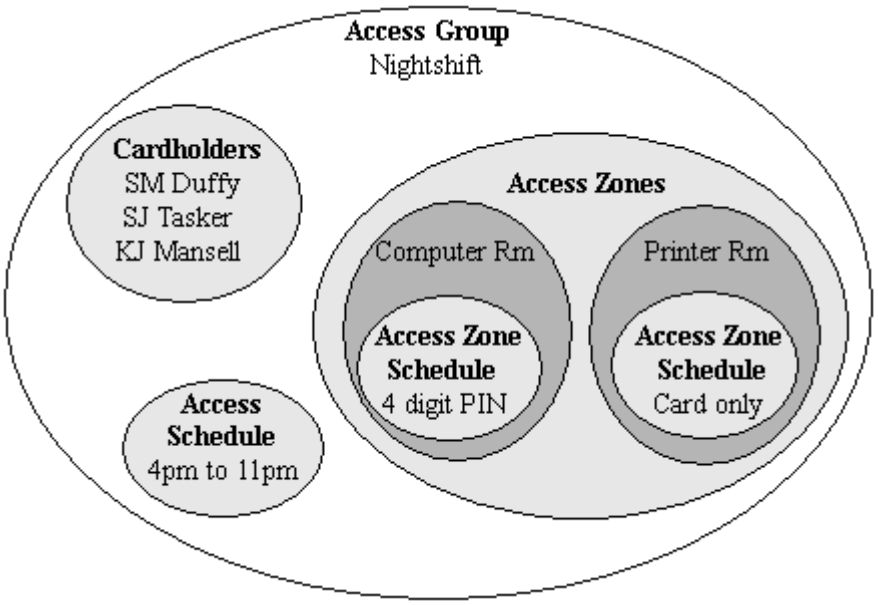
The image is saved to the cardholder.

# Chapter 34: Access Groups

## Understanding Access Groups

An Access Group is a group of cardholders.
An Access Group also defines the access (and other properties) that these cardholders have.
You can define the 'Name' and 'Privileges' for an Access Group, and assign the following properties to an Access Group:

- Members (who - which cardholders belong)
- Access Zones (where the members have access to go)
  **Note:** There is a limit of 255 Alarm Zones/Access Zones per Access Group per Controller. If this limit is exceeded, an alarm will be generated (in the Alarm Viewer window), and the first 255 zones only will be sent to the Controller.
- Access Schedule (when the members have access)



## Access Groups 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

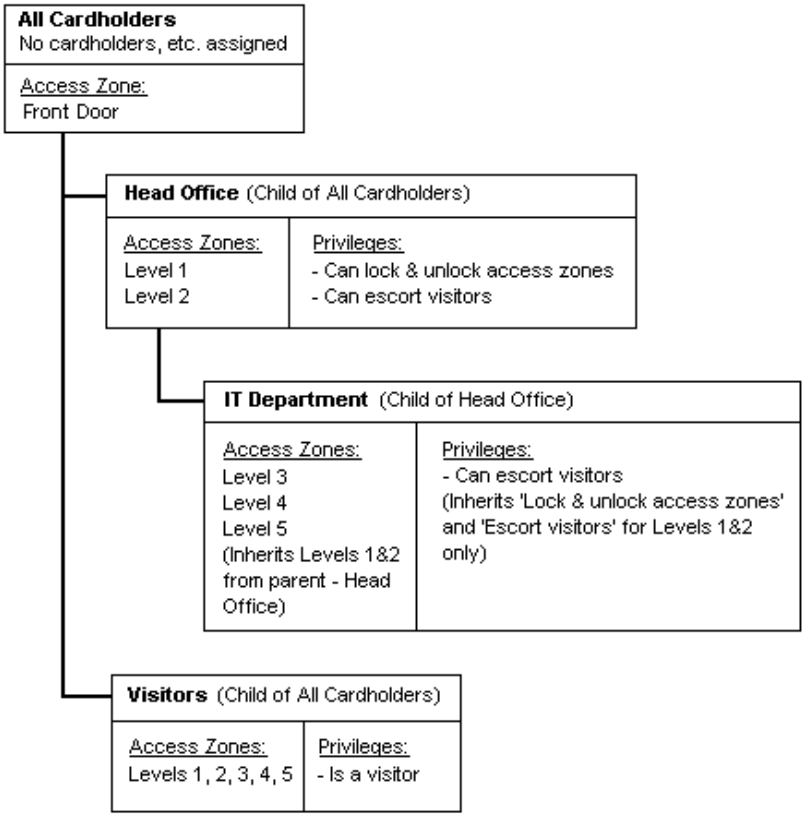
The procedure for setting up Lineage is the same for both Access Groups and Divisions. However, to some degree, lineage works in opposite ways for these two areas. This topic explains how lineage works for Access Groups. See Divisions and Lineage for an explanation of how it works for Divisions.

### Inheritance of Access Group Privileges

If you belong to an Access Group, you automatically have the privileges of its parents in the hierarchy.

A cardholder may need to belong to more than one Access Group to obtain their full access requirements, (i.e. access zones and schedules). There are also privileges assigned to Access Groups, (e.g. to escort visitors). These privileges relate to the access zones and schedules defined for that Access Group.

Child Access Groups inherit both the access requirements, (i.e. access zones and schedules) and Access Group privileges, (e.g. to escort visitors) from their parent(s). The way this works is illustrated in the following example.




In this example, cardholders in the 'Head Office' Access Group can lock and unlock access zones, as well as escort a visitor through Levels 1 & 2. They can also access the Front Door as they inherit the access rights of their immediate parent, (i.e. 'All Cardholders').
A visitor wishing to go through Levels 3, 4 & 5 however will need to be escorted by a cardholder from the 'IT Department' Access Group.

As part of the configuration of an Access Group you can configure Lineage functionality (via the **Lineage** tab). See ***Setting up Access Groups*** (on page 34-4) for the procedure.

## Setting up Access Groups

### Introduction

This procedure is split into two parts, as follows:

- Creating an Access Group,
  (i.e. providing the minimum information required to create a new Access Group)
- Configuring an Access Group,
  (i.e. linking the various components to it - Divisions, Cardholders, Schedules, Access Zones and Personal Data Fields are the components of an Access Group).

You can create a new Access Group, then configure it at a later stage, once you have set up the necessary components for it.

### Procedure

***Create the Access Group***

1. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).
2. **Right click** and select **New...Access Group**.
   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 Access Group is created.

   The rest of this procedure allows you to fully configure the Access Group.

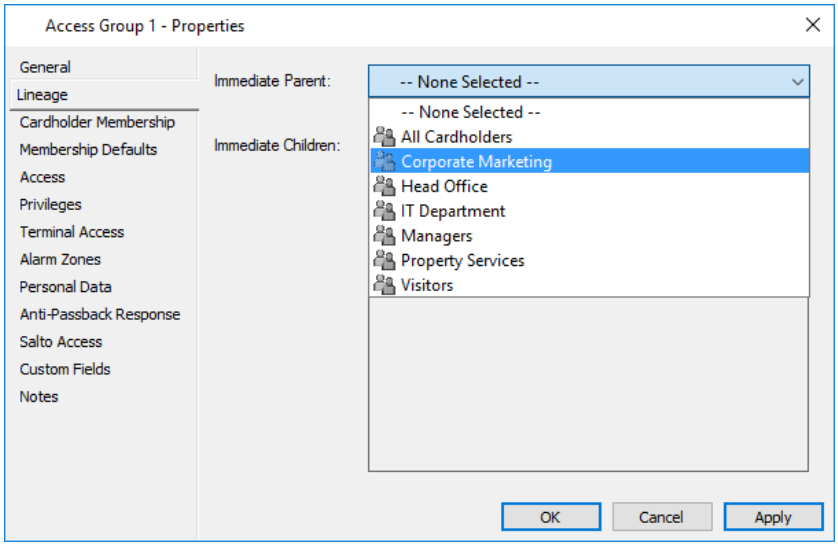
***Configure the Access Group***

5. Ensure the following information has already been set up:
   *Divisions*
   Refer to ***Setting up System Division*** (on page 9-3).
   *Cardholders*
   Refer to ***Add New Cardholder*** (on page 32-2).
   *Schedules*
   Access Schedules = relating to cardholders
   Access Zone Schedules = relating to how the doors within the zone behave
   Refer to ***Schedules*** (on page 12-1).
   *Access zones*
   Includes a linked Access Zone Schedule
   Refer to ***Adding a new Access Zone*** (on page 10-3).

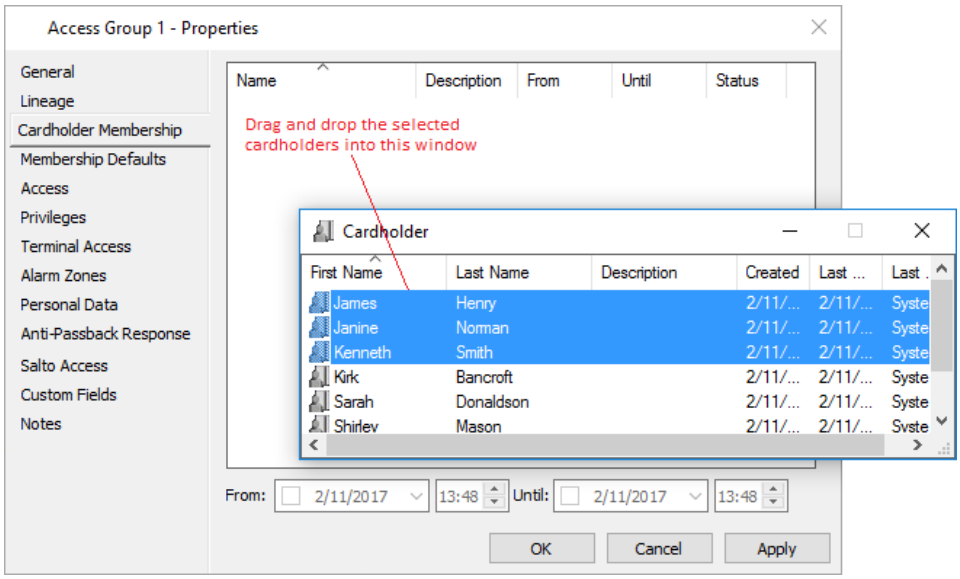
*Personal Data Fields*
Refer to ***Creating a new Personal Data Field*** (on page 33-2).

*Notifications*
Refer to ***Creating a Notification Filter*** (on page 35-4).

6. Click the **Lineage** tab.



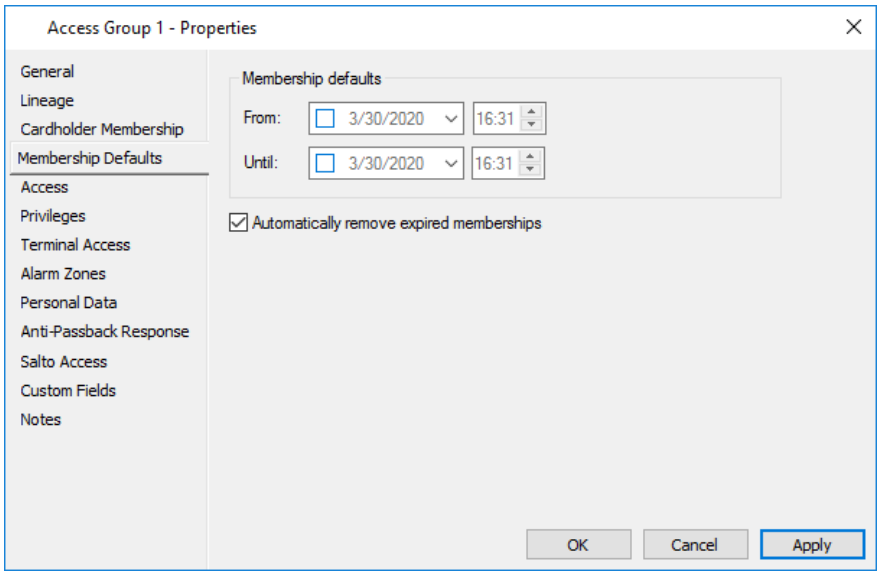

7. If this Access Group is part of a hierarchy, select the "Immediate Parent" access group from the drop-down list.
   All privileges assigned to the parent will be inherited by this Access Group.
8. Click the **Cardholder Membership** tab.
9. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
10. Select those Cardholders to belong to the new Access Group.
    Drag and drop them into the **Cardholder Membership** tab.




11. Close the **Cardholder** List Window.
12. Cardholders that have no 'From' and 'Until' dates beside their names are

permanent members of the Access Group.
If you want to make any Cardholders temporary members, (i.e. give them access for a limited period of time), see ***Granting Temporary Access by Access Group*** (on page 34-18) for the procedure.

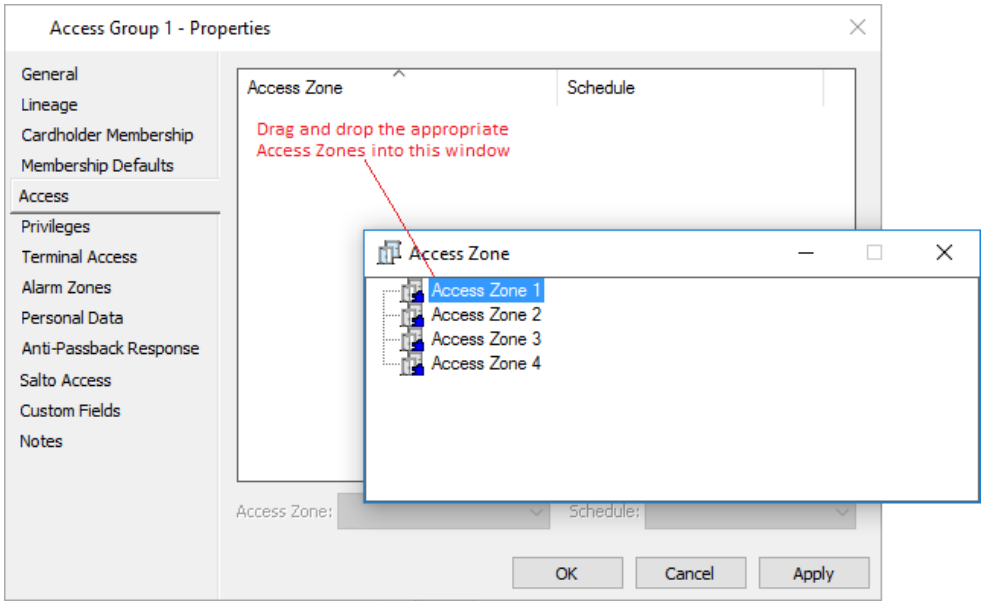
13. Click the **Membership Defaults** tab.




This screen allows a membership period to be set up for the Access Group. By default, the start and end dates are set to none, therefore membership is permanent. See ***Granting Temporary Access by Access Group*** (on page 34-18) for further detail.

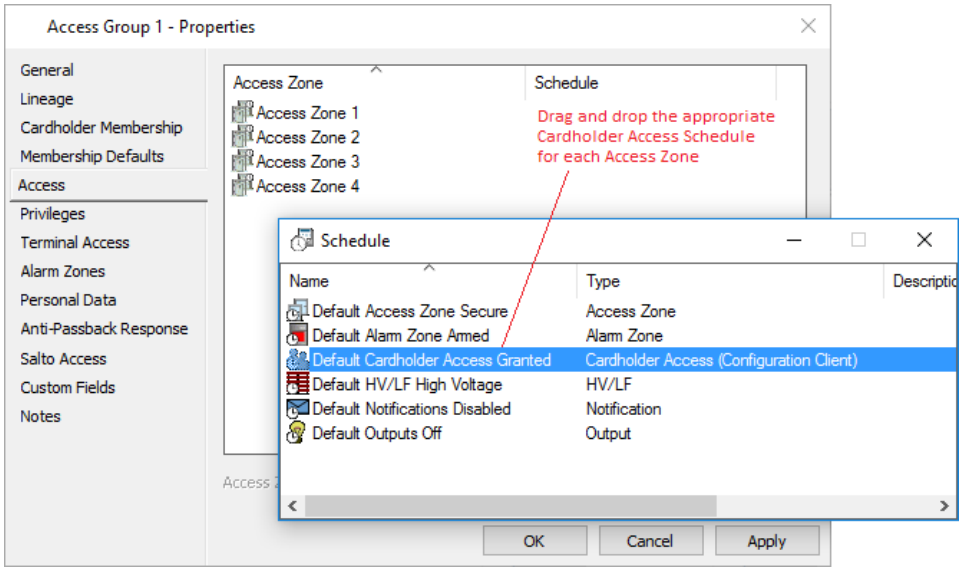
14. Click the **Access** tab.

15. Click **Configure** from the menu bar, then **Access Zones**.
The **Access Zone** List Window opens.
Select those zones appropriate for this Access Group.
Drag and drop them into the **Access** tab window.

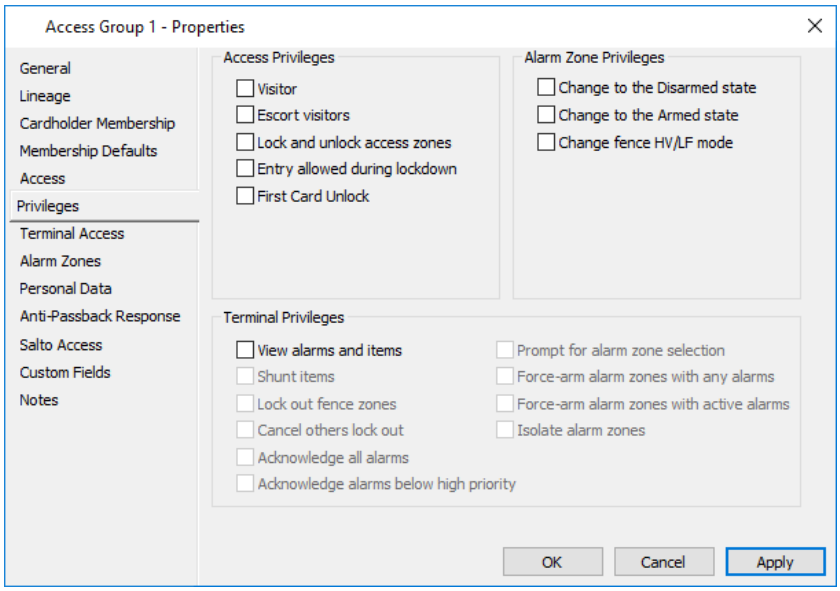


**Note:** There is a limit of 255 Alarm Zones/Access Zones per Access Group per Controller. If this limit is exceeded, an alarm will be generated (in the Alarm Viewer window), and the first 255 zones only will be sent to the Controller.

16. Close the **Access Zone** List Window.
17. Click **Configure** from the menu bar, then **Schedules**.
    The **Schedule** List Window opens.
18. Select those Access Schedules appropriate for this Access Group.
    Drag and drop them into the **Access** tab window.




19. Close the **Schedule** List Window.
20. Click the **Privileges** tab.




Cardholder Privileges are configured in Access Groups.
When you add Cardholders to an Access Group they automatically inherit the privileges as configured for that Access Group. (For a more detailed explanation see ***Inheritance of Access Group Privileges*** on page 34-2.)

21. Select the appropriate **Access Privileges** as required for the Access Group.

| Access Privilege | Enables members to... |
|---|---|
| Visitor | be escorted through selected Access Zones by some-one with 'Escort' privileges for the same Access Zones. |
| Escort visitors | escort visitors to the Access Zones (according to the schedules) assigned to the Access Group. |
| Lock and unlock access zones | change the state of an Access Zone that the Access Group gives access to, from a card reader. This is known as a 'local override'. For further details refer to ***Configuring Local Overrides at Card Readers*** (on page 45-14). |
| Entry allowed during lockdown | enter Access Zones contained in the Access Group when those Access Zones are in lockdown mode, provided they meet the access criteria required during lockdown. When a site is placed in lockdown mode, certain people, (e.g. emergency services) will still require entry. For further details refer to ***Performing a Lockdown Override*** (on page 10-11). |
| First Card Unlock | unlock an Access Zone from SECURE state to FREE state, once access is granted. |

**Note:** When a site is licensed for Aperio Doors, there will be two additional access privileges, as follows:

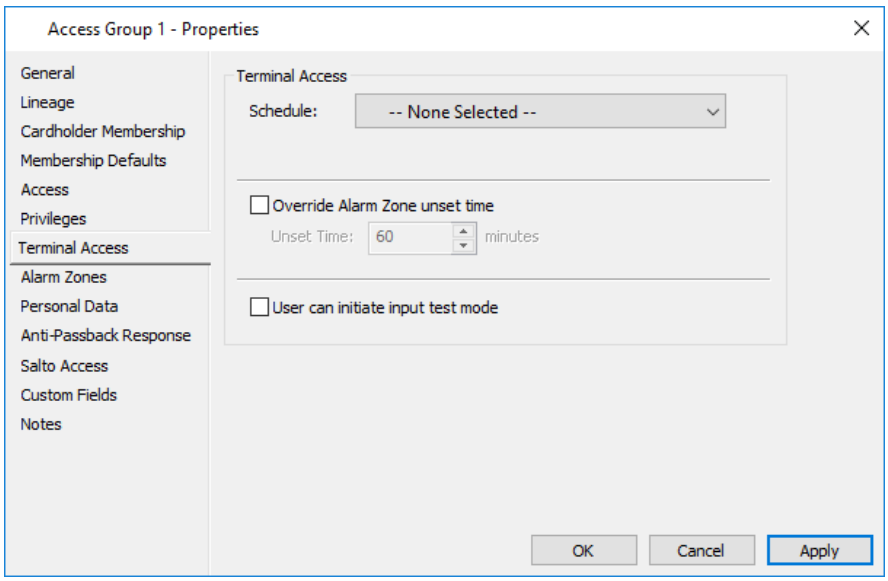
| Access Privilege | Enables members to… |
|---|---|
| Aperio Privacy Override | unlock doors even when in Privacy Mode. Default = unticked.<br>**Notes:**<br>• Privacy Mode is activated by a button on certain Aperio locks. This feature needs to be enabled in Aperio Programming Application Protocol (PAP) in order to take effect.<br>• An Aperio door that is closed, locked, and in Privacy Mode displays a red and yellow padlock icon in the **Hardware** window of Configuration Client. |
| Aperio Offline Access | Cardholders in an Access Group with this privilege enabled will have their card details held at the Aperio door/lock, hence enabling the lock to open for these cardholders without wireless connectivity. |

22. Select the **Alarm Zone Privileges** required for this Access Group.

| Alarm Zone Privilege | Enables members to... |
|---|---|
| Change to the Disarmed state | disarm Alarm Zones associated with any Access Zone associated with the Access Group. |
| Change to the Armed state | arm Alarm Zones associated with any Access Zone associated with the Access Group |
| Change fence HV/LF mode | change the HV/LF mode of an Alarm Zone associated with any Access Zone associated with the Access Group. |

**Note:** The **Terminal Privileges** section of this tab relates only to HBUS Terminals or HBUS Alarms Only Terminals. Therefore, these privileges should only be selected if your site is using one of these terminals and this Access Group will be using them.
Refer to ***Configuring Access Group Privileges for Terminal Access*** (on page 34-13) for further detail.

23. Click the **Terminal Access** tab.

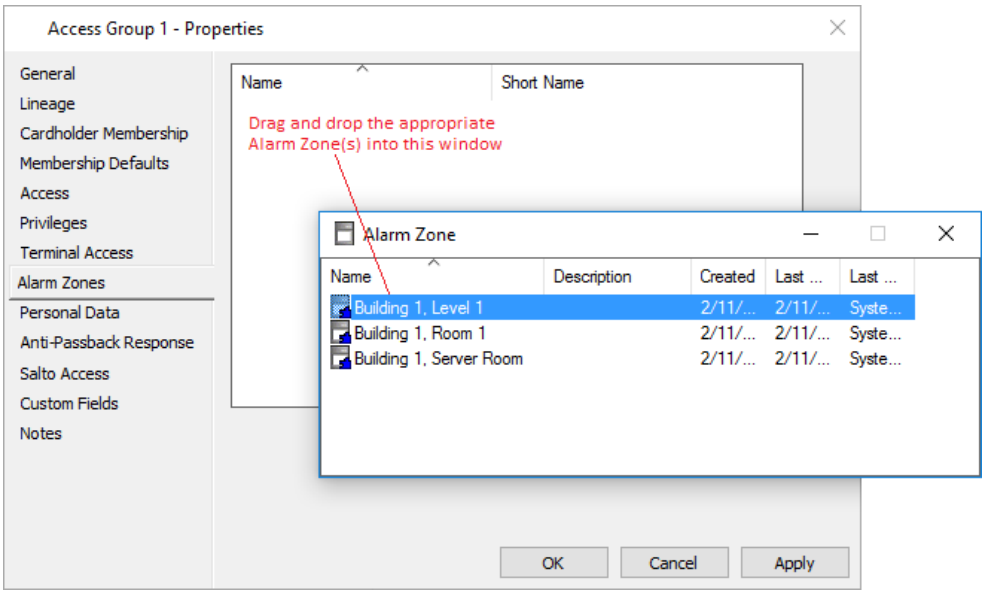



The Cardholder Access Schedule selected here, determines when the members of this Access Group can log on to an HBUS Terminal or HBUS Alarms Only Terminal.

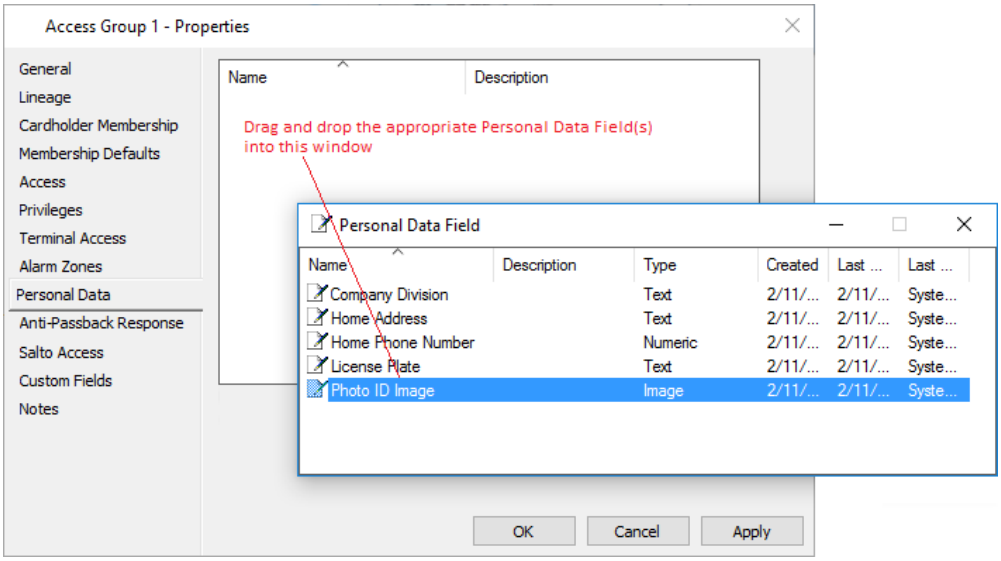
The **Terminal Access** tab can be used to configure periodic testing, to allow members of this Access Group to disarm the system via a Terminal. If this functionality is required, refer to ***Configuring Access Groups for Test Modes*** (on page 47-9) for further detail.

24. Click the **Alarm Zones** tab.

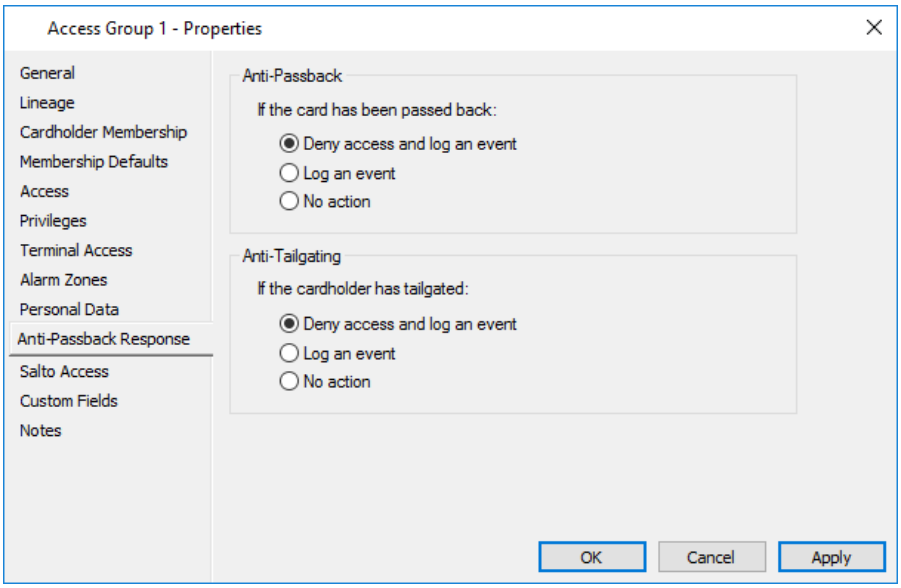
25. Click **Configure** from the menu bar, then **Alarm Zones**.
The **Alarm Zone** List Window opens.
Select those Alarm Zones appropriate for this Access Group.
Drag and drop them into the **Alarm Zones** tab window.




26. Close the **Alarm Zone** List Window.
27. Click the **Personal Data** tab.
28. Click **Configure** from the menu bar, then **Personal Data Fields**.
    The **Personal Data Field** List Window opens.
    Select those Personal Data Fields appropriate for this Access Group.
    Drag and drop them into the **Personal Data** tab window.




29. Close the **Personal Data Field** list Window.
30. Click the **Anti-Passback Response** tab.




This tab allows you to configure the responses you require for Anti-Passback violations and Anti-Tailgating violations.

| Term | Definition |
|---|---|
| Anti-Passback violation | A condition where the system has detected that a card passback has occurred, (i.e. a cardholder has attempted to enter an Access Zone, or Access Zone Group, when they are already recorded as within it). |
| Anti-Tailgating violation | A condition where the system has detected that a cardholder has tailgated, (i.e. a cardholder has attempted to enter an Access Zone when they are currently recorded as outside the Access Zone, or Access Zone Group, from which they are entering).<br><br>**Note:** While the anti-tailgating response is configured here on the Access Group, the "Check for tailgating on exit from zone" option is configured on the Access Zone. |

31. Click the appropriate radio buttons for the responses you require.
32. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Access Group.
    For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
33. Click the **Notes** tab if you want to add a note(s) about this Access Group.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
34. 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**

Cardholders belonging to the Access Group can gain access to the specified zones at the specified times.
**Note:** This new Access Group defaults into the "Immediate Children" box on the Lineage tab of the Access Group you selected as the "Immediate Parent".

**Hints**

*Find tool*
Dragging individual items (for example Access Zones) can be laborious. Using the Find tool you can speed up the procedure:
- Open the Find window.
- Set up the appropriate search criteria.
- Within the Search list window, select a continuous range or the required separate items.
- Drag the items into the appropriate Access Group window.

*Editing and Deleting Access Groups*
Refer to Editing items and Deleting items for procedures on how to edit and delete Access Groups.

*Copy and paste*
An alternative to the drag and drop method is to use the copy and paste method.

*Personal Data details*
The Personal Data Field(s) you added to this Access Group (in Step 27) will now have this Access Group displayed in the **Group Membership** tab of their Properties screen.

# Configuring Access Group Privileges for Terminal Access

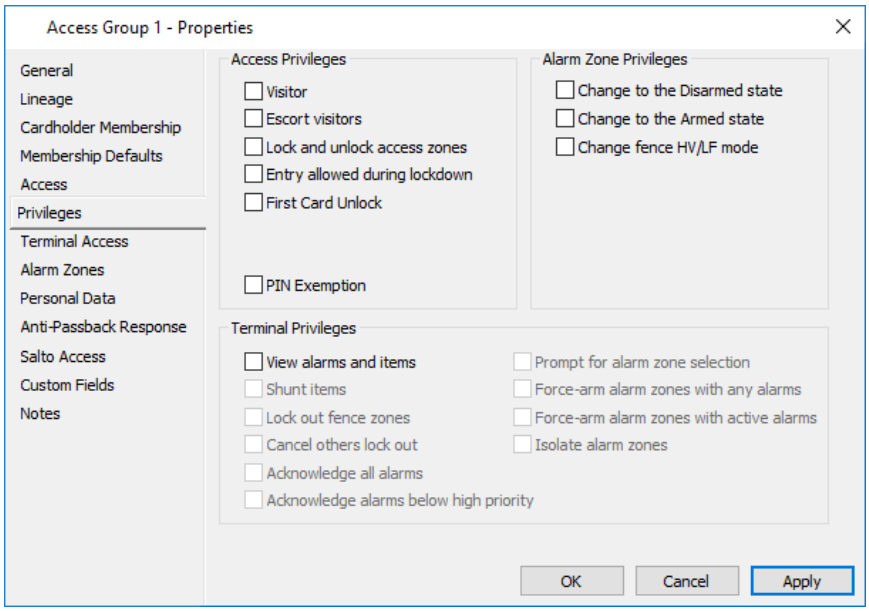
## Introduction

This procedure describes how to assign Alarm Zones to an Access Group and specify associated privileges for HBUS Terminal and HBUS Alarms Only Terminal use.

Operators require the “Edit Access Group” operator privilege, and must be in the same or parent Division of the Access Group and the Alarm Zones.

## Procedure

1. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).
2. Highlight the Access Group you wish to assign Alarm Zones to and **double-click** the mouse button.
3. Click the **Privileges** tab of the Access Group.



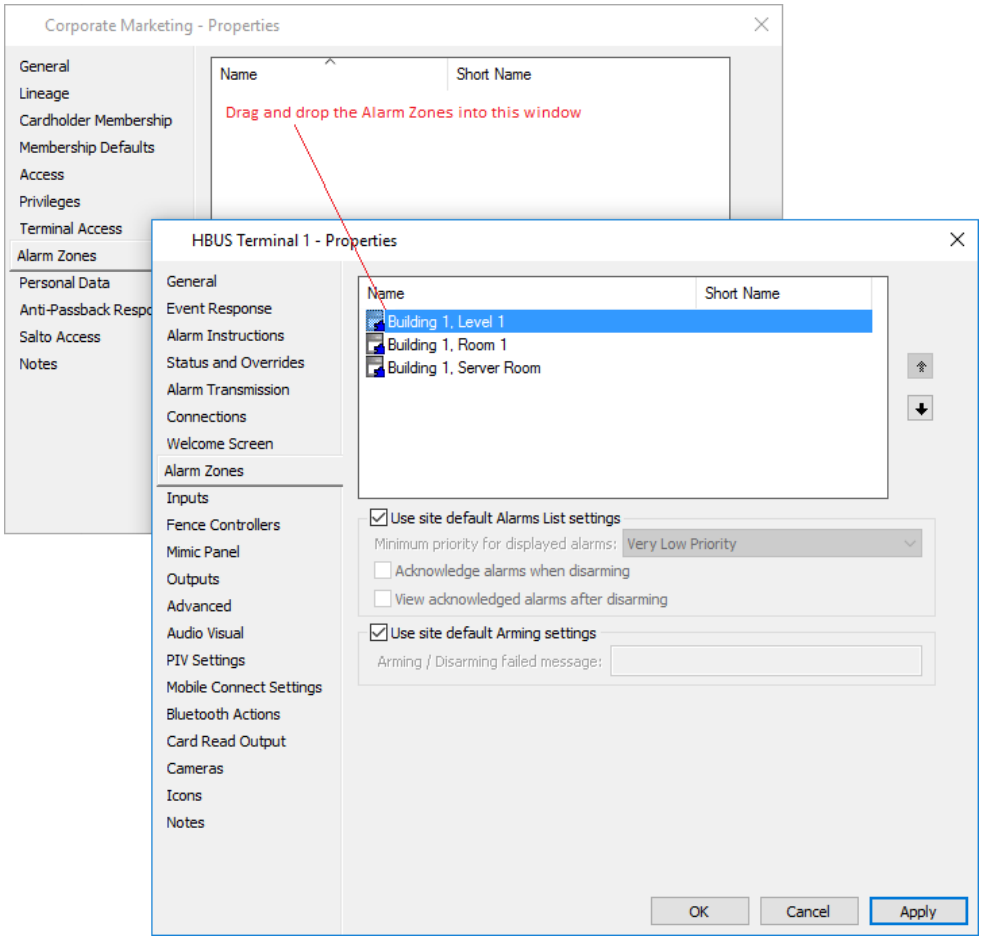

4. The **Access Privileges** and **Alarm Zones Privileges** have probably already been configured when this Access Group was created.
   Change if necessary.
5. In the **Terminal Privileges** section of this tab, select the appropriate privileges as required for the Access Group.

| Privilege | HBUS Terminals |
|---|---|
| View alarms and items | This privilege enables a user to view all available alarms and items on an HBUS Terminal or HBUS Alarms Only Terminal. |
| Shunt items | This privilege enables a user to shunt and unshunt items using an HBUS Terminal or HBUS Alarms Only Terminal. |

| Privilege | HBUS Terminals |
|---|---|
| Acknowledge all alarms | This privilege enables a user to acknowledge all available alarms using an HBUS Terminal or HBUS Alarms Only Terminal. |
| Acknowledge alarms below high priority | This privilege enables a user to acknowledge all available alarms below high priority using an HBUS Terminal or HBUS Alarms Only Terminal. |
| Lock out fence zones | This privilege enables a user to lockout selected Fence Zones using an HBUS Terminal or HBUS Alarms Only Terminal.<br><br>The fence cannot be energized when in lockout mode. Lockout is persisted during a Fence Controller or Controller restart (it is not persisted during a DIP Switch 2 Controller restart).<br>Only the user that placed the fence into lockout mode can remove lockout mode (unless the "Cancel others lockout" privilege has been assigned to another user).<br>Lockout mode can only be removed using the HBUS Terminal or HBUS Alarms Only Terminal that was used to put the fence into lockout. |
| Cancel others lock out | This privilege enables a user to cancel the lockout of selected Fence Zones initiated by another user.<br>This is only possible from the HBUS Terminal or HBUS Alarms Only Terminal that was used to put the fence into lockout. |
| Prompt for alarm zone selection | This privilege enables a user to view a list of Alarm Zones for which the user's Access Group assignment provides privilege for, from the **Menu** screen on an HBUS Terminal or HBUS Alarms Only Terminal. |
| Force-arm alarm zones with any alarms | If an Alarm Zone would not normally arm because there were any potential, unacknowledged or active alarms, by having this privilege and either the "Override" or "Override up to Medium Priority" operator privilege, a user will be provided with the option to force-arm the Alarm Zone, when arming from an HBUS Terminal or HBUS Alarms Only Terminal.<br>**Notes:**<br>• If selected, the **Force-arm alarm zone with active alarms** option (below) becomes disabled.<br>• Without this privilege the force-arm options are not available. |

| Privilege | HBUS Terminals |
|---|---|
| Force-arm alarm zones with active alarms | If an Alarm Zone would not normally arm because there were any active alarms, by having this privilege and either the "Override" or "Override up to Medium Priority" operator privilege, a user will be provided with the option to force-arm the Alarm Zone, when arming from an HBUS Terminal or HBUS Alarms Only Terminal (as long as doing so will not cause any new alarms).<br>**Notes:**<br>• If selected, the **Force-arm alarm zone with any alarms** option (above) becomes disabled.<br>• Without this privilege the force-arm options are not available on the HBUS Terminal or HBUS Alarms Only Terminal. |
| Isolate alarm zones | If an Alarm Zone would not normally set because there were open Inputs or a Fence Zone is in alarm, by having this privilege a user will be provided with the option to auto-isolate the Input's Alarm Zones, when arming from an HBUS Terminal or HBUS Alarms Only Terminal.<br>**Note:** Without this privilege the auto-isolate options are not available. |

6. Click the **Alarm Zones** tab.
   This tab provides a grid of Alarm Zones that can be controlled using HBUS Terminals and HBUS Alarms Only Terminals.
7. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens.
8. Highlight the appropriate HBUS Terminal or HBUS Alarms Only Terminal, and **double-click** the mouse button.
9. Click the **Alarm Zones** tab of the HBUS Terminal or HBUS Alarms Only Terminal.
10. Highlight the Alarm Zones to be managed by this Access Group, and drag and drop them into it's **Alarm Zones** tab.




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

The Access Group has been updated with the new Alarm Zones and Privileges for HBUS Terminal or HBUS Alarms Only Terminal use.

## Temporary Access

### Understanding Temporary Access

A cardholder can be a temporary member of an Access Group, (i.e. they are only a member for a specified period between the start and end date and time of the temporary membership). During this time, a cardholder with temporary access has the same rights as any other member of that Access Group.
Temporary access can be configured by Access Group or by individual Cardholder.

### Personal Data Fields

Any Personal Data Fields (PDFs) that belong to a particular Access Group can be associated with the cardholder as soon as the temporary access information is entered (not necessarily active), until the temporary access record is deleted. Therefore, if the temporary access records are never deleted, the temporary member will retain that PDF. If however, the temporary access records are deleted the PDF will also be deleted for the cardholder.

*For example:*
A student may be enrolled in a course that does not start until June and requires special access and a particular piece of information that will be entered into a PDF. At the beginning of the year, this student enrols in the course and temporary access is set up to start at the beginning of the June and end in November. The cardholder would have the PDF added to their cardholder information and the data required may be entered at the start of the year even though it will not be required until later.
If the system is set to delete all temporary access after it has expired, the PDF would disappear from the cardholders information at the end of November when the access expired. If the system is NOT set to delete temporary access records, the cardholder would retain the PDF, until the records were manually cleared.

### Multiple temporary memberships

A cardholder can have several temporary memberships to the same Access Group.

*For example:*
A University has two courses that share a resource.
Course 1 runs from 14/02 to 21/04.
Course 2 runs from 18/03 to 25/07.
Students in both courses require access to a computer lab, and there are several students taking both courses. These students therefore require access to the computer lab from 14/02 until 25/07.

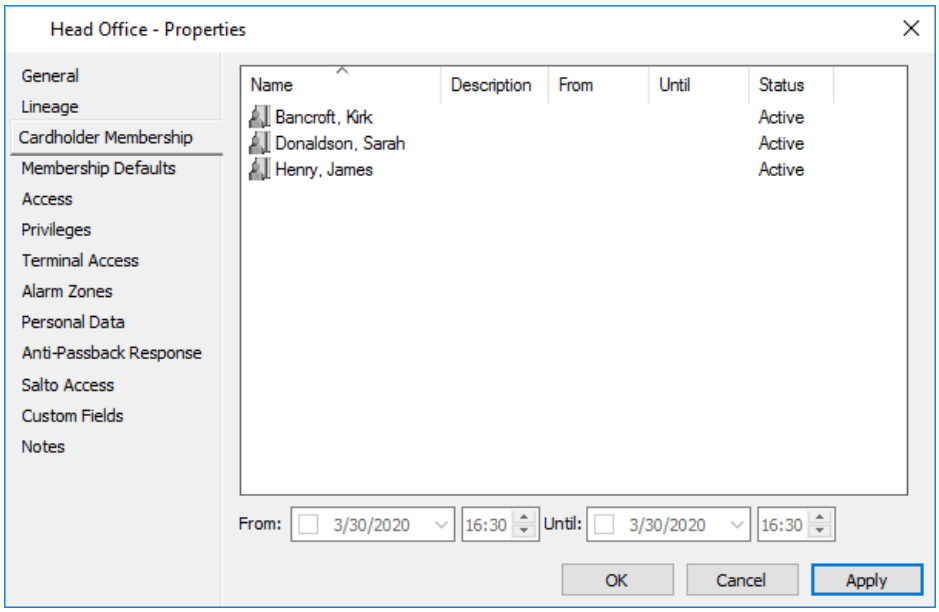
## Granting Temporary Access by Access Group

### Introduction

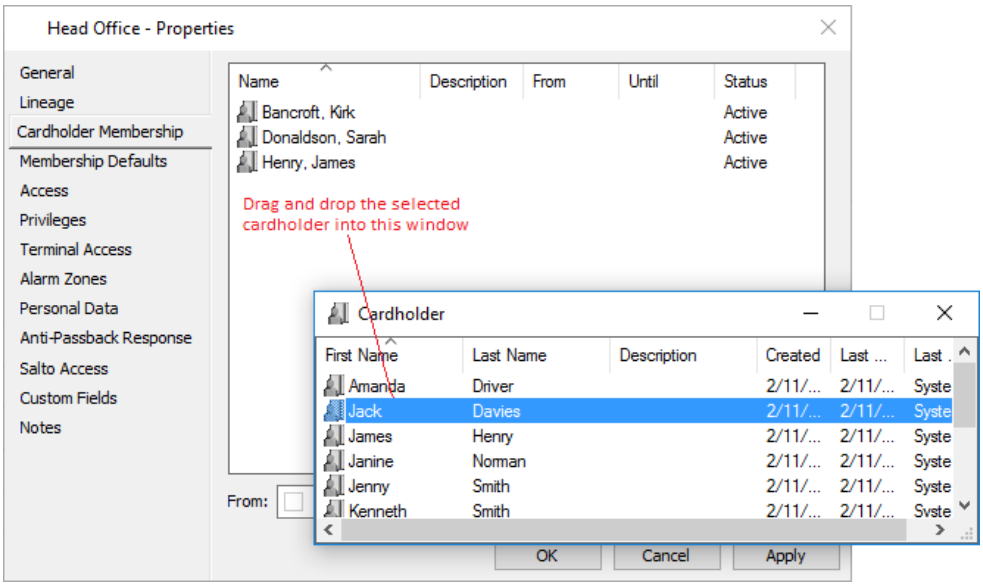
This procedure details how to grant temporary access to members of an Access Group.

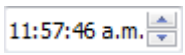
### Procedure

1. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).
2. Highlight the Access Group you want to add temporary members to.
3. **Right click** and select **Properties**.
4. Click the **Cardholder Membership** tab.

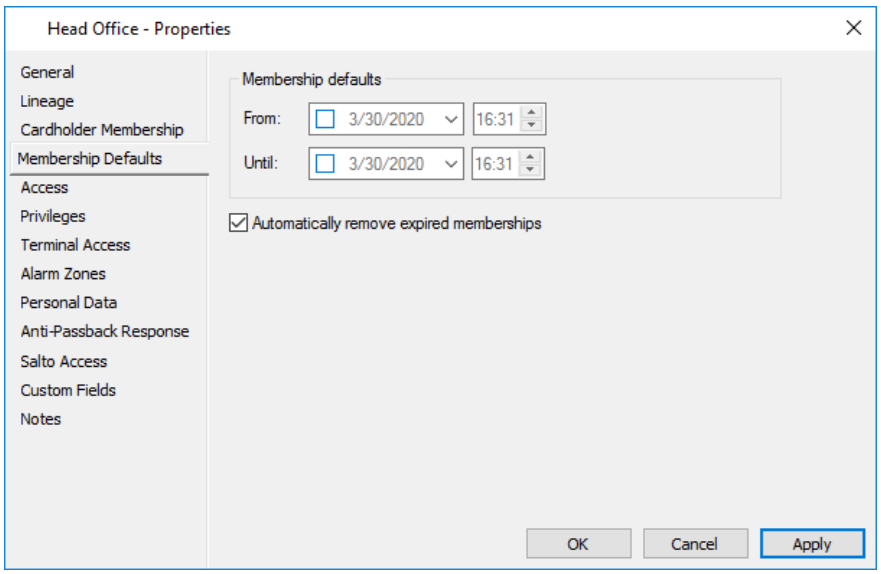



5. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
6. Select the cardholder(s) that you want to add as temporary members to the Access Group.
   Drag and drop them into the **Cardholder Membership** tab.




7. Close the **Cardholder** List Window.
8. Highlight the cardholder (on the **Cardholder Membership** tab) that requires temporary access.
   The 'From' and 'Until' Date fields become enabled.
   **Note:**
   The order of the columns can be repositioned if you want, (e.g. you may find having the Date columns first useful so you can sort by date and see which cardholders have the same temporary access periods). See ***Repositioning Column Headers*** (on page 3-6) for the procedure.
9. Click the 'From' drop-down box and select the date the cardholder needs access from.
   The 'From' Time Box becomes enabled, and the 'From' date now displays in the main grid beside the cardholders name.
10. Alter the time in the 'From' Time Box 

to the time the cardholder needs access from on this date.
11. Repeat Steps 9 and 10 for the 'Until' fields, (i.e. the date and time of the last day the Cardholder needs access up to).
    The 'Until' date displays in the main grid beside the cardholders name.
12. Click the **Membership Defaults** tab.




By default, the start and end dates are set to none, meaning that by default, membership is permanent.

13. Do you want temporary members to be removed from the **Cardholder Membership** tab when their temporary access period expires?

| If... | then... |
|---|---|
| yes | leave the **Automatically remove expired memberships** checkbox ticked.<br>**Note:** By leaving the checkbox ticked, all expired memberships shall be deleted automatically from the list on the **Cardholder Membership** tab when they expire. |
| no | uncheck the **Automatically remove expired memberships** checkbox.<br>**Note:** By unchecking the checkbox, cardholders with temporary access will remain in the list on the **Cardholder Membership** tab once their access period expires. |

**Note:** Cardholders can only belong to 255 unique, and active or pending, Access Groups.

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 Access Group now has temporary member(s).

**Notes:**

- The cardholder(s) you have granted temporary access to will now have this Access Group displayed in the **Access Groups** tab of their properties.
- If two operators concurrently add the same temporary membership, (i.e. one via the Access Group properties and the other via the Cardholder properties), **two** new memberships will appear in both the **Access Group** and **Cardholder** properties. Two events will also be generated, indicating that separate operators created the new memberships.

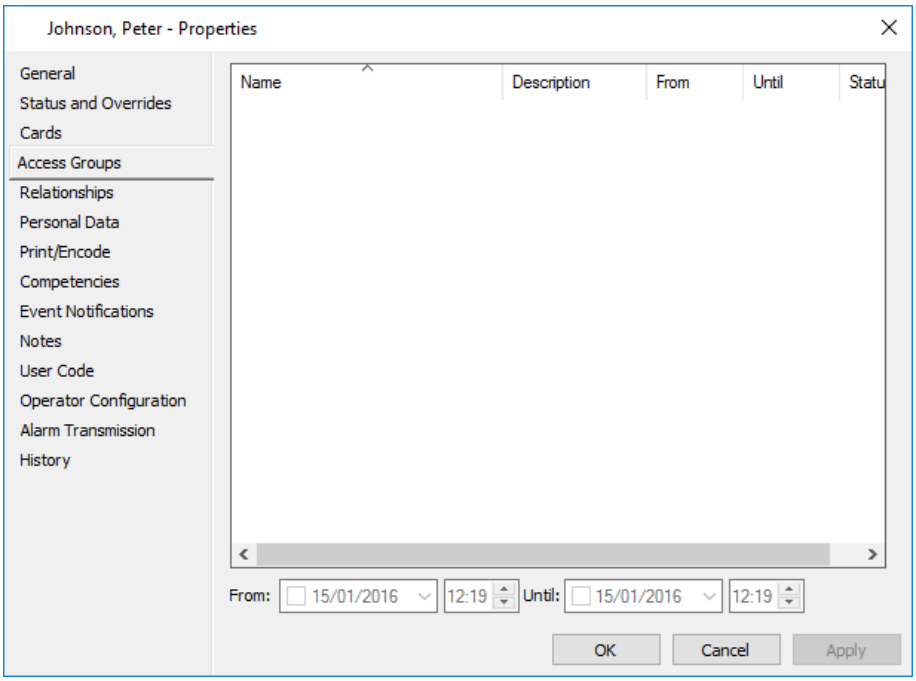
# Granting Temporary Access by Cardholder

## Introduction

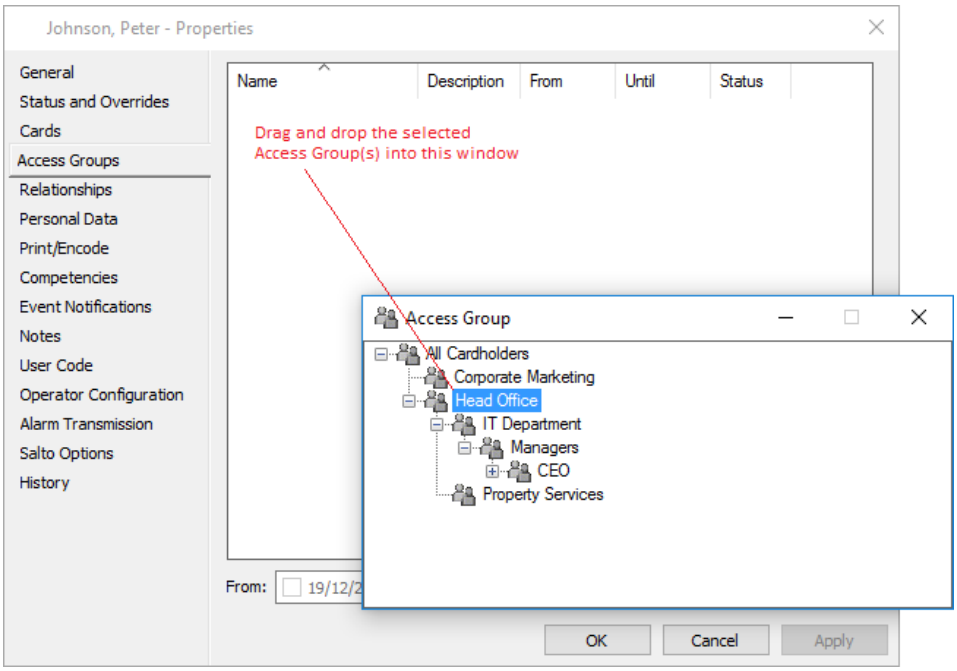
This procedure details how to grant temporary access to Access Groups for individual cardholders.

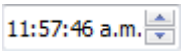
## Procedure

1. Click Manage from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Highlight the cardholder you want to grant temporary access to.
3. **Right click** and select **Properties**.
4. Click the **Access Groups** tab.




5. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens.
6. Select the Access Group(s) that you want to give this cardholder temporary access to.
   Drag and drop them into the **Access Groups** tab.




7. Close the **Access Group** List Window.
8. Highlight the Access Group (on the **Access Groups** tab) that this cardholder requires temporary access for.
   The 'From' and 'Until' Date fields become enabled.
9. Click the 'From' drop-down box and select the date the cardholder needs access from.
   The 'From' Time Box becomes enabled, and the 'From' date now displays in the main grid beside the Access Group name.
10. Alter the time in the 'From' Time Box 

to the time the cardholder needs access from on this date.
11. Repeat Steps 9 and 10 for the 'Until' fields, (i.e. the date and time of the last day the Cardholder needs access up to).
    The 'Until' date displays in the main grid beside the Access Group name.
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 cardholder now has temporary access to an Access Group.

**Notes:**

- This cardholder will now display in the **Cardholder Membership** tab of the Access Group properties.
- On the **Cardholder Membership** tab, cardholders display in different colours to indicate whether their membership is in "pending" or "expired" state.

- If two operators concurrently add the same temporary membership, (i.e. one via the Access Group properties and the other via the Cardholder properties), **two** new memberships will appear in both the **Access Group** and **Cardholder** properties.
  Two events will also be generated, indicating that separate operators created the new memberships.

## Deleting Temporary Memberships

### Introduction

Expired temporary membership records can be deleted from Access Groups. While Command Centre can be configured to automatically delete temporary memberships when the period expires (via a checkbox on the Access Group **Membership Defaults** tab), they can also be deleted manually.
This procedure describes how to manually delete expired temporary membership records, which can be done either by Access Group or by individual cardholder.

### Procedure

***Via Access Group***

1. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).
2. Highlight the required Access Group.
3. **Right click** and select **Properties**.
4. Click the **Cardholder Membership** tab.
5. Highlight the cardholder(s) whose membership has expired.
   **Note:** Multiple cardholders can be selected at once by holding down the <**Shift**> or <**Ctrl**> key on your keyboard while clicking the mouse button.
6. **Right click** and select **Remove from List**.
   The cardholder(s) is removed from the list, and once **Apply** is clicked, records of the Access Group will also disappear off the **Access Groups** tab on the Cardholder properties.

***Via Cardholder***

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Highlight the required cardholder.
3. **Right click** and select **Properties**.
4. Click the **Access Groups** tab.
5. Highlight the **Access Group**.
6. **Right click** and select **Remove from List**.
   The Access Group is removed from the list, and once **Apply** is clicked, records of the cardholder will also disappear off the **Cardholder Membership** tab on the Access Group properties.

### Result

The expired temporary access record(s) have been deleted from the system.

# Chapter 35: Notifications

This feature allows administrators to configure Command Centre to automatically send notifications of:

- significant events, such as alarms, to cardholders via SMS to their mobile phone, or to a nominated email address. Suitably privileged message recipients will have the ability to respond to messages to acknowledge alarms. See ***Acknowledging alarms via SMS or email*** (on page 35-28) for the procedure.
- card and competency expiry warnings to individuals, Administrators or Supervisors.

**Notes:**

- Mobile Connect users **cannot** be sent Alarm Notifications, they can be sent Broadcast notifications.
  Only operators can be sent Alarm notifications, so only to the Mobile Command Centre App, not the Mobile Connect.
- Message content will only be written using the local server language.
- Command Centre does not override the default Mailkit supported protocols, TLS1.2 and TLS1.3 are used.

## Mobile Notifications

Enabling Mobile Notifications allows a Command Centre site to send alarm notifications to Mobile Client users. Selecting a notification allows you to view the alarm's details within the Mobile Client.

Only alarm notifications from the most recent Command Centre site that the Mobile Client user has logged into will be sent. Only alarms are sent as notifications, not events.

**Note:** If you receive notifications from Site A, and then you log into Site B (that doesn't have Mobile Notifications enabled), you will continue to receive notifications from the previous site (Site A).

## Custom Notifications

Users can create custom email notifications for guards, Cardholders, administrators, supervisors, and Access Group members. Users can customise the wording of the email subject line, specify the font and colour of the email body, modify content in the email body, and add images to the email, among other things.

These custom notifications are configured using HTML. 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 can send themselves test emails from this tab to ensure that the email has been configured according to their requirements. For further information on configuring emails refer to the **HTML Help.pdf** located in the `'Documentation'` folder of the Command Centre installation files.

## Personalised Notifications

Personalised Notifications is the ability to automatically send emails to a Cardholder within an Access Group when an event occurs that directly relates to that Cardholder. This is set up by assigning a Notification Filter to that Access Group in the notifications filter configuration only. The 'event notification' settings for the Cardholder do not apply to personalised notifications. Personalised Notifications can be configured via Configuration Client or Command Centre Client, and are linked to events only (not expiries).
For example:

*Access Group A contains Cardholders X, Y and Z. When Cardholder Z badges their card, an email is sent to Cardholder Z to notify them that an event has occurred that relates to them. Cardholders X and Y are not informed of Cardholder Z's access event, even though they are in the same Access Group, because the event does not specifically relate to Cardholders X and Y.*

To use the Personalised Notifications feature, you must have a Gallagher Controller set up with, at minimum, a Reader, an Access Zone, and a Door. Refer to ***Overall Process - Setting up Notifications*** (on page 35-3) for more information on how to set up Personalised Notifications.

### Examples of how this feature can be used:

- Security Guards can direct all or some events/alarms to be sent to their mobile phone or PDA (email) when leaving the control room.
- Maintenance contractors can receive maintenance alarms (e.g. low battery warning) via SMS or email.
- After hours and on weekends or holidays, building managers can be notified via mobile phone of all high priority alarms occurring on their facility.
- Relevant personnel, (e.g. managers, supervisors, administrators) can receive other Cardholders' event notifications, (e.g. Cardholder Competency Expired), and take appropriate action.
- Operators can notify a group of personnel about site hazards, upcoming expirations, or general notices such as fire alarm testing.

Select the item below that you require further detail on:


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

## Overall Process - Setting up Notifications

### Introduction

This section describes the overall process (to be performed by the System Administrator) for configuring Command Centre for Messaging.
Five types of Notifications can be configured in Command Centre:

- Event/Alarm Notifications to specified Cardholders;
- Event/Alarm Notifications to related Cardholders within an Access Group (Personalised Notifications);
- Card and Competency Expiry Notifications;
- Broadcast Notifications; and
- Mobile Notifications for Mobile Client users.

When necessary, this process refers to separate step-by-step procedures that are detailed elsewhere, (i.e. either as separate procedures in this section, or in other sections in this help).
**Note:** To help you understand how the Notifications feature works, and the various components that need configuring depending on what your site wants to achieve, see ***Notification Examples*** (on page 35-25).

### Process

Follow the steps below for the type of Notification you want to set up:

#### *Setup for Event/Alarm Notifications and Personalised Notifications*

1. Set up the Notification, Email, and SMS Server properties.
   Refer to Notifications, Outgoing Email, Incoming Email and Mobile/SMS Notifications for the procedures.
2. Configure Notification Filters.
   Notification Filters define the types of events/alarms and the event sources (doors, inputs, etc.) about which a person will be notified.
   Refer to ***Creating a Notification Filter*** (on page 35-5) for the procedure.
3. Create "Email" and "Mobile" type PDFs, assign them to an Access Group, and enter email addresses and mobile phone numbers against all Cardholders/Operators that need to receive email and SMS notification of certain events and/or alarms.
   Refer to ***Setting Cardholder "Email" and "Mobile" PDFs*** (on page 35-9) for the procedure.
4. Enable which Cardholders can be sent messages, and when and how they should be sent. Refer to ***Enabling Event/Alarm Notifications for a Cardholder*** (on page 35-10) for the procedure.
   **Note:** Continue to Step 5 if you want to set up Personalised Notifications. Otherwise, stop here.

5. Assign Access Groups to Notification Filters (this allows Cardholders to be sent notifications of events that are related to them).
   Refer to ***Creating a Notification Filter*** (on page 35-5) for the procedure.
6. If you want another person, (e.g. supervisor, administrator) to receive the same notifications as a Cardholder, create a Role and assign both the employee (Cardholder) and the additional person to the Role.
   Refer to ***Setting up Roles*** (on page 35-17) for the procedure.

***Setup for Card and Competency Expiry Notifications***

1. Set up the Notification, Email, and SMS Server properties.
   Refer to Notifications, Outgoing Email, Incoming Email and Mobile/SMS Notifications for the procedures.
2. Set the Time that the daily Card and Competency Expiry Notification procedure should be run.
   Refer to Notifications for the procedure.
3. Create "Email" and "Mobile" type PDFs, assign them to an Access Group, and enter email addresses and mobile phone numbers against all Cardholders/Operators that need to receive email and SMS notification of pending Card and Competency expiries.
   Refer to ***Setting Cardholder "Email" and "Mobile" PDFs*** (on page 35-9) for the procedure.
4. Determine Cardholder and Competency expiry threshold values.
   Refer to ***Setting Expiry Notification Threshold Values*** (on page 35-14) for the procedure.
5. Create Roles to define relationships between cardholders, (for the purpose of routing notifications), and assign cardholders to the Roles.
   Refer to ***Setting up Roles*** (on page 35-17) for the procedure.

***Setup for Broadcast Notifications***

Refer to the topic *"Broadcast Notification Configuration"* in the Command Centre Online Help.

***Setup for Mobile Notifications***

1. Enable Mobile Notifications.
   Refer to ***Mobile/SMS Notifications*** (on page 6-54) for the procedure.
2. Connect Command Centre to the Cloud.
   Refer to ***Connecting to the Cloud*** (on page 31-3) for the procedure.
3. Configure Notification Filters. Notification Filters define the alarms that will be sent as Mobile Notifications.
   Refer to ***Creating a Notification Filter*** (on page 35-5) for the procedure.
4. Enable which Mobile Client users can be sent Mobile Notifications, and when they should be sent. Refer to ***Enabling Event/Alarm Notifications for a Cardholder*** (on page 35-10) for the procedure.

## Creating a Notification Filter

### Introduction

A Notification Filter is a set of criteria determining which events and alarms should be notified to Cardholders. There are two ways of assigning a Notification filter to a Cardholder:

- Assigning the Notification Filter to the Cardholder on the Cardholder's Event Notifications tab. This means the Cardholder will be notified about any matching events relating to any Cardholder. See ***Enabling Event/Alarm Notifications for a Cardholder*** (on page 35-10).
- Assigning an Access Group that the Cardholder is into Notification Filter on the Notification Filter's **Personalised Notifications** tab (explained later in this topic). This means that only the Cardholder (if within that group) for whom the event was about will be notified.

**Note:** Roles also allow for notification of someone else linked to the person being notified in either case 1 or 2.

This procedure describes how to create a Notification Filter. Notification Filters are normally configured against Cardholder records and send event notifications to those Cardholders, (e.g. Guards). Personalised Notifications are configured by assigning Access Groups to the Notification Filter, and send Cardholder related events only to the related Cardholder if that Cardholder is a member of one of the assigned Access Groups (or a child Access Group).

| **To send event email or SMS to...** | **assign...** |
|---|---|
| Guards (or non-related Cardholders), | a Notification Filter to each particular Guard's/Cardholder's **Event Notifications** tab. |
| event-related Cardholders, | to a Notification Filter the Access Group(s) containing the Cardholders to receive event notifications about themselves. |
| Event-related Cardholders' Relationships (Roles), | to a Notification Filter the Roles to receive notifications about the Cardholders for whom they are that Role. They only receive notifications about Cardholders who are in the Access Groups assigned to the Notification Filter. |

When an Access Group is assigned to a Notification Filter, Cardholders belonging to the Access Group or any of its child Access Groups will receive notifications as specified by the Notification Filter.

If Cardholders in these Access Groups have Roles assigned on their **Relationships** tab, and these Roles are assigned alongside the Access Groups on the Notification Filter's **Personalised Notifications** tab, then event notifications are sent to these Roles.

**Notes:**

- If configuring a Notification Filter for Mobile Notifications, only alarms can be sent, not events. Mobile Notifications will not work when the Notification Filter is assigned to an Access Group. The Notification Filter must be assigned to individual Cardholders.

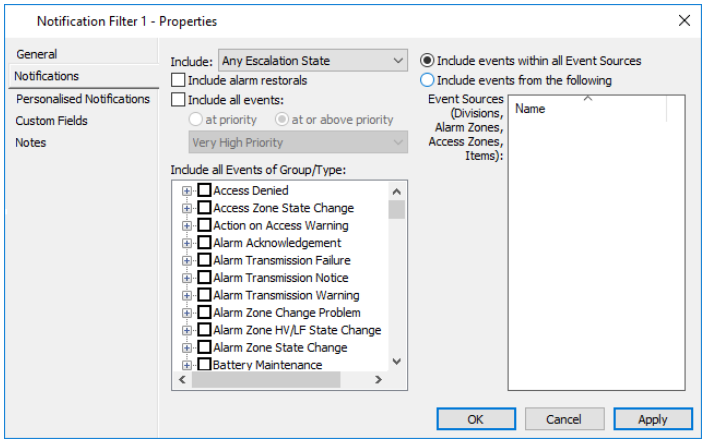
- Notifications is a licensable feature.

## Operator Privileges

| To... | you require the... |
|---|---|
| make a change to a Notification Filter | "Configure Site" privilege in the appropriate division. |
| Edit the Personalised Notifications tab on a Notification Filter | "Edit Personalised Notifications" privilege in the appropriate division. |
| see/view a Notification Filter | "View Site" privilege in the appropriate division. |

## Procedure

1. Click **Configure** from the menu bar, then **Notification Filters**.
   The **Notification Filter** List Window opens (in grid view).
2. **Right click** and select **New...Notification Filter**.
   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 **Notifications** tab.

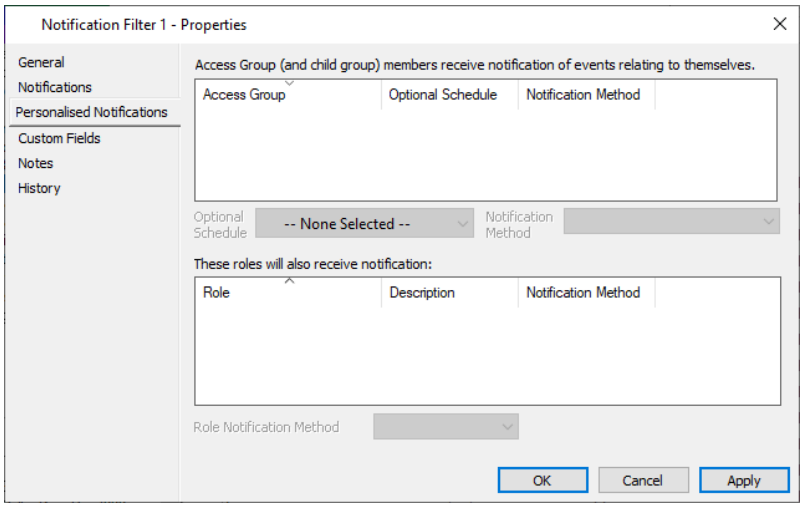



5. To define the Notification Filters, configure as appropriate:

| Field | Description |
|---|---|
| Include: | Select the required Escalation state from the drop-down list. Options are:<br>**Any Escalation State:** Events/alarms that are in any escalation state will be notified.<br>**Escalated Events Only:** Only events/alarms that are escalated will be notified.<br>**Non-escalated Events Only:** Only non-escalated events/alarms will be notified. |
| Include alarm restorals | Checking this option will send separate notifications for each restoral and reactivation of a stateful alarm. |
| Include all events at (or above) priority: | Checking this option:<br>• enables the drop-down list of priorities, allowing you to select another of the existing priorities, &<br>• the text below changes from "**Include all** Events of Group/Type" to "**As well as** Events of Group/Type"<br>**Note:** If you do not check this option, at least one Group or Type must be selected. |

| Field | Description |
|---|---|
| | Default = The second highest Priority level<br>Selecting the **at priority** option only notifies that priority's events, whereas the **at or above priority** option notifies events of that priority and above. |
| Include all Events of Group/Type: | If an Event Group is selected then all Event Types belonging to the Event Group will be notified. It is possible to select various Event Types within a particular Event Group. Default = None selected |
| Include events within all Event Sources | If enabled, then you cannot restrict the Event Sources, (i.e. you cannot select specific Event Source items). Notifications are not restricted by event source when this option is selected.<br>Default = Enabled |
| Include events from the following Event Sources | If you check this radio button, then at least one item needs to be dragged and dropped into the Event Sources grid. There is no restriction to the number of Event Sources, (i.e. Divisions, Cardholders, Alarm Zones, Access Zones and Items), that can be included in this grid. Notifications will be restricted only to these event source(s) when this option is selected.<br>Default = Disabled (None included) |

6. Click the **Personalised Notifications** tab.




7. In the top grid, drag and drop the Access Groups whose Cardholders (and Cardholders of child Access Groups) are to receive personal notifications as per the configuration in the **Notifications** tab. The Cardholders in these Access Groups will only receive notifications about events that relate to themselves.
   **Note:** If a Cardholder is in more than one of the Access Groups in this grid, they will still only receive one notification per related event, unless the different Access Groups have different notification methods, in which case they will receive the separate notifications.
8. Optionally assign a schedule to an Access Group by selecting the Access Group then choosing a schedule from the **Optional Schedule** drop-down list.

9. Select the notification method (**Email** or **SMS**) for an Access Group by selecting the Access Group then choosing a notification method from the **Notification Method** drop-down list.
10. Enable or disable notifications from this Notification Filter for each Access Group by selecting (to enable) or deselecting (to disable) the checkbox to the left of each Access Group's name.
11. In the bottom grid, drag and drop the Roles that are also to receive notifications as per the configuration in the **Notifications** tab. These Roles will be notified for every notification that is:
    - sent to a Cardholder who they have a relationship with, and
    - sent as a result of this Notification Filter.
12. Select the notification method (**Email - Separate**, **Email - CC**, or **SMS**) for a Role by selecting the Role, then choosing a notification method from the **Role Notification Method** drop-down list.

    **Email - Separate** will send a separate email notification to the Role for all notifications that are sent to Cardholders (functionality prior to Command Centre v8.40).
    **Email - CC** will carbon copy (Cc) the Role in all emails sent to Cardholders.
    **SMS** will send a separate SMS to the Role for all notifications that are sent to Cardholders.
    **Note:** For Roles to receive notifications via a certain method, the Cardholder who receives the original notification must be in an Access Group that is configured with that same notification method.
    For example, for a Role to receive a notification via SMS, the notification-related Cardholder must be in an Access Group that that is configured with the SMS Notification Method.
13. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Notification Filter. 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 Notification Filter. For further details, 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.

**Hints**

*Deleting Notification Filters*
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete a Notification Filter.
**Note:** Notification Filters cannot be deleted if they are attached to one or more cardholder records.

*Escalated Events*
Normally an event that matches the assigned Notification Filters will trigger an email, and when the event escalates, it triggers another email. However, when the Messaging service is under significant strain, the event may be escalated before the first email is sent, which results in only the second email being sent. The details of the second email are almost identical to the first, except that the event will show as being "escalated".

## Setting Cardholder "Email" and "Mobile" PDFs

### Introduction

Contact details are held in contact type Personal Data Fields, (i.e. "Address", "Phone", "Email" and "Mobile"). "Email" and "Mobile" type PDFs also have a notification check box editable at the cardholder level. They are set for individual cardholders, and assigned to cardholders via Access Groups, as is common with other PDFs.
**Note:** Notifications is a licensable feature.

### Procedure

1. Set up an "Email" and a "Mobile" contact type Personal Data Field for use with notifications.
   Refer to Creating a new Personal Data Field for the procedure.
2. Optionally, on the **Type** tab of the Personal Data Field, check the **Default Notifications** checkbox.
   This provides a default value for this property when a PDF is first assigned to a Cardholder.
3. Assign the Personal Data Fields to an appropriate Access Group, as follows:
   a) Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens.
   b) Highlight the Access Group you want to assign Personal Data Fields to, and double-click the mouse button.
   c) Click the **Personal Data** tab.
   d) From the **Personal Data Field** List Window, select the Personal Data Fields created at Step 1.
   Drag and drop them into the **Personal Data** tab window.
4. On the **Personal Data** tab of the Cardholder, populate the "Email" and "Mobile" Personal Data Fields and ensure the **Notifications** checkbox is ticked. Refer to Editing a Cardholders PDF data for the procedure. **Notes:**
   - As long as the email addresses and mobile phone numbers entered are valid, checking the **Notifications** checkbox ensures that the Cardholders will receive email and/or SMS notifications.
   - Mobile phone numbers can include spaces or dashes. These will be removed for notifications using this number.
   - It is possible to setup more than one Email and/or more than one Mobile PDF, and have a cardholder receive notifications to more than one email account and/or mobile phone number.

## Enabling Event/Alarm Notifications for a Cardholder

### Introduction

The **Event Notifications** tab on the Cardholder properties page allows a privileged operator to Enable and Disable notifications for a particular Cardholder, either instantly, or at a future time or for a particular period of time. This page also displays the messaging filters that are active for the Cardholder alongside an optional schedule for each filter, as well as a notification method, (i.e. Email, SMS, or Mobile Notifications).

### Operator Privileges

The "Edit Cardholder Notification" operator privilege is required to:

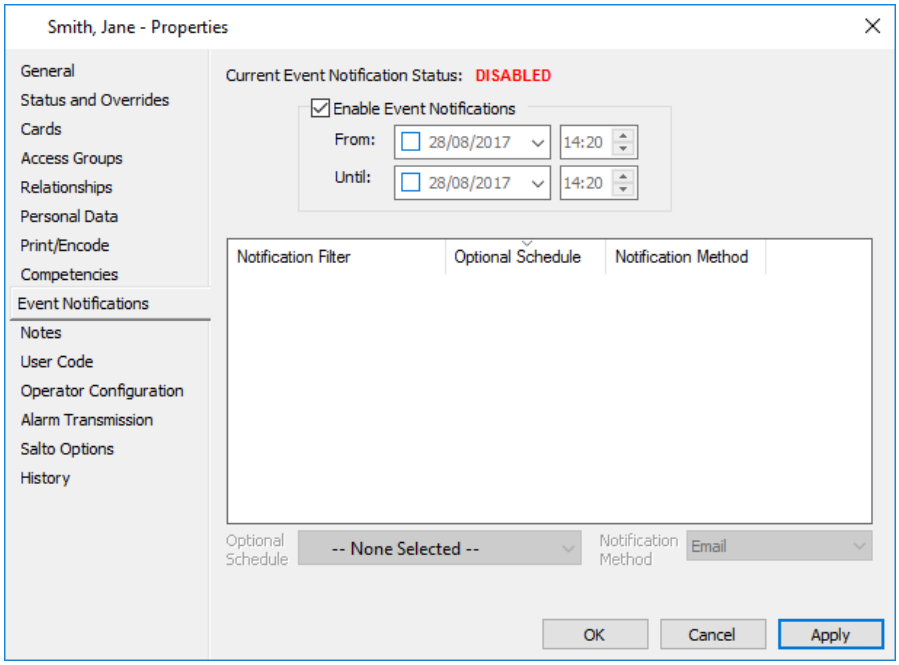
- enable/disable notifications on the **Event Notifications** tab of the Cardholder record.
- change the preferred notification method at the filter level.

In addition to the "Edit Cardholder Notification" privilege, you may require another privilege depending on what function you want to perform, as follows:

| To... | you also require the... |
|---|---|
| add or remove a Notification Filter from the Cardholder | "View Site" privilege in the Notification Filter's division. |
| add or remove a Schedule from the Cardholder's Notifications tab | "View Schedule" privilege in the Schedule's division. |
| see and/or update any other Cardholder tabs other than the **Event Notifications** tab | appropriate Cardholder privilege, (i.e. "Edit Cardholder", "Delete Cardholder", "View Cardholder" or "Edit Cardholder Notes"). |

### Procedure

1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the Cardholder to edit.
3. **Right click** and select **Properties**.
4. Click the **Event Notifications** tab.
   **Note:** The **Current Event Notification Status** only affects event notifications, (i.e. it does not affect expiry notifications). By default, all Cardholders **Current Event Notification Status** will be DISABLED.



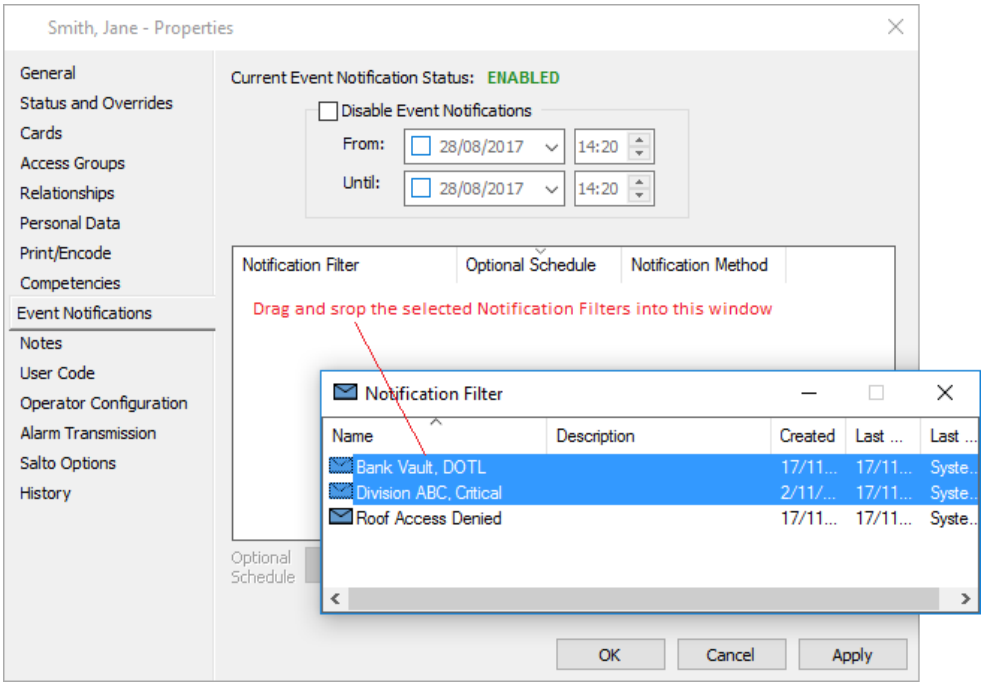

5. Check the **Enable Event Notifications** checkbox.
   **Note:** The status will not change until the **Apply** button is clicked, and the name of the checkbox changes from **Enable Event Notifications** to **Disable Event Notifications**.



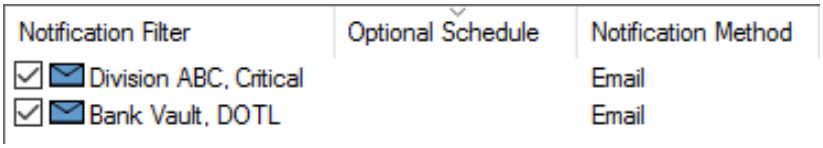

   If you require Notifications to be enabled for a specific time, set the **From** and **Until** dates and times.
   **Notes:**

| **If you...** | **when the Apply button is clicked, the Event Notification status...** |
|---|---|
| enter a date from the future in the **From** field, | will remain as DISABLED. It will not change to ENABLED until the date and time indicated in the **From** field. |
| do not enter a date in the **From** field, | will become ENABLED immediately. |
| do not enter a date in the **Until** field, | will become ENABLED indefinitely. |

6. Click **Configure** from the menu bar, then **Notification Filters**.
   The **Notification Filter** List Window opens.
7. Select those Notification Filter(s) you want to assign to this Cardholder. Drag and drop them into the **Event Notifications** tab.



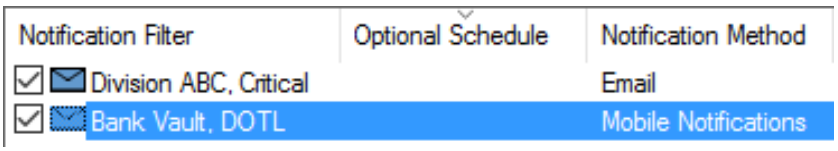

**Note:** By default, when you drag a Notification Filter into this window, it will not have a Schedule associated with it, and the notification method will be "Email".




8. Close the **Notification Filter** List Window.
   Notification Filters can optionally have a schedule associated. A schedule defines the times when events selected by this filter are notified to the Cardholder.
   **Note:** If a schedule is not assigned to a messaging filter, then that filter will be assumed to be enabled at all times.
9. Do you want to associate a schedule with the Notification Filter(s)?
   If **yes**, go to Step 10.
   If **no**, go to Step 13.
10. Click on the required Notification Filter so it is highlighted.
    The **Optional Schedule** and **Notification Method** fields become enabled.
11. Select an **Optional Schedule** from the drop-down list. Alternatively, drag and drop the schedule from the Schedule List Window.
    **Note:** The drop-down list contains only "Notification" type schedules.
12. Repeat Steps 11-12 for any other Filters you want to associate a Schedule with.
    **Note:** A Filters property pages and/or Schedule property pages can be opened from this window, by either:
    - double-clicking on the Filter or Schedule in the grid, or

- right-clicking on the Filter. A context-menu displays, with the option to select either **Filter Properties** or **Schedule Properties**.
  **Note:** If the Filter does not have a Schedule associated with it, the **Schedule Properties** option will be disabled.

13. If you want to change the notification method from "Email", select another option from the **Notification Method** drop-down list.
    See ***Mobile/SMS Notifications*** (on page 6-54) for further detail.




    **Note:** If configuring Mobile Notifications, select **Mobile Notifications** from the **Notification Method** drop-down list.

14. By default, the ☑ tick-boxes beside each Notification Filter indicates that they are selected to activate the filter.
    If you want to deactivate a filter, deselect the tick-box beside the relevant filter. Events selected by this filter will no longer be notified to the Cardholder.

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.

**Hint**

*My Notifications*
The logged-in operator can quickly access the **Event Notifications** tab of their own Cardholder properties (via **Manage** > **My Notifications**), primarily for the purpose of quick enablement/disablement of event notifications.

## Setting Expiry Notification Threshold Values

### Introduction

Supervisors/Managers need to be notified via SMS and/or Email when:

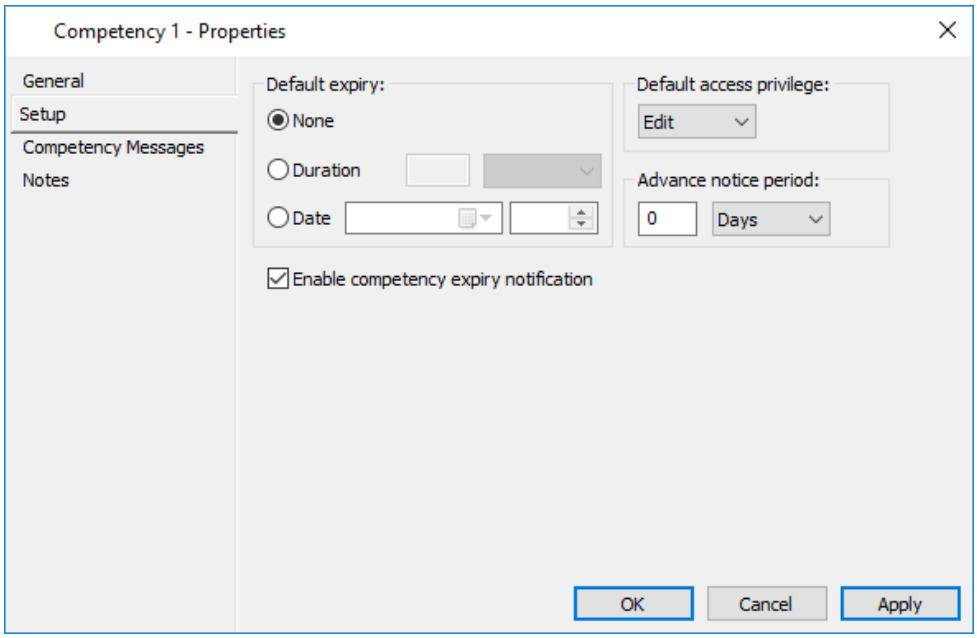
- a card is nearing expiry for one of their staff,
- a competency is nearing expiry for one of their staff.

**Note:** Individual Cardholders may also need to be notified of this via SMS and/or Email.

For this to occur, expiry threshold values need to be set for these access elements, so the system will generate events when the access is nearing expiry.
**Note:** Expiry notifications will not be sent for 'old' cards and competencies that have already expired.

### Procedure

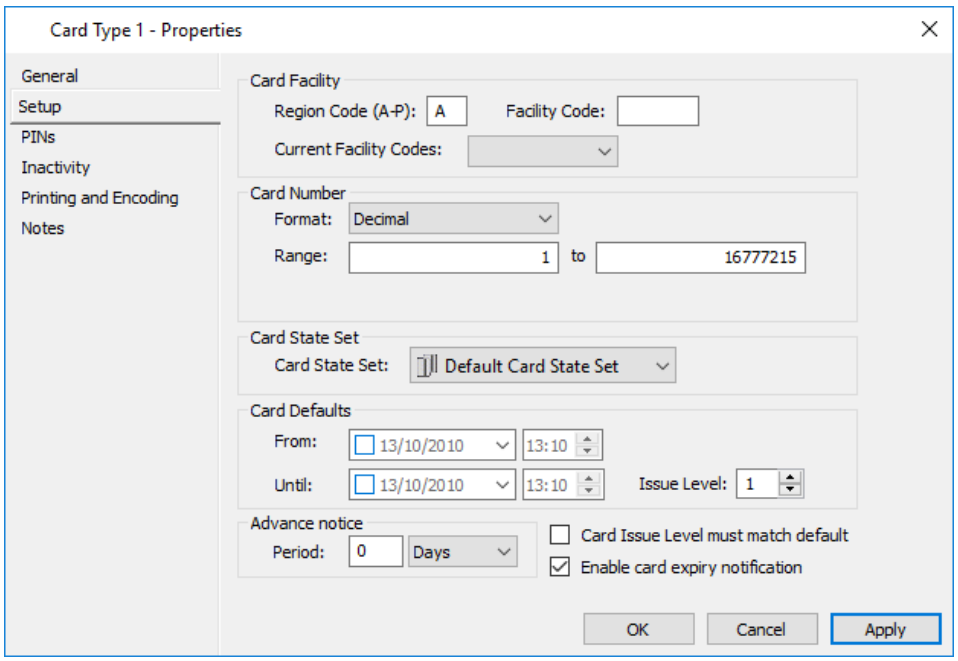
1. Click **Configure** from the menu bar, then **Competencies**.
   The **Competency** List Window opens (in grid view).
2. **Right click** on the required competency, and select **Properties**.
3. Click the **Setup** tab.




4. Set the **Advance notice period** to the value that is required to represent the number of days, weeks, months or years prior to competency expiry to initiate the warning notification.
   **Notes:**

- The maximum equivalent period is 999 days.
- This notice period also controls the period used to display competency expiry warning at a reader.

5. Ensure the **Enable competency expiry notification** checkbox is ticked.
   **Note:** The running of the daily expiry notifications does not send a notification for a competency that has expired by a date earlier than the current date, less the Advance notice period. If the Advance notice period is set to zero, competencies that have expired in the past 24 hours will still be notified at the time the daily expiry notifications are run.
6. Click the **OK** button.
7. Repeat Steps 2-6 for each competency requiring warning notification of expiry.
8. Close the **Competency** List Window.
9. Click **Configure** from the menu bar, then **Card Types**.
   The **Card Type** List Window opens (in grid view).
10. **Right click** on the required card type, and select **Properties**.
11. Click the **Setup** tab.




12. Set the **Advance notice period** to the value that is required to represent the number of days, weeks, months or years prior to card expiry to initiate the warning notification.
    **Note:** The maximum equivalent period is 999 days.

13. Ensure the **Enable card expiry notification** checkbox is ticked.
    **Note:** The running of the daily expiry notifications does not send a notification for a card that has expired by a date earlier than the current date, less the Advance notice period. If the Advance notice period is set to zero, cards that have expired in the past 24 hours will still be notified at the time the daily expiry notifications are run.
14. Click the **OK** button.
15. Repeat Steps 10-14 for each card type requiring warning notification of expiry.

**Result**

The values you have set default as the threshold values for each of the two expiry types held on the Cardholder properties, as follows:

- Card expiry: The **Until** date and time on the **Cards** tab
- Competency expiry: The **Expires** date and time on the **Competencies** tab.

# Setting up Roles

## Introduction

Notifications are required to be sent to Cardholders, supervisors, managers, or administrators/operators for the cases of card expiry and competency expiry. Roles are therefore required to define the relationships between Cardholders - to route a notification to the appropriate person.

This procedure is split into two parts, as follows:

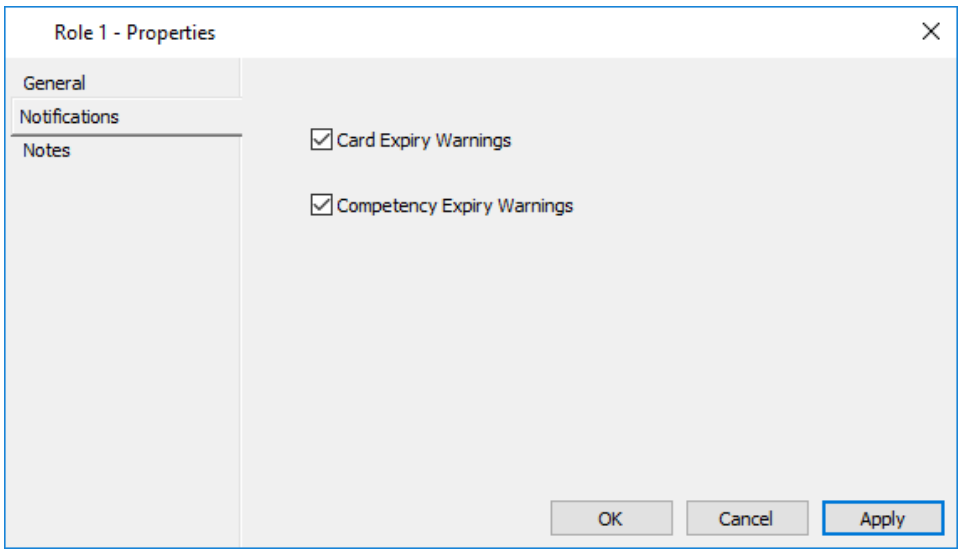
- Creating Roles, and
- Assigning Cardholders to the Roles

## Procedure

### *Creating a Role*

**Note:** Operators require either the "Edit Site" or "Edit Role Definitions" privilege to create, edit or delete a Role.

1. Click **Manage** from the menu bar, then **Roles**.
   The **Role** List Window opens (in grid view).
2. **Right click** and select **New...Role**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
   **Note:** Examples for the **Name** are Supervisor, HR Manager, Administrator.
4. Click the **Notifications** tab.




The options on this tab allow Cardholders in this Role to be notified of pending Card and/or Competency expiries for their staff, via email.

5. Both checkboxes are enabled (checked) by default.
   Leave enabled the checkbox(es) required for this Role, deselect the checkboxes that are not required for this Role.

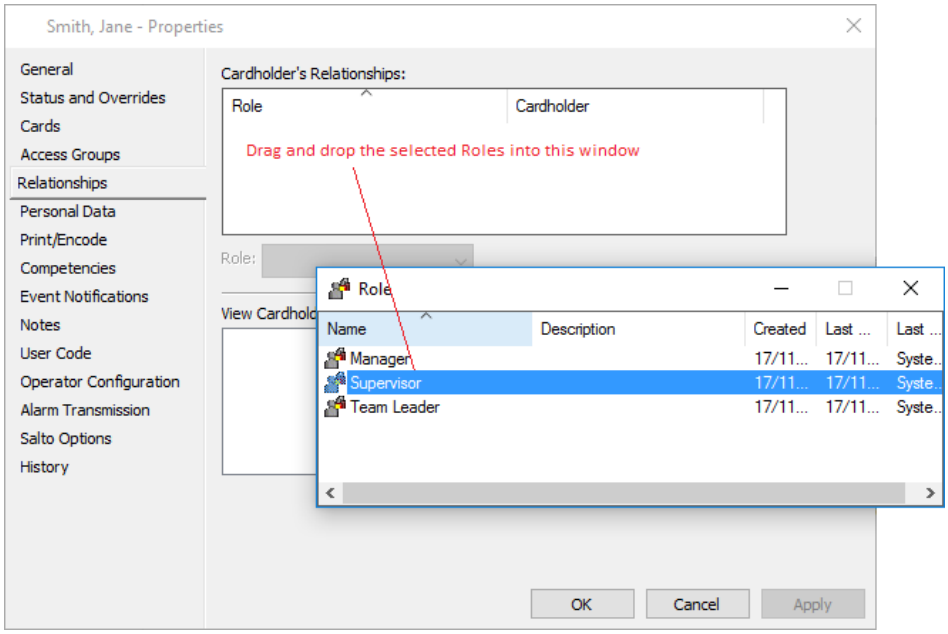
**Note:** The **Cardholder Related Events** checkbox is new in the Personalised Notifications feature. When ticked, the event notifications sent to the Cardholder are also sent, for example, to the Cardholder's supervisor, (i.e. the filter(s) belonging to the Cardholder do not need to belong to the supervisor, or whomever the additional recipient is).

6. Click the **Notes** tab if you want to add a note(s) about this Role. For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
7. Click the **OK** button to exit and save this Role.

### *Assigning Cardholders to Roles*

Cardholders can either be assigned to Roles manually or by using the bulk change feature. This procedure describes the manual method. If you require the bulk change method, refer to ***Assigning Cardholders to Roles via Bulk Change*** (next) for the procedure.

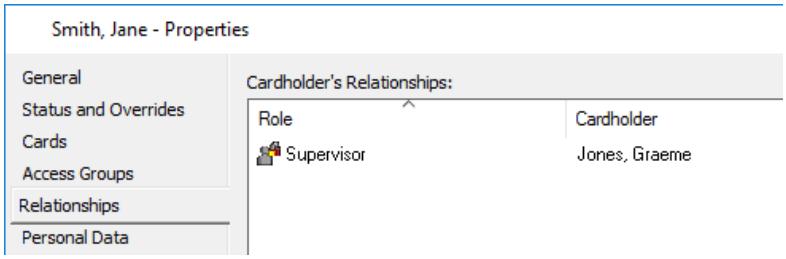
8. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
9. Locate, and highlight, the cardholder to assign the Role to.
10. **Right click** and select **Properties**.
11. Click the **Relationships** tab.
12. From the **Role** List Window, select those Role(s) you want to assign to this Cardholder.
    Drag and drop them into the **Cardholder's Relationships** grid on the **Relationships** tab.




**Note:** Multiple Roles can be assigned to a Cardholder, (e.g. each Cardholder can have one Supervisor, one Card Administrator, one Manager).

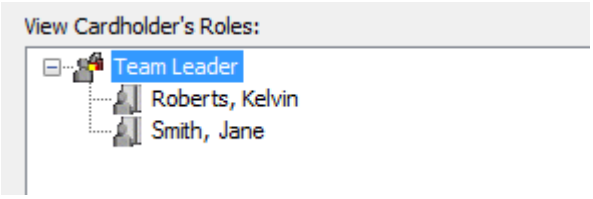
13. Click on the Role so it is highlighted.
    The **Role** field becomes enabled.

14. Drag and drop the Cardholder who fills this Role from the **Cardholder** List Window onto the Role in the **Cardholder's Relationships** grid. *For example:*
    Graeme Jones is Jane Smith's Supervisor, so Graeme Jones is dragged and dropped onto the Supervisor Role in the grid.

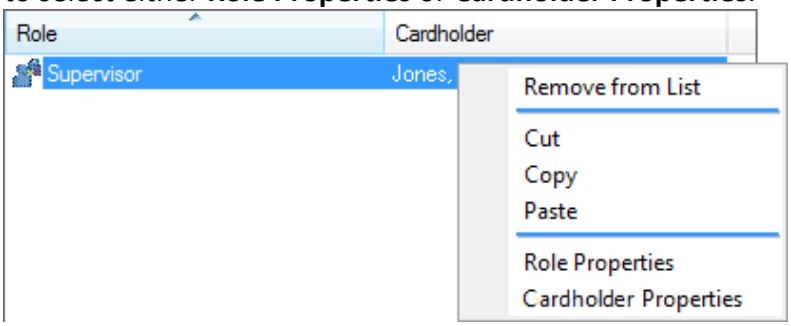



**Notes:**

- The **View Cardholder's Roles** grid on this screen displays a "read-only" view of any Roles that this Cardholder fills, and which Cardholders the Role is filled for. Click the ⊞ beside a Role to expand the list of Cardholders below it.
  *For example:*
  This Cardholder is a Team Leader for Jane Smith and Kelvin Roberts.




- A Role's property pages and/or Cardholder's property pages can be opened from this window, by either:
  - double-clicking on the Role or Cardholder in the grid, or
  - right-clicking on the Role. A context menu displays, with the option to select either **Role Properties** or **Cardholder Properties**.




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.

    **Note:** Ensure any Cardholder that fills a Role for other Cardholders has an email Personal Data Field (PDF) entered on the **Personal Data** tab of their properties. The email PDF must also be enabled for Notifications.

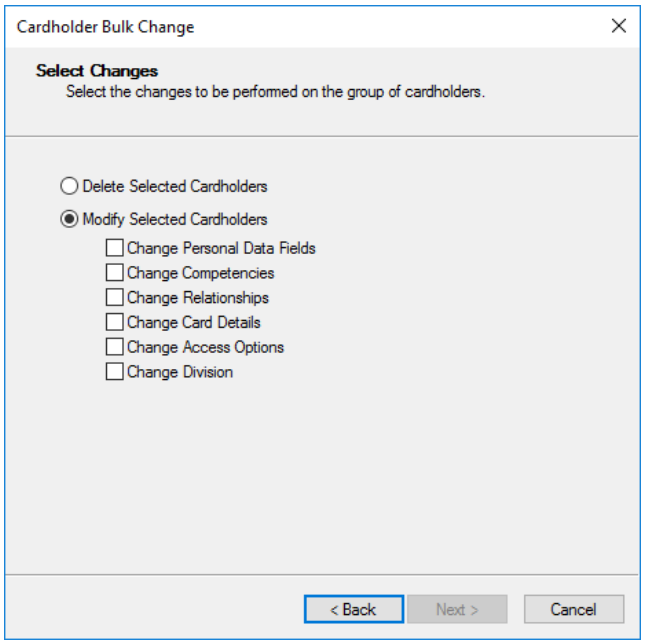
# Assigning Cardholders to Roles via Bulk Change

## Introduction

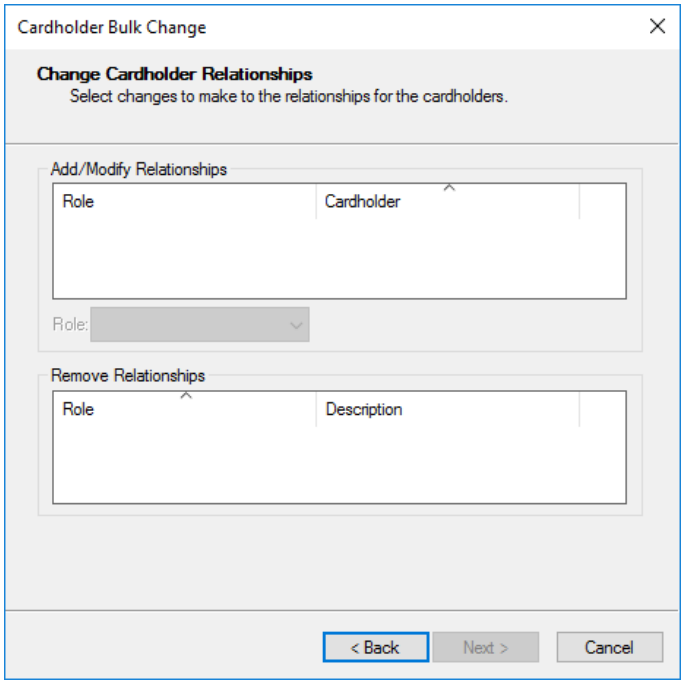
This procedure describes how to initiate a bulk change of multiple cardholder role relationships in Command Centre. To perform this procedure operators need both the "Bulk Change" and "Edit Cardholders" operator privileges. In addition, operator's need sufficient divisional and other privileges to carry out each individual change listed within a bulk change.

## Procedure

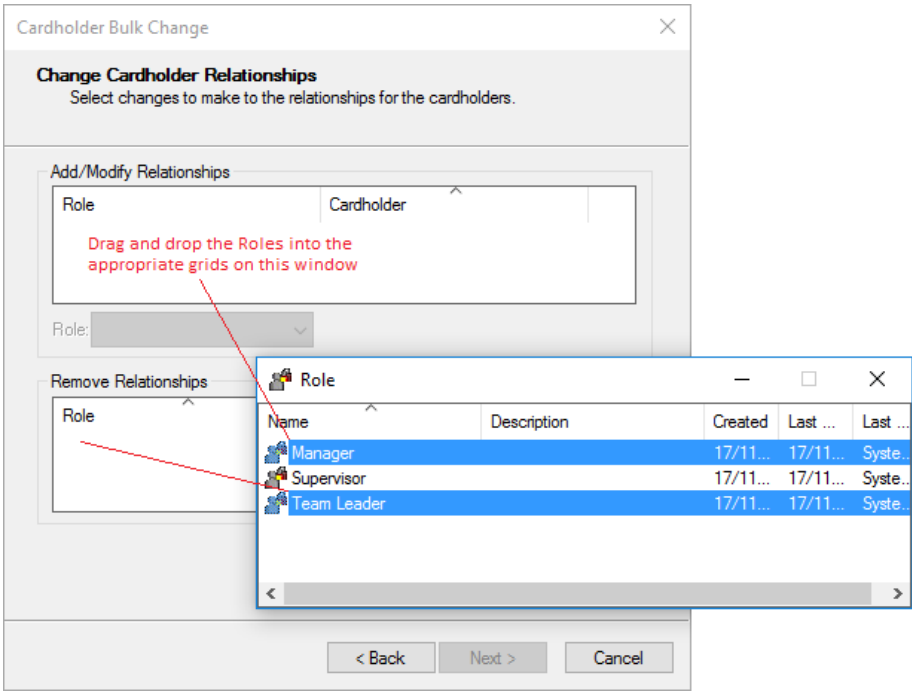
1. Perform Steps 1 - 4 of the Initiating a new Cardholder Bulk Change procedure and then go to Step 2 of this procedure.
   **Notes:**
   - These steps cover selecting all the cardholders or Access Groups that require changing, and placing them onto the "Select Cardholders or Access Groups" screen of the Cardholder Bulk Changes Wizard.
   - The **Copy all cardholders** feature, which allows a simple change for all cardholders, can be used here. You can copy all cardholders currently reporting to a person in a role, from his/her **Relationships** tab. This is useful when a person in a role leaves and you want to copy the people currently reporting to them to a new person, via a bulk change. See ***Copying all cardholders under a Role*** (next) for the procedure.
2. Click the **Next** button.
   The "Select Changes" screen of the Cardholder Bulk Changes Wizard displays.



3. Click the **Modify Selected Cardholders** radio button, and tick the **Change Relationships** checkbox.
4. Click the **Next** button.
   The "Change Cardholder Relationships" screen of the Cardholder Bulk Changes Wizard displays.




   This screen allows you to select changes to make to the relationships for the cardholders.
5. Click **Manage** from the menu bar, then **Roles**.
   The **Role** List Window opens.
6. Select the Roles that need adding to and/or deleting from the cardholders, and drag and drop them into the appropriate grids on this screen of the Wizard, then close the **Role** List Window.




**Notes:**

- In the "Add/Modify Relationships" section of this screen, Roles can be added to the grid using drag-and-drop, and then cardholders can be added using drag-and drop or the Cardholder drop-down list.
  Roles and Cardholder values can be changed using the applicable drop-down list, prior to processing the bulk change.
- If the Bulk Change action is to 'add' a relationship record to a cardholder for a Role that is already filled, then the result will effectively be a change to the cardholder held against the role.
- All Roles added to a cardholder, must be accompanied with a populated cardholder filling that role, (i.e. a Role cannot be added that is 'blank').
- Removing Relationships is achieved using drag-and-drop of the Role into the grid and processing of the Bulk Change, to remove the role and cardholder relationship record from each cardholder selected for the process.

7. Click the **Next** button.
8. Return to the ***Initiating a new Cardholder Bulk Change*** procedure and perform Steps 28 - 31 to complete the bulk change.

## Copying all Cardholders under a Role

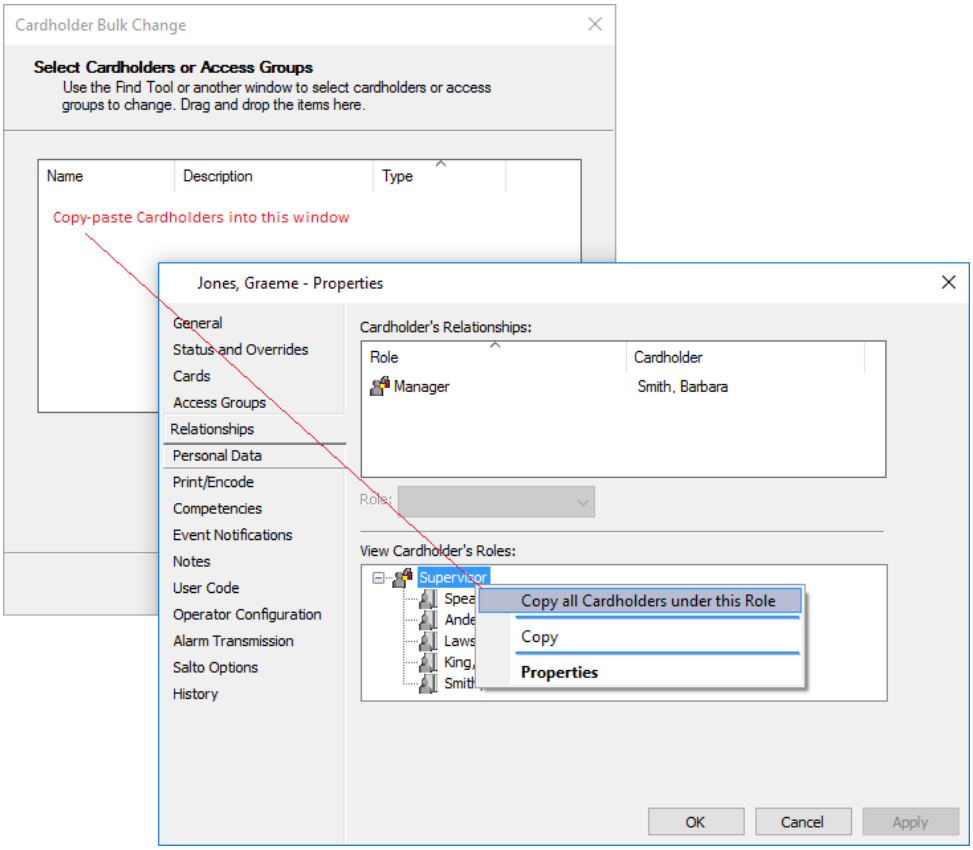
### Introduction

The **Copy all cardholders** feature allows you to easily select all cardholders that have a particular cardholder filling a role, and be able to drag-and-drop or copy-paste into the Cardholder Bulk Changes Wizard, to allow a simple change for all cardholders.

*For example:*
Graeme Jones is currently the Supervisor of 46 staff. However, Graeme is leaving and Barbara Smith is taking over his role of Supervisor. Rather than individually dragging and dropping all 46 cardholders into the Cardholder Bulk Changes Wizard so their Supervisor can be changed, the **Copy all cardholders** feature can be used.

### Procedure

1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** List Window opens (in grid view).
2. **Right click** and select **New...Cardholder Bulk Change**.
   The "Select Cardholders or Access Groups" screen of the Cardholder Bulk Changes Wizard displays.
3. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
4. Locate, and highlight, the cardholder in the role.
5. **Right click** and select **Properties**.
6. Click the **Relationships** tab.
7. Highlight the applicable Role, (e.g. Supervisor), within the **View Cardholder's Roles** grid.




8. **Right click** and select **Copy all Cardholders under this Role**.
9. Move the cursor to the grid on the "Select Cardholders or Access Groups" screen of the Cardholder Bulk Changes Wizard.
10. **Right click** and select **Paste**.
    All the Cardholders in the list below the Role appear in the "Select Cardholders or Access Groups" screen of the Cardholder Bulk Changes Wizard.
11. Go to the Initiating a new Cardholder Bulk Change procedure and perform Steps 5 - 31 to complete the bulk change.

## Result

A Cardholder Bulk Change has been initiated.

## Notification Examples

### Introduction

This topic provides three different scenarios, and the configuration required to set up Notifications.

### Example 1

For the Security Manager to receive all Critical alarms 24 hours per day, as well as all Door Open Too Long alarms during working hours only (both via SMS and Email), configure the following:

1. Set up the email server details on the **Outgoing Email** tab of the Server Properties to enable outgoing emails.
2. Set up the SMS details on the **SMS Notifications** tab of the Server Properties to enable outgoing SMS.
3. Create a **Notification Filter** (named something like "Critical Alarms"), and on the **Notifications** tab:
   - set "Include all Events at or above priority:" to Critical Priority
   - ensure the "Include events within all Event Sources" radio button is selected.
4. Create another **Notification Filter** (named something like "Door Open Too Long"), and on the **Notifications** tab:
   - do not set a minimum priority level
   - select the "Door Open Too Long" Event Group/Type.
5. Create a **Notifications Schedule** (named something like "Working Hours Notifications"), and set the Notifications Enabled times between 8:30am and 5:00pm.
6. Open the Security Manager's cardholder properties, and on the **Event Notifications** tab:
   - drag and drop the two Notification Filters created in Steps 3 and 4.
   - drag and drop the "Working Hours Notifications" schedule (created at Step 5) against the "Door Open Too Long" Notification Filter.
     **Note:** Since the "Critical Alarms" Notification Filter is required 24x7, there is no need to have a schedule associated with it, (i.e. no schedule means the same as "always enabled").
   - ensure the Notification Method is set to "SMS" alongside both of the filters. Repeat the previous two bullet points and ensure the Notification Method is set to "Email" alongside both of the filters.
   - set the **Current Event Notification Status** to ENABLED.

On the **Personal Data** tab, ensure there is an "Email" PDF and "Mobile" PDF setup correctly, and that the **Notifications** check boxes are ticked alongside these.

**Example 2**

For the HR Manager to receive email expiry warning notifications for all cardholders that have a card or competency expiry due, configure the following:

1. Set up the email server details on the **Outgoing Email** tab of the Server Properties to enable outgoing emails.
2. For the relevant Card Types and Competencies, on the **Setup** tabs:
   - set the **Advance notice period**, and
   - ensure the related "Enable card/competency expiry notification" checkboxes are ticked.
3. Create the "HR Manager" role, and on the **Notifications** tab enable the Card and Competency Expiry Warnings for this role.
4. Add the "HR Manager" role to each cardholder (on each cardholder's **Relationship** tab), and populate with the name of the HR Manager.
   **Note:** This can be achieved easily for large numbers of cardholders using ***Cardholder Bulk Change*** (on page 38-3).
5. Open the HR Manager's cardholder properties, and on the **Personal Data** tab ensure that:
   - there is an "Email" PDF setup correctly, and
   - the **Notifications** checkbox is ticked.

**Example 3**

For John Smith to receive an SMS for his card expiry warning notifications, configure the following:

1. Set up the email server details on the **Outgoing Email** tab of the Server Properties to enable outgoing emails.
2. Set up the SMS details on the **SMS Notifications** tab of the Server Properties to enable outgoing SMS.
3. For the relevant Card Types, on the **Setup** tab:
   - set the **Advance notice period**, and
   - ensure the "Enable card expiry notification" checkbox is ticked for each card type.
4. Open John Smith's cardholder properties, and on the **Personal Data** tab ensure that:
   - there is a "Mobile" PDF setup correctly, and
   - the **Notifications** checkbox is ticked.

**Example 4**

For a Cardholder within an Access Group to receive their own Access Denied alarms via email, configure the following.

**Note:** Cardholder records must each have an email PDF set up correctly and the **Notifications** checkbox must be ticked. You can do this by navigating to **Manage** > **Cardholders** and reviewing the **Personal Data** tab.

1. Set up the email server details on the **Email Notifications** tab of the Server Properties page to enable outgoing emails.
2. Create a Notification Filter called, for example, ‘Access Denied Alarms’.
3. From the **Notifications** tab:
   - Select the 'Access Denied' event group.
   - Ensure the **Include events within all Event Sources** radio button is selected.
4. On the **Personalised Notifications** tab, drag and drop the Access Group into the grid.

   **Note:** Selecting a schedule for this Access Group is optional; no schedule means the same as ‘always enabled’.
5. Ensure the Access Group’s **Notification Method** is set to ‘Email’.

**Example 5**

For a supervisor to receive Access Denied alarms via email, configure the following.

**Note:** For every person who you want to receive notifications (whether a supervisor receiving notifications related to their staff, or a Cardholder receiving their own notifications), their Cardholder records must each have an email PDF set up correctly and the **Notifications** checkbox must be ticked. You can do this by navigating to **Manage** > **Cardholders** and reviewing the **Personal Data** tab.

1. Complete Example 4 above.
2. Create a ‘Supervisor’ role.
3. Open the Properties of the Cardholder to whom you want to add this relationship.
4. Add the 'Supervisor' role to the **Relationship** tab, and drag and drop the Cardholder who is this Cardholder's supervisor onto the Role in the grid.
5. Drag and drop the 'Supervisor' Role into the bottom grid on the Notification Filter's **Personalised Notifications** tab.
6. Set the **Notification Method** for this Role to 'Email - Separate' or 'Email - CC' as required.

## Acknowledging alarms via SMS or email

### Introduction

This procedure allows an operator who receives an alarm SMS or email message, to acknowledge it remotely via SMS and/or email message response. Operators require the "Edit Alarm" privilege to acknowledge an alarm.

**Note:** Mobile Client users can use the Mobile Client to acknowledge Mobile Notifications.

### Procedure

Use the appropriate procedure below for the type of message you want to acknowledge:

***Acknowledging Email messages***

1. Select either **Reply** or **Reply with History**.
   **Note:** Either option for replying is acceptable as the Alarm ID is always in the subject line.
2. Type the letters **ACK** in the body of the email.
   **Note:** This is not case sensitive, as long as the letters are typed in sequence without spaces.
3. Select **Send**.

Example reply: **ACK**

***Acknowledging SMS messages***

1. Select **Reply**.
2. Type in the Alarm ID number.
   **Note:** Only the numbers need to be entered. There is no need for the "ALM" characters.
3. Enter a space and type in the letters **ACK**.
   **Note:** This is not case sensitive, as long as the letters are typed in sequence without spaces.
4. Select **Send**.

Example reply: **36 ACK** (where 36 is the Alarm ID).

**Notes:**

- Set the Event Group "Unrecognised Sender" to "Log an event" on the **Event Defaults** tab of the Server Properties, while testing or troubleshooting alarm acknowledgements via email or SMS. This will log an event if an incoming **ACK** cannot be processed for some reason.
- If your sites Bulk SMS Service Provider attaches the outbound message to the incoming acknowledgement, then the Alarm ID is not necessary, (e.g. behaves like email. **ACK** only is required).

**Result**

Command Centre does the following:

- Receives the response and correlates it to the outbound event/message. **Note:** If correlation cannot be determined, an event is raised.
- Processes the inbound message and acknowledges the alarm.
- Logs an acknowledgement response/inbound message details.

# Chapter 36: Operator Groups

## Introduction

An Operator Group is a group of cardholders who are authorised to use the Command Centre software. Each Operator Group defines the privileges its members have as Command Centre operators, (e.g. view only access, editing ability, site configuration ability, etc.). The privileges only apply within the Divisions assigned to that Operator Group. Operator Groups generally represent roles that an operator can have, (e.g. "Monitoring Alarms for Buildings 1 and 2").

**Note:** An operators system view can be changed to include all, some or only one of the Operator Groups they belong to. System view is limited to the site items, cardholders, Personal Data Fields (PDFs) and operator privileges assigned to them from the selected Operator Groups. See ***Restricting System View*** (on page 2-9) for further details.

## Configuring Operator Groups

An operator needs to have the "Edit Operators" privilege in at least one Division to create and configure operators and Operator Groups.

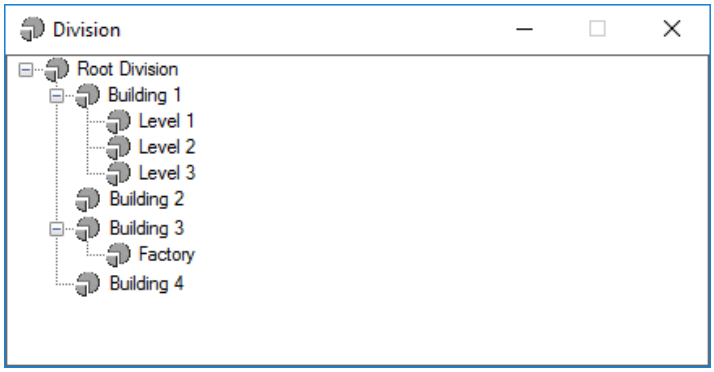
The "Edit Operators" privilege within a Division allows an operator to create Operator Groups in that Division and assign any (or all) operator privileges to that group.

An operator configuring an Operator Group will only be able to:

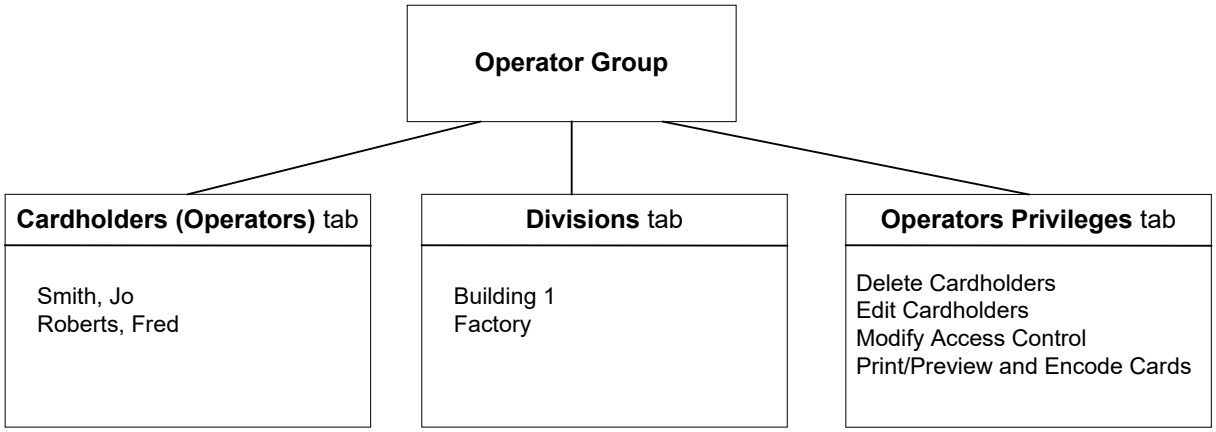
- assign cardholders to the Operator Group if they have "View Cardholders" or "Edit Cardholders" privilege in the cardholder's Division.
- assign or remove Divisions configured in the Operator Group if they have "Edit Operators" privilege in that Division.
- assign or remove Personal Data Field privileges configured in the Operator Group if they have "View Personal Data Definitions" or "Edit Personal Data Definitions" privilege in the Personal Data Field's Division.

## Example: How Operator Groups work

A site's divisional hierarchy is as follows:

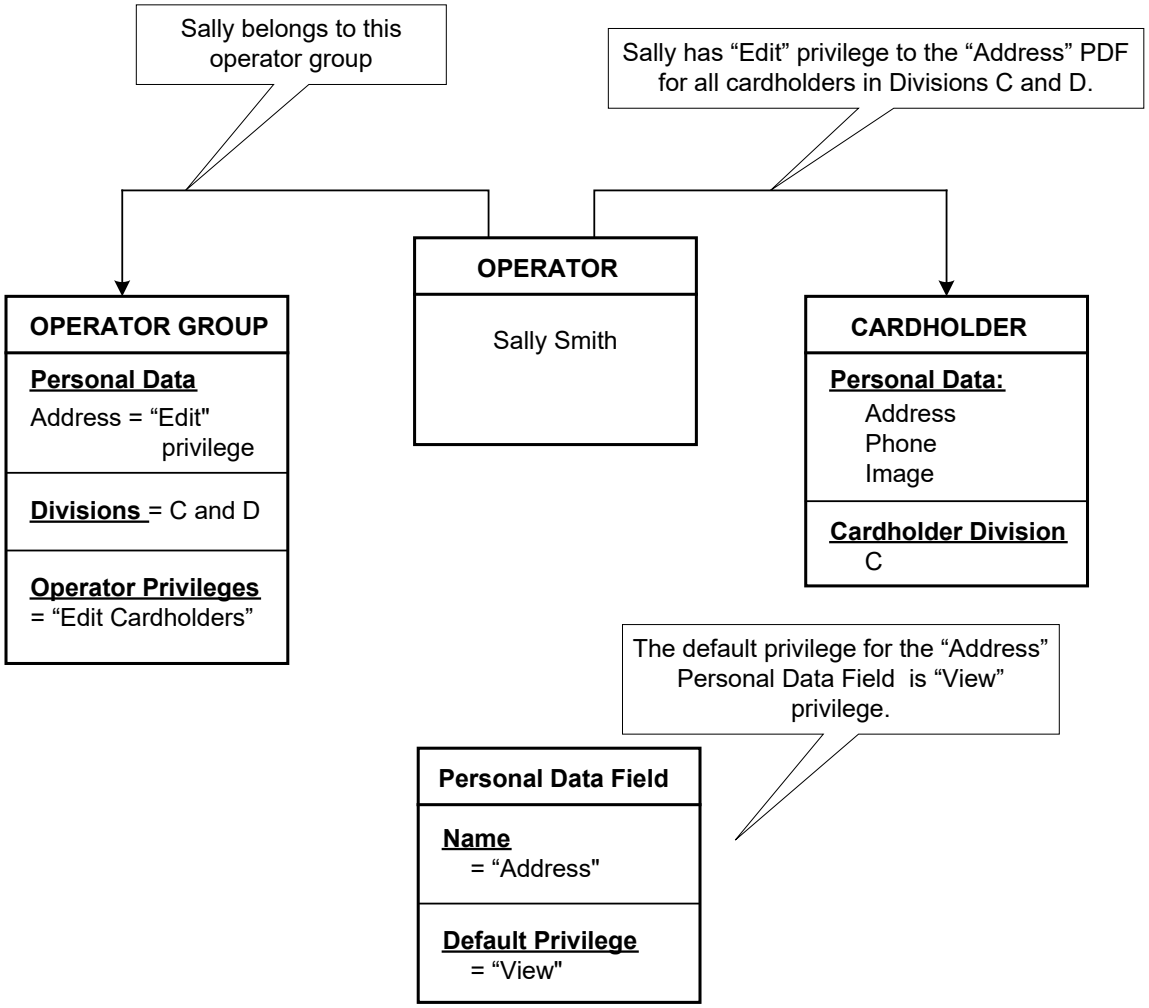



An Operator Group has the following cardholders (operators), Divisions and operator privileges configured:




This means Jo Smith and Fred Roberts can "Delete Cardholders", "Edit Cardholders", "Modify Access Control" and "Print/Preview & Encode Cards" in the "Building 1" or "Factory" Divisions. As the "Building 1" Division has three children Divisions, (i.e. Level 1, Level 2 and Level 3), they also have the same privileges for these Divisions.

### Assigning Personal Data Field Privileges




In the example above, Sally Smith belongs to an Operator Group that gives her "Edit" privilege to the "Address" Personal Data Field for all cardholders in Divisions C and D. This Operator Group privilege overrides the default "View" privilege. Other operators who do not have a privilege for the "Address" Personal Data Field assigned to them from one of their Operator Groups, will only be able to view the content of the "Address" Personal Data Field.

An operator inherits the Personal Data Field privileges assigned to the Operator Groups that they belong to. The PDF privileges only apply to cardholders that belong to one of the Operator Group's Divisions (as configured in the **Divisions** tab).

If an operator belongs to more than one Operator Group and each assigns a privilege for the same PDF within the same Division, then the least restrictive PDF privilege is the one they inherit. For example, if one Operator Group gives the operator "View" privilege to a Personal Data Field for cardholders in Division C, but another Operator Group gives the same operator "Edit" privileges to that Personal Data Field for cardholders in Division C, then it is the "Edit" privilege that they actually receive.

If operators do not belong to any groups that assign Personal Data Field privileges for a particular Personal Data Field, then it is the default privilege (as specified in the Personal Data Field properties) that they inherit.

An operator's Personal Data Field privileges are assigned by Division, so it is possible to allow an operator to edit a particular Personal Data Field for cardholders in one Division, but only view the same Personal Data Field for cardholders in other Divisions.

The Personal Data Field privileges are also subject to the following:

- The operator has to have at least "View Cardholders" privilege in the cardholder's Division before they can view any Personal Data Fields for that cardholder.
- The operator has to have "Edit Cardholders" privilege in the cardholder's Division before they can edit any Personal Data Fields for that cardholder.
- The cardholder has to have been assigned the Personal Data Field through one of the Access Groups that they belong to.

## Setting up Operator Groups

### Introduction

This procedure is split into two parts, as follows:

- Creating an Operator Group,
  (i.e. providing the minimum information required to create a new Operator Group)
- Configuring an Operator Group,
  (i.e. linking the various components to it - Divisions, Privileges, Cardholders and Personal Data Fields are the components of an Operator Group).

You can create a new Operator Group, then configure it at a later stage, once you have set up the necessary components for it.

### Procedure

***Create the Operator Group***

1. Click **Manage** from the menu bar, then **Operator Groups**.
   The **Operator Group** List Window opens (in grid view).
2. **Right click** and select **New...Operator Group**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
   **Note:** The Operator Group's Division controls which operators can view or edit the Operator Group. It does not affect which Divisions the privileges in this group apply to.
4. Click the **Apply** button, and the Operator Group is created.
   The rest of this procedure allows you to fully configure the Operator Group.

***Configure the Operator Group***

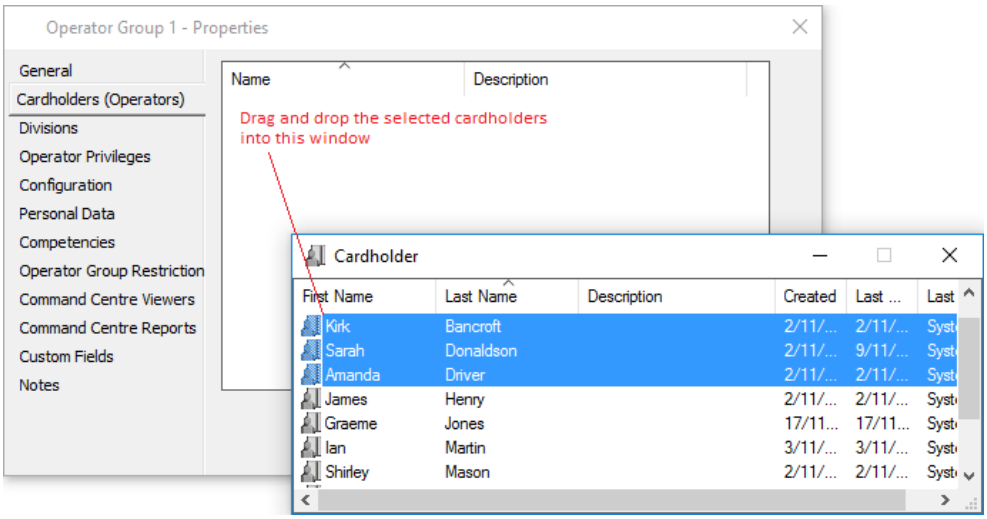
5. Ensure the following components have already been set up:

   *Divisions*
   Refer to **Setting up System Division** (on page 9-3).

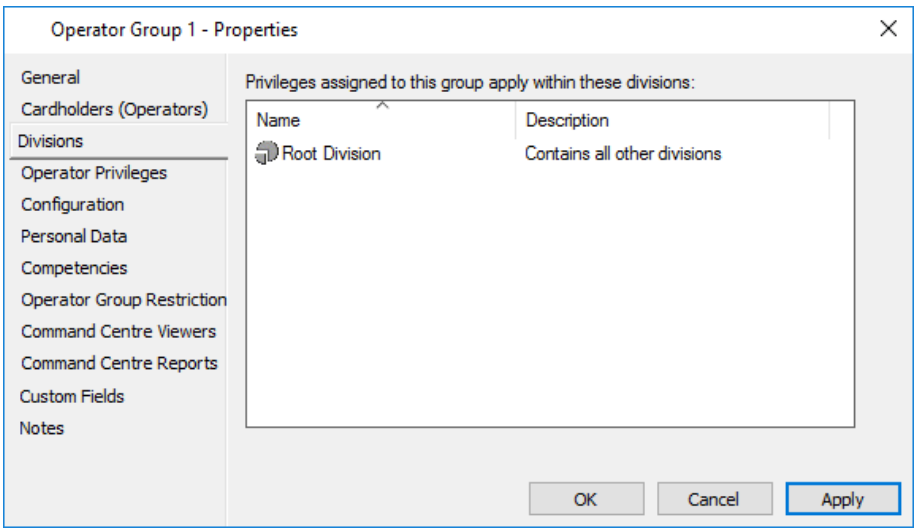
   *Cardholders*
   Refer to **Add new cardholder** (on page 32-2).

   *Personal Data Fields*
   Refer to **Creating a new Personal Data Field** (on page 33-2).
6. Click the **Cardholders (Operators)** tab.

7. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
8. Select those cardholder(s) to belong to the new Operator Group.
   Drag and drop them into the **Cardholders (Operators)** tab.



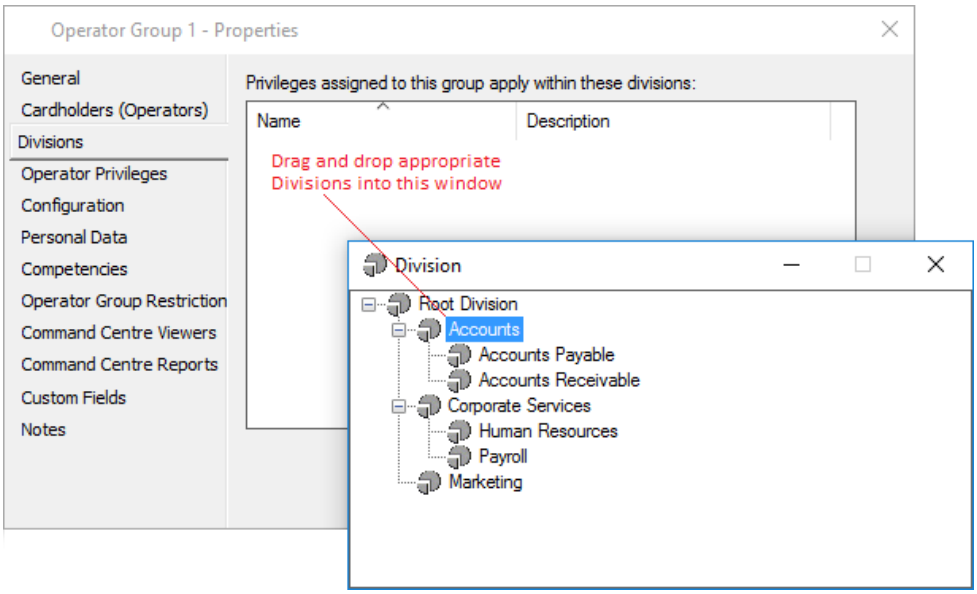

9. Close the **Cardholder** List Window.
10. Click the **Divisions** tab.
    This tab dictates where you can use the operator privileges you select for this group (in Step 15). By default, the Division automatically assigned on the **General** tab is assigned to this tab also.



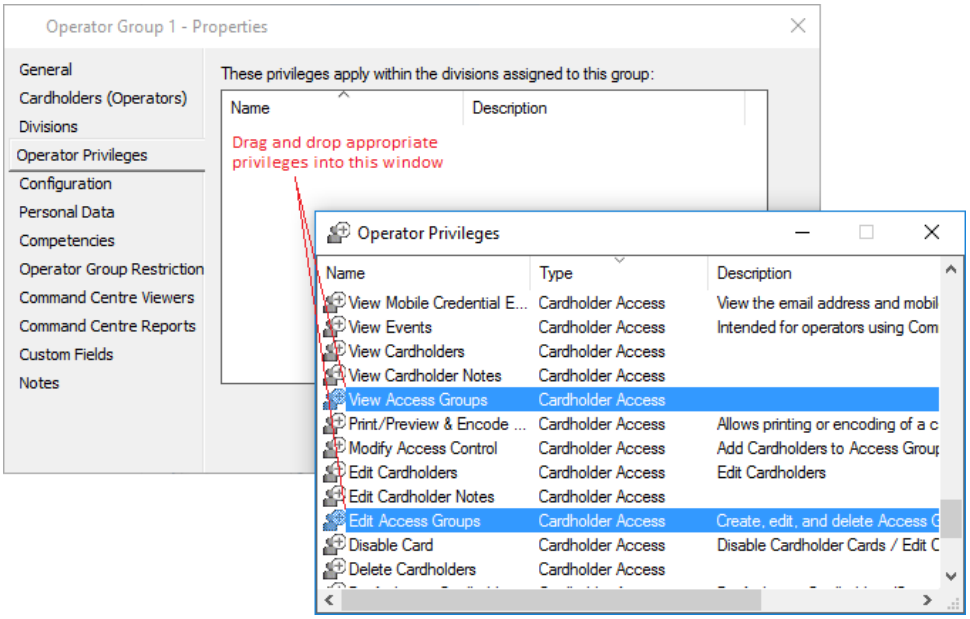

11. Do you require the privileges assigned to this group to apply to **all** Divisions?

| If... | then... |
|---|---|
| yes | leave the "Root Division" in the grid, as all other Divisions will be included with it.<br>Go to Step 15. |
| no | right click on the "Root Division" and select **Remove from List**. |

12. Click **Configure** from the menu bar, then **Divisions**.
    The **Division** List Window opens.
13. Select those Division(s) this Operator Group conveys privileges for.
    Drag and drop them into the **Divisions** tab.
    **Note:**
    If a Division is selected, its child(ren) Divisions are automatically included also.

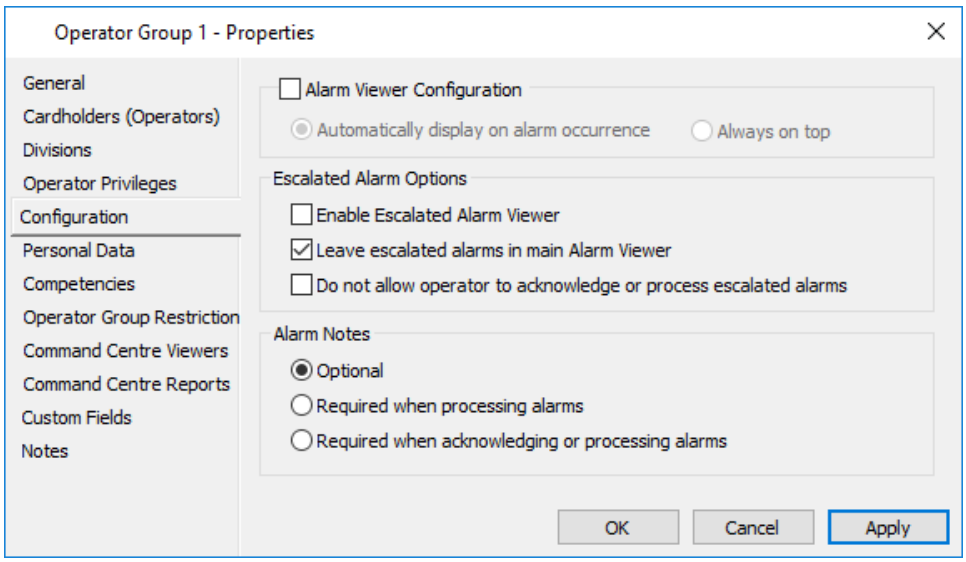



14. Close the **Division** List Window.
15. Click the **Operator Privileges** tab.
16. Click **Manage** from the menu bar, then **Operator Privileges**.
    The **Operator Privileges** List Window opens.
    Select those privileges appropriate for this Operator Group.
    Drag and drop them into the **Operator Privileges** tab.



**Note:** Operators may end up without the privileges required to see their own operator events. This happens when the Division used for events is different to the Division used to change items.

17. Close the **Operator Privileges** List Window.
18. Click the **Configuration** tab.




19. Do you wish to alter the behaviour of the Alarm Viewer window?

| If... | then... |
|---|---|
| yes | Check the **Alarm Viewer Configuration** checkbox.<br>Go to Step 20. |
| no | Leave the **Alarm Viewer Configuration** checkbox unchecked.<br>Go to Step 21.<br><br>**Note:** By leaving the checkbox unchecked, the Alarm Viewer will remain wherever it is placed by the currently logged on operator and will not automatically pop to the front of other windows. |

20. Click the appropriate radio button for the option you prefer.

**Automatically displays on alarm occurrence**
The Alarm Viewer will be opened, made visible and brought to the front of all other windows on the occurrence of any new alarm. With this option enabled you can not locate the Alarm Viewer off screen and the entire Alarm Viewer will be visible at all times.

**Always on top**
The Alarm Viewer will always be in front of all other windows. With this option enabled the entire Alarm Viewer will be visible at all times and you can not:
- minimise the Alarm Viewer, or
- locate the Alarm Viewer off screen.

21. The **Escalated Alarm Options** section of this screen allows you to set what will happen to escalated alarms.
    **Note:** The Escalated Alarm Viewer privileges are conveyed via an Operator Group, but are intended to be applied system-wide for an operator, (i.e. they are not divisionally based like most other privileges conveyed via an Operator Group). Hence, disabling the Operator Group from your system view will not affect these settings, (e.g. An operator belongs to multiple Operator Groups, all with different escalated alarm option settings. If the operator narrows their system view to one Operator Group whose settings do not enable the Escalated Alarm Viewer, it will ignore that and still display the Escalated Alarm Viewer if one of the Operator Groups has that setting checked).

    Do you want escalated alarms to display in a separate window from the main Alarm Viewer?

    | If... | then check the... |
    |---|---|
    | yes | **Enable Escalated Alarm Viewer** checkbox. The Escalated Alarm Viewer will be accessible from the **Monitor** menu, along with the main Alarm Viewer. |
    | no | **Leave escalated alarms in main Alarm Viewer** checkbox. Any escalated alarms will remain in the main Alarm Viewer with non-escalated alarms. |

    **Note:** By checking both options you can have escalated alarms appear in both the main Alarm Viewer as well as the Escalated Alarm Viewer.
22. Check the **Do not allow operator to acknowledge or process escalated alarms** checkbox if required for operators in this group.
    **Note:** If checked, the **Acknowledge** and **Process** buttons will be disabled on the Alarm Details property page for escalated alarms.
23. Do you wish to configure alarm note options?
    If **no**, then go to Step 24.
    If **yes**, then click the appropriate radio button for the option you require.

    **Optional** *(Option A)*
    The privileged operator can optionally select alarm note(s) before processing or acknowledging an alarm.

    **Required when processing alarms** *(Option B)*
    The privileged operator must select one or more alarm notes in order to process, or bulk process alarms at a priority level that is equal to or higher than the alarm notes priority threshold.

    **Required when acknowledging or processing alarms** *(Option C)*
    The privileged operator must select one or more alarm notes in order to acknowledge, process or bulk process alarms at a priority level that is equal to or higher than the alarm notes priority threshold.

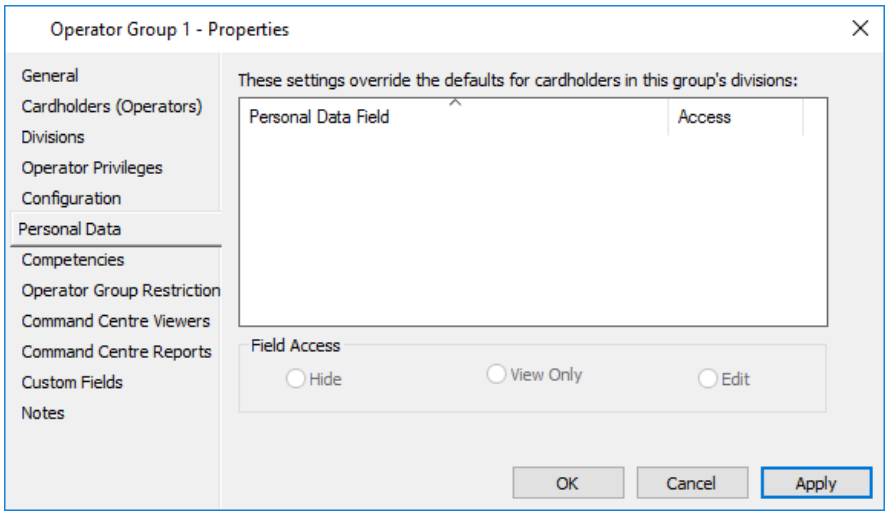
    **Notes:**
    - Where an alarm monitoring operator is a member of more than one Operator Group then the following rules apply:

1. IF at least one Operator Group to which the operator belongs is set to *Option A*, THEN alarm notes are optional to Acknowledge, Process or Bulk Process.
2. IF at least one Operator Group to which the operator belongs is set to *Option B*, THEN alarm notes are mandatory to Process or Bulk Process and optional to Acknowledge.
3. IF all Operator Groups to which the operator belongs are set to *Option C*, THEN alarm notes are mandatory to Acknowledge, Process or Bulk Process.

These rules are given in order of precedence, therefore an operator that belongs to three operator groups each of which has a different option setting *(A, B, C)* will not be forced to enter alarm notes for any alarms since Rule 1 takes precedence over Rule 2 and Rule 3. This is based on the assumption that an operator that is forced to enter alarm notes is likely to have been given this restriction because they are considered to be less reliable than those who are not forced.

- If none or only one alarm note has been configured in the Server properties, then the 'Alarm Notes' option will not be enabled.

24. Click the **Personal Data** tab.




By default, this tab will not be populated with any Personal Data Fields (PDFs). Instead, this Operator Group will get the privileges for PDFs that are assigned at the PDF level. If you want to override the default privilege to something else, you can drag PDFs onto this tab.

The level of operator privilege to view or edit cardholder information stored in a cardholder's Personal Data is determined for individual PDFs. The PDF privileges only apply to cardholders in the Operator Group's Divisions (as configured on the **Divisions** tab).

The default operator privilege for each PDF is determined when the properties of the PDF are configured. The default operator privilege can be overridden for each PDF by selecting a new option.

25. To determine the level of operator privilege for each of the PDFs, highlight the PDF and then click the appropriate radio button for it. To assign a privilege for a PDF, drag and drop the PDF into the **Personal Data** tab.

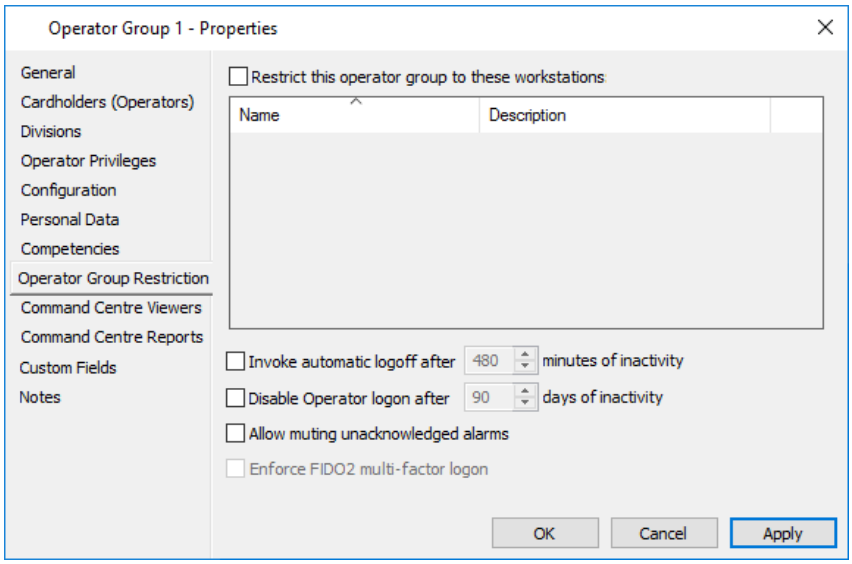
Click on the PDF to select it, then choose one of the following privileges.

| Privilege | Description |
|---|---|
| Hide | Operators will not see the cardholder information recorded for this PDF, for cardholders in this group's Divisions. |
| View Only | Operators will be able to view cardholder information for this PDF, for cardholders in this group's Divisions. |
| Edit | Operators will be able to enter, view, change and delete cardholder information for this PDF, for cardholders in this group's Divsions. |

**Notes:**

- There are separate Operator Privileges to view and edit the properties for PDFs. If operators do not have the "View Personal Data Field" or "Edit Personal Data Field" operator privilege (as listed in the **Operator Privileges** tab), and an individual PDF is 'hidden' from their view, they will not even be aware of its existence.
- If Operator Groups and PDFs are being created at the same time, the list of PDFs that will be saved into the new Operator Group will only include those that were "Applied" before the Operator Group was created. To ensure all PDFs are included in the list either create all PDFs first, or check Operator Groups as you create them, and drag any new PDFs in.
- To remove a PDF privilege assigned in this Operator Group, **right click** on the PDF and select **Remove from List**.

26. Do you want to override the default access of a competency for the operators in this Operator Group?
    If **yes**, refer to ***Overriding Operator Group Competencies*** (on page 53-17) for the procedure.
    If **no**, go to Step 27.
27. Click the **Operator Group Restriction** tab.




**Note:** By default, the **Restrict this operator group to these workstations** checkbox is unchecked and the grid is disabled. This means that the

Operator Group is unrestricted and therefore its privileges are available for use at any workstations.

28. Do you want to restrict the workstations accessible to this Operator Group?
    If **yes**, go to Step 29.
    If **no**, go to Step 33.
29. Check the **Restrict this operator group to these workstations** checkbox. The grid is enabled.
    **Notes:**
    - Once this checkbox is checked, at least one workstation must be assigned to the grid before you can apply and save the changes.
    - 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.
30. Click **Configure** from the menu bar, then **Services & Workstations**. The **Services and Workstations** List Window opens.
31. Select those workstations you want to restrict this Operator Group to. Drag and drop them into the **Operator Group Restriction** tab.
32. Close the **Services and Workstations** List Window.
33. Do you want members of this Operator Group to be automatically logged off after a specified period of inactivity?

| If... | then... |
|---|---|
| yes | tick the **Invoke automatic logoff** checkbox and indicate the period of inactivity in the timebox. (Default = 60 minutes. Range = 1 minute - 1440 minutes, i.e. 24 hours)<br>See ***Automatic Logoff*** (on page 2-12) for a full explanation. |
| no | go to Step 34.<br>**Note:** By leaving the automatic logoff time as disabled, the Operator Group's automatic logoff time will be the same as the Server's value, (i.e. on the **Operator Defaults** tab of the Server Properties). |

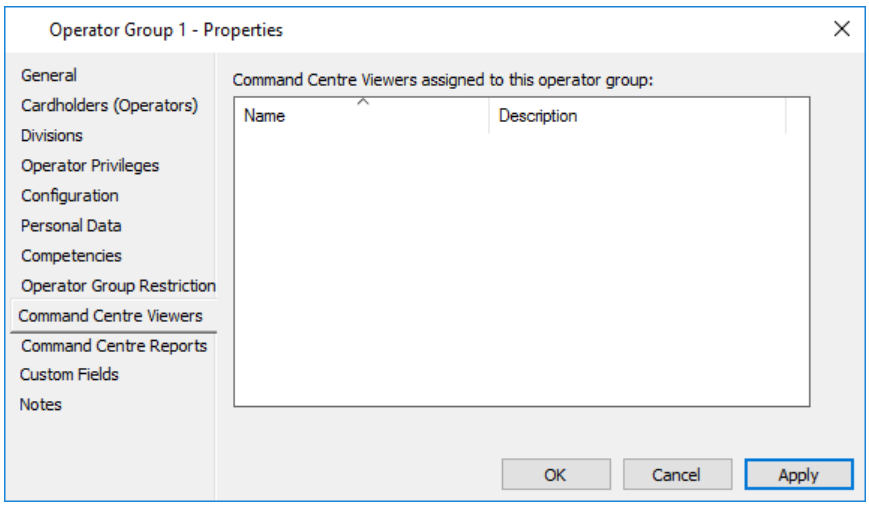
34. Do you want members of this Operator Group to have their operator logon automatically disabled after not logging on for a specified number of days?

| If... | then... |
|---|---|
| no | go to Step 35. |
| yes | tick the **Disable Operator logon** checkbox and indicate the number of days before logon is disabled in the timebox.<br>(Default = 90 days. Range = 1 day to 999 days)<br>**Notes:**<br>• If an operator is assigned to multiple operator groups, the largest number of days assigned to those operator groups will be the time used, this means if one of those operator groups does not |

| If... | then... |
|---|---|
| | have this restriction enable then the operator logon will not become disabled due to not logging on.<br>• It is recommended that only non-administrative operator groups be configured to be disabled due to inactivity. If all operators with the "Edit Operators" privilege can become disabled due to inactivity and the System operator is disabled (as recommended), there is a danger that the ability to properly manage the site may be lost.<br>• Scheduled Macros or Reports use the operator's credentials, that last modified it. When these Macros or Reports are run it counts as activity, similarly, if this operator became locked due to inactivity, the scheduled Macro or Report will fail to run. |

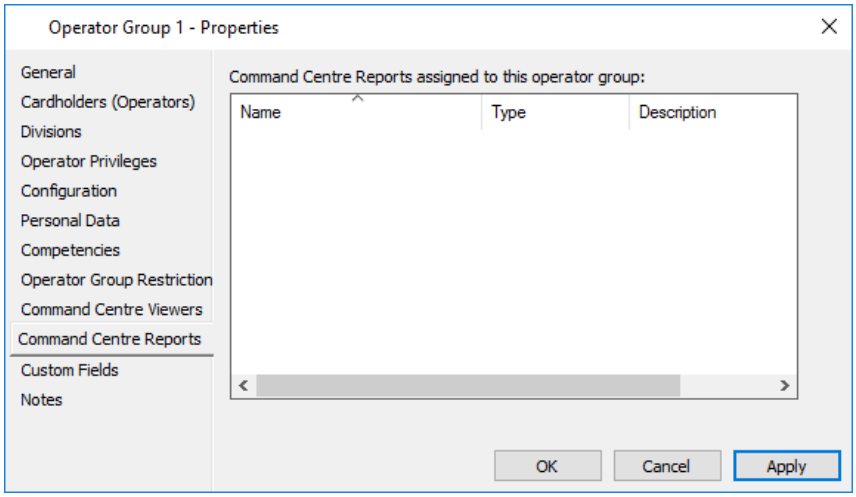
35. If you want Command Centre operators to be able to mute unacknowledged alarms (by pressing the <**F9**> key), select the **Allow muting unacknowledged alarms** checkbox. To prevent operators from muting unacknowledged alarms, deselect the checkbox.
    **Notes:**
    - An operator only needs to be in one Operator Group with this checkbox checked in order to mute unacknowledged alarms.
    - This checkbox does not prevent operators from silencing alarms via other methods such as turning down their workstation's volume.
36. The **Enforce FIDO2 multi-factor logon** checkbox will be disabled (greyed out) if FIDO2 Credentials have not been enrolled against cardholders. Configuration of FIDO2 Credentials is performed in Command Centre Client. For further information refer to the "FIDO2 Credentials" section in the *Command Centre Client User Guide*.

    **Note:** Command Centre will enforce that if any Operator Group has **Enforce FIDO2 multi-factor logon** enabled, that there must be at least one Operator who can logon to Command Centre with a FIDO2 credential. This will mean that the last Operator will fail to be disabled due to inactivity.
37. Click the **Command Centre Viewers** tab.



This tab is 'read-only' and displays all Viewers from Command Centre Client that are assigned to the Operator Group in alphabetical order.

38. Click the **Command Centre Reports** tab.




This tab is 'read-only' and displays all Reports from Command Centre Client that are assigned to the Operator Group in alphabetical order.

39. Click the **Custom Fields** tab if you want to add and assign a custom field value to this Operator Group. For further details regarding the **Custom Fields** tab, see ***Custom Fields*** (on page 6-81).
40. Click the **Notes** tab if you want to add a note(s) about this Operator Group.
    For further details regarding the **Notes** tab, see ***Notes*** (on page 6-85).
41. 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 Operator Group is created.

## Hints

*Editing and Deleting Operator Groups*
Refer to ***Editing items*** (on page 3-26) and ***Deleting items*** (on page 3-27) for procedures on how to edit and delete Operator Groups.
**Note:** The system will only allow the deletion of an Operator Group if all Operators (listed in the **Cardholders (Operators)** tab), are removed from the Operator Group first.

*Copy and paste*
An alternative to the drag and drop method is to use the copy and paste method.

*Cardholder (Operators) details*
The cardholders you added to this Operator Group (in Step 10) will now have details displayed in the **Operator Configuration** tab of their Cardholder Properties screen, (i.e. Logon Name and Operator Group Membership details).

# Configuring Operators

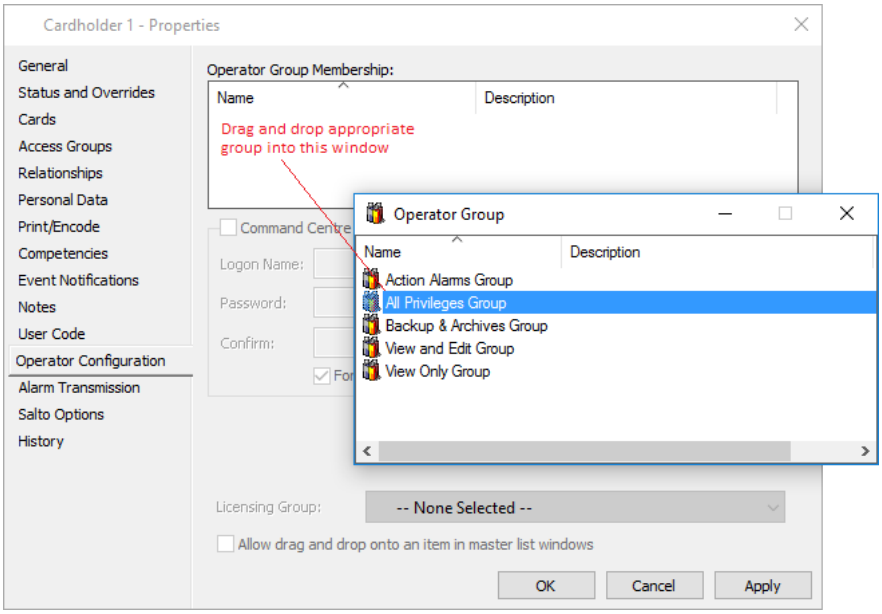
## Introduction

System administrators can set up cardholders as operators in Command Centre using the following procedure.

**Note:** Each person is unique in the Command Centre system. Whilst it is possible for people to have the same name, Command Centre ensures that each entity must have a unique username and password.

## Procedure

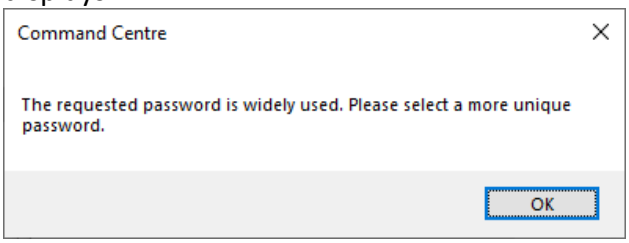
1. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens (in grid view).
2. Locate, and highlight, the Cardholder to edit.
3. **Right click** and select **Properties.**
4. Click the **Operator Configuration** tab.
5. Does the group the operator needs to be a member of appear in the **Operator Group Membership** grid?
   If **yes**, check the **Command Centre logon** checkbox and go to Step 9.
   If **no**, go to Step 6.
6. Click **Manage** from the menu bar, then **Operator Groups**.
   The **Operator Group** List Window opens.
7. Select the appropriate operator group for this cardholder, and drag and drop it into the **Operator Configuration** tab.



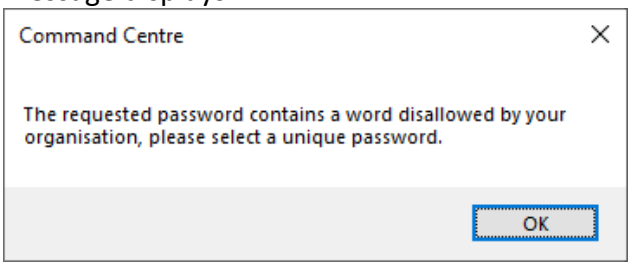

8. Close the **Operator Group** List Window.
9. The **Command Centre logon** section becomes enabled, and the **Logon Name** field is populated.
   The Logon Name is made up of the first letter of the operators First Name and their entire Last Name.

10. 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.

    **Notes:**
    - The **Force password change at next logon** checkbox is selected by default. This means that when the operator logs on for the first time the 'Password has expired' dialog will display, 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.
    - 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).
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.
12. Notify the operator what their Logon Name and Password are.

**Result**

An operator has been configured.
The first time the operator logs on they will be forced to change their password.

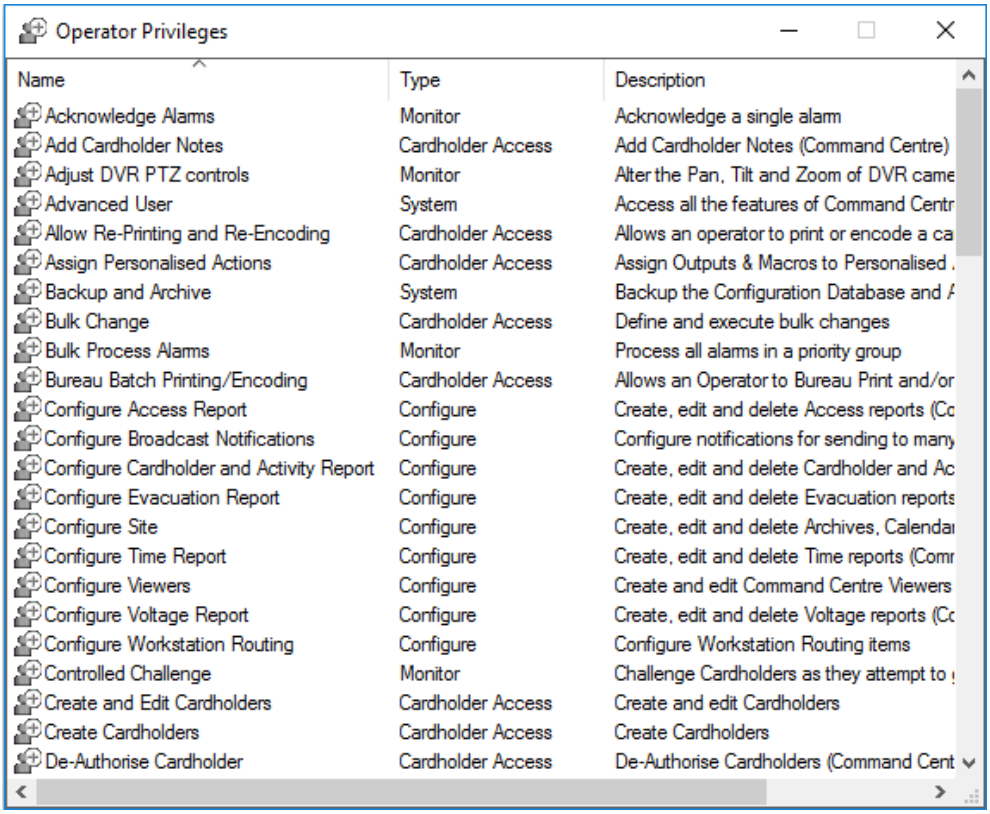
# Chapter 37: Operator Privileges

## Introduction

Operator Privileges restrict the functionality available to operators, (e.g. a receptionist will have access to fewer features than a person responsible for the system's configuration and maintenance).

## Operator Privileges List Window

The **Operator Privileges** List Window opens in grid view.




Each operator privilege has a privilege "Type". Privilege types map to a particular operator role, and those privileges that are related have the same type.

This window can be sorted by privilege type, providing a way of sorting the operator privileges into logical groupings. This makes it easier when configuring Operator Groups.

## Which Operator Privileges you require

### Introduction

The following lists of Operator Privileges are sorted by privilege "Type". Privilege types provide a way of sorting the operator privileges into logical groupings, which can help when configuring Operator Groups. These lists indicate what each privilege will enable you to do, or give you access to.
**Notes:**

- **View** means a user can open the List Window and look at Property pages, but can not edit them.
- **Edit** means a user can change the properties of the associated items, create new ones and delete old ones.
- **No properties** means that although an operator might be able to see something in a List Window, they can't actually "view" the properties of it, (e.g. all Operators can see the **Report Description** List Window, and if there are any Cardholder reports in existence they will be able to see them listed there, however they will not be able to open the Properties to actually view these reports unless they have "View Cardholders" privilege).

This topic covers the following privilege types:


- ***Cardholder Access*** (on page 37-3)
- ***Configure*** (on page 37-11)
- ***Manage*** (on page 37-24)
- ***Monitor*** (on page 37-26)
- ***Override*** (on page 37-30)
- ***System*** (on page 37-33)

## Cardholder Access

### Add Card or Credential

An operator with "Add Card or Credential" privilege in a division can add a card, mobile credential or FIDO2 credential to a cardholder in that division in both Command Centre client and Configuration client.
**Notes:**

- This privilege includes "View Cardholders", (i.e. can view cardholder properties, except for the cardholder notes and operator configuration details, for any cardholder in that division).
- "Edit Cardholders" retains the ability to perform this action.
- Does not allow removal of the card or credential, (i.e. the "Remove Card or Credential" privilege is needed to do this).
- Does not allow editing of an existing card or credential, (i.e. the "Edit Card or Credential Attribute" is needed for this).

### Add Cardholder Notes

An operator with "Add Cardholder Notes" privilege in a division can perform the following in Command Centre:

- View and add Cardholder Notes but cannot modify or delete existing Notes (Command Centre Client only).
- View Cardholder Notes only (Configuration Client only).
- Find Cardholders and view only all properties of a Cardholder except the **Operator Configuration** tab.
- See changes to Notes on the **History** tab.
- See the PhotoID option in the **Configure** menu but cannot edit.

### Allow Re-Printing and Re-Encoding

An operator with "Allows Re-Printing and Re-Encoding" privilege in a division can perform the following:

- Anything that the "Print/Preview & Encode Card" privilege allows.
- Print and/or encode a Card that has already been printed/encoded on a Card before with the same identification details, (i.e. Facility Code, Card Number and Issue level).
  **Note:** Without this privilege cards can only be printed and encoded once.

### Assign Personalised Actions

This privilege applies only to the Cardholder Personalised Actions tile in the Command Centre Client.

An operator requires the "Assign Personalised Actions" privilege in the division of the output or macro, to be able to assign that item to the Cardholder Personalised Actions tile.
**Note:** The operator requires “View Site” or “Edit Site” in the division of the Access Zone to assign it to the tile.

**Bulk Change**

An operator with "Bulk Change" privilege in a division can perform the following:

- Add or delete a Bulk Change in that division.
- View and configure the properties of any Bulk Change in that division.
- Save a Bulk Change in that division.
- Run a Bulk Change in that division. [A bulk change only changes those items that the operator would have sufficient privilege to change via the standard Command Centre user interface (that is, outside of the bulk change).]

**Bureau Batch Printing/Encoding**

An operator with "Bureau Batch Printing/Encoding" privilege in a division can perform the following:

- View the properties of Card Types in that division.
- Encode, or print and encode multiple cards of a Card Type in that division.

**Create and Edit Cardholders**

An operator with "Create and Edit Cardholders" privilege in a division can perform the following:

- View and edit the properties of a Cardholder report description or Time & Attendance report description in that division.
- Create new Cardholder report descriptions or Time & Attendance report descriptions in that division.
- View and edit cardholder properties for all cardholders in that division, EXCEPT the **Cardholder Notes** and **Operator Configuration** tabs (neither tab is visible).
- Forgive a cardholder in that division anti-passback violations for a selected Access Zone (must also have "Override" privilege within the Access Zone's division).
- Add new cardholders in that division.
- Run Enrolment wizards in that division. [Can edit cardholder data within an Enrolment wizard only according to their normal edit privileges to that cardholder.]
- Use the **Read MIFARE Card** utility to read card data.

**Create Cardholders**

An operator with "Create Cardholders" privilege in a division can create Cardholders, but cannot edit Cardholders.

**De-Authorise Cardholder**

An operator with "De-Authorise Cardholder" privilege in a division can perform the following in Command Centre:

- Anything that the "View Cardholders" privilege allows, AND
- Not applicable to the Configuration Client:
  De-authorise a Cardholder (Command Centre), but cannot enable them or modify other entries on the **Cards** tile.

**Delete Cardholders**

An operator with "Delete Cardholder" privilege in a division, can delete any cardholder in that division.

**Disable Card**

An operator with "Disable Card" privilege in a division can perform the following in the Command Centre Client:

- Anything that the "View Cardholders" privilege allows, AND
- Not applicable to the Configuration Client:
  Disable a Cardholders Card or edit its From/Until Dates for an enabled card, but cannot enable a Cardholders Card or modify any other entries on the **Cards** tile.

**Edit Access Groups**

An operator with "Edit Access Groups" privilege in a division can perform the following:

- View and edit the properties of Access Groups in that division, EXCEPT adding or removing cardholders to/from the Access Group (can still "View" the cardholder names).
- Add or delete Access Groups in that division.
- View and edit the properties of an Access Group report description, in that division.
- Add or delete Access Group report descriptions in that division.
- Run Access Group report descriptions in that division. In this case, the Access Group report will only include those Access Groups to which the operator has either "View Access Groups" or "Edit Access Groups" privilege.

### Edit Biometric Data

An operator with "Edit Biometric Data" privilege in a Division can capture/ enrol Cardholder Biometric data for Morpho Readers using Finger/Vein/Wave.
**Notes:**

- This privilege will include "View Cardholders", (i.e. can view cardholder properties, except for the cardholder notes and operator configuration details, for any cardholder in that division).
- "Edit Cardholders" will retain the ability to perform this action.

### Edit Card or Credential

An operator with "Edit Card or Credential" privilege in a division can add, remove or edit the attributes (status, issue level, activation and expiry dates) of a card or mobile credential of any cardholder in that division in both Command Centre client and Configuration client.
The privilege exclusively includes the following:

- "Add Card or Credential" privilege
- "Remove Card or Credential" privilege
- "Edit Card or Credential Attribute" privilege

**Notes:**

- This privilege includes "View Cardholders", (i.e. can view cardholder properties, except for the cardholder notes and operator configu-ration details, for any cardholder in that division).
- "Edit Cardholders" retains the ability to perform these actions.

### Edit Card or Credential Attribute

An operator with "Edit Card or Credential Attribute" privilege in a division can edit the following attributes of an existing card or mobile credential of a cardholder in that division in both Command Centre client and Configuration client.
The attributes that can be edited are:

- Status
- Issue Level
- Activation date (From)
- Expiry date (Until)

**Exclusions:**

- The privilege does not allow Print and Encode nor View Pins functionality. These functions have their own privileges.
- Card numbers, mobile numbers, email addresses, and mobile model descriptions are not editable (for existing cards and credentials these are not editable by any privilege).

**Notes:**

- This privilege includes "View Cardholders", (i.e. can view cardholder properties, except for the cardholder notes and operator configuration details, for any cardholder in that division).
- "Edit Cardholders" retains the ability to perform this action.

**Edit Cardholder Name**

An operator with "Edit Cardholder Name" privilege in a division can edit, the First Name, Last Name and Short Name of a cardholder in that division in both Command Centre client and Configuration client.

**Notes:**

- This privilege includes "View Cardholders", (i.e. can view cardholder properties, except for the cardholder notes and operator configuration details, for any cardholder in that division).
- "Edit Cardholders" retains the ability to perform this action.

**Edit Cardholder Notes**

An operator with "Edit Cardholder Notes" privilege in a division can perform the following:

- View, add or delete Cardholder Notes for cardholders in that division.
- View all cardholder properties for cardholders in that division, EXCEPT the **Operator Configuration** tab.

**Edit Cardholder Personal Data**

An operator with "Edit Cardholder Personal Data" privilege in a division can edit the Personal Data Field values of a cardholder in that division in both Command Centre client and Configuration client.

**Notes:**

- This privilege includes "View Cardholders", (i.e. can view cardholder properties, except for the cardholder notes and operator configuration details, for any cardholder in that division).
- "Edit Cardholders" retains the ability to perform these actions.
- This privilege complements the existing operator group Personal Data privilege overrides to allow PDFs to be edited, only viewed, or hidden. *For example*, an operator with "Edit Cardholder Personal Data" privilege cannot edit a PDF that is hidden from them or is view only.

**Edit Cardholders**

An operator with "Edit Cardholders" privilege in a division can edit all Cardholder fields EXCEPT the **Division**, and restricts those operators from creating new Cardholders.

### Edit Passenger Details

An operator with "Edit Passenger Details" privilege in a Division can add/ change/remove a default floor for a ThyssenKrupp Elevator System. This allows the operator to view a list of elevator groups, and from this list view eligible default floor Access Zones and assign them.

### Modify Access Control

An operator with "Modify Access Control" privilege in a division can perform the following:

- View the properties of Access Groups in that division.
- Add or remove cardholders (to whom they must have "View" privilege) from Access Groups in that division.

### Print/Preview & Encode Card

An operator with "Print/Preview & Encode" privilege in a division can perform the following:

- Preview or print cards for cardholders in that division.
- Encode or print and encode cards for cardholders in that division, with the ability to enter user-defined PINs or generate random PINs, but not view PINs (as they will be masked).
  **Note:** The card's card type does not need to be in that division.
- View the cardholder's properties for all cardholders in that division.
- View cardholder properties for all cardholders in that division, with the exception of the Cardholder Notes and the Operator Configuration tab.
- Run Enrolment wizards in that division, but in a view only mode (no ability to edit cardholder data or create new cards for a cardholder).
- Run Enrolment wizards in that division with the ability to print or encode cards for cardholders in that division. Enter user-defined PINs or generate random PINs when encoding cards but not view them (since they are masked).
  **Note:** The card's card type does not need to be in that division.

### Remove Apple Account Binding

An operator with "Remove Apple Account Binding" privilege in a division can remove an Apple Account Binding allowing a Cardholder to provision an Apple badge.

### Remove Card or Credential

An operator with "Remove Card or Credential" privilege in a division can remove a card, mobile credential or FIDO2 credential from a cardholder in that division in both Command Centre client and Configuration client.
**Notes:**

- This privilege includes "View Cardholders", (i.e. can view cardholder properties, except for the cardholder notes and operator configuration details, for any cardholder in that division).
- Does not allow adding cards or credential.
- Does not allow editing of card or credential attributes.
- "Edit Cardholders" retains the ability to perform this action.

**View Access Groups**

An operator with "View Access Groups" privilege in a division can perform the following:

- View the properties of Access Groups in that division, including the names of all cardholders who belong to the Access Group.
- View and edit the properties of an Access Group report description, in that division.
- Run Access Group reports in that division. In this case, the Access Group report will only include those Access Groups to which the Operator has "View Access Groups" privilege.
- Add or delete Access Group report descriptions in that division.

**View Cardholder Notes**

An operator with "View Cardholder Notes" privilege in a division can perform the following:

- View Cardholder Notes for cardholders in that division.
- View all cardholder properties for cardholders in that division, EXCEPT the **Operator Configuration** tab.

**View Cardholders**

An operator with "View Cardholders" privilege in a division can perform the following:

- View and edit the properties of a Cardholder report description or Time & Attendance report description in that division.
- Create new Cardholder report descriptions or Time & Attendance report descriptions in that division.
- View cardholder properties for all cardholders in that division, EXCEPT the **Cardholder Notes** and **Operator Configuration** tabs.
- Run Enrolment wizards in that division, but in a view only mode (no ability to edit cardholder data or create, print or encode cards).
- Use the **Read MIFARE Card** utility to read card data.

**View Encrypted Cardholder User Codes (API Only)**

An operator with the "View Encrypted Cardholder User Codes" privilege can view encrypted Cardholder user codes (REST API only).
**Note:** The "Advanced User" privilege does not automatically convey this privilege.

**View Events**

**Note:** The purpose of this privilege is to allow operators who do not (and should not) have the "View Events and Alarms" privilege, and whose role does not involve monitoring/managing Alarms, to view events in the Command Centre Client, (in particular, but not exclusively, events on the Event Trail tile), and seeing the Alarm state of an item in either client. It will not be possible to view the details of the Alarm.

An operator with "View Events" privilege in a division can perform the following:

- View events in that Division using the Command Centre Client.
- With the exception of the above, will NOT be able to do any of the other things the "View Events and Alarms" privilege allows.

**View PINs**

There are two types of PINs (personal identification numbers); System Generated PINs and User Defined PINs. An operator with "View PINs" privilege can view PINs assigned to cards according to the following rules:

- An operator can only see a System Generated PIN if they have the "View PINs" privilege AND the PIN has not been changed. If changed, it then becomes a User Defined PIN and the rules below apply.
- An operator can only see a User Defined PIN if they have the "View PINs" privilege AND the **Store PINs for later viewing** checkbox was checked on the Server Properties **Card Security** tab at the time the PIN was set.
- A User Defined PIN that was set or changed while the **Store PINs for later viewing** checkbox was unchecked (on the Server Properties **Card Security** tab) is not retrievable and will need to be reallocated if the cardholder has forgotten it.

**Note:** "View PINs" functionality is not supported for PIV cards.

## Configure

### Configure Access Report

An operator with "Configure Access Report" privilege in a division can save or delete any Access Report in the Command Centre Client, for the Report's Division, but only if the operator also has the privilege to view reports.

### Configure Broadcast Notifications

An operator on a site with 'Notifications' included in the license file and the "Configure Broadcast Notifications" privilege in a division, can view, save, edit and delete Broadcast Notification items in the Command Centre Client.

### Configure Cardholder and Activity Report

An operator with "Configure Cardholder and Activity Report" privilege in a division can save or delete any Cardholder and Activity Report in the Command Centre Client, for the Report's Division, but only if the operator also has the privilege to view reports.

### Configure Evacuation Report

An operator with "Configure Evacuation Report" privilege in a division can perform the following in the Command Centre Client:

- Create a new Evacuation Report in that division.
- Delete an Evacuation Report in that division.
- Edit the properties of an Evacuation Report in that division.

**Note**: To view the properties of and/or run an existing saved Evacuation Report, an operator must have the "View Events and Alarms" operator privilege in the Evacuation Report's division. Having different privileges for creating and running Evacuation Reports ensures that operators who are able to run and print pre-configured Evacuation Reports (when there is an emergency), are prevented from changing their configuration.

### Configure Site

An operator with "Configure Site" privilege in a division can add or remove Command Centre items or view and edit their properties, (i.e. use the "New", "Delete", "Properties" context menu options), for all Command Centre items within that division and of the following types:

- Archives
- CardType, including editing Card Layout
- Universal Card Format
- Division
- Day Category *
- Calendar
- Special Calendar
- Morpho Biometric Type

- Competencies
- Notification Filter

* Day Categories are divisionless, so having "Configure Site" in any division allows an operator to configure any Day Category.

*Exclusions:*
The following actions, previously included under this privilege, are explicitly excluded from this privilege and require the "Edit Site" privilege to perform:
- FTP Stop
- FTP Start
- Resync Databases

**Configure Time Report**

An operator with "Configure Time Report" privilege in a division can save or delete any Time Report in the Command Centre Client, for the Report's Division, but only if the operator also has the privilege to view reports.

**Configure Viewers**

An operator with the "Configure Viewers" privilege in a Division can create, edit the configuration of and delete Viewers in that Division, in the Command Centre Client.
**Note:** This privilege does not automatically grant any other privilege which means the Operator will need additional privileges to be able to see the items (including Cardholders) to include in the configuration.

**Configure Voltage Report**

An operator with the "Configure Voltage Report" privilege in a division can save or delete any Voltage Report in the Command Centre Client, for the Report's Division, but only if the operator also has the privilege to view reports.

**Configure Workstation Routing**

An operator with the "Configure Workstation Routing" privilege in a Division can create, edit and delete Workstation Routing items in that Division, in the Command Centre Client.

**Edit Alarm Configuration**

An operator with "Edit Alarm Configuration" privilege in a division can perform the following:

- Create or delete Action Plans in that division.
- View and modify the properties of Action Plans in that division.
- Create or delete Insertion Tags in that division.
- View and modify the properties of Insertion Tags in that division.
- Create or delete Alarm Instructions in that division.
- View and modify the properties of Alarm Instructions in that division.

### Edit Card State Sets

An operator with the "Edit Card State Sets" privilege in a division can create, edit and delete Card State Sets in that Division, in the Command Centre Client.
**Note:** Operators must have this privilege in at least one Division in order to see the Card States icon on the **Administration** Toolbar in the Command Centre Client.

### Edit Card Types

An operator with the "Edit Card Types" privilege in a division can perform the following:

- Edit the properties of Card Types in that division, except the properties that are non-editable.
- Add or delete Card Types in that division.
- Edit Card Layouts in that division.

### Edit Cardholder Notification

An operator with the "Edit Cardholder Notification" privilege in a division can perform the following:

- Enable/disable notifications on the **Event Notifications** tab of a cardholder record.
- Change the Notification Method assigned to each Notification Filter on the **Event Notifications** tab of a cardholder record.
- Change the calendar assigned to a cardholder to either the default calendar or a specific special calendar.
- The following functions require an additional privilege as well as the "Edit Cardholder Notification" privilege:

| **To be able to…** | **an operator must also have the…** |
|---|---|
| add or remove a Filter from a cardholder, | "View Site" privilege in the Notification Filter's division. |
| add a schedule to a cardholder's Notifications page, | "View Schedules" privilege in the Schedule's division. |
| update Cardholder tabs other than the **Event Notification** tab, | appropriate cardholder privilege, (e.g. "Edit Cardholder", "Delete Cardholder", "Edit Cardholder Notes") |

The "Edit Cardholder Notification" privilege inherently receives the privilege of "View Cardholders".

### Edit Competency Definitions

An operator with "Edit Competency Defintions" privilege in a division can perform the following:

- Add or delete a competency in that division.
- View or modify a competency in the division.

### Edit Divisions

An operator with "Edit Divisions" privilege can perform the following:

- Add or delete a division.
- View or modify a division.

### Edit Enrolment Templates

An operator with "Edit Enrolment Templates" privilege in a division can perform the following:

- Create an Enrolment Template in that division.
- Delete an Enrolment Template in that division.
- View the properties of Enrolment Templates in that division.
- Edit the properties of Enrolment Templates in that division.

**Note:** Some Enrolment Template properties will require additional privileges to configure, (i.e. "View Site" is needed in the Card Type's division to select the Card Type, and "View Personal Data Definitions" is needed in a PDF's division to select that PDF within the Enrolment Template).

**Edit Enterprise Data Interfaces**

An operator with the "Edit Enterprise Data Interfaces" privilege can perform the following:

- Create an Enterprise Data Interface (EDI)
- Save an EDI
- Edit an EDI
- Run an EDI
- Enable/disable an EDI.

**Edit Evacuation Report**

An operator with "Edit Evacuation Report" privilege in a division can edit the properties of an Evacuation Report in that division, in the Configuration Client.
**Note:** To view the properties of and/or run an existing saved Evacuation Report, an operator must have the "View Events and Alarms" operator privilege in the Evacuation Report's division. Having different privileges for creating and running Evacuation Reports ensures that operators who are able to run and print pre-configured Evacuation Reports (when there is an emergency), are prevented from changing their configuration.

**Edit Guard Tours**

An operator with "Edit Guard Tours" privilege in a division can perform the following:

- Edit the properties of Guard Tours in that division, including the list of checkpoints that are configured for the tour.
- Add or delete Guard Tours in that division.

**Edit Icon Sets**

An operator with "Edit Icon Sets" privilege can perform the following:

- Add or delete an Icon Set in ANY division.
- View and modify the properties of any Icon Set in ANY division.

**Note:** Icon sets are divisionless, hence this privilege applies system-wide.

**Edit Lockers**

An operator with "Edit Lockers" privilege in a division can create, edit and delete Lockers and Locker Banks.

**Edit Macros**

An operator with "Edit Macros" privilege in a division can perform the following:

- View and edit properties of Macros in that division (with the exception of the Macro’s schedule).

- Add or delete Macros in that division (with the exception of the Macro's schedule).
- Duplicate a Macro in that division (with the exception of the Macro's schedule).

**Edit Operators**

An operator with "Edit Operators" privilege in a division can perform the following:

- View all Operator Privileges (their name and description).
- View and edit the properties of Operator Groups in that division (including adding any privileges to those Operator Groups, providing the operator has "Edit Operators" privilege in each division to which those privileges will apply).
- Add or delete Operator Groups in that division.
- View the **Operator Configuration** tab on a cardholder's properties for cardholders in that division, if the operator also has "View Cardholders" privilege in that division.
  View and edit the **Operator Configuration** tab on a cardholder's properties for cardholders in that division, if the operator also has "Edit Cardholders" privilege in that division.

**Edit Personal Data Definitions**

An operator with "Edit Personal Data Definitions" privilege in a division can perform the following:

- Add or delete Personal Data Fields in that division.
- View or modify the properties of Personal Data Field definitions in that division.

**Edit Report Descriptions**

An operator with "Edit Report Descriptions" privilege in a division can save or delete any type of Report Description (with the exception of the Evacuation Report) in the Configuration Client, for the Report Description's Division, but only if the operator also has the privilege to view reports.
**Note:** This applies to all reports except for the Evacuation Report which is controlled by the "Edit Evacuation Report" operator privilege.

**Edit Role Definitions**

An operator with "Edit Role Definitions" privilege in a division can perform the following:

- View and edit the properties of Roles in that division.
- Add or delete Roles in that division.

**Edit Salto Items**

An operator with "Edit Salto Items" privilege in a division can perform the following:

- Delete or change names, descriptions and door-zone relationships of Salto Doors and Zones.
- Re-synchronise with the Salto application.

**Note:** Names, descriptions or door-zone relationships of Rooms, Lockers or Suites cannot be deleted or changed. These are changed only through a re-sync, and then only from the Salto side.

### Edit Schedules

An operator with "Edit Schedules" privilege in a division can perform the following:

- View and edit the properties of Schedules in that division.
- Add or delete Schedules in that division.
- Duplicate Schedules.

### Edit Site

An operator with “Edit Site” privilege in the root division can edit the list of reasons for printing or encoding a card.

An operator with "Edit Site" privilege in a division can perform the following:

- Create and delete workstations.
- View the Status Viewer.
- View icon sets and change the icons on Command Centre items.
- View and edit the properties of any of the following Command Centre items in that division, (i.e. can use the **Properties** context menu option in the appropriate List Window).
- Add or remove any of the following Command Centre items in that division, with the exception of the Server, (i.e. can use the **New** or **Delete** context menu options in the appropriate List Window).
- See any Command Centre Client Monitor Site Viewers in that division.
- View Notification Filters and competencies, but not create them.
- Use the "Identify device" override.

**Hardware Controllers:**
- Controller 6000 or 7000

**Hardware - HBUS:**
- HBUS Reader
- HBUS Terminal
- HBUS Alarms Only Terminal
- HBUS F31/F32/F41/F42 Fence Controller
- HBUS F22 Fence Controller
- HBUS I/O Interface
- HBUS Z10 Tension Sensor Group

**Hardware - Sensor:**
- D10 Taut Wire Sensor
- Z20 Disturbance Sensor

**Hardware - Aperio:**
- Aperio Door

**Hardware - Other:**
- Input
- Output (virtual or physical)
- Third Party Reader
- Morpho Biometric Reader (Third Party Reader)
- Alarm Dialler
- Elevator HLI
- DVR System
- DVR Camera

**Other items:**
- Server **
- Workstation
- Access Zone
- Alarm Zone
- Door
- Site Plan
- Elevator Car
- Salto Server **
- Salto Access Zone
- Elevator Car HLI
- Intercom
- Intercom System
- Interlock Group
- External System
- External System Item
- Logic Block
- Salto Door
- Receptions
- IP Alarm Transmitter

**Device software:**
- Controller Software
- RIO Software
- Controller Customisation Software

** This item CANNOT be added or removed with the "Edit Site" privilege.

An operator with "Edit Site" privilege in a division can view and edit the properties of any of the following Services and Workstations items, in that division, as well as deleting the Services and Workstations items (**Services and Workstations item** > **Delete** or, > **Properties**).

- FT Controller Service
- FT Import-Export Service
- FT Bootstrap Protocol Service
- FT Intercom Service

An operator with "Edit Site" privilege in a division can perform the following:

- Re-synchronise databases between the Server and any Controller in that division.
- Re-synchronise databases between the Server and any Morpho Biometric Reader in that division.
- Re-synchronise with the Salto application.
- Accept a new certificate for a remote server.
- Create a new Elevator Car in that division by duplicating (or copying) the properties of another Elevator Car (to which the operator also has "Edit Site" privilege).
- Create a new Elevator Car HLI in that division by duplicating (or copying) the properties of another Elevator Car HLI (to which the operator also has "Edit Site" privilege).
- Create a new External System in that division by duplicating (or copying) the properties of another External System (to which the operator also has "Edit Site" privilege).

- Create a new External System Item in that division by duplicating (or copying) the properties of another External System Item (to which the operator also has "Edit Site" privilege).

An operator with "Edit Site" privilege in a division can push the configuration of that item to the Controller that hosts the item for any of the following Command Centre items in that division (Context menu option is **Command Centre item** > **Push Configuration**).

| | | | |
|---|---|---|---|
| Controller 6000 or 7000 | HBUS Reader | HBUS Terminal | HBUS Alarms Only Terminal |
| HBUS F31/F32/ F41/F42 Fence Controller | HBUS F22 Fence Controller | Elevator HLI | Elevator Car HLI |
| Elevator Car | Door | Interlock Group | Input |
| Output | External System | External System Item | DVR System |
| DVR Camera | Fence Zone | Access Zone | Alarm Zone |
| Alarm Dialler | Cardax IV Reader | | Third Party Reader |

**Site Configuration Report:**
An operator with "Edit Site" privilege in a division can add, delete, generate, view and modify the properties of a Site Configuration Report description in that division. When run, the Site Configuration Report will only report the properties for Command Centre items to which the operator has "View" privilege.

**Contact ID Report:**
An operator with "Edit Site" privilege in a division can add, delete, generate, view and modify the properties of a Contact ID Report description in that division. The Contact ID Report will only include those Command Centre items to which the operator has "View" privilege.

**Access Report:**
An operator with "Edit Site" privilege in a division can add, delete, generate, view and modify the properties of an Access Report description (Summary or Detailed) in that division. The following rules apply:

- When the Access Report is run, it will only report on those Access Zones or Salto Access Zones to which the operator has "View Site" privilege.
- If a Door rather than an Access Zone is configured in the report description, then the Access Zone that the Door provides entry to, is the effective Access Zone that is reported on. The same does not apply for Salto Doors, as these may be reported on directly.

**Detailed Access Report:**
If the operator has the privilege to view properties of an Access Zone, Salto Access Zone or Salto Door included in the report then all cardholders which have access to that item (their name only) at the time configured in the report description (or for the configured day category) will be displayed in the Detailed Access Report. This applies regardless of the operator's privileges, or lack of them, to that cardholder.

The content of a PDF is only displayed in the Detailed Access Report, for each cardholder, if the operator has privilege to view the content of that PDF for that cardholder.

The cardholder's card number is only displayed in the Detailed Access Report, if the operator has "View cardholder" privilege for that cardholder.

**Summary Access Report:**
When the Summary Access Report is run, it displays the names of any Access Groups, and other information about that Access Group, for any Access Groups that provide access to that item at the time configured in the report description (or for the configured day category). This applies regardless of the operator's privileges, or lack of them, to these Access Groups.

**Fence Voltage Report:**
An operator with "Edit Site" privilege in a division can add, delete, generate, view and modify the properties of a Fence Voltage Report description in that division. The Fence Voltage Report must only include those Command Centre items to which the operator has "View" privilege.

### Edit Visits

An operator with "Edit Visits" privilege can perform the following in the Visitor Management system:

- Create and edit visits, including adding and removing visitors from the visit.
- Perform any of the actions, all of which update the status of the visitor for the visit and maintain a record of the actions performed.
- To send an arrival or general notification.

### Enable/disable Operator

An operator with "Enable/disable Operator" privilege in a division can enable and disable the Command Centre Logon for operators via either:

- the **Operator Configuration** tab of the Cardholder properties in the Configuration Client, OR
- the **Logon Details** button on the Cardholder Operator Groups tile of the Cardholder Viewer in the Command Centre Client.

**Manage Keys**

An operator with "Manage Keys" privilege in the Root Division can perform the following operations:

- Change/import/export site keys
- Start/stop migration
- Encode admin cards
- Change/import/export Morpho biometric type keys
- Change Salto keyset and Configure Encryption Override

The above operations will not be available to any operator who does not have the "Manage Keys" privilege or equivalent, (i.e. "Advanced User" in the same division, or System Operator).

**Manage Locker Assignments**

An operator with "Manage Locker Assignments" privilege in a division can manually assign (allocate), modify and/or remove Lockers from Cardholders. **Note:** It does not include "View Cardholder" privilege however. "View Cardholder" privilege is not required to see existing Locker assignments in the Locker Viewer.

**Modify Operator Group Membership**

An operator with "Modify Operator Group Membership" privilege (but without the "Edit Operators" privilege) will be able to add and remove Cardholders from Operator Groups, but will not be able to edit the Operator Group in any other way.

**Run Bulk Random Selection**

An operator with "Run Bulk Random Selection" privilege in a division can run Bulk Random Selection items in that Division. The operator can modify the ‘Cardholder Probability of Selection’ and ‘Per-Run Total Cardholder Selection Limit’ settings when they run a Bulk Random Selection, but these modifications are applied to that run only and not saved to configuration.

**Schedule Access Zone**

An operator with "Schedule Access Zone" privilege in a division can change a Schedule on an Access Zone to another which has already been created.

**Select System View**

An operator with "Select System View" privilege within any division, is able to restrict their system view within Command Centre to one or more of the Operator Groups to which they belong.

This makes the **Select System View** selection dialog available to them.

**View Alarm Configuration**

An operator with "View Alarm Configuration" privilege in a division can perform the following:

- View the properties of Action Plans in that division.
- View the properties of Insertion Tags in that division.
- View the properties of Alarm Instructions in that division.

### View Lockers

An operator with "View Lockers and Assignments" privilege in a division can view Lockers, Locker Banks and Locker assignments.

### View Operators

An operator with "View Operators" privilege in a division can perform the following:

- View all Operator Privileges (Name and Description).
- View the properties of Operator Groups in that division.
- View the **Operator Configuration** tab on a cardholder's properties for cardholders in that division, but only if the operator also has "View Cardholders" or "Edit Cardholders" privilege in that division.

### View Personal Data Definitions

An operator with "View Personal Data Definitions" privilege in a division can view the properties of Personal Data Fields in that division.

### View Schedules

An operator with "View Schedules" privilege in a division can view the properties of Schedules in that division.

### View Site

An operator with "View Site" privilege in a division can view the properties of any of the following Command Centre items in that division, (i.e. use the **Properties** context menu option for the appropriate Command Centre item).

**Hardware Controllers:** -
Controller 6000 or 7000

**Hardware - HBUS:**
- HBUS Reader
- HBUS Terminal
- HBUS Alarms Only Terminal
- HBUS F31/F32/F41/F42 Fence Controller
- HBUS F22 Fence Controller
- HBUS I/O Interface
- HBUS Z10 Tension Sensor Group

**Hardware - Sensor:**
- D10 Taut Wire Sensor
- Z20 Disturbance Sensor

**Hardware - Aperio:**
- Aperio Door

**Hardware - Other:**
- Input
- Output (virtual or physical)
- Third Party Reader
- Morpho Biometric Reader (3rd Party Reader)
- Alarm Dialler
- Elevator HLI
- DVR System
- DVR Camera

**Other items:** (these items edited with "Configure Site", "Edit Icon Sets" or "Edit Macros")
- Archive
- Calendar
- Special Calendar
- Card Type
- Day Category *
- Division
- Universal Card Formats
- Notification Filters
- Macro
- Icon Sets *

**Other items:** (these items edited with "Edit Site")

- Server **
- Workstation
- Access Zone
- Alarm Zone
- Door
- Site Plan
- Elevator Car
- Elevator Car HLI
- Intercom
- Receptions
- Interlock Group
- External System
- External System Item
- Fence Controller
- Fence Zone
- Salto Server **
- Salto Door
- Salto Access Zone
- Competencies

* This item is divisionless, so having "View Site" in any division allows an operator to view the properties of this item.

** This item CANNOT be added or removed with "Edit Site" privilege.

An operator with "View Site" privilege in a division can view the properties of any of the following Device Software items, in that division.

- FT Controller Service
- FT Import-Export Service
- FT Bootstrap Protocol Service
- FT Intercom Service
- Remote Server

An operator with "View Site" privilege in a division can see any Command Centre Client Monitor Site Viewers, in that division.

**Reports:**

An operator with "View Site" privilege in a division can add, delete, generate, view and modify the properties of a Site Configuration Report description in that division. When run, the Site Configuration Report will only report the properties for Command Centre items to which the operator has "View" privilege.

An operator with "View Site" privilege in a division can add, delete, generate, view and modify the properties of a Contact ID Report description in that division. The Contact ID Report will only include those Command Centre items to which the operator has "View" privilege.

An operator with "View Site" privilege in a division can add, delete, generate, view and modify the properties of an Access Report description (Summary or Detailed) in that division. The following rules apply:

- When the Access Report is run, it will only report on those Access Zones or Salto Access Zones to which the operator has the privilege to view the Access Zone's properties.
- If a Door rather than an Access Zone is configured in the report description, then the Access Zone that the Door provides entry to, is the effective Access Zone that is reported on. The same does not apply for Salto Doors, as these may be reported on directly

**Detailed Access Report:**
If the operator has privilege to view the properties of an Access Zone, Salto Access Zone or Salto Door included in the report then all cardholders which have access to that item (their name only) at the time configured in the report description (or for the configured day category) will be displayed in the Detailed Access Report. This applies regardless of the operator's privileges, or lack of them, to that cardholder.

The content of a PDF is only displayed in the Detailed Access Report, for each cardholder, if the operator has privilege to view the content of that PDF for that cardholder.

The cardholder's card number is only displayed in the Detailed Access Report, if the operator has the privilege to view the card number for that cardholder.

**Summary Access Report:**
When the Summary Access Report is run, it displays the names of any Access Groups, and other information about that Access Group, for any Access Groups that provide access to that item at the time configured in the report description (or for the configured day category). This applies regardless of the operator's privileges, or lack of them, to these Access Groups.

**Fence Voltage Report:**
An operator with "View Site" privilege in a division can add, delete, generate, view and modify the properties of a Fence Voltage Report description in that division. The Fence Voltage Report must only include those Command Centre items to which the operator has "View" privilege.

### View Vists

An operator with "View Visits" privilege can perform the following in the Visitor Management system:

- View visits for a Reception that the Receptionist does not have edit rights for. Guards may be given 'view only' access.
- Print Visitor Management reports (with the exception of the Evacuation Report).

**Note:** This privilege is not required if the "Edit Visits" privilege is granted.

## Manage

### Manage Cardholder Location

The "Manage Cardholder Location" relates to the following features in Command Centre Client:
- Mobile Evacuation,
- Tagboards, and
- "Move to Location" action from the Cardholder Viewer

- To move one or more Cardholders from one Access Zone to another Zone, an Operator requires the "Manage Cardholder Location" privilege in the target Access Zone's division.
- To move a Cardholder outside the system, an Operator requires the "Manage Cardholder Location" privilege in any division and the **Allow moving cardholders outside of the system** option must also be enabled on the **General** tab of the Mobile Viewer Global Settings.

### Manage Guard Tours

An operator with "Manage Guard Tours" privilege in a division can perform the following:
- Override to "Start" or "Stop" any Guard Tour in that division, in the Configuration Client.
- View the properties of Guard Tours in that division, including the list of checkpoints that are configured for the tour, in the Configuration Client.
- See a Guard Tour in the browse tool when configuring a Guard Tour tile, in the Command Centre Client. Only Tours in that division in which the privilege (or one of the other qualifying privileges) is held will be available.
- See a division in the browse tool when configuring a Guard Tour tile, in the Command Centre Client. Only divisions in which the privilege (or one of the other qualifying privileges) is held will be available.
- In operational mode in the Command Centre Client, to see a Tour, select the Guard, start and stop configured Guard Tours (in that division) on a Guard Tour tile.

**Note:** Additional privileges are required to configure tiles in the Command Centre Client.

### Manage Historical Cardholder Location

The "Manage Historical Cardholder Location" privilege grants the same abilities as the “Manage Cardholder Location” privilege, but additionally allows operators to select a past movement time when creating manual access events.

- To historically move one or more Cardholders from one Access Zone to another Zone, an Operator requires the "Manage Historical Cardholder Location" privilege in the target Access Zone's division.

- To historically move a Cardholder outside the system, an Operator requires the "Manage Historical Cardholder Location" privilege in any division and the Allow moving cardholders outside of the system option must also be enabled on the General tab of the Mobile Viewer Global Settings.

**Manage Receptions**

An operator with "Manage Receptions" privilege in a division can perform the following:

- Determine whether a user is a Receptionist for a particular Reception.
- View Card Type data which is used to validate an access card when assigning it to a visitor.

**Manage Visitor Attributes**

A Receptionist using the Visitor Management system with "Manage Visitor Attributes" privilege can assign an escort to a Cardholder in a division for which they do not have "Edit Cardholder" privileges.

**Multiple Monitor Layout**

An operator with "Multiple Monitor Layout" privilege is any division can move Viewers between existing windows, or create new Viewer windows, in the Command Centre Client.

## Monitor

### Acknowledge Alarms

An operator with the "Acknowledge Alarms" privilege in a division can perform the following actions on a single alarm:

- Acknowledge and edit properties of alarms whose source is any Command Centre item within that division. This includes adding a Note or Comment to the alarm.
- View events and alarms whose source is a Command Centre item within that division.
- View an image sequence in that division.
- Refresh alarms from a Controller in that division, but only with "View Site" privilege in that division as well.
- Add, delete, edit properties of, or run an Activity or Exception report description in that division. If the report contains items to which the operator does not have "View" privilege they are excluded from the report.
- View the properties of an Evacuation Report in that division, or run an Evacuation report description in that division.

### Adjust DVR PTZ controls

An operator with "Adjust DVR PTZ controls" privilege in a division can alter the pan, tilt or zoom (or other controls as provided by the DVR integrator) of a DVR camera in that division, while watching live image sequences from that DVR Camera.

### Bulk Process Alarms

An operator with "Bulk Process Alarms" privilege in one or more divisions can perform the following:

- Bulk process all inactive alarms within an alarm priority group. This processes all the alarms, not just those in the division in which the privilege is held.
  **Notes:**
  - "Edit alarms" privilege in a division is also needed to bulk process alarms whose source is an item from that division.
  - For escalated alarms, the operator must also belong to an Operator Group which allows them to acknowledge or process escalated alarms (configured via the Operator Group properties, **Configuration** tab).

### Controlled Challenge

An operator with "Controlled Challenge" privilege can open the Challenge Viewer in "Controlled" mode, and grant or deny access to cardholders entering via any Door in that division. The operator must also have "View Events & Alarms" privilege in the Door's division, to operate the Challenge Viewer, and "View Digital Camera" privilege if using DVR cameras.

### Edit Alarms

An operator with "Edit Alarms" privilege in a division can perform the following:

- Acknowledge, edit properties of, and process alarms whose source is any Command Centre item within that division.
- View events and alarms whose source is an Command Centre item within that division.
- View an image sequence in that division.
- Add, delete, edit properties of, or run an Activity report description in that division. If the report contains items to which the operator does not have "View" privilege they are excluded from the report.
- Add, delete, edit properties of, or run an Exception report description in that division. If the report contains items to which the operator does not have "View" privilege they are excluded from the report.
- View the properties of an Evacuation report description in that division, or run an Evacuation report description in that division.
  **Note:** This is the only report that includes all Access Zones configured in the report description, regardless of the (generating) operator's privileges (or lack of them) to these Access Zones.
- "Quick process" an alarm whose source is any Command Centre item within that division.

### Edit Alarms Below High Priority

An operator with "Edit Alarms Below High Priority" privilege can only acknowledge and process alarms of the following priorities:
- Medium High,
- Medium,
- Medium Low,
- Low, and
- Very Low

### Force Process

An operator with "Force Process" privilege in a division, and "View Site" and "Edit Alarms", can force process active alarms.

### Launch Configuration Client

An operator with the "Launch Configuration Client" privilege in any one or more divisions can perform the following:

- Login to the Configuration Client through CCFT.exe
- See the **Configuration Client** button on the Administration tab of the Command Centre Client.
- Click the **Configuration Client** button once to launch the Configuration Client from this icon.

### Record live DVR stream

An operator with "Record live DVR stream" privilege in a division can record the live DVR image sequences, while watching them from a DVR Camera in that division.

### Use Intercom

An operator with "Use Intercom" privilege in a division can perform the following:
**Note:** The operator also needs "View Site" in the Intercom's division, to view the Intercom Command Centre item, and "View Events & Alarms" in the Intercom's division to receive a call from the Intercom.

- Place a call to an Intercom in that division.
- Answer a call or end a call from an Intercom in that division.
- Place a call on hold or forward a call from an Intercom in that division.

### View Cardholder Events (API Only)

This privilege is only applicable to operators used as a REST Client Operator for a REST Client item. A REST Client Operator with "View Cardholder Events (API Only)" privilege can view Cardholder events (e.g. Door Access Granted) via the REST API. This can allow a REST client to monitor Cardholders' movements without being able to view non-Cardholder events.

### View Challenge

An operator with "View Challenge" privilege in a division can perform the following:

- Open the Challenge Viewer in "View only" mode and operate the Challenge Viewer for any Doors in that division.
- View the properties of all Doors in that division.
- The operator must also have "View Events & Alarms" privilege in the Door's division, to operate the Challenge Viewer.

### View Digital Camera

An operator with "View Digital Camera" privilege for a Digital Camera's or DVR Camera's division can view the properties of that Camera.

### View Events and Alarms

An operator with "View events and alarms" privilege in a division can perform the following:

- View events and alarms whose source is a Command Centre item within that division.
- View an image sequence in that division.
- Refresh alarms from a Controller (all types) in that division, but only with "View Site" privilege in that division as well.
- Add, delete, edit properties of, or run an Activity report description in that division. If the report contains items to which the operator does not have "View" privilege they are excluded from the report.
- Add, delete, view and edit properties of, or run an Exception report description in that division. If the report contains alarms whose source is an Command Centre item in a division which the operator does not have "View Events and Alarms" privilege within, they are excluded from the report.
- View the properties of an Evacuation report in that division, or run an Evacuation Report description in that division.
- See Alarm Viewers stored in that division which have been configured for use in the Command Centre Client.

### View Guard Tours

An operator with "View Guard Tours" privilege in a division can view the properties of Guard Tours in that division, including the list of checkpoints that are configured for the Tour.

## Override

### Disable Workstation

An operator with "Disable Workstation" privilege in a division can disable a Workstation in that division.

### Disable Workstation Routing

An operator with "Disable Workstation Routing" privilege in a division can perform the following in the Command Centre Client:

- Move any Workstation Routing item in that division to the "Disabled" state, and
- Move any Workstation Routing item in that division out of the "Disabled" state to either of the other states.

### Enable Workstation

An operator with "Enable Workstation" privilege in in a division can enable a Workstation (that has been disabled) in that division.

### Maintenance Override

An operator with "Maintenance Override" privilege in a division can perform the following:

- Override to "Shunt", "Unshunt", "Isolate" or "De-isolate" any Input in that division.
- Override to "Shunt" or "Unshunt" any Fence Zone in that division, (i.e. the deterrent is still active and will respond to commands, but all warning or alarm events are ignored).
- Override to "On" or "Off" any Fence Zone in that division.
- Override to “High Voltage” or “Low Feel” for any Fence Zone connected to an F31, F32, F41, F42 or F22 Fence Controller in that division.
- Override to “Maintenance Mode” or “Walk Test Mode” any Z10 Tension Sensor Group in that division.
- Override to "Reset", "Shunt" or "Unshunt" specific* hardware Command Centre items in that division.
- Override to "Shunt" or "Unshunt" specific** hardware Command Centre items in that division.
- Override to "Reset", "Disable Communication", "Enable Communication", "Enable WWW Connections" or "Cancel WWW Override" any Controller in that division.
- Override to “Renew DHCP Settings”, “Revalidate certificate” Controller 6000 in that division.
- Override to "Use secondary ethernet" or "Cancel use secondary ethernet" Controller 6000's only (if dual ethernet is enabled).
- Override to "Reset Reader Keys" for Cardax IV Readers, with either "View Site" or "Edit Site" privilege also.
- Override any Logic Block in that division to "On", "Off" or "Reset Logic".

- Disable or enable communication with a remote server.
- Reset replication with a remote server.
- Cancel overrides that can be established with this privilege.

Operator must be able to "View" the items that they are wanting to override so they can access the **Status and Overrides** tab on the properties page in order to perform the override/shunt.

* Override to "Reset", "Shunt" or "Unshunt" the following hardware Command Centre items in that division:

| | | | |
|---|---|---|---|
| HBUS 8-In 2-Out Door Module | HBUS 8-In Board | HBUS 8-In 4-Out Board | HBUS 16-In 16-Out Board |
| HBUS Terminal | HBUS Alarms Only Terminal | HBUS F22 Fence Controller | HBUS F31/F32/F41/F42 Fence Controller |

** Override to "Shunt" or "Unshunt" the following Command Centre items in that division:

| | |
|---|---|
| Z10 Tension Sensor Group | Elevator HLI |

**Override**

An operator with "Override" privilege in a division can perform the following:

- Override Access Zone state for a specified time or until the next scheduled change or until the override is cancelled, for any Access Zone in that division for any of the twelve possible Access Zone states.
- Forgive cardholders in that division (to whom they also have "View cardholder" privilege, or any higher privilege that enables them to view the cardholder's properties) anti-passback violations, for any access zone in that division.
- Forgive all cardholders anti-passback violations for any Access Zone in that division.
- Perform a Lockdown or Cancel a Lockdown on an Access Zone in that division.
- Override the zone count for any Access Zone in that division.
- Override an Output (to "On", "Off", or "Pulse") for a specified time or until the next scheduled change, for any Output in that division.
- Override an Alarm Zone state (to "Armed", "Disarmed", "User1" or "User2"), for any Alarm Zone in that division.
- Override an Interlock Group in that division ("Enable" or "Disable" the Interlock Group).
- Override a lift car to Go to Floor.
- Cancel stateful overrides that can be established with this privilege.
  **Note:** If an override is selected that cannot be cancelled, (i.e. shunt or unshunt), then there is no option for the user to Cancel the override.

This privilege also allows an operator to view any of the items that they can override with this privilege (except cardholders).

**Override up to Medium Priority**

The "Override up to Medium Priority" privilege allows the same privilege set as the "Override" privilege (see above), but the Operator can only override active alarms up to (and including) ‘Medium Priority’ (as long as doing so will not cause any alarms).

**Override - Lock Door**

An operator with "Override - Lock Door" privilege can manually lock a Half-Cycle lock type Door. A Half-Cycle door will remain unlocked after access is granted until either it is opened and shut or the Lock Door override is used.

**Override - Open Door**

An operator with "Override - Open Door" privilege in a division can unlock a locked door for a short time, for any Controller door in that division.

**Override - Open Locker**

An operator with "Override - Open Locker" privilege in a division can open and/or isolate Lockers.

**Override Card Status**

An operator with "Override Card Status" privilege in a division can perform the following:

- Change the state of a card that is in a Permanently Disabled state.
- Allow a card to be created with the same details (card number, facility code, issue level) as a card that is in a 'Stolen', or other Permanently Disabled state.

**Run Macros**

An operator with "Run Macros" privilege in a division can perform the following:

- View the properties of Macros in that division.
- Run a Macro in that division.

**Schedule & Run Macros**

An operator with "Schedule & Run Macros" privilege in a division can perform the following:

- View the properties of Macros in that division.
- Edit the scheduled run times for a Macro in that division (add or remove scheduled run times).
- Run a macro in that division.

**Send Broadcast Notification**

When added to a Viewer, an operator with the “Send Broadcast Notification” privilege can view, edit before sending and send the same email or SMS message (Short Message Service) to many Cardholders at once in the Command Centre Client.

**Use Workstation Routing**

An operator with "Use Workstation Routing" privilege in a division can move any Workstation Routing item in that Division between the non-Disabled states, in the Command Centre Client.

## System

### Advanced User

An operator with "Advanced User" privilege within a division has all privileges within that division, except the "Controlled Challenge" privilege. This includes the "Select System View" privilege, which applies system-wide rather than to a specific division.

An operator with "Advanced User" privilege within one or more divisions can also:

- Process active alarms (either individually, or via a bulk-process).
  **Note:** The "Force-Process All" option processes all active and inactive alarms that are within the alarm priority group and whose source is an item within a division in which the "Advanced User" privilege is held. It also processes all inactive alarms within the alarm priority group whose source is an item within a division in which the "Edit Alarm" privilege is held.
- Configure events and/or image sequences to be detected from the event database instead of being archived. Once configured, events and/or image sequences are deleted instead of being archived when the archive is run, by an operator.
- View and edit the content of all PDFs for all cardholders in that division, (i.e. the operator is not limited by the normal PDF privileges defined in the PDF definition or in the operator groups to which they belong).
- Run the Quickstart Wizards.
- Create remote servers, and perform "Accept Certificate" overrides of remote servers.

### Backup and Archive

An operator with "Backup and Archive" privilege in a division can perform the following:

- View the properties of an Archive in that division.
- Start (run) an Archive or stop an Archive that is currently running, within that division.
  **Note:** The Archive's division controls which operators can see the Archive, and start or stop the Archive from running. It does not control what events it contains. Every Archive always archives all events from all divisions.
- Configure and run a Backup.

# Chapter 38: Bulk Changes

## Understanding Bulk Changes

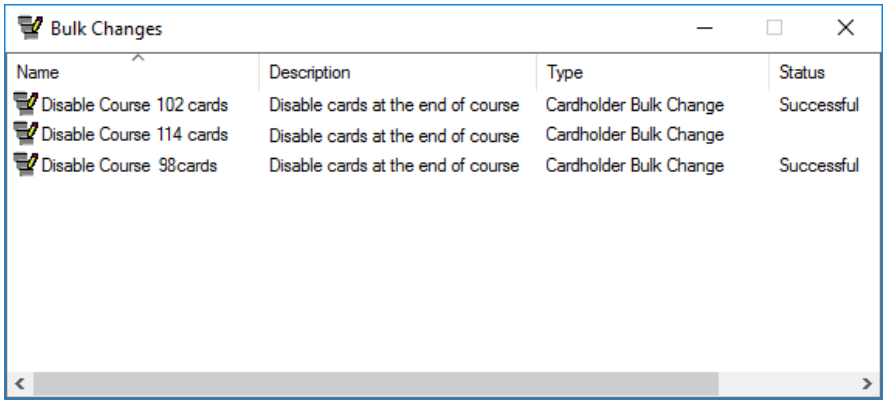
The bulk changes feature provides an automated method of changing a common set of properties on a group of items in Command Centre. Bulk changes can be scheduled to run at specific times. This is achieved using the Macro functionality. See ***Macros*** (on page 20-1) for further details.

Only one bulk change can be run at one time. If an operator attempts to start a bulk change when there is already one running the second one will be queued and run once the first one has finished. Likewise, if bulk changes are scheduled to run (via macros), they will be queued and run in the order scheduled, with only one being executed at a time.

**IMPORTANT:**
As authorisations will not be checked before a bulk change is run, an operator with the "Bulk Change" operator privilege will be able to see any data that is contained in a bulk change that has been saved. Even if they do not have the privilege to view the data any other way, they will be able to see it in the bulk change.
*For example:*
A bulk change may contain a number of cardholders or Access Groups that the bulk change editor does not have access to view. However, in the bulk change they will be able to see this information.

## Bulk Changes List Window

The **Bulk Changes** List Window opens in grid view.




All saved bulk changes are listed in this window. For each bulk change the operator who last edited it, the date and time it was last edited, and the status of the bulk change is provided. If a bulk change has only been saved but not executed, the status will be blank. A bulk change that has been

successfully completed shall remain on the 'Successful' status until the next time it is edited, at which time it will revert to blank.

| Status | The bulk change... |
|---|---|
| Blank | has no status. The bulk change either has not been run or it has been redefined/saved since the last run. |
| Active | is running.<br>**Note:** Bulk changes go through a run twice to check if any items that were locked during the first run are now unlocked. |
| Cancelled | is idle, having been stopped due to an operator cancelling the operation. |
| Queued | is queued waiting for another bulk change that is running, to complete. |
| Successful | is idle, having completed with 100% success. |
| Failed | is idle, having completed with less than 100% success. |
| Failed -- Server Interruption | has failed due to a server failure while the bulk change is active or queued. |

**Note:** Saved bulk changes can be added to the Status Viewer.

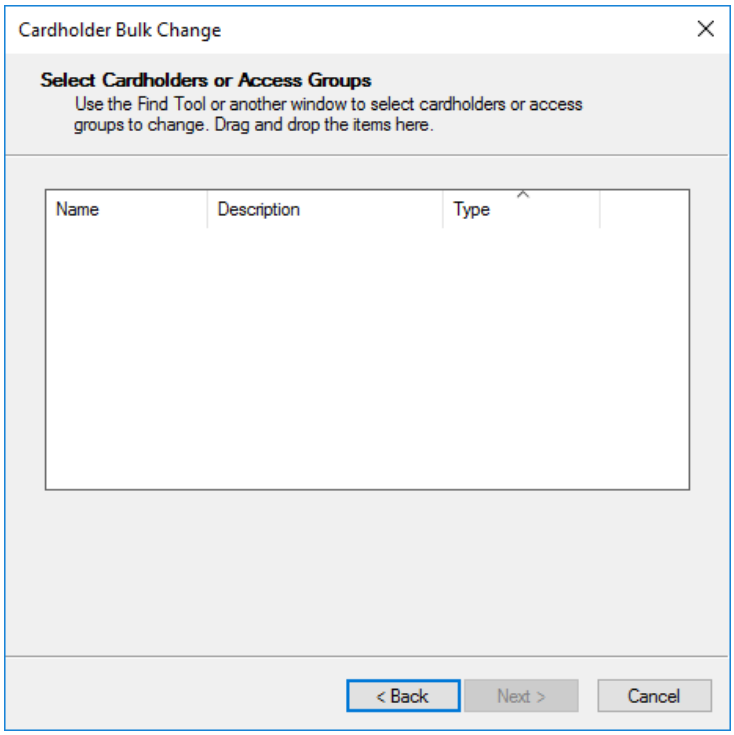
## Initiating a new Cardholder Bulk Change

### Introduction

This procedure describes how to initiate a new cardholder bulk change in Command Centre. To perform this procedure operator's need both the "Bulk Change" and "Edit Cardholders" operator privileges. In addition, operator's need sufficient divisional and other privileges to carry out each individual change listed within a bulk change.

### Procedure

1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** List Window opens (in grid view).
2. **Right click** and select **New...Cardholder Bulk Change**.
   The "Select Cardholders or Access Groups" screen of the Cardholder Bulk Changes Wizard displays.



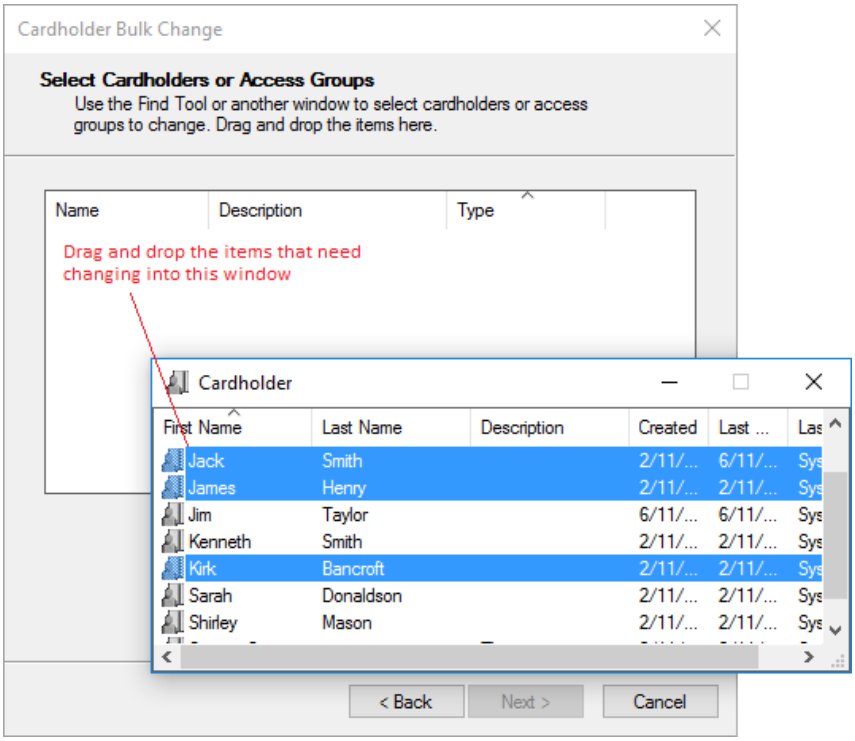

All the cardholders or Access Groups that require changing need to be placed onto this screen, by dragging and dropping them from either the **Cardholder** List Window or **Access Group** List Window as appropriate, or the Find Tool can be used. In this procedure the **Cardholder** List Window has been used.

**Notes:**

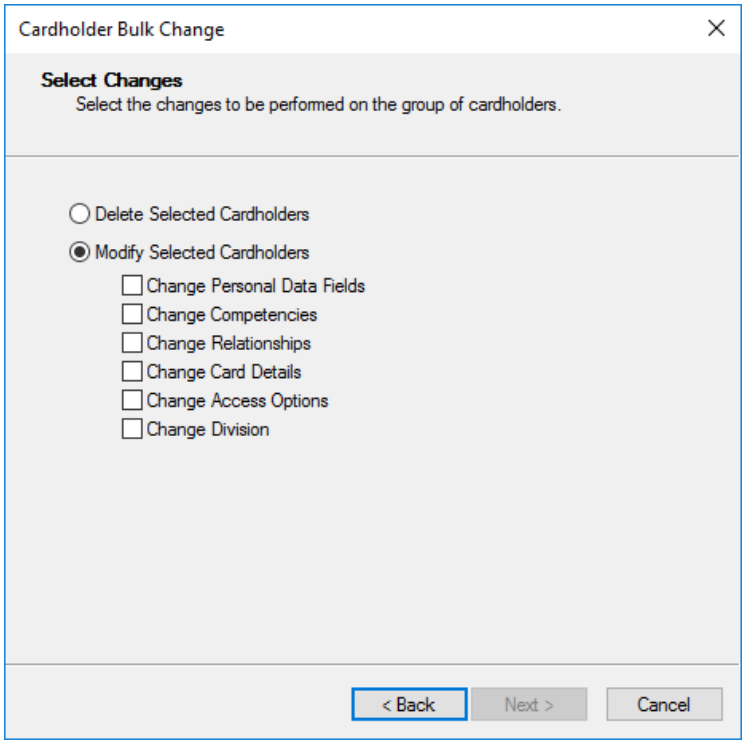
- Individual cardholders can be selected, or an Access Group can be selected if all the cardholders belonging to the group require changing.

- If a division bulk change is created, and an Access Group is dragged in to be changed, only the division of the Access Group will be changed. To change the cardholders in the division, either drag the Access Group into a cardholder bulk change and change the division, or drag the cardholders individually into the division change.

3. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
   Select those cardholders that need changing, and drag and drop them into this screen of the Wizard.




4. Close the **Cardholder** List Window.
5. Click the **Next** button.
   The "Select Changes" screen of the Cardholder Bulk Changes Wizard displays.




6. Click the radio button for the option you require, (i.e. either **Delete Selected Cardholders** or **Modify Selected Cardholders**). Only one of these options can be selected.

7. If **Modify Selected Cardholders** is selected, tick the checkboxes for the items you want to change.
   One or more of these options can be selected.
   **Note:** If your site is licensed for both Visitor Management and Notifications, a **Change Visitor Management Notifications** checkbox will also be available.

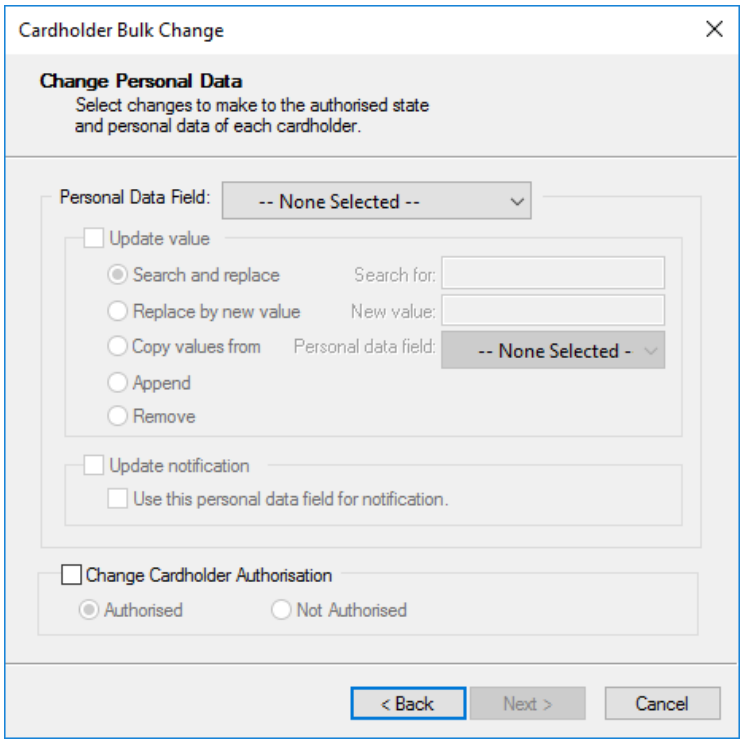
   The screen that displays next depends on what selections you made on the "Select Changes" screen.

| If you clicked the... | then... |
|---|---|
| **Delete Selected Cardholders** radio button | click the **Next** button, and go to Step 31. |
| **Modify Selected Cardholders** radio button | go to Step 8. |

8. Click the **Next** button.
   Individual screens will display for each of the items you ticked for changing.

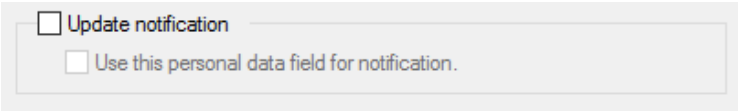
   **Note:** If you ticked the **Change Competencies** checkbox, see ***Competency Bulk Changes*** (on page 53-28) for further details.
   If you ticked the Change Relationships checkbox, see ***Assigning Cardholders to Roles via Bulk Change*** (on page 35-19) for further details.

9. The "Change Personal Data" screen will only display if the **Change Personal Data Fields** checkbox was ticked on the "Select Changes" screen. If not, go to Step 14.
   This screen allows you to select changes to make to the authorised state and personal data of each cardholder.




10. If you want to make personal data changes, select the Personal Data Field (PDF) from the drop-down list.
    The other options in the Personal Data Field section of this screen become enabled.
    **Notes:**

    - This Personal Data Field is the target PDF.
    - Image PDFs and unique PDFs cannot be changed in a bulk change, therefore these PDF types will not appear in the drop-down list.
    - If the PDF is an "Email" or "Mobile" type PDF, then an **Update Notification** checkbox becomes available, along with a **Use this personal data field for notification** checkbox.

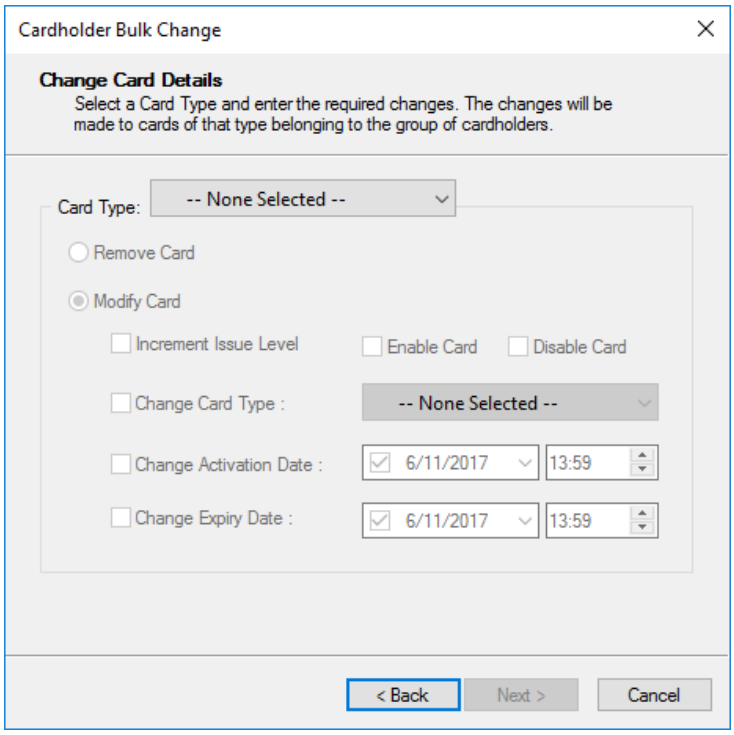
      These checkboxes can be selected in conjunction with any of the radio buttons in the **Update value** section above, with the exception of the **Remove** radio button.

11. Click the radio button for the type of change you want to make.

| Radio Button/Field | Description |
|---|---|
| Search and replace | When clicked, the **Search for** and **New value** fields are enabled allowing you to replace a selected value with a new one. |
| Replace by new value | When clicked, the **New value** field is enabled allowing you to replace a value. |
| Copy values from | When clicked, the **Personal data field** drop-down list beside it is enabled allowing you to replace the target PDF data with the data existing in the source PDF. |
| Append | When clicked, the **New value** field is enabled allowing you to append a new value to existing data.<br>**Note:** If the Personal Data Field selected is a "Numeric", "Text - list" or "Date" PDF, this field will not be enabled as it is not possible to append these types of PDFs. |
| Remove | When clicked, no additional fields are enabled, but this allows you to remove data.<br>**Note:** If the PDF is required to have data in it, (i.e. it is mandatory), the **Remove** option will not be available. |
| Search for | The text to be searched for is entered (limited to 200 characters), and replaced with what is entered in the **New value** field wherever it is found in the PDF of the selected cardholders.<br>**Notes:**<br>• If the Personal Data Field selected is a "Text - list" PDF, the **Search for** field becomes a drop-down list containing the optional text strings available.<br>• For "Date" PDFs the **Search for** field changes to a Date/Time control and a checkbox is included to represent 'no value', but only for non required PDFs. |
| New value | Enter new value for PDF (limited to 200 characters). This is checked to make sure it contains valid data.<br>**Notes:**<br>• If the Personal Data Field selected is a "Text - list" PDF, the **New value** field becomes a drop-down list containing the optional text strings available. |

| Radio Button/Field | Description |
|---|---|
| | • For "Date" PDFs the **New value** field changes to a Date/Time control and a checkbox is included to represent 'no value', but only for non required PDFs. |
| Personal data field (source) | This is the source PDF. When selecting the **Copy values from** option, the data in this source PDF will be "copied" to the target PDF.<br>**Note:** The source PDF must be of the same data type as the target PDF. However "Text", "Text-List", "Email", "Mobile", "Address" and "Phone" type PDFs can be used interchangeably since the underlying type is "Text" for all of these. |

12. If you want to make changes to the authorised state of each cardholder tick the **Change Cardholder Authorised** checkbox.
    The radio buttons in that section become enabled.
13. Click the radio button for the state you require, (i.e. **Authorised** enables a card for use and **Unauthorised** disables a card), and click the **Next** button.
14. The "Change Card Details" screen will only display if the **Change Card Details** checkbox was ticked on the "Select Changes" screen. If not, go to Step 17.
    This screen allows you to select changes to make to the Card Type.




15. Select the Card Type from the drop-down list.
    The fields on this screen become enabled.
16. Do you want to remove or modify the selected card type for cardholders?

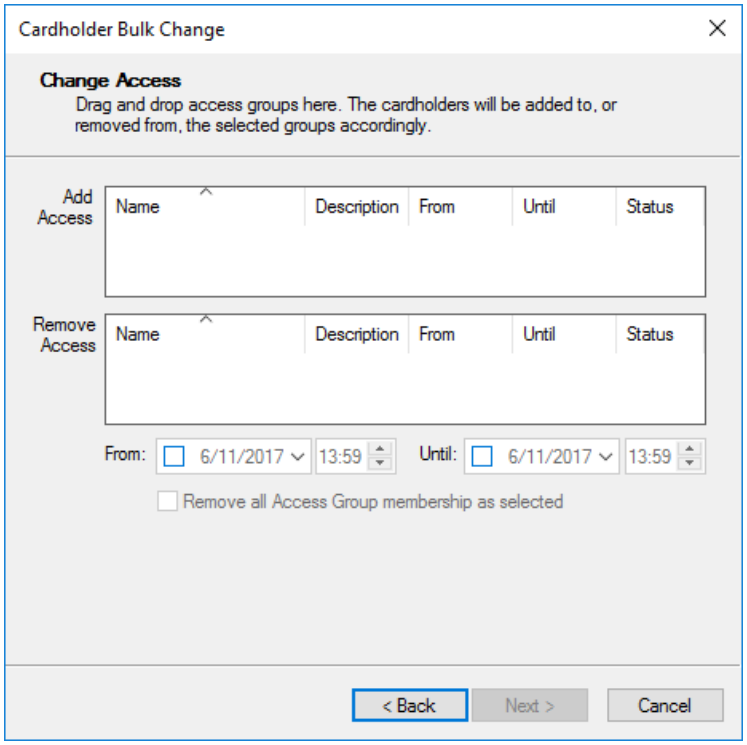
| If... | then... |
|---|---|
| remove, | click the **Remove Card** radio button and go to Step 18. |
| modify, | click the **Modify Card** button. |

17. Configure the changes you want to make as necessary, and click the **Next** button.
    One or more of these options can be selected.

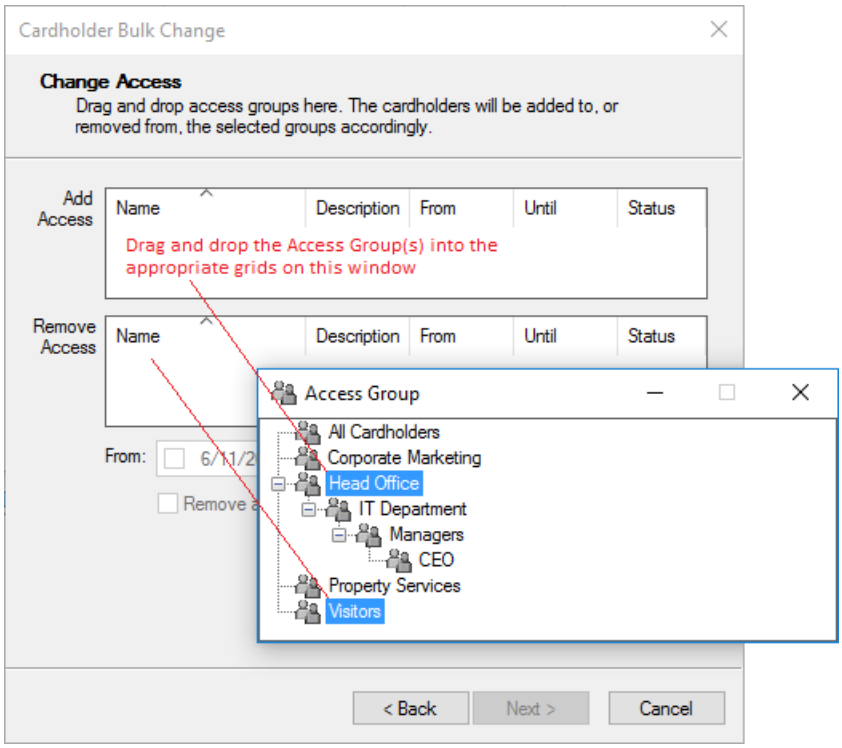
| Checkbox | Description |
|---|---|
| Increment Issue Level | Tick if the selected cardholders require bulk incrementation of card issue level. |
| Enable/Disable Card | Choose to either enable or disable the card by ticking the appropriate checkbox. |
| Change Card Type | Tick if the card type of the card for the selected cardholders requires changing. When ticked, the drop-down field is enabled allowing you to select a different card type.<br>**Notes:**<br>• Only card types with the same Card Number Formats can be exchanged.<br>• Only those card types that you have view privileges for will appear in the drop-down list.<br>• If a cardholder has more than one card of a Card Type, they will all be changed unless one card fails to update. When a card fails to update, no cards for that particular cardholder will be updated.<br>• Only cards in a non-customised card state at the time the bulk change is run will be able to change card type, (i.e. cards in any state including Lost, Stolen and Damaged can be changed, but not cards in a card state that is added manually by an operator. |
| Change Activation Date | Tick if the access start date needs to be changed. When ticked, the date and time fields are enabled allowing you to select a new activation date. |
| Change Expiry Date | Tick if the access end date needs to be changed. When ticked, the date and time fields are enabled allowing you to select a new expiry date. |

18. The "Change Access" screen will only display if the **Change Access Options**

checkbox was ticked on the "Select Changes" screen. If not, go to Step 26. This screen allows you to change access options for Access Groups as necessary.



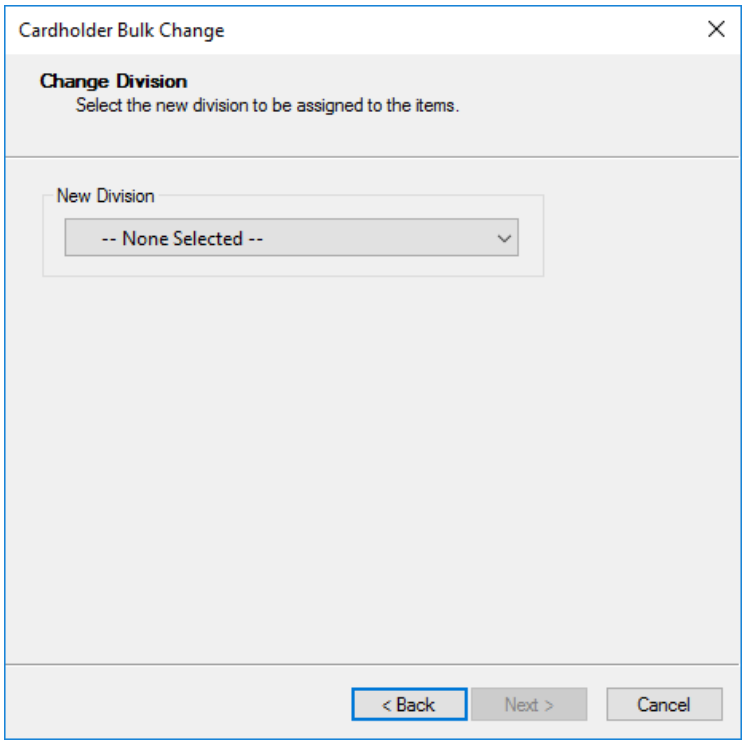

19. Click **Manage** from the menu bar, then **Access Groups**.
The **Access Group** List Window opens.
Select the Access Groups that the cardholders need adding to and/or removing from, and drag and drop them into the appropriate grids on this screen of the Wizard, then close the **Access Group** List Window.



20. The 'From' and 'Until' date/time fields on this screen allow temporary membership to an Access Group to be configured if necessary.
    If temporary access is required, go to Step 21.
    If permanent access is required, go to Step 25.
21. Highlight the Access Group (on the **Change Access** screen of the Wizard) the cardholders require temporary access to.
    The 'From' and 'Until' Date fields become enabled.
22. Click the 'From' drop-down box and select the date the cardholders need access to this Access Group from.
    The 'From' Time Box becomes enabled, and the 'From' date now displays in the grid beside the Access Group name.
23. Select the time in the 'From' Time Box that the cardholders need access from on this date.
24. Repeat Steps 21 and 22 for the 'Until' fields, (i.e. the date and time of the last day the cardholders need access up to).
    The 'Until' date now displays in the grid beside the Access Group name.
25. Check the **Remove all Access Group membership as selected** checkbox if required.

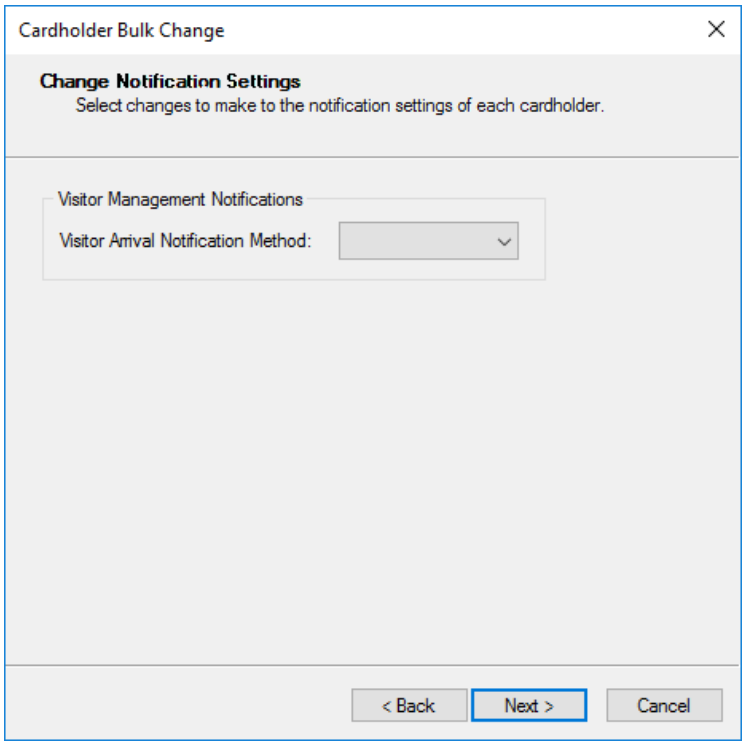
| If... | then... |
|---|---|
| checked | all Access Groups listed in the 'Remove Access' grid will be removed from the nominated Cardholders irrespective of 'From' and 'Until' dates/times, that may or may not have been entered for each Access Group selection. |
| unchecked, and no 'From' date/time is entered | only permanent access will be removed. |
| unchecked, and a 'From' date/time is entered | only one temporary access for that exact period will be removed. |

26. Click the **Next** button.
27. The "Change Division" screen will only display if the **Change Division** checkbox was ticked on the "Select Changes" screen. If not, go to Step 29.
    This screen allows you to select a new division to which these cardholders will be changed.

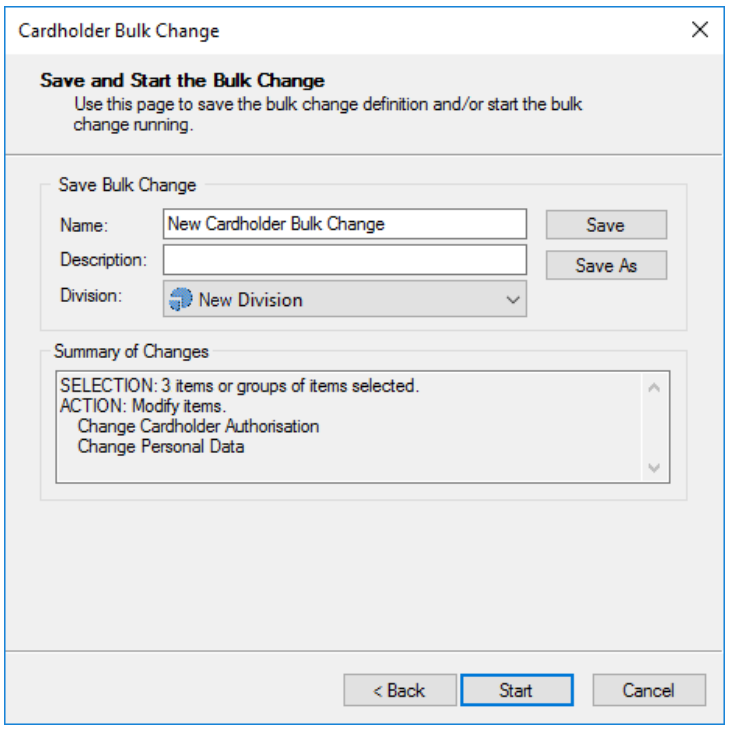



28. Select a division from the drop-down list.
    **Note:** Only divisions to which you have "Edit Cardholder" operator privilege will appear in the drop-down list.

29. The "Change Notification Settings" screen will only display if the **Change Visitor Management Notifications** checkbox was ticked on the "Select Changes" screen. If not, go to Step 30.
    This screen allows you to select the notification method that will be assigned to each Cardholder, to indicate the arrival of a visitor.



30. Select a notification method from the drop-down list, (i.e. "None", "Email", "SMS" or "Email and SMS").
31. The "Save and Start the Bulk Change" screen of the Cardholder Bulk Changes Wizard displays.

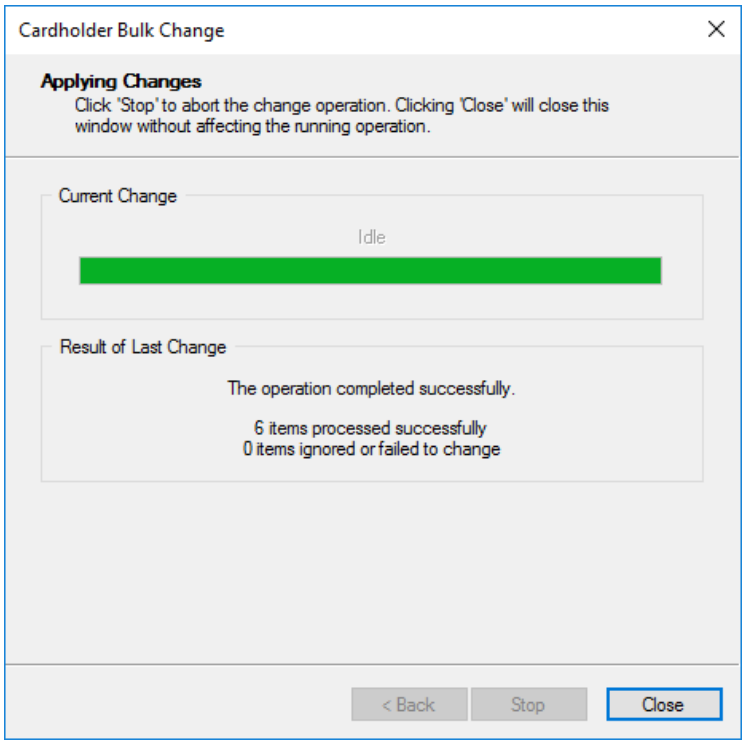



The **Summary of Changes** section provides a summary of the changes for you to check before proceeding.

32. Do you want to save this bulk change and it's settings before running?

| If... | then... |
|---|---|
| no | go to Step 34. |
| yes | type in a name and description.<br>**Note:** The **Name** field is limited to 60 characters and the **Description** field is limited to 200 characters. |

33. Click the **Save** button.
    This Bulk Change and its settings are saved and now displays in the **Bulk Changes** List Window.
    **Note:** The **Save As** button allows you to change an existing Bulk Change and re-save it as a new Bulk Change with a different name. If you open an existing saved Bulk Change and click the **Save As** button without changing the name, a message displays indicating that a Bulk Change with that name already exists.
34. Click the **Start** button.
    The "Applying Changes" screen of the Cardholder Bulk Changes Wizard displays.




This screen shows the progress of the bulk change. While in progress, the status of this bulk change will show as 'Active' in the **Bulk Changes** List Window, and if it completes successfully, (i.e. the progress bar reaches 100%), the status will change to 'Successful'. When it completes the number of cardholders changed displays.

**Notes:**

- If you did not name and save the bulk change before clicking the **Start** button, while the "Applying Changes" screen displays, the bulk change will appear in the **Bulk Changes** List Window with a system-generated name, until is completes successfully, at which time the system will delete it. While it is active or if it fails, it will remain in the **Bulk Changes** List Window until an operator deletes it.
- If you click the **Stop** button while the bulk change is in progress, any changes already made when it is stopped cannot be cancelled, instead they are completed. If the **Stop** button is clicked, you get the option to end the bulk change, or to go back and edit it.

**Result**

A Cardholder Bulk Change has been initiated.

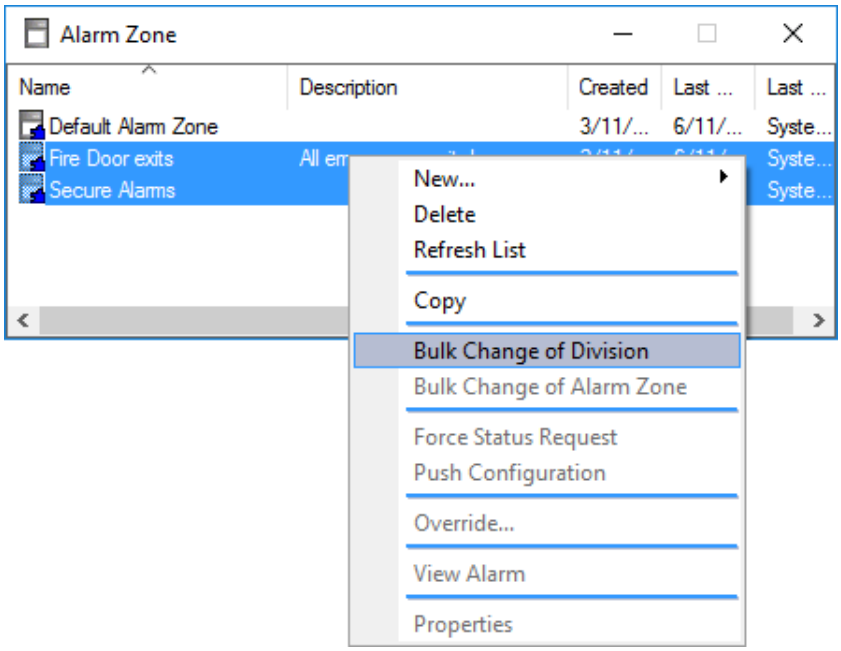
# Initiating a new Division Bulk Change

## Introduction

This procedure describes how to initiate a new division bulk change in Command Centre. Bulk changes to divisions can be performed on any Command Centre item that allows you to multiple select items, and has 'Division' as one of its fields, (e.g. Card Types, Personal Data Fields, Doors, Alarm Zones, Access Zones, etc.).
To perform this procedure operator's need both the "Bulk Change" operator privilege as well as the appropriate item editing privilege.

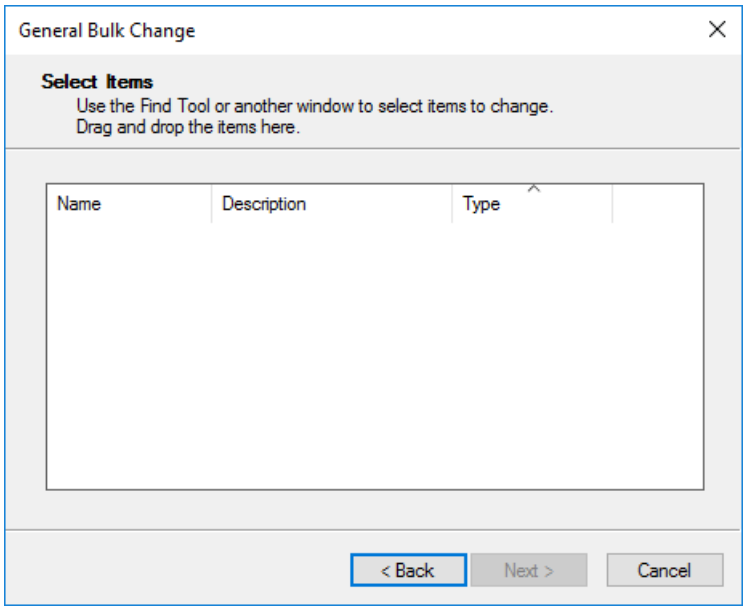
There are two methods of performing this procedure. You can either use:

- the General Change Wizard, or
- the context menu option available from an items List Window. Using this method, you select the items that need their division changing, **right click** and select **Bulk Change of Division** from the context menu. The "Change Division" screen of the Bulk Changes of Division Wizard displays. Complete Steps 7 and 8 in the following procedure to complete a bulk change of division using this method.



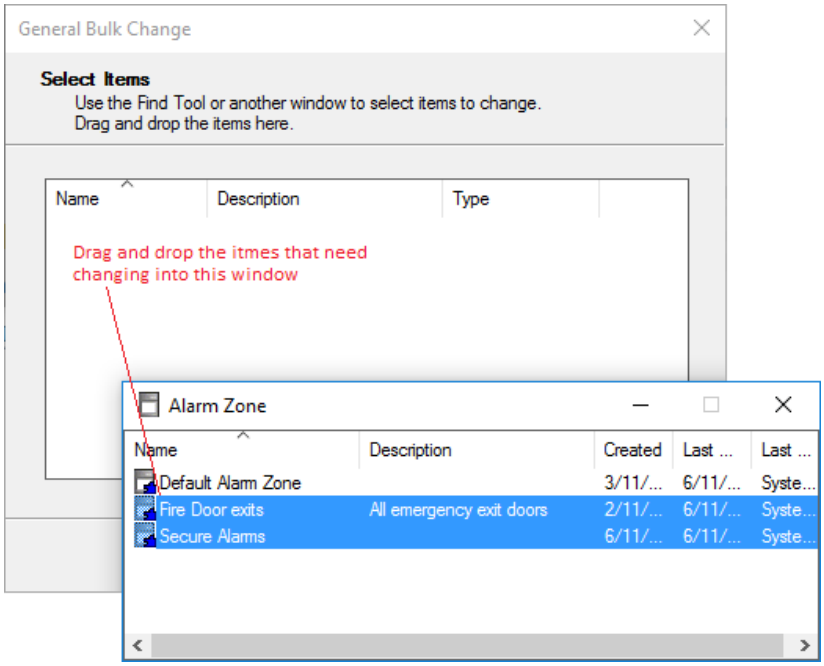

## Procedure (using the Wizard)

1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** List Window opens (in grid view).
2. **Right click** and select **New...General Bulk Change**.
   The "Select Items" screen of the General Bulk Change Wizard displays.

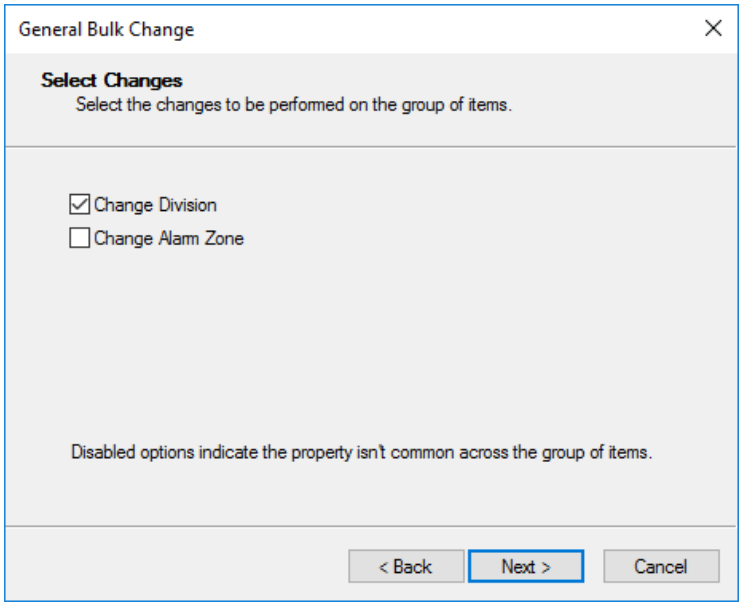



All the items that require changing need to be placed onto this screen, by dragging and dropping them from the appropriate List Window, or the Find Tool can be used. As an example, in this procedure Alarm Zones require division changes.

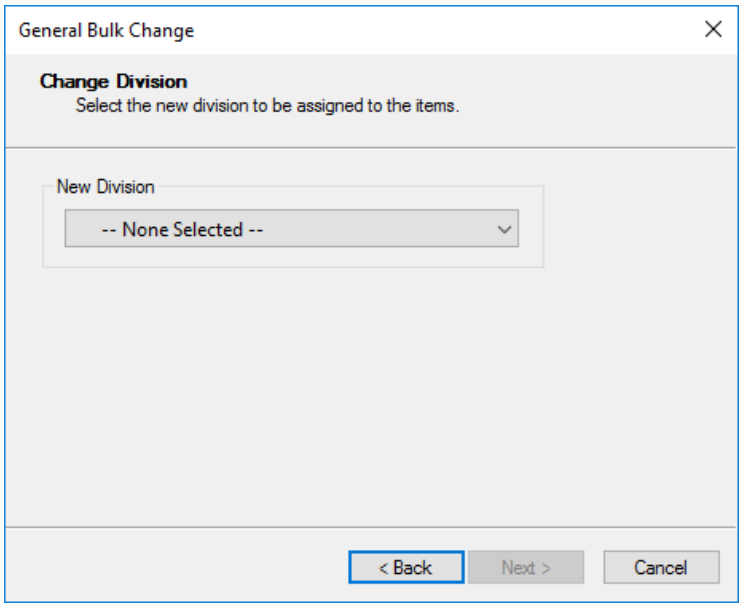
3. Open the Command Centre item List Window and select those items that need changing.
   Drag and drop them into this screen of the Wizard.



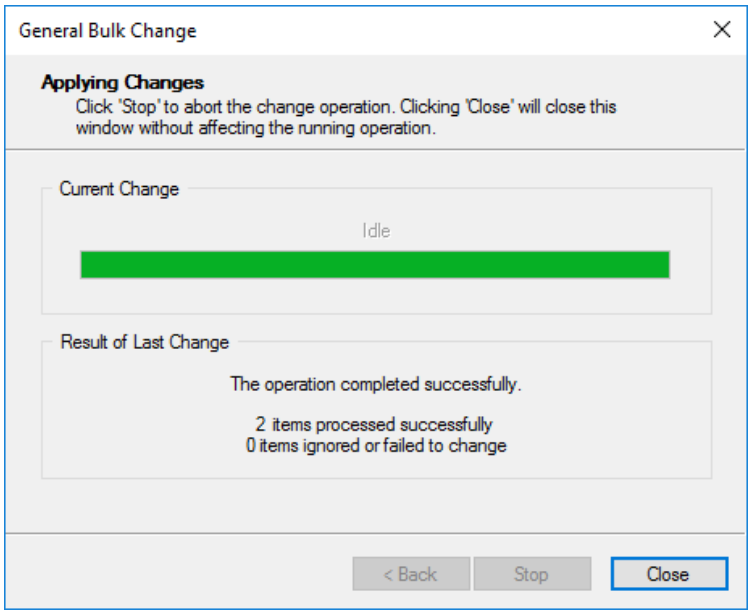

4. Close the Command Centre item List Window.
5. Click the **Next** button.
   The "Select Changes" screen of the General Bulk Change Wizard displays.




6. Ensure the **Change Division** checkbox is checked, and click the **Next** button.
   The "Change Division" screen of the General Bulk Change Wizard displays.




7. Select a new division to be assigned to these items from the drop-down list.
   **Note:** Only divisions to which you have the appropriate editing privilege will appear in the drop-down list.
8. Click the **Start** button.
   The "Applying Changes" screen of the General Bulk Change 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 Division 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 Divisions has been initiated, and the selected items have had their division changed.

# Initiating an Inactive Cardholder Bulk Purge

## Introduction

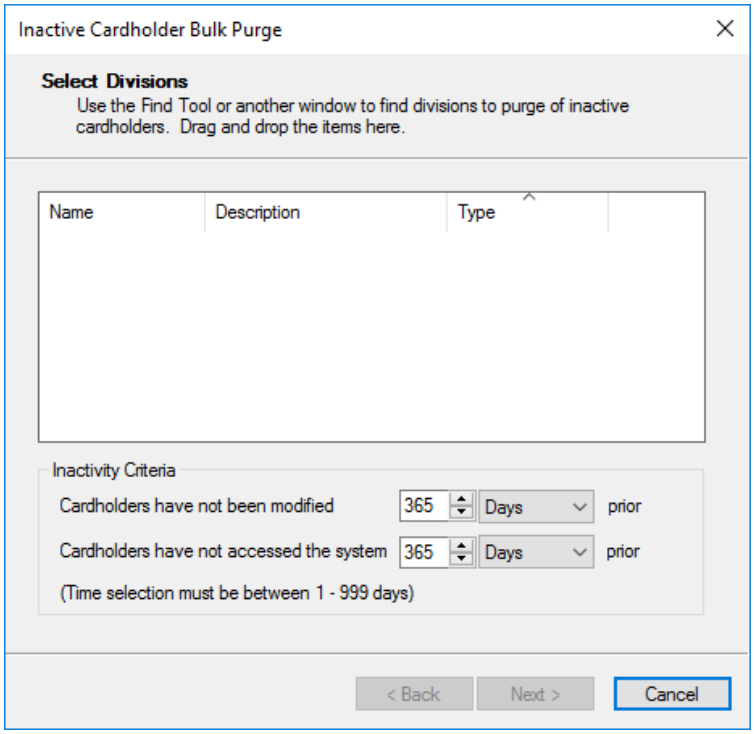
This procedure describes how to purge all cardholders stored in one of a specified list of divisions, where:

- the most recent activity on the cardholder exceeds a specified number of days, and
- the cardholder is not a visitor or host on an active visit, (i.e. a visit with a status of 'Scheduled' or 'In Progress'), for the purposes of Visitor Management (a licensable feature).

To perform this procedure operator's need both the "Bulk Change" and "Edit Cardholders" operator privileges. In addition, operator's need sufficient divisional and other privileges to carry out each individual change listed within a bulk purge.
**Note:** An Inactive Cardholder Bulk Purge can be scheduled to run at specific times, via a Macro. See ***Macros*** (on page 20-1) for further details.

## Procedure

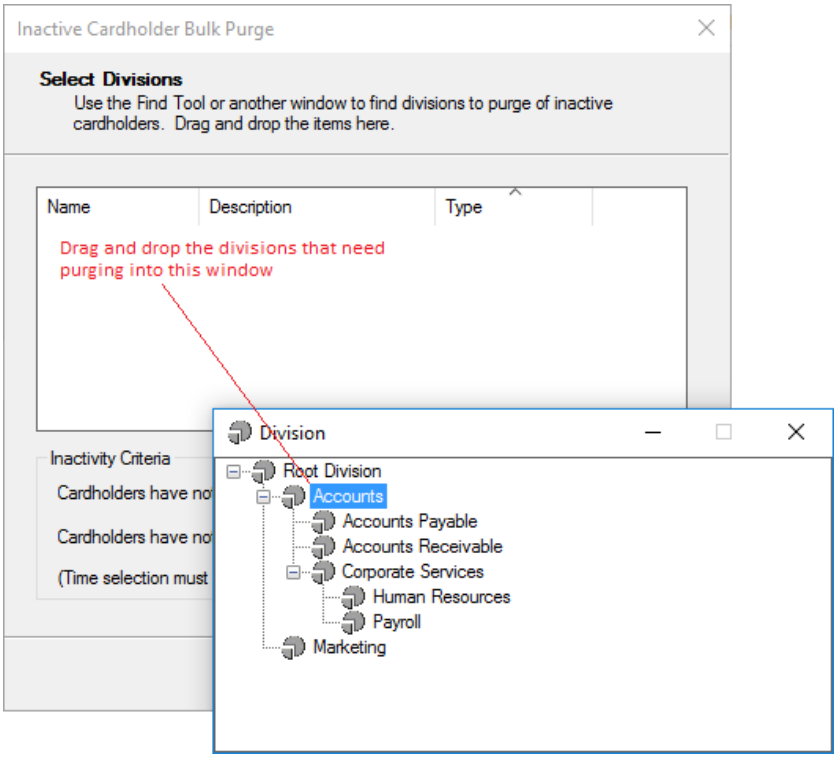
1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** List Window opens (in grid view).
2. **Right click** and select **New...Inactive Cardholder Bulk Purge**.
   The "Select Divisions" screen of the Inactive Cardholder Bulk Purges Wizard displays.



All the divisions that need to be placed onto this screen can be dragged and dropped from either the **Division** List Window or the Find Tool can be used. In this procedure the **Division** List Window has been used.

3. Click **Configure** from the menu bar, then **Divisions**.

   The **Division** List Window opens.
   Select those divisions that have inactive cardholders that require purging, and drag and drop them into this screen of the Wizard.

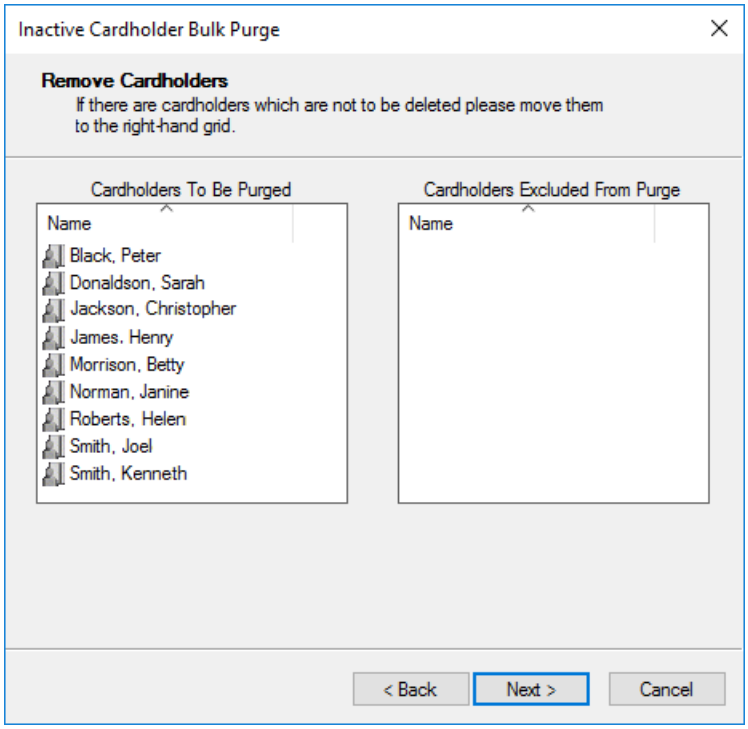



   **Note:** When a division is dragged on, it's entire child hierarchy is dragged on also. In the above screen example, if the "Accounts" division is dragged onto the Wizard, the "Accounts Payable" and "Accounts Receivable" divisions will also be dragged on.

4. Specify the number of days it will be until a cardholder is classified as inactive, by entering a number in the 365 field. (Default = 365 days; Limit = 1 -999 days)

5. Close the **Division** List Window.

6. Click the **Next** button.
   The "Remove Cardholders" screen of the Inactive Cardholder Bulk Purges Wizard displays.

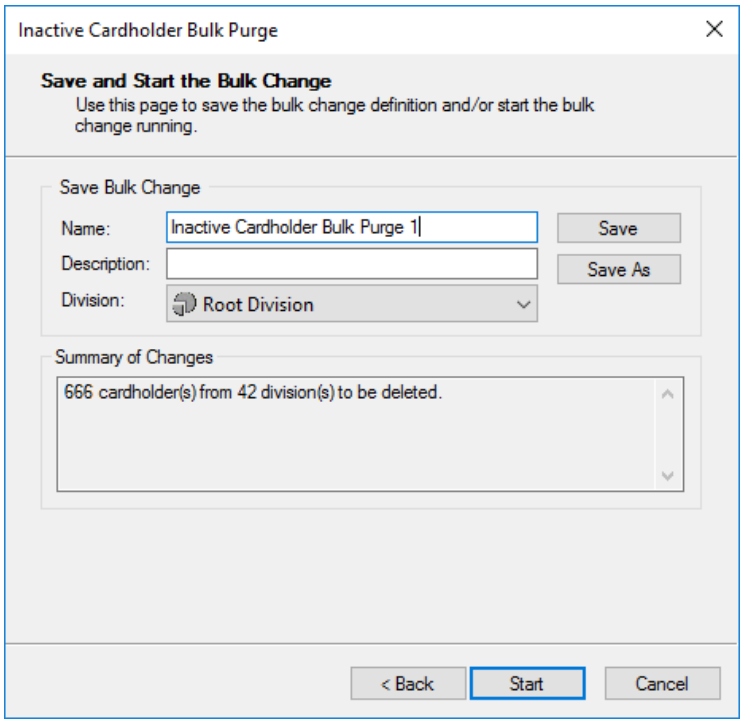



The **Cardholders To Be Purged** grid on the left is populated with the inactive cardholders from the chosen divisions.

**Notes:**

- An inactive cardholder is one where the cardholder last badged their card more than the specified number of days ago, and has not been modified in that time either. If they are associated with a visit somehow they will not be able to be deleted.
- Cardholders that are part of an Operator Group will always be excluded even if they are not placed in the **Cardholders Excluded From Purge** grid (on the right).

7. Drag any cardholders you do not want to delete from the **Cardholders To Be Purged** grid (on the left) to the **Cardholders Excluded From Purge** grid (on the right).
8. Click the **Next** button.
   The "Save and Start the Bulk Change" screen of the Inactive Cardholder Bulk Purges Wizard displays.

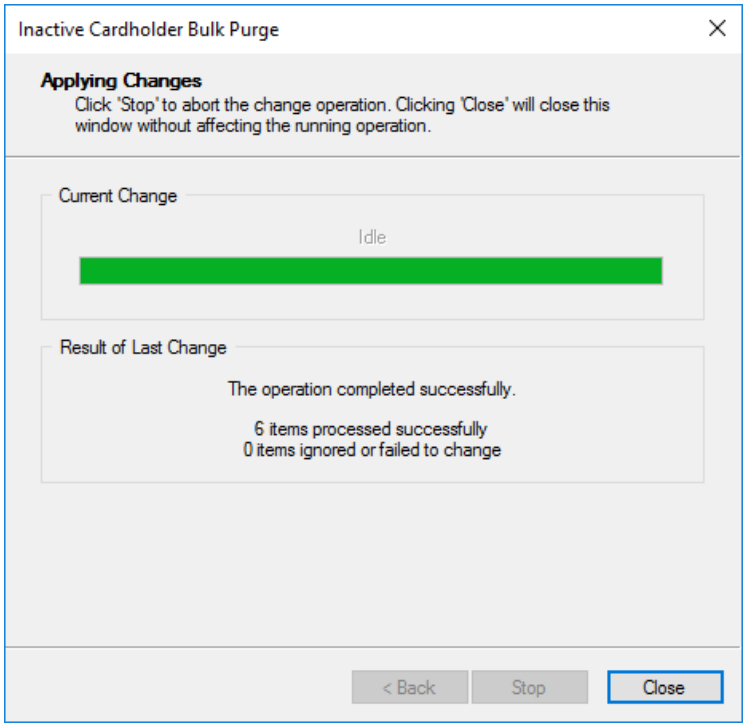



The **Summary of Changes** section provides a summary of the changes for you to check before proceeding.

9. Do you want to save this bulk change and it's settings before running?

| If... | then... |
|---|---|
| no | go to Step 11. |
| yes | type in a name and description.<br>**Note:**<br>The **Name** field is limited to 60 characters and the **Description** field is limited to 200 characters. |

10. Click the **Save** button.
    This Bulk Purge and its settings are saved and now displays in the **Bulk Changes** List Window.
    **Note:**
    The **Save As** button allows you to change an existing Bulk Purge and re-save it as a new Bulk Purge with a different name. If you open an existing saved Bulk Purge and click the **Save As** button without changing the name, a message displays indicating that a Bulk Purge with that name already exists.
11. Click the **Start** button.
    The "Applying Changes" screen of the Inactive Cardholder Bulk Purges Wizard displays.




This screen shows the progress of the bulk purge. While in progress, the status of this bulk purge will show as 'Active' in the **Bulk Changes** List Window, and if it completes successfully, (i.e. the progress bar reaches 100%), the status will change to 'Successful'. When it completes the number of cardholders changed displays.

**Notes:**

- If you did not name and save the bulk change before clicking the **Start** button, while the "Applying Changes" screen displays, the bulk change will appear in the **Bulk Changes** List Window with a system-generated name, until is completes successfully, at which time the system will delete it. While it is active or if it fails, it will remain in the **Bulk Changes** List Window until an operator deletes it.
- If you click the **Stop** button while the bulk change is in progress, any changes already made when it is stopped cannot be cancelled, instead they are completed. If the **Stop** button is clicked, you get the option to end the bulk purge, or to go back and edit it.

**Result**

Selected cardholders have been deleted from the system.

## Editing and Running a saved Cardholder Bulk Change

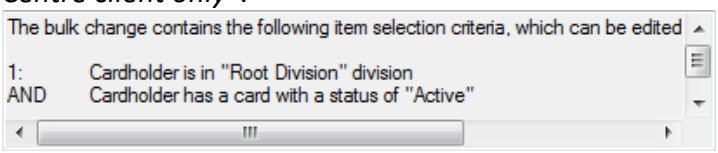
### Introduction

This procedure describes how to edit and run an existing bulk change in Command Centre. To perform this procedure operator's need both the "Bulk Change" operator privilege as well as the appropriate item editing privilege.
**Notes:**

- When a bulk change is run, it uses ALL privileges an operator has, regardless of their currently selected system view. For example, an operator may exclude an operator privilege from their current system view, but if a bulk change is run, that privilege will form part of the operator privileges under which the bulk change will run.
- Bulk changes are subject to any workstation restrictions in place on the workstation at which it is run.

### Procedure

1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** List Window opens (in grid view).
2. Highlight the bulk change that you want to edit and run, and **double click** the mouse button.
3. Has the bulk change been run before?

| If... | then the Bulk Changes Wizard opens at the... |
|---|---|
| no, (i.e. it has no status in the **Bulk Changes** List Window) | "Select Cardholders or Access Groups" screen.<br>a) Using the **Next** button, work your way through the Wizard, making any changes as necessary.<br>b) When you get to the "Save and Start the Bulk Change" screen, go to Step 4.<br>**Note:** If the Cardholder Bulk Change was configured in the Command Centre Client rather than the Configuration Client, AND it was configured with criteria, (i.e. advanced search rules), then the following message will display at the bottom of the wizard screen: *"The bulk change contains the following item selection criteria, which can be edited in the Command Centre client only"*.<br> |

| If... | then the Bulk Changes Wizard opens at the... |
|---|---|
| yes, (i.e. it has a status in the **Bulk Changes** List Window) | "Applying Changes" screen. This allows you to view the results from the last time it was run.<br>a) Using the **Back** button, work your way back through the Wizard to make any changes if necessary, or just go back to the "Save and Start the Bulk Change" screen to run it.<br>b) Go to Step 4. |

4. On the "Save and Start the Bulk Change" screen, the name and description of the existing bulk change populate the **Name** and **Description** fields. Do you want to save the changes to the existing bulk change or do you want to save these changes as a new bulk change?

| If you want to... | then... |
|---|---|
| save the changes to the existing bulk change | click the **Save** button. The bulk change will be re-saved with your edits made. |
| save this as a new bulk change | change the name and description, then click the **Save As** button.<br>Both the original bulk change and the newly named bulk change will display in the **Bulk Changes** List Window.<br>**Note:** If you click the **Save As** button without changing the Name, an error message will display indicating that the Name must be changed. |

5. Click the **Start** button.
   The "Applying Changes" screen of the Cardholder Bulk Changes Wizard displays. This screen shows the progress of the bulk change. While in progress, the status of this bulk change will show as 'Active' in the **Bulk Changes** List Window, and if it completes successfully, (i.e. the progress bar reaches 100%), the status will change to 'Successful'. When it completes the number of cardholders changed displays.
   **Note:** If you click the **Stop** button while the bulk change is in progress, any changes already made when it is stopped cannot be cancelled, instead they are completed. If the **Stop** button is clicked, you get the option to end the bulk change, or to go back and edit it.

**Result**

An existing (saved) bulk change has been edited and run.

**Hint**

*Deleting saved Cardholder Bulk Changes*
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete a saved Cardholder Bulk Change.
**Note:** A bulk change cannot be deleted if it is included in a macro.

# Initiating a new Alarm Zone Bulk Change

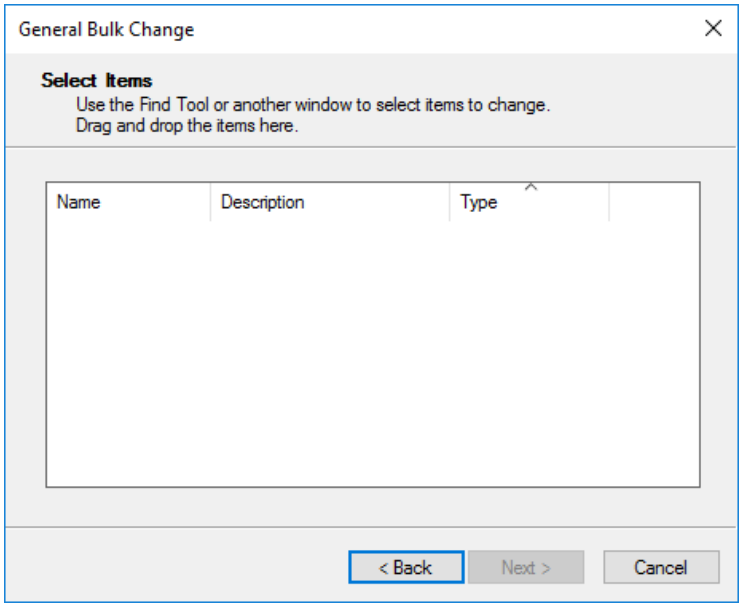
## Introduction

This procedure describes how to add multiple Command Centre items to an Alarm Zone. Bulk changes to Alarm Zones can be performed on any Command Centre item that allows you to multiple select items, (e.g. Card Types, Personal Data Fields, Doors, Access Zones, etc.). To perform this procedure operator's need both the "Bulk Change" operator privilege as well as the appropriate item editing privilege.

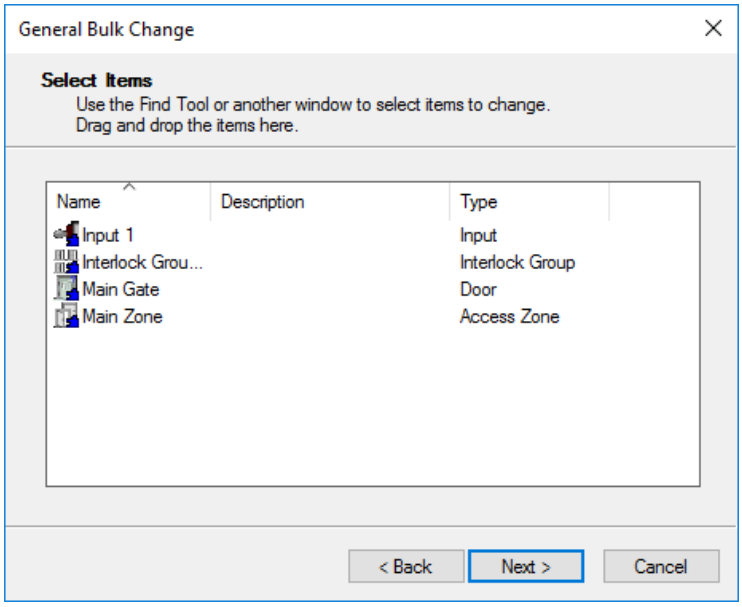
There are three methods of adding multiple Command Centre items to an Alarm Zone. This procedure describes using the General Change Wizard. For the other methods, refer to ***Adding multiple items to Alarm Zones*** (on page 14-18).

## Procedure (using the Wizard)

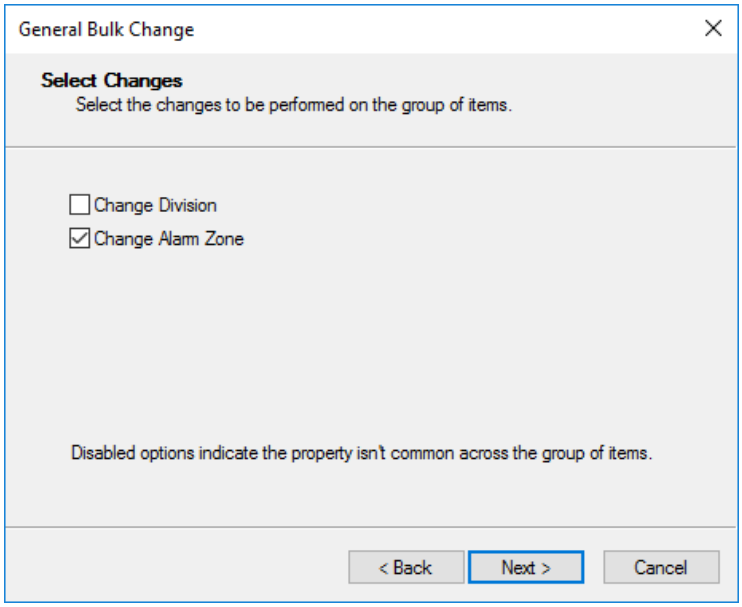
1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** List Window opens (in grid view).
2. **Right click** and select **New...General Bulk Change**.
   The "Select Items" screen of the General Bulk Change Wizard displays.



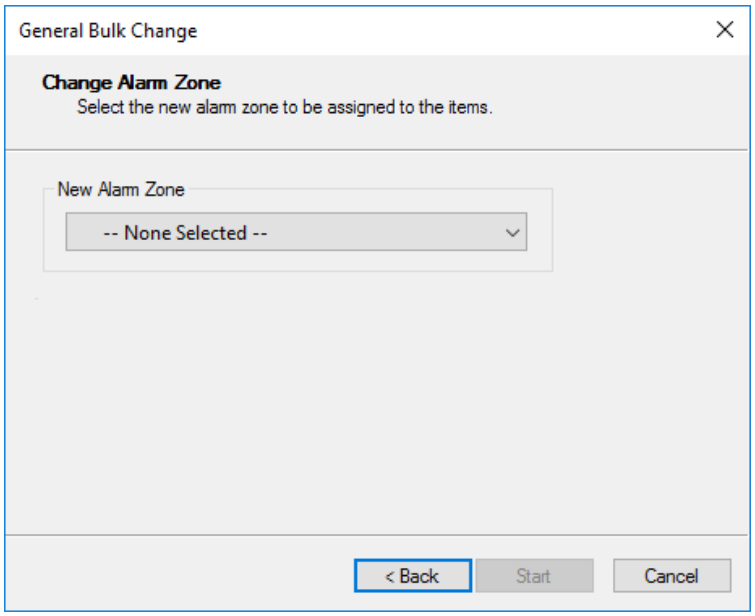

3. Place all the items to be added to the Alarm Zone onto this screen, by dragging and dropping them from the appropriate List Window, or by using the Find Tool.




4. Click the **Next** button.
   The "Select Changes" screen of the General Bulk Change Wizard displays.

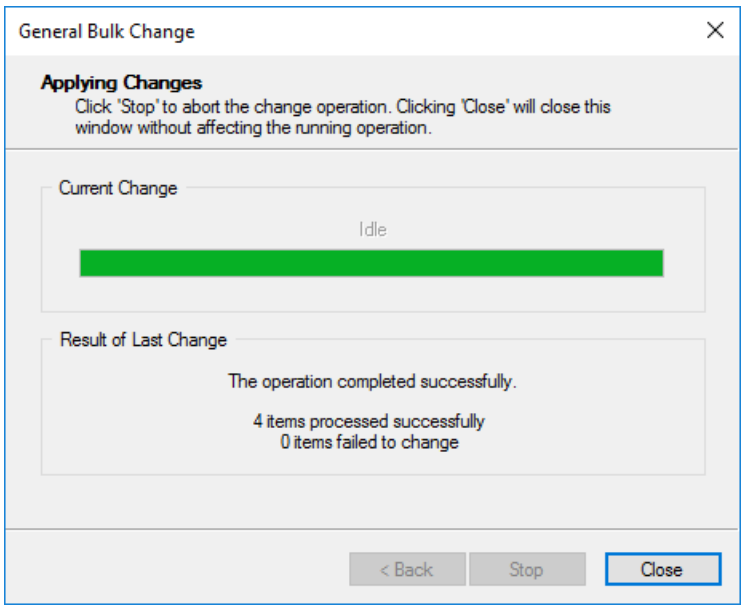



5. Ensure the **Change Alarm Zone** checkbox is checked, and click the **Next** button.
   The "Change Alarm Zone" screen of the General Bulk Change Wizard displays.




6. Select a new Alarm Zone to be assigned to these items from the drop-down list.
   **Note:** Only Alarm Zones to which you have the appropriate editing privilege will appear in the drop-down list.

7. Click the **Start** button.
   The "Applying Changes" screen of the General Bulk Change 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 Alarm Zones has been initiated, and the selected items have been added to the Alarm Zone.

# Initiating a new Controller 6000 Bulk Change

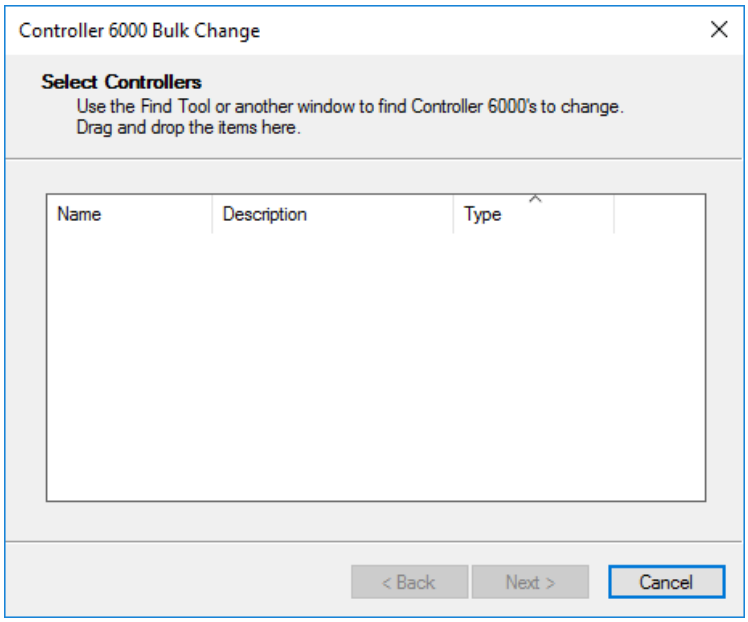
## Introduction

This procedure describes how to initiate a new Controller 6000 bulk change in Command Centre. To perform this procedure operator's need the "Bulk Change" operator privilege.

**Note:** It is recommended that you do **NOT** run multiple Controller bulk changes at once. This could mean that Controller bulk changes are run after hours. If this is the case, it is important that someone is on site when they are running in case there is a problem that needs addressing.

## Procedure (using the Wizard)

1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** List Window opens (in grid view).
2. **Right click** and select **New...Controller 6000 Bulk Change**.
   The "Select Controllers" screen of the Controller 6000 Bulk Change Wizard displays.

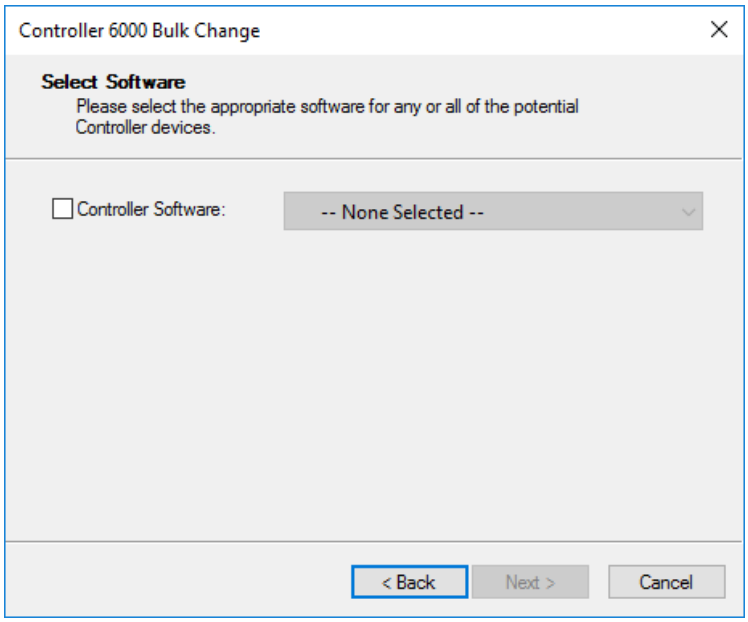



All the Controller 6000s that require changing need to be placed onto this screen, by dragging and dropping them from the **Hardware** List Window, or the Find Tool can be used.

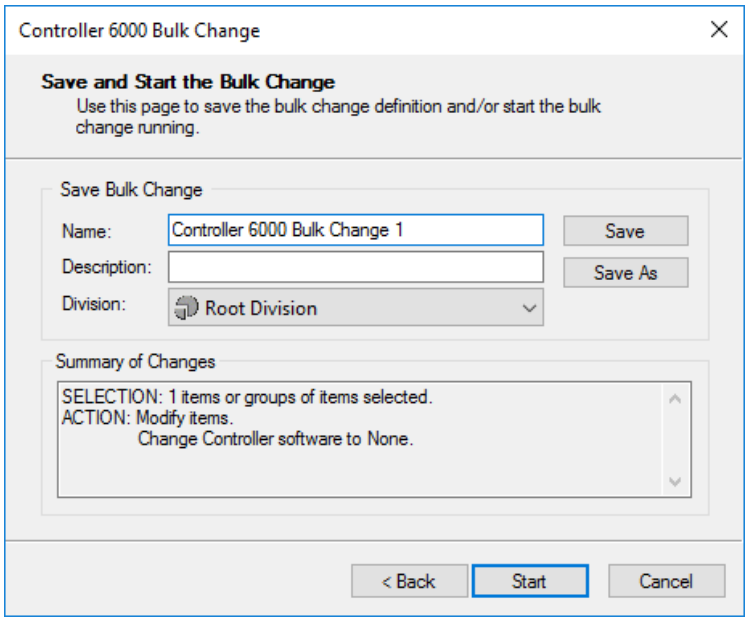
**Notes:**

- Only Controller 6000s can be dragged onto this grid.
- Up to 20 Controllers can be changed at a time in a bulk change, therefore if the number of Controllers in the grid exceeds 20, the **Next** button will remain disabled until there are less than 20 Controllers in the grid.

3. Select those Controllers that need changing (from either the Hardware List Window or the Find Tool), and drag and drop them into this screen of the Wizard.
4. Click the **Next** button.
   The "Select Software" screen of the Controller 6000 Bulk Change Wizard displays.




   Checking the **Controller Software** checkbox indicates that the software will be changed on the Controller(s). It will be possible to change the software to **-- None Selected --**, which will set the Controller(s) so that they do not have a specific software of that type, just as if it was chosen from the Controllers **Software** property page.
5. Check the appropriate checkbox and select the software from the drop-down list if required.
6. Click the **Next** button.
   The "Save and Start the Bulk Change" screen of the Controller 6000 Bulk Change Wizard displays.

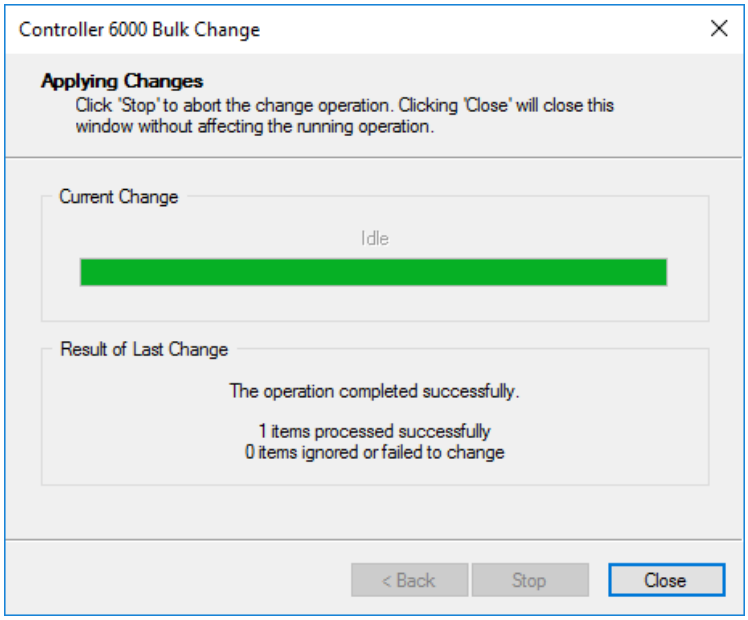



The **Summary of Changes** section provides a summary of the changes for you to check before proceeding.

7. Do you want to save this bulk change and it's settings before running?

| If... | then... |
|---|---|
| no | go to Step 9. |
| yes | type in a name and description.<br>**Note:** The **Name** field is limited to 60 characters and the Description field is limited to 200 characters. |

8. Click the **Save** button.
   This Bulk Change and its settings are saved and now displays in the **Bulk Changes** List Window.
   **Note:** The **Save As** button allows you to change an existing Bulk Change and re-save it as a new Bulk Change with a different name. If you open an existing saved Bulk Change and click the **Save As** button without changing the name, a message displays indicating that a Bulk Change with that name already exists.
9. Click the **Start** button.
   The "Applying Changes" screen of the Controller 6000 Bulk Change 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 Controller 6000s is active, or if it fails, it will remain in the **Bulk Changes** List Window until an operator deletes it.

**Result**

A Controller 6000 Bulk Change has been initiated.
**Note:** If the bulk change has previously been successfully run, then when the bulk change is opened again it will default to the **Select Software** screen.

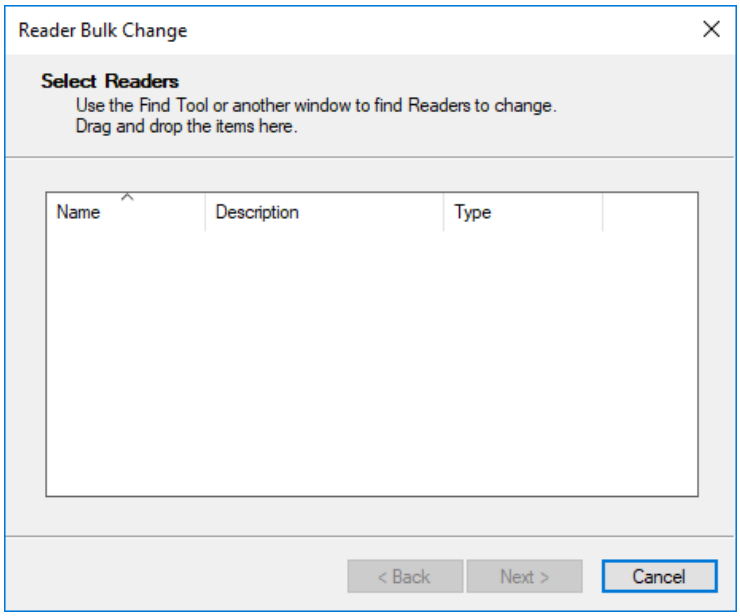
## Initiating a new Reader Bulk Change

### Introduction

This procedure describes how to initiate a new reader bulk change in Command Centre. A reader bulk change can be performed to change the card technologies accepted at readers.

### Procedure

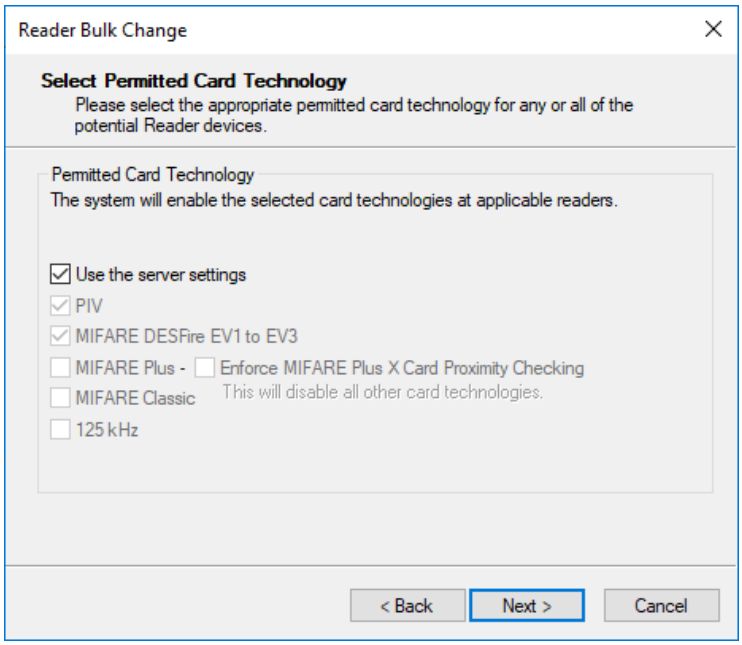
1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** List Window opens (in grid view).
2. **Right click** and select **New...Reader Bulk Change**.
   The "Select Readers" screen of the Reader Bulk Change Wizard displays.



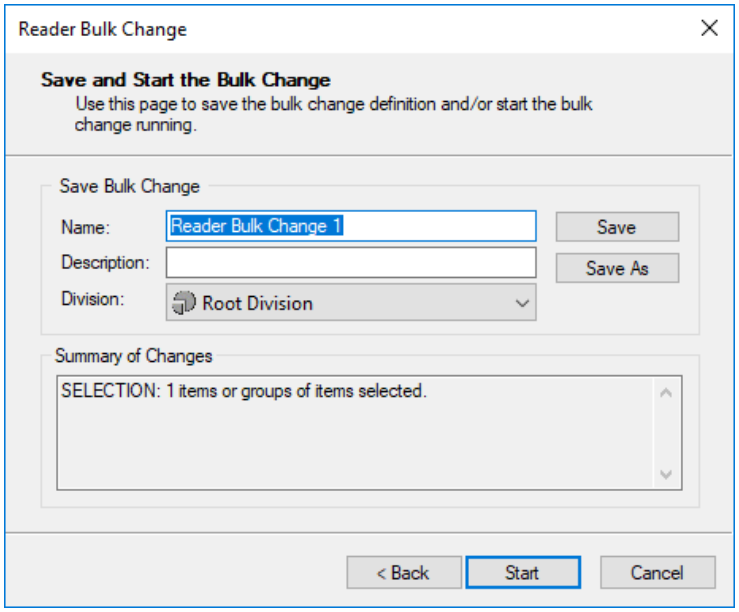

   All the readers that require changing need to be placed onto this screen, by dragging and dropping them from the appropriate List Window, or the Find Tool can be used.

   **Note:** You can use the Find Tool to locate all the readers you want to change the card technologies for, and then drag the search results onto this screen. See **Example 4: Advanced** (Example 4-D) for further detail.

3. Click the **Next** button.
   The "Select Permitted Card Technology" screen of the Reader Bulk Change Wizard displays.



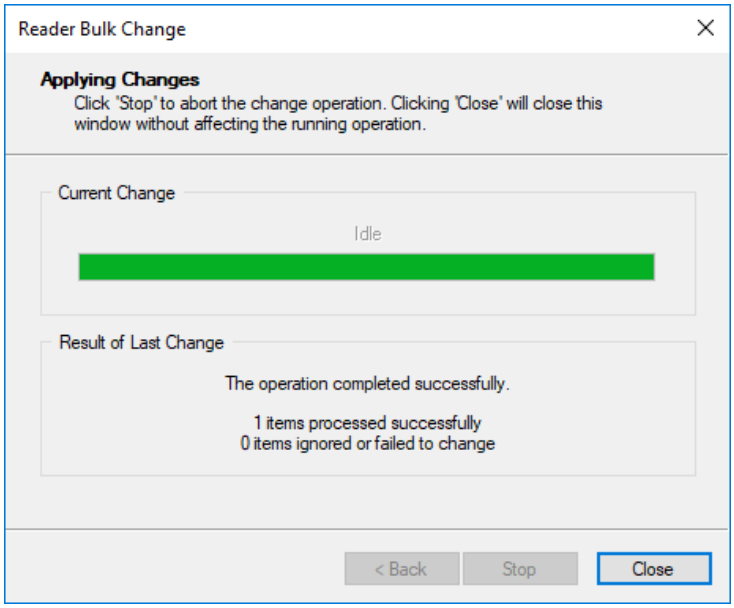

4. In the Permitted Card Technology section, **Use the server settings** is selected by default. If you want to select other types of cards to be accepted at the reader, uncheck the **Use the server settings** checkbox and select the appropriate checkboxes.
5. If your site is using MIFARE Plus cards 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.
6. 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.
7. Click the **Next** button.
   The "Save and Start the Bulk Change" screen of the Reader Bulk Change Wizard displays.




8. Do you want to save this bulk change and it's settings before running?

| If... | then... |
|---|---|
| no | go to Step 8. |
| yes | type in a name and description.<br>**Note:** The **Name** field is limited to 60 characters and the Description field is limited to 200 characters. |

9. Click the **Save** button.
   This Bulk Change and its settings are saved and now displays in the **Bulk Changes** List Window.
   **Note:** The **Save As** button allows you to change an existing Bulk Change and re-save it as a new Bulk Change with a different name. If you open an existing saved Bulk Change and click the **Save As** button without changing the name, a message displays indicating that a Bulk Change with that name already exists.
10. Click the **Start** button.
    The "Applying Changes" screen of the Reader Bulk Change 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 Readers 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 Readers has been initiated, and the selected readers have had the card technologies that are accepted at them changed.

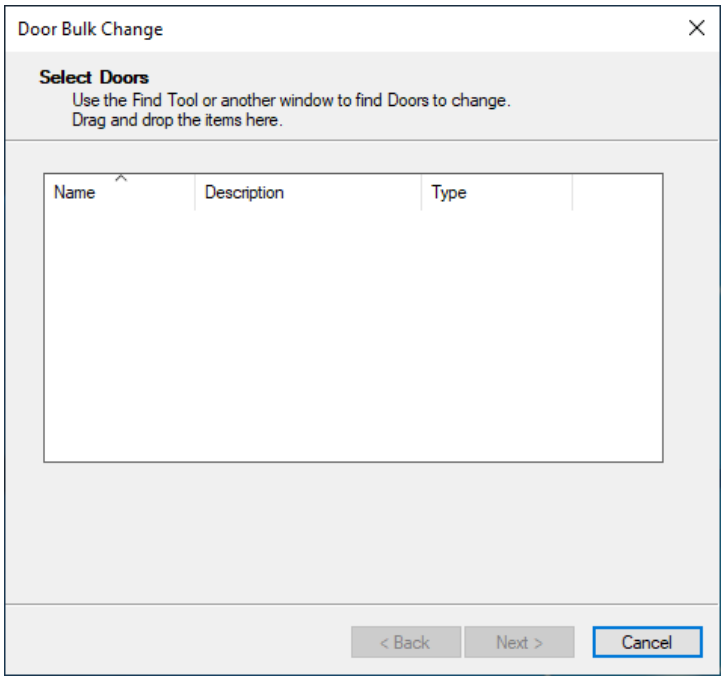
# Initiating a new Door Bulk Change

## Introduction

This procedure describes how to initiate a new Door Bulk Change in Command Centre. A Door Bulk Change can be performed to change the custom Terminal Display Messages used for access granted, access denied, and access denied for anti-tailgating/anti-passback at specific Doors.

## Procedure

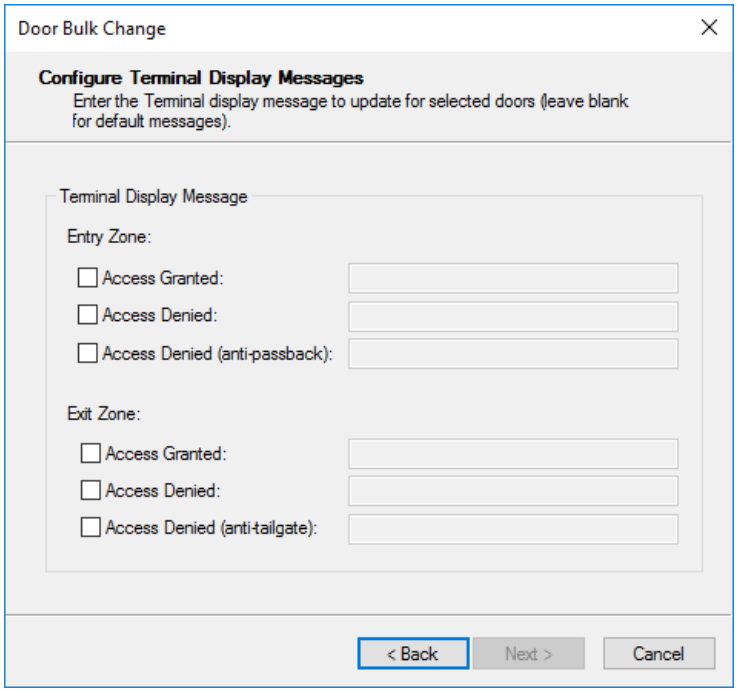
1. Click **Manage** from the menu bar, then **Bulk Changes**.
   The **Bulk Changes** Master List Window opens (in grid view).
2. **Right click** and select **New...Door Bulk Change**.
   The "Select Doors" screen of the Door Bulk Change Wizard display.



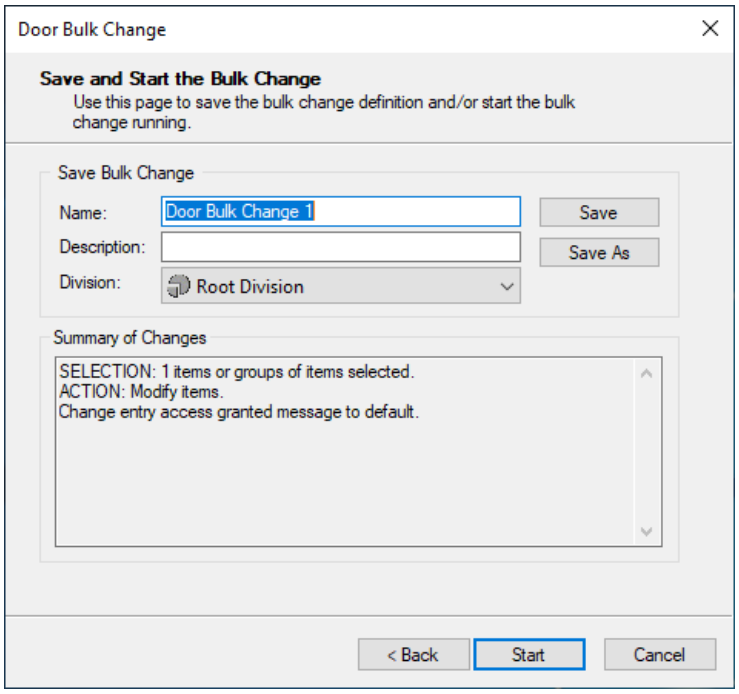

   Add all the Doors that require changing to this screen by dragging and dropping them from the Door window, or from the Find Tool.

   **Note:** You can use the Find Tool to locate all the Doors you want to change the Terminal display messages for, and then drag the search results onto this screen.

3. Click the **Next** button.
   The "Configure Terminal Display Messages" screen of the Door Bulk Change Wizard displays.



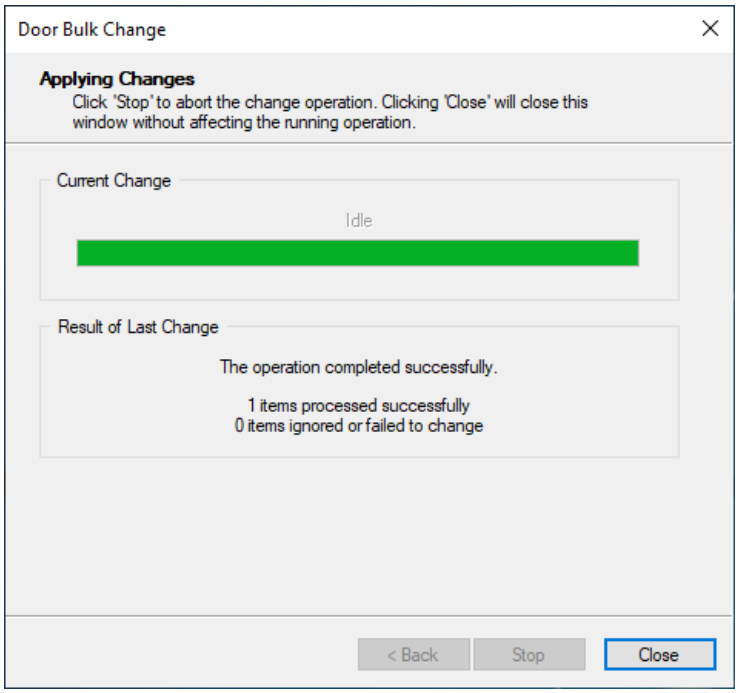

4. Set the Exit Zone and Entry Zone access messages for all Terminals used by the Doors you selected for this Bulk Change.
   **Note:** To reset an access message to the default message, select the check box and leave the text field empty.
5. Click the **Next** button.
   The "Save and Start the Bulk Change" screen of the Door Bulk Change Wizard displays.




6. Do you want to save this bulk change and it's settings before running?

| If... | then... |
|---|---|
| no | go to Step 8. |
| yes | type in a name and description.<br>**Note:** The **Name** field is limited to 60 characters and the Description field is limited to 200 characters. |

7. Click the **Save** button.
   This Bulk Change and its settings are saved, and it now displays in the **Bulk Changes** window.
   **Note:** The **Save As** button allows you to change an existing Bulk Change and re-save it as a new Bulk Change with a different name. If you open an existing saved Bulk Change and click the **Save As** button without changing the name, a message displays indicating that a Bulk Change with that name already exists.
8. Click the **Start** button.
   The "Applying Changes" screen of the Door Bulk Change Wizard displays.




This screen shows the progress of the bulk change.
If you didn't choose to save this Bulk Change, the bulk change will appear in the **Bulk Changes** window with a system-generated name while in progress. The in-progress Bulk Change will have an 'Active' status in the **Bulk Changes** window. If it completes successfully, it will briefly show as 'Successful', then the system will delete it.

**Note:** While a Door Bulk Change is active, or if it fails, it will remain in the **Bulk Changes** window until an operator deletes it.

## Result

A Door Bulk Change has been performed, and the selected Doors have had their Reader Display Messages changed.

# Chapter 39: Reports

Command Centre enables you to create and print a selection of reports, listed below, providing you have the correct operator privileges (see ***Operator Privileges*** on page 37-1 to check):

- Cardholder Report (Configuration Client)
- Activity Report (Configuration Client)
- Evacuation Report (Configuration Client)
- Access Group Report
- Access Report
- Exception Report
- Time and Attendance Report (Configuration Client)
- Site Configuration Report
- Contact ID Assignment Report
- Voltage Report
  **Note:** The Voltage Report will only be available on the drop-down list of report types (from the **Report Description** List Window) if your site is licensed for Fence Controllers. For further detail see ***Creating a Voltage Report (Configuration Client)*** (on page 49-40).
- Wiring Report
- Guard Tour Report
  **Note:** The Guard Tour Report will only be available on the drop-down list of report types (from the **Report Description** List Window) if your site is licensed for Guard Tours. For further detail see Creating a Guard Tour Report.
- Temperature Report
  **Note:** The Temperature Report will only be available on the drop-down list of report types (from the **Report Description** List Window) if your site is licensed for F22 Fence Controllers. For further detail see ***Creating a Temperature Report*** (on page 49-42).

When you create a new report a wizard displays for you to specify what particular information you want to include in the report and where the report should be printed.
**Note:** Reports which allow the selection of cardholders as criteria only support the selection of up to 10,000 cardholders.
The **Report Description** List Window is where you initiate managing your reports.

## Creating a new report

### Introduction

Creating a new report is simple using the Reports wizard. You step through the report building process using the **Next** button to access each wizard page, accepting default settings/values or making custom choices. At any stage you can backtrack via the **Back** button, or stop the report generation process by choosing the **Cancel** button (which also exits the wizard without offering to save changes).

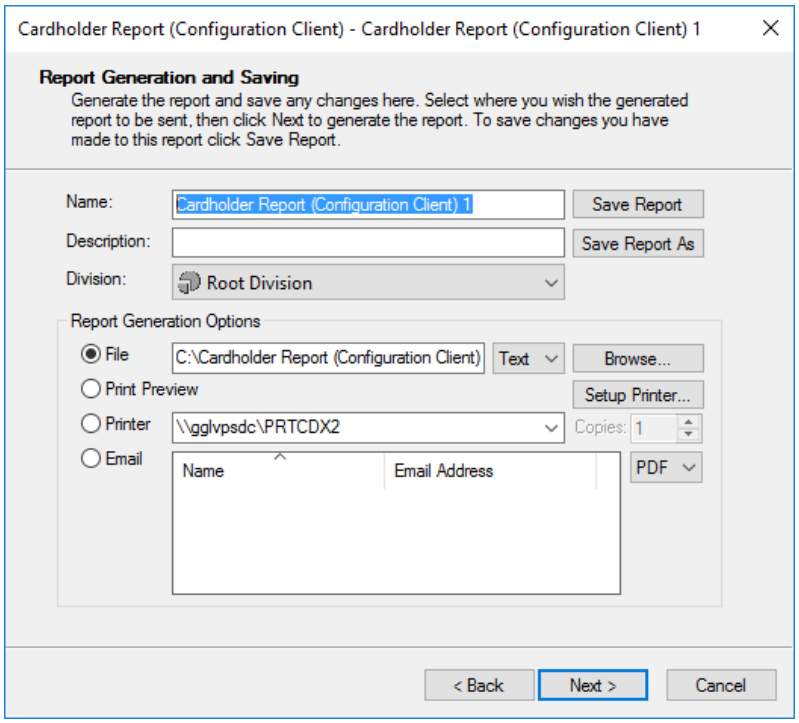
The information displayed to you when stepping through the Report wizard will vary depending on what report type you are creating.

You are given the option to save the report. This means it is available within the **Report Description** List Window to be used again and again.

### Procedure

1. Click **Report** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
   **Note:** All reports your site has set up are shown in this window.
2. **Right click** and select **New**.
3. From the displayed sub-menu, select which **type of report** you want to create.
4. The first screen of the appropriate report wizard displays.
   Click the **Next** and **Back** keys to step through the wizard.
5. Refer to the relevant topic for details relating to the particular **report type** you selected.
   **Note:** Those reports with "(Configuration Client)" after the name indicates there is an equivalent report in the Command Centre Client.
   ***Cardholder Report (Configuration Client)*** (on page 39-7)
   ***Activity Report (Configuration Client)*** (on page 39-15)
   ***Evacuation Report (Configuration Client)*** (on page 39-23)
   ***Access Group Report*** (on page 39-31)
   ***Access Report*** (on page 39-33)
   ***Exception Report*** (on page 39-35)
   ***Time and Attendance Report (Configuration Client)*** (on page 39-40) ***Site Configuration Report*** (on page 39-55)
   ***Contact ID Assignment Report*** (on page 39-58)
   ***Wiring Report*** (on page 39-61)

### *Report Generation and Saving*

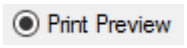



The final wizard page (for all report types) is titled "Report Generation and Saving".
**Note:** The 'Report Generation Options' section of this page differs slightly from that shown for some report types, as follows:

- *Access Reports* have a drop-down box for selecting a file type beside the **File** option.
- *Cardholder, Activity, Evacuation* and *Exception Reports* have a drop-down box for selecting for selecting a file type beside the **File** option, and they also have an additional **Email** output option.

6. Type the report **Name**.
7. Type the report **Description**. For example, you may mention the report is printed to the screen.
8. Select the **Division** from the drop-down list that you want to save this report in, (i.e. only operators with access to the Division you select will be able to see the report).
9. Click the radio button corresponding to where you want the report to be generated:

| Click the... | to... |
|---|---|
| File radio button | save the information **to file**, and type in the location and file name.<br>Alternatively, click the **Browse** button to select from the existing directory paths and |

| Click the... | to... |
|---|---|
| | type in the file name.<br>**Note:** When reports are saved to file, they get saved as **text** files, with the exception of:<br>• Access Reports, as there is the option to save these as either **Text** or **XML** file types. **XML** output allows you to analyse the data using a variety of tools, (e.g. Excel 2003).<br>• Cardholder, Activity, Evacuation and Exception Reports, as there is the option to save these as either **Text** or **PDF** file types. |
|  radio button | preview the information **on screen**. |
|  radio button | print the information to a selected **printer**, and select a printer from the drop-down list of available printers, or type in the printer name.<br>**Notes:**<br>• In the case of Auto-Evacuation Reports, if the operator does not have access to the printer on which the report is to print to, it will not appear in the list of available printers. Instead, the operator can type in the path to the printer, in which case the **Setup Printer** and **Next** buttons become disabled. Auto-Evacuation Reports are run via the server, therefore they cannot be tested from individual workstations.<br>• Via the **Setup Printer** button you can set information about the printer (for example; paper size and paper orientation).<br>The default paper orientation for reports is portrait. You can change the report orientation however, which can be useful for long names, (e.g. Cardholder names in the Evacuation Report).<br>See ***Customising Report Printouts*** (on page 39-75) if you wish to produce a report this way.<br>• By default, only one copy of the report |

| Click the... | to... |
|---|---|
| | will print to the printer, however you can set this to another amount if you require additional copies. |
| Email radio button<br>**Note:** This option is only available on the Cardholder, Activity, Evacuation and Exception Reports. | select Cardholders for the Report to be emailed to, by dragging and dropping them into the grid, and selecting the appropriate file type for the report, (i.e. either **Text** or **PDF**).<br>**Notes**:<br>• If a selected cardholder has more than one email address, the 'first' one displays, with the string ', …' (indicating they have more than one).<br>• If a selected cardholder has no email address, then a warning message displays when the **Next** button is clicked.<br>• Email addresses display here as 'Read-only'. |

10. To save this report and its settings, click the **Save Report** button Save Report.
    This report will now display within the **Reports Description** List Window, and the **Save Report** button becomes disabled and changes to **Report Saved**.
    **Note:** When an operator prints an existing report from the **Reports Description** List Window (i.e. a report that was saved), new data gets retrieved, as only the query was saved.
    The **Save Report As** button Save Report As allows multiple reports to be saved using the one wizard window.
    By opening an existing saved report and clicking the **Save Report As** button, the new report will display in the **Report Description** List Window, along with the original one.
    **Note:** If you open an existing saved report and click the **Save Report As** button without changing the report name a message displays indicating that the report already exists, and asks if you wish to replace it. By clicking **Yes** the original report is overwritten, and clicking **No** returns you to the "Report Generation and Saving" page, giving you the opportunity to change the file name for the report.
11. Click the **Next** button.
    A **Report Generation Progress** window displays. This provides feedback to the operator while data is retrieved from the server and formatted. An operator may choose to cancel the report by selecting the **Cancel** or **Back**

button. No other functionality is available on this page.

**Notes:**

- Larger reports take longer to generate.
- Two reports that access the same archive files can be run simultaneously. This can be done on two separate workstations, or on the same PC running two workstations.
- You may receive the following error message when restoring files: *"Connection to the specified path <pathname> has failed. Please check:*
  - *you have entered the path correctly*
  - *the Archiver User Account has the appropriate permissions to use this network resource."*

  If you do, you need to get the System Administrator who set up your archives to check that the User Account has sufficient privileges.

12. Click the **Finish** button.

**Result**

The report is generated and sent to the specified destination (printer, on screen or saved to file).

**Hint**

*Deleting existing Reports*
Refer to ***Deleting items*** (on page 3-27) for the procedure on how to delete an existing report.

*One -off Reports*
You may be required to create a "one-off" report and print it. Because the report is not required again, do **not** click the button "Save Report". The report will print but will not be saved.

# Cardholder Report

## Introduction

The Cardholder Report allows the operator to print a listing of Cardholder information. The operator specifies a report style, (i.e. detailed or summary), and a set of cardholders as criteria.

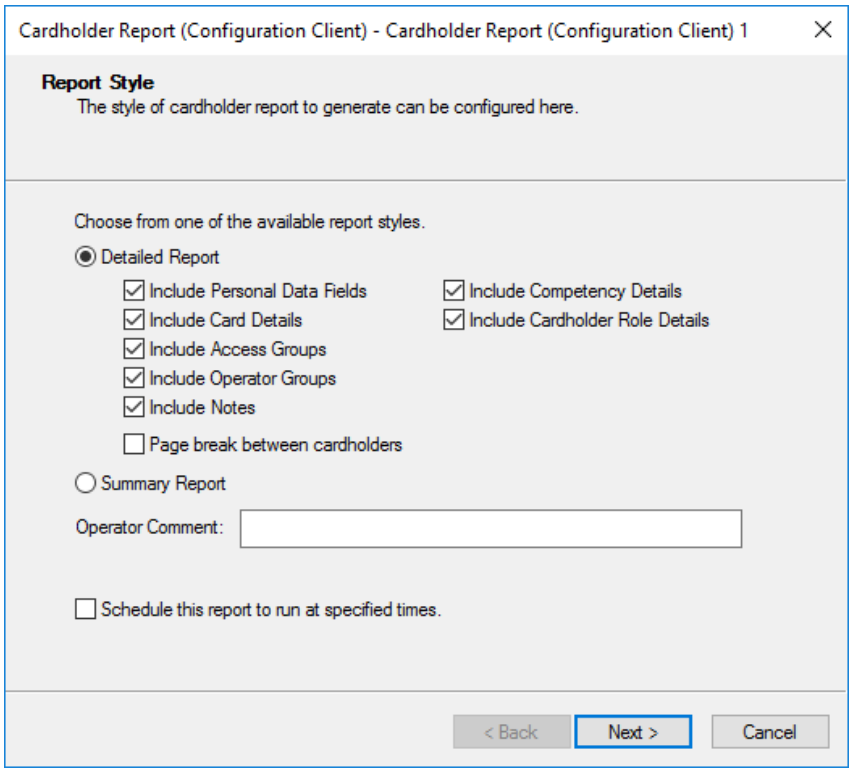
Operators must have the "View Cardholders" and the "Edit Report Descriptions" privileges to create, save, edit and delete Cardholder Reports.

This report can be scheduled to run automatically at regular times (via Action Plans or scheduled Macros). For further information refer to ***Automatically Generated Reports*** (on page 39-63) and ***Configuring Report Scheduling*** (on page 39-65).

## Report Wizard

The Cardholder Report wizard contains a number of pages which prompt you to enter certain information to create a report.
**Follow the instructions displayed**.

### *Report Style page*




This is the first page of the Cardholder Report wizard. It allows the operator to select either a **detailed** or **summary** version of the report.

**Detailed reports** include the Cardholder's name, the date they were created and last modified, the operator that last modified them and optionally one or more of the following information:

- Personal Data Fields
- Card Details (includes card status, i.e. whether cards are active or not)
- Access Groups
  **Note:** If you include Access Groups, for each Access Group that a cardholder belongs to, the report will show their temporary Access Group membership 'start' and 'end' dates/times. If they remain blank in the report, then the cardholder is a permanent member of the Access Group. Temporary membership records that have expired, but have not been deleted from the system, will also appear in the report.
- Operator Groups
- Notes, (i.e. entries recorded on the **Notes** tab of a Cardholder).
- Competency Details
  **Note:** If you want to include Cardholder Competency details in the report, see ***Reporting on Cardholder Competencies*** (on page 53-20) for further details.
- Cardholder Role Details
  **Note:** Selecting this option will list cardholders that fill each role defined for each cardholder selected in the report. It will not show the relationship from the parent cardholder's perspective, (i.e. it will not show all cardholders that a cardholder is "responsible for"). Only a **Summary** Report will show the "responsible for" directional relationship.

**Notes:**

- If your site is licensed for Biometric Integration there will also be an **Include Biometric Details** checkbox, that can be turned off/on as required.
- If your site if licensed for the Notifications feature there will also be an **Include Notification Details** checkbox, that can be turned off/on as required.
- **Detailed** Cardholder Reports can also be run from the Cardholder List Window.
  See ***Running a Cardholder Report from a Cardholder*** (on page 32-30) for further detail.

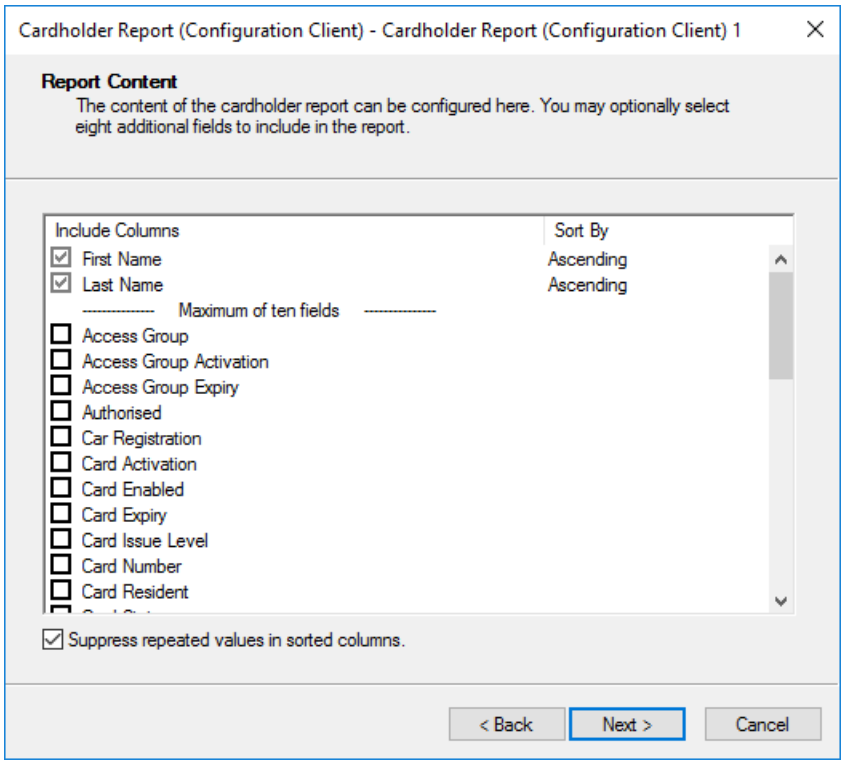
The detailed report may be configured to start each Cardholder on a new page. The report's sort order is fixed to the Cardholder's last and first names in ascending order.

**Summary Reports** provide no additional options on the first wizard page. Instead, configuration settings for the summary report are included on the next wizard page.

An **operator comment** may be entered for both report styles, which will be shown in the main header of the report. Comments are limited to a maximum of 200 characters.

You can optionally **Schedule this report to run at specified times** for both report styles.

### *Report Content page*




This page only displays if the Summary Report style is selected.
**Note:** If Detailed Report is selected, the wizard moves directly to the **Select Cardholders and Operators** page.

The summary report always includes the Cardholder's first and last names, but in addition to this, the operator may select up to eight additional Cardholder fields (by marking them with a tick), from the list provided.
**Notes:**

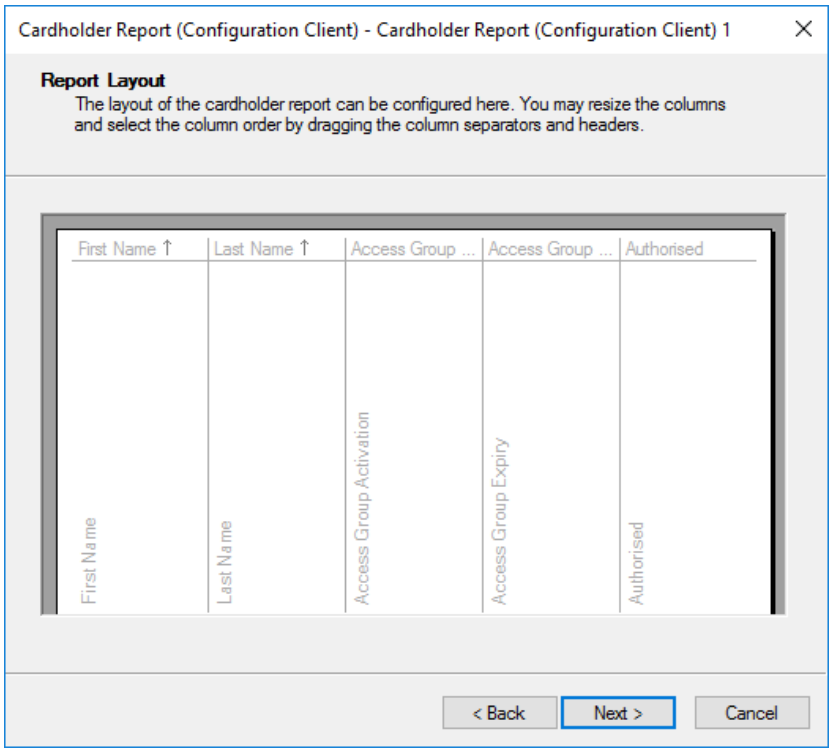
- Two options available in the list are "Access Group Activation" and "Access Group Expiry". By selecting these, your report will show a cardholder's temporary Access Group membership 'start' and 'end' dates/times. If these columns remain blank in the report, then the cardholder is a permanent member of the Access Group.
  Temporary membership records that have expired, but have not been deleted from the system, will also appear in the report.
- One of the options available in this list is "User Code". This is the only way that you can filter on who has a user code, but the actual codes will not be

disclosed in the report.

The order of the information in the summary report can be controlled through the setting of sort options against one or more of the shown fields. A field can be sorted in ascending or descending order, or may have no sort option applied.

Check the **Suppress repeated values in sorted columns** checkbox to control how the report will display repeated values in your summary cardholder report, (e.g. in a report that shows Access Group as the first column, it will display unique Access Groups as headers without repeating the Access Group name on each line).

### *Report Layout page*




This page allows the operator to configure the layout of the report.

You can determine the position of the columns horizontally across the page, as follows:

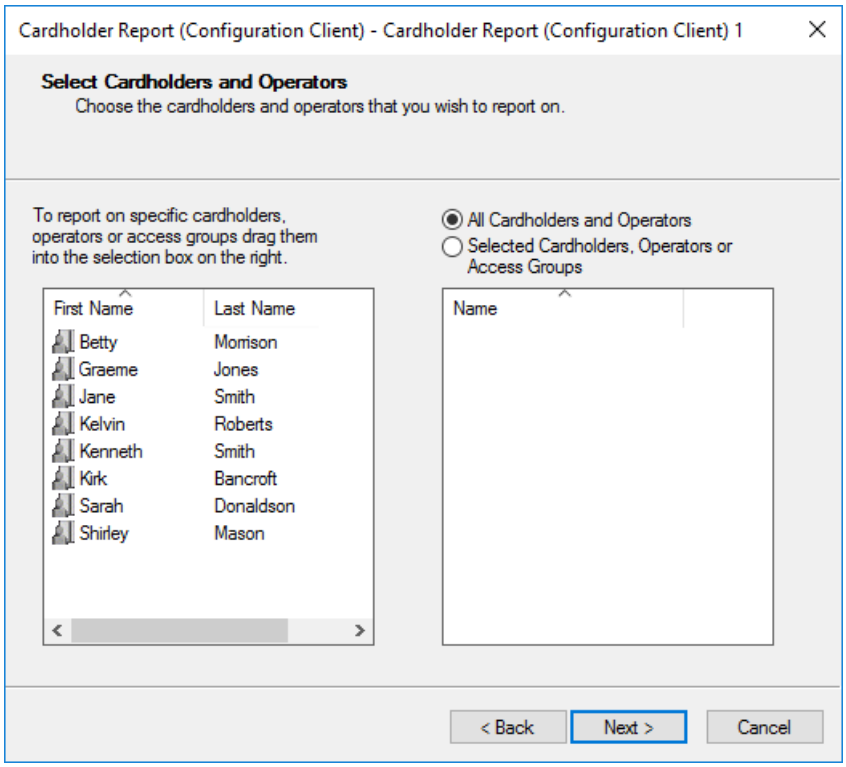
1. Move the mouse pointer to the column header you want to reposition. The mouse pointer changes to a hand symbol.
2. Click and hold down the mouse button. The hand changes indicating it is grabbing the header.
3. Move the hand (and hence the column header) to the desired new position.
4. Release the mouse button.

You can also resize the width of the columns, as follows:

1. Move the mouse pointer to a column separator.
2. When the mouse pointer changes to a double-ended arrow ↔, drag the column separator in the required direction to achieve the desired column width.

**Note:** If **Card**, **Access Group** or **Operator Group** details are included as the first column in the report, then the names of the Cardholders that are members of multiple groups, or have multiple cards, will appear more than once in the report. Alternatively, if the Cardholder's name is the first column, then a Cardholder's name will appear only once even if they have multiple **Cards**, **Access Groups** or **Operator Groups**.

### *Select Cardholders and Operators page*



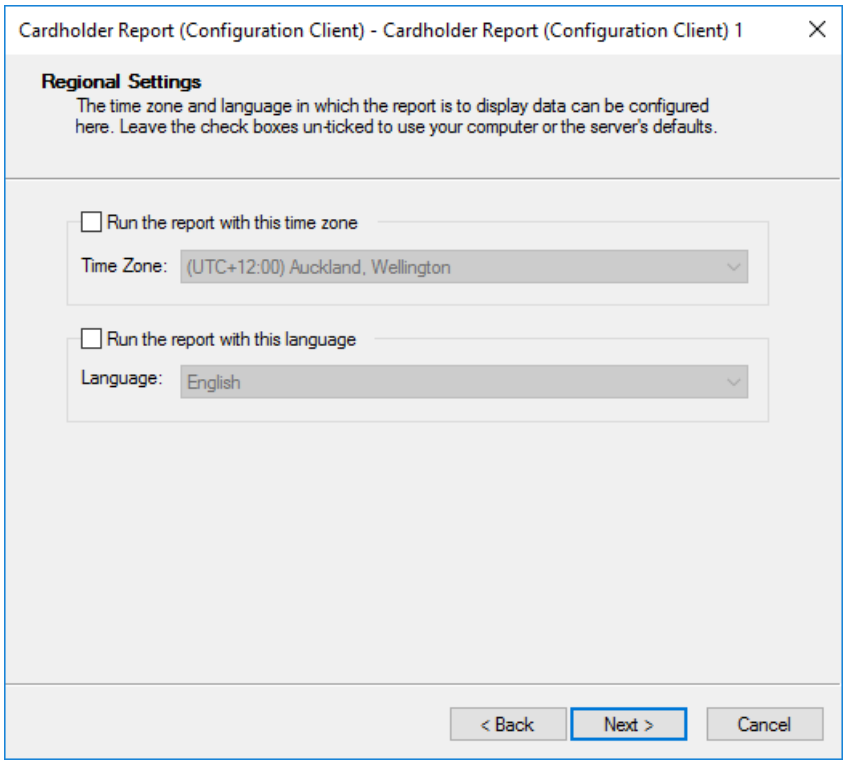

This page provides a list of Cardholders that an operator may include in the report. Cardholders shown here are restricted to those under the Division of the operator.

The Find Tool may be used to locate Cardholders, which can then be dragged and dropped onto this page. Alternatively, you can open the **Access Group** List Window and drag and drop those Access Groups you require onto this page.
**Note:** Only cardholders that are currently active within an Access Group will be reported on. Therefore, if you want the report to include 'expired' Access Group members, you need to select cardholders rather than Access Groups.

The "Automatic removal of expired members" from Access Groups will alter the information in the report depending on when the report is run.

Should you wish to delete a Cardholder or Access Group from your list on the right, **right click** on the item and click **Remove from List**.

### *Regional Settings page*

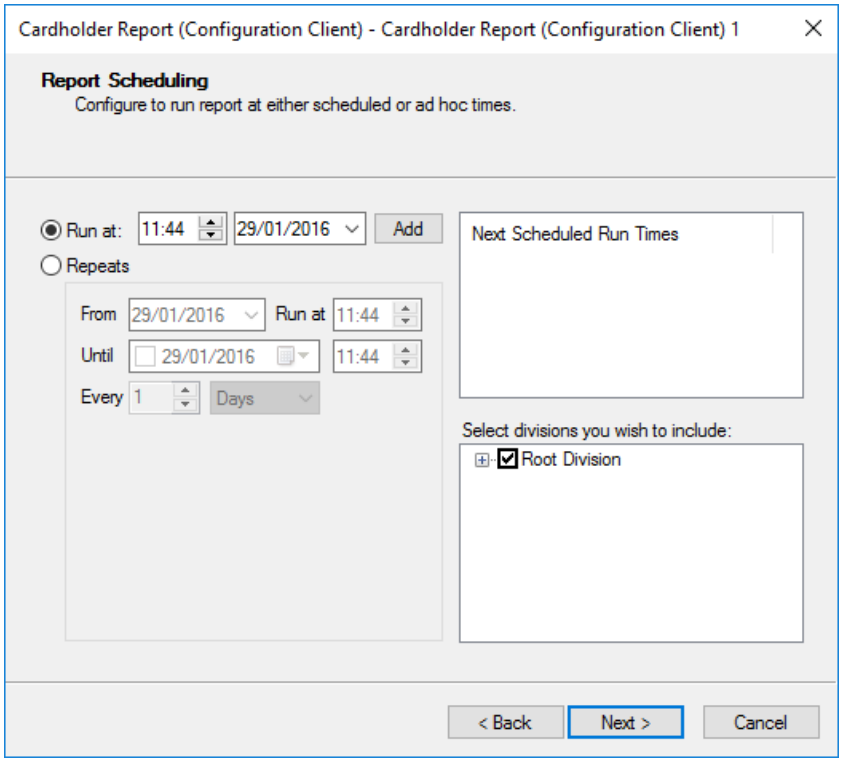



This page allows a time zone and/or language to be selected for the report. These options are specifically provided to support the Cardholder Report, (i.e. when the report is run via a macro on the server). Selection of a time zone is optional, as it is only required for Command Centre sites that span time zones. Selection of a language is also optional as it is only required for sites that have multiple languages.

If no time zone is selected, the report uses the time zone of the Command Centre server, only if the report was initiated from a macro which was triggered by an Action Plan, or a macro that was run from its schedule. In all other cases, the report uses the time zone on the workstation of the operator who has run the report, or the time zone on the workstation of the operator who ran the macro that triggered the report.

If a time zone is selected, when the report is run, all dates and times within the report will display in the selected time zone. Any dates and times configured within the report are assumed to be within the selected time zone (rather than the time zone on the configuring operator's workstation).

### *Report Scheduling page*




This page only displays if the "Schedule this report to run at specified times" checkbox is checked on the **Report Style** page. It allows run times and repetition properties to be defined for the report.
Multiple explicit times for the report to be run can be configured, as follows:

1. Click the **Run at** radio button.
2. Enter a date and time, and click the **Add** button.
   The date and time appears in the **Next Scheduled Run Times** grid.
3. Repeat Steps 1-2 for each explicit time you require.
   **Note:** If you click the **Repeats** radio button, then the explicit additions are removed from the **Next Scheduled Run Times** grid.

Repeat times for the report to be run can be configured, as follows:

1. Click the **Repeats** radio button.
2. Select the 'initial' **From** date and time.
3. Select an **Until** date and time if required.
   **Note:** If no **Until** date is entered, the report will repeat indefinitely.
4. Select the regularity for the report to be run, (i.e. **Every** one or many **Hours**, **Days**, **Weeks** or **Months**).
   **Note:** When **Weeks** is selected from the drop-down list, the days of the week display with an ability to select one or multiple days, (e.g. Monday and Thursday).
   The next five dates and times appear in the **Next Scheduled Run Times**

grid.

The **Division** selection grid allows the report to be scheduled for specific divisions.
**Note:** Only Divisions to which you have the appropriate editing privilege will appear in the drop-down list.

***Report Generation and Saving page***

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

# Activity Report

## Introduction

The Activity Report is a tool for reporting exactly what has been occurring in the system. It is a query tool and is not expected to be used to print regular reports for filing purposes.

This report can be scheduled to run automatically at regular times (via Action Plans or scheduled Macros). For further information refer to ***Automatically Generated Reports*** (on page 39-63) and ***Configuring Report Scheduling*** (on page 39-65).

**Note:** In a multi-server environment, for any given server where event aggregation is enabled, an operator can run an Activity Report which incorporates events from remote site items. The Activity Report can be filtered by remote site items.

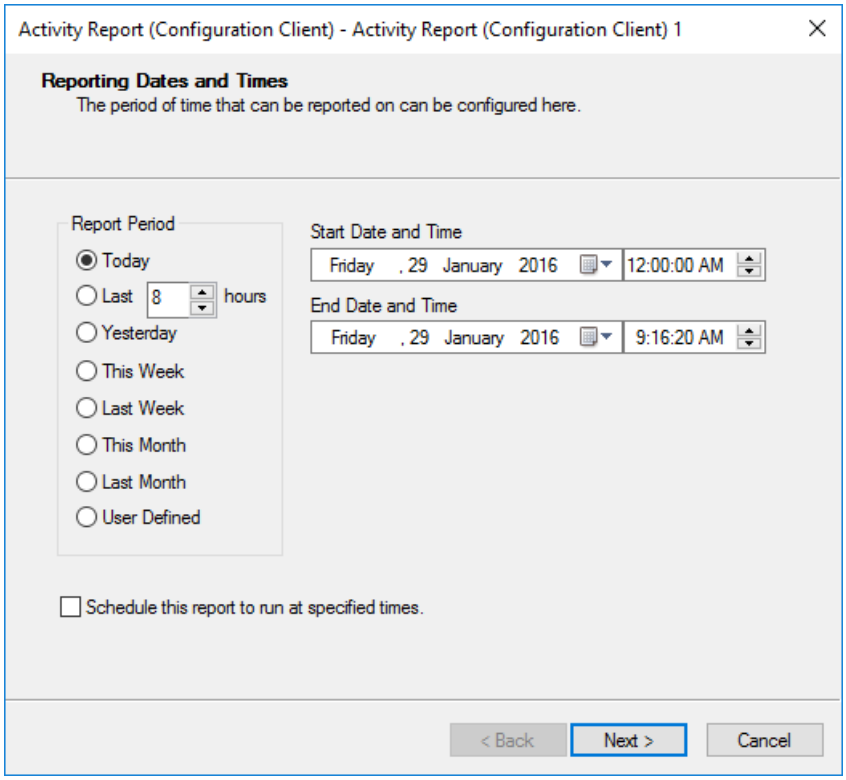
## Operator Privileges

| Privilege(s) | is required to... |
|---|---|
| "Edit Report Description" and either "View Events and Alarms" or "Edit Alarms" | create, view, edit, print, save and delete Activity Reports. |
| "View Events and Alarms" or "Edit Alarms" | create, view, edit, and print Activity Reports. |

## Report Wizard

The Activity Report wizard contains a number of pages which prompt you to enter certain information to create a report.
**Follow the instructions displayed**.

### *Reporting Dates and Times page*



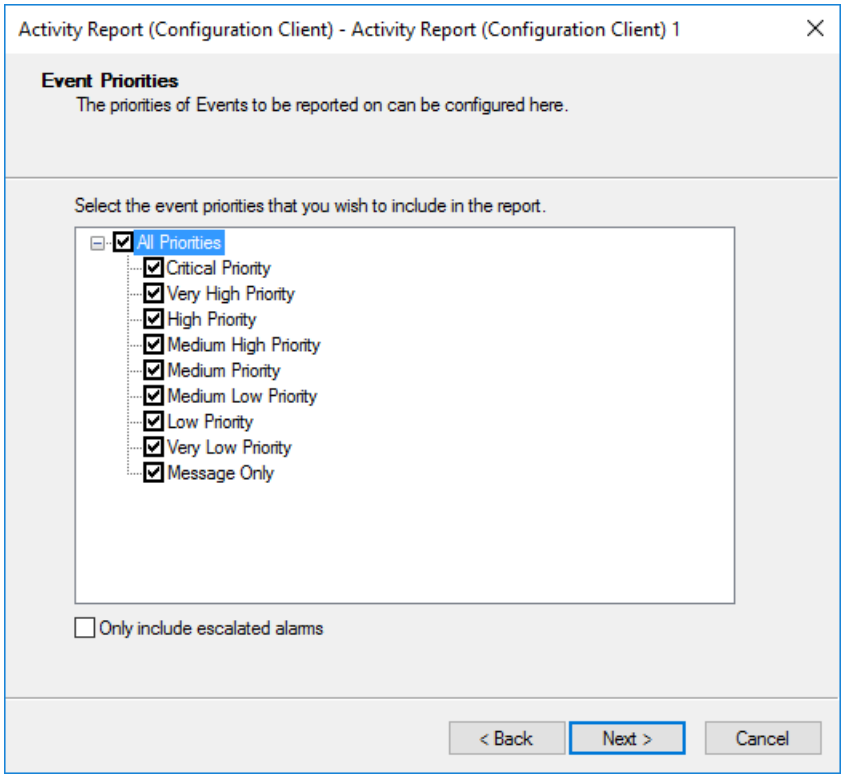

This is the first page of the Activity Report wizard. This page allows an operator to enter a start and end time for the report. Pre-defined periods are provided for simplicity, or custom start and end times can be entered.

The default option is set as **Today**, with the start and end Date/Time set to midnight to the current time.

The default value for **Last [n] hours** is set as "8" hours (valid range is 1 - 999), with the idea that at a shift change an operator may want to run a report based on however many hours the last shift was. A standard shift would normally be 8 hours, hence the 8 hour default setting.

You can optionally **Schedule this report to run at specified times**.

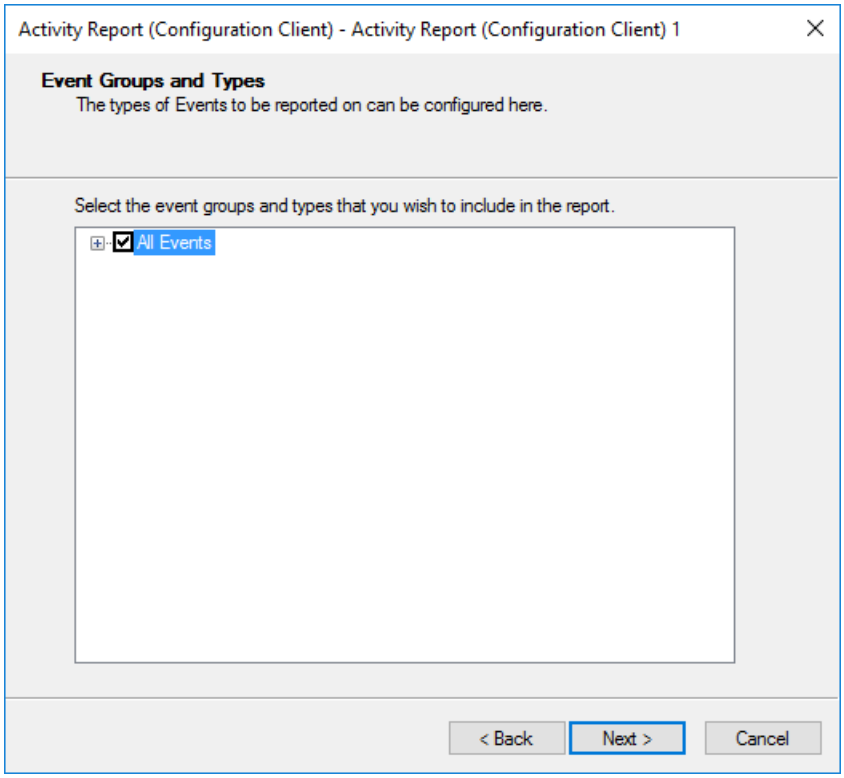
### *Event Priorities page*




This page provides a tree representation of all the event priorities, and allows the different priorities to be selected for inclusion in the report. Priority selection is indicated by a "tick" box and is made be clicking in the checkbox next to the name.
**Note:** The priority names are user-defined (via the **Event Priorities** tab of the Server Properties).

Check the **Only include escalated alarm** checkbox if you wish to run a report that will just have escalated alarms in it. An Activity Report with only escalated alarms will include the full alarm details for each escalated alarm.

### *Event Groups and Types page*

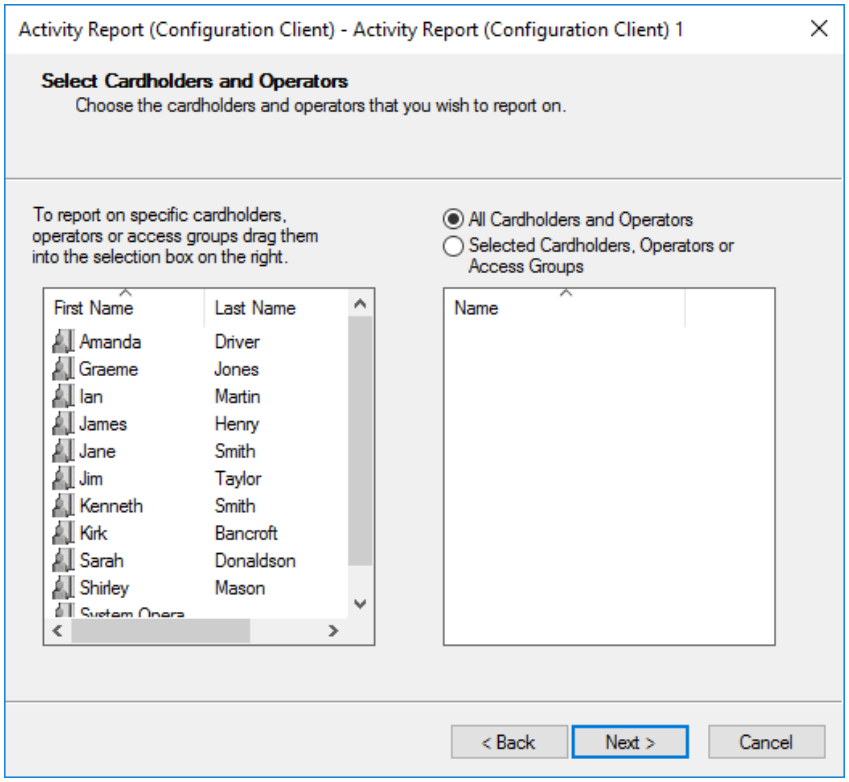



This page provides a tree view representation of the Event Categories and types. Event type selection is indicated by a "tick" box and is made by clicking in the checkbox next to the event name. Clicking the icon expands or contracts that branch of the tree.

Selecting an event category also selects all it's sub-events. De-selecting an event category also de-selects all it's sub-events.

**Note:** An online help file listing all the event/alarm messages can be accessed via the **Help** menu bar in Command Centre, and provides explanations of what each message means.

### *Select Cardholders and Operators page*



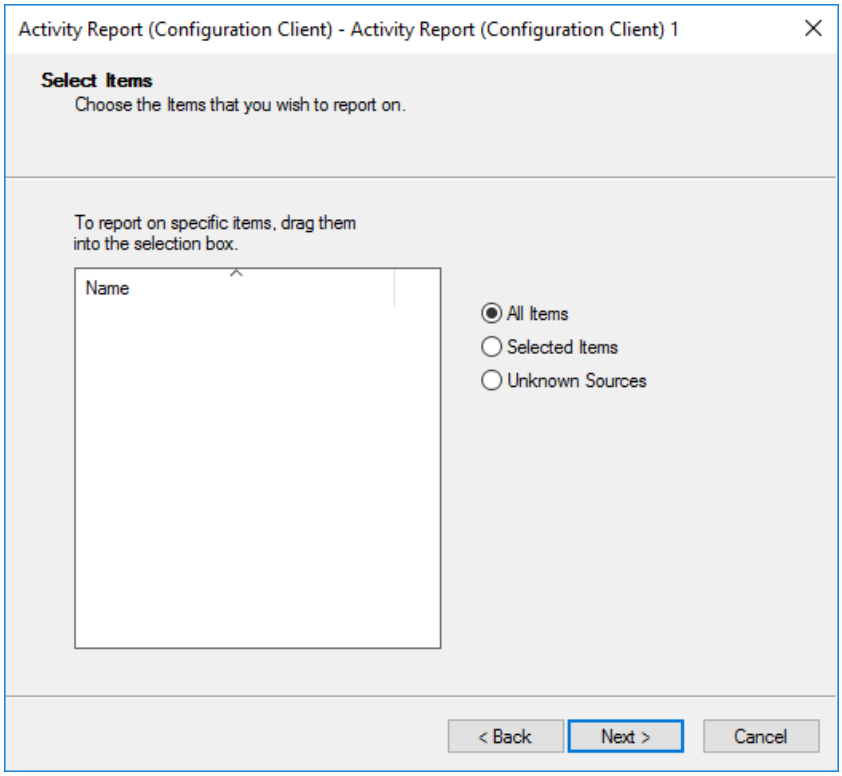

This page provides a list of Cardholders that an operator may include in the report. Cardholders shown here are restricted to those under the Division of the operator.

The Find Tool may be used to locate Cardholders, which can then be dragged and dropped onto this page. Alternatively, you can open the **Access Group** List Window and drag and drop those Access Groups you require onto this page.

**Note:**
Only cardholders that are currently active within an Access Group will be reported on. Therefore, if you want the report to include 'expired' Access Group members, you need to select cardholders rather than Access Groups. The "Automatic removal of expired members" from Access Groups will alter the information in the report depending on when the report is run.

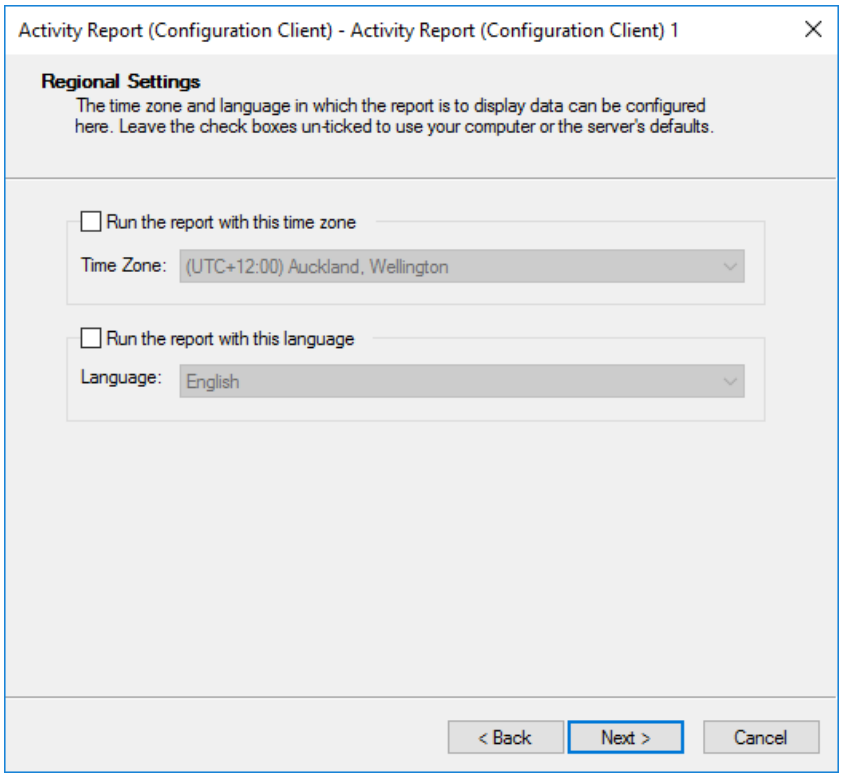
Should you wish to delete a Cardholder or Access Group from your list on the right, **right click** on the item and click **Remove from List**.

### *Select Items page*




This page allows the operator to select the items they wish to report on, (i.e. all items or selected items by dragging and dropping them).

### *Regional Settings page*

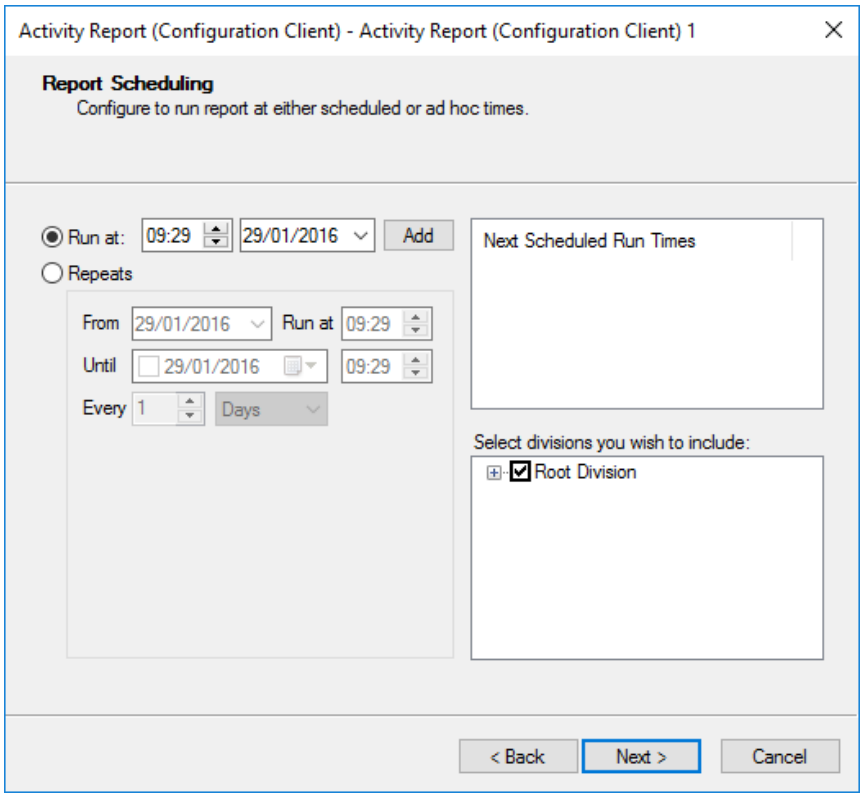


This page allows a time zone and/or language to be selected for the report. Selection of a time zone is optional, as it is only required for Command Centre sites that span time zones. Selection of a language is also optional as it is only required for sites that have multiple languages.

If no time zone is selected, the report uses the time zone of the Command Centre server, only if the report was initiated from a macro which was triggered by an Action Plan, or a macro that was run from its schedule. In all other cases, the report uses the time zone on the workstation of the operator who has run the report, or the time zone on the workstation of the operator who ran the macro that triggered the report.

If a time zone is selected, when the report is run, all dates and times within the report will display in the selected time zone. Any dates and times configured within the report are assumed to be within the selected time zone (rather than the time zone on the configuring operator's workstation).

### *Report Scheduling page*




This page only displays if the "Schedule this report to run at specified times" checkbox is checked on the **Reporting Dates and Times** page. It allows run times and repetition properties to be defined for the report.
Multiple explicit times for the report to be run can be configured, as follows:

1. Click the **Run at** radio button.
2. Enter a date and time, and click the **Add** button.

The date and time appears in the **Next Scheduled Run Times** grid.

3. Repeat Steps 1-2 for each explicit time you require.
   **Note:** If you click the **Repeats** radio button, then the explicit additions are removed from the **Next Scheduled Run Times** grid.

Repeat times for the report to be run can be configured, as follows:

1. Click the **Repeats** radio button.
2. Select the 'initial' **From** date and time.
3. Select an **Until** date and time if required.
   **Note:** If no **Until** date is entered, the report will repeat indefinitely.
4. Select the regularity for the report to be run, (i.e. **Every** one or many **Hours**, **Days**, **Weeks** or **Months**).
   **Note:** When **Weeks** is selected from the drop-down list, the days of the week display with an ability to select one or multiple days, (e.g. Monday and Thursday).
   The next five dates and times appear in the **Next Scheduled Run Times** grid.

The **Division** selection grid allows the report to be scheduled for specific divisions.
**Note:** Only Divisions to which you have the appropriate editing privilege will appear in the drop-down list.

### *Report Generation and Saving page*

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

## Evacuation Report

### Introduction

The Evacuation Report provides a list of cardholders present on a site. This can be used in an evacuation situation, such as a fire, and allows better management of evacuation situations and improved cardholder safety.
**Note:** In a multi-server system that uses Visitor Management (a licensable feature), visit data does not get replicated between servers. Therefore, the Evacuation Report cannot report on remote visitors.

Evacuation Reports can be set up to generate automatically via an Action Plan or a scheduled macro. These are referred to as 'Auto-Evacuation' Reports, and are triggered by an event or alarm. For further detail see ***Automatically Generated Reports*** (on page 39-63) and ***Configuring Report Scheduling*** (on page 39-65).

### Prerequisite

The Evacuation Report relies on cardholder location information, and is therefore only effective at sites where **all** cardholders swipe their cards **every** time they enter or exit an Access Zone.

### Operator Privileges

To create a new Evacuation Report, or to delete or edit the properties of an Evacuation Report an operator must have the "Edit Evacuation Report" operator privilege in the Evacuation Report's Division.

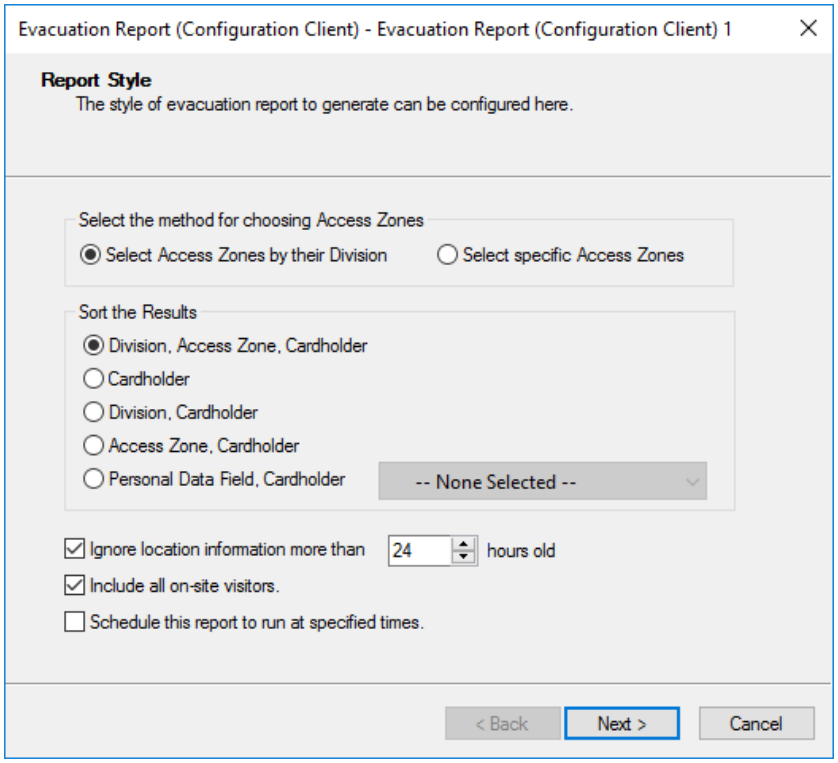
To view the properties of and/or run an existing saved Evacuation Report, an operator must have the "View Events and Alarms" operator privilege in the Evacuation Report's Division. An operator will still be able to see all the properties, (i.e. items like PDFs, Access Zones, etc.) even if the report contains items that the operator has no privileges for.

Having different privileges for creating and running Evacuation Reports ensures that operators who are able to run and print pre-configured Evacuation Reports (when there is an emergency), are prevented from changing their configuration.

### Report Wizard

The Evacuation Report wizard contains a number of pages which prompt you to enter certain information to create the report.
**Follow the instructions displayed.**

### *Report Style page*




On this page you are prompted for the following:

- Decide on the method for choosing Access Zones to include:
  - **Select Access Zones by their Division** - This option provides a quick and easy method if you know the parts of the site you want to include.
  - **Select specific Access Zones** - This option allows for finer definition than the Division the zone belongs to, by selecting specific Access Zones.

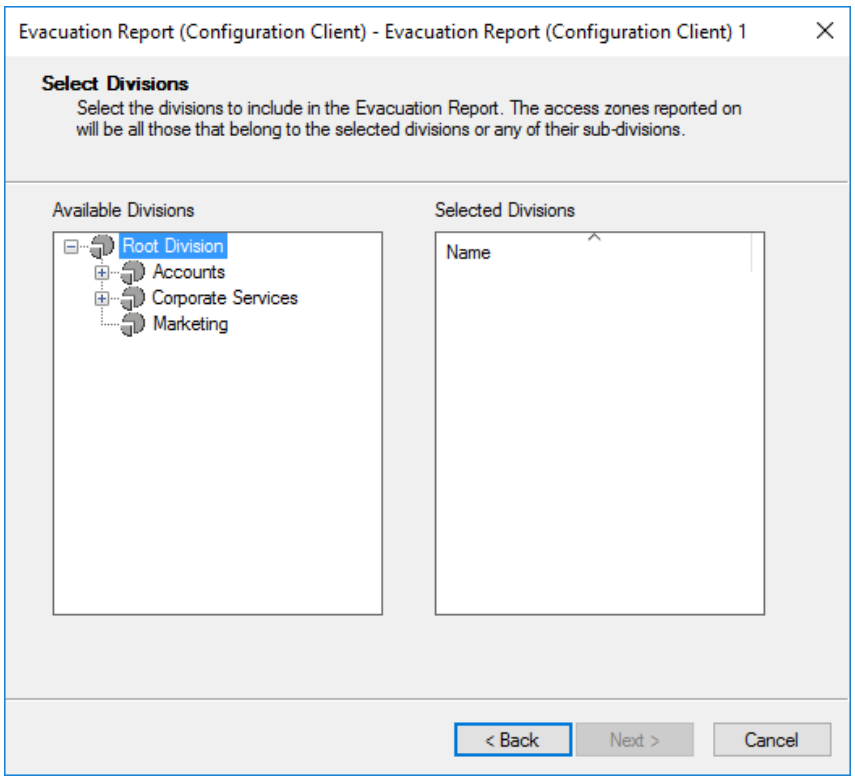
The option you select will determine which wizard page displays next, (i.e. either the "Select Divisions" page or the "Select Access Zones" page).

- Decide how to sort the information. Either by:
  - Division, Access Zone and Cardholder (records will be grouped by Access Zone)
  - Cardholder name
  - Division and Cardholder (records will be grouped by Division)
  - Access Zone and Cardholder (records will be grouped by Access Zone)
  - Personal Data Field and Cardholder
    **Note:** The drop-down list box next to **Personal Data Field** is only enabled if the **Personal Data Field** radio button is selected.
    You can elect whether to include a Personal Data Field in the report (because cardholder names are not always unique, you may wish to include a unique PDF to distinguish between those cardholders with

the same name, e.g. 'Date of Birth' PDF)
Operators can only select PDFs available to them.

- You can optionally set the report to ignore location information older than a certain age.
  (Default = set to ignore location information more than 24 hours old. Maximum allowed is up to 999 hours.)
- You can optionally **Schedule this report to run at specified times**.
- If your site is licensed for the Visitor Management feature, there is also an option to "Include all on-site visitors" (checked by default).
  If selected, a new section is added to the end of the report listing all On-Site, Due to Leave and Overdue Visitors and Tour Groups.
  **Note:** All visitors are included in the report, regardless of the Divisions or Access Zones selected, and Tour Groups will indicate the number of visitors and a contact name for the Tour.

***Select Divisions page***

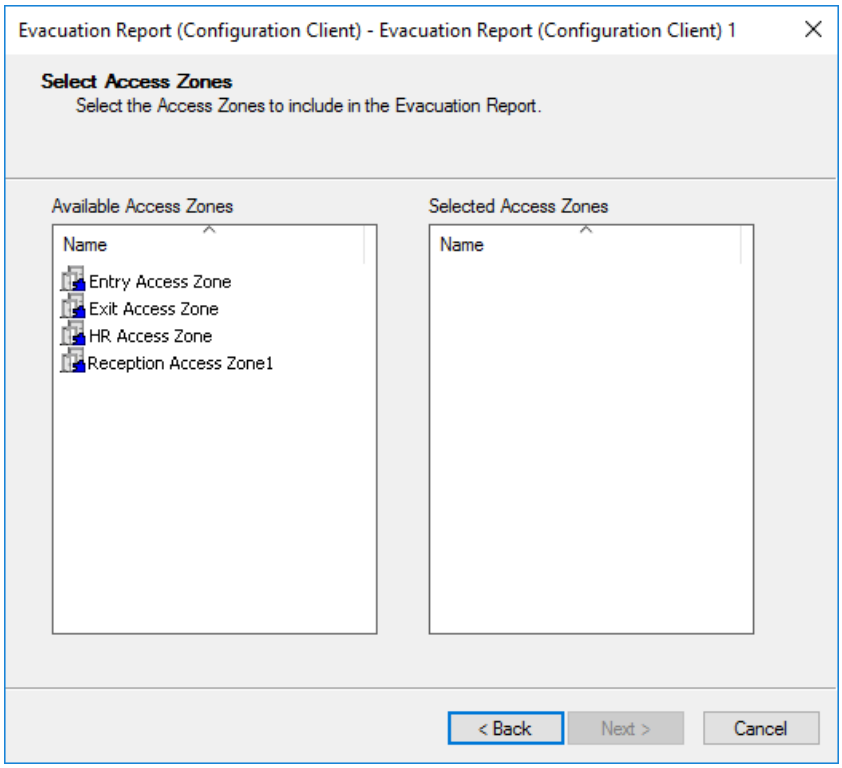



This page only displays if the "Select Access Zones by their Division" option is selected.
The grid on the left displays the current operator's "Available Divisions". The available Divisions are all Divisions in which the operator has "View Site" or "Edit Site" privilege.

Drag and drop the Division(s) you want included in the Evacuation Report from the list of available Divisions (the grid on the left), to the grid on the right.

If you have opened an existing saved Evacuation Report the Divisions that were originally selected for inclusion in the report display in the grid on the right. These display regardless of the current operator's privileges in these Divisions. An operator can remove a "Selected Division" from the list if they have "View Site" or "Edit Site" privilege in that Division.

### *Select Access Zones page*

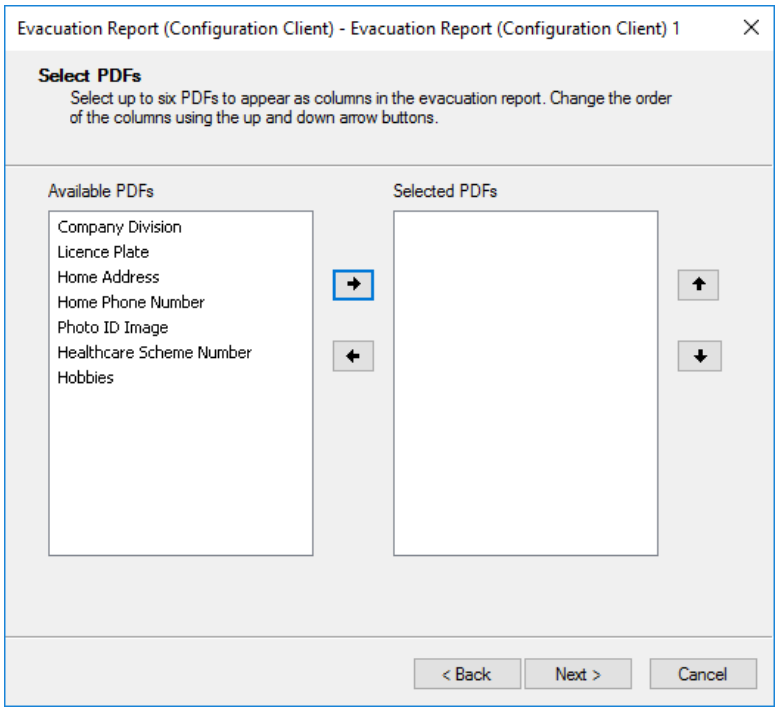



This page only displays if the "Select specific Access Zones" option is selected. The grid on the left displays the current operator's "Available Access Zones". The available Access Zones are all Access Zones in which the operator has "View Site" privilege.

Drag and drop the Access Zone(s) you want included in the Evacuation Report from the list of available Access Zones (the grid on the left), to the grid on the right.

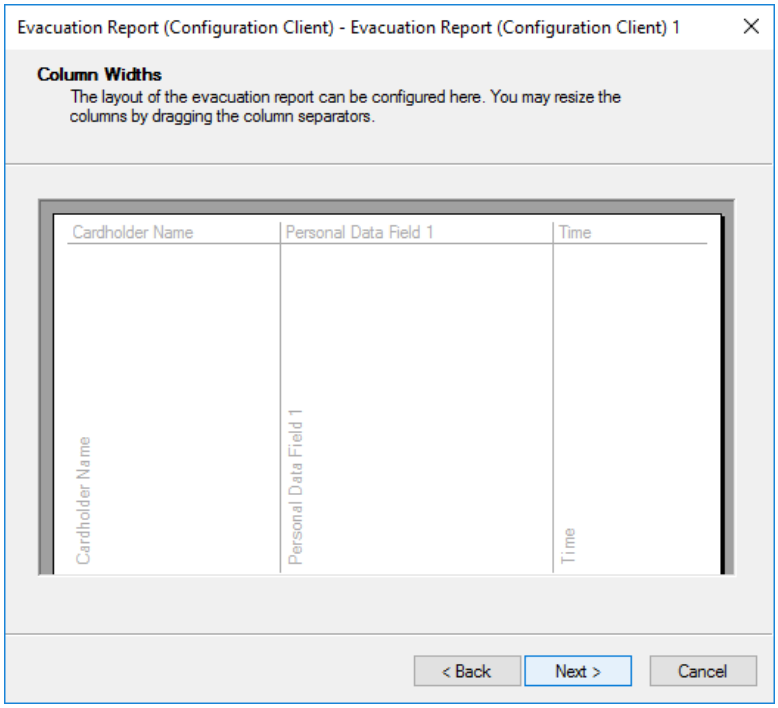
If you have opened an existing saved Evacuation Report the Access Zones that were originally selected for inclusion in the report display in the grid on the right. These display regardless of the current operator's privileges. An operator can remove a "Selected Access Zone" from the list if they have "View Site" privilege in the Access Zone's Division.

### *Select PDFs page*




This page allows you to optionally include up to six Personal Data Fields in the report output. Using the arrow buttons, place the Personal Data Fields that you require from the **Available PDF's** grid to the **Selected PDF's** grid.
Once you have the Personal Data Fields you require in the **Selected PDF's** grid on the right, the up and down arrows to the side can be used to change the order of them, (i.e. Select the PDF you want to move and click either the up or down arrow to move it).

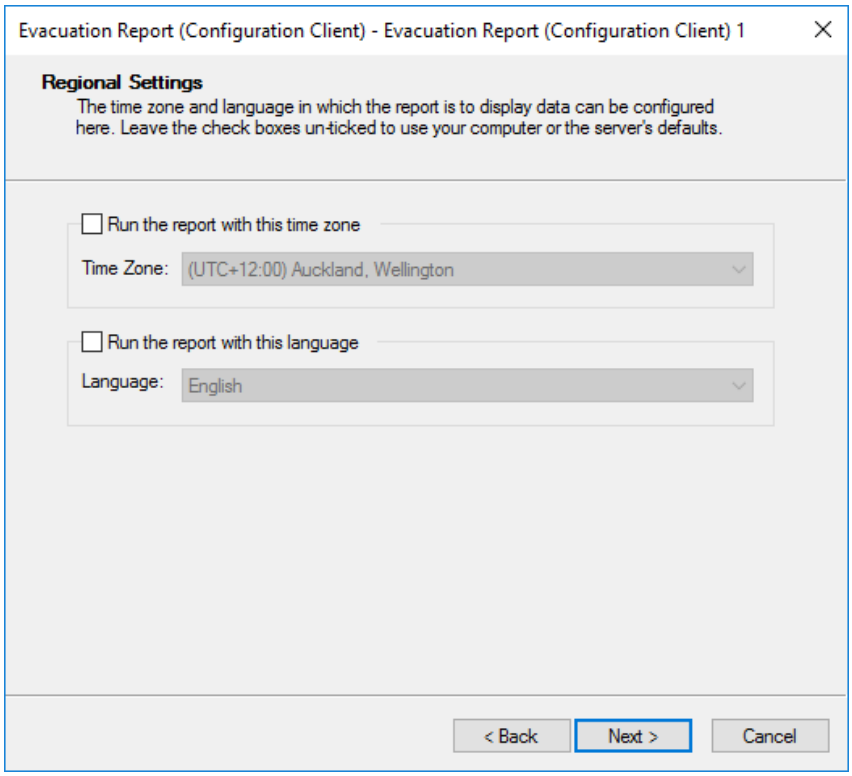
### *Column Widths page*



This page allows the operator to configure the layout of the report. You can resize the width of the columns, as follows:

1. Move the mouse pointer to a column separator.
2. When the mouse pointer changes to a double-ended arrow ↔, drag the column separator in the required direction to achieve the desired column width.

### *Regional Settings page*

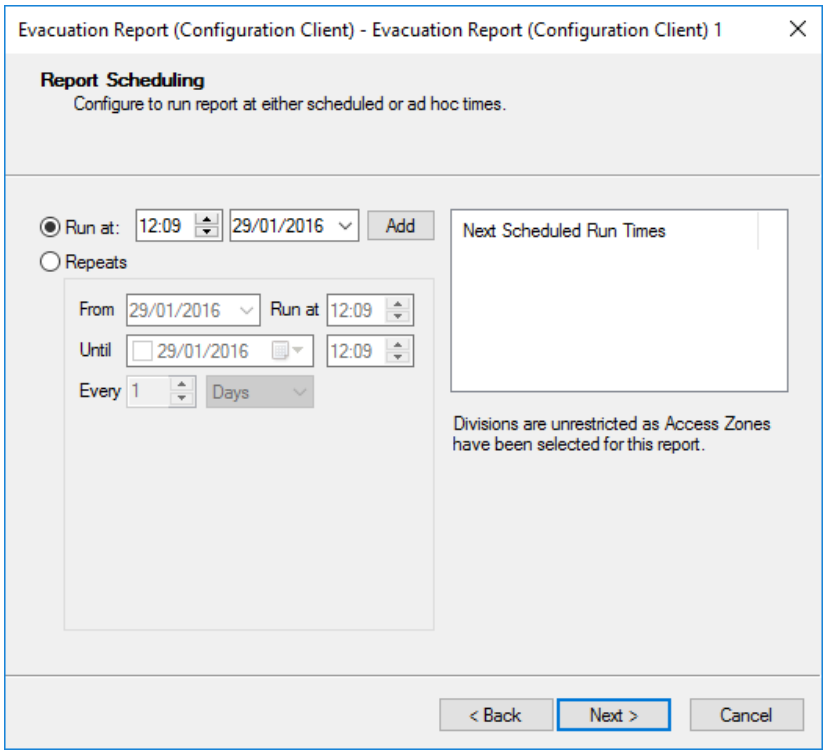



This page allows a time zone and/or language to be selected for the report. These options are specifically provided to support the Auto-Evacuation Report, (i.e. when the report is run via a macro on the server). Selection of a time zone is optional, as it is only required for Command Centre sites that span time zones. Selection of a language is also optional as it is only required for sites that have multiple languages.

If no time zone is selected, the report uses the time zone of the Command Centre server, only if the report was initiated from a macro which was triggered by an Action Plan, or a macro that was run from its schedule. In all other cases, the report uses the time zone on the workstation of the operator who has run the report, or the time zone on the workstation of the operator who ran the macro that triggered the report.

If a time zone is selected, when the report is run, all dates and times within the report will display in the selected time zone. Any dates and times configured within the report are assumed to be within the selected time zone (rather than the time zone on the configuring operator's workstation).

### *Report Scheduling page*




This page only displays if the "Schedule this report to run at specified times" checkbox is checked on the **Report Style** page. It allows run times and repetition properties to be defined for the report.
Multiple explicit times for the report to be run can be configured, as follows:

1. Click the **Run at** radio button.
2. Enter a date and time, and click the **Add** button.
   The date and time appears in the **Next Scheduled Run Times** grid.
3. Repeat Steps 1-2 for each explicit time you require.
   **Note:** If you click the **Repeats** radio button, then the explicit additions are removed from the **Next Scheduled Run Times** grid.

Repeat times for the report to be run can be configured, as follows:

1. Click the **Repeats** radio button.
2. Select the 'initial' **From** date and time.
3. Select an **Until** date and time if required.
   **Note:** If no **Until** date is entered, the report will repeat indefinitely.
4. Select the regularity for the report to be run, (i.e. **Every** one or many **Hours**, **Days**, **Weeks** or **Months**).
   **Note:** When **Weeks** is selected from the drop-down list, the days of the week display with an ability to select one or multiple days, (e.g. Monday and Thursday).
   The next five dates and times appear in the **Next Scheduled Run Times** grid.

***Report Generation and Saving page***

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

**Recommendation:**
It is strongly recommended that sites perform trial runs of the Evacuation Report to ensure the reports are:
- configured correctly
- will be printed on the correct printer from all workstations.

**Disclaimer:**
The following disclaimer appears in the report:
*"The information presented in this report is dependent on system and report configuration. Gallagher does not accept responsibility for sites relying on this Evacuation Report."*

## Quick Method of Printing

In an emergency situation, operators with the 'View Events and Alarms' operator privilege can print a pre-configured Evacuation Report quickly and easily. Use the following procedure in this situation:

1. Click **Report** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
2. Highlight the required report.
3. **Right click** and select **Print**.
   The **Report Generation and Saving** page of the report wizard opens.
4. Click the **Printer** radio button (if not already selected) and click the **Next** button.
   The Evacuation Report prints to the printer pre-configured in the report. If this printer is not available to the operator generating the report, then the printers that are available to the operator are listed, and the operator is prompted to select one.

# Access Group Report

## Introduction

The Access Group Report provides a unified list of access groups with their membership, access and properties.
The Access Group Report compliments the Cardholder Reports. Cardholder Reports include information about Cardholders including Personal Data Field (PDF) information, cards, the Access Groups the Cardholder belongs to, etc.
The Access Group Report provides information specifically about Access Groups, including:

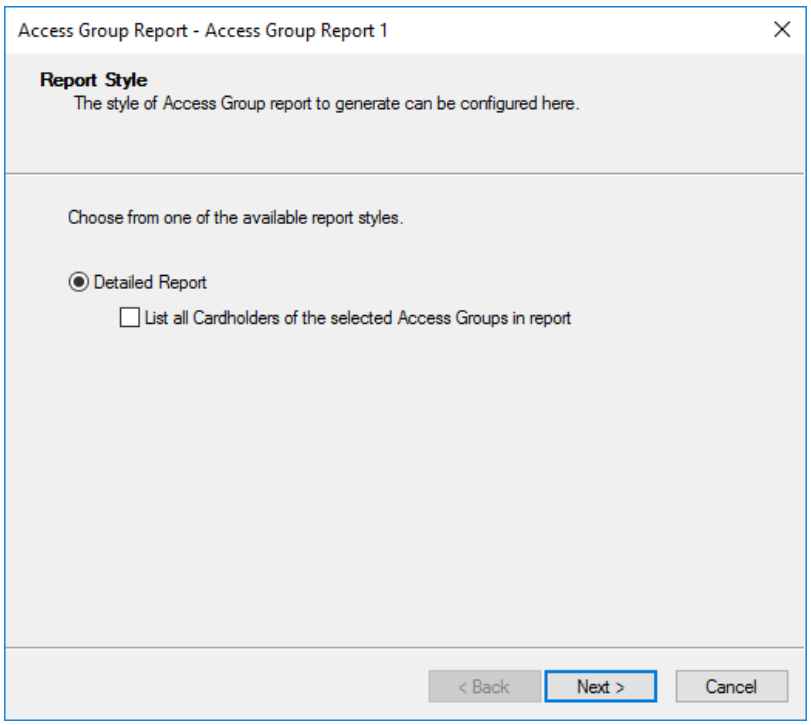
- Privileges assigned to an Access Group
- Access provisions
- The list of PDF fields assigned to an Access Group
- A list of Cardholders who are members of the Access Group

Operators must have the "View Access Groups" and "Edit Report Descriptions" privileges to create, save, edit and delete Access Group Reports.

## Report Wizard

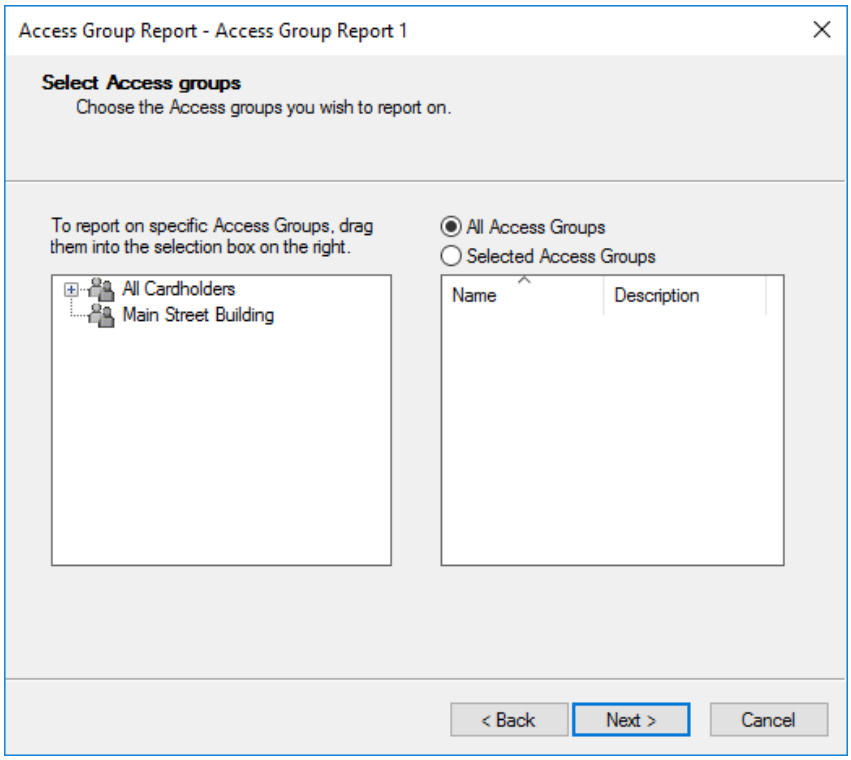
The Access Group Report wizard contains a number of pages which prompt you to enter certain information to create a report.
**Follow the instructions displayed**.

### *Report Style page*



This is the first page of the Access Group Report wizard. The operator has the option here to include all Cardholders of the selected Access Group in the report. If this is chosen, there will be a membership section in the report for each of the Access Groups chosen. This section will show cardholders temporary Access Group membership 'start' and 'end' dates/times. Cardholders with no 'start' and 'end' dates/times are permanent members of an Access Group. Temporary membership records that have expired but have not been deleted from the system, will also appear in the report.

### *Select Access groups page*




This page allows the operator to include all Access Groups or selected Access Groups, (i.e. by dragging and dropping them), in the report.

**Note:**

Only cardholders that are currently active within an Access Group will be reported on. The "Automatic removal of expired members" from Access Groups will alter the information in the report depending on when the report is run.

Should you wish to delete an Access Group from your list on the right, **right click** on the Access Group and click **Remove from List**.

### *Report Generation and Saving page*

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

# Access Report

## Introduction

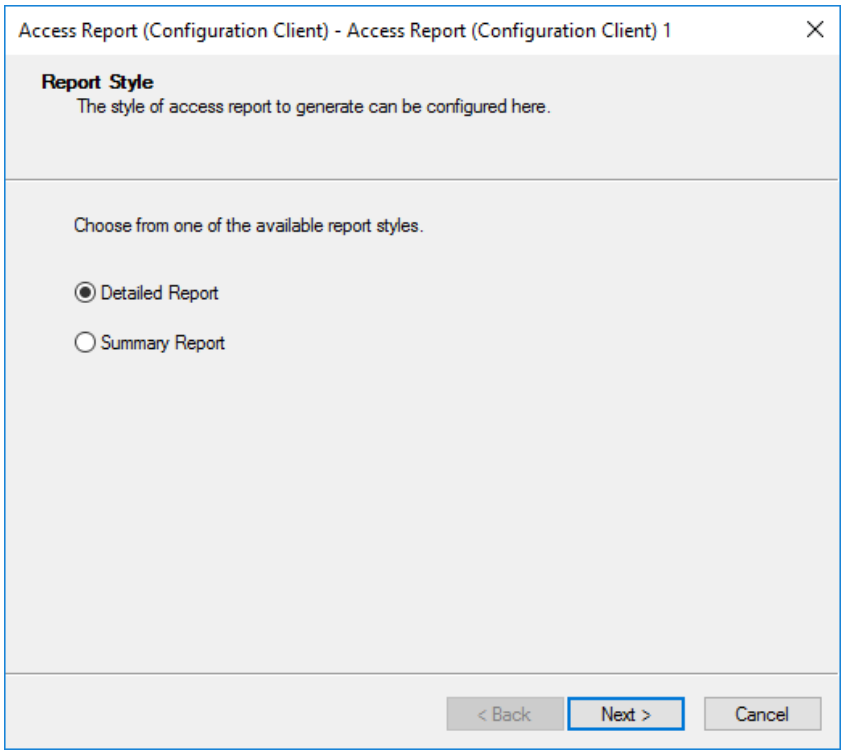
The Access Report provides a list of Cardholders who can access a door/zone during a specified time period.

Operators must have the "Edit Cardholders", "Edit Report Descriptions" and "View Site" operator privileges to create, save, edit and delete Access Reports.

## Report Wizard

The Access Report wizard contains a number of pages which prompt you to enter certain information to create a report.
**Follow the instructions displayed**.

### *Report Style page*

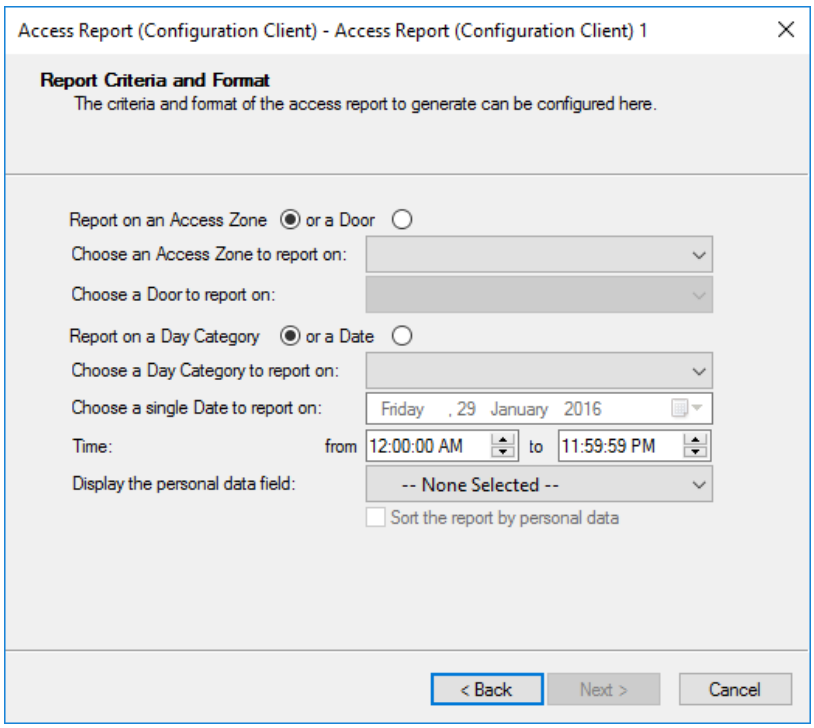



This is the first page of the Access Report wizard. It allows the operator to select either a **detailed** or **summary** version of the report.

**Detailed Access Reports** include a list of Cardholders along with their Personal Data and allocated cards. This style of the report is orientated around Cardholders, with the report sorted by Cardholder name or Personal Data Field. This report style also shows the date range over which a Cardholders access applies, which is determined from activation and expiry times of temporary access.

**Summary Access Reports** are orientated around Access Groups, and do not contain Cardholder information.

### *Report Criteria and Format page*




This page allows the operator to choose criteria for the report and set basic formatting features such as inclusion of a Personal Data Field (PDF) and the report's sort order. The **Access Zone** and **Door** fields are mutually exclusive in that the operator may only set criteria in one field or the other. The **Day Category** and **Date** fields are also mutually exclusive, and a date in the past cannot be selected. The time range fields are restricted to a single day, (i.e. they may not be set to cross midnight).

### *Report Generation and Saving page*

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

# Exception Report

## Introduction

The Exception Report allows operators to generate a list of exceptions to the normal system operation, (i.e. outstanding issues such as unprocessed alarms).

This report may be generated by an operator at the start of their shift, to obtain an overview of the system's current status. They request an Exception Report on the division for which they have responsibility immediately after logging onto the system.

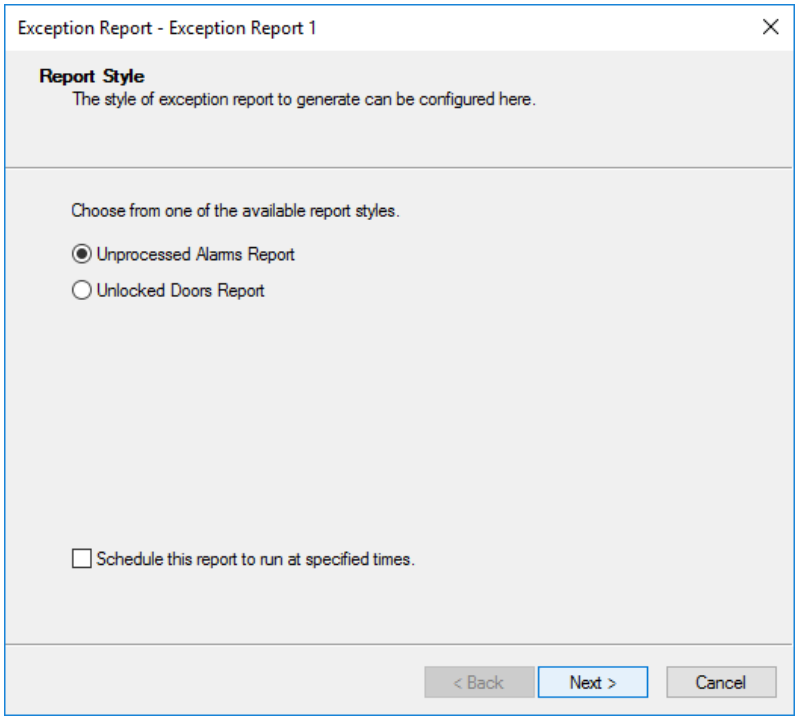
Operators must have the "Edit Report Descriptions" privilege to create, save, edit and delete Exception Reports.

This report can be scheduled to run automatically at regular times (via Action Plans or scheduled Macros). For further information refer to ***Automatically Generated Reports*** (on page 39-63) and ***Configuring Report Scheduling*** (on page 39-65).

## Report Wizard

The Exception Report wizard contains a number of pages which prompt you to enter certain information to create a report.
**Follow the instructions displayed.**

### *Report Style page*



This is the first page of the Exception Report wizard. It allows the operator to select either an **Unprocessed Alarms Report**, or an **Unlocked Doors Report**.

**Unprocessed Alarms Reports** include all unprocessed alarms, whether or not they are acknowledged. For this option to be enabled, an operator needs the “View Events and Alarms” or the “Edit Alarms” operator privileges.

**Unlocked Doors Reports** include all doors that are scheduled to be secure but are currently unlocked because of an override or an active alarm condition related to the door. This report is split into the following two sections:

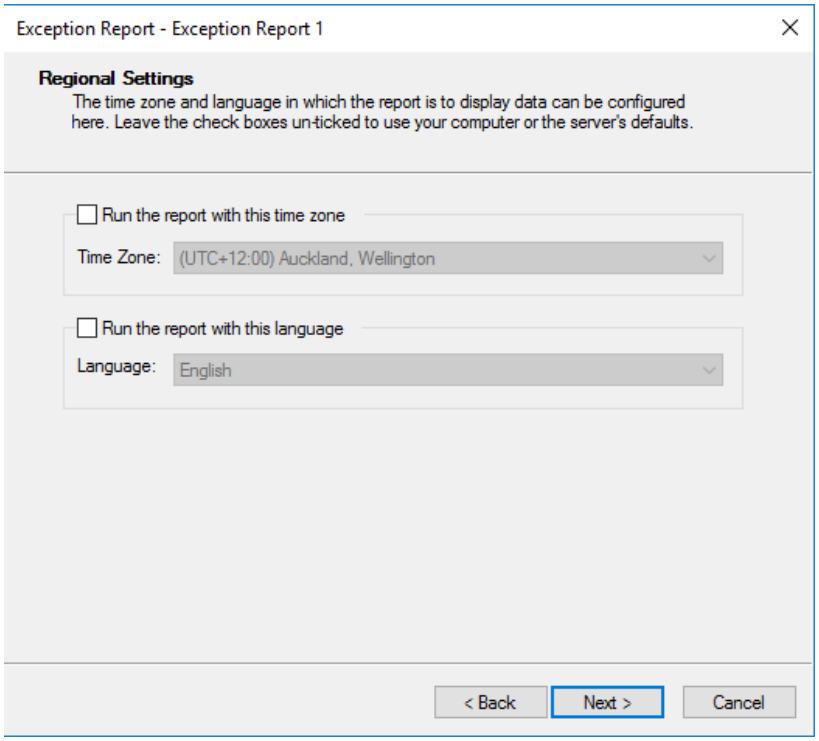
**Override section:**
This section of the report lists doors that are scheduled to be secure, but are currently in 'Free' mode.
**Note:** If a door has two zones (one entry zone and one exit zone), both zones need to be overridden to 'Free', otherwise the door will remain 'secure'.

**Active Alarms section:**
This section of the report lists doors with any of the active alarms:
- Forced Door
- Door Not Locked
- Door Open Too Long
- Door Emergency Release

For the 'Unlocked Doors Report' option to be enabled, an operator needs either the “View Site” or “Edit Site” operator privileges. This allows them to run the report, but they will only be able to view the Override section. They also require the "View Events and Alarms" operator privilege to view the Active Alarms section of the report.
**Note:** A secure door will not be listed as unlocked simply as a result of a cardholder opening the door temporarily to gain access at the time the report performs its checks.

You can optionally **Schedule this report to run at specified times** for both report styles.

### *Regional Settings page*

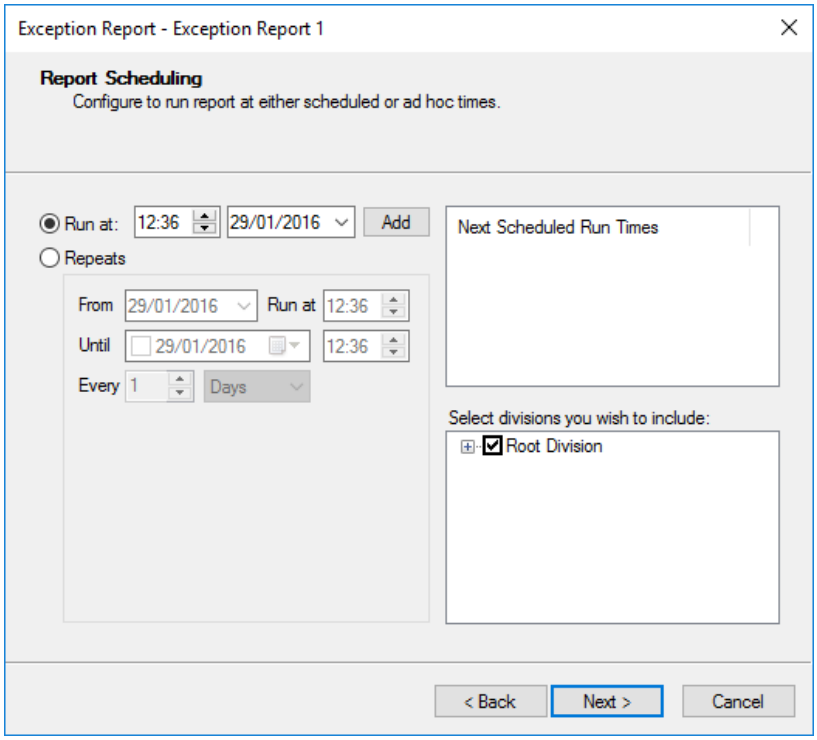



This page allows a time zone and/or language to be selected for the report. Selection of a time zone is optional, as it is only required for Command Centre sites that span time zones. Selection of a language is also optional as it is only required for sites that have multiple languages.

If no time zone is selected, the report uses the time zone of the Command Centre server, only if the report was initiated from a macro which was triggered by an Action Plan, or a macro that was run from its schedule. In all other cases, the report uses the time zone on the workstation of the operator who has run the report, or the time zone on the workstation of the operator who ran the macro that triggered the report.

If a time zone is selected, when the report is run, all dates and times within the report will display in the selected time zone. Any dates and times configured within the report are assumed to be within the selected time zone (rather than the time zone on the configuring operator's workstation).

### *Report Scheduling page*




This page only displays if the "Schedule this report to run at specified times" checkbox is checked on the **Report Style** page. It allows run times and repetition properties to be defined for the report.
Multiple explicit times for the report to be run can be configured, as follows:

1. Click the **Run at** radio button.
2. Enter a date and time, and click the **Add** button.
   The date and time appears in the **Next Scheduled Run Times** grid.
3. Repeat Steps 1-2 for each explicit time you require.
   **Note:** If you click the **Repeats** radio button, then the explicit additions are removed from the **Next Scheduled Run Times** grid.

Repeat times for the report to be run can be configured, as follows:

1. Click the **Repeats** radio button.
2. Select the 'initial' **From** date and time.
3. Select an **Until** date and time if required.
   **Note:** If no **Until** date is entered, the report will repeat indefinitely.
4. Select the regularity for the report to be run, (i.e. **Every** one or many **Hours**, **Days**, **Weeks** or **Months**).
   **Note:** When **Weeks** is selected from the drop-down list, the days of the week display with an ability to select one or multiple days, (e.g. Monday and Thursday).
   The next five dates and times appear in the **Next Scheduled Run Times** grid.

The **Division** selection grid allows the report to be scheduled for specific divisions.
**Note:** Only Divisions to which you have the appropriate editing privilege will appear in the drop-down list.

### *Report Generation and Saving page*

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

# Time and Attendance Report

## Introduction

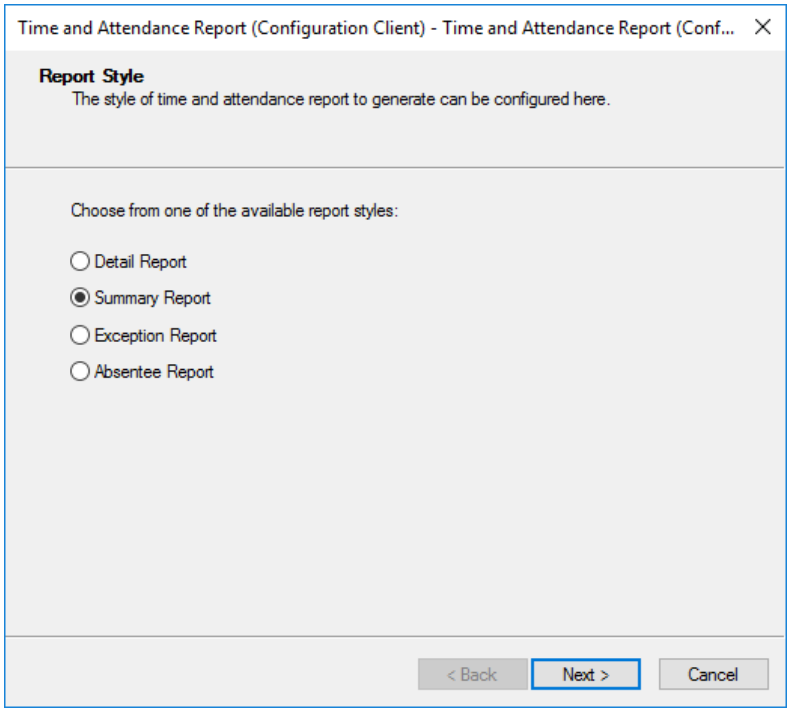
The Time and Attendance Report provides the ability to track hours worked by individual Cardholders. Door entry and exit events are used in the system to calculate hours worked by individual Cardholders. In general, a Door entry event is equated to a Cardholder clocking in or starting work, while a Door exit event equates to a Cardholder clocking out or ending work.

Operators must have the "View Cardholders", "Edit Report Descriptions" and "View Site" privileges to create, save, edit and delete Time and Attendance Reports. "View Site" privilege is required to see the readers used for the Time and Attendance Report.
**Note:** In a multi-server environment, for any given server where event aggregation is enabled, an operator can run a Time and Attendance Report which incorporates events from remote readers. The Time and Attendance Report can be filtered by remote readers.

## Report Wizard

The Time and Attendance Report wizard contains a number of pages which prompt you to enter certain information to create a report.
**Follow the instructions displayed**.

### *Report Style page*




This is the first page of the Time and Attendance Report wizard. It allows the

operator to choose between a **Detail** or **Summary** Time and Attendance Report, an **Exception Report** or an **Absentee Report**.

**Detail Reports** show the hours worked by selected Cardholders over the time period defined. They show every time a Cardholder clocked in or out during the reporting period, with a total of hours worked between each pair of clock in and out events.

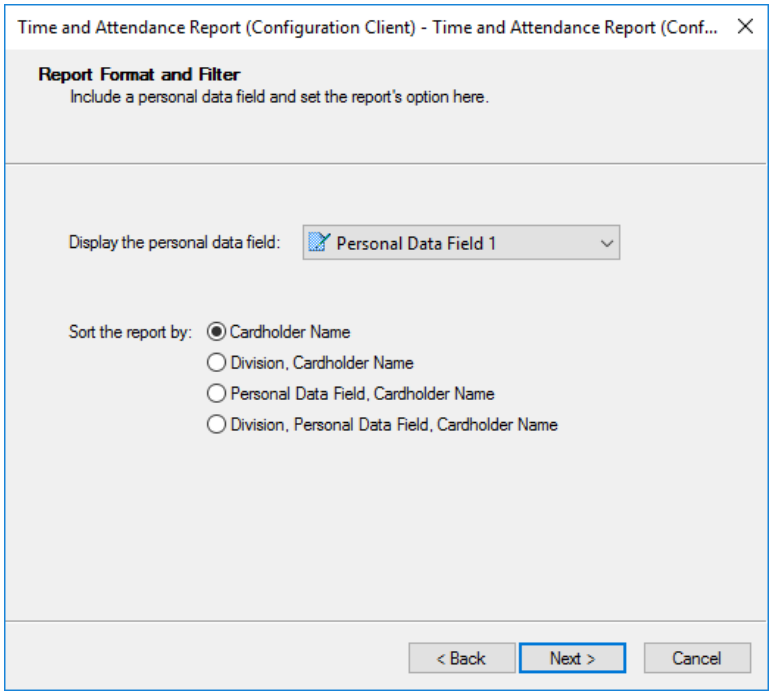
**Summary Reports** also show the hours worked by each Cardholder, but summarises this information on a daily basis. They show the first time a Cardholder clocked in for work and the last time they clocked out at the end of the day, with a total of actual hours worked between these times.

Detail Reports can have two entries for the one day - one that has insufficient data and one that is real, (e.g. a Cardholder badged their card at an entry reader and opened the door, but then decided not to enter. Ten minutes later the same Cardholder enters again at the same entry reader and exits eight hours later). In the Detail Report the time would all be added up correctly, but in a Summary Report it would note that day as having insufficient data.
If you run a Summary Report and get insufficient data for a Cardholder, run a Detail Report for that Cardholder.
**Note:**
It is recommended that if you run a Summary Report, you should also run an Exception Report. This is due to a Summary Report output giving no indication as to whether or not the report contains unusable events, whereas an Exception Report identifies any unusable events.

**Exception Reports** provide analysis of events that affect accurate time and attendance reporting, (e.g. a Cardholder may forget to clock out at the end of the day or present their card more than once when starting or leaving work). Accurate event information is critical to calculating hours worked for each Cardholder, and this allows you to identify incorrect events when a Cardholder's worked hours cannot be calculated or are excessive.

**Absentee Reports** provide information regarding days that a Cardholder did not work. They determine that a Cardholder was absent on a particular day if there were no clock in or out events.
**Note:**
You need to configure an absentee report to exclude weekends and/or other days that a Cardholder is not expected to work.

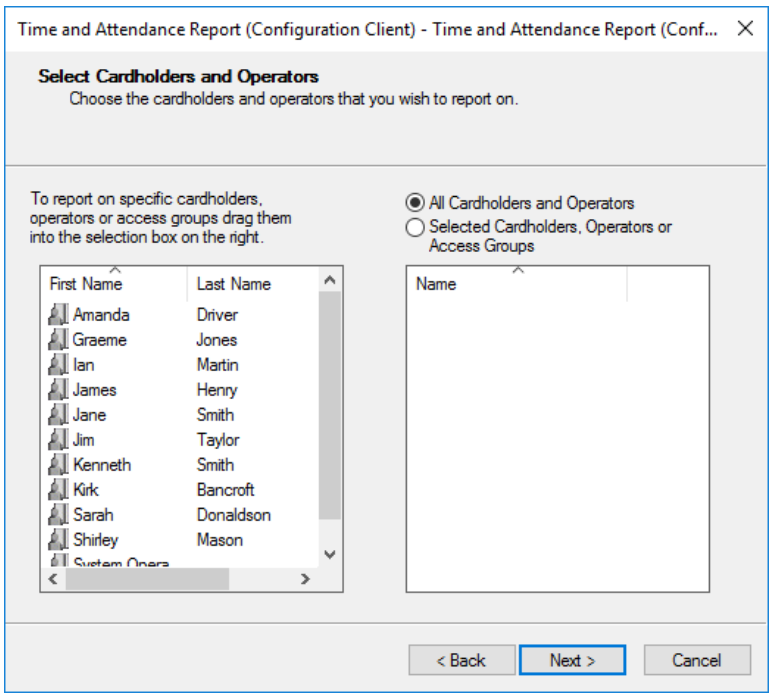
### *Report Format and Filter page*




This page allows the operator to set two options as follows:

- A string or numeric **Personal Data Field** can be selected for display in the report.
- The operator can sort the report by **Cardholder** name or **Personal Data Field**, with an optional top level sort by **Division**.

### *Select Cardholders and Operators page*




This page provides a list of Cardholders that an operator may include in the

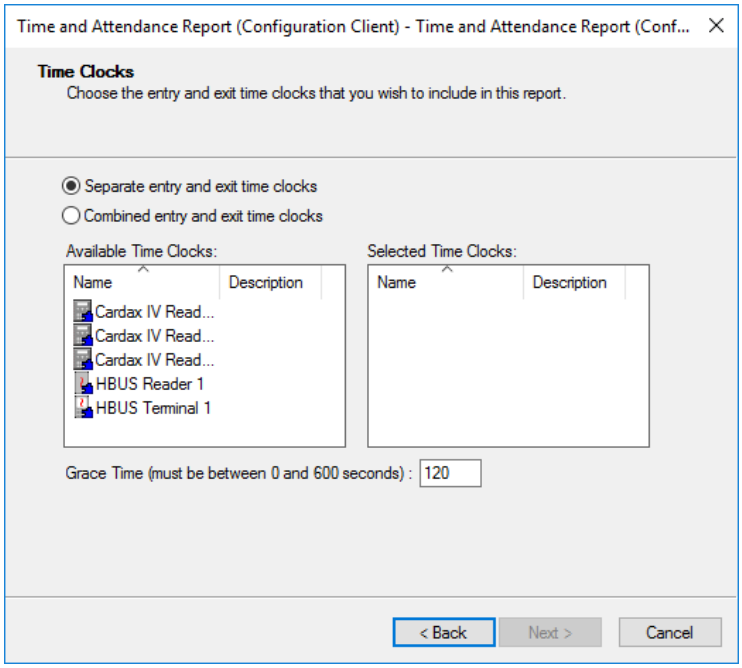
report. Cardholders shown here are restricted to those under the Division of the operator.

The Find Tool may be used to locate Cardholders, which can then be dragged and dropped onto this page. Alternatively, you can open the **Access Group** List Window and drag and drop those Access Groups you require onto this page.
**Note:** Only cardholders that are currently active within an Access Group will be reported on. Therefore, if you want the report to include 'expired' Access Group members, you need to select cardholders rather than Access Groups. The "Automatic removal of expired members" from Access Groups will alter the information in the report depending on when the report is run.

If an operator selects the **All Cardholders** option, then the report is run for all Cardholders under the current operator's Division.

Should you wish to delete a Cardholder from your list on the right, **right click** on the Cardholder and click **Remove from List**.

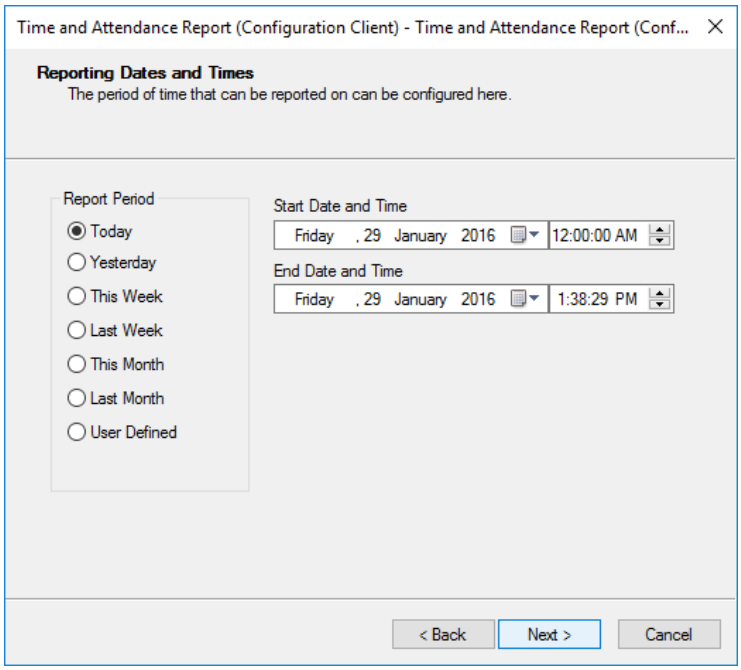
### *Time Clocks page*




This page provides a list of available Time Clocks or readers, from which an operator can select those to include in the report. The operator must also indicate if they are using combined or separate entry and exit Time Clocks (see explanations below), and adjust the Grace Time for duplicate events if required.
**Separate entry and exit time clocks:** One reader/clock for entry and another reader/clock for exit.
**Combined entry and exit time clocks:** A cardholder can swipe their card at any reader (entry or exit), and the FIRST read/badge is taken as the "Entry" read and the NEXT read/badge is taken as the "Exit" read for that cardholder.

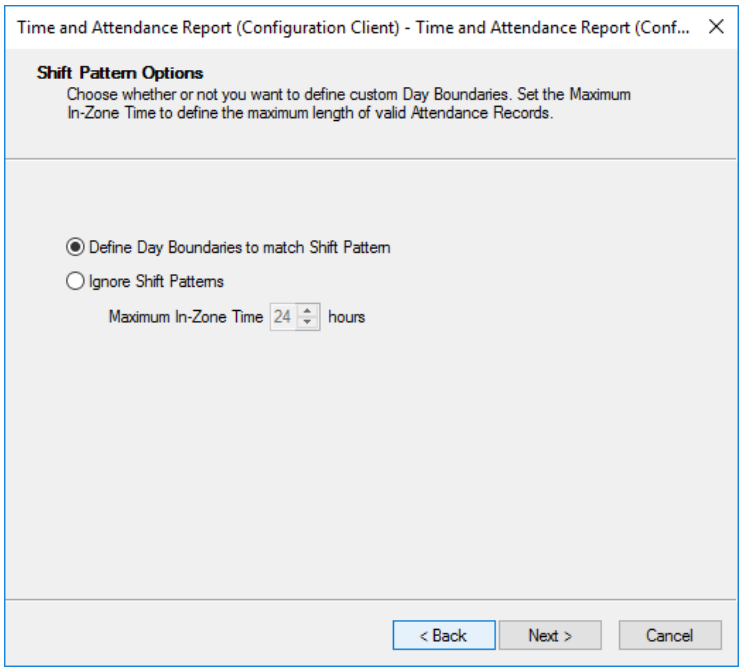
The system also does not check that the entry or exit was actually taken, as some sites just use the readers as time clocks, so they are not attached to doors at all.

### *Reporting Dates and Times page*




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

### *Shift Pattern Options page*

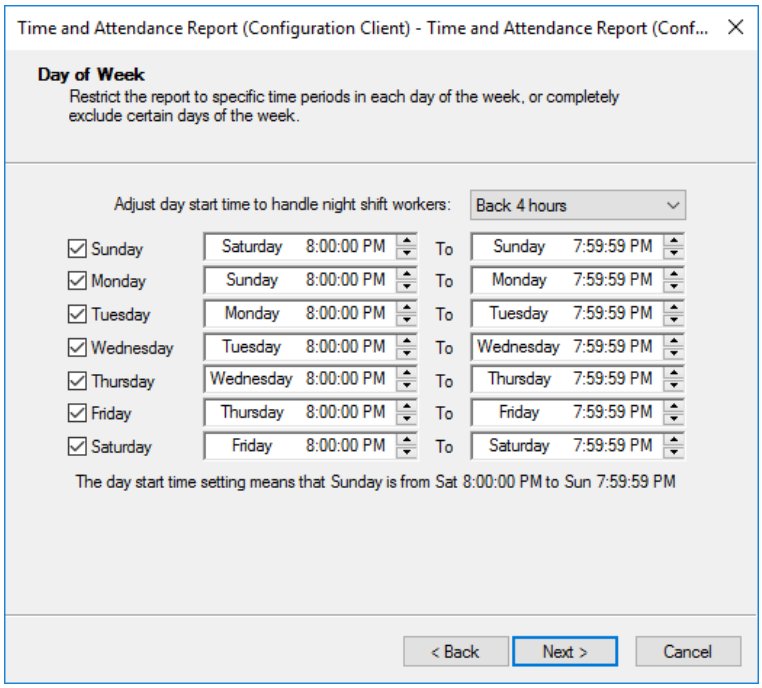



This page provides an operator options for determining what rules will be applied when calculating Attendance records for the report. It only displays if

**Detail**, **Summary** or **Exception Report** was selected on the first page of the wizard, (i.e. the 'Report Style' page). It will not display if **Absentee Report** is selected. If you click the **Define Day Boundaries to match Shift Pattern** radio button, and then the **Next** button, the 'Day of Week' page displays.

If you click the **Ignore Shift Patterns** radio button, and then the **Next** button, the 'Report Generation and Saving' page displays (skipping the 'Day of Week' page). The Ignore Shift Patterns option determines the appropriate report output using the Flexible Shift Pattern rules, and when selected also enables the **Maximum In-Zone time** field which is used by the Flexible Shift Pattern rules. The figure entered in this field determines the time span after which a cardholder has exited without badging their card. See ***Flexible Shift Pattern rules*** (on page 39-46) for a full explanation of these rules, and ***Working Examples*** (on page 39-48) to help explain how this option works.

### *Day of Week page*




This page allows time restrictions to be applied within the overall reporting period. It only displays if **Absentee Report** was selected on the first page of the wizard, (i.e. the 'Report Style' page), or if the **Define Day Boundaries to match Shift Pattern** radio button was selected on the 'Shift Pattern Options' page. Individual days of the week can be excluded from the report, or alternatively the report may be restricted to a specific time slice in specific days of the week. The operator can also adjust the day start time to accommodate night shift workers, (i.e. move the concept of midnight).

### *Report Generation and Saving page*

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

## Flexible Shift Pattern rules

When the Ignore Shift Patterns option is selected on the 'Shift Pattern Options' page of the Time and Attendance Report wizard, the following rules apply:

**Usable Events**

1. The following describes events that will be used to create Attendance Records.
   - An Entry Event will only be used if its subsequent event is an Exit Event, or if it has no subsequent event within the Report Time-Frame. An Entry Event will NOT be used if its subsequent event is also an Entry Event.
   - An Exit Event will only be used if its preceding event is an Entry Event, or if it has no preceding event within the Report Time-Frame. An Exit Event will NOT be used if its preceding event is also an Exit Event.
   - The usability of an event is subject to the resulting Attendance Record being valid. See “Valid Attendance Records” below.

**Creating normal Attendance Records**

2. A normal Attendance Record is created by finding the first unused Usable Entry Event for a Cardholder and matching it with the next Usable Exit Event to determine the total contiguous In-Zone Time for the Cardholder. See “Usable Events” for the definition of Usable Entry and Exit Events.

**Creating Attendance Records using assumptions**

3. If the Cardholder’s First Event is an Exit Event, then assume the Cardholder was In-Zone at the Report Start Date-Time and create an Attendance Record to reflect this. Use the Report Start Date-Time as the Entry Time. NB: The resulting Attendance Record will be subject to the “Valid Attendance Records” rule (see below).
4. If the Cardholder’s Final Event is an Entry Event, then assume the Cardholder was In-Zone at the Report End Date-Time and create an Attendance Record to reflect this. Use the Report End Date-Time as the Exit Time. NB: The resulting Attendance Record will be subject to the “Valid Attendance Records” rule (see below).

**Valid Attendance Records**

5. Any Attendance Record whose Attendance Time is greater than the Maximum In-Zone Time is considered invalid. Both the Entry Event and the Exit Event for that record must be classed as unusable and reported accordingly.

6. Day Boundaries are not a consideration for Flexible Shift Pattern rules. Attendance Records that span across a Day Boundary are considered valid.

**Creating Summary Attendance Records**

7. A Summary Attendance Record is created by combining all valid Attendance Records (for a particular Cardholder) that have the same Entry Date, regardless of the Attendance Record's End Date-Time.
8. A Summary Attendance Record is given a Entry Date-Time equal to the Entry Date-Time of the first Attendance Record in the summarised group, and an End Date-Time equal to the End Date-Time of the last Attendance Record in the summarised group.
9. The Summary Attendance Record has a Total Worked Time equal to the sum of Time Worked for all Attendance Records in the summarised group (any time the Cardholder was absent in-between the Summary Attendance Record's Entry Date-Time and End Date-Time is not included).

**Valid Summary Attendance Records**

10. All calculated Summary Attendance Records are considered valid regardless of their length.
11. If any unusable events occur in-between the Summary Attendance Record's Entry Date-Time and End Date-Time, the unusable events are ignored and this does not invalidate the Summary Attendance Record.
12. The Maximum In-Zone Time setting is not a consideration when creating Summary Attendance Records. The Total Worked Time of a Summary Attendance Record can exceed the Maximum In-Zone Time setting but none of the individual Attendance Records in the summarised group will.

## Working Examples

The following examples help explain how the 'Ignore Shift Patterns' option in the **Time and Attendance Report** works, by showing examples of report output. There are four examples provided, with Examples 1 - 3 being examples of a 'Detail Report', and Example 4 being an example of a 'Summary Report'.

***Example 1: Maximum In-Zone Time (Detail Report)***

***Example 2: First event is an Exit or last event an Entry (Detail Report)***

***Example 3: Missing Entry or Exit events (Detail Report)***

***Example 4: Summary Report***

### Example 1: Maximum In-Zone Time (Detail Report)

In this example, the raw data contains an Entry Event and Exit Event that would result in an invalid Attendance Record. The Cardholder has tailgated out after work on Monday and tailgated back in on Tuesday morning.

#### Raw Data

| Event | Date | Time |
|---|---|---|
| Entry | Mon 22 Jan | 8:30 a.m. |
| Exit | Mon 22 Jan | 12:30 p.m. |
| Entry | Mon 22 Jan | 1:00 p.m. |
| Exit | Tue 23 Jan | 12:30 p.m. |
| Entry | Tue 23 Jan | 1:00 p.m. |
| Exit | Tue 23 Jan | 5:00 p.m. |

#### Report Scenario 1

In this scenario we use the above raw data and set the following values when running the report.

**Report Start Date-Time:** Monday, 22 Jan 2007 00:00:00

**Report End Date-Time:** Tuesday, 23 Jan 2007 23:59:59

**Maximum In-Zone Time:** 24hrs

#### Report Output

The Entry Event at 1:00pm on Monday is matched with the Exit Event at 12:30pm on Tuesday and an Attendance Record is created for 23.5hrs. This is treated as a valid record because its length is less than the Maximum In-Zone Time setting of 24hrs.

| Entry Clock | Entry Card | Entry Date/Time | Exit Clock | Exit Card | Exit Date/Time | Time Worked |
|---|---|---|---|---|---|---|
| Main Entry Reader | 501 | 22/01/2007 8:30:00 a.m. | Main Exit Reader | 501 | 22/01/2007 12:30:00 p.m. | 4:00:00 |
| Main Entry Reader | 501 | 22/01/2007 1:00:00 p.m. | Main Exit Reader | 501 | 23/01/2007 12:30:00 p.m. | 23:30:00 |
| Main Entry Reader | 501 | 23/01/2007 1:00:00 p.m. | Main Exit Reader | 501 | 23/01/2007 5:00:00 p.m. | 4:00:00 |
| | | | | | Total Working Time (Excluding insufficient Data): | 31:30:00 |

### Report Scenario 2

In this scenario we use the same raw data but reduce the Maximum In-Zone Time setting to 20hrs.

**Report Start Date-Time:** Monday, 22 Jan 2007 00:00:00

**Report End Date-Time:** Tuesday, 23 Jan 2007 23:59:59

**Maximum In-Zone Time:** 20hrs

### Report Output

Now the Entry Event at 1:00pm on Monday is not matched with the Exit Event at 12:30pm on Tuesday because the resulting Attendance Record would be invalid because its length (23.5hrs) would exceed the Maximum In-Zone Time setting of 20hrs. Instead, these events are displayed showing “Insufficient Data”.

| Entry Clock | Entry Card | Entry Date/Time | Exit Clock | Exit Card | Exit Date/Time | Time Worked |
|---|---|---|---|---|---|---|
| Main Entry Reader | 501 | 22/01/2007 8:30:00 a.m. | Main Exit Reader | 501 | 22/01/2007 12:30:00 p.m. | 4:00:00 |
| Main Entry Reader | 501 | 22/01/2007 1:00:00 p.m. | | | | Insuff. D. |
| | | | Main Exit Reader | 501 | 23/01/2007 12:30:00 p.m. | Insuff. D. |
| Main Entry Reader | 501 | 23/01/2007 1:00:00 p.m. | Main Exit Reader | 501 | 23/01/2007 5:00:00 p.m. | 4:00:00 |
| | | | | | Total Working Time (Excluding insufficient Data): | 8:00:00 |

## Example 2: First event is an Exit or last event an Entry (Detail Report)

In this example, the Cardholder’s first event within the Report Time-Frame is an Exit Event, and the Cardholder’s last event within the Report Time-Frame is an Entry Event.

### Raw Data

| Event | Date | Time |
|---|---|---|
| Exit | Mon 22 Jan | 12:30 p.m. |
| Entry | Mon 22 Jan | 1:00 p.m. |
| Exit | Mon 22 Jan | 5:00 p.m. |
| Entry | Tue 23 Jan | 8:30 a.m. |
| Exit | Tue 23 Jan | 12:30 p.m. |
| Entry | Tue 23 Jan | 1:00 p.m. |

### Report Scenario 1

In this scenario we use the above raw data and set the following values when running the report.

**Report Start Date-Time:** Monday, 22 Jan 2007 00:00:00

**Report End Date-Time:** Tuesday, 23 Jan 2007 23:59:59

**Maximum In-Zone Time:** 24hrs

### Report Output

The time between the Report Start Date-Time (22 Jan) and the first event (an Exit Event) is 12.5hrs which does not exceed the Maximum In-Zone Time setting (24hrs) so an Attendance Record is created using the Report Start Date-Time as the assumed entry time.

Similarly, the time between the last event (an Entry Event) and the Report End Date-Time does not exceed the Maximum In-Zone Time setting so an Attendance Record is created using the Report End Date-Time as the assumed exit time.

Note that if the Maximum In-Zone Time had been set to say, 10hrs, then the first and last Attendance Records would NOT have been created because they exceed this length.

| Entry Clock | Entry Card | Entry Date/Time | Exit Clock | Exit Card | Exit Date/Time | Time Worked |
|---|---|---|---|---|---|---|
| Report Start Date-Time | | 22/01/2007 12:00:00 a.m. | Main Exit Reader | 501 | 22/01/2007 12:30:00 p.m. | 12:30:00 |
| Main Entry Reader | 500 | 22/01/2007 1:00:00 p.m. | Main Exit Reader | 500 | 22/01/2007 5:00:00 p.m. | 4:00:00 |
| Main Entry Reader | 501 | 23/01/2007 8:30:00 a.m. | Main Exit Reader | 501 | 23/01/2007 12:30:00 p.m. | 4:00:00 |
| Main Entry Reader | 501 | 23/01/2007 1:00:00 p.m. | Report End Date-Time | | 23/01/2007 11:59:59 p.m. | 10:59:59 |

Total Working Time (Excluding insufficient Data): 31:29:59

### Report Scenario 2

In this scenario we use the same raw data as in Scenario 1 but we use a different Report Time-Frame. We'll report on the whole month (1 Jan – 31 Jan).

| | |
|---|---|
| **Report Start Date-Time:** | Monday, 1 Jan 2007 00:00:00 |
| **Report End Date-Time:** | Wednesday, 31 Jan 2007 23:59:59 |
| **Maximum In-Zone Time:** | 24hrs |

### Report Output

The Cardholder's first event within the Report Time-Frame is an Exit Event and the time between the Report Start Date-Time and this first event exceeds the Maximum In-Zone Time so no Attendance Record is created.

Similarly, the time between the last event (an Entry Event) and the Report End Date-Time exceeds the Maximum In-Zone Time setting so no Attendance Record is created.

| Entry Clock | Entry Card | Entry Date/Time | Exit Clock | Exit Card | Exit Date/Time | Time Worked |
|---|---|---|---|---|---|---|
| | | | Main Exit Reader | 501 | 22/01/2007 12:30:00 p.m. | Insuff. D. |
| Main Entry Reader | 500 | 22/01/2007 1:00:00 p.m. | Main Exit Reader | 500 | 22/01/2007 5:00:00 p.m. | 4:00:00 |
| Main Entry Reader | 501 | 23/01/2007 8:30:00 a.m. | Main Exit Reader | 501 | 23/01/2007 12:30:00 p.m. | 4:00:00 |
| Main Entry Reader | 501 | 23/01/2007 1:00:00 p.m. | | | | Insuff. D. |
| | | | | | Total Working Time (Excluding insufficient Data): | 8:00:00 |

### Comments

Note that the same raw data has produced different Total Working Times in different reports. To minimize this effect, the Maximum In-Zone Time should be set as low as it can be set without excluding valid Attendance Records, and Report Time-Frames should be set to the minimum time-frame required to cover all the desired raw data.

## Example 3: Missing Entry or Exit events (Detail Report)

In this example, the raw data contains multiple consecutive Entry Events as well as multiple consecutive Exit Events. On Monday the Cardholder has tailgated out to lunch. On Tuesday the Cardholder has tailgated back in after lunch.

### Raw Data

| Event | Date | Time |
|---|---|---|
| Entry | Mon 22 Jan | 8:30 a.m. |
| Entry | Mon 22 Jan | 1:00 p.m. |
| Exit | Mon 22 Jan | 5:00 p.m. |
| Entry | Tue 23 Jan | 8:30 a.m. |
| Exit | Tue 23 Jan | 12:30 p.m. |
| Exit | Tue 23 Jan | 5:00 p.m. |

### Report Scenario 1

In this scenario we use the above raw data and set the following values when running the report.

**Report Start Date-Time:** Monday, 22 Jan 2007 00:00:00

**Report End Date-Time:** Tuesday, 23 Jan 2007 23:59:59

**Maximum In-Zone Time:** 24hrs

### Report Output

The first Entry Event is unusable because its subsequent event is not an Exit Event, so no Attendance Record is created. The event is displayed showing “Insufficient Data”.

Similarly, the last Exit Event is unusable because its previous event is not an Entry Event, so no Attendance Record is created. The event is displayed showing “Insufficient Data”.

| Entry Clock | Entry Card | Entry Date/Time | Exit Clock | Exit Card | Exit Date/Time | Time Worked |
|---|---|---|---|---|---|---|
| Main Entry Reader | 501 | 22/01/2007 8:30:00 a.m. | | | | Insuff. D. |
| Main Entry Reader | 501 | 22/01/2007 1:00:00 p.m. | Main Exit Reader | 501 | 22/01/2007 5:00:00 p.m. | 4:00:00 |
| Main Entry Reader | 501 | 23/01/2007 8:30:00 a.m. | Main Exit Reader | 501 | 23/01/2007 12:30:00 p.m. | 4:00:00 |
| | | | Main Exit Reader | 501 | 23/01/2007 5:00:00 p.m. | Insuff. D. |
| | | | | | Total Working Time (Excluding insufficient Data): | 8:00:00 |

### Comments

In this example, extending the Report Time-Frame to start earlier and/or end later, will not affect the output of the report because the Report Start and End Date-Times are not being used to create any Attendance Records.

### Example 4: Summary Report

In this example, the raw data contains matched Entry and Exit Events that cross over midnight. The Cardholder works a morning shift on Monday, a night shift on Tuesday, an afternoon shift on Wednesday and Thursday, and has Friday off.

#### Raw Data

| Event | Date | Time |
|---|---|---|
| Entry | Mon 22 Jan | 7:00 a.m. |
| Exit | Mon 22 Jan | 11:30 a.m. |
| Entry | Mon 22 Jan | 12:00 p.m. |
| Exit | Mon 22 Jan | 3:30 p.m. |
| Entry | Tue 23 Jan | 11:00 p.m. |
| Exit | Wed 24 Jan | 3:00 a.m. |
| Entry | Wed 24 Jan | 3:30 a.m. |
| Exit | Wed 24 Jan | 7:30 a.m. |
| Entry | Wed 24 Jan | 11:00 p.m. |
| Exit | Thu 25 Jan | 3:00 a.m. |
| Entry | Thu 25 Jan | 3:30 a.m. |
| Exit | Thu 25 Jan | 7:30 a.m. |
| Entry | Thu 25 Jan | 3:00 p.m. |
| Exit | Thu 25 Jan | 7:00 p.m. |
| Entry | Thu 25 Jan | 7:30 p.m. |
| Exit | Thu 25 Jan | 11:30 p.m. |

#### Report Scenario 1

In this scenario we use the above raw data and set the following values when running the report.

| | |
|---|---|
| **Report Start Date-Time:** | Monday, 22 Jan 2007 00:00:00 |
| **Report End Date-Time:** | Friday, 26 Jan 2007 23:59:59 |
| **Maximum In-Zone Time:** | 20hrs |

#### Report Output

The Cardholder has worked a total of 8 hours on Monday (lunch breaks are excluded).

On Tuesday the Cardholder starts a night shift at 11:00pm and clocks out for a break at 3:00 Wednesday morning, so the report shows this as a total of 4 hours for Tuesday.

The second half of the Tuesday night shift (Wednesday morning) is combined with the first half of the Wednesday night shift to give a total of 8 hours for Wednesday.

The second half of the Wednesday night shift (Thursday morning) is combined with the Thursday afternoon shift to give a total of 12 hours for Thursday.

| Entry Clock Name | First Entry Date/Time | Exit Clock Name | Exit Date/Time | Time Worked |
|---|---|---|---|---|
| Main Entry Reader | 22/01/2007 7:00:00 a.m. | Main Exit Reader | 22/01/2007 3:30:00 p.m. | 8:00:00 |
| Main Entry Reader | 23/01/2007 11:00:00 p.m. | Main Exit Reader | 24/01/2007 3:00:00 a.m. | 4:00:00 |
| Main Entry Reader | 24/01/2007 3:30:00 a.m. | Main Exit Reader | 25/01/2007 3:00:00 a.m. | 8:00:00 |
| Main Entry Reader | 25/01/2007 3:30:00 a.m. | Main Exit Reader | 25/01/2007 7:30:00 a.m. | 12:00:00 |
| | | | Total Working Time (Excluding insufficient Data): | 32:00:00 |

**Comments**

Because the Cardholder clocks out for mid-shift breaks, night shift hours are spread across different days – the first half of the shift being shown on one day and the second half of the shift being shown on the next. To get the entire Tuesday night shift to be included in Tuesday's total, the Cardholder must not clock out between midnight and the end of the shift.

Note that if the Report End Date-Time had been set to Wednesday, 24 Jan 2007 00:00:00, then Tuesday's Time Worked would only show 1 hour because the report would assume an exit at the Report End Date-Time.

# Site Configuration Report

## Introduction

The Site Configuration Report allows an operator to obtain a hard copy record of the configuration for selected items. The report may be generated for any selected items within the operator's division. Items **not** reported on are: Crypt Seed, Facility Code, Cardholders, Access Groups, Personal Data Fields, Operator Groups and Operator Privileges.

Operators must have the "View Site" and "Edit Report Descriptions" privileges to create, save, edit and delete Site Configuration Reports. System division restricts the level of item information that an operator may view through the report.

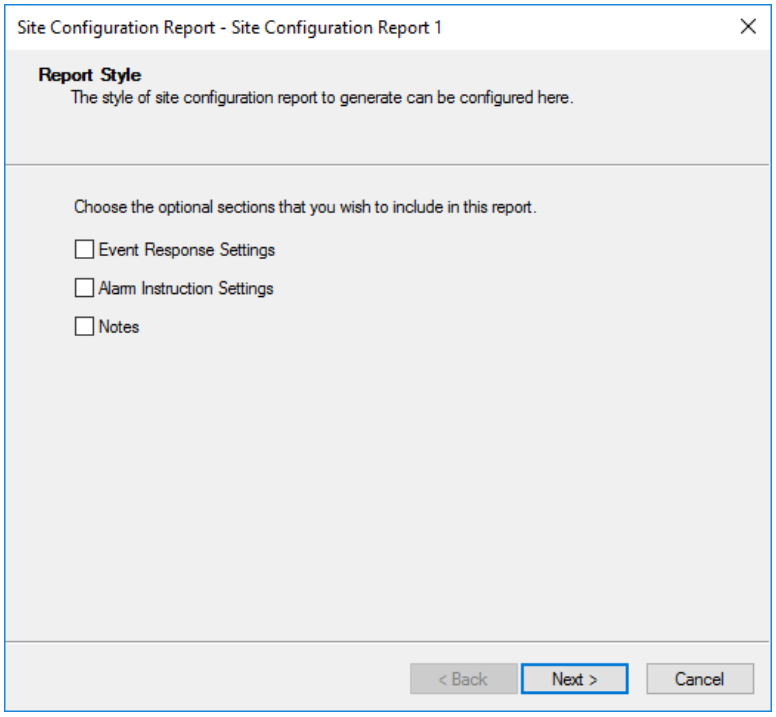
**Note:** The Site Configuration Report can be used for Guard Tours, (i.e. it can list the checkpoints for a security guard to follow on a specific Guard Tour route, and indicate times allowed (and tolerances) between checkpoints). The report can be run so that:

- text held in the **Notes** tab of a Guard Tour can be optionally displayed on the report (by checking the **Notes** checkbox on the **Report Style** page). This allows special instructions to be printed for the benefit of the guard.
- all other site configuration data is eliminated (on the **Select Items** page).

## Report Wizard

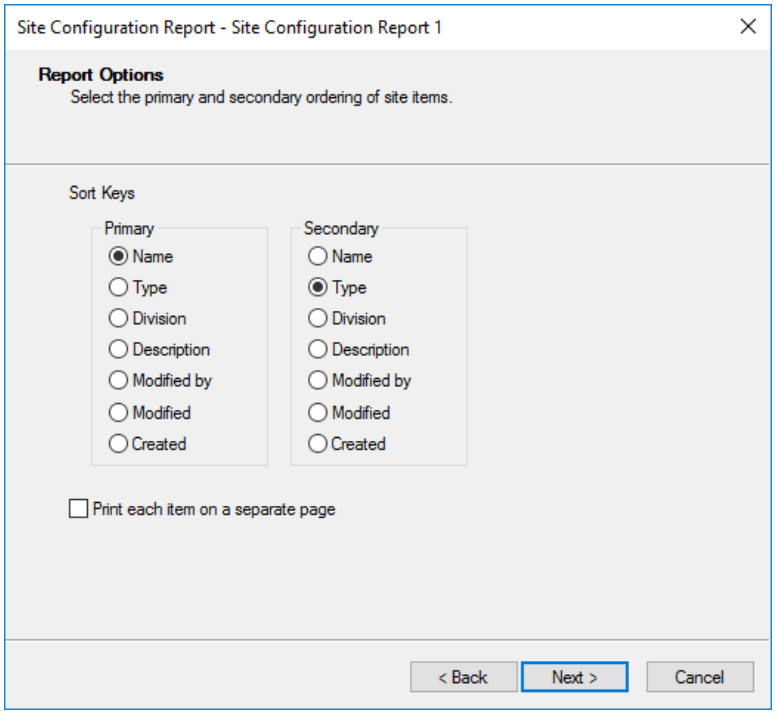
The Site Configuration Report wizard contains a number of pages which prompt you to enter certain information to create a report.
**Follow the instructions displayed**.

### *Report Style page*




This is the first page of the Site Configuration Report and allows the operator to choose optional section(s) to include in the report, (i.e. either one or two, or all three options can be selected).

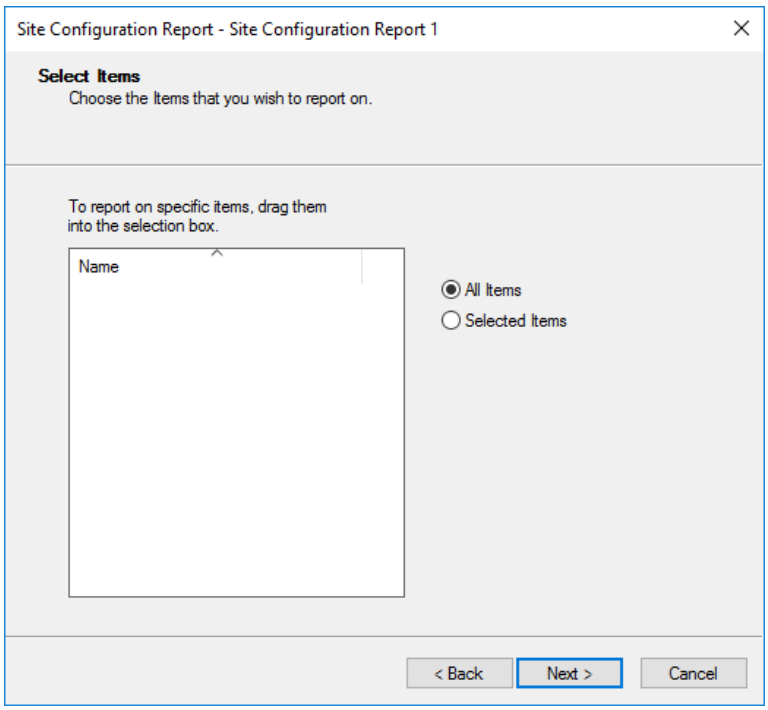
### *Report Options page*




This page allows the operator to choose a primary and secondary sort key for the report. The default sort keys are 'Name' for the primary key, and 'Type' for the secondary key.

The operator can also choose whether to have each item printed on a separate page, or to have them printed continuously.

### *Select Items page*




This page allows the operator to include specific items in the report, (i.e. all items or selected items). If the operator selects the radio button for all items, the **Next** button is enabled. If however the operator selects the radio button for selected items, the **Next** button will not be enabled until items have been placed in the selection box.

The operator can either use the Find Tool to search for items, and drag and drop them into the selection box as criteria for this report, or alternatively drag items from list windows.

### *Report Generation and Saving page*

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

# Contact ID Assignment Report

## Introduction

The Contact ID Assignment Report allows an operator to produce a report of all the possible Contact ID strings that can be sent from a Dialler to a remote monitoring station. This report is designed to be sent to the remote monitoring station to help them interpret the Contact ID messages for this site. See External Alarm Monitoring for further details.
The report has three sections, as follows:

**Alarm Zones:** Alarm Zones that are listed are all those with a GG value set to something other than 00.

**Cardholders:** Cardholders that are listed are all those with a CCC value set to something other than 000.

**Contact ID Area Code (GG):** Items in this section have:
- an **Alarm Dialling** tab,
- a CCC set to something other than 000, and
- an Alarm Zone assigned on their **Event Response** tab.

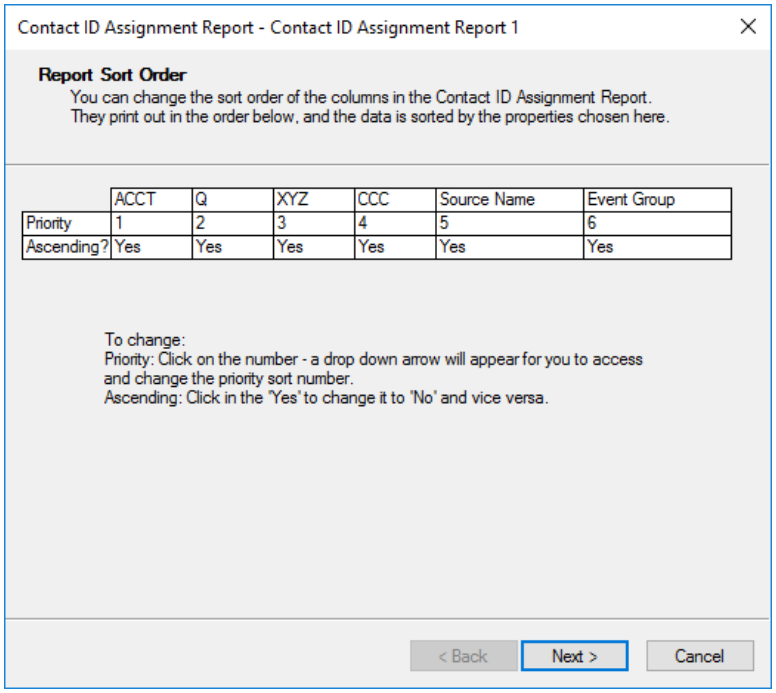
**Note:** All 400 level XYZ plus 121, 313 XYZ are user type, so they will display as "CCC" and "User Dependent" in the report rather than the actual Site Item name.

Operators must have the "View Site" and "Edit Report Descriptions" privileges to create, save, edit and delete Contact ID Assignment Reports with Contact ID data relating to *site items*. To create, save, edit and delete Contact ID Assignment Reports with Contact ID data relating to *cardholders*, they must have the "Edit Cardholders" privilege. System division restricts the level of site item information that an operator may view through the report.

## Report Wizard

The Contact ID Assignment Report wizard contains three pages which enable you to create a report.
**Follow the instructions displayed**.

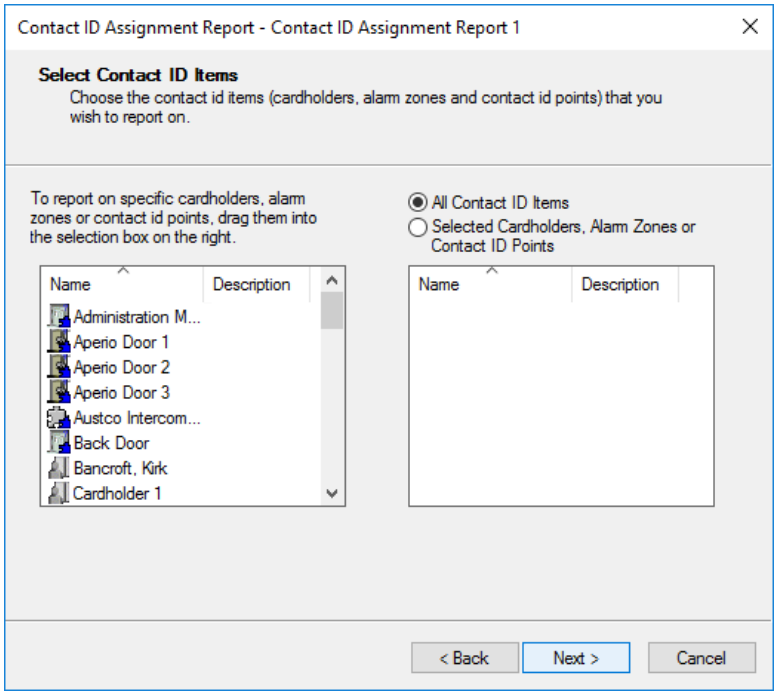
### *Report Sort Order page*




This is the first page of the Contact ID Assignment Report wizard. It allows the operator to alter the sort order of the columns in a Contact ID Assignment Report.

By clicking on a Priority number (1-6), a drop-down arrow will appear from which you can select a different priority sort number. You can also choose whether to sort a column by ascending or descending order, by clicking on **Yes**, which will automatically change to **No**, and vice versa.

### *Select Contact ID Items page*



This page provides a list of Contact ID Items, (i.e. Cardholders, Alarm Zones and Contact ID points), that an operator may include in the report, rather than having to report on everything. Items shown here are restricted to those under the Division of the operator.

The Find Tool may be used to locate the Contact ID Items, which can then be dragged and dropped onto this page. Alternatively, you can open the appropriate List Window and drag and drop those items you require onto this page.

Should you wish to delete an item from your list on the right, **right click** on the item and click **Remove from List**.

**Sample Output:**

| ACCT | Q | XYZ | GG | CCC | Source Name | Event Group |
|---|---|---|---|---|---|---|
| 0281 | 1 | 130 | 00 | 000 | Input to be Triggered | Open/Off |
| 0281 | 3 | 130 | 00 | 000 | Input to be Triggered | Open/Off |
| 0282 | 1 | 130 | 00 | 082 | 004 on 2.82 | Open/Off |
| 0282 | 1 | 393 | 00 | 282 | Modem on 2.82 | Alarm Dialling Failure |
| 0282 | 1 | 602 | 00 | 282 | Modem on 2.82 | {Periodic Test} |
| 0282 | 3 | 130 | 00 | 082 | 004 on 2.82 | Open/Off |
| 0282 | 3 | 393 | 00 | 282 | Modem on 2.82 | Alarm Dialling Failure |
| 0283 | 1 | 393 | 00 | 283 | Modem on 2.83 | Alarm Dialling Failure |
| 0283 | 1 | 602 | 00 | 283 | Modem on 2.83 | {Periodic Test} |
| 0283 | 3 | 393 | 00 | 283 | Modem on 2.83 | Alarm Dialling Failure |
| 0284 | 1 | 130 | 00 | 084 | 004 on 2.84 | Open/Off |
| 0284 | 3 | 130 | 00 | 084 | 004 on 2.84 | Open/Off |
| 1234 | 1 | 130 | 00 | 000 | 001 | Open/Off |
| 1234 | 1 | 130 | 00 | 000 | 002 | Open/Off |
| 1234 | 1 | 393 | 00 | 000 | Cardax 3000 Modem | Alarm Dialling Failure |
| 1234 | 1 | 602 | 00 | 000 | Cardax 3000 Modem | {Periodic Test} |
| 1234 | 1 | 602 | 00 | 000 | Flooding # 2 | {Periodic Test} |
| 1234 | 3 | 130 | 00 | 000 | 001 | Open/Off |

### *Report Generation and Saving page*

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

# Wiring Report

## Introduction

The Wiring Report allows the operator to create a new report, or set of reports, which can be run after hardware has been configured in Command Centre. The report provides documentation which tells the installer how the hardware must be wired. Ideally installers will run this at the end of running a wizard to configure the hardware.

Operators require the "View Site" and "Edit Report Descriptions" operator privileges to create, save, edit and delete Wiring Reports.

The items that can be reported on are listed below:

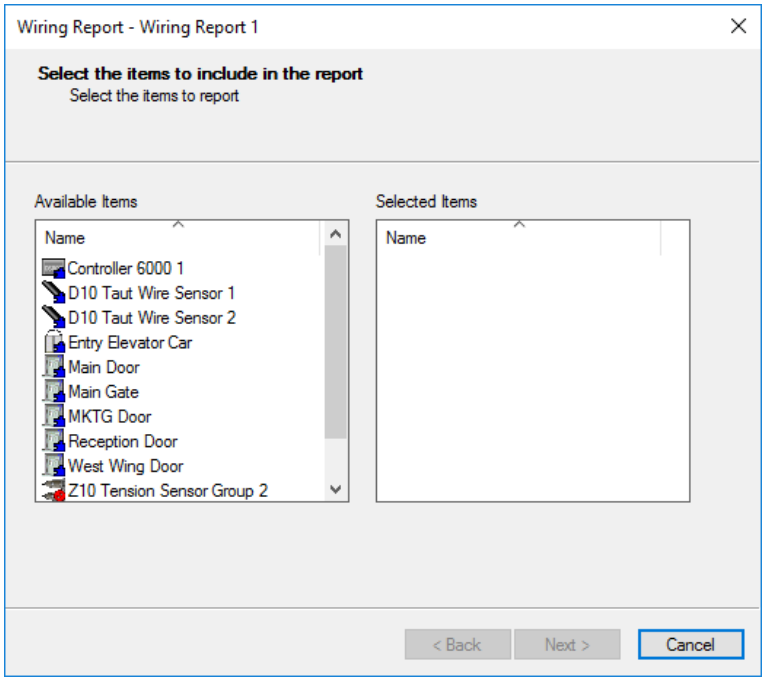
Controller 6000s

| | |
|---|---|
| HBUS Devices: | HBUS F31/F32/F41/F42 Fence Controller<br>HBUS F22 Fence Controller<br>HBUS Z10 Tension Sensor Group<br>HBUS I/O |
| Other: | Doors<br>Elevator Car |

## Report Wizard

The Wiring Report wizard contains only two pages which enable you to create a report.
**Follow the instructions displayed**.

### *'Device Selection' page*



This page provides a list of all the items that an operator may include in the report. Drag and drop those items you require from the **Available Items** list, to the **Selected Items** column on the right.

**Note:** As long as the **Selected Items** list on the right remains empty, the **Next** button will be disabled.

Should you wish to remove an item from the **Selected Items** list, **right click** on the item and click **Remove from List**.

### *Report Generation and Saving page*

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

## Automatically Generated Reports

### Introduction

The following three reports can be set to generate automatically:
**Note:** There are a number of ways these reports can be scheduled to generate automatically. For examples, refer to ***Configuring Report Scheduling*** (on page 39-65).

| Report type | Purpose |
|---|---|
| Evacuation Report (referred to as an 'Auto-Evacuation' Report) | Used in emergency type situations, (e.g. fire evacuation). |
| Exception Report | Used mostly for information purposes, (e.g. doors currently unlocked which were scheduled to be secure). |
| Activity Report | Used mostly for information purposes, (e.g. alarms occurring over the last 8 hours). |

These reports are supported by macros so they can be generated automatically when a specific system event occurs, (e.g. a fire alarm in the case of an Evacuation Report). They are triggered by an event or alarm. To achieve automatic generation of one of these reports, a macro which executes the report must be able to be initiated from an Action Plan. Using the macro scheduling feature, these reports can be set up to run automatically on a scheduled basis, (e.g. every 8 hours at a shift change, to present to the next guard).
**Note:** These reports can only print to printers that are on the same domain as the server. To print from a workstation, the workstation user needs privileges to that printer. See ***Configuring Printers for Reports automatically generated via Macros*** (on page 39-71) for further detail.

When a macro initiates one of these reports, and the report is configured to send the report to "Print Preview", the report will fail as there is no operator to view the print preview or to send the report to a printer. When a macro initiates a report, and the report is configured to send the report to a file on a local drive, the report is placed on the Command Centre Server's local drive rather than the local drive of the operator running the macro. This is due to there not always being an operator currently logged on and hence the local workstation drive may not be available.

When an automatically generated report is triggered by an alarm, if the server is offline at the time, the report will be produced once the server comes back online. However, if the report is included in a scheduled macro, after one minute the action will be cancelled and the report will not be produced.

### Auto-Generated Report Events

When an automatically generated report is run, an event is generated indicating it has run. Also receiving a "Report Completed" event indicates that the report has been spooled to the printer. If this event is **not** generated, it may be because the printer setup is incorrect.

If printing fails it will be for one of the following reasons:

| Reason | Result |
|---|---|
| The report description is configured with an unknown printer | An alarm will generate with details of the unknown printer. |
| The printer is offline or out of paper | An event will not generate, as Command Centre will not know. |

# Configuring Report Scheduling

## Introduction

Activity, Cardholder, Exception and Evacuation Reports can be set to generate automatically. There are a number of ways report scheduling can be configured, as the following two examples demonstrate.

**Example 1:**
An Evacuation Report is usually produced in an emergency situation. We recommend that an Action Plan be set up on the Door's Emergency Release input so that an alarm is created when the input is turned on. One way to automatically produce the Evacuation Report when the Doors Emergency release is turned on, is to add a macro to the Action Plan, where the macro's action is to print a report to a certain location.

**Example 2:**
A Schedule can be set up instructing a Virtual Output to switch on at a certain time or date. When the output switches on it uses an Action Plan which will run a macro, where the macro's action is to produce the report, (i.e. if you set up the Schedule to turn the output on every 8 hours at shift change, a report will be automatically produced every 8 hours).

Example 2 has been expanded with more detail, and is split into three parts, in the order they should be performed:

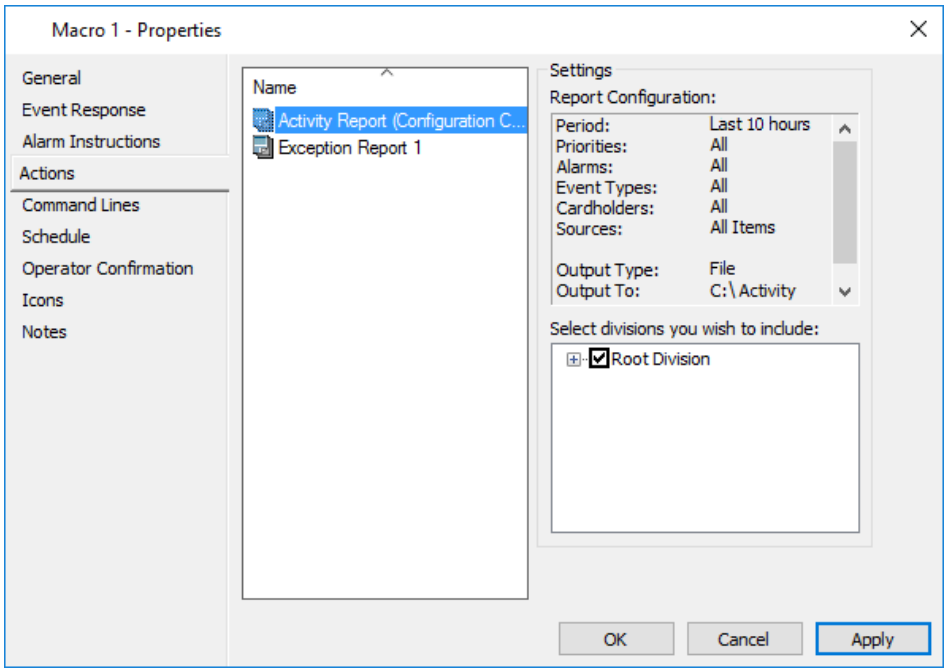
- Configuring a Macro for a Report
- Configuring Report scheduling options
- Configuring Report Macro triggers

When necessary, this procedure refers to separate step-by-step procedures that are detailed elsewhere in this online help.

## Example 2

### *Configuring a Macro for a Report*

1. Create a new macro, or modify an existing macro from the **Macro** List Window.
   Refer to Creating a new Macro for the generic procedure for creating macros, or **right click** on an existing macro and select **Properties**.
2. Click the **Actions** tab.
3. Drag the Report you require for scheduling from the **Report Description** List Window, and drop it into the **Name** grid.
4. Click on the Report in the **Name** grid.
   The settings that have been saved for the report display in a **Settings** panel to the right of the **Name** grid.




**Notes:**

- The report 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 and Cardholder Reports, a **Select divisions you wish to include** grid displays also. You need to select the report in the **Name** grid in order for its Division to be selected automatically.

5. Click the **Schedule** tab.
6. One or more entries can be added for one-off report scheduling. Refer to Scheduling a Macro for the procedure.
7. Click the **OK** button to save the Macro.

### *Configuring Report scheduling options*

8. Configure Day Categories and Default Calendar as necessary. Refer to Adding a new day category and Viewing/Editing the Default Calendar for the procedures.
9. Create a new Schedule. Refer to Creating a new Schedule for the procedure.
10. Add the Day Category(s) appropriate for the type of schedule you are configuring, as indicated below:

| For a ... | then add the... |
|---|---|
| **Daily** based schedule, (e.g. every day at 8am and 4pm) | Day Categories covering every day, (e.g. Weekday and Weekend). |

| For a ... | then add the... |
|---|---|
| **Day of the week** based schedule, (e.g. every Monday at 8am and 4pm) | Day Category representing Monday. |
| **Days of the week** based schedule, (e.g. every Monday to Friday at 8am and 4pm) | Day Categories covering from Monday to Friday, (e.g. Weekday). |

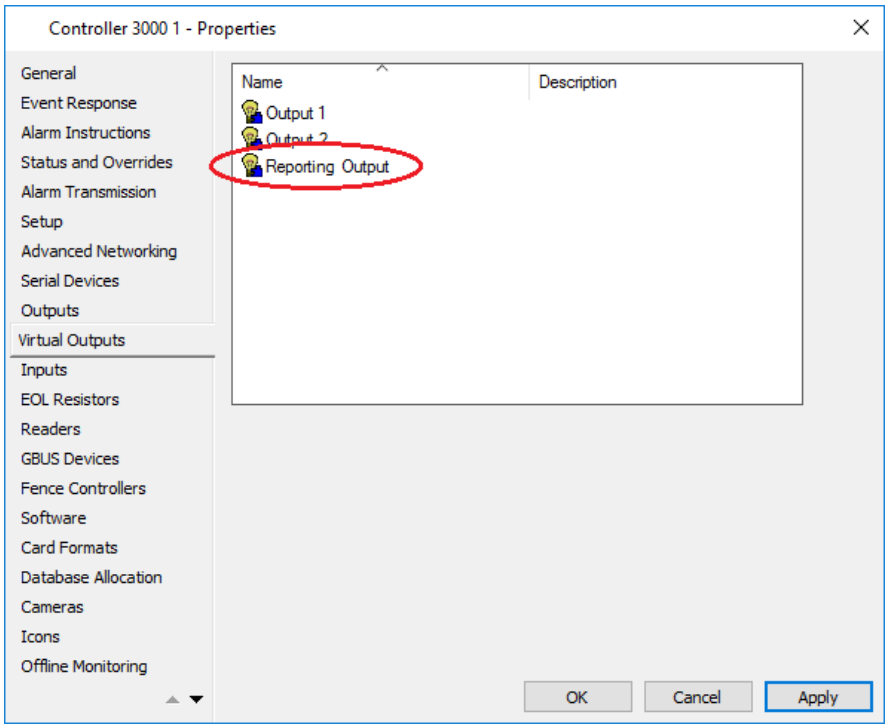
11. Click the **OK** button to save the Schedule.

### *Configuring Report macro triggers*

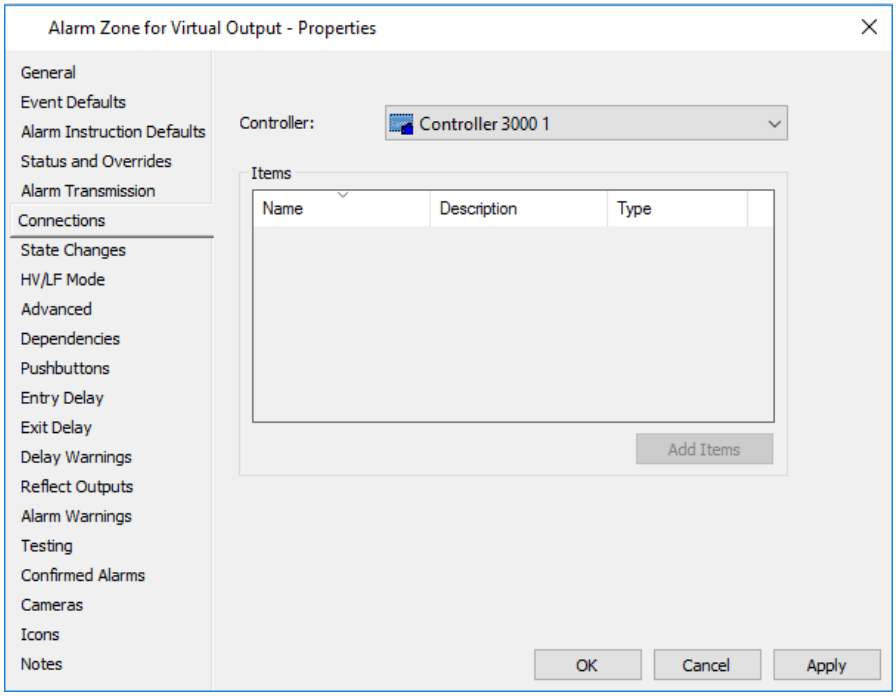
The steps involved in configuring report macro triggers include the following:

a) Configuring an Event Trigger, (i.e. a Virtual Output)
b) Linking the Virtual Output to the Controller
c) Creating an Alarm Zone specifically for the Virtual Output
d) Configuring an Action Plan

12. Configure the event trigger by creating a new Virtual Output.
    **Note:** For repeating report scheduling, it is recommended to use Virtual Outputs as triggers when the Output's state changes, such as from **OFF** to **ON**.
    Refer to ***Creating Inputs and Outputs*** (on page 21-44) for the generic procedure for creating Outputs.
13. Click the **OK** button to save the Virtual Output.
14. From the **Hardware** List Window, open the Controller that the Virtual Output is to be linked to.
15. Click the **Virtual Outputs** tab.
16. Drag the Virtual Output (already configured at Step 12) and drop it into the grid.



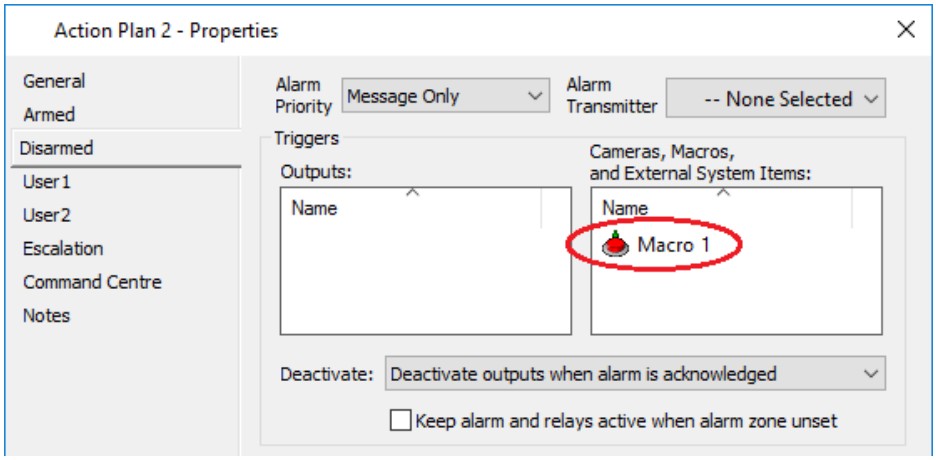

17. Click the **OK** button to save the change to the Controller.
18. Create a new Alarm Zone specifically for the Virtual Output.
    **Note:** Minimal configuration is needed as this is not a 'real' zone.
19. Click the **Connections** tab.
20. Select the Controller that the Virtual Output has been linked to from the **Controller** drop-down list.



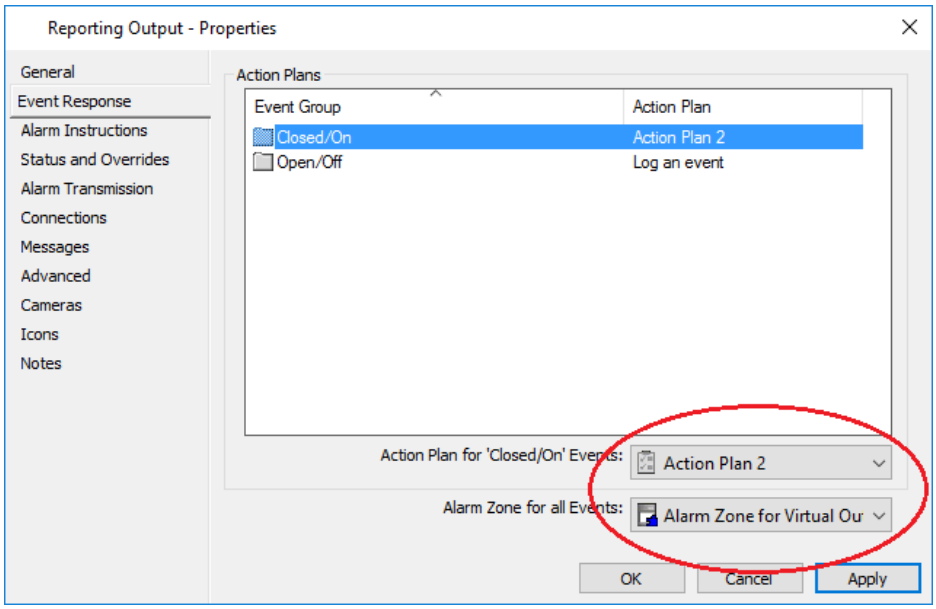

21. Click the **OK** button to save the Alarm Zone.
22. Create a new Action Plan, or modify an existing Action Plan from the

**Action Plan** List Window.
Refer to Creating a new Action Plan for the generic procedure for creating Action Plans, or **right click** on an existing Action Plan and select **Properties**.

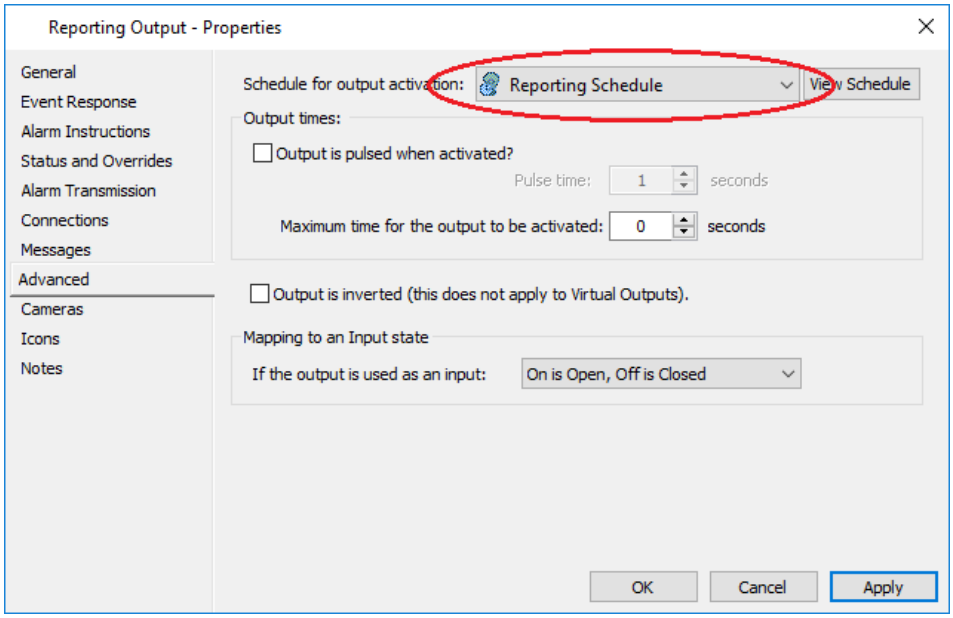
23. Click the appropriate tab that represents the status of the Alarm Zone.
The **Disarmed** tab is selected on the example screen below.
24. Drag the reporting macro (already configured in Step 1) into the **Cameras, Macros, and External System Items** grid.




25. Click the **OK** button to save the Action Plan.
26. Re-open the Virtual Output created in Step 12.
27. Click the **Event Response** tab.
28. Select the Event Group “Closed/On”, and change its Action Plan to the one configured in Step 22 above.
This will trigger the Report Macro to run when the Output state changes from **OFF** to **ON**.
29. Select the **Alarm Zone** (already created in Step 18) from the drop-down list.



30. Click the **Advanced** tab.
31. Select the reporting Schedule (already configured at Step 9), from the **Schedule for output activation** drop-down list.




32. Click the **OK** button to save the changes to the Virtual Output.

## Configuring Printers for Reports automatically generated via Macros

### Introduction

The issues surrounding printing scheduled reports using macros will depend on the type of printer being used (local or network) and the operating system the FT Command Centre service is running on.
**Important details to know:**

- Network printers are only installed for the logged on user, unless deployed machine wide.
- Macros are run from the Command Centre server, even if started from a workstation.
- Macros are run using the logon user account configured for the FT Command Centre service.
- If the report is to be configured from the workstation, the same printer will need to be installed on the workstation and server. Otherwise the printer will not be able to be selected from the report drop down list on the workstation.
- Authentication could also become an issue. The User Account configured as the logon for the FT Command Centre service will need print rights on the shared printer.

This is why a report may print successfully when run manually, (from the Command Centre report properties, which is run under the logged on user). To resolve these issues, follow one of the procedures below appropriate for your operating system:

### METHOD 1

To install a network printer machine wide, deploy the printer using Rundll32, PrintUI.dll function as follows:

1. Log on to the Command Centre server.
2. Open a command prompt, run as an administrator, and enter:

   RUNDLL32 PRINTUI.DLL,PrintUIEntry /ga
   /n\\Server_name\Printer_sharename
3. The Command Centre Server will need to be restarted as the printer is installed at login.
4. When the server has restarted, check to see the new printer is installed by opening a command prompt and entering:

   RUNDLL32 PRINTUI.DLL,PrintUIEntry /ge

Create and configure the Report (see ***Creating a new report*** on page 39-2) and Macro (see ***Creating a new Macro*** on page 20-2).

**METHOD 2**

The logon account that the FT Command Centre service runs under needs to be changed to a local user or administrator account.

1. From the **Start** menu, click **Run…**, and type in services.msc
2. Double-click the FT Command Centre Service.
   The FT Command Centre Service Properties window displays.
3. Click the **Log On** tab, and select the **This account** radio button.
4. Either click the **Browse…** button to locate the account name, or type in the account name, and enter the password for this account.
5. Click the **Apply** button.
   **Note:** The service needs to be restarted to take effect.

**Note:** These steps will need to be repeated if Command Centre is upgraded again, as the FT Command Centre service logon will revert to the Local System account each time Command Centre is upgraded.

Now that the service has been changed the printer needs to be installed for this user. This can be done by either:

- logging in as the user and installing the network printer, or
- installing the network printer as a local printer.
  **Note:** Local printers are installed for all users, not just the logged in user.

To install a network printer as a local printer:

1. From the **Start** menu, click **Printers and Faxes**.
2. Click **File** from the menu bar, then **Add Printer**.
   The Welcome screen of the "Add Printer Wizard" displays.
3. Click the **Next** button.
4. Click the **Local printer attached to this computer** radio button, and then uncheck the **Automatically detect and install my Plug and Play printer** option under it.
5. Click the **Next** button.
6. Click the **Create a new port** radio button.
7. From the **Type of port** drop-down list select either:
   - **Local Port** if the printer is shared from another machine on the network, (i.e. \\XP_workstation_name\Printer_share_name), or
   - **Standard TCP/IP Port** if the printer is a true network printer with an IP address, (i.e. 192.168.1.200).
8. Continue with the printer install as normal, selecting the printer drivers, a name for the printer, printing defaults, etc.

Create and configure the Report (see ***Creating a new report*** on page 39-2) and Macro (see ***Creating a new Macro*** on page 20-2).

## Printing an existing report

### Introduction

Once a report has been created and saved, it is displayed within the **Report Description** List Window. At any time you can select this report and print it out, providing you have the correct operator privileges. This will depend on the operator who originally created the report, and what division they are in.

### Procedure

- Click **Report** from the menu bar, then **Report Descriptions**.
  The **Report Description** List Window opens (in grid view).
- Highlight the **required report**.
- **Right click** and select **Properties**.
- Click the **Next** button on each screen until you get to the "Report Generation and Saving" screen.
- Click the radio button beside **Printer**.
6. Select the required printer from the drop-down list of available printers.
7. Click the **Setup Printer...** button if you need to set information about the printer, (e.g. paper size, or printing more than one page on a single sheet of paper). See ***Customising Report Printouts*** (on page 39-75) if you require further detail.
   Once printer settings are made, click the **OK** button to return to the "Report Generation and Saving" screen.
8. Click the **Next** button.
   The Report prints to the printer indicated.
9. Click the **Finish** button to return to the **Report Description** List Window.

### Result

The report is printed.
Depending on the settings when the report was created, the report may print to one of the following destinations:

- to the screen
- a hardcopy is printed
- to a file

**Hints**

- An alternative method to print is via the (right click) Properties option. Step through the wizard until the "Report Saving" screen displays. This method enables you to make any necessary changes to the report.

  If a specific selected printer is not available, the report is directed to the default printer.

  If the default printer is not available, the report is directed to the print preview (on screen).
- When the report is saved to file, the file can be opened using Microsoft Excel or Access. This enables various sorting and data Extraction tools to be used, such as Excels Data, Filter, Auto Filter or Access Queries.

## Customising Report Printouts

### Introduction

Printer settings can be altered, depending on the printer you are using, to customise how a report will print out, (e.g. paper orientation, double-sided printing, multiple pages per sheet, etc.). This can be achieved for both new reports and reports that have already been created and saved.

The following example provides instructions for how to alter your printer settings so that a report will print multiple pages on one sheet of paper (to reduce the amount of paper used).

***EXAMPLE: Printing multiple pages per sheet***

### Procedure

1. Click **Report** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
2. Either:
   - select an already saved report, or
   - **right click** and select **New**, and then the required report type.
3. Using the **Next** and **Back** buttons, step through the report wizard choosing appropriate report settings on each screen until you get to the "Report Generation and Saving" screen.
4. Click the radio button beside **Printer**.
5. Select the required printer from the drop-down list of available printers.
6. Click the **Setup Printer...** button.
   The **Print Setup** screen displays.
7. Click the radio button for the orientation you require, (i.e. Portrait or Landscape).
8. Click the **Properties** button.
   By default the **Paper/Output** tab of the Printer properties displays.
9. If you want the report to be printed double-sided, (i.e. on both sides of each sheet of paper), select "2-Sided Print" from the **2-Sided Print** drop-down.
10. Click the **Layout/Watermark** tab and select the required number of pages per sheet from the options under **Pages Per Sheet (N-Up)**.
11. Click the **OK** button.
    The **Print Setup** screen re-displays.
12. Click the **OK** button.

The "Report Generation and Saving" screen re-displays.

13. Click the **Save Report** button if you wish to save this report.
    **Note:**
    Ignore this step if you are re-running an already saved report, as the **Save Report** button is disabled.
14. Click the **Next** button.
    The Report prints to the printer indicated.
15. Click the **Finish** button to return to the **Report Description** List Window.

**Result**

The report is printed.
**Important:**
Any deviation from the above procedure can cause the report to return to the default settings, and not print as you expected. For example:

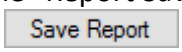
- If you do Steps 1-13, and then exit, when you do re-run the report, it will use the default settings, (i.e. single-sided and one page per sheet).
- If you do everything, but at Step 4 you click the **Print Preview** radio button instead of the **Printer** radio button, again, the report will run using the default settings.

## Editing settings of an existing report

### Introduction

Once a report has been created, it displays within the **Report Description** List Window. You can edit these reports at any stage. For example, you may want to extend the reported time period within an existing Activity report.

### Procedure

1. Click **Report** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
2. Highlight the required report.
3. **Right click** and select **Properties**.
   The report wizard displays.
4. Using the **Next** and **Back** keys, step through the different wizard screens. Where appropriate, edit the setting(s).
5. Step through the wizard to the "Report Saving" screen.
   Click the **Save Report** button 

   to ensure the settings you changed are saved.

### Result

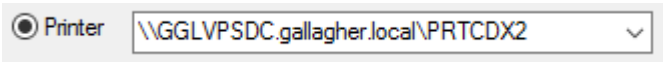
The changes you made to the report are saved.

# The Report Print Preview window

## Introduction

Some reports have been set up to print to screen. This enables you to preview the report - try before you buy.
Once you have viewed the report you have the option to print it.

Staying within the **Report Preview** window you can print the report. It is sent to the default printer, as set within the following field:

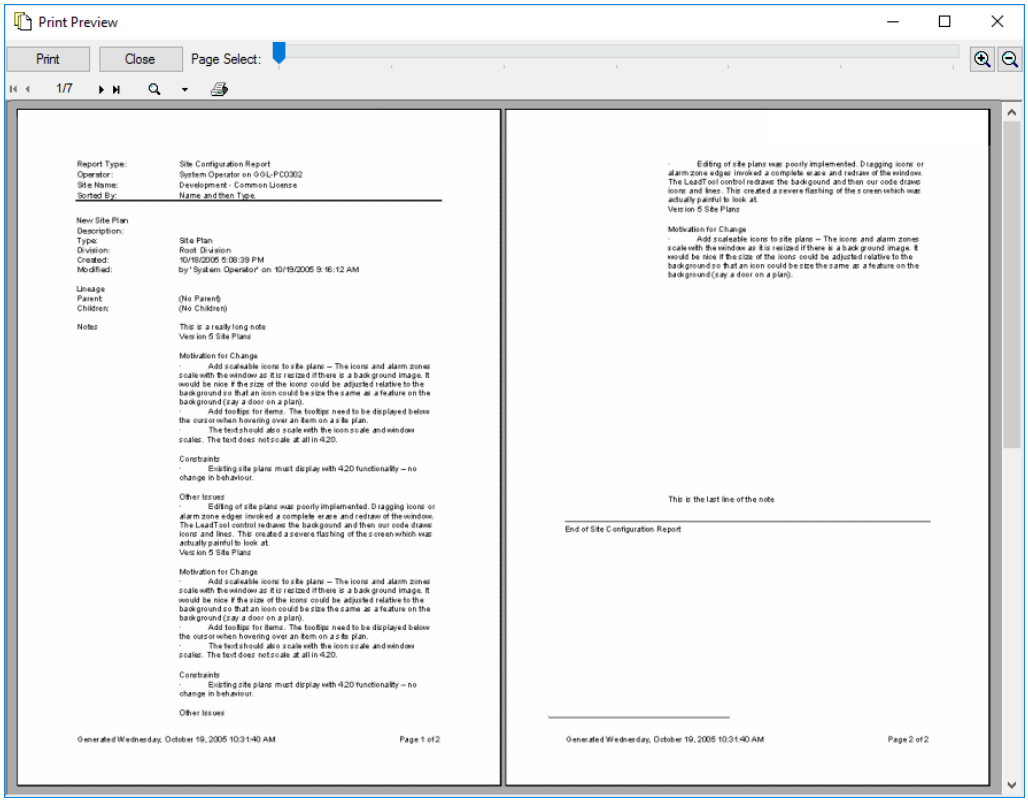



## Procedure

1. Click **Report** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
2. From the displayed list **select, and print a report** that you know will **print to screen**. The description field (within the **Reports Description** List Window) may indicate the report is printed to the screen.

## Result

The report is generated and displays within the Report Print Preview window:

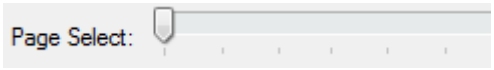


### *Viewing specific pages*

When the report is generated, the first page of the report displays on screen. There are a number of ways to view other pages in a report, as follows:

- Use the navigation arrows 

(First page, Previous page, Next page and Last page) to move through the report.
- The Page Select indicator enables you to select different pages to view. The Page markers represent the different pages within the report.
  - Move the mouse pointer to the appropriate page marker.
  - Click the mouse button to display this selected page.

  *For example:*
  To display Page 3 of the report, click on the Page Select indicator as shown below.
  

- Use the vertical scroll bar to move forward and backward through the report.

### *Magnifying glass*

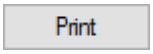
The Magnifying glass  switches the display between the entire page and 100%. Clicking the arrow displays a drop-down menu offering some further sizing options to enable you to enlarge or reduce the size of the text displayed within the Print Preview window.

### *Printing your report*

The report looks good and contains all the information you want.
You can now print out the report.

You can print either from within the Print Preview window, or you can close the Print Preview window, return to the report wizard and print from there. Use one of the following methods:

Either:

1. Click **Print** 

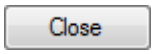
   The Report prints to the default printer. The Print Preview window closes and you return to the Report wizard.

Or:

1. Click the  button.
2. Check /alter any printer settings, including the printer that the report will print to.

3. Click the **OK** button.

Or:

1. Click **Close** 

2. Click the **Back** button to step back to the Report Generation and Saving screen. Check/alter any printer settings.
3. Select the **Printer** radio button.
4. Click the **Next** button.
5. Click the **Finish** button.

### *Closing without printing*

When you have viewed your report you can close the Print Preview window without printing the actual report.

1. Click the **Close** button.
2. Click the **Finish** button.

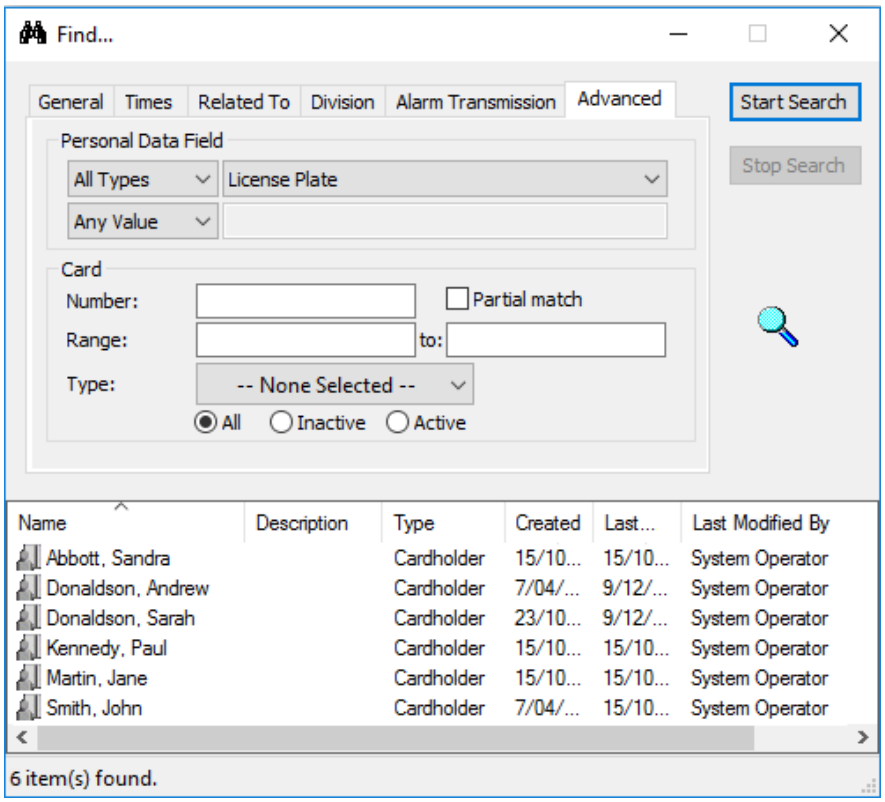
# Advanced Reports

## Introduction

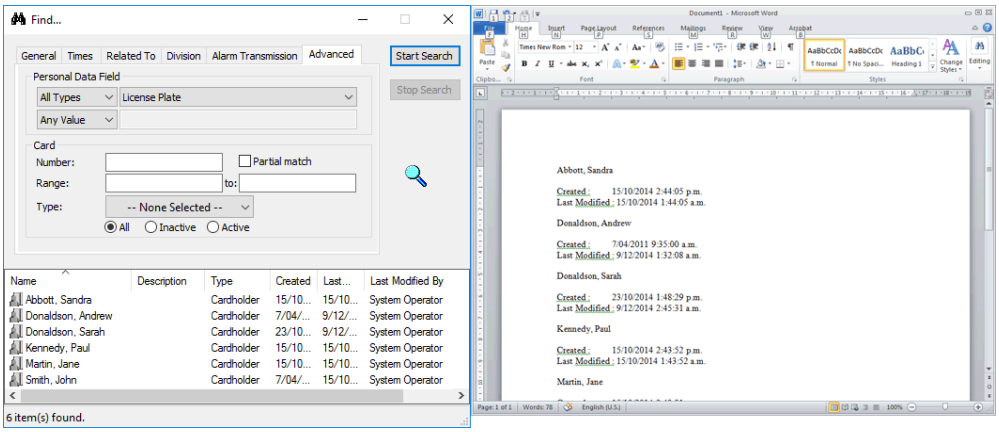
Command Centre can perform advanced reports. You can find items and "drag and drop" them into another application for fast, adhoc reports. Reports can also be generated in a more conventional way through Report Wizard. Refer to ***Creating a new report*** (on page 39-2).

## Procedure

1. Using the **Find** Tool search for any group of items. Refer to "Find" for details on using the Find Tool.
   **Note:** These can be any entities within the Command Centre environment.

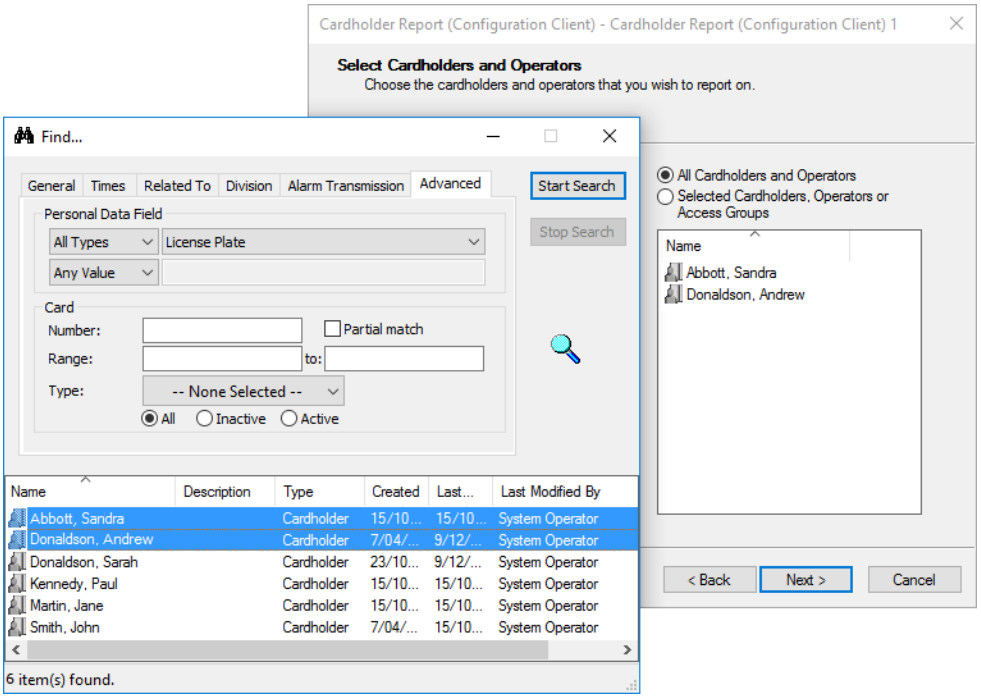



2. Select the items you require and "drag and drop" them into Microsoft Word. This displays data about the entities in a Word file.




**Note:** When creating a report in the conventional manner, using the "Report Wizards" (see ***Creating a new report*** on page 39-2), you can also use "drag and drop".

3. On the Report Wizard screen titled "Select Cardholders and Operators", (i.e. the screen that allows you to select the items to be included in the report), you can "drag and drop" entities (in the below example, Cardholders), from the **Find** window directly in the selection panel in the report wizard.



# Chapter 40: Archives, Backups and Restores

This chapter details the archiving process, and the backup and restoring process.

Operators must have the correct operator privileges to perform these functions.

## Archives

Every event that appears in the Event window gets logged in the Event database (CCFTEvent). As a way of keeping the size of the Event database down, the Archiver manipulates the data in the Event database and stores it in a number of files, (i.e. one per day), in the location the user specified. After an archive, events from the period specified are removed from the Events database.

The archived data is restored when an operator runs an Activity report that covers a period in which the data only resides in archive files, otherwise the data is retrieved from the Event database.

The Archiver has three main responsibilities:

1. Copy and/or move activity from the online database into external files.
2. Recover space by removing archived activity from the online database.
3. Retrieve archived activity from external files when needed for a report.

**Notes:**

- If an Archive and Backup are required, perform the Archive before the Backup.
- Because reporting from archived data can be slow, it is recommended that you keep data on which you want to report within the event database, and only archive the data which you do not report on regularly.

## Backups/Restores

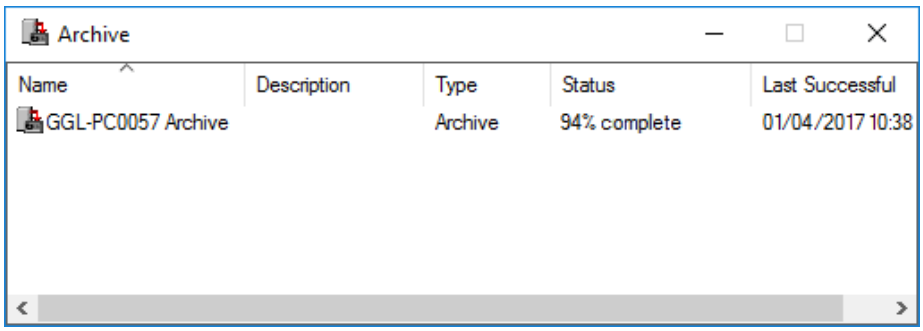
The Backup/Restore process records the state of the sites setup (CCFTCentral) at a single point in time, (i.e. when the backup is launched). After a backup, the system will behave as normal and a restore should only be required if something happens to your system.

**Backups:**
You can backup the systems working data to a file. The system can be backed up while it is online and operators are logged in.

**Restores:**
You can restore the working system from a backup file record.

## Archive List Window

The **Archive** List Window opens in grid view.




This window displays the status of an archive. If an archive is running, then it displays the percentage complete. If the last archive was stopped or failed, or the archive cannot start, then it displays the reason, otherwise it displays nothing.

# Configuring Archives

## Introduction

All archive configuration is performed from the Archive property pages. The properties mandatory to configuring an archive are the archive paths and user account. Those properties are covered in the first eight steps of this procedure, while the remaining steps are optional parameters.

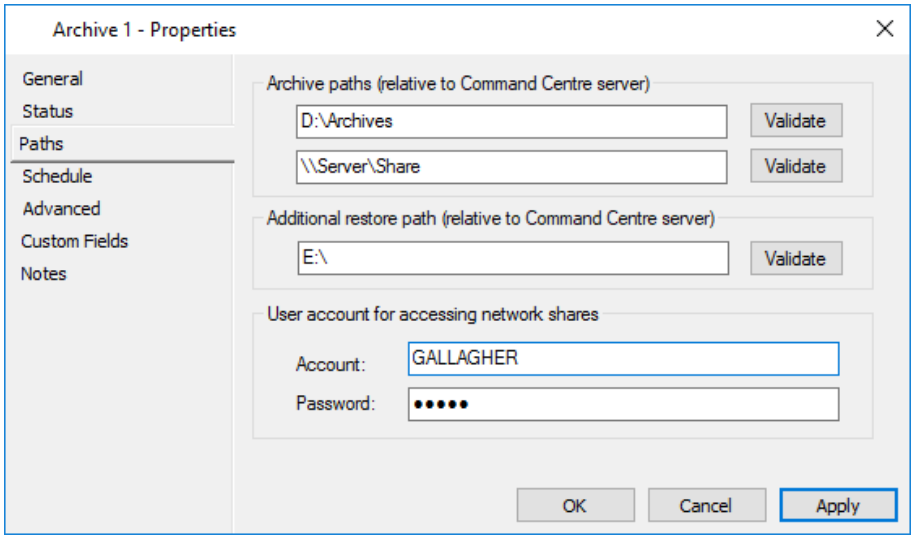
This procedure describes how to configure an Archive. To perform this procedure you must have the "View Site", "Configure Site" and "Backup and Archive" operator privileges. Note that the "Configure Site" operator privilege is only given to high level administrators.

If you wish to configure an archive that removes data from the database without archiving the events you need the "Advanced User" operator privilege. Note that the "Advanced User" operator privilege is only allocated to extremely high level administrators.

**Note:** The system only allows one archive to be configured.

## Procedure

1. Click **File** from the menu bar, then **Archives**.
   The **Archive** List Window opens (in grid view).
2. **Right click** and select **New...Archive**.
   By default the **General** tab displays.
3. Complete the fields as required.
   For further detail see ***General tab*** (on page 3-18).
   **Notes:**
   - The Division you select here will determine who will be able to see the archive.
   - All data for all Divisions is always archived. You cannot archive individual Divisions data separately.
4. Click the **Paths** tab.
   This tab allows you to specify a server's archive and restore locations.




The fields on this tab are described below:

| Field | Description |
|---|---|
| Archive paths | These specify the paths to which archive files will be written. All archive files will be written to both locations. Always ensure the 'relative to Command Centre server' is appropriate. Maximum length = 260 characters. **Note:** The Archive paths require "Network Service" permissions to write. |
| Additional restore path | The system searches the current archive paths for archive files when reporting on archived activity. This allows an additional path to be specified which will be searched for archive files when reporting, but will not be written to, (e.g. a CD-ROM drive). Maximum length = 260 characters. |
| User account for accessing network shares | The name and password of the user account to use when accessing archive and restore locations on network shares. If this is left blank, the archive and restore locations will be accessed using the logon account the FT Command Centre Service has been configured to use (Local System account by default). Maximum = 50 characters. |

The **Validate** buttons check that the archive or restore location can be accessed by the server.

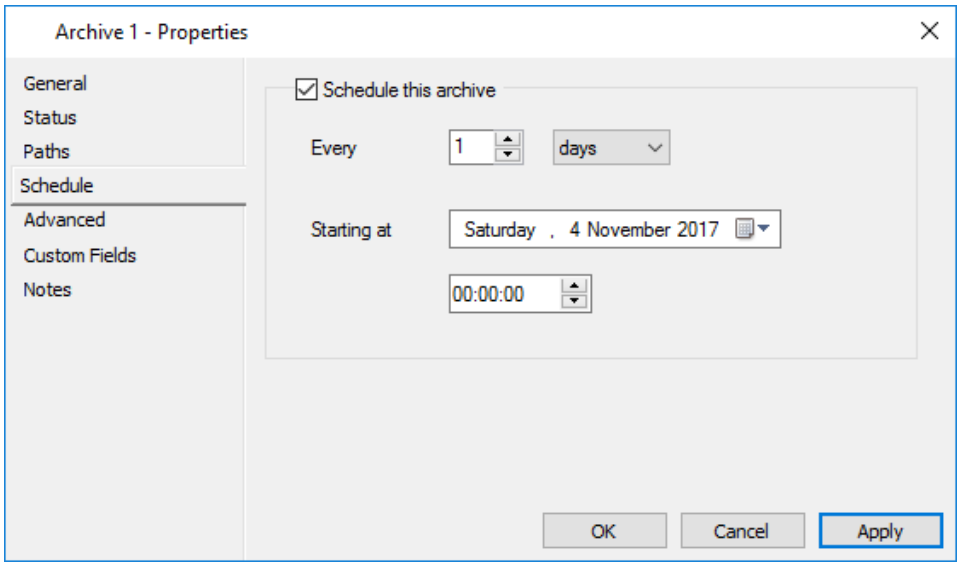
**Note:** You may receive the following error message when restoring files:
*"Connection to the specified path <pathname> has failed. Please check:*
- *you have entered the path correctly*
- *the Archiver User Account has the appropriate permissions to use this network resource."*

If you do, you should check the User Account on this tab has sufficient privileges.

5. Do you want to schedule this archive so it happens automatically?

| If... | then go to... |
|---|---|
| yes | Step 9. |
| no | Step 8. |

6. Click the **Schedule** tab.
This tab allows you to specify a simple repeating schedule for automated archives.




7. Check the **Schedule this archive** checkbox to enable automated archives.
**Note:** The other fields on this tab are disabled until this checkbox is checked. (Default = Off)

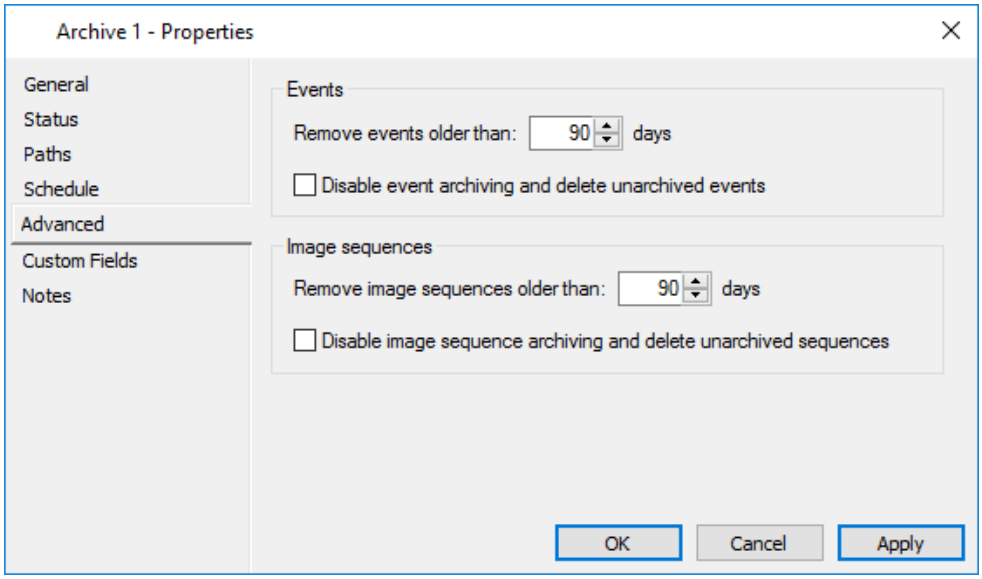
The fields on this tab are described below:

| Field | Description |
|---|---|
| Every [count] [units] | Specifies the interval between the start of each scheduled archive. The count can be between 1 and 99, and the units can be minutes, hours, days or weeks.<br>Therefore the minimum is 1 minute and the maximum is 99 weeks.<br>(Default = 1 day) |
| Starting at [date] [time] | This specifies when the repeating schedule will start.<br>Default = Midnight of day after Archive item's creation date. |

**Note:** The archive schedule (start time and interval) is specified in local time relative to the central server. This means the interval between archives can vary if it crosses a daylight savings transition.

*Example:*
If an archive is scheduled to occur every 6 hours from midnight. Archives will occur at midnight, 6am, midday and 6pm local time, even if there is only 5 hours between midnight and 6am due to a daylight savings transition.

8. Click the **Advanced** tab.
This tab allows you to specify if the data will be archived and how much will be kept online (in the database).




| Field/Checkbox | Description |
|---|---|
| Remove events older than:<br>AND<br>Remove image sequences older than: | The archive process ARCHIVES all unarchived event/images and then removes events/images older than xxxx days. Unarchived events/images are NOT removed.<br>The minimum is 0 days and the maximum is 9999 days.<br>(Default = 90 days) |
| Disable event archiving and delete unarchived events<br>AND<br>Disable image sequence archiving and delete unarchived sequences | The archive process DELETES all (archived/unarchived) events/images that are more than xxxx days old.<br>The minimum is 0 megabytes and the maximum is 999,999 megabytes.<br>The "Advanced User" operator privilege is required to make this field active.<br>(Default = unticked) |

**IMPORTANT:**
We do not recommend the disabling of event/image archiving. It may be useful if you do not want to keep or report on data older than xxxx days.

UTC date standards determine what data is to be removed from the database. Calculating 90 days using standard time may vary by a day.
0 days removes all data
1 day removes todays data
90 days converts standard time to UTC time and removes all data 90 days and older

| | **Events & Images 'Archive Enabled'** | **Events & Images 'Archive Disabled'** | **Events 'Archive Enabled' Images 'Archive Disabled'** | **Events 'Archive disabled' Images 'Archive Enabled'** |
|---|---|---|---|---|
| **Events newer than xx days** | Archived | No Archive | Archived | No Archive |
| **Events older than xx days** | Archived and removed | No Archive and removed | Archived and removed | No Archive and removed |
| **Images newer than xx days** | Archived | No Archive | No Archive | Archived |
| **Images older than xx days** | Archived and removed | No Archive and removed | No Archive and removed | Archived and removed |

9. Click the **Custom Fields** tab if you want to add and assign a custom field value to this archive.
   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 archive.
    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 Archive item has been configured.

## Performing Archives

### Introduction

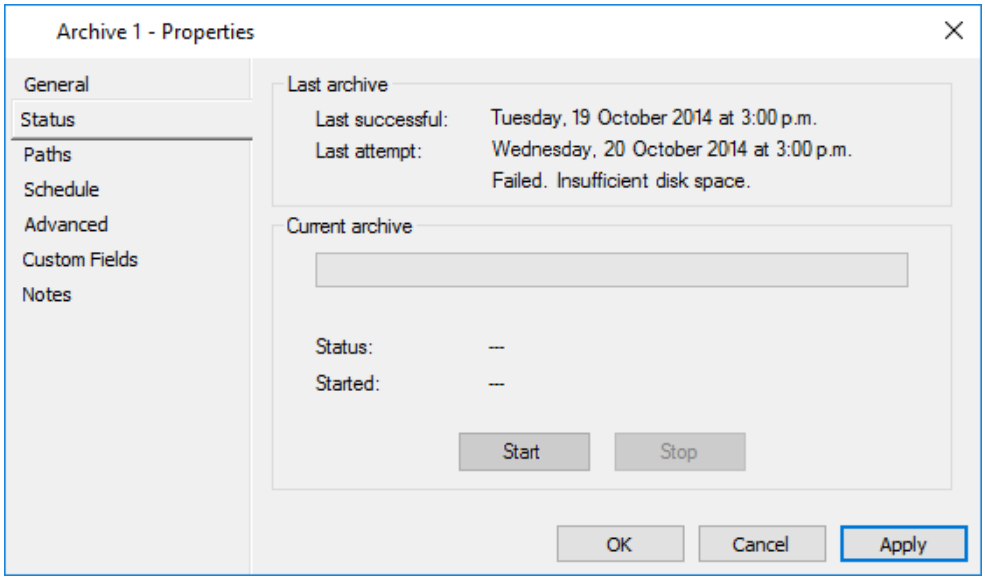
At least one archive path must be configured before an archive can be started. Archives can be started manually or automatically by setting a schedule. This procedure covers a manual archive. For detail on setting a schedule for an automated archive, refer to ***Configuring Archives*** (on page 40-3).

To perform this procedure you must have the "View Site" and "Backup and Archive" operator privileges. Having these privileges will allow you to run an archive, but you will not be able to configure or alter an archive.

### Procedure

1. Click **File** from the menu bar, then **Archives**.
   The **Archive** List Window opens (in grid view).
2. Highlight the Archive item you want to run.
3. **Right click** the mouse button.
4. Click **Properties**.

   **Note:** Alternatively, you can click **Start Archive**. While a "percentage complete" figure will display in the "Status" column on the list window, this method does not provide enough detail about the progress of the archive.
5. Click the **Status** tab.

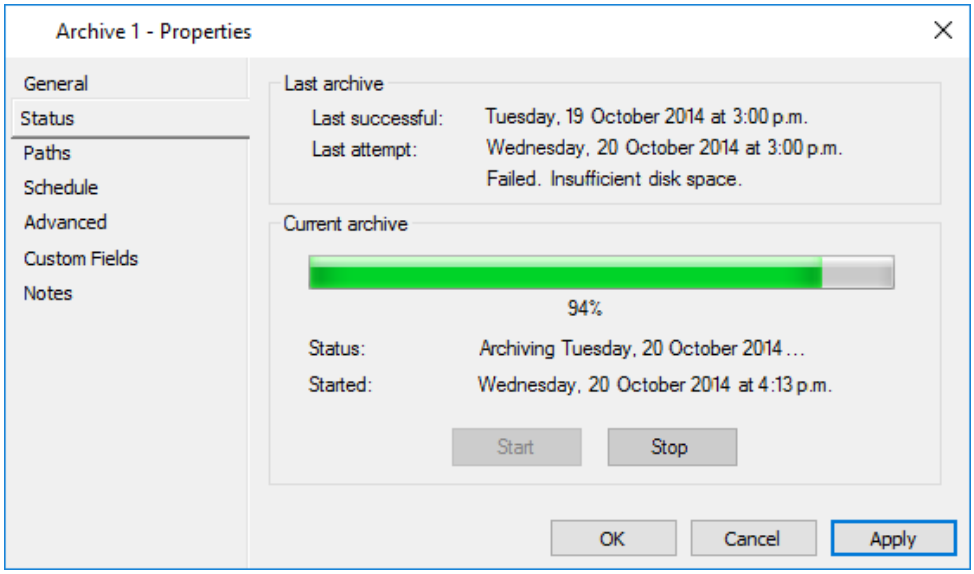



The **Last archive** section of this tab displays the results of the last archive, and the **Current archive** section will remain empty if an archive is not currently running.

The fields in the **Last archive** section are described next:

| Field | Description |
|---|---|
| Last successful: | The time the last successful archive started. |
| Last attempt: | The time the last attempted archive started.<br>If the last attempted archive succeeded, this will be the same as 'Last successful'. The result of the last archive attempt will also be displayed, (e.g. 'Success', 'Stopped by operator', 'Insufficient disk space' or 'Server offline'). |

6. Click the **Start** button to start an archive.
   **Note:** If the **Start** button is disabled, it will be for one of the following reasons:
   - the archive item has not been configured, (i.e. it does not have a server and at least one archive path),
   - an archive is already in progress, or
   - the server is offline.




The progress bar indicates the progress of the archive, and the fields in the **Current archive** section are now populated as described below:

| Field | Description |
|---|---|
| Status: | Describes what the archiver is currently doing, (e.g. searching for data to archive, compacting database, etc.). This will usually include the day that is currently being archived. |
| Started: | The time the current archive started. |

**Note:** Once the archive has completed, it is a good time to perform a Backup, however not absolutely necessary. Refer to ***Performing Backups*** (on page 40-14) for procedure.

**Result**

An Archive is complete, and archive files are stored in the destination(s) specified.

**Hints**

*Stopping an Archive*
An archive can be stopped while it is running, either by:
- clicking the **Stop** button on the **Status** tab, or by
- right clicking on the Archive in the list window, and clicking **Stop Archive** from the drop-down menu.

When an archive is stopped, any incomplete archive files will be deleted.

*Archive failures*
If the Archiver is unable to complete an archive for any reason, (e.g. lack of disk space, or SQL Server is shut down), then the archive will stop and the archive files will be removed from the archive file index (if necessary), and deleted. If the archive files cannot be removed from the archive file index then they will not be deleted.

# Restoring Archives

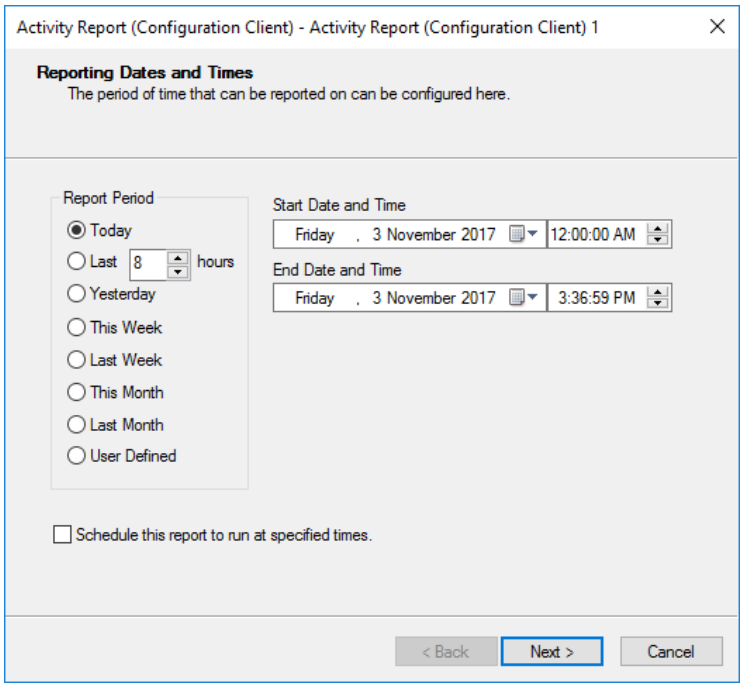
## Introduction

Most of the archive configuration also applies to the restore. The archive paths are also restore paths, and the same user account will be used to access restore paths on network shares. The only restore-specific property is the additional restore path on the **Paths** tab. This allows a site to specify another path that is searched for archive files.

Restores are started automatically whenever an event requires activity that has been archived and removed from the Event database.

## Procedure

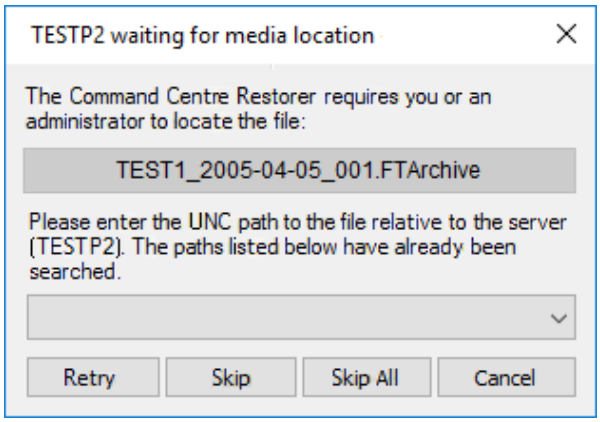
1. Click **Report** from the menu bar, then **Report Descriptions**.
   The **Report Description** List Window opens (in grid view).
2. **Right click** and select **New...Activity Report**.
   The first screen ('Reporting Dates and Times' screen) of the wizard displays.




3. Specify the report period as appropriate for the archive you wish to restore.
4. Step through each of the wizard screens, following the instructions displayed and clicking the **Next** and **Back** buttons.
   When the report generates, (i.e. after you click the **Next** button on the 'Report Generation and Saving' screen), a dialog box displays.
5. Enter the location of the archive files for that period, and click the **OK** button.

**Result**

The events are loaded into the Restored database (CCFTRestored) and are included if they are relevant, then deleted after the report is generated to maintain free disk space.
**Note:** If the restorer can not find an archive file in any of the restore paths, the following screen displays:




You have several options, as follows:

1. Retry the operation by clicking the **Retry** button.
2. Specify a new restore location.
3. Skip the missing file by clicking the **Skip** button.
   The Restorer will add a missing file entry to the report output and will move on to the next file.
4. Skip all missing files by clicking the **Skip All** button.
   This has the same result as clicking the Skip button for this file and all subsequent missing files.

If there is more than one server with missing files, then you may be presented with several **Restorer waiting for media location** screens, (i.e. one for each server).

**Hint**

*Stopping a Restore*
A restore can be stopped by cancelling the search which initiated the restore, (e.g. by cancelling the report or stopping the Find Tool).

*Restoring from a remote workstation*
If you are a user on a remote workstation, (i.e. in a different city to the server), a number of scenarios may occur when you try to restore the archive by running an Activity Report.

Take the appropriate action indicated next:

| If... | then... |
|---|---|
| at report generation you receive a request for an archive file | contact the system administrator where the server is, to get them to place the archive files in the server PC. |
| the files are on DVD | type in the DVD drive letter. |
| the files are on a network drive | specify the drive letter of the mapped network drive.<br>**Note:** All paths are referenced from the Command Centre server PC and not the workstation PC. |

## Performing Backups

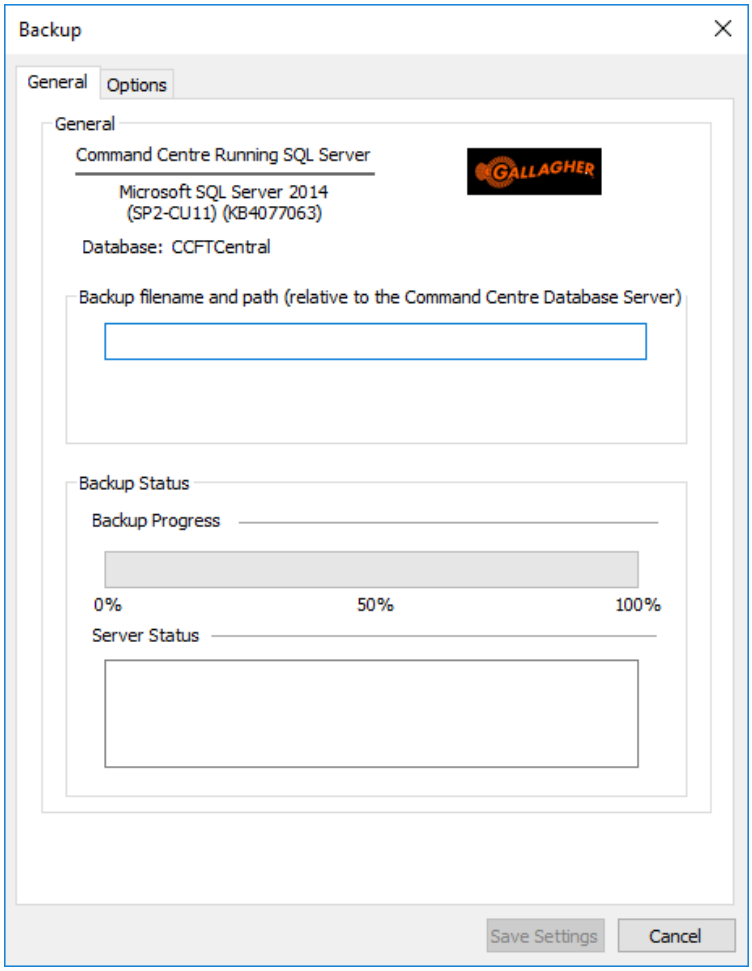
### Introduction

SQL Server performs the backups of Command Centre. Therefore in order to get SQL Server to write to the destination you specify, and for the backup to succeed, you have to run the SQL Server service under the account of a user who has permission to do so.

If your workstation is remote, then the path you specify is relative to the SQL Server machine and not your local machine.

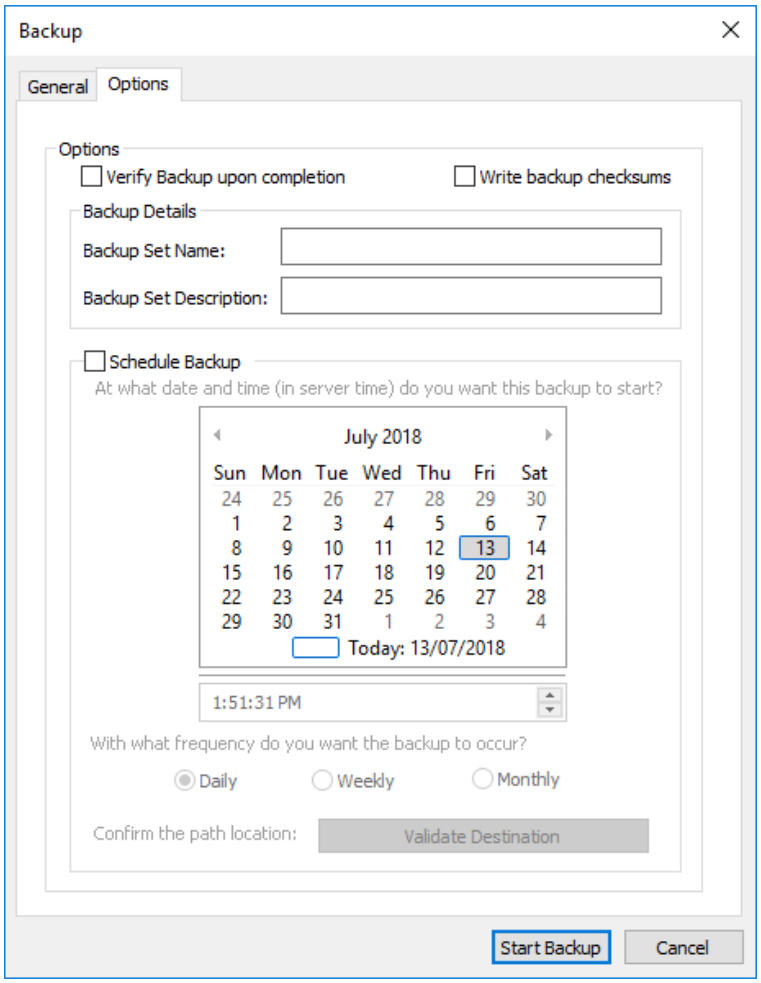
### Procedure

1. Click **File** from the menu bar, then **Backup**.
   By default the **General** tab of the Backup window displays.




2. Enter the backup destination, (i.e. both the path and the file name), in the **Backup filename and path** field.
   As you begin entering details in this field the **Save Settings** button is enabled.

3. If you require the Backup filename and path to be saved, click the **Save Settings** button.
4. Click the **Options** tab.




5. Check the **Verify Backup upon completion** box if required.
   **Note:**
   Although not required, verifying a backup checks that the backup is intact physically, and that you can rely on your backup in the event you need to use it. Verifying a backup involves:
   - Checking the backup set to ensure that all files have been written.
   - Checking to ensure that the files in the backup are readable.

   Verifying a backup does not check that the structure of the data contained within the backup set is correct. For example, although the backup set may have been written correctly, it may be possible for some type of database integrity problem to be present within the database files that comprise the backup set. To verify the structure of the data before creating a backup, you can perform database consistency checks.
6. Sometimes database integrity problems can occur with the database files that comprise a backup set. To verify the structure of the data, check the **Write backup checksums** box.

7. Type in a Backup Set Name and Description as appropriate.

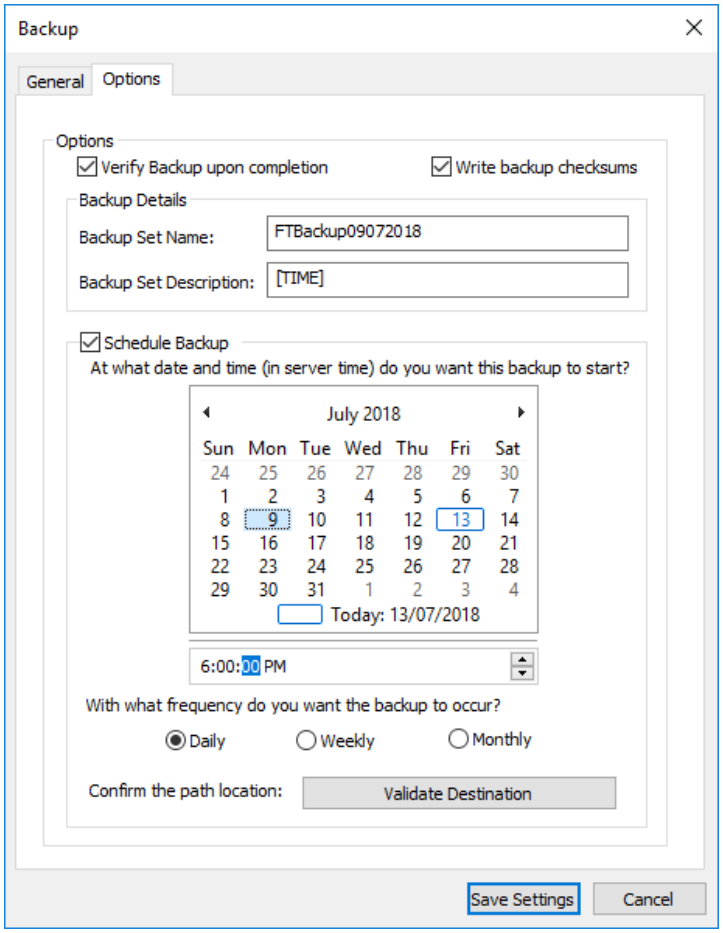
| Field | Description |
|---|---|
| Backup Set Name | This identifies a unit of backup work. |
| Backup Set Description | This provides descriptive or identifying text for the result of a backup operation.<br>**Note:**<br>If you type [TIME] in the Backup Set Description field the actual server date and time will replace it when the backup is created. |

**Note:**
These fields are embedded in the actual .FTBackup file. When browsing for a backup set (.FTBackup file) using the CCFTRestore program, these names and descriptions appear at the bottom of the browse window, allowing a user to identify a backup even if the file itself has been renamed.

8. Do you wish to run the backup now or schedule it on a regular basis?

| If you want to... | then... |
|---|---|
| run the backup now | Click the **Start Backup** button.<br>The **General** tab re-displays and shows the progress of the backup. When the backup is complete the message "Backup Successful!" displays in the **Server Status** field.<br><br>Close the Backup window. |
| schedule the backup on a regular basis | go to Step 9. |

9. Check the **Schedule Backup** box.




10. Select the 'Start date' for your backup from the calendar, by using the ◂▸ keys to select the month, then clicking on the day of the month.
11. Adjust the time of day you want the backup to occur as appropriate.
12. Click the appropriate radio button for how often you want the backup to occur.

| If you select... | then a backup will occur... |
|---|---|
| Daily | at the time you indicated each day. |
| Weekly | on the day of the week you selected as the 'Start date' on the calendar, (e.g. in the previous screen example, the 19th August was selected, which is a Monday. Therefore, a backup would always occur on a Monday). |
| Monthly | on the date selected as the 'Start date' on the calendar, (e.g. in the previous screen example, the 19th August was selected, therefore a backup would always occur on the 19th of the month).<br>**Note:** If you select a day which does not occur in every month, (e.g. Day 31), the backup will occur on the final day of those months. |

**Note:**
The date specified is the first time the backup will occur, (e.g. a day six months in the future could be specified for backups to start). If a date/time that has passed was specified, the backup would take a 'best guess' as to when the backup was intended to occur, (e.g. if the 9th August 2002 was selected with a monthly schedule, and today's date is the 22nd August 2002, then the backup would advance the first backup time to the 9th September 2002).

13. Click the **Validate Destination** button to confirm the path you have entered. An error message will display if you have entered an incorrect file path.
14. Click the **Save Settings** button.
15. Close the Backup window.

**Result**

A backup is either run or scheduled to run on a regular basis.

## Restoring Backups

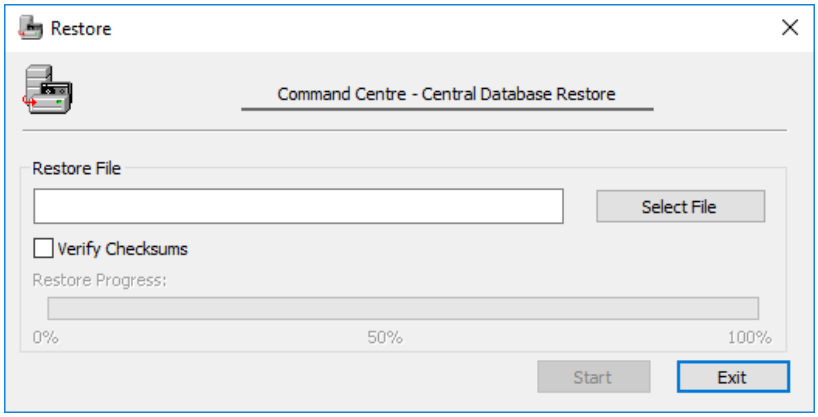
### Introduction

This procedure enables you to restore the working system from a backup file record, therefore a backup must already have been performed. See ***Performing Backups*** (on page 40-14) for the procedure.
**IMPORTANT:** If you are restoring a backup to another machine you will need the Database Recovery Code, otherwise you will be prevented from restoring your database.
**Notes:**

- If you have performed a backup over the network, the backup should be copied to a non-network drive before restoring. A restore can only be performed on the Server.
- Some of the screen shots in this topic may differ depending on your operating system.
- The procedure below describes one method for restoring backups. Alternatively, you could **double-click** on a backup file OR Restore from the Service Manager Utility.
- The Gallagher Command Centre CA certificate is copied from the Gallagher Database into the Trusted Root certificate store for New Installs, Upgrades and when the Recovery tool is used. The Gallagher Command Centre CA certificate is used for Mobile Client authentication and can be safely removed if the Mobile Client is not utilised on site.

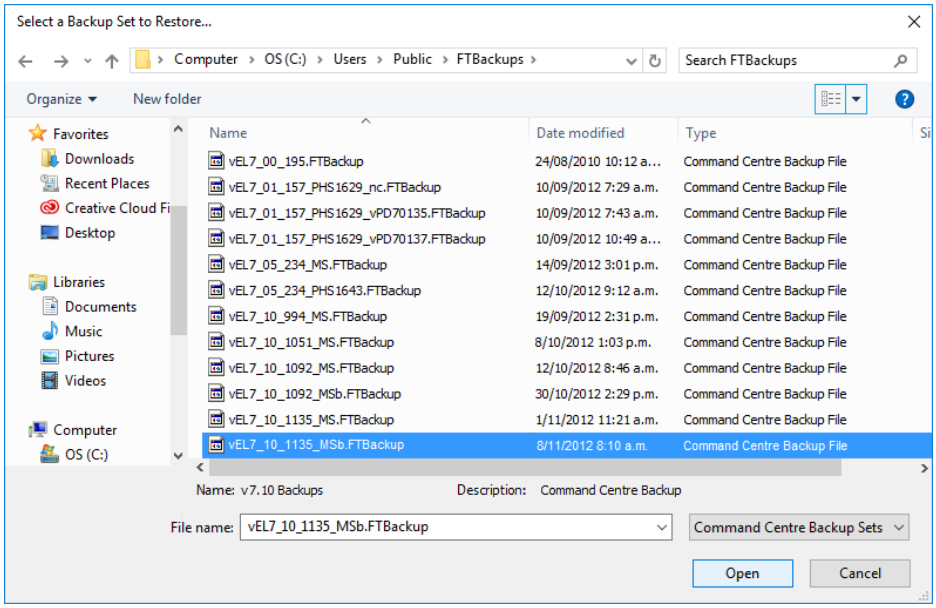
### Procedure

1. From the **Start** menu, click **Programs**, then **Gallagher**.
2. Click **Command Centre Restore**.
   The Restore window displays.




3. Click the **Select File** button.
4. From the displayed pop-up window, path your way to the backup file you wish to use for the restore.

**Note:**
The names you entered in the **Backup Set Name** and **Backup Set Description** fields when you performed a backup appear at the bottom of the browse window, allowing you to identify a backup even if the file itself has been renamed.




5. Click the **Open** button.
   The file path and name display in the **Restore File** field, and the **Start** button control is enabled.
   The restore utility requires exclusive access to the CCFT Central database and needs to shut down the following FT services to allow this:
   - FT Command Centre Service
   - FT Controller Service
   - FT Bootstrap Protocol Service
   - FT Import - Export Service
   - FT Intercom Service
   - FT Visitor Management Service

6. If 'Write backup checksums' was selected when the backup was performed, check the **Verify Checksums** box.

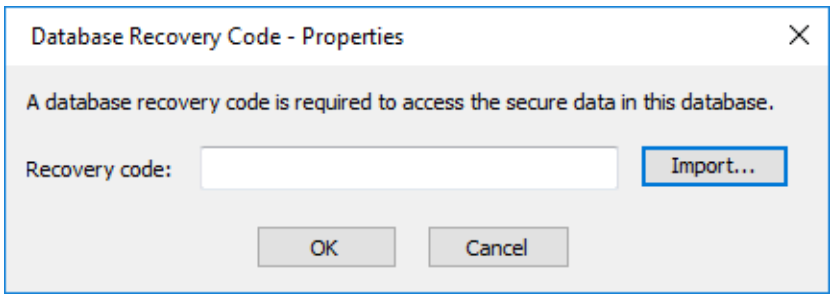
   **Note:** If you check the **Verify Checksums** box and 'Write backup checksums' was NOT selected at the time of the backup, an error message will display to indicate the backup file does not contain checksum information. If this occurs, deselecting **Verify Checksums** will let you continue with the restore.

7. Click the **Start** button.
   A message displays indicating that the Services need to be stopped.

8. Click the **Yes** button.
   The Restore starts. When the Restore Progress bar reaches 100% the Restore is complete, and a pop-up message *"The Restore has Completed. Do you want to restart the Command Centre Services?"* displays.

9. Click the **Yes** button.
   Once the FT Services have restarted, another pop-up message *"Restore completed successfully!"* displays.

   **Note:** At the end of the restore the code checks to see if it can work with the database. If it can't (probably due to it being a database backup from another system), the following dialog displays to prompt for the corresponding recovery code (for the source database):




10. Click the **OK** button, then the **Exit** button.

**Result**

A restore of a backup file is complete.

**Hint**

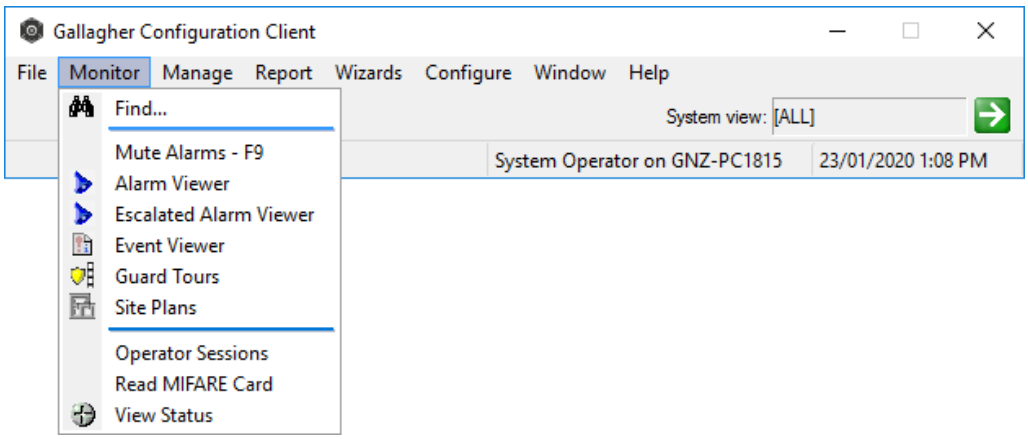
*Restore from Windows Explorer*
An alternative method of restoring a backup is to double-click on the **.FTBackup** file from Windows Explorer on the Server machine.
The Restore window displays, and you complete the previous procedure described, with the exception of selecting the Backup file, as the name is already displayed in the **Database File Location (From)** field.

# Part 4: Site Monitoring

It is the role of the Operator, who is often a security guard, to monitor events and alarms that occur on a system. Operators are very seldom required to perform configuration.

This part of the User Guide provides details on how to perform the functions required for monitoring 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 **Monitor** option on the Command Centre main menu bar.




**Note:**
Depending on your operator privileges or your current system view, some of the menu items referred to may not be visible to you. For example, the "Escalated Alarm Window" (for this item to display you must belong to an Operator Group that has the escalated alarm window option enabled).

# Chapter 41: Find Tool

## Introduction

Using the Find tool, you can locate items within Command Centre. Each of the tabs make it easier to fully define your search criteria.
**Note:** An extra **Alarm Transmission** tab will also be available if your site is licensed for the ContactID feature.

The Find function defines the search as per the settings within each of the tabs. The search results will only include items which meet all the conditions set across all the tabs.

When you have defined your search criteria, ensure any tabs you do not want to use are "blank" - that is, they do not contain previous search criteria data.

**Note:** Pressing **F3** on your keyboard brings up a new **Find** tool window, except if an Alarm Details window is open.

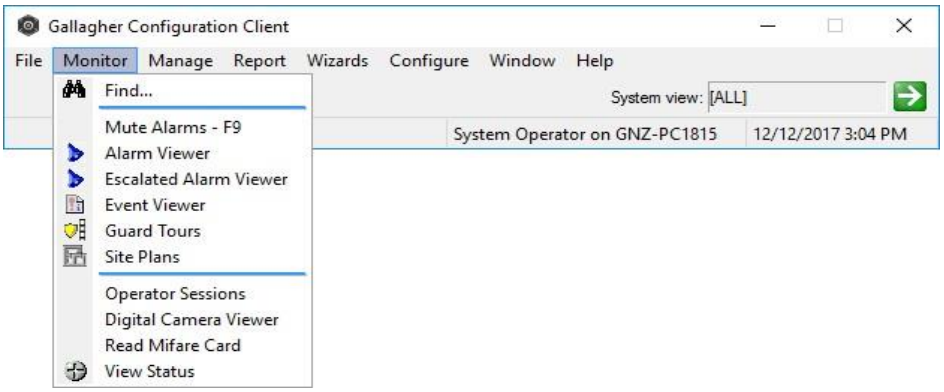
# Using the Find Tool

## Introduction

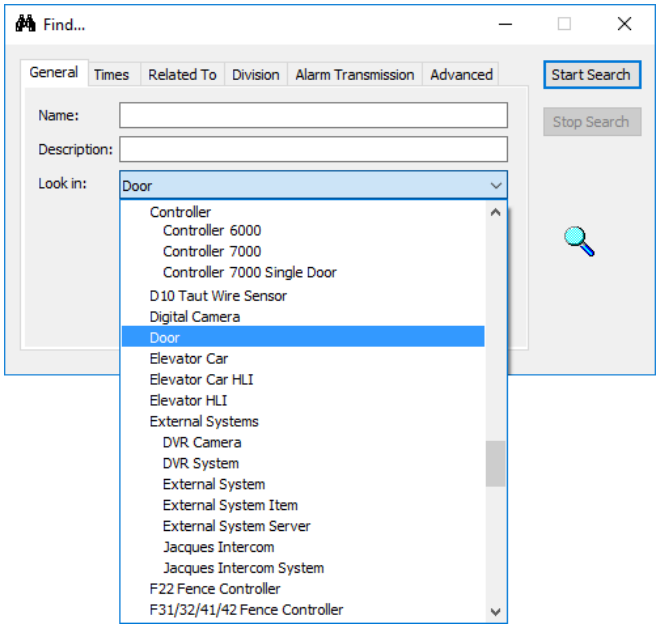
Use the following procedure to search for an item in Command Centre, using the Find Tool.

## Procedure

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

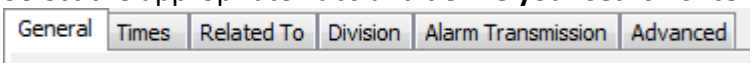



2. Enter text in the **Name** and/or **Description** fields to help define your search criteria, if required.
   **Note:** Partial text and wildcards (%) can be used. See **Hints** at the end of this topic for further detail.
3. Click within the **Look in** field.
   From the displayed drop-down menu, click which **area to search** within Command Centre.




**Note:** When searching for Controllers, you can opt to search either by the different Controller types, or for all Controllers at once.

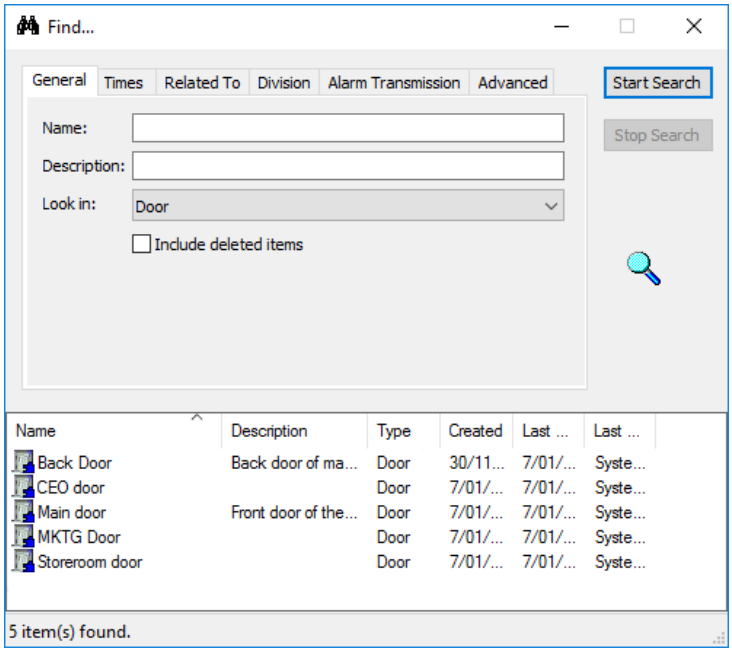
4. Check the **Include deleted items** checkbox if you want to include these in your search.
   **Note:** When this option is checked, you can then search by 'Name' or 'Description' (on the **General** tab), or by 'Created', 'Modified' or 'Deleted' time (on the **Times** tab).
5. Select the appropriate Tabs and **define your search criteria**.




6. See ***Examples*** (on page 41-5), using these tabs, to show how you can define your searches.
7. Click the **Start search** button.

## Result

Search list window opens and lists all items found.




## Hints

*Stop search*
If you click on the **Stop Search** button, those items already found remain in the displayed list. To restart the search from the beginning click the **Start Search** button.

*Partial text*
The Command Centre system will automatically search on partial text entered in the **Name** and **Description** fields. The search will find matches which contain partial text searched on.
For example, if you enter Will in the **Name** field, the search results will include any "Williams" or "Willis" in the system.

*Wildcards (%)*
The percentage symbol (%) can be used as a wildcard in the **Name** and **Description** fields.
For example, if you enter partial text and include a % as a wildcard, so you have **co%er** in the **Name** field, the search results will include items with the word "controller" or "computer" in their name.
**Note:**
If you want to search for the actual symbol %, you need to enclose it in square brackets [%].

*Case sensitive*
The find search is not case sensitive. You can enter either lower-case or upper-case characters.

*Properties of search list items*
You can go straight to the Properties window of any item in the list of Search results by right clicking on an item, then selecting Properties.

## Examples

Click the example below that you require further detail on:

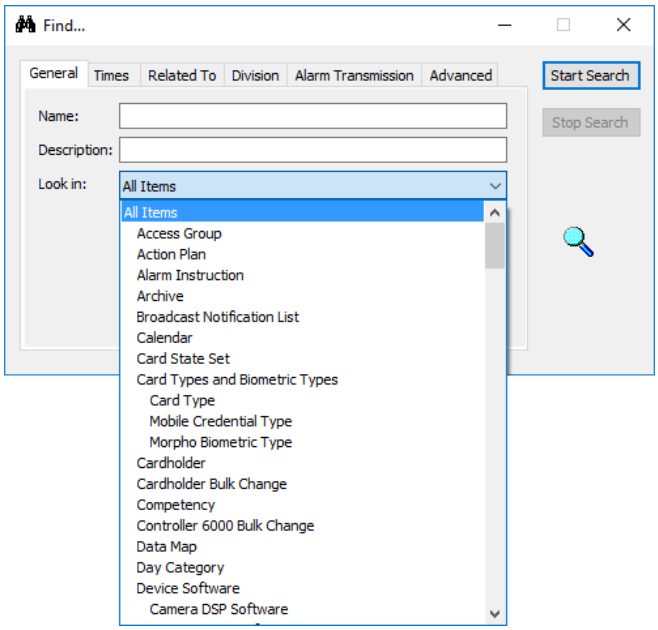

- ***Example 1: Searching using General and Time details*** (on page 41-6)
- ***Example 2: Searching using Related To details*** (on page 41-8)
- ***Example 3: Searching using Divisions*** (on page 41-9)
- ***Example 4: Advanced*** (on page 41-10)

## Example 1: Searching using General and Time details

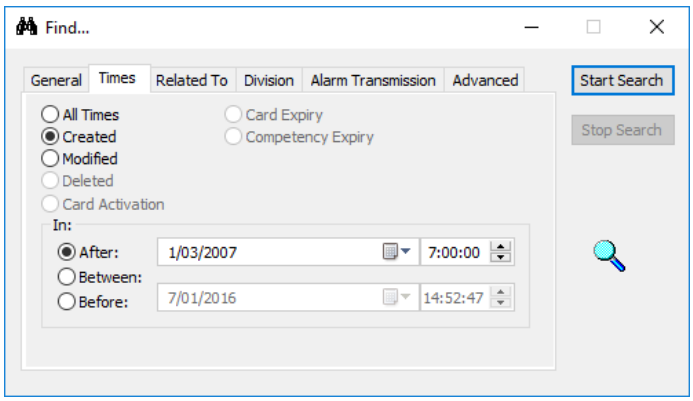
This example uses fields within the *General* and *Times* tabs to define the search.

Follow the procedure below to find **all items** that include the name **office** and that were **created after 7am on 01/03/2007**.

1. Click the **General** tab.




2. Within the Name field, type **office**.
3. Click the **Look in** field and select the option "All Items".
4. Click the **Times** tab.
   The Times tab is used to search for items based on types of events and time criteria.
   **Note:**
   In this example the **Card Activation** and **Card Expiry** radio buttons are disabled. They are only enabled for cardholder searches.




5. Select the **Created** option, then the **After** option.

6. Type in the **date** 01/03/2007 and the **time** 07:00:00.
7. Click the **Start Search** button.

The Search window opens and displays all those items that match the set search criteria.

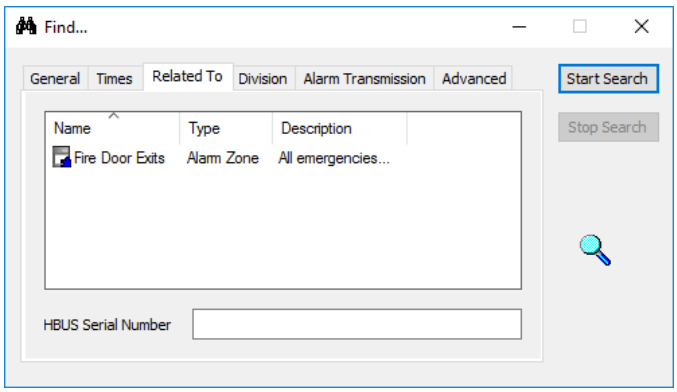
## Example 2: Searching using Related To details

This example shows how, using fields within the *General* and *Related To* tabs, you can define your search.

**Note:** To remove search criteria right click on the unwanted item and select **Remove from List**.

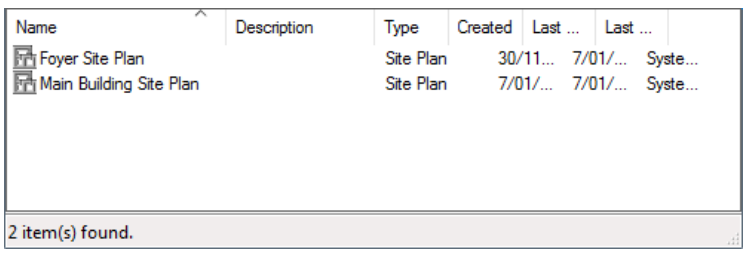
Follow the procedure below to find out which Site Plan(s) a particular Alarm Zone appears on.

1. Click the **General** tab.
2. Click the **Look In** field and select the option "Site Plan".
3. Click the **Related To** tab.
   The Related To tab searches for items in the **Look In** field on the General tab that are related to the item in this window.
4. Open the **Alarm Zone** List Window (Configure - Alarm Zones).
5. Select the relevant Alarm Zone and drag and drop it into the "Related To" window.




**Note:** The **HBUS Serial Number** field is always displayed, whether an HBUS Item type has been selected or not, and allows a search to be run based on the Serial number assigned to an HBUS Device. This search can be based on either a partial, or full, serial number. The field is limited to the maximum serial number size, and only hexadecimal characters can be entered into it, (i.e. 0-9 and A-F).

6. Click the **Start Search** button.
   The Search window opens and displays all those Site Plan(s) the Alarm Zone appears on.

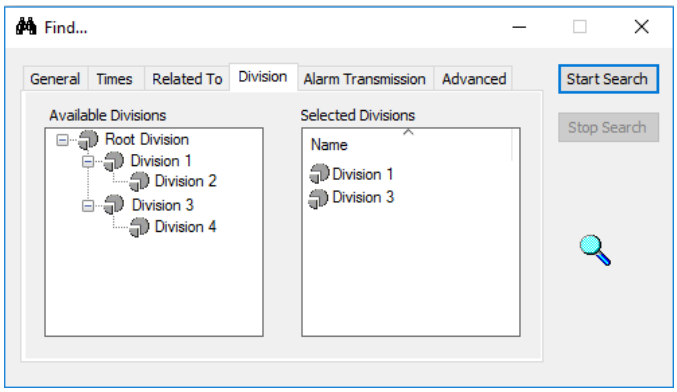


## Example 3: Searching using Divisions

The **Division** tab allows you to directly select a division in which to search. Operators can select and search within more than one division at a time. Results returned will include all information from within all selected divisions, including their associated sub-divisions.

This example shows how, using fields within the **General**, **Related To** and **Division** tabs, you can define your search.

1. Click the **General** tab.
2. Click the **Look In** field and select the option "All Items".
3. Click the **Related To** tab.
4. Open the **Operator Group** List Window (Manage - Operator Groups).
5. Select the relevant Operator Group and drag and drop it into the "Related To" window.
6. Click the **Division** tab.
   The **Available Divisions** grid includes all divisions in which the current operator can view any kind of item.
7. Select "Division 1" and "Division 3" from the **Available Divisions** grid, and drag and drop them into the **Selected Divisions** grid.




8. Click the **Start Search** button.
   All items related to the selected Operator Group, in **Division 1** or **Division 3**, or **Division 2** or **Division 4** display within the Search window.
   Items in **Division 2** and **Division 4** are included in the search result because they are sub-divisions of the divisions that were selected.

## Example 4: Advanced

The following four examples show how, using fields within the Advanced tab, you can define your search.

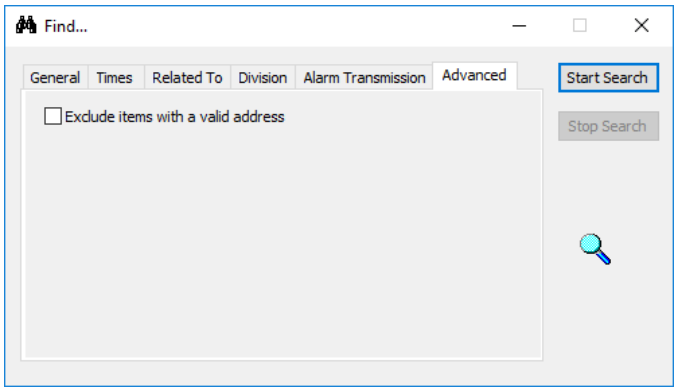
**Note:** The information displayed on the Advanced tab will vary depending on the item you select within the "Look in" field on the General tab.

For example, if within the General tab, you select "Cardholder", you are prompted to enter criteria related to cardholders. This same information would not be displayed if you selected "HBUS I/O".

### *Example 4-A*

You may want to check which HBUS I/O Interfaces within the system have not yet been configured.

1. Click the **General** tab.
2. Within the **Look in** field select "HBUS I/O".
3. Click the **Advanced** tab.
4. **Check the box** to exclude those items with a valid address.



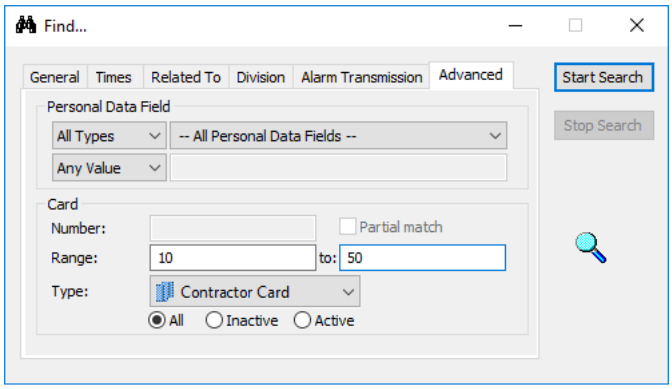

5. Click the **Start Search** button.
   Those HBUS I/O Interfaces with an invalid address display within the Search window.

### *Example 4-B*

You may want to find out which Cardholders issued with card numbers between 10 and 50 are Contractors.
**Note:**
This example would only be possible if you had a card type for "Contractor Card" set up.

1. Click the **General** tab.
2. Within the **Look in** field select "Cardholder".
3. Click the **Advanced** tab.

4. Within the **Range** field, type in the range of card numbers 10 to 50.
   **Notes:**
   - "Card Number" and "Card Range" cannot both be defined in your search. When you start to enter details in one of these fields, the other becomes disabled.
   - The **Number** field accepts wildcard characters, (e.g. %), if there is no **Type** selected or the card number format is NOT decimal.
5. From the **Type** drop-down list, select **Contractor Card**.




6. Click the appropriate radio button for the status of the card type to be included in your search.

| Option | Purpose |
|---|---|
| All | The default setting.<br>Performs a Cardholder find based on the configured parameters where the search is not limited by card enable/disable status. |
| Inactive | Performs a Cardholder find based on the configured parameters where the search will only return Cardholders with at least one inactive card. An inactive card is where:<br>a) Card is disabled, OR<br>b) Current date/time is outside the bounds of scheduled activation and expiry date/times. |
| Active | Performs a Cardholder find based on the configured parameters where the search will only return Cardholders with at least one active card. An active card is where:<br>a) Card is enabled, AND<br>b) Current date/time is between the card's activation date/time and scheduled expiry date/time. |

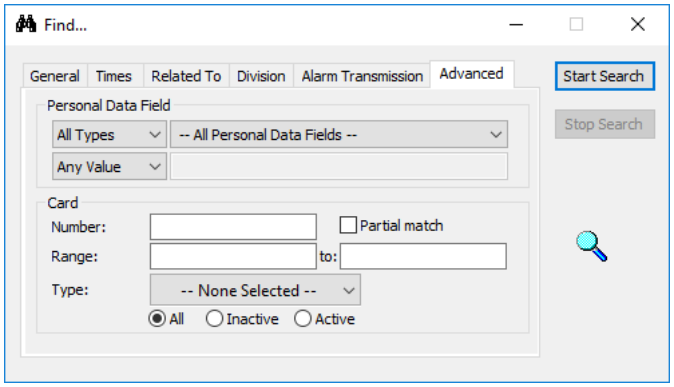
7. Click the **Start Search** button.
   All cardholders issued with Contractor cards numbered between 10 and 50 display within the Search window.

### *Example 4-C*

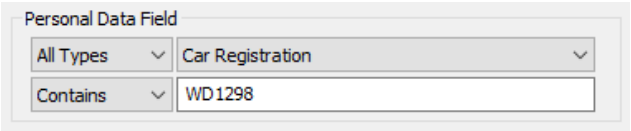
You may need to find out the owner of a car that needs to be shifted from where it is currently parked on site.

**Note:** This example would only be possible if you had a Personal Data Field (PDF) set up for car registration.

1. Click the **General** tab.
2. Within the **Look in** field select "Cardholder".
3. Click the **Advanced** tab.




4. From the **Personal Data Field** drop-down list (currently populated with **-- All Personal Data Fields --**), select "Car Registration".
5. In the field that is currently populated with **Any Value**, select "Contains" from the drop-down list.
   This enables the free-text field beside it.
6. Enter the registration number of the car that needs to be shifted in the free-text field.



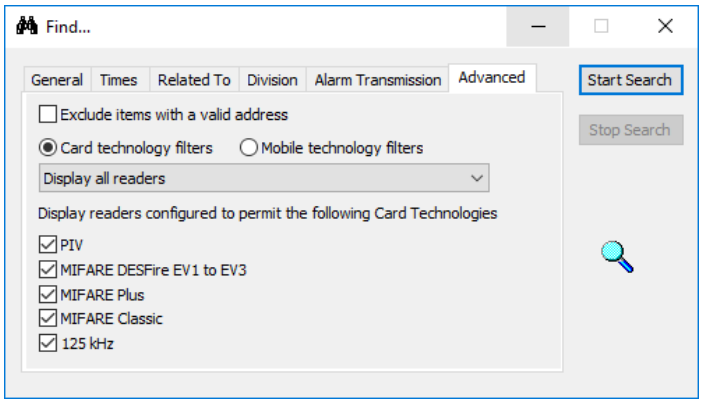

7. Click the **Start Search** button.
   The cardholder who owns the car with the entered car registration number displays within the Search window.

### *Example 4-D*

There is an option on the **Advanced** tab that allows a site to find out what card technologies Readers are using. This example demonstrates how to find out what HBUS Readers on your site are configured to accept MIFARE Classic or 125 kHz card technologies.
**Note:** Permitted Card Technology is configured on the **Advanced** tab of the readers properties.

1. Click the **General** tab.

2. Within the **Look in** field select "HBUS Reader".
   **Note:** The search will be limited to HBUS Readers. Likewise, if you selected "Cardax IV Reader", the search would be limited to Cardax IV Readers, and if you selected "Card Reader" the search would include both Cardax IV and HBUS Readers.
3. Click the **Advanced** tab.




4. Uncheck the first three options, leaving **MIFARE Classic** and **125 kHz** checked.
   The **via 125 kHz cards** checkbox becomes disabled.
5. Click the **Start Search** button.
   The HBUS Readers that are configured to allow access via MIFARE Classic or 125 kHz cards display within the Search window.

# Chapter 42: The Event and Alarm Viewers

## Introduction

The Event Viewer window enables you to view events and alarms occurring at your site.

Everything that occurs in the system, from "site configuration changes" to "overrides" to "cardholder changes", is recorded as an activity on the event log. As new activity occurs the appropriate message is displayed at the top of the window.

The event and alarm messages are displayed in a summarised format (which messages are displayed to you will depend on your privilege level):

- What happened
- Where it was generated
- Who was concerned
- When it happened and when it was logged
- The type of event

You can select an individual message and view the details about the activity. From here, and with the correct privilege level, you can also acknowledge and process alarms.

If you want to see all operator events/workstation events associated with a cardholder you need to place the workstation into a division that you have the "View Events" operator privilege for.

**Note:** An online help file listing all the event/alarm messages can be accessed via the **Help** menu bar in Command Centre, and provides explanations of what each message means.

## Scrolling through the Event Viewer

When scrolling through the Event Viewer window while new events are arriving, the Event Viewer window behaves as follows:

- If no events are selected then the Event Viewer window will return to the top when a new event arrives.
- If an event is selected then the Event Viewer window will keep its position, and will allow an operator to scroll back through the events in the window.
- If the selected event scrolls off the bottom of the Event Viewer window then it will be de-selected, causing the Event Viewer window to start showing the most recent events again.
- A selected event can be de-selected by clicking on it. Do this if you want to start displaying the most recent events again.

## Opening the Event Viewer window

### Introduction

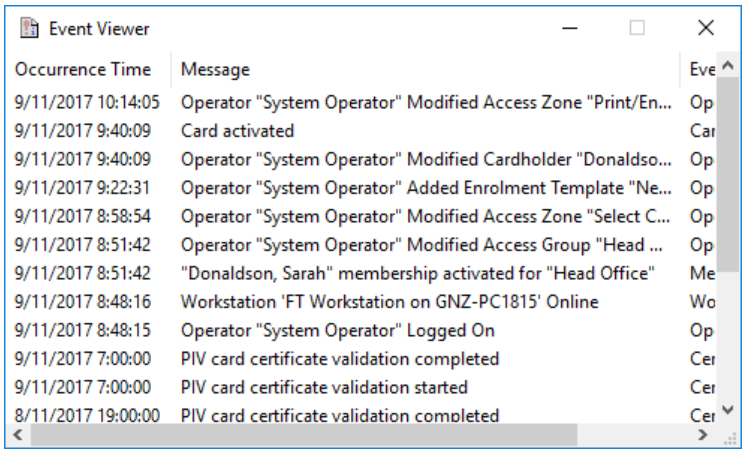
The Event Viewer window lists the activity on your site; event messages and alarm messages.

### Procedure

1. Click **Monitor** from the menu bar.
2. Click **Event Viewer**.

### Result

The Event Viewer window displays:




**Notes:**

- If you have a mouse with a scroll wheel, it is possible to scroll (up or down) one event at a time, providing the scroll bar appears at the side of the Event Viewer window.
- When the Event Viewer is resized or moved, it will remember its size and position, even if Command Centre is closed and re-opened.

### Hints

*New activity*
The Event Viewer window updates dynamically; when new activity occurs, the appropriate alarm or event message is displayed at the top of the window.

*Old activity*
The Command Centre system has a limit as to how many messages are displayed, (i.e. 500 events). However, generating an Activity report will enable you to view older activity that has occurred.

## Viewing event details

### Introduction

You may want to see more details about a particular event or alarm.

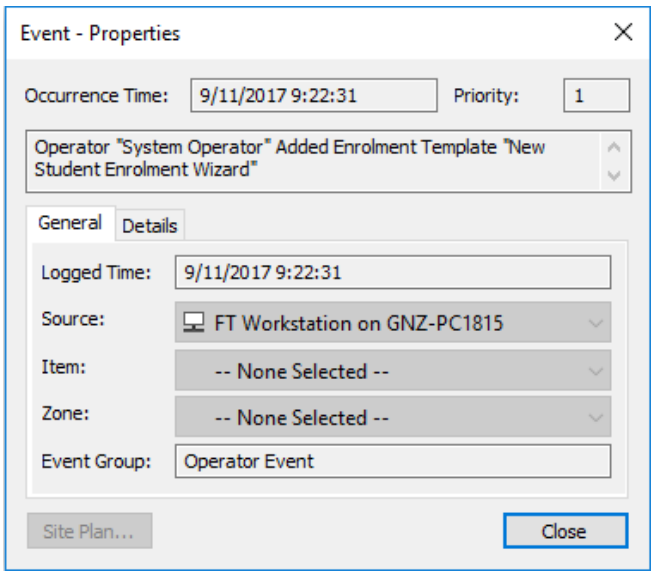
### Procedure

1. Click **Monitor** from the menu bar, then **Event Viewer**.
   The **Event Viewer** window opens.
2. Highlight the **activity message**.
3. Either:
   - **Right click** and select **Properties**.
     **Note:** If the event has associated image sequences, there will also be the option to **View** on the pop-up menu. When selected another pop-up menu displays from which you select the camera to view. The Sequence Viewer then displays.

   Or:

   - **Double-click** the event.

   If you selected an event, the **Event** Properties window opens:




   If you selected an alarm, the **Alarm** Properties window opens.
   This window is similar to the Events window but contains additional information specific to alarms. Refer to ***Viewing Alarm details*** (on page 42-11).

Site Plan...

This button will be enabled if the site item for which the event has occurred is on a Site Plan. Clicking this button will display the relevant site plan indicating the site item.

4. Click the tabs as necessary to view specific details relating to the event.

   General

   General details (who, what, where) about the selected activity message are displayed.

   Details

   Additional details regarding the activity message are displayed.

   Images

   This tab only appears on the Event Properties page if there is an image sequence associated with the event. Clicking this button will display the Sequence Viewer window.

5. Click **Close**.

**Result**

The Event Properties window closes.
You have viewed details about the event but taken no action.

## Events with Restorals

### Introduction

Events belonging to the following Event Groups in Command Centre are considered stateful, and hence have 'Return to Normal' events, (i.e. Restorals). These are the events that can have a red bell icon in the Alarm Viewer window.

**Note:** Each of these Event Groups is able to send Contact ID alarms and restores. See ***External Alarm Monitoring*** (on page 29-1) for further detail.

| Event Group | Event Type |
|---|---|
| Open/Off | Input Open<br>Output Off |
| Closed/On | Input Closed<br>Output On |
| Tamper | Controller tampered (front)<br>Controller tampered (rear)<br>Input Break<br>Input Short<br>Unit Tampered (Front)<br>Unit Tampered (Rear) |
| Input Shunted/Isolated | Input Isolated<br>Input Shunted |
| Unit Stopped Responding | Unit Not Responding |
| Door Open Too Long | Door Open Too Long |
| Door Not Locked | Door Not Locked |
| Forced Door | Forced Door |
| Power out of Range | Controller power high<br>Controller power low<br>Unit - power high<br>Unit - power low |
| Command Centre Comms Interrupted | Comms failed to Command Centre |

## Alarm Viewers

### *The windows*

There are two alarm viewer windows available in Command Centre that can co-exist, (i.e. can both be opened on the same workstation). However, your operator privileges and what escalated alarm options have been configured will determine whether they are both accessible to you. They are:

- the main **Alarm Viewer**
- the **Escalated Alarm Viewer** (this window displays escalated alarms only, i.e. Alarms that have not been acknowledged within a specified time will display in the Escalated Alarm Viewer)
  **Note:** Escalation is set up via Action Plans.

The Alarm Viewer windows enable you to monitor alarms occurring at your site. The windows contain alarm messages only. However, these alarm messages are also included within the Event Viewer window.

The behaviour of both the main Alarm Viewer window and the Escalated Alarm Window can be configured via the Configuration tab of an Operator Groups properties. See ***Changing the Alarm Viewer behaviour*** (on page 42-26) for the procedure.

As the Escalated Alarm Viewer is essentially a filtered view of the main Alarm Viewer, both alarm viewers conform to the same behaviour as described in this chapter. Therefore, all the topics covered in this chapter relate to both Alarm Viewers.

**IMPORTANT:**
Where all operator configurations have been set to remove escalated alarms from the main Alarm Viewer, at least one operator must have the Escalated Alarm Viewer open at all times, to ensure escalated alarms remain viewable.

### *Alarm Grouping*

The alarms are grouped according to their priority level. When an alarm occurs, the alarm message displays at the top of the appropriate alarm group.

- The highest priority alarm grouping is displayed at the top of the window.
- The lowest priority alarm grouping is displayed at the bottom of the window.

### *Alarm Flooding*

Alarm flooding occurs when the same alarm is generated numerous times and fills up the Alarm Viewer window. Command Centre allows these alarms to be summarised by only displaying one instance of a flood alarm, with a flood count indicating the number of times the alarm has occurred.

### *The alarm message*

The alarm messages display in a summarised format (which messages are displayed to you will depend on your privilege level):

- what happened
- where it was generated
- who was concerned.

The date and time of the alarm message will flash until you acknowledge the alarm.

### *Actions you can take*

You can select an individual alarm message and view its details. From here, and with the correct privilege level, you can acknowledge and process the alarm.

## Opening the Alarm Viewer window

### Introduction

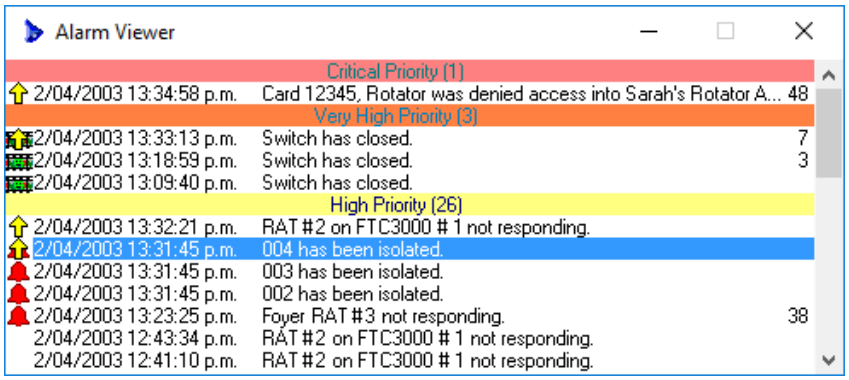
The Alarm Viewer window lists the alarm activity on your site. The alarms are grouped according to their priority level.

### Procedure

1. Click **Monitor** from the menu bar.
2. Click **Alarm Viewer**.

### Result

The Alarm Viewer window displays:




**Note:** If you have a mouse with a scroll wheel, it is possible to scroll (up or down) one alarm at a time, providing the scroll bar appears at the side of the Alarm Viewer window.

### Hints

The Alarm Viewer window updates dynamically; when a new alarm occurs, the appropriate alarm message displays at the top of its priority group.

The date and time of an alarm message flashes until it is acknowledged, and an alarm message is only removed from the Alarm Viewer window when it has been processed.

Numbers to the far right of the window indicate either:

- the flood count for an alarm flood. Only one instance of an alarm flood will display, with the flood count for each alarm flood, or
- the number of times a stateful alarm has occurred.

An operator should be able to distinguish these two scenarios by looking at the event history.

Alarm entries can have different background colours. See ***Alarm Sounds*** (on page 42-23) for further detail.

Various icons may appear to the left of an alarm. The following table describes what these icons are used to indicate:

| Icon | Indicates that an alarm.... |
|---|---|
| Red Bell  | is active, (i.e. the problem has not yet been resolved). You can acknowledge an alarm in this state, but not process it. |
| Film Reel  | has images associated with it. See ***Viewing Images associated with an alarm*** (on page 42-15) for further detail. |
| Yellow Arrow  | is escalated. The yellow arrow appears as an overlay over both the Film Reel icon and the Red Bell icon.<br><br>**Note:** All events and alarms that escalate to the escalated priority will:<br>- also appear in the **Escalated Alarm Viewer**, and<br>- display as “Escalated” in the Alarm Details. |
| Crossed Circle  | comes from a remote server that is currently offline, and the operator will be unable to process the alarm. |

**Note:**
The attributes that display for 'Notify Restoral' alarms may differ slightly from what has been mentioned above. Refer to ***Notify Restoral*** (on page 42-29) for further detail.

## Collapsing the alarm groups

### Introduction

For each alarm grouping, you can hide (collapse) or display (expand) all the associated alarms. By default, the alarm groups are expanded.

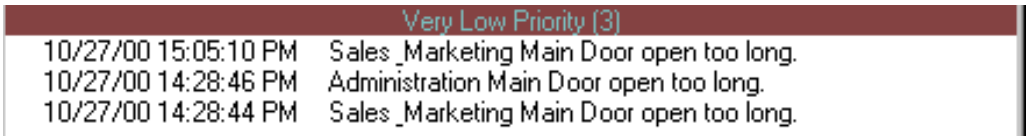
### Procedure

1. Click **Monitor** from the menu bar, then **Alarm Viewer**.
   The **Alarm Viewer** window opens.
2. **Double click** on the appropriate alarm grouping header,
   or,
   **Right click** and select **Collapse**.

### Result

The alarm messages are hidden.
The alarm grouping header indicates the number of alarms in brackets.

*Example before:*




*Example after:*




### Hint

To re-display the associated alarms, simply double click on the alarm grouping header again, or right click and select Expand.

## Viewing alarm details

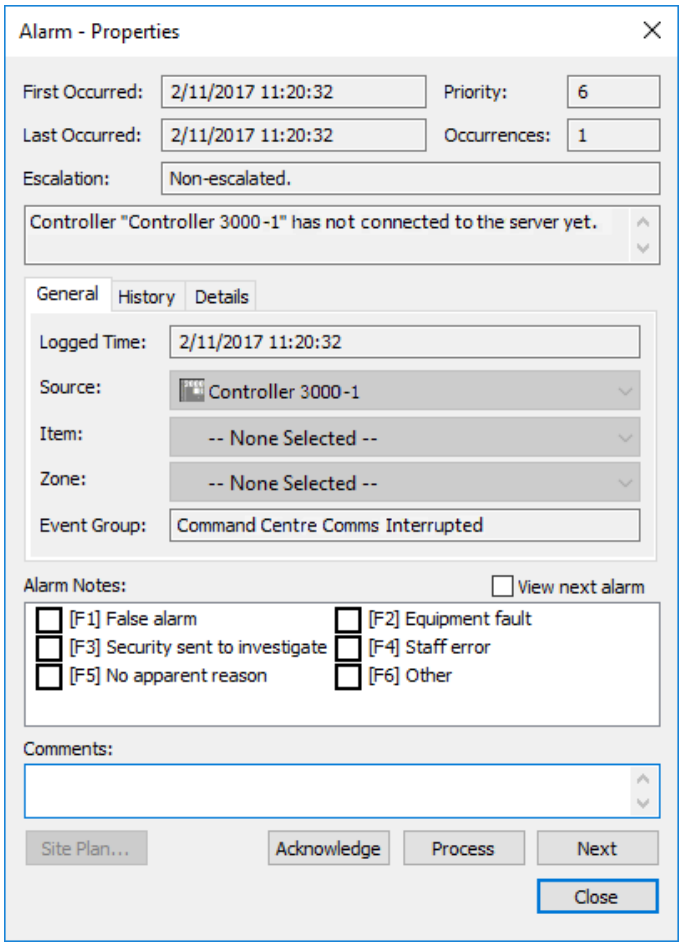
### Introduction

You may want to see more details about a particular alarm.
**Notes:**

- The "Edit Alarms" operator privilege is needed to Acknowledge or Process alarms, however operators without this privilege are still able to add comments in the 'Comments' field.
- In a multi-server system, when a remote server is off-line, a user will not be able to acknowledge the alarm and it will be marked as offline if they attempt to do so. All other remote alarms from that remote server will appear as offline, read only and the user will not be able to process or enter details against them.

### Procedure

1. Click **Monitor** from the menu bar, then **Alarm Viewer**.
   The **Alarm Viewer** window opens.
2. Highlight the alarm message.
3. Either:
   - **Right click** and select **Properties**, or
   - **Double-click** the alarm.
   If an Alarm Instruction has been defined, the **Instructions** tab displays by default. If there is no Alarm Instruction defined however, the **General** tab displays.




The Occurrence Time section of this window relates to Alarm Flooding (see ***Alarm Flooding*** on page 42-7 for a description of what Alarm Flooding is and how to configure it). The following details are displayed:

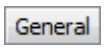
- the Date/Time of the **first** occurrence of an Alarm Flood,
- the Date/Time of the **most recent** alarm,
- number of **occurrences** (i.e. flood count) of an alarm.

The **Escalation** field indicates the escalation state of the alarm. The states are:

- Non-escalated
- Escalated
- Escalated. Acknowledge/process disallowed.

The Escalation field updates dynamically. If you belong to an Operator Group that is not allowed to acknowledge or process escalated alarms, the **Acknowledge** and **Process** buttons become disabled as an alarm escalates.

4. Click the other tabs as necessary to view specific details relating to the alarm:




This tab provides general details (who, what, where) about the alarm. It also includes the 'Event Group' the alarm falls under, which is useful to know in case you wish to run an Activity Report to try to resolve the problem raised by the alarm.

Instructions

This tab only appears on the Alarm Properties page if there is an alarm instruction associated with the alarm. It displays the alarm instructions which you should follow before processing or acknowledging the alarm.

History

All past actions regarding this alarm are displayed, (e.g. When an operator enters notes and acknowledges the alarm, this information will be entered into the **History** tab).
An audit entry is also added to this tab every time an alarm is viewed, indicating which operator viewed it.

Details

Additional details regarding this alarm are displayed, (e.g. the reason why the alarm occurred).

Images

This tab only appears on the Alarm Properties page if there is an image sequence associated with the alarm. It displays a grid of images. When one is selected the Sequence Viewer window is displayed.

5. The **Alarm Notes** field only displays if alarm notes have been configured in the system, on the **Alarm Notes** tab of the Server properties. Refer to ***Alarm Notes*** (on page 6-17) for further information.
   The title of this field displays as either **Alarm Notes (required)** or **Alarm Notes**. This indicates whether the operator needs to select alarm note(s) in order to process or acknowledge the alarm or not.
   When the Alarm Property window is closed, all the selected alarm notes and optional comments are saved. They can then be traced from the **History** tab.
   When the focus is set on the Alarm Property window, Alarm Notes can be selected via function keys. By default, <**F1**> to <**F8**> are assigned to match the first eight alarm notes.
   **Note:** If a function key that has no matching alarm note is pressed, then nothing happens.
6. The View next alarm checkbox allows you to step through the alarm queue and display each alarm when more than one is present. When it is checked the next alarm in sequence automatically pops-up after you have either acknowledged or processed an alarm, or you press the <**F12**> function key on your keyboard.
   The next Alarm Properties window will be that of the next in decreasing priority/time (as displayed in the Alarm Viewer window) if you are processing alarms from the Alarm Viewer, or if entered from the hardware item (either via the Hardware window or Site Plan) then it would further filter on the hardware item.
   **Note:** To use this feature you need the "Edit Alarms" operator privilege.
7. Click the buttons as required:

Site Plan...

This button will be enabled if the site item for which the alarm has occurred is on a Site Plan. Clicking this button will display the relevant site plan indicating the site item.

Acknowledge (or press the <**F10**> function key on your keyboard)

This allows you to acknowledge an alarm so that any relays or alerts triggered by the alarm are reset. See ***Acknowledging an alarm*** (on page 42-16) for further detail.

Process (or press the <**F11**> function key on your keyboard)

This allows you to process an alarm once the alarm condition has been dealt with. See ***Processing an alarm*** (on page 42-17) for further detail.

**Note:**
The **Acknowledge** and **Process** buttons may be disabled for escalated alarms if you belong to an Operator Group that is not allowed to acknowledge or process escalated alarms (via the Operator Group **Configuration** tab).

Next

This button allows you to go to the properties of the next alarm without closing the Alarm Properties window. When there are no more alarms this window closes.

8. Click **Close**.

**Result**

The Alarm Properties window closes.
You have viewed details about the alarm (or alarm flood), but taken no action.

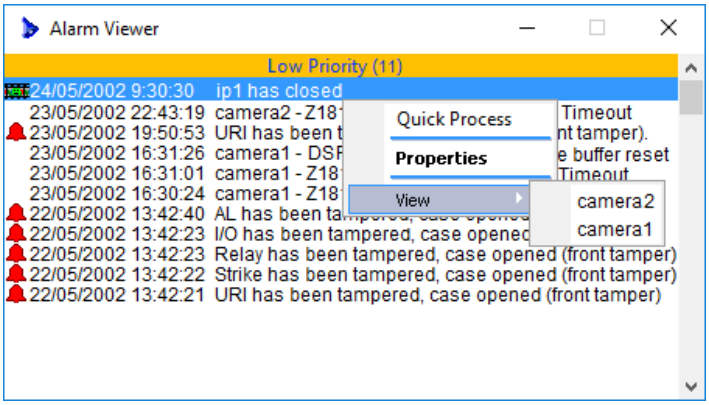
## Viewing Images associated with an alarm

### Introduction

If configured to do so, a Camera will activate and record images associated with an alarm. When the alarm appears in the Alarm Viewer window you can recognise that it has images associated with it by the Film Reel icon on the left hand side of the alarm message.

### Procedure

1. Click **Monitor** from the menu bar, then **Alarm Viewer**.
   The **Alarm Viewer** window opens.
2. Either:
   - **Right click** on the alarm message that has an Image associated with it, and select **View**.




   If the alarms associated Action Plan has two cameras configured to capture image sequences, another pop-up menu will display with the option of both cameras.
   Select the Camera you wish to view.

   Or:

   - Double-click the alarm.
     The Alarm Properties window displays.
     Click the **Images** tab.

   The Sequence Viewer screen displays.
3. View pre-event images and post-event images by clicking the ▶ symbol to play the Sequence Viewer.

### Hint

For flood alarms with images associated, the recommended method of viewing the images is to open the Properties window for the alarm and clicking on the **Images** tab.

## Acknowledging an alarm

### Introduction

This is usually the first action you take regarding an alarm.
By acknowledging an alarm, any relays or alerts triggered by the alarm are reset.

**Note:**
The 'Edit Alarm' operator privilege is needed to Acknowledge an alarm, however operators without this privilege are still able to add comments in the 'Comments' field (limited to 1024 characters).

### Procedure

1. Click **Monitor** from the menu bar, then **Alarm Viewer**.
   The **Alarm Viewer** window opens.
2. Highlight the alarm message.
3. Either:
   - **Right click** and select **Properties**, or
   - **Double-click** the alarm.
4. Select the appropriate **Alarm Note(s)**, and optionally enter details of what action you have taken in the **Comments** field.
5. Either:
   - Click the **Acknowledge** button, or
   - Press the <**F10**> function key on your keyboard.

### Result

The alarm message remains within the Alarm Viewer window.
The date and time of the alarm message no longer flashes.

## Processing an alarm

### Introduction

After the alarm condition (what actually caused the alarm to be generated) has been dealt with, you can process the alarm.

**Note:**
The 'Edit Alarm' operator privilege is needed to Process an alarm, however operators without this privilege are still able to add comments in the 'Comments' field (limited to 1024 characters).

### Procedure

1. Click **Monitor** from the menu bar, then **Alarm Viewer**.
   The **Alarm Viewer** window opens.
2. Highlight the alarm message.
3. Either:
   - **Right click** and select **Properties**, or
   - **Double-click** the alarm.
4. If there is an **Instructions** tab displayed, perform the necessary action according to the alarm instruction before processing the alarm.
5. Select the appropriate **Alarm Note(s)**, and optionally enter details of what action you have taken in the **Comments** field.
6. Either:
   - Click the **Process** button, or
   - Press the <**F11**> function key on your keyboard.

### Result

The alarm message is removed from the Alarm Viewer window, but it remains within the Event Viewer window.

## Quick Processing an alarm

### Introduction

You can quick process certain alarms, (i.e. those that are set up for this type of processing), once the alarm condition has been dealt with.

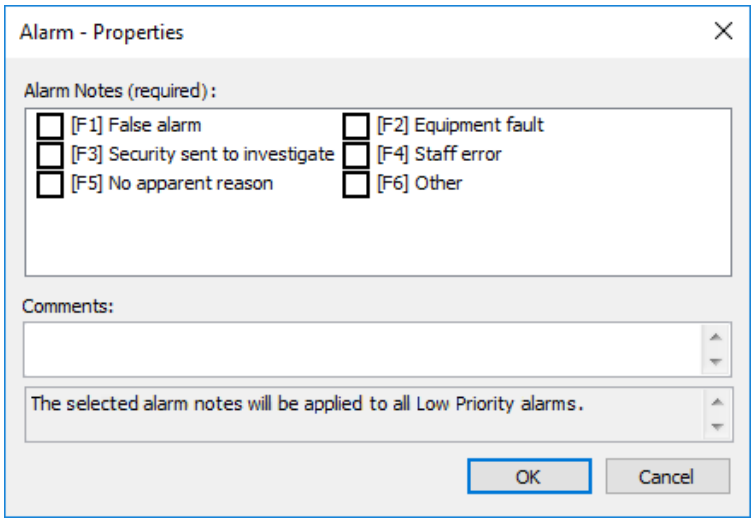
You must have the correct privilege level to quick process alarms. Refer to ***Operator Privileges*** (on page 37-1).

**Note:**
For escalated alarms you must belong to an Operator Group that is allowed to acknowledge or process escalated alarms (via the Operator Group **Configuration** tab) to have the "Quick Process" function available.

### Procedure

1. Click **Monitor** from the menu bar, then **Alarm Viewer**.
   The **Alarm Viewer** window opens.
2. Highlight the alarm message.
3. Either:
   - Press the <**Application**> key on your keyboard and select **Quick Process**, or
   - **Right click** and select **Quick Process**.

   **Note:**
   An Alarm Notes dialog displays, if the alarm notes feature is mandatory. (Clicking the **Close** button cancels this operation.)




To process the alarm:

a) Select the appropriate Alarm Note(s).
   They can be selected via the function keys indicated.

b) Optionally enter any comments in the **Comments** field.

c) Click the **Process** button.

Clicking the **Close** button saves the selected alarm note(s) and/or comments for this alarm.

**Result**

The alarm message is removed from the Alarm Viewer window, but it remains within the Event Viewer window.

**Hint**

If the alarm condition is still active, the **Quick Process** option will not be available on the pop-up menu, (i.e. it will be greyed out).

## Processing numerous alarms

### Introduction

There are instances, (e.g. when setting up a new site), where a large number of alarms get into the system.

With the 'Advanced User' operator privilege, you can:

- process all inactive alarms in a Priority group, or
- process all alarms, both active and inactive, in a Priority Group.

With the "Bulk Process Alarms" operator privilege you can only process all the inactive alarms in a Priority Group. Refer to ***Operator Privileges*** (on page 37-1).

**Note:** For escalated alarms you must belong to an Operator Group that is allowed to acknowledge or process escalated alarms (via the Operator Group **Configuration** tab) to have the "Process All" and "Force - Process All" functions available.

### Procedure

#### *Process Inactive alarms in a Priority Group*

1. Click **Monitor** from the menu bar, then **Alarm Viewer**.
   The **Alarm Viewer** window opens.
2. **Right click** on the alarm priority group header.




3. From the displayed pop-up menu, select **Process All**.

#### *Process All Alarms in a Priority Group*

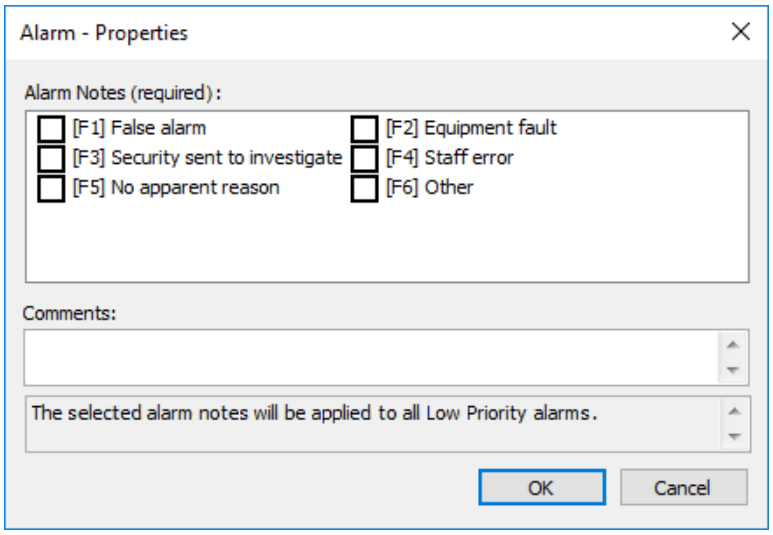
1. Click **Monitor** from the menu bar, then **Alarm Viewer**.
   The **Alarm Viewer** window opens.
2. **Right click** on an alarm priority group header and press the **Shift** key at the same time.




3. Select **Force-Process All**.

### Result

An Alarm Notes dialog displays, regardless of whether or not the alarm notes feature is mandatory, if there are alarm notes configured.

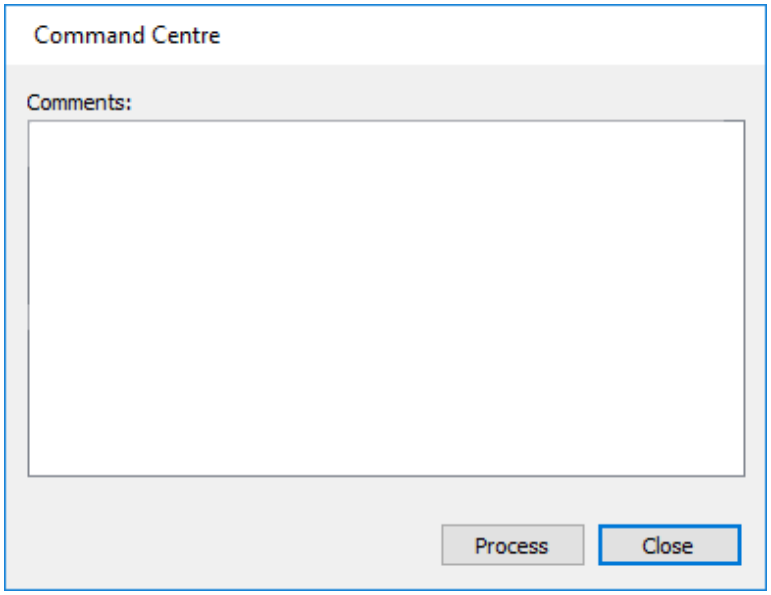



If the alarm notes feature is mandatory, and the alarm group's priority is greater than or equal to the minimum priority for alarm notes, then the title is set as **Alarm Notes (required)**, and the **Process** button is not enabled until you select at least one alarm note.

If the alarm notes feature is **not** mandatory, then the title is set as **Alarm Notes**, and the **Process** button is enabled.

If there are no alarm notes configured:

- the **Alarm Notes** grid is hidden,
- the **Comments** textbox expands to fill up the entire area, and
- the dialog is renamed **Command Centre**.



| If you were processing... | then... |
|---|---|
| **Inactive alarms** in a Priority group | all the inactive alarms in that Priority group are processed and disappear from the Alarm Viewer window. Any active alarms, (i.e. alarms with a red bell icon), in that Priority group will still display. |
| **All Alarms** in a Priority group | all alarms, (i.e. both active and inactive), in that Priority group, are processed and disappear from the Alarm Viewer window. |

## Alarm Sounds

### Introduction

Audio feedback is an option for when an alarm message is generated. A sound (configurable via the **Event Priorities** tab of the Server Properties), is played when there are unacknowledged alarms within either the Alarm Viewer or the Escalated Alarm Viewer. Refer to Event Priorities for details on configuring alarm sounds.

### Recommendation

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.

### Which alarm sound plays

In the Alarm Viewer, the alarm sound that plays is the alarm sound selected for the highest priority, unacknowledged alarm, provided that this alarm occurred, or was escalated, since the last time the operator muted alarm sounds.

Once the operator has muted the alarm sounds, no alarm sound plays until:

- the next new alarm occurs,
- the next existing alarm is escalated, or
- a new instance of a flood alarm occurs that is outside the "Forget Flood Interval".

### What stops alarm sounds from playing

Any of the following actions stops an alarm sound from playing at an operator's workstation:

- The operator mutes alarms (see ***Mute Alarm*** on page 42-25 for details).
  In this case, no alarm sound plays.
- A new, higher priority alarm occurs (than the alarm that is currently the cause of the alarm sound).
  In this case, the alarm sound for the new, higher priority alarm is played (if any).
- All alarms in the operator's Alarm Viewer are acknowledged.
  In this case, no alarm sound plays.

- All unacknowledged alarms of the priority currently triggering the alarm sound, are acknowledged.
  In this case, the standard rules determine which alarm sound plays (if any).

**Background colours**

Different background colours for alarm entries in the Alarm Viewer can assist you to determine which alarm has caused an alarm sound. The standard background colour (usually white, but can differ depending on your Windows settings), of alarm entries indicates the alarms that **may** be the cause of an alarm sound, depending on their priority, whereas alarm entries with the alternate background colour (usually grey), can be eliminated as possible causes of an alarm sound.

When a new instance of an alarm occurs it has the standard background colour, and changes to the alternate background colour when it is acknowledged. When an operator mutes alarms the background colour for **all** alarm entries changes to the alternate background colour.

# Mute Alarm

### Introduction

The sound that plays when there are unacknowledged alarms within the Alarm Viewer or Escalated Alarm Viewer can be muted for current alarms. Once muted, if further alarms occur, the sound will play again.

### Procedure

1. Click **Monitor** from the menu bar.
2. Click **Mute Alarms - F9**.

### Result

The sound is muted.

### Hints

There is an accelerator key for this mute function, as the menu item indicates, (i.e. press the **F9** key to mute the alarm sound).

## Changing the Alarm Viewer behaviour

### Introduction

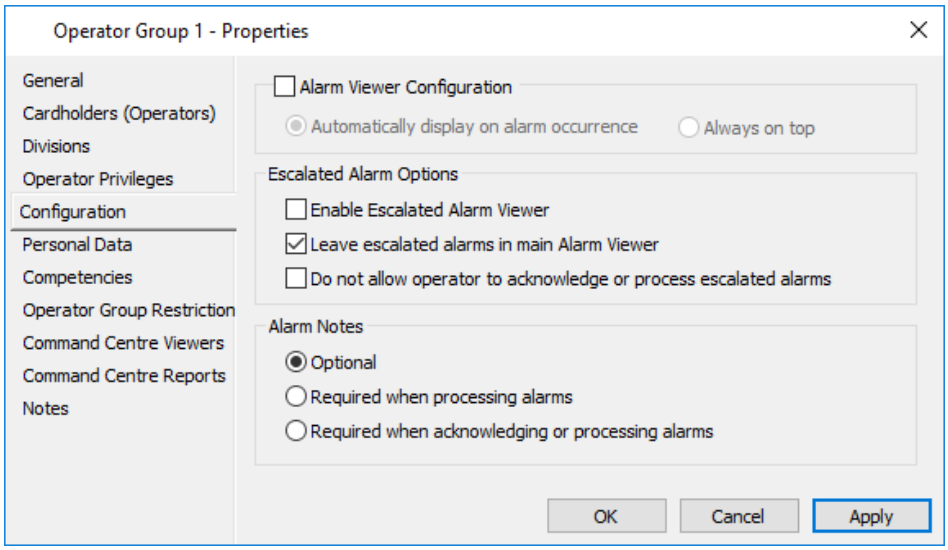
The behaviour of the Alarm Viewer window can be configured via the **Configuration** tab of an Operator Group properties. Therefore, the Alarm Viewer window will behave the same for all operators in an Operator Group.

The options for how the Alarm Viewer window will behave are:

- The Alarm Viewer will remain wherever it is placed by the currently logged on operator, and does not pop to the front of other windows.
- The Alarm Viewer will always be in front of all other windows.
- The Alarm Viewer will be made visible and brought to the front of all other windows when a new alarm occurs.

### Procedure

1. Click **Manage** from the menu bar, then **Operator Groups**.
   The **Operator Group** List Window opens (in grid view).
2. **Highlight** the appropriate Operator Group.
3. **Right click** the mouse button, and select **Properties**.
4. Click the **Configuration** tab.




5. If you want the Alarm Viewer to remain wherever it is placed by the currently logged on operator, and not to automatically pop to the front of other windows, then ensure the **Alarm Viewer Configuration** checkbox is unchecked.
   Go to Step 8.
6. Check the **Alarm Viewer Configuration** checkbox.

7. Click the appropriate radio button for the option you prefer.

| Option | Description |
|---|---|
| Automatically displays on alarm occurrence | The Alarm Viewer will be opened, made visible and brought to the front of all other windows on the occurrence of any new alarm.<br>With this option enabled you can not locate the Alarm Viewer off screen and the entire Alarm Viewer will be visible at all times. |
| Always on top | The Alarm Viewer will always be in front of all other windows.<br>With this option enabled the entire Alarm Viewer will be visible at all times and you can not:<br>• minimise the Alarm window, or<br>• locate the Alarm window off screen. |

8. Do you want escalated alarms to display in a separate window from the main Alarm Viewer?

| If... | then check the... |
|---|---|
| yes | **Enable Escalated Alarm Viewer** checkbox. The Escalated Alarm Viewer will be accessible from the **Monitor** menu, as well as the main Alarm Viewer. |
| no | **Leave escalated alarms in main Alarm Viewer** checkbox. Any escalated alarms will remain in the main Alarm Viewer with non-escalated alarms. |

**Note:** By checking both options you can have escalated alarms appear in both the main Alarm Viewer as well as the Escalated Alarm Viewer.

9. Check the **Do not allow operator to acknowledge or process escalated alarms** checkbox if required for this group.
**Note:**
If checked, the **Acknowledge** and **Process** buttons will be disabled on the Alarm Details property page for escalated alarms.

10. Do you wish to configure alarm note options?
If **no**, then go to Step 11.
If **yes**, then click the appropriate radio button for the option you require.
    - **Optional**
      The privileged operator can optionally select alarm note(s) before processing or acknowledging an alarm.

- **Required when processing alarms**
  The privileged operator must select one or more alarm notes in order to process, or bulk process alarms at a priority level that is equal to or higher than the alarm notes priority threshold.
- **Required when acknowledging or processing alarms**
  The privileged operator must select one or more alarm notes in order to acknowledge, process or bulk process alarms at a priority level that is equal to or higher than the alarm notes priority threshold.

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**

The behaviour of the Alarm Viewer window has been altered accordingly.

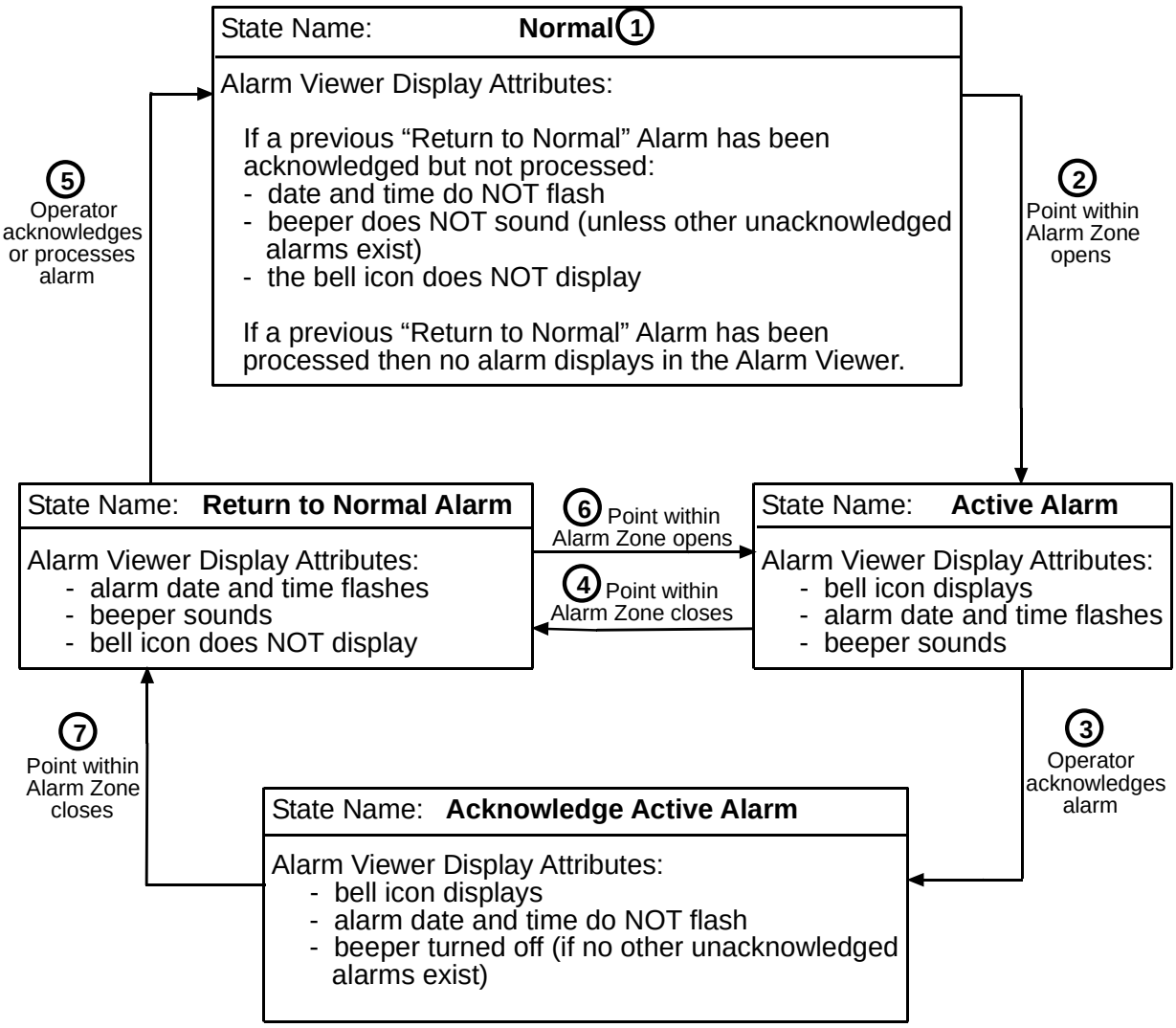
# Notify Restoral

## Introduction

Notify Restoral can only be configured for those events that are considered stateful, and hence have "Return to Normal" events. Refer to ***Events with Restorals*** (on page 42-5) for a list. Notify Restoral causes an alarm to be raised on both the open and closed events for an Alarm Zone and is configured on the **Advanced** tab of an Alarm Zone. 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.).

## Overview

Points that are configured as Notify Restoral points support the alarm states shown in the following diagram and display in the Alarm Viewer as described. Each Notify Restoral alarm will be in one of the states shown at any time.



If a user configures an Alarm Zone with "Notify Restoral", then all points within the Alarm Zone will follow the alarm and other behaviour specified in the diagram on the previous page.

**Example of a Notify Restoral Input**

***① 'Normal' state:***

When Notify Restoral is configured for an input a new alarm instance is created in the Alarm Viewer in the following circumstances:

1. Alarm is in the Normal state and the input opens.
2. Alarm flooding is disabled. A 'Return to Normal' alarm exists. The input contacts open.
3. Alarm flooding is enabled and the next input open event is outside the Tolerance setting.

In all other circumstances the attributes of the existing alarm in the Alarm Viewer window are updated.

***② 'Active Alarm' state:***

When a Notify Restoral alarm transitions from a Normal to an 'Active Alarm' state, the alarm displays in the Alarm Viewer with the following attributes:
- The date and time flash (until acknowledged by an operator).
- The beeper sounds (until all alarms are acknowledged by an operator).
- The bell icon is displayed (while the input contacts remain open).

***③ 'Acknowledge Active Alarm' state:***

A Notify Restoral alarm in an 'Active Alarm' state can be acknowledged but not processed. This places the alarm in an 'Acknowledge Active Alarm' state. When a Notify Restoral Active Alarm is acknowledged the alarm attributes in the Alarm Viewer window are updated as follows:
- The alarm date and time stops flashing.
- The beeper turns off (if there are no other unacknowledged alarms in the Alarm Viewer).
- The bell icon remains displayed.

***'Return to Normal' state:***

④ When a Notify Restoral alarm transitions from an 'Active Alarm' state directly to a 'Return to Normal' Alarm state (due to the input contacts closing), and if the operator has not acknowledged the alarm, the attributes in the Alarm Viewer change as follows:
- The alarm displays at the same priority as specified in the Action Plan for the "Input open" event.
- The alarm date and time continues to flash.
- The beeper continues to sound (unless it has been muted by the operator).

- The bell icon is NOT displayed.

It is possible for an operator to acknowledge and process an alarm in the 'Return to Normal' Alarm state. Either action transitions the alarm to the 'Normal' state. When an operator processes a 'Return to Normal' Alarm, it is removed from the Alarm Viewer.

When a 'Return to Normal' Alarm is acknowledged, the alarm attributes displayed in the Alarm Viewer window change as follows:

- The alarm continues to display at the priority specified in the Action Plan for the "Input open" event.
- The alarm date and time does NOT flash.
- The beeper does NOT sound (unless other unacknowledged alarms exist in the Alarm Viewer window).
- The bell icon is NOT displayed.

When a Notify Restoral alarm is in a 'Return to Normal' Alarm state and the input contacts then open, the alarm transitions to the 'Active Alarm' state. If alarm flooding is disabled, or the input open event is outside the tolerance setting for alarm flooding, a new alarm is created and displayed in the Alarm Viewer window as follows:

- The alarm displays at the priority specified in the Action Plan for the 'Input open' event.
- The alarm date and time flash.
- The beeper sounds.
- The bell icon is displayed.

If the 'Input open' event is within the tolerance setting for alarm flooding, the alarm count is incremented by 1 and the alarm attributes in the Alarm Viewer window update as follows:

- The alarm continues to display at the priority specified in the Action Plan for the 'Input open' event.
- The alarm date and time continue to flash.
- The beeper continues to sound (unless it has previously been muted by the operator).
- The bell icon is displayed.

When a Notify Restoral alarm is in an 'Acknowledge Active Alarm' state and the input contacts then close, the alarm transitions to the 'Return to Normal' Alarm state. The alarm is returned to an unacknowledged state. The alarm attributes displayed in the Alarm Viewer window change as follows:

- The alarm continues to display at the priority specified in the Action Plan for the 'Input open' event.
- The alarm date and time flash.
- The beeper sounds.
- The bell icon is NOT displayed.

Command Centre handles alarm events and operator interventions differently when Notify Restoral is set, compared to when Notify Restoral is not set. The following table compares functionality as an Input item changes from the 'Open/Off' state to the 'Closed/On' state.

| Sequence of events | Notify Restoral | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Set | | | | Unset | | | |
| | Alarm displays | Display flashes | Sound | Bell icon | Alarm displays | Display flashes | Sound | Bell icon |
| Open/off event | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Acknowledged | ✓ | ✖ | ✖ | ✓ | ✓ | ✖ | ✖ | ✓ |
| Closed/on event | ✓ | ✓ | ✓ | ✖ | ✓ | ✖ | ✖ | ✖ |
| Acknowledged | ✓ | ✖ | ✖ | ✖ | *Not possible* | | | |
| Processed | ✖ | ✖ | ✖ | ✖ | ✖ | ✖ | ✖ | ✖ |

# Chapter 43: Site Plans

This chapter provides the following procedures required for monitoring Site Plans.

- ***Viewing an Existing Site Plan*** (on page 43-2)
- ***Viewing Alarms from Site Plans*** (on page 43-4)

If however you require further information about Site Plans, refer to Site Plans in Part 2 - Site Installation of this manual.

### Touch screens

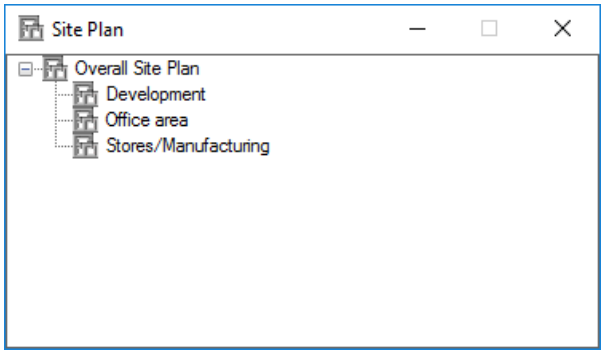
Site Plans is the only feature in Gallagher to support the use of touch screens, and is only applicable when in "View" mode, (i.e. it does not work in "Edit" mode). The implementation of single/double click is an added feature for the touch screen support.

If the users touch screen software currently "enables right click on hold", they do not need to do anything to enable the feature in Gallagher FT (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.

### Site Plan List Window

The **Site Plan** List Window opens in tree view. This tree view is achieved via the **Lineage** tab when Site Plans are set up.




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"*

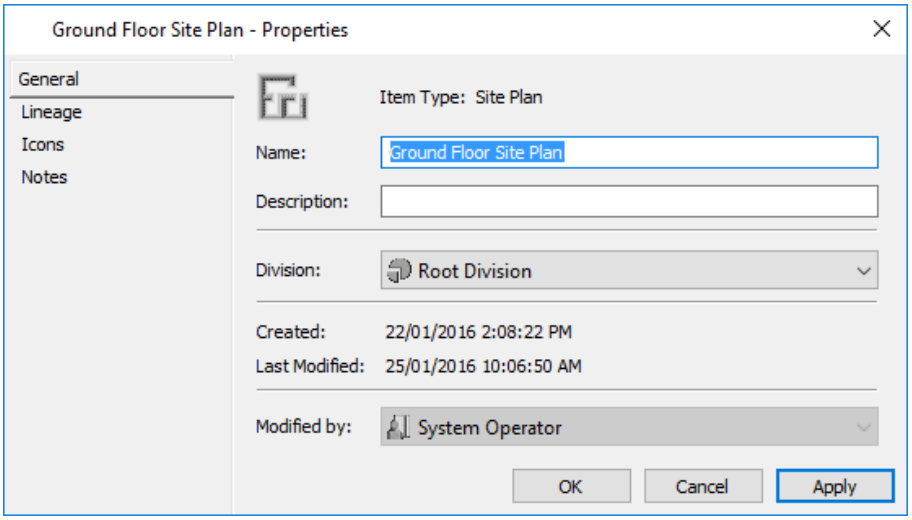
## Viewing an Existing Site Plan

### Introduction

You may want to see more details about a particular site plan. This can be done by opening either the Site Plan properties or the Site Plan layout, (i.e. the graphical image of a site, or part of a site).

### Procedure

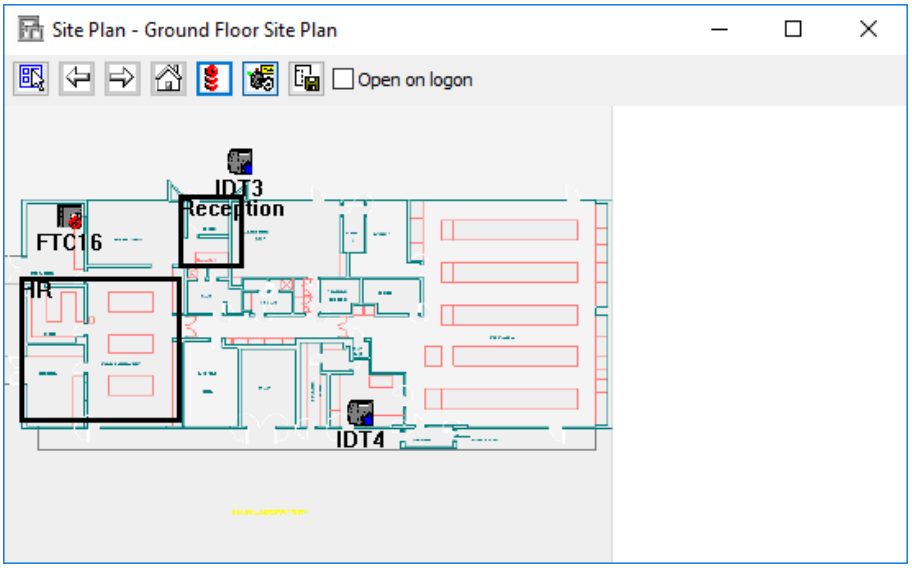
1. Click **Monitor** from the menu bar, then **Site Plans**.
   The **Site Plan** List Window opens (in tree view).
2. Highlight the Site Plan you want to view.
3. **Right click** the mouse button.
4. From the displayed pop-up menu, either:
   - select **Properties**.
     The Site Plan property pages open. By default the **General** tab displays.




   or:

   - select **View in New Window**.
     The Site Plan opens in "View" mode if it is a legacy Site Plan, (i.e. created in Configuration Client).

     If the Site Plan was created in Command Centre Client, the following message will display:
     *"This site plan is edited or viewed in the Command Centre Client"*




**Note:**
For further detail and a description of the Toolbar buttons on a Site Plan, see Site Plan "Edit" and "View" modes.

## Hints

*"Edit" and "View" mode*

By clicking the "Site Plan editing mode" button you can change back and forth between "Edit" and "View" mode.

*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 window, 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.

## Viewing Alarms from Site Plans

### Introduction

When an item, (e.g. a shape, icon, etc., indicating either a linked Site Plan or another item), on a Site Plan starts flashing, this indicates an alarm has occurred. When this happens, you can view the alarms directly from the Site Plan, and acknowledge and process them accordingly.

**Note:** If a linked Site Plan in alarm 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

#### *Viewing linked Site Plans in Alarm*

Either:

- **Right click** on the flashing linked Site Plan item and select **View Site Plan with Alarm**.
  The Site Plan window automatically navigates straight to the Site Plan containing the most important alarm, skipping any intermediate Site Plans. You can then view the actual alarm on the site item (see below).

  Or:

- **Double click** on the flashing linked Site Plan item.
  The Site Plan indicated by the link will display, enabling you to work your way forward to the actual alarm, but see each of the linked Site Plans as you go.

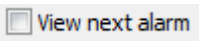
#### *Viewing site items in Alarm*

Either:

- **Right click** on the flashing item and select **View Alarm**.

  Or:

- **Double click** on the flashing item.
  The most important Alarm Properties page for the site item displays.
  **Notes:**
  - Double-clicking on a flashing icon from here or from the Status Viewer results in the Alarm Properties page for the item opening. Whereas, double-clicking on an item in alarm from a List Window or from the Find Tool results in the items Property pages opening.

- When **View Alarm** is selected on a Site Plan and the 

checkbox is checked, the alarm next viewed will be the next in decreasing priority/time related to the Site Plan.

**Hints**

*Alarms in the Site Plan List Window*
Site Plans in alarm will flash on the **Site Plan** List Window also. If the Site Plan that is in alarm is a child Site Plan, the parent Site Plan will flash also. The **View Site Plan with Alarm** and **View Alarm** options are available directly from the **Site Plan** List Window, by right clicking on the Site Plan in alarm, and selecting the required option from the pop-up menu.

*Acknowledging Alarms*
Site Plan items stop flashing and go solid in colour once the alarm is acknowledged.
For more information on acknowledging and processing alarms, see ***Alarm Viewer*** (o n page 42-6).

# Chapter 44: Operator Sessions

Operator Sessions can be terminated to allow immediate release of Workstation (Configuration Client or Command Centre Client), Mobile Client and Visitor Management Kiosk licenses. The only session types that can be terminated are Operator, Operator (Configuration Client), Receptionist, Visit Host and Mobile.

**Note:** Sessions of type Operator (Configuration Client) are limited to 64 sessions per server.

Viewing and termination of operator sessions are controlled via operator privileges.


- ***Opening the Operator Sessions Viewer*** (on page 44-2)
- ***Terminating an Operator Session*** (on page 44-4)
- ***Disabling a Workstation*** (on page 44-5)

## Opening the Operator Sessions Viewer

### Introduction

This viewer provides details of the operators currently logged onto the Command Centre Server. An operator using this viewer can terminate the active sessions of other operators and disable active workstations.

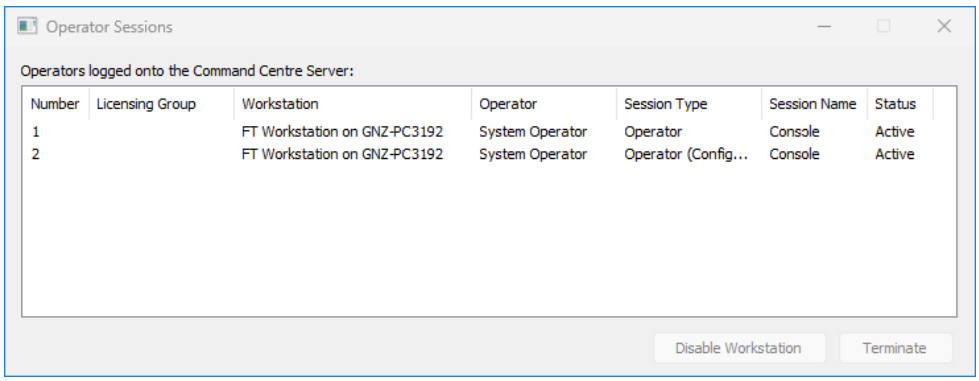
To see a session in the Operator Sessions Viewer, you require the "View Operator Sessions", "Terminate Operator Sessions" or the "Disable Workstation" privilege in the division of the workstation or mobile device associated with the session.

### Procedure

1. Click **Monitor** from the menu bar.
2. Click **Operator Sessions**.

### Result

The session list is retrieved from the server and displayed on the Operator Sessions Viewer.




The columns on the Operator Sessions Viewer are described in the following table:

| If... | then... |
|---|---|
| Number | Assists with counting the number of sessions in the list. |
| Licensing Group | The name of the Licensing Group that the workstation belongs to, if one exists. |
| Workstation | The name of the workstation FT item associated with the session. |
| Operator | The name of the cardholder who has logged on as an operator. |

| If... | then... |
|---|---|
| Session Type | Shows the role assigned to the session for licensing purposes. The user that is logged on will have one of the following roles:<br>• None, (i.e. empty)<br>• Operator<br>• Operator (Configuration Client)<br>• Mobile<br>• Receptionist<br>• Visit Pre-registration<br>• Import/Export<br>• OPC<br>• Remote<br>**Note:** In a multi-server system, when an operator is logged onto a remote server, (e.g. monitoring remote alarms), they will show as a "Remote" session. |
| Session Name | The Windows Terminal Services Session Name. |
| Status | Each session has a Status of either "Active" or "Expired". An **Active** session is alive and has pinged the server in the past 50 seconds.<br>An **Expired** session is an orphaned session that has not pinged the server in the past 50 seconds, and has been disconnected. |

## Terminating an Operator Session

### Introduction

This procedure describes how to terminate an operator session.

To terminate a session, you require the "Terminate Operator Sessions" or "Disable Workstation" privilege in the division of the workstation or mobile device associated with the session. "Terminate Operator Sessions" privilege includes the privileges provided by View Operator Session.

### Procedure

1. Click **Monitor** from the menu bar, then **Operator Sessions**.
   The Operator Sessions Viewer opens.
2. Click on the Session you want to terminate, and click the **Terminate** button.
   The confirmation message *"Are you sure you wish to terminate this operator session?"* displays.
3. Click the **Yes** button.
   The session disappears from the Operator Sessions Viewer.
4. Click the **Close (X)** button to close the Operator Sessions Viewer.

### Result

An Operator Session is terminated and:

- the following Network Connection Failure message displays for the operator whose session has been terminated:
  *"Your session has been terminated by a system administrator"*
- an Operator Event is generated.

## Disabling a Workstation

### Introduction

This procedure describes how to disable a workstation using the Operator Sessions Viewer. This disables the Workstation so that it cannot be logged into using either Command Centre or Configuration Client. Any currently logged-in Command Centre or Configuration Client operator will be logged off.

To disable a workstation, you require the "Disable Workstation" privilege in the Division of the workstation or mobile device associated with the session. "Disable Workstation" privilege includes the privileges provided by Terminate Operator Sessions and View Operator Session.

### Procedure

1. Click **Monitor** from the menu bar, then **Operator Sessions**.
   The Operator Sessions Viewer opens.
2. Click on the Workstation you want to disable, and click the **Disable Workstation** button. A confirmation message displays.
   **Notes:**
   - You cannot disable your own workstation or the server workstation.
   - If the selected workstation has an active session for both Command Centre and Configuration Client, both sessions will be terminated.
   - The disabled workstation will remain disabled until enabled by an operator with the "Enable Workstation" privilege. Workstations can only be enabled from the Workstation item's **Status and Overrides** tab or Command Centre client.
3. Click the **Yes** button.
   The session disappears from the Operator Sessions Viewer.
4. Click the **Close (X)** button to close the Operator Sessions Viewer.

### Result

A workstation is disabled and:

- the following message displays for the operator whose workstation has been disabled: *"Your session has been terminated by a system administrator"*
- an Operator event is generated.
- the workstation cannot be logged onto until it is enabled by an operator with the "Enable Workstation" privilege.

# Chapter 45: Status and Overrides

This chapter provides information about viewing the status of system items, and performing overrides to temporarily change the status of items.

Refer to ***Operator Privileges*** (on page 37-1) to check you have the correct operator privilege level for the activity you wish to perform.

# Understanding Status and Overrides

## Status

The current status of items attached to your Command Centre system can be viewed in the Status Viewer. The information displayed for each item depends upon the type of device, (e.g. an Input would normally display whether it is open or closed, whereas a Door would display whether it is secure, free, etc.)

The Status Viewer updates dynamically; when the state of an item changes, the Viewer also changes.

## Overrides

Overrides enable an operator/cardholder to temporarily change the status of an item attached to your Command Centre system. They enable operators to respond to common, random events. For example, temporarily unlocking the door to give access to a cardholder who has forgotten their card.

All override events are fully reported to the Event Log.

Only one override can be in effect for a single object. If a second override is started, the first override is effectively cancelled.

Operators can **override time schedules** for:

- Time clock relays
  (e.g. to temporarily change the time when air conditioning is automatically switched on)
- The access mode for an Access Zone
  (e.g. to temporarily change the scheduled mode of an access zone to enable easy access for visitors to a meeting venue)
- Alarm Zone state
  (e.g. to temporarily change the status of an Alarm Zone in response to people working overtime)

Overrides can stay in effect until either the next automatic change (as programmed on the time schedule), or for a specified length of time entered by the operator. Overrides that have been implemented for a specified time will persist if the Server resets, or a configuration in the system occurs.

## Opening the Status Viewer

### Introduction

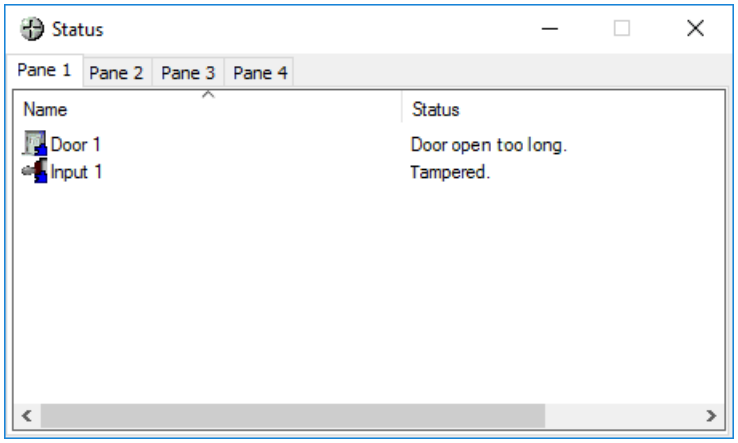
Within the Status Viewer you can add and remove items.

### Procedure

1. Click **Monitor** from the menu bar.
2. Click **View Status**.

### Result

The Status Viewer displays.




The status description depends upon the type of item you selected. For example; an input status would indicate tamper, open, closed, etc., whereas a door status would indicate door open too long, etc.

**Note:** Items in alarm will flash on this screen. Double-clicking on a flashing item from here or from a Site Plan results in the Alarm Properties page for the item opening. Whereas, double-clicking on an item in alarm from a List Window or from the Find Tool results in the items Property pages opening.

### Hints

*Pane tabs*
By default there are 4 Panes (named 'Pane 1' through to 'Pane 4'). These enable you to group items to suit your requirements. For example, into one pane, add only those items you are dealing with. You can add or remove panes (with a limit of 24 panes), and rename them to suit your requirements by right clicking on a tab and selecting the appropriate action, (i.e. **Rename**, **New Pane** or **Remove Pane**).

*Information saved*
When an operator logs off, items in the Viewer are saved along with any preferences, (e.g. renamed panes). When the same operator logs on again, the saved preferences and item lists are re-displayed.

*Properties*
Alternative method to viewing Status is via the Properties window of the required item.

## Adding items to the Status Viewer

### Introduction

You can easily add items to the Status Viewer.
**Note:** Any item that has a **Status and Overrides** tab in its properties can be added to the Status Viewer, along with Archives, Macros and Bulk Changes.

### Procedure

*Drag and Drop method:*

1. Click **Monitor** from the menu bar, then **View Status**.
   The **Status** Viewer opens.
2. Open the List Window that contains the item whose status you want to see.
   For example, open the **Hardware** List Window.
3. Locate the required item.
4. Drag and drop this item into the **Status** Viewer.
   For example, drag Hardware item "H/O Controller 6000" into the **Status** Viewer.

*Copy and Paste method:*

1. Open the List Window that contains the item whose status you want to see.
2. **Right click** the required item.
3. Click **Copy**.
4. Click **Monitor** from the menu bar, then **View Status**.
   The **Status** Viewer opens.
5. **Right click** and click **Paste**.

### Result

Item is added to the Status list.
**Note:** Command Centre will only save 100 items to one Status pane. If you try to add more than 100, an error message will display.

### Hint

You can select multiple items and drag them into the Viewer. Refer to ***Selecting items in a list*** (on page 3-7).

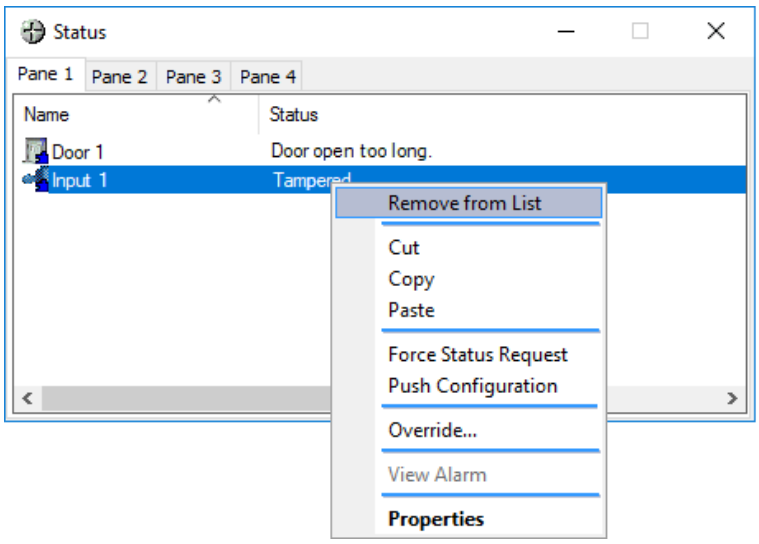
## Removing an item from the Status Viewer

### Introduction

When an item is no longer wanted in the Status Viewer it is a simple procedure to remove it.

### Procedure

1. Click **Monitor** from the menu bar, then **View Status**.
   The **Status** Viewer opens.
2. **Right click** on the item you want to remove.
3. Click **Remove from List**.




### Result

The item is removed from the Status Viewer.

## Performing Overrides

### Introduction

This procedure describes how to temporarily override the status of an item. The items you can perform overrides on are:

- Outputs
- Inputs
- Access Zones
  **Note:** Lockdown overrides and pushbutton overrides can also be performed on Access Zones. Refer to ***Access Zone Lockdown*** (on page 10-8) and ***Configuring Pushbutton Overrides*** (on page 10-32).
- Alarm Zones
- Fence Zones
- Logic Blocks
- Hardware items:
  - Controller 6000 or 7000
  - HBUS Reader
  - HBUS Terminal
  - HBUS Alarms Only Terminal
  - HBUS Contact Card Reader
  - HBUS I/O
  - HBUS F3x/F4x/F5x/F6x Fence Controller
  - HBUS F22 Fence Controller
  - HBUS Z10 Tension Sensor Group
- High Level Elevator Interfaces (Elevator HLIs)
- Guard Tours
  **Note:** Refer to ***Running a Guard Tour*** (on page 54-6) for details on overriding, (i.e. stopping and starting) Guard Tours.
- Workstations
- Doors (including Interlock Groups)
  There are three override options for Doors, as follows:

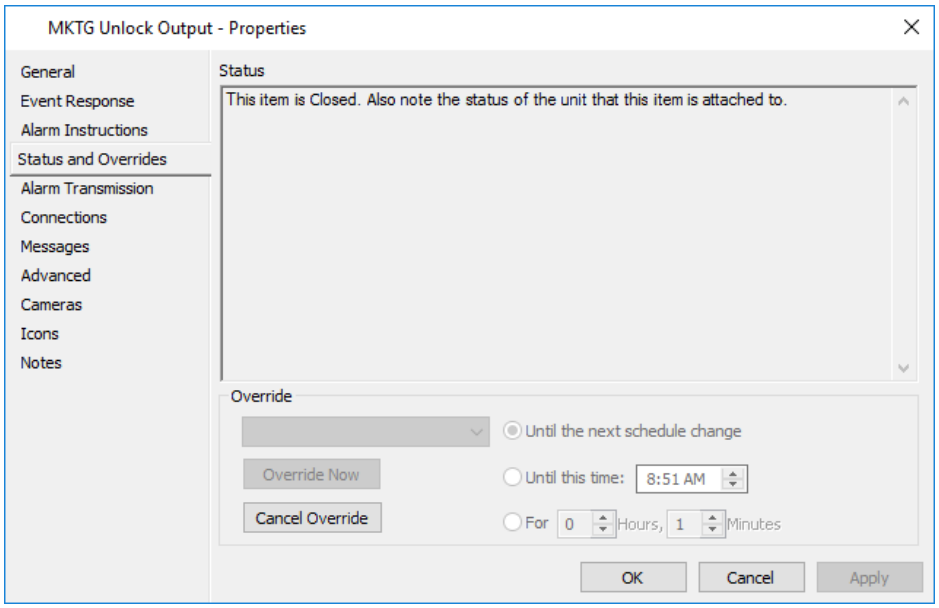
| Menu option | Function |
|---|---|
| Lock Door | This option is only available for Doors with the 'Half-Cycle' Lock type. After access is granted at a half-cycle door, it remains unlocked indefinitely until either it is opened and shut or the Lock Door override is used. This option can lock a half-cycle door while it is shut and unlocked. |
| Open Door | This option releases a door to allow a person to pass through. Refer to ***Open a Door Request*** (on page 45-13) for separate procedure. |
| Override Entry Access | This option opens the 'Status and Overrides' tab of the Access Zone (i.e. entry zone) that is attached to the door. If there is no entry zone this option is greyed out.<br>**Note:** Overriding an entry zone will override ALL doors in that zone. |

Refer to the topic ***Override*** (on page 37-26) to view the privileges required to perform an override in Command Centre.

## Procedure

**Note:** You may not be able to start an override if the target item is offline, as the override will not be immediately applied and could be lost if the target does not come online for over a minute.

1. Open the List Window of the item you want to override.
2. **Right click** on the particular item, and click **Override...** from the drop-down menu.
   The **Status and Overrides** tab on the Properties window for this item displays.




   **Note:** If you wish to override the access entry of a door, click **Override Entry Access** from the drop-down menu.
   The **Status and Overrides** tab on the Properties window of the Access Zone displays.
3. Click within the **Override** field and select the appropriate status from the drop-down list.

| If you are overriding... | then... |
|---|---|
| an Output, Access Zone or Alarm Zone | set the duration for the override to be implemented. You can either:<br>• select the **Until the next schedule change** radio button, or<br>• select the **Until this time** radio button, and enter the time of day you want the override to occur, or<br>• select the **For xx Hours, xx Minutes** radio button, and enter the hours and/or minutes (this is limited to a maximum of 23 hours and 59 minutes). |

| If you are overriding... | then... |
|---|---|
| | **Notes:**<br>• If you do not select an option, it will default until the next schedule change.<br>• When viewing the event log, it is not possible to tell the difference between a 'time of day' override, (e.g. override until 4pm), and a duration based override, (e.g. override for 4 minutes). However, it is possible to calculate the end time for an override by adding the duration of the override to the time the override event occurred.<br>***ALARM ZONES ONLY***<br>If an Alarm Zone **fails to arm due to active** alarms and the operator has either the "Override" or "Override up to Medium Priority" operator privilege, there will be an **Armed (with active alarms)** option available in the Override drop-down list instead of an **Armed** option. Privilege rules apply, (i.e. if the operator has the "Override up to Medium Priority" privilege, the override will only work on active alarms up to and including medium priority, and if the operator has the "Override" privilege they can override active alarms of any priority). |
| an Input | **Shunt:** This stops communication with the Input and will remain this way until you "Unshunt".<br>**Unshunt:** This starts polling of the Input.<br>**Isolate:** Will isolate the Input, so that the Alarm Zone can be armed. Alarms from the Input will no longer be raised.<br>**De-isolate:** The Input is no longer isolated. |
| a Fence Zone | **Shunt:** This stops communication with the Fence Zone and will remain this way until you "Unshunt".<br>**Unshunt:** This starts polling of the Fence Zone.<br>**On:** This causes the Fence Zone to become active, (i.e. pulsing).<br>**Off:** This causes the Fence Zone to become inactive, (i.e. not pulsing).<br>**High Voltage:** This will change the HV/LF mode to high voltage for this Fence Zone. This override is compatible with the F31, F32, F41, F42 and F22 Fence Controllers only.<br>**Low Feel:** This will change the HV/LF mode to low feel for this Fence Zone. This override is compatible with the F31, F32, F41, F42 and F22 Fence Controllers only. |

| If you are overriding... | then... |
|---|---|
| a Hardware item | **Reset:** This performs a software reset on the hardware item. (NB: We recommend you check the state of DIP Switch 2 before performing a "Reset" on a Controller.)<br>**Shunt (not for Controllers):** This stops communication to the device, and all inputs and outputs on that device will no longer be available by the system. It will remain that way until you "Unshunt".<br>***HBUS READERS, HBUS TERMINALS, HBUS ALARMS ONLY TERMINALS AND HBUS I/O INTERFACES ONLY***<br>**Start Identifying Device:** *HBUS Readers, HBUS Terminals, HBUS Alarms Only Terminals, and HBUS Contact Card Reader:* This causes the reader/terminal to flash amber five times and beep five times repeatedly, spaced approximately three seconds apart.<br>*HBUS I/O Interfaces:* The board's status LED will stay on until the override is cancelled. This enables an installer to identify the board within a cabinet<br>**Stop Identifying Device:** *HBUS Readers, HBUS Terminals, HBUS Alarms Only Terminals, and HBUS Contact Card Readers:* This causes the reader/terminal to stop identifying itself.<br>*HBUS I/O Interfaces:* This causes the board to stop identifying itself.<br>***CONTROLLERS ONLY***<br>**Disable Communication:** This stops a server communicating with the Controller and remains that way until you "Enable Communication". It prevents the server from attempting to connect to the Controller, or the server from accepting contact from the Controller.<br>**Enable Communication:** This enables a server to start communicating with the Controller.<br>**Enable WWW Connections:** This is a timed override that allows web access to the Controller until the given expiry time, irrespective of DIP Switch 1 settings.<br>**Cancel WWW Override:** This expires an "Enable WWW Connections" override, and web access will once again be controlled by DIP Switch 1 settings.<br>**Revalidate Certificate:** This tells the server to forget the previous stored identity of the Controller, and to re-challenge the Controller the next time it establishes a connection to the server. After performing the override, the Controller's status message will show *"Controller using legacy encryption"*, until the Controller reconnects. This status message will however stay if the Controller is running firmware earlier than v7.80.<br>**Send Server address:** If a controller is unable to connect |

| If you are overriding... | then... |
|---|---|
| | to the server (and is therefore "offline") this override enables the controller to establish communication with the server. It will establish a connection to the controller and then use this connection to send the server's address. When successful, the controller will connect to the server and come "online" again.<br>**Note:** A warning message *"Controller and all related items may be unusable for a period of time"* will display if you use this override when the Controller's status message shows as *"Controller using legacy encryption"* (on the Controller's **Status & Overrides** property page).<br>***CONTROLLERS ONLY (when configured for 'Enable Secondary Ethernet Link')***<br>**Use Secondary Ethernet:** This is a timed override that requests the Controller to switch the ethernet link it is using.<br>**Cancel use Secondary Ethernet:** This expires a "Use Secondary Ethernet" override, and switches back to the original ethernet link it is using.<br>***CONTROLLER 7000 ONLY***<br>**Start Identifying Device:** This causes the controller Run LED to flash amber five times repeatedly, spaced approximately three seconds apart.<br>**Stop Identifying Device:** This causes the controller Run LED to stop identifying itself.<br>**Note:** F5x/F6x Fence Controllers can also have **Initiate Battery Test** and/or **Reset LV Sync Secondaries** overrides performed on them. See ***Configuring an F3x/F4x/F5x/F6x Fence Controller*** (on page 48-9) for a description of these overrides. |
| an Elevator HLI | **Shunt:** This stops communication with the elevator system and remains that way until you "Unshunt". Once the elevator system has detected that communication has been lost it will apply the default access mode. Normally this means access to any floor from an elevator car is allowed. (Some elevator systems, however, will allow a configurable access mode to be applied when communication is lost.)<br>**Unshunt:** This starts polling of the elevator system. Access to floors from the elevator cars will now be controlled by Command Centre. |
| an Interlock Group | **Disable Group:** This disables the interlocking functionality by ignoring all interlocking rules. The doors in the group operate as if they do not belong to an Interlocking Group.<br>**Enable Group:** This enforces the interlocking rules defined for the group. |

| If you are overriding... | then... |
|---|---|
| | **Note:** Items other than doors in an Interlock Group give misleading status, (i.e. a status message about preventing XXX from opening only applies when XXX is a door). |
| a Logic Block | **On:** This disables the Logic Block's rules and timing options, and sets its output "on".<br>**Off:** This disables the Logic Block's rules and timing options, and sets its output "off".<br>**Reset Logic:** This restores the logic to a known state, and cancels long delay times or pulse times if these are unwanted. |
| a Workstation | **Deregister Workstation:** Workstations only need to be registered if Server Properties have been configured with workstation restrictions or an Operator Group is restricted to the Workstation. When a Workstation is registered, the Command Centre server expects a certain certificate to be used when the Workstation connects. If this certificate is lost or changed, or the Workstation is re-installed, the Workstation needs to be deregistered and registered again. While deregistered, the Workstation cannot logon until a new registration code is entered. Refer to the "Client Authentication" appendix in the *Release Note Command Centre* document for details about registration and the WorkstationCertificateInstaller utility.<br>**Disable Workstation:** This disables the Workstation so that it cannot be logged into using either Command Centre or Configuration Client. Any currently logged-in Command Centre or Configuration Client operator will be logged off. These clients will remain disabled until the Workstation is manually enabled again with the 'Enable Workstation' override.<br>**Enable Workstation:** This returns the Workstation to the normal enabled state so it can be used by operators. |

**Note:** You cannot specify the duration of the override on Inputs, Hardware items and Elevator HLIs, (i.e. until the next schedule change or for a specified time).

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

**Result**

The item is overridden for the time specified.
While the "Shunt" override is in place, the system will not monitor the item, and the item will not generate alarms or cause event initiated actions.

## Open a Door Request

### Introduction

This procedure enables an operator with the "Override - Open Door" privilege, to open a specific door for a few seconds to allow a person to pass through.

### Procedure

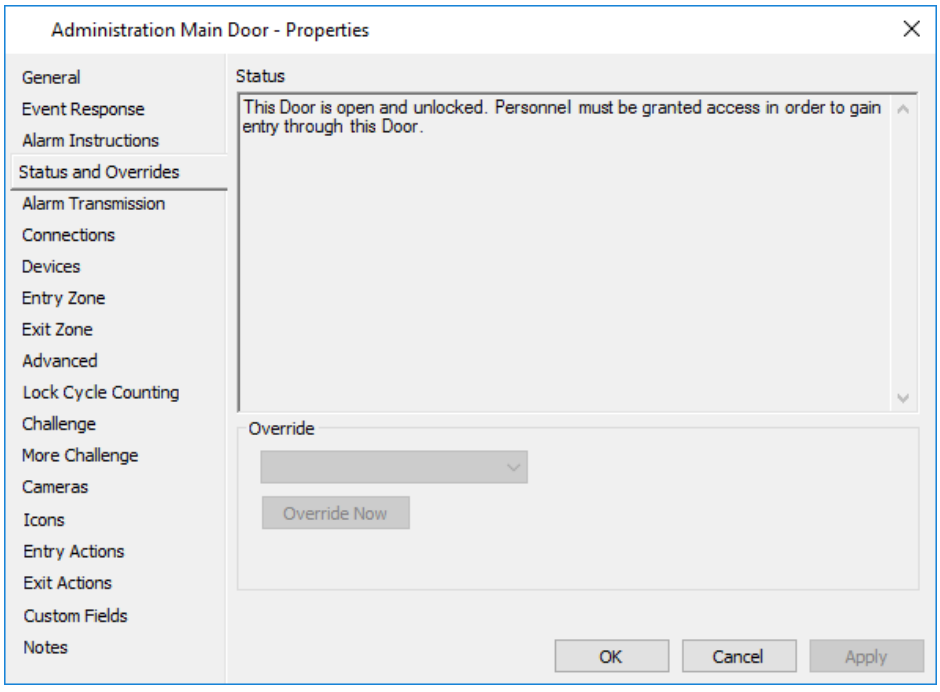
1. Click **Configure** from the menu bar, then **Doors**.
   The **Door** List Window opens (in grid view).
2. **Right click** on the door you wish to open, and click **Open Door** from the drop-down menu.

### Result

The door is briefly unlocked (for a length of time set by the system), and the person can open the door and pass through.

### Hint

Alternatively, instead of clicking Open Door from the drop-down menu, you can 'open the door' from the **Status and Overrides** tab on the Properties window for the Door.




Click within the **Override** field and select "Open Door", then click the **Override Now** button to open the door.
From this screen you can see the status change as a result of the override.

**Note:** You can not specify that an override to open a door be implemented until the next schedule change or for a specified time.

## Configuring Local Overrides at Card Readers

### Introduction

A local override at a reader enables Cardholders to arm or disarm the Alarm Zone associated with the Access Zone of a reader. A local override can also be used to change the access mode, (e.g. from Secure to Free) for the Access Zone associated with the reader.

**Note:** Cardholders require the appropriate privileges in order to perform local overrides at readers. Refer to the procedures below for details on how to configure the appropriate privileges for local overrides at readers.

There are three methods of performing local overrides, as follows:

1. For a Gallagher T20 Terminal connected as an HBUS Terminal, press the **Arm** button and then log on to the terminal. The required log on credentials are configured on the "Welcome Screen" tab of the HBUS Terminal item.

   For a Gallagher T20 Terminal connected as a Cardax IV Reader, press the **Arm** button and then perform the necessary action(s) in order to access the zone, (e.g. present your card) at the terminal.

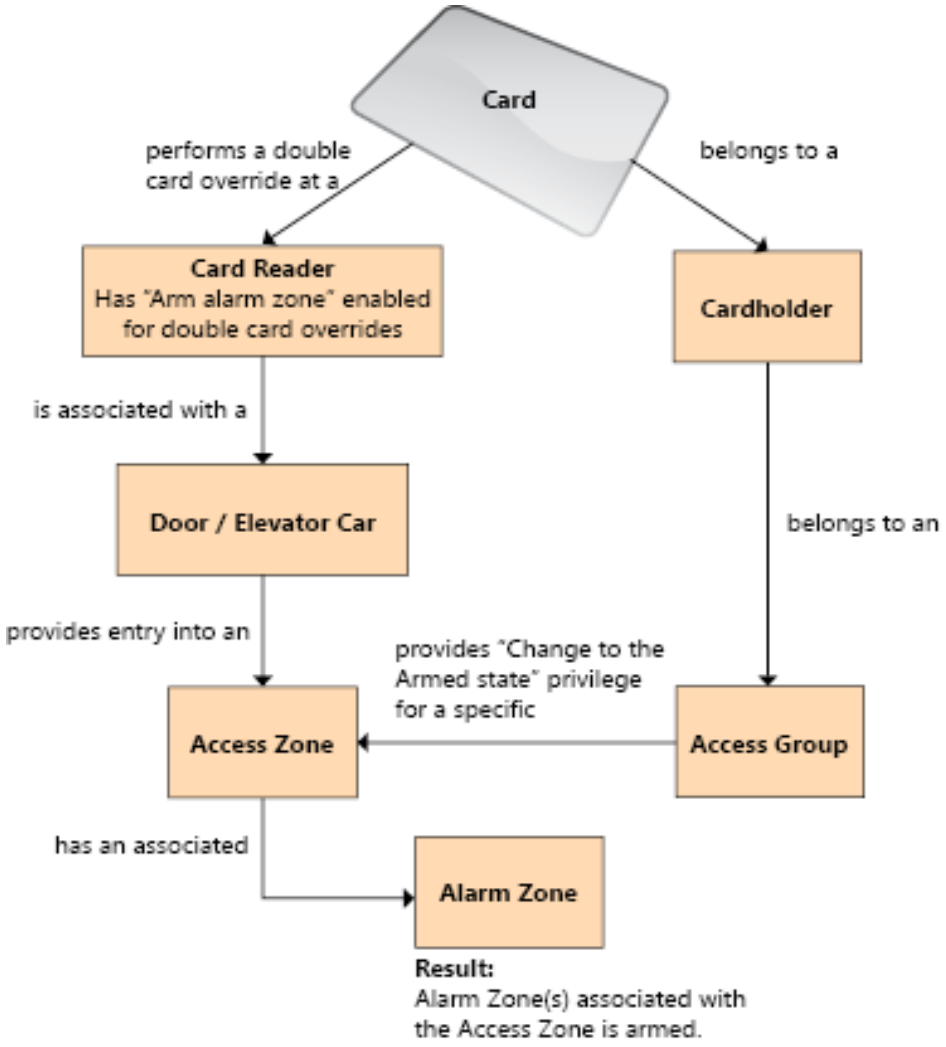
2. For a Gallagher T20 Terminal connected as an HBUS Terminal, press the **Mode** button and then log on to the terminal. The required log on credentials are configured on the "Welcome Screen" tab of the HBUS Terminal item. The Access Mode screen displays on the terminal. Select the Access Mode you require.

   For a Gallagher T20 Terminal connected as a Cardax IV Reader, press the **Mode** button and then perform the necessary action(s) in order to access the zone, (e.g. present your card) at the terminal. Press the number, (i.e. 1, 2 or 3) representing the Access Mode you require, (i.e. Mode 1, Mode 2 or Scheduled).

   **Note:** You cannot perform an Access Zone override at a reader unless the Alarm Zone associated with the Access Zone is disarmed.

3. Badge your card twice, (known as a 'double-card override'), from any reader. Depending on what has been configured in Command Centre, this either overrides the mode of an Access Zone, alternating between Mode 2 and scheduled, or it arms the Alarm Zone associated with the reader.

   The following diagram describes how a double-card override is configured to arm the Alarm Zone associated with a reader.




## Readers in elevators

If a reader has been installed in an elevator and a Cardholder performs an override at the reader, the override is attempted on all the Access Zones or Alarm Zones on all levels the Cardholder has privilege to perform overrides.

*For example:*
If an Alarm Zone override is performed at the reader of a 10-level elevator, and the Cardholder only has "Change to the Armed state" privilege to six of the levels, then only the Alarm Zones on those six levels will attempt to arm. Depending on configuration, for the four levels that the Cardholder did not have privilege to arm the alarm zone, an "Access Override Denied" event will occur. This also results in an Access Denied tone sounding at the reader.

**Note:** If an HBUS Terminal is assigned as the reader for an elevator car, a Cardholder cannot perform an override using the function keys (Arm and Mode) keys at the terminal. However, double card overrides can still be performed, although not recommended.

**Important:**

- This is not the recommended setup, as overrides should be performed at the individual readers in each Access or Alarm Zone.
- While double card overrides can be performed at elevator car readers, it is not recommended because of the potential to accidentally override multiple Alarm Zone or Access Zone states.

### Alarm Zone override at a reader

This table summarises the effect of overriding an Alarm Zone at a local reader on a door and the privileges that are required. Where the override is performed at an elevator car reader, Alarm Zones on any level are armed or disarmed as shown, provided that the Cardholder has the required privilege for that level.

| Action | Alarm Zone (Before) | Alarm Zone (After) | Privileges Required |
|---|---|---|---|
| Double card badge | Disarmed | Armed | "Change to the Armed state" privilege for the Alarm zone.<br>Reader set to "Arm alarm zone" for double card overrides. |
| Double card badge | Armed | Armed | "Change to the Disarmed state" privilege for the Alarm Zone.<br>"Change to the Armed state" privilege for the Alarm zone.<br>Reader set to "Arm alarm zone" for double card overrides. |
| Single card badge | Armed | Disarmed | "Change to the Disarmed state" privilege for the Alarm Zone. |
| Arm and access method (Cardax IV T20 Terminal) or Arm and log on (HBUS Terminal) | Disarmed | Armed | "Change to the Armed state" privilege for the Alarm zone. |

### Access Zone override at a reader

This table summarises the effect of overriding an Access Zone at a local reader on a door and the privileges that are required. Where the override is performed at an elevator car reader, the Access Zone state for any level is changed as shown, provided that the Cardholder has the required privilege for that level.

**Note:** You cannot perform an Access Zone override at a reader unless the Alarm Zone associated with the Access Zone is disarmed.

| Action | Access Zone (Before) | Access Zone (After) | Privileges Required |
|---|---|---|---|
| Double card badge | Scheduled | Mode 2 | "Lock and unlock access zones" privilege for the Access Zone.<br>Reader set to "Override access zone" for double card overrides. |
| Double card badge | Mode 2 | Scheduled | "Lock and unlock access zones" privilege for the Access Zone.<br>Reader set to "Override access zone" for double card overrides. |
| Mode and access method (Cardax IV T20 Terminal) or Mode and log on (HBUS Terminal) | Any | Mode 1, Mode 2 or Scheduled state, whichever is selected by the cardholder performing the override. | "Lock and unlock access zones" privilege for the Access Zone. |

### Procedure

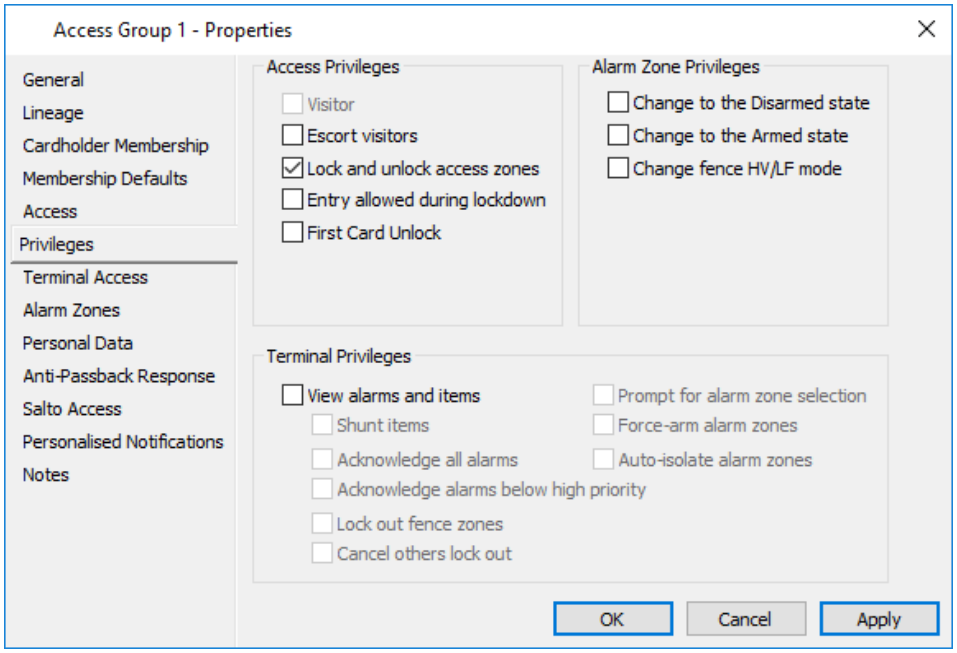
This procedure has been split into four, as follows:
- Configuring an Access Zone Override at a Reader
- Configuring an Alarm Zone Override at a Reader
- Configuring the Card Badge Time-out
- Configuring Double Card Overrides at a Reader

Follow the procedures that are appropriate for the configuration you require.

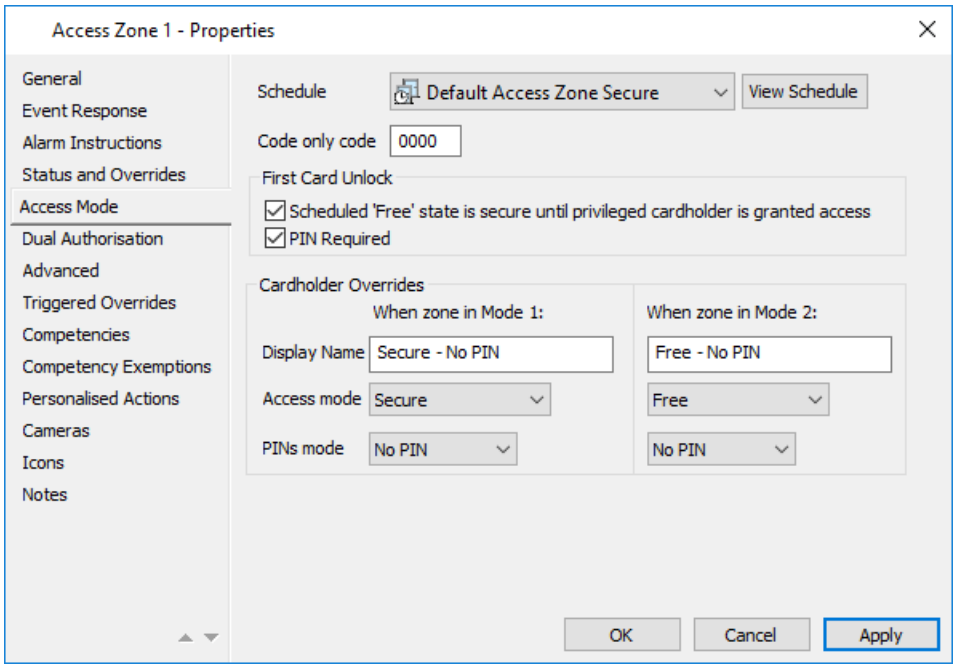
#### *Configuring an Access Zone Override at a Reader*

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

2. Open the relevant Access Group(s) for the people to have this privilege.
3. Click the **Privileges** tab.
4. Check the **Lock and unlock access zones** checkbox.
   This privilege enables members to override the state of an Access Zone from a reader.
   The Access Zones that the privilege applies to are listed on the **Access** tab of the Access Group.




5. Click the **OK** button.
6. Click **Configure** from the menu bar, then **Access Zones**.
   The **Access Zone** List Window opens (in tree view).
7. Open the Access Zone associated with the reader where these local overrides will be performed from.
8. Click the **Access Mode** tab.




9. The 'Cardholder Overrides' section of this screen determines what happens when a cardholder overrides this Access Zone. Otherwise the mode is determined by the Schedule.
   When performing overrides, you can select which state (Mode 1, Mode 2 or Scheduled) the Access Zone is overridden to. When performing double card overrides the Access Zone state changes between Mode 2 and the scheduled state with each successive override that is applied.

   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 Mode.

   Specify the required access modes for Mode 1 and Mode 2.
10. Click the **OK** button.
11. To configure the maximum time allowed between card badges or between pressing a function key and badging your card refer to *Configuring the Card Badge Time-out* (later in this section).
12. Do you intend using double card overrides?
    - If **no**, then this procedure is complete.
    - If **yes**, then go to *Configuring Double Card Overrides at a Reader* (later in this section).

**Result**

Cardholders belonging to this Access Group can now perform overrides of the Access Zones assigned to this Access Group from a local reader.

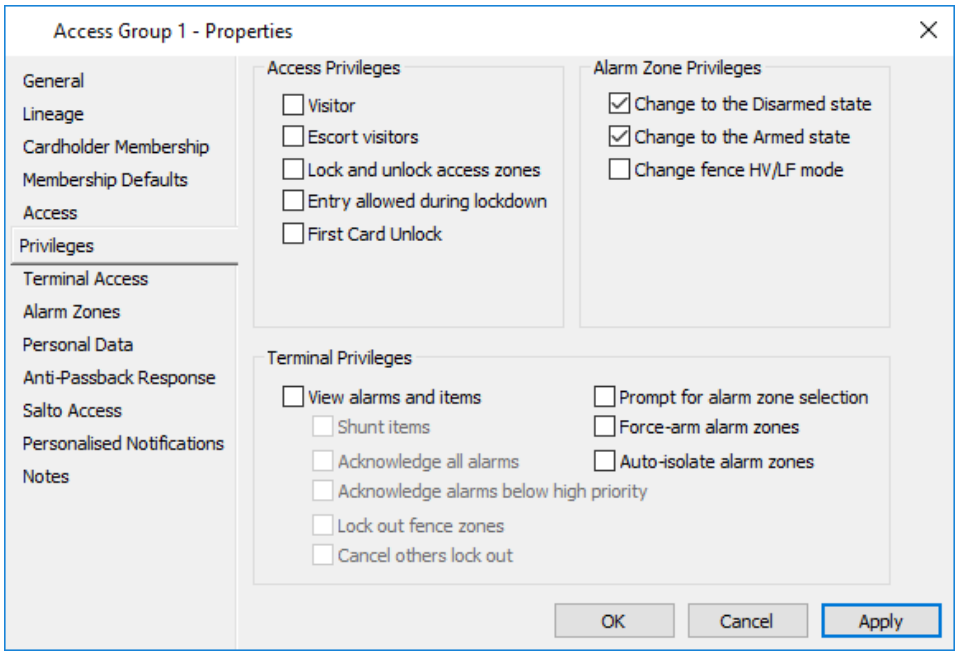
**Hint**

If the Door has been configured with an exit Access Zone, the override is

successfully performed on the entry Access Zone, however the door will remain locked, if the exit Access Zone Access Mode is set to secure. To ensure the lock status of the door follows the entry zone Access Mode, check the **Door lock status follows entry zone only** checkbox on the **Advanced** tab of the Door's properties.

### *Configuring an Alarm Zone Override at a Reader*

1. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).
2. Open the relevant Access Group(s) for the Cardholders to have this privilege. This Access Group must contain the Access Zone associated with the Alarm Zone that you want to provide override privilege for.
3. Click the **Privileges** tab.
   Check the **Change to the Armed state** checkbox if you want to provide the privilege to arm alarm zones.
   Check the **Change to the Disarmed state** checkbox if you want to provide the privilege to disarm alarm zones.
   The privilege applies to Alarm Zones associated with the Access Zones listed on the **Access** tab. It is also confined to the time-frames in which access is allowed to the Access Zone, as specified in the associated Schedule.
   **Note:** The privilege applies to the Alarm Zones listed in the Alarm Zones tab of this Access Group, if you are performing the override at a terminal.




4. Click the **OK** button.
5. To configure the card badge time-out when performing the override, refer to *Configuring the Card Badge Time-out* (later in this section). This is the

maximum time allowed between card badges, when performing a double card override, or between pressing a function key and badging your card.

6. Do you intend using double card overrides?
   - If **no**, then this procedure is complete.
   - If **yes**, then go to *Configuring Double Card Overrides at a Reader* (later in this section).

**Result**

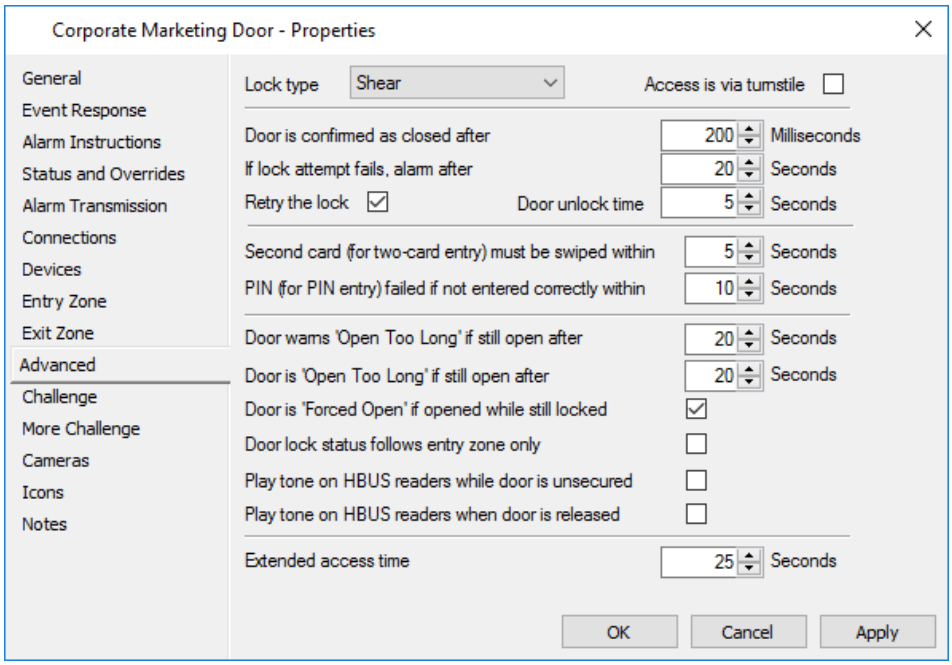
Cardholders belonging to this Access Group can now perform overrides of the Alarm Zones associated with the Access Zones assigned to this Access Group from a local reader.

### *Configuring the Card Badge Time-out*

This procedure configures the card swipe time-out at a reader installed at a door or in an elevator car.
**Note:** The Arm and Mode override card time-outs on an HBUS Terminal are configured on the **Welcome Screen** tab of the HBUS Terminal FT item.

1. Open the **Door** List Window (for doors) or the **Elevator Car** List Window (for elevator cars).
2. Open the door or elevator car which the reader, (i.e. the reader where the override will be performed from), is connected to.
3. Click the **Advanced** tab.
4. Are you configuring the local override for a door or elevator car?

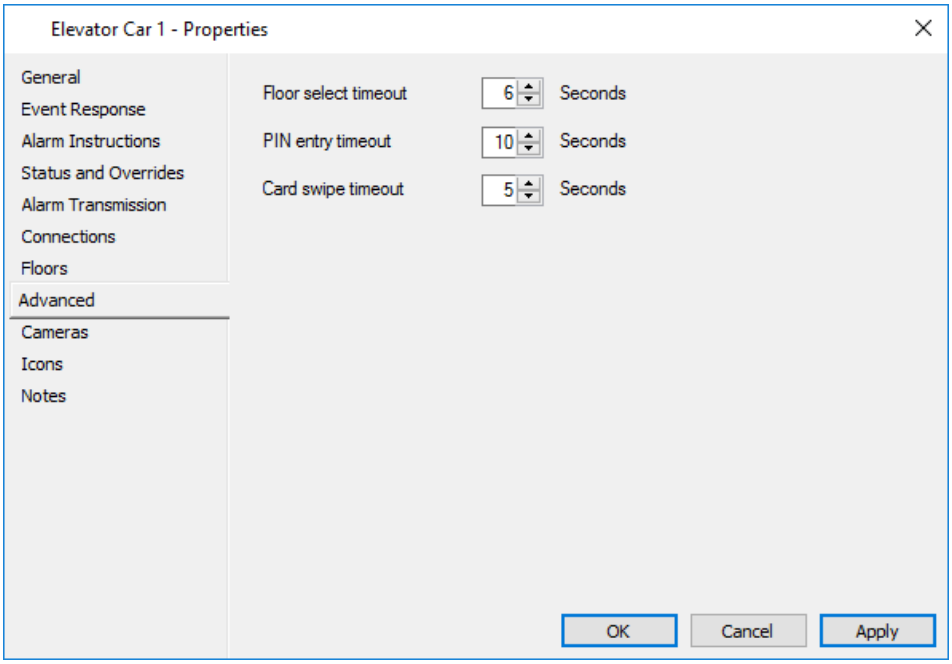
   - If it is at a **door**, refer to this step and skip Step 5.
   - If it is at an **elevator car**, refer to Step 5.



Enter the number (in seconds) in the **Second card (for two-card entry) must be swiped** field for the time required between the two card badges, or between pressing a function key then badging your card.

**Note:** Altering this also modifies the second card swipe time for visitors and Dual Authorisation mode.

5. Enter the number (in seconds) in the **Card swipe timeout** field for the time required between the two card badges, or between pressing a function key then badging your card.




6. Click the **OK** button.

**Result**

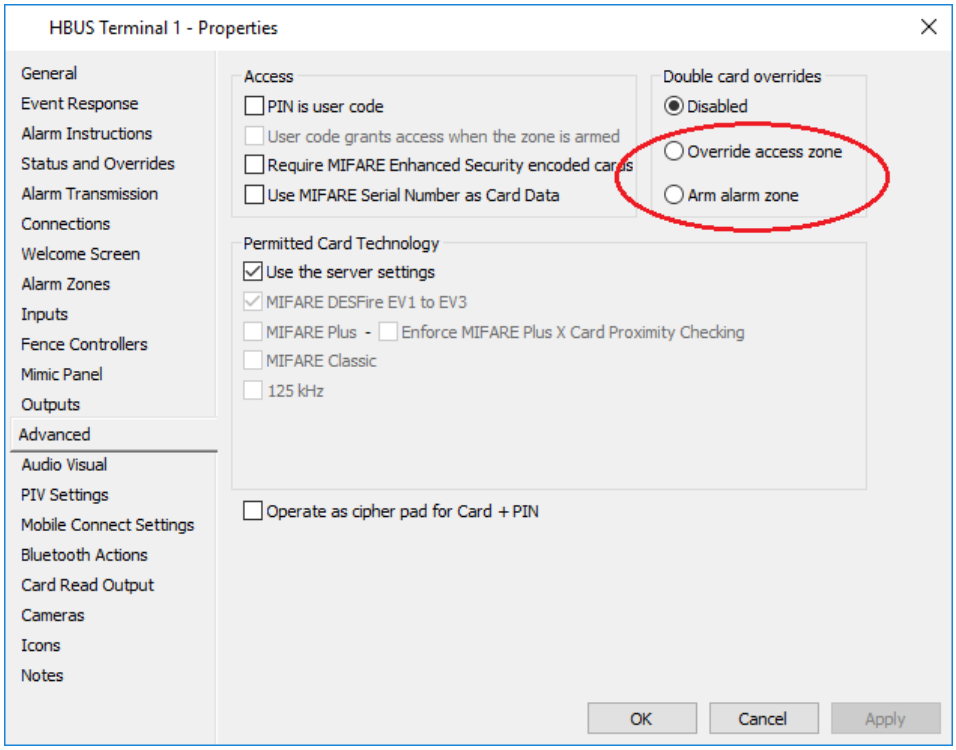
The configured card badge time-out will be applied to any overrides performed at the door or elevator car.

### *Configuring Double-Card Overrides at a Reader*

1. Open the Property page for the reader(s) associated with the door, (i.e. as specified on the **Entry Zone** and **Exit Zone** tabs of the Door Properties).

   **Note:** If you are configuring an override at an Elevator Car, select the reader associated with the Elevator Car (i.e. as specified on the **Connections** tab of the Elevator Car Properties).

2. Click the **Advanced** tab.
3. Click either the **Override access zone** or the **Arm alarm zone** radio button, depending on whether you want the double card override to override the state of the Access Zone or arm the Alarm Zone associated with the Access Zone.




4. Click the **OK** button.
   The double card override feature is enabled.
5. Repeat this procedure for each Door or Elevator Car associated with a reader from which you want to perform double card overrides.

**Result**

Cardholders with the appropriate override privilege can now override the Access Zone state or Alarm Zone state (whichever was configured) at this reader using a double card override.

**Note:** The double card override feature is not supported whilst an Access Zone is in Dual Authorisation mode.

# Chapter 46: Alarm Input Test Modes

Select the item below that you require further detail on:
(Refer to ***Operator Privileges*** on page 37-1 to check you have the correct operator privilege level for the activity you wish to perform.)


- ***Functionality provided by Alarm Input Test Modes*** (on page 46-2)
- ***Configuring Inputs for Test Modes*** (on page 46-5)
- ***Configuring Alarm Zones for Test Modes*** (on page 46-7)
- ***Configuring Access Groups for Test Modes*** (on page 46-9)
- ***Configuring Cardholders for Test Modes*** (on page 46-11)
- ***Configuring Terminals for Test Modes*** (on page 46-12)
- ***Configuring Event/Alarm Notifications for Test Modes*** (on page 46-13)

## Functionality provided by Alarm Input Test Modes

The Alarm Input Test Modes feature provides the following functionality:

### Periodic Testing

Periodic Testing occurs when a staff member authorised to perform Periodic Test Mode disarms the system using aGallagher terminal. The staff member can then choose to enter Test Mode or disarm as usual.

There is a configurable time of one to thirty days for which the test is optional. After the configurable time, the test is no longer optional.

The staff member is then required to check that all inputs configured for testing are functioning correctly. They do this by activating each input.

At any time during Test Mode it is possible for the staff member to end the test manually using the terminal. When this happens an email is sent to the manager advising that the test was aborted.

The test will need to be completed within a configurable length of time. The time left displays as a countdown on the terminal. An audible warning will sound with one minute to go and the staff member is given the opportunity to extend the testing time.

If all the inputs are successfully activated before the timeout, the terminal provides an indication that all inputs have been successfully tested. When the test completes, the system disarms and a report is sent to the alarm monitoring company and an email is sent to the manager.

If one or more inputs failed to activate before the test timeout, the test completes and the system disarms. The terminal lists all the inputs that failed the test, a report is sent to the alarm monitoring company and an email is sent to the manager for each input that failed to activate during the test.

### Manual Testing

Manual testing allows inputs to be tested without changing the state of the Alarm Zone.

A staff member or technician will be able to put areas of the system into Test Mode whilst tests are carried out. The terminal will indicate if the input is functioning correctly and no alarm will be raised during this time.

### Mask Testing

Mask Testing raises an alarm for inputs that haven't been activated within a specified period of time. The intention of this test is to identify any devices that are not working, (e.g. PIRs or door sensors).

When a configured input hasn't been activated at least once within the period of time an alarm will be raised, a message will be sent to the alarm monitoring company and an email will be sent to the manager.

### Seismic Detector Testing

Vibration devices and seismic detectors can be used to detect vibrations and/or possible attacks, (e.g. drilling or similar in a bank vault). The Controller will trigger the vibration devices that will then trigger the seismic detectors. A failed test is one where the Controller triggers the vibration devices and the seismic detectors fail to detect it. Any failed tests will raise an alarm, be reported to the alarm monitoring company and emailed to the manager.

Alarms from the seismic detectors will not be raised during testing.

### Restricted Disarming

It is possible to configure groups of staff members within the Alarm Zones they are allowed to disarm and the times they can disarm them for, (e.g. cleaners).

### Timed Disarm

It is possible to configure groups of staff members with the period of time they are allowed to disarm Alarm Zones for.

### Remote Arming and Disarming

It is possible for the system to be remotely armed or disarmed by the alarm monitoring company.

### Auto-Processing Alarms

This feature allows Command Centre to automatically process all alarms that are both inactive and acknowledged. This service can be switched On or Off as required. (By default the service is Off.)

### Multi-Break Alarms

It is possible for an input to send an alarm to the alarm monitoring company every time it transitions. When the input is sealed again, a restoral event is sent.

Alternatively, it is possible to latch alarm inputs that are sent to the alarm monitoring company. This means that only one alarm will be sent to the alarm monitoring company per input and the restoral event will not be sent until the alarm is acknowledged.

# Configuring Inputs for Test Modes

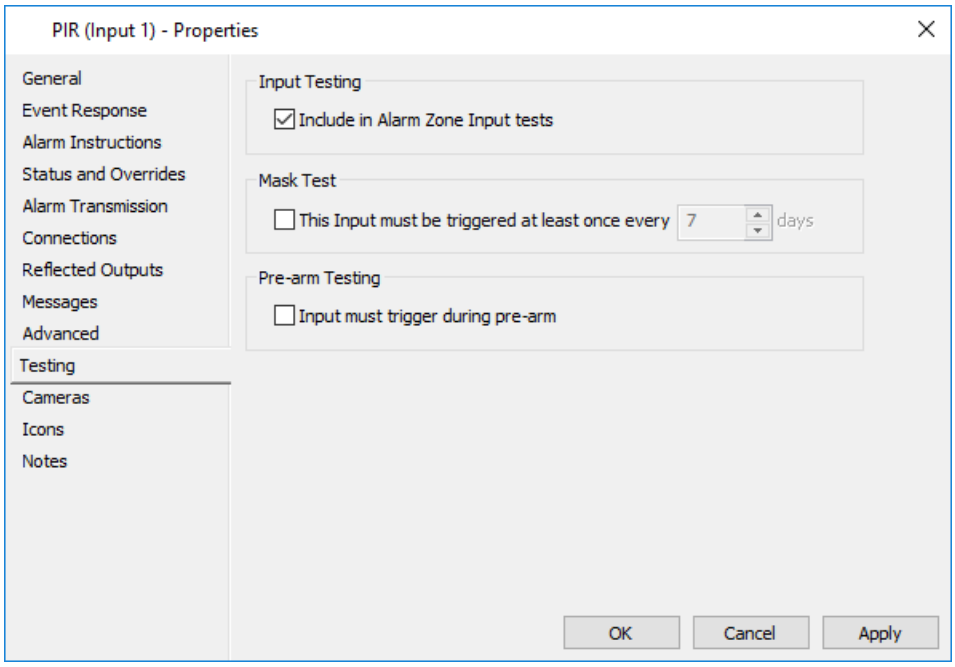
## Introduction

This procedure describes how to configure each input that requires testing.

**Note:** The normal state of all inputs should be 'closed'. If an input is 'open' you will need to reverse the state of the input, by checking the Input is inverted checkbox on the **Advanced** property page for the input.

## Procedure

1. Click **Configure** from the menu bar, then **Hardware**.
   The **Hardware** List Window opens (in tree view).
2. **Right click** on the appropriate Input and select **Properties**.
3. Click the **Event Response** tab.
4. If the input requires a visual indication that it is working, (e.g. a light turns on when the input is activated) assign an Action Plan to the Open/Off Event Group.
   This Action Plan will need to trigger the light when the input changes state.
5. Assign a primary Alarm Zone for all events from the drop-down list.
6. Click the **Testing** tab.




7. If the input requires periodic or manual testing, check the **Include in Alarm Zone Input tests** checkbox.
   The input will be included in all periodic and manual tests.

8. If the input requires mask testing, check the **This Input must be triggered at least once every X days** checkbox and enter the number of days the input must be activated within.
   (Default = 7 days. Configurable from 1 to 30 days.)
9. If the input is a seismic detector, check the **Input must trigger during pre-arm** checkbox.
10. Click the **OK** button to exit and save your changes.
11. Repeat this procedure for each input that requires testing.

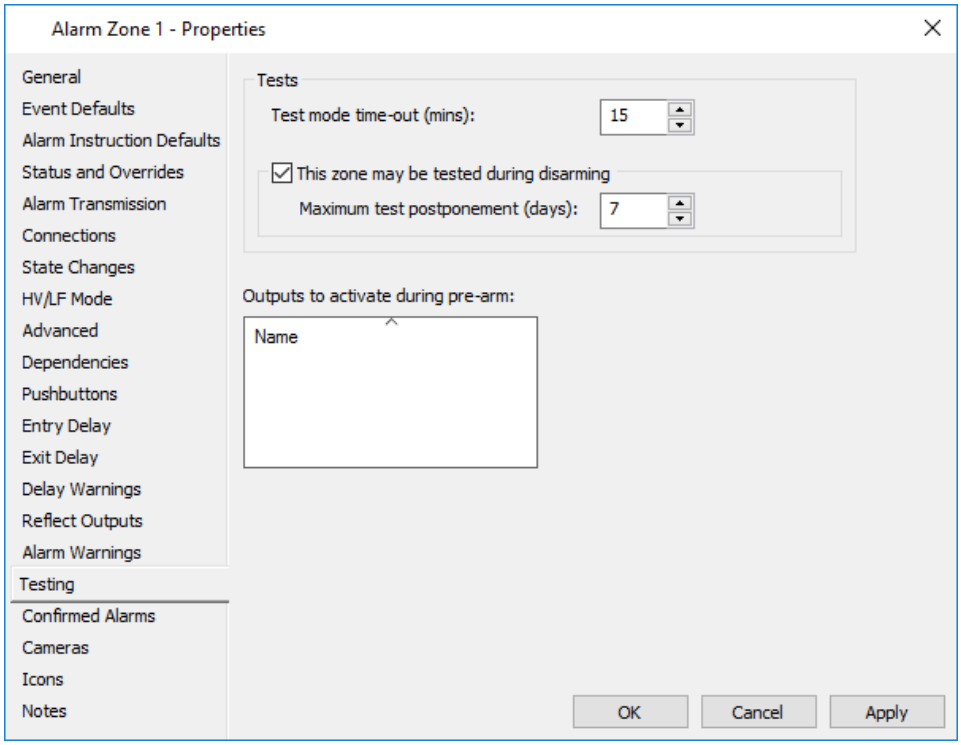
## Configuring Alarm Zones for Test Modes

### Introduction

This procedure describes how to configure each Alarm Zone that requires testing.

### Procedure

1. Click **Configure** from the menu bar, then **Alarm Zone**.
   The **Alarm Zone** List Window opens (in grid view).
2. **Right click** on the appropriate Alarm Zone and select **Properties**.
3. Click the **Testing** tab.




4. In the **Test mode time-out** field, enter the number of minutes required to complete the test.
   (Default = 15 minutes. Configurable from 1 to 60 minutes.)

   In the example above, the test will timeout after 15 minutes.

   The time left will be displayed as a countdown on the terminal. An audible warning will sound with one minute to go and the staff member will be given the opportunity to extend the testing time.

   When the test is extended, the time to complete the test will revert back to the original time period configured. The test can be extended multiple times.
5. Check the **This zone may be tested during disarming** checkbox.

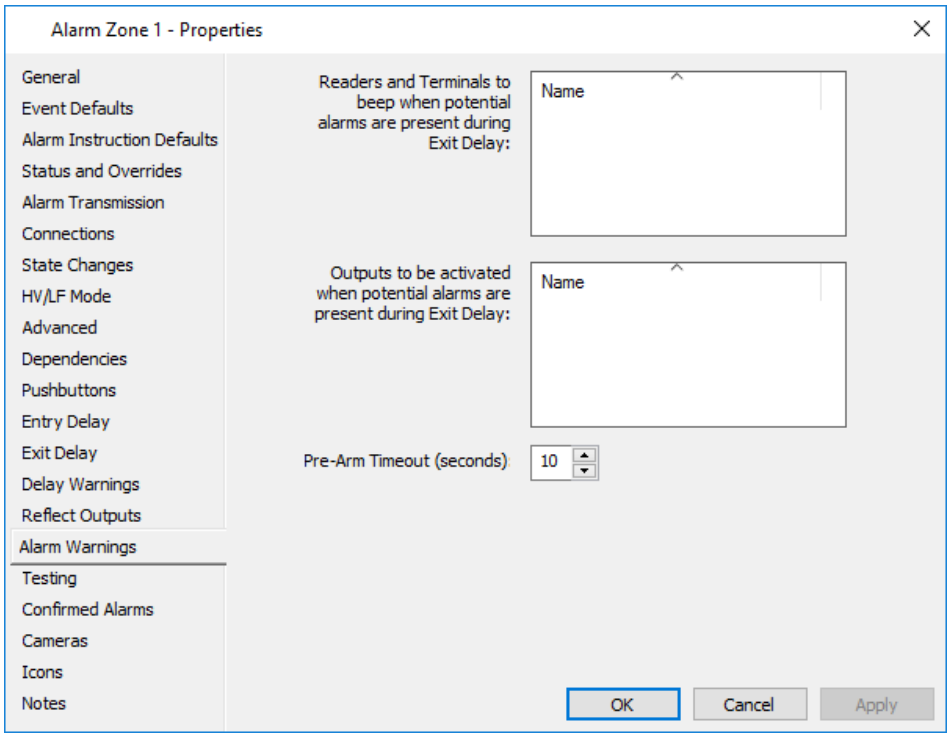
6. In the **Maximum test postponement** field, enter the maximum number of days that can pass before a mandatory test is required.
   (Default = 7 days. Configurable from 1 to 30 days.)

   In the example above, after 7 days the test is no longer optional.

7. Does the Alarm Zone contain vibration devices?
   If **yes**, go to Step 8.
   If **no**, go to Step 11.

8. Drag and drop Drag and drop the vibration devices (outputs) you require to trigger during the pre-arm timeout period into the grid.
   **Note:** These outputs must be set to pulse when triggered.

9. Click the **Alarm Warnings** tab.




10. In the **Pre-Arm Timeout** field, enter an appropriate period that you want Controllers to ignore alarms for, (i.e. 0-60 seconds).
    **Note:** The pre-arm timeout period will need to allow enough time for the vibration devices to settle before any alarms are raised. A pre-arm timeout value of approximately 10 seconds is suggested.

11. Click the **OK** button to exit and save your changes.

12. Repeat this procedure for each Alarm Zone that requires testing.

## Configuring Access Groups for Test Modes

### Introduction

This procedure describes how to configure the Access Groups you require for testing.

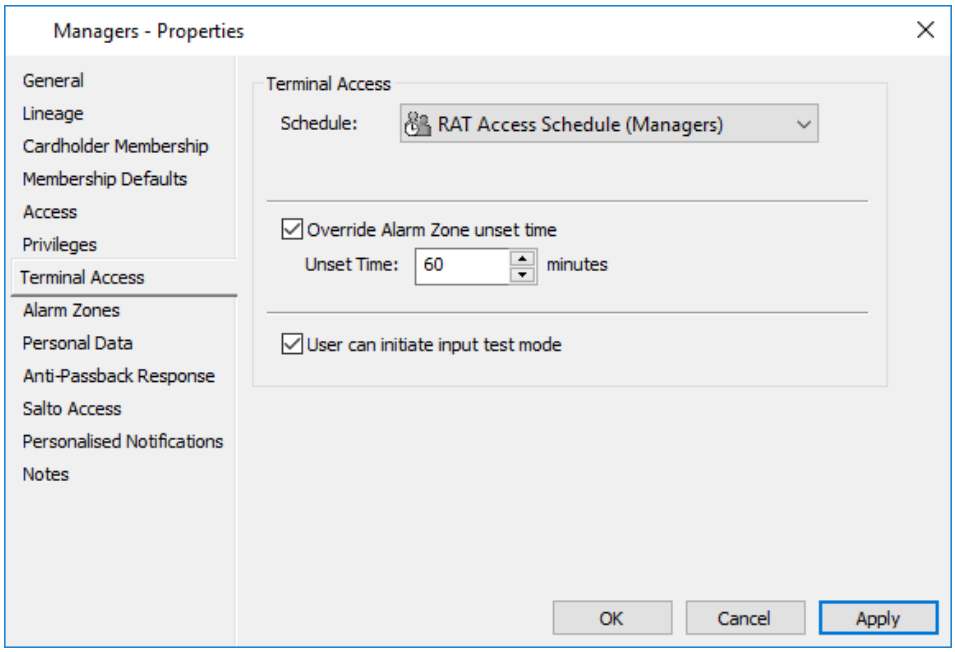
It is possible to configure groups of staff members with the Alarm Zones they are allowed to disarm and the times they can disarm them for.

It is also possible to configure groups of staff members with the period of time they are allowed to disarm the Alarm Zones for.

### Procedure

1. Ensure the following information has already been set up:
   *Divisions*
   Refer to **Setting up System Division** (on page 9-3).
   *Cardholders*
   Refer to **Add New Cardholder** (on page 32-2).
   *Schedules*
   Access Schedules = relating to cardholders
   Access Zone Schedules = relating to how the doors within the zone behave
   Refer to ***Schedules*** (on page 12-1).
   *Access zones*
   Includes a linked Access Zone Schedule
   Refer to ***Adding a new Access Zone*** (on page 10-3).
   *Personal Data Fields*
   Refer to **Creating a new Personal Data Field** (on page 33-2).
2. Click **Manage** from the menu bar, then **Access Groups**.
   The **Access Group** List Window opens (in tree view).
3. **Right click** on the appropriate Access Group and select **Properties**.
4. Click the **Cardholder Membership** tab.
5. Click **Manage** from the menu bar, then **Cardholders**.
   The **Cardholder** List Window opens.
6. Select the Cardholders who are required to perform input tests.
   Drag and drop them into the **Cardholder Membership** tab.
7. Close the **Cardholder** List Window.
8. Click the **Privileges** tab.
9. Check the **Change to the Disarmed state** checkbox.

10. If Cardholders are required to arm Alarm Zones associated with any Access Zone associated with this Access Group, check the **Change to the Armed state** checkbox.
11. If Cardholders are required to select an Alarm Zone to test on the terminal, check the **Prompt for alarm zone selection** checkbox.
12. Click the **Terminal Access** tab.




13. Select the appropriate **Cardholder Access Schedule** for this Access Group. This schedule will control when the Cardholder can access the terminal.
14. Check the **Override Alarm Zone unset time** checkbox and enter the period of time you require the Alarm Zones to be unset. (Default = 60 minutes) This time will override the Alarm Zone unset time for all Alarm Zones associated with this Access Group, when unset from the terminal only.
    **Note:** If an Alarm Zone unset time is greater than the configured override unset time, the Alarm Zone will be reset at the time specified by the override.
15. Check the **User can initiate input test mode** checkbox.
    Cardholders belonging to this Access Group will able to perform input tests.
16. Click the **Alarm Zones** tab.
17. Click **Configure** from the menu bar, then **Alarm Zones**.
    the **Alarm Zone** List Window opens.
18. Select the Alarm Zones that the members of this Access Group are authorised to test.
    Drag and drop them into the **Alarm Zones** tab window.
19. Close the **Alarm Zone** List Window.
20. Click the **OK** button to exit and save your changes.

## Configuring Cardholders for Test Modes

You will need to configure Cardholders to log on to the terminal, either using a separate card reader or using a user code.

For details on how to configure a user code for a Cardholder, refer to ***Configuring User Codes for access at Card Readers with keypads*** (on page 32-25) for the procedure.

## Configuring terminals for Test Modes

You will need to add the Alarm Zones containing the test inputs to the terminals. Cardholders will then be able to perform input tests for these zones using the terminals.

For details on how to associate an Alarm Zone with an HBUS Terminal, refer to ***Configuring an HBUS Terminal*** (on page 21-54).

For details on how to associate an Alarm Zone with an HBUS Alarms Only Terminal, refer to ***Configuring an HBUS Alarms Only Terminal*** (on page 21-70).

## Configuring Event/Alarm Notifications for Test Modes

You will need to configure Event/Alarm Notifications for the Manager. The Notification Filter assigned to the Manager will need to include the following Event Groups:

- Test Events
- Point Not Tested
- Input Not Activated

For details on how to configure Event/Alarm Notifications, refer to ***Notifications*** (on page 6-47) for the procedure.