



# GuardPoint 10 Users Guide

Version 1.80



**Setup**

**Security**

**Management**

© Copyright 2017 - 2022 Sensor Access. All rights reserved.

This document is the protected intellectual property of Sensor Access.

Information in this document is subject to change without notice.

The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Sensor Access.

Document version: 1.80.01



# CONTENT

## CHAPTER 1: Welcome to GuardPoint10 Online Help

GuardPoint10 Installation & Maintenance .....	2
Getting familiar with the GuardPoint10 console .....	28
Roadmap to Site Building .....	33
GuardPoint10 API Center .....	34
MultiSite Implementation also includes a MultiCompany solution .....	34
GuardPoint10 WebApp .....	36

## CHAPTER 2: Infrastructure

Initial Setup .....	38
Controller Activation Wizard .....	40
Edit/Delete a Site Item .....	41
Installing a MultiSplit .....	43
Adding a New Network .....	49
Edit/Delete a Network .....	50
Adding a New Controller to a Network .....	51
Understanding the Lift Setup concept in GuardPoint10 .....	53
Understanding and setting up an ELSGW Lift in GuardPoint10 .....	56
Edit/Delete a Controller .....	59
Adding a New Reader to a Controller .....	60
Adding a New Biometric Reader to a Controller .....	62
Adding a Slave Reader to a Controller .....	64
Edit/Delete a Reader .....	67
Managing a Mantrap .....	69
Adding a Mantrap .....	72
Adding a New Input Device to a Controller .....	73

Edit/Delete an Input Device .....	74
Adding a New Relay to a Controller .....	75
Edit/Delete a Relay .....	76
Adding a New Local Reflex to a Controller .....	77
Edit/Delete a Local Reflex .....	78
After the Infrastructure is Setup, What's Next? .....	79
Understanding Anti-passback in GuardPoint10 .....	80
Integrating a Galaxy System into the Infrastructure .....	82
Configuring a Galaxy system panel .....	83
Infrastructure: MultiSite Impact .....	87

### CHAPTER 3: Profiles

Adding a New Profile .....	92
Duplicating a Profile .....	94
Assigning Multiple Access Groups to a Profile .....	96
Editing a Profile's Details & Authorizations .....	97
Deleting a Profile from the System .....	100
Profiles: MultiSite Impact .....	101

### CHAPTER 4: Operators (Users)

Adding a New Operator .....	104
Editing an Operator's Details .....	105
Attaching a Cardholder to Operator Details .....	106
Attach Active Directory Credentials to User .....	108
Deleting an Operator from the System .....	110
Operator (User): MultiSite Impact .....	111

### CHAPTER 5: Time Zones

Daily Program Time Zones .....	114
Weekly Program Time Zones .....	120
Time Zones Holiday & Special Day .....	130
Time Zones: MultiSite Impact .....	136

### CHAPTER 6: Access

Access Groups .....	140
Multiple Access Groups .....	156
Temporary Access .....	168
Access: MultiSite Impact .....	174

### CHAPTER 7: Badges

Changing the Badges Table View .....	176
Manage the Badges Table Layout with Templates .....	177
Adding New Badges .....	178
Adding Multiple Badges where the Badge Code is Sequential .....	180
Assigning a Badge to an Existing Cardholder from the Badges Screen .....	182
Assigning a Badge to a New Cardholder .....	183
Changing the Status of a Badge .....	185

Manually Assigning a Cardholder a Badge Template via the Badges Screen .....	186
Printing a Cardholder Badge via the Badges Screen .....	189
Deleting a Badge .....	190

## CHAPTER 8: Cardholders

Changing Cardholder Report Table View .....	194
Manage the Cardholder Table Layout with Templates .....	196
Adding a New Cardholder .....	196
Adding Customized Fields to Cardholder Details .....	199
Importing Cardholder Data .....	201
Duplicating a Cardholder .....	203
Add/Edit/Delete a Cardholder Type .....	205
Manually assigning a Cardholder a Badge Template via the Cardholders Screen .....	208
Assigning a Preexisting Multiple Access Group to a Cardholder via the Cardholders Screen .....	211
Manage a Cardholder's Door Access Group assignment from the Cardholders screen - Without a Multiple Access Group .....	212
Enrolling / Deleting a Cardholder's Biometric Sample .....	214
Editing Cardholder Details .....	216
Creating and Assigning a New Multiple Access Group in a Single Cardholder Operation .....	219
Assigning a Badge Code to an Existing Cardholder from the Cardholders Screen .....	221
Printing a Cardholder Badge via the Cardholders Screen .....	223
Changing the Status of Cardholders .....	224
Generating a Cardholders Report Output (PDF, Excel, or Print) .....	226
Cardholder: MultiSite Impact .....	227

## CHAPTER 9: Departments

Editing Department Details .....	229
Assigning a Department to a Cardholder .....	232
Deleting a Department .....	233
Departments: MultiSite Impact .....	234
Departments: MultiSite Impact .....	235

## CHAPTER 10: Options

Changing Option settings .....	237
Restoring Default Options Settings .....	238
System Database and Journal Management Options .....	239

## CHAPTER 11: Video (Setup) and NVR/DVR

Configuring a Video NVR/DVR connection .....	244
Configuring & Editing the Video Logic Tree .....	245
Video Setup: MultiSite Impact .....	249

## CHAPTER 12: Event History

Load and View a Previously Archived Journal .....	252
Manage the Cardholder Table Layout with Templates .....	253
Changing Event History Report Table View .....	254

Generating Event History Report Output (PDF, Excel, or Print) .....	254
<b>CHAPTER 13: Time &amp; Attendance</b>	
Generating a Timesheet Report & Exporting the Report .....	258
<b>CHAPTER 14: Position</b>	
Managing a Map Tree .....	263
Add and Manage Customized Palettes .....	267
Create XAML icons for Custom Palettes .....	269
Adding a New Icon to a Custom Palette .....	272
Edit or Delete an Icon in a Custom Palette .....	276
Position: MultiSite Impact .....	278
What to Know About Designing a Map Page .....	279
<b>CHAPTER 15: Badge Templates</b>	
Adding a Badge Template .....	294
Editing an Existing Badge Template .....	295
Deleting a Badge Template .....	300
<b>CHAPTER 16: Alarm Zones (Setup)</b>	
Adding a New Alarm Zone .....	302
Editing / Deleting a Galaxy Group or Zone .....	305
How to delete a zone from a Galaxy Group .....	306
How to edit a zone in a Galaxy Group .....	307
Deleting an Alarm Zone .....	307
Adding a New Galaxy Group .....	307
Adding a Galaxy Zone to a Galaxy Group .....	308
Editing / Deleting a Galaxy Group or Zone .....	310
How to delete a zone from a Galaxy Group .....	311
How to edit a zone in a Galaxy Group .....	312
Alarm Zone Setup: MultiSite Impact .....	313
<b>CHAPTER 17: Area</b>	
Adding a New Area .....	316
Adding a Global Anti-passback Area .....	318
Editing an Area .....	319
Deleting an Area .....	319
Area Setup: MultiSite Impact .....	320
<b>CHAPTER 18: Report Templates</b>	
Handling Report Template .....	322
Report Templates: MultiSite Impact .....	323
<b>CHAPTER 19: Global Reflex</b>	
Adding a New Global Reflex .....	326
Adding a Global Reflex Manual Event .....	328
Enable / Disable Strategy for a Global Reflex .....	330

Deleting a Global Reflex .....	330
Global Reflex: MultiSite Impact .....	331
<b>CHAPTER 20: Dashboard</b>	
Dashboard Content & Actions .....	334
<b>CHAPTER 21: Diagnostics</b>	
Checking Controller Communications .....	342
Reset a Controller .....	343
Activate/Deactivate a Controller .....	343
Override a Normal Door Relay State .....	344
Overwrite a Controller's Local Data .....	345
Send Selective Data to a Controller's Local Database .....	346
Clearing Memory in a Controller .....	347
Diagnostic: MultiSite Impact .....	348
<b>SECURITY TASKS</b>	
<b>CHAPTER 22: Security Tasks: MultiSite Impact</b>	
<b>CHAPTER 23: Display Events Screen</b>	
Managing Events from an Event Card in the Display Events Screen .....	354
<b>CHAPTER 24: Event Log Screen</b>	
Managing the Events Table Log .....	358
<b>CHAPTER 25: Display Photo</b>	
Working with the Display Photo Window .....	362
<b>CHAPTER 26: Alarm Zones (Security)</b>	
Overriding an Alarm Zone's Status .....	366
Canceling a Temporary Override .....	368
Canceling Any Override, Where the Alarm Zone Is Assigned a Weekly Program (WP) .....	369
Changing the setting of a Galaxy Group or Zone .....	370
Managing a Galaxy Zone Alarm .....	371
<b>CHAPTER 27: Video (Security)</b>	
Configuring the Video Panel .....	374
Managing Tile Content .....	377
Managing Access/Alarm Event Log .....	379
Managing a Video Tab & Tab Bar .....	380
Sharing a Video Tab Configuration .....	382
Overriding a Door's Lock/Unlock State .....	383
Overriding an Alarm Zone's Status from the Video Security Screen .....	385
Handling an Alarm Event in the Video Security Screen .....	387
Play a Playback from a Log Entry .....	388
Perform a Playback from a Specific Date and Time .....	388

## CHAPTER 28: Security Center

Opening a Map Page .....	390
Changing the Map Page View .....	390
Addressing Alarms via a Security Center Icon .....	391
Accessing Alarm Zone Details Via a Miscellaneous Icon, Shape, and Textbox .....	394
Managing an Object's Status from a Map Page .....	395
Managing an Alarm from an Alarm Card .....	397
Monitoring Areas on a Map Page .....	399

## CHAPTER 29: Area Roll Call

Manually Change a Cardholder's Area .....	402
Generating Area Roll Call Report Output .....	403

## CHAPTER 30: T&A Roll Call

Generating T&A Roll Call Report Output .....	406
--	-----

## CHAPTER 31: Visitor Control Management

Visit .....	410
Meeting .....	410
Reports .....	410
VM Visitor .....	411
VM Meetings .....	422

## CHAPTER 32: From the Dashboard: License, Help, and About

## APPENDIX A: Screen Descriptions

Infrastructure Screen Views: Tree and Table .....	438
Setup Wizard: Site -> Network -> Controllers .....	440
Site Details .....	443
Network Details .....	445
Controller Details .....	450
Reader Details .....	453
Reader Table .....	474
Input Device Details .....	476
Input Device Table .....	480
Relay Details .....	485
Relays Table .....	488
Local Reflex Details .....	490
Local Reflex Table .....	492
Galaxy Panel Details .....	494
Galaxy Zone Table .....	496
Zone Details .....	499
Time Zone Daily Program .....	501
Time Zone Weekly Program .....	503
Time Zone Holidays & Special Days .....	505
Access Groups Screen .....	506
Video Setup Screen .....	519



Alarm Zone Setup Screen .....	521
Area Screen .....	525
Report Template Screen .....	529
Global Reflex Screen .....	532
Position Screen .....	554
Badge Templates Screen .....	564
Options Screen .....	567
Diagnostic Screen .....	584
Badges Screen .....	597
Cardholders Screen .....	600
Operator (User): MultiSite Impact Cardholder Details .....	607
Profiles Screen .....	620
Users Screen .....	627
Departments Screen .....	630
Event History Screen .....	631
Time & Attendance Screen .....	641
Visitor Control Web Application .....	645
Display Events Screen .....	657
Events Log Screen .....	659
Display Photo Screen .....	661
Alarm Zone Security Screen for GuardPoint10 Alarm Zones .....	662
Alarm Zone Security Screen for Galaxy Groups .....	664
Video Security Screen .....	667
Video NVR/DVR Screen .....	678
Security Center Screen .....	680
Area Roll Call Screen .....	686
T&A Roll Call Screen .....	690
License, Help, and About .....	693

## APPENDIX B: Table Filters

## APPENDIX C: Escort Rules for Access Events

## APPENDIX D: Hardware Information

Hardware Installation .....	700
Common Controller Features .....	704
Controller Comparison Tables .....	705
Controller ROM Versions Table for Different Door/Reader Configurations .....	709
Convention for Reader Transaction Codes .....	710
Controller Support for Readers, Inputs, and Outputs .....	711
Default Connections for Inputs, Relays, and RTX .....	712

## INDEX

## FAQ

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 1:

## Welcome to GuardPoint10 Online Help

The Place to Find Information, Instruction, FAQs, and More

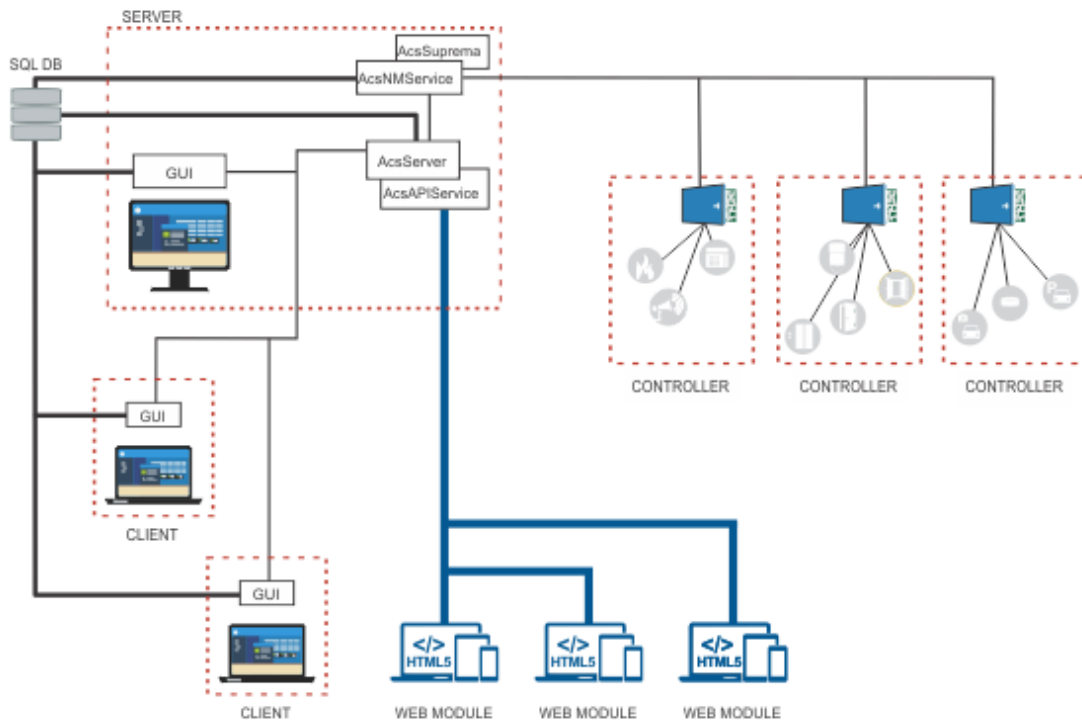
# GuardPoint10 Installation & Maintenance



**Warning:** All GuardPoint10 installations should be performed by a qualified installer. For additional information, contact your GuardPoint10 vendor.

Before describing the installation process and steps, it is important to have a general understanding of the GuardPoint10 system architecture.

Figure 1-1



There are three parts to the GuardPoint10 system architecture:

» **Server PC:** This includes the GPPServer and the AcsNMService services and, in most cases, a GUI operator access point. The Server PC communicates with the SQL database, all Client PCs, and controllers.

- **GPPServer service:** The application service updates/fetches information from the SQL database and downloads/uploads data to the AcsNMService service.

This GPPServer service works all the time, even when the GUI is closed. It implements user requests behind the scenes, refreshes GUI(s), and enables integration with external systems.

- **AcsNMService service:** Communicates with controllers, performs polling, and releases other parts of the system to deal with other tasks in parallel.

The AcsNMService service downloads the cardholder data and definitions to the controllers and uploads the events to the GPPServer service, where it is then sent to the GUI installations.

Third-party systems communicate with GuardPoint10 via the AcsNMService service. The AcsNMService service receives third-party system events (i.e. via the AcsSuprema service for Suprema biometric data) and sends them to the GPPServer service where the event data is incorporated into the GuardPoint10 system data.

The AcsSuprema service is dependent on the AcsNMService service. If the AcsNMService service is started or stopped, the AcsSuprema service is automatically started or stopped.

The AcsNMService service works all the time and may communicate with multiple networks simultaneously.

- **GUI:** A user-friendly desktop interface application. It includes a flexible and modern design with rich graphics, and displays complex data in a simple and intuitive way.

Multiple GUIs (theoretically unlimited) can run on different machines simultaneously. Data updates will appear on all opened GUIs at runtime.

- » **SQL Database:** The SQL Database stores system information. It may be installed on any machine with access to the Server PC and the Client PCs. In addition, there is an option to include an SQL Server on the same machine as the SQL Database.

This installation includes an SQL Server installation option.

- » **Client PC:** A thin client that includes a GUI installation and communicates primarily with the GuardPoint10 Server PC. For very specific operations (i.e. report generation and batch processing), a Client PC also communicates directly with the SQL Database.

An independent Client PC is not required to access the GuardPoint10 application, the Server PC's GUI can stand alone as an operator access point.

## Prerequisites

### SQL Server Prerequisites:

GuardPoint10 supports MS SQL SQL 2016 SP1 or later.

### Server on a Host Server machine prerequisites

Table 1-1 Host Server machine prerequisites

Item	Requirement
Processor	Intel Xeon E3-1270 v5, 3.60GHz, 8 Cores, 8MB Cache or compatible
Memory	8GB RAM
Hard drive	Solid State Drive (SSD) with 20GB of free space
Graphics hardware	If the GUI is not used, a graphics device and monitor are optional
Network Interface Card	Ethernet adapter capable of at least 100Mbit throughput

Item	Requirement
Operating system	Microsoft Windows Server 2012 R2 or later
Available TCP ports	7654, 4567, 4568, 8765, 5678, 5679, 49999

## Server or Client on a PC prerequisites:

*Table 1-2 Server / Client on a PC prerequisites*

Item	Requirement
Processor	Intel Core i7-6700, 3.4GHz, 8 Cores, 8MB SmartCache or compatible
Memory	8GB RAM
Hard drive	Solid State Drive (SSD) with 20GB of free space
Graphics hardware	Graphics device and monitor capable of Full HD (1920 x 1080) or higher
Network Interface Card	Ethernet adapter capable of at least 100Mbit throughput
Operating system	Microsoft Windows 10 version 1909 or higher
Available TCP ports	Server: 7654, 4567, 4568, 8765, 5678, 5679, 49999 Client: 4568, 5679

## Visitor web application PC (without GuardPoint10) prerequisites:

*Table 1-3 Visitor web application prerequisites*

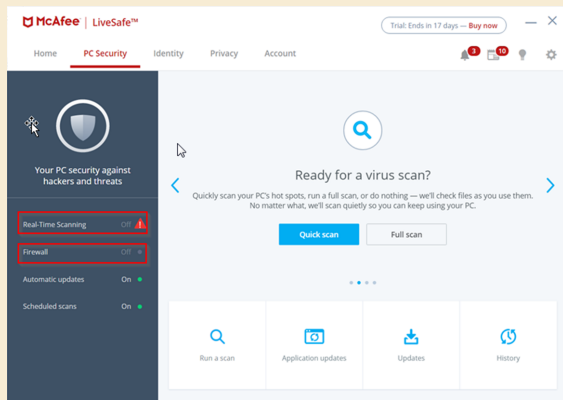
Item	Requirement
Graphics hardware	Graphics device and monitor capable of Full HD (1920 x 1080) or higher
Network Interface Card	Ethernet adapter capable of at least 100Mbit throughput
Browser	An up-to-date version of Chrome

## GuardPoint10 WebApp (without GuardPoint10) prerequisites:

Modern web browser and a connection to the GuardPoint10 server installation.

# First-Time Installation of GuardPoint10

**Note:** If McAfee™ Antivirus is installed on the computer, you MUST turn off Real-Time Scanning and the firewall via McAfee LiveSafe interface BEFORE launching the GuardPoint10 setup.



**Note:** Some antivirus software may corrupt the GuardPoint10 installation. A best practice is to pause the antivirus until the installation is successfully completed.

1. If you are about to install GuardPoint10 in Server mode, to support the Visitor web page, the IIS (Internet Information Services) must be set on the Server machine before installing GuardPoint10. See "[IIS \(Internet Information Services\) installation](#)" on page 11.
2. After you receive the GuardPoint10 EXE file, save the GuardPoint10 installation file to the desktop on the computer where the installation will take place.
3. From the desktop, launch the EXE file. The installation wizard begins.
4. Enter the "Param Code" sent to you by your provider.
5. Accept the terms of the license. The Welcome screen appears.



6. From the wizard's Welcome screen, click one of the following options:

- » **Full Installation:** This is the GuardPoint10 default Server installation. It will link to the SQL Server bundled in the installation EXE file and install the SQL Server on the same computer as the Full Installation.
- » **Workstation:** This is the default Client installation. It will communicate with the GuardPoint10 Server and the SQL Server. A Client may be installed only after the Server has been installed.
- » **Advanced:** Press this button if you want to change the default application folder, or if you want to connect to an existing SQL Server.

### Server Installation (default)

After clicking Full Installation in Step 6 above, GuardPoint10 will automatically start the installation process. When the installation has successfully completed, GuardPoint10 specific files will be found in

`C:\Program Files (x86)\GuardPoint10` and `C:\ProgramData\ACS`

on the PC where GuardPoint10 was installed.

In addition to the GuardPoint10 software, the installation process will also install the SQL Server Express 2016 with two databases designated for the GuardPoint10 system.

After the installation has successfully completed, restart the computer.

### Server Installation (advanced)

After clicking Advanced in Step 6 above, the following window is displayed:



Figure 1-2



Select **Full Installation**.

- » To change the default application folder, click **Browse** to select the folder where the installation will take place.

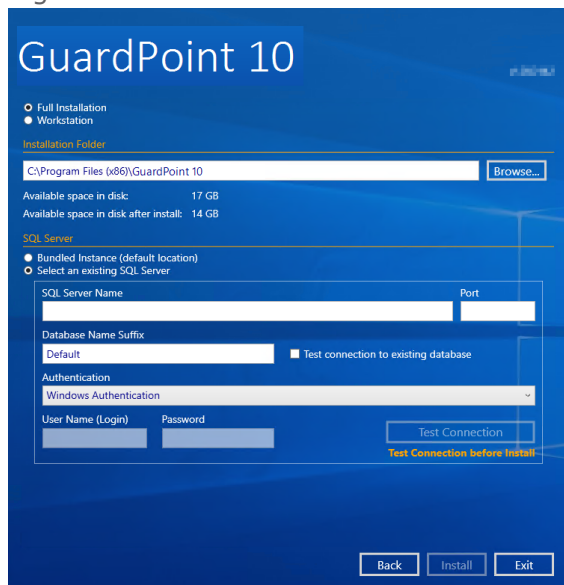
The sub-folder name will be "GuardPoint10". For example, if you browse to "D:\My Installation\" in the Installation Folder field, GuardPoint10 will be installed in "D:\My Installation\GuardPoint10\".

Figure 1-3



- » To install the GuardPoint10 databases on an existing SQL Server, in the SQL Server area, click **Select an existing SQL Server**. Options for selecting a new location will be displayed.

Figure 1-4



Make sure the existing SQL Server is running before continuing.

Enter the **SQL Server Name**, the **Port**, and the **Database Name Suffix** that will be appended to the name of the GuardPoint10 databases.

If the GuardPoint10 databases already exist, select **Test connection to existing database**. Finally, select the **Authentication** type, and if necessary, enter the relevant **User name** and **Password**.

Click the **Test Connection** button and make sure that the connection is established successfully. If the **Test connection to existing database** checkbox was left unchecked, the connection to the existing SQL Server is tested. If this checkbox was selected, the connection to the existing databases is also tested.

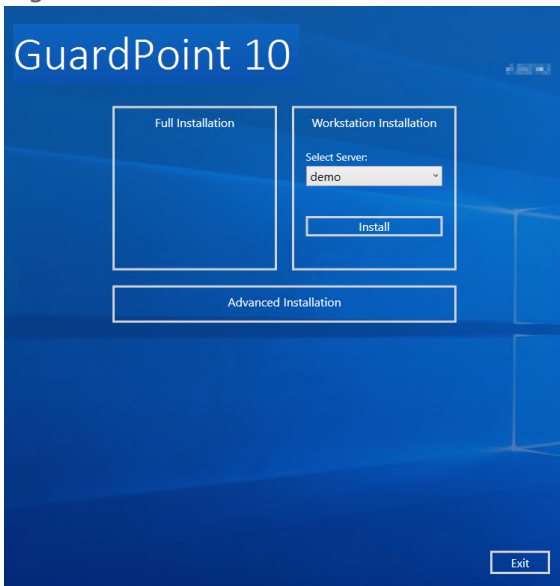
Click **Install** to start the installation process with the advanced parameters. After the installation has successfully completed, restart the computer.

### Client Installation (default)

**Note:** A Client may be installed only after the Server has been installed.

After clicking Workstation in Step 6 above, a list of GuardPoint10 Servers to which the Client may connect is created.

Figure 1-5



Select the relevant Server from the drop-down list and click Install.

The Workstation installation process starts.

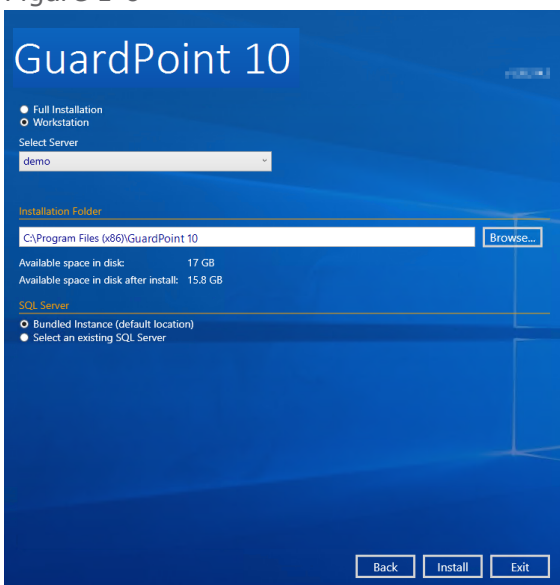
After the GuardPoint10 installation is successfully completed, click **Restart**. The PC restarts and the installation is ready for work.

**Note:** A site may have only one GuardPoint10 Server installation, but as many Client installations as the license permits.

### Client Installation (advanced)

After clicking Advanced in Step 6 above, the following window is displayed:

Figure 1-6



Select **Workstation**.

From the **Select Server** drop-down list, select the Server computer where the Client will connect.

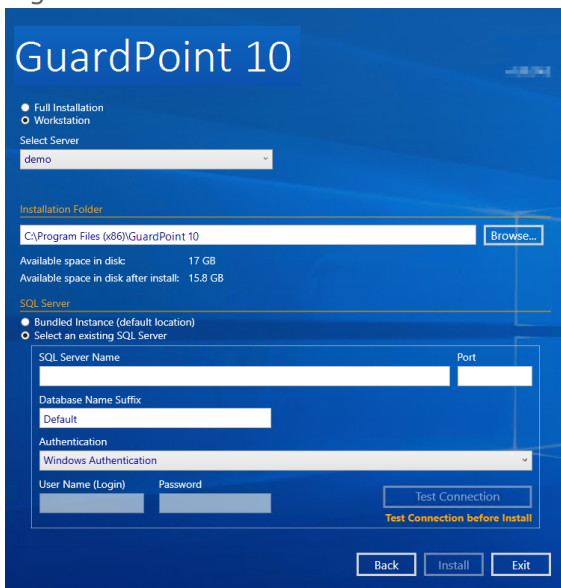
**Note:** Note: Initially, a Server search is performed before the Select Server field appears.

To change the default application folder, click **Browse** to select the folder where the installation will take place.

The sub-folder name will be "GuardPoint10".

- » If the SQL Server was installed during the Server installation, in the SQL Server area select **Bundled Instance (default location)**.
- » If the SQL Server was installed before the Server installation, in the SQL Server area click **Select an existing SQL Server**. Options for the SQL Server location will appear in the window.

Figure 1-7



Enter the **SQL Server Name**, the **Port**, and the **Database Name Suffix** that will be appended to the name of the GuardPoint10 databases. Finally, select the **Authentication** type, and if necessary, enter the relevant **User name** and **Password**.

Click the **Test Connection** button to make sure that the connection to the existing databases is established.


Click **Install** to start the installation process with the advanced parameters.

After the installation has successfully completed, restart the computer.

## Upgrade installation from GuardPoint10 version 1.10.152

1. Make sure the SQL Server is running.
2. After you receive the EXE file of the new GuardPoint10 version, save the GuardPoint10 installation file (the EXE file) to the desktop where GuardPoint10 will be upgraded.
3. From the desktop, launch the EXE file. The installation wizard begins.
4. Accept the terms of the license. The Welcome screen appears.

5. From the wizard's Welcome screen, click **Upgrade**. GuardPoint10 will automatically start the installation process. There is no difference if the existing installation is a Server installation or a Client installation. The GuardPoint10 folder locations will not change.
6. After the GuardPoint10 upgrade is successfully completed, click **Restart**. The computer restarts and GuardPoint10 is ready for work.



**Note:** If a pre 1.10.152 version of GuardPoint10 is running at your site and you need to retain the existing database, open a support ticket and our support team will provide you with an alternative installation process. This would be a one-time alternative installation; future updates will be automatic via the installation wizard.


## Update installation GuardPoint10

### Installing an update:

- » Install the new version (update) using the installation instructions above, just click **Upgrade** in the Installation wizard's Welcome screen.

There is no need to uninstall the older version. The new version will update your existing GuardPoint10 application and, if necessary, update your system database schema.


The initial installation should always be the Full Server installation followed by the Workstation Client installations.



**Note:** The GuardPoint10 GUI application from a previous installation may not work with a new GuardPoint10 server installation. Therefore, a best practice is to perform all of the installations in a relatively short time.

If an update includes a new module or a new feature in an existing module, after installing the new update of GuardPoint10's Server application, check the Profiles screen authorizations for each listed profile and make any necessary adjustments.

For information about the Profiles, see ["Profiles" on page 91](#).



**Note:** If you experience system anomalies after an GuardPoint10 update, do the following:  
Re-initialize your controllers.  
Stop and restart GuardPoint10 services via the Watchdog on the Server installation.

## IIS (Internet Information Services) installation

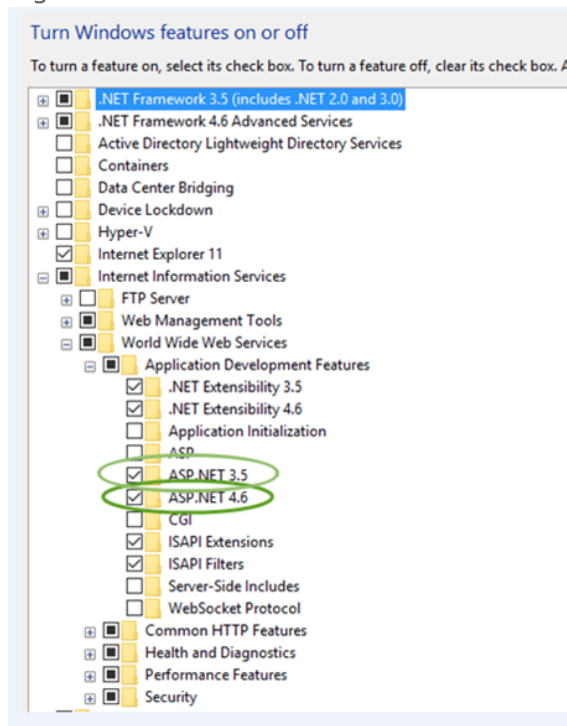
The IIS is required to support the GuardPoint10 Visitor web page. Ideally, IIS was configured before GuardPoint10 is installed (see ["Configure IIS" below](#)). When the IIS is configured before GuardPoint10 is installed, a default Visitor application is automatically added to the IIS during the GuardPoint10 installation.

If you've installed GuardPoint10 before configuring IIS, you will have to configure the IIS and then manually add the Visitor application to the IIS (see ["Manually Add the Visitor Application to the IIS" on the next page](#)).

### Configure IIS

1. In the Windows Start menu's search field, type **Turn Windows Features On or Off**.
2. In the search results list, click **Turn Windows Features On or Off**. The Turn Windows Features On or Off window is displayed.
3. In the Turn Windows Features On or Off tree, navigate to  
Internet Information Services / World Wide Web Services / Application Development Features
4. Select all of the **ASP.NET** version checkboxes under **Application Development Features**. When you do this, more checkboxes will be automatically selected, **do not uncheck these other checkboxes**.

Figure 1-8



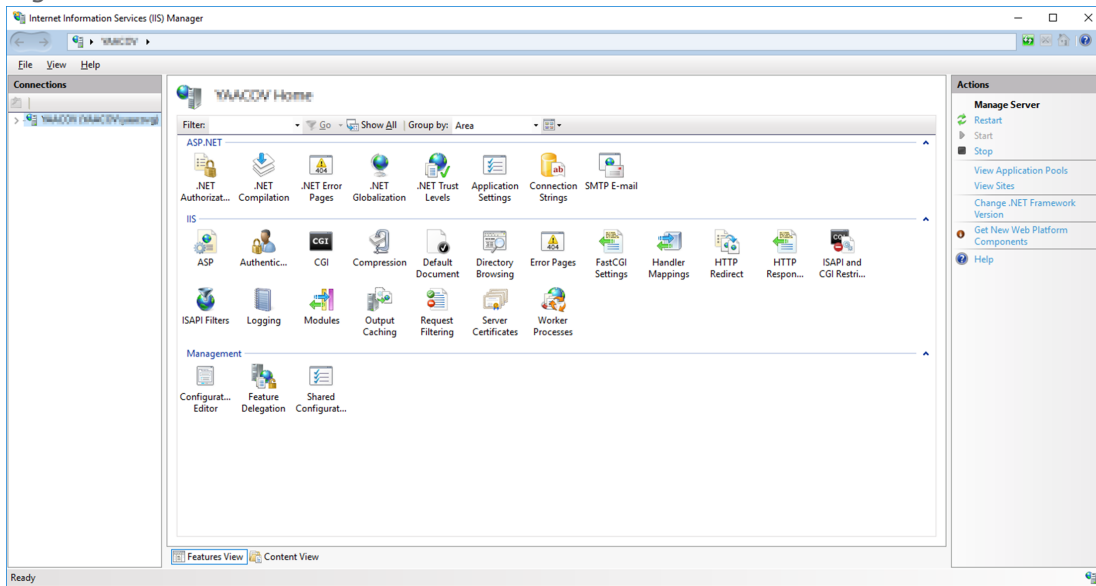
5. Under Common HTTP Feature, make sure that the **Static Content** checkbox is checked.
6. Click **OK**. After the Configuration is complete, you can continue to the GuardPoint10 installation. If GuardPoint10 has already been installed, manually add the Visitor application to the IIS (see ["Manually Add the Visitor Application to the IIS"](#) below).

### Manually Add the Visitor Application to the IIS

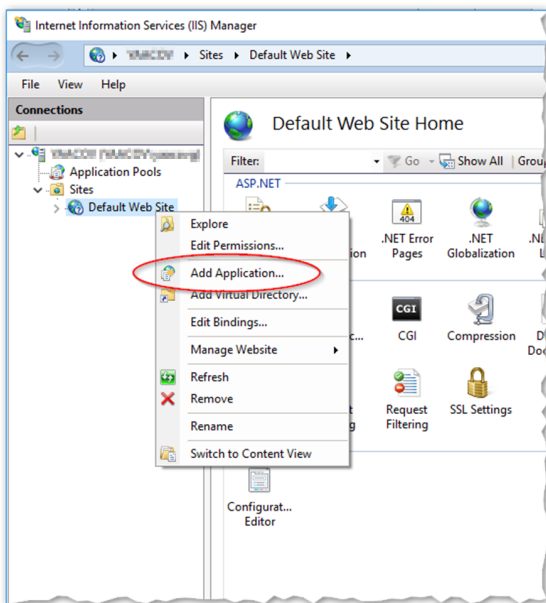
If IIS was configured before GuardPoint10 was installed, the Visitor application was added automatically to the IIS, via the GuardPoint10 installation. However, if you installed GuardPoint10 before configuring the IIS, you must manually add the Visitor application to the IIS.

1. If IIS is not configured yet, follow the instructions in ["Configure IIS" on the previous page](#).
2. In the Windows Start menu's search field, type **IIS**.
3. In the search results list, click **Internet Information Services (IIS) Manager**. The Internet Information Services (IIS) Manager window is displayed.

Figure 1-9



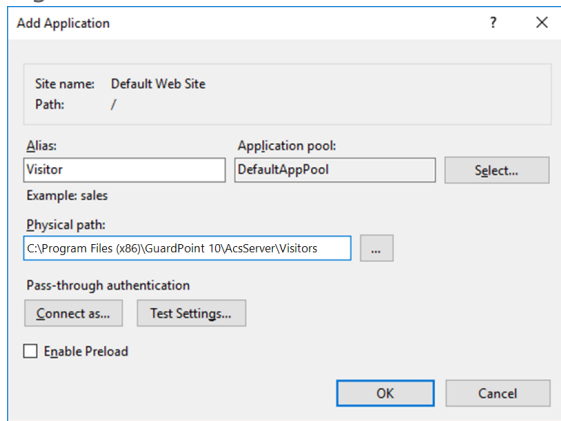
4. From the Connections tree, right-click Default Web Site and select Add Application. The Add Application window is displayed.



5. In the Add Application window enter the following:

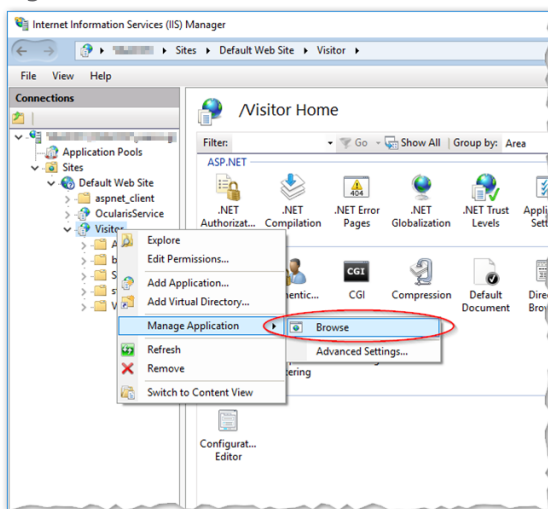
- » "Visitor" in the Alias field
- » "...\GuardPoint10\AcsServer\Visitors" in the Physical path field. This is the location of the Visitor folder that was added during the GuardPoint10 installation.

Figure 1-10



6. Click **OK**. Visitor appears in the Connections tree.
7. Test the Visitor application (web page) from the Connections tree by right-clicking Visitor > Manage Application > Browse.

Figure 1-11



The GuardPoint10 Visitor Control Login web page appears in your web browser.

The Visitor application is now operational. To access the GuardPoint10 Visitor web page from any browser, type the following address in the address bar:

`http://[SERVER NAME]/Visitors/`

where [SERVER NAME] is the name of the PC where the GuardPoint10 Server is located.

## Configurator

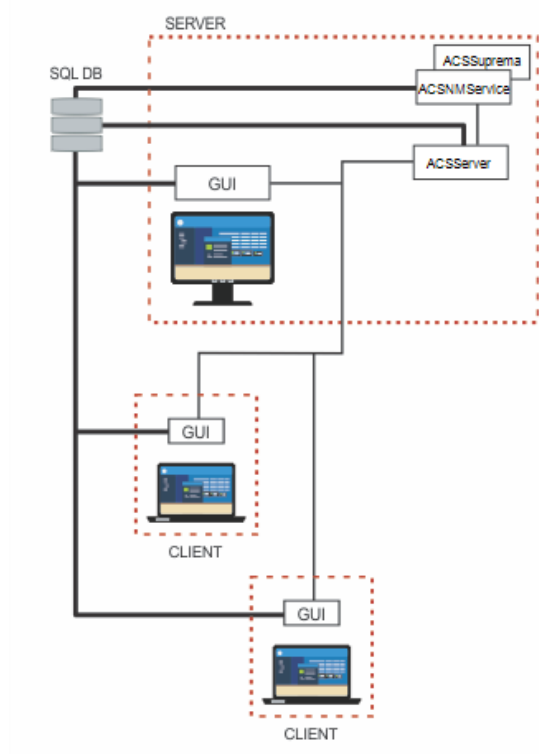
For standard installations, configuration settings are automatically set during the installation process. However, there may be situations where custom settings may be required. The Configurator provides you with a simple user-friendly interface designed to customize your GuardPoint10 configuration settings.

The Configurator is a utility that records information in services.xml files. The GPPServer service, AcsNMSservice service, and GUI each have their own services.xml file. The information recorded in



these files are used to define the PC and services where data is sent to and from (Self-Definition and Server List). In addition, protocols, ports, and other required information related to data communication within the GuardPoint10 architecture are recorded.

Figure 1-12



The Configurator is automatically installed by the Installation wizard. The Configurator records the following types of information in a services.xml file:

- » For client only (workstation) PC installations:
  - The name and IP address of the workstation PC (GUI).
  - The name and IP address of the GPPServer service that communicates with workstation installations.
- » For server PC installations:
  - The name and IP address of the GPPServer service that communicates with workstation installations.
  - The name and IP address of the AcsNMService service that communicates with the GPPServer service.
  - The name and IP address of all PCs that have a workstation installation (GUI).

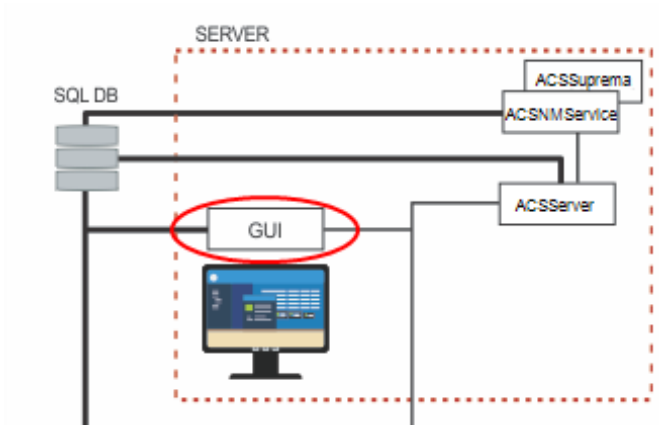
In human terms, the Configurator records the "Who am I" and the "Who do I talk to" data for each service and workstation GUI.

## Configurator prerequisites (architecture information)

- » For the server PC: A list containing the machine name and IP address of all PCs designated as GuardPoint10 workstations. You will also need the name and IP address of the server PC.
- » For workstation PCs: The SQL Server name, database name, the server PC name, and IP address.

# How to record a server PC - GUI

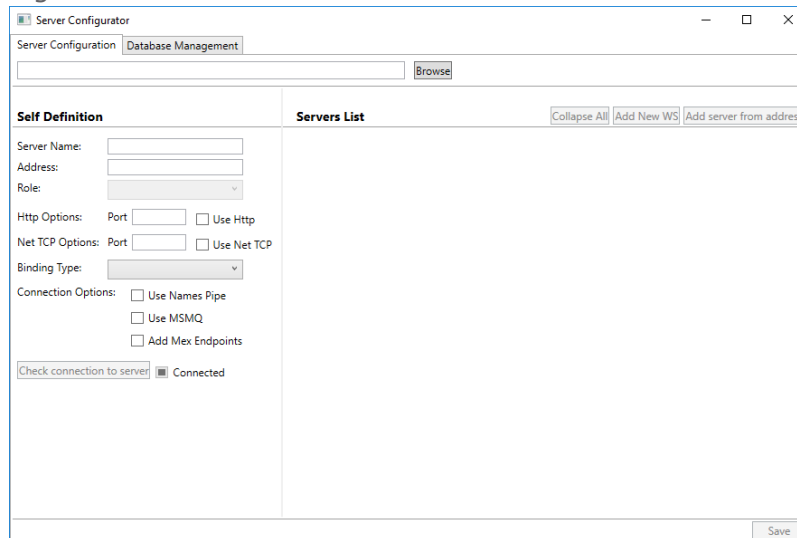
Figure 1-13



The server GUI only communicates with the GPPServer service (for that matter, all workstation GUIs in the GuardPoint10 architecture communicate with the same GPPServer service). Therefore, the Configurator needs to only record the workstation information ("Who am I") and the GPPServer service information ("Who do I talk to").

1. If the Configurator is not already opened, go to  
`C:\Program Files (x86)\GuardPoint10\Configurator\`  
and click **.ACS.Util.UI.exe**. The Configurator window is displayed.

Figure 1-14



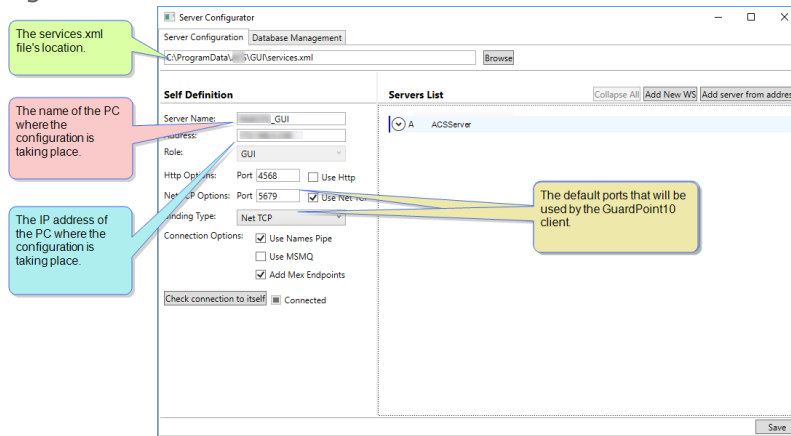
2. Click **Browse** at the top of the window. A file Selection dialog is displayed.
3. Select

`C:\ProgramData\ACS\GUI\services.xml`

The path appears in the Browse field and "<machineName>\_GUI" appears in the Server Name field.

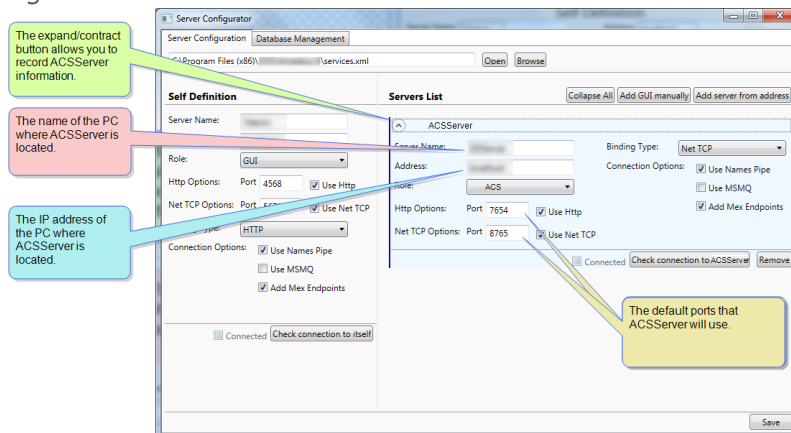
- In the Server Name field, change "GUI" to the name of the PC where the configuration is taking place.
- In the Address field, where it currently says "localhost", enter the IP address of the PC, where the configuration is taking place.
- Leave all other fields untouched and click **Save**. The information is saved to the services.xml file selected in Step 3.

Figure 1-15



- In the Servers List, below the Self-Definition area, click **GPPServer**. Fields related to the GPPServer service appear.

Figure 1-16



This is done because the client GUI needs to communicate with the GPPServer service; and for that to happen, the GUI needs to know where to find the GPPServer service.

- In the GPPServer's Server Name field, change "GPPServer" to the name of the PC where the configuration is taking place.
- In the GPPServer's Address field, where the current value is "localhost", change the value to the IP address of the PC, where the configuration is taking place.
- Leave all other fields untouched and click **Save**. The configuration is saved in the services.xml file selected in Step 3.

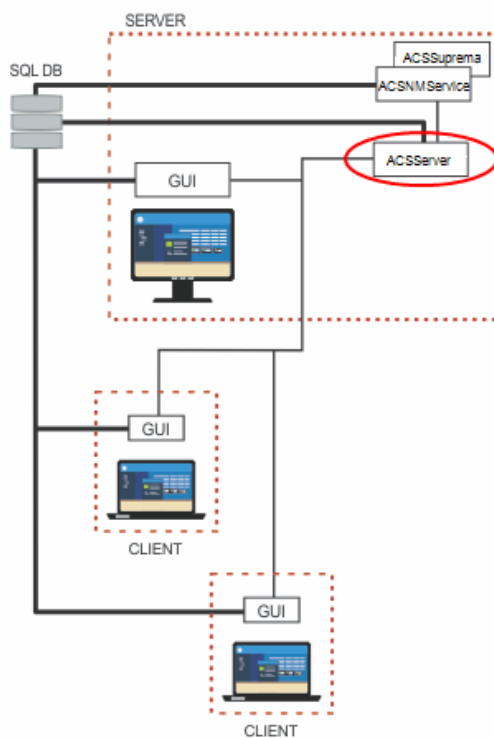
**Note:** The ports specified in the instructions and prerequisites are the default ports used by GuardPoint10. If your IT department or GuardPoint10 technical support directs you to use different ports, please change the values in the relevant fields.

A best practice is to click the **Check connection to server** button after completing a client or service entry. This will confirm that the data entered (PC name and IP address) is correct.

## How to record a Server PC - GPPServer

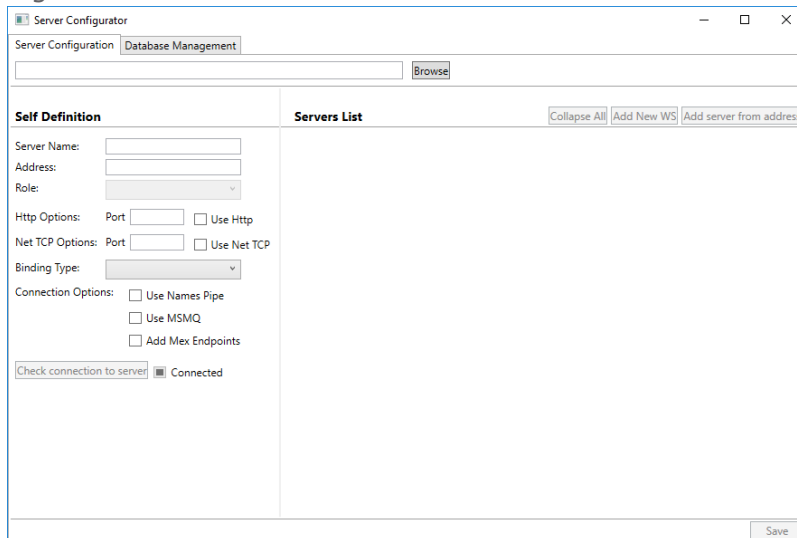
The Server PC's GPPServer service communicates the Server PC's AcsNMService service and with each client GUI in the GuardPoint10 architecture. Therefore, the Configurator needs to record the GPPServer service information ("Who am I"), the AcsNMService service information ("Who do I talk to"), and all PC Client GUI information in the architecture -including the client GUI on the Server PC- ("Who else do I talk to").

Figure 1-17



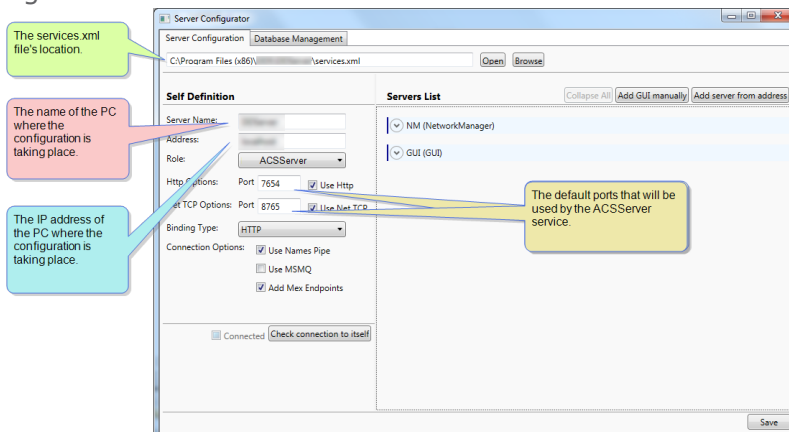
1. If the Configurator is not already opened, go to  
C:\Program Files (x86)\ACS\Configurator\  
and click **.ACS.Utilis.UI.exe**. The Configurator window is displayed.

Figure 1-18



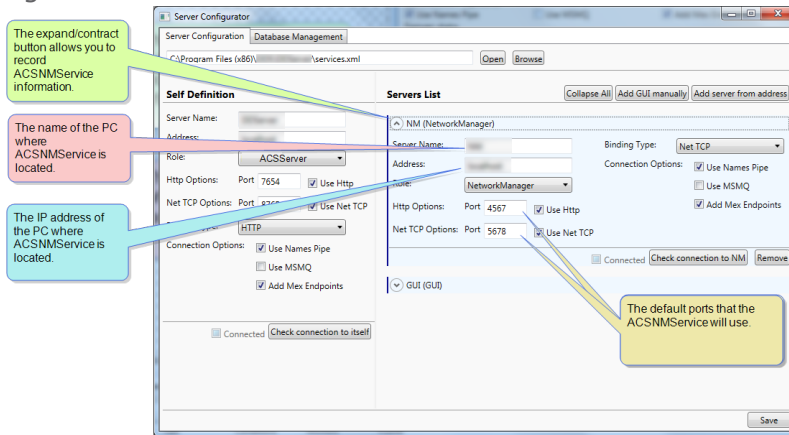
2. Click **Browse** at the top of the window. A file Selection dialog is displayed.
3. Select  
`C:\Program Files (x86)\ACS\GPPServer\services.xml`  
The path appears in the Open field and "GPPServer" appears in the Server Name field.
4. In the Server Name field, change "GPPServer" to the name of the PC, where the configuration is taking place.
5. In the Address field, where the current value is "localhost", change the value to the IP address of the PC, where the configuration is taking place.
6. Leave all other fields untouched and click **Save**. The configuration is saved in the services.xml file selected in Step 3.

Figure 1-19



7. In the Servers List, below the Self-Definition area, click **NM (Network Manager)**. Fields related to the AcnsNMService service appear.

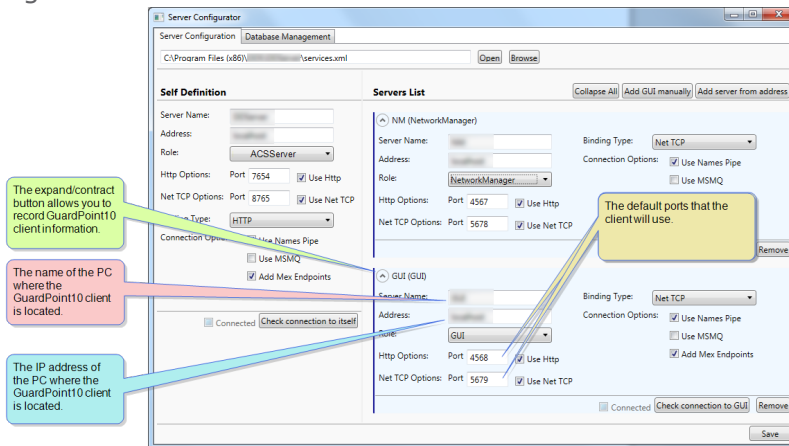
Figure 1-20



This is done because the GPPServer service needs to communicate with the AcsNMSERVICE service; and for that to happen, the GPPServer service needs to know where to find the AcsNMSERVICE service.

8. In the AcsNMSERVICE's Server Name field, change "NM" to the name of the PC where the configuration is taking place.
9. In the AcsNMSERVICE's Address field, where the current value is "localhost", change the value to the IP address of the PC, where the configuration is taking place.
10. Leave all other fields untouched and click **Save**. The configuration is saved in the services.xml file selected in Step 3.
11. In the Servers List, below the Self-Definition area, click **GUI (GUI)**. Fields related to a client GUI appear.

Figure 1-21



This is done because the GPPServer service needs to communicate with each client GUI in the GuardPoint10 architecture. For that to happen, the GPPServer service needs to know where to find each client GUI.

12. If you are configuring the client GUI on the Server PC, in the Server Name field, change "GUI" to the name of the PC where the configuration is taking place.

If you are configuring the client GUI for a Client-only PC (not the Server PC), in the Server Name field, change "GUI" to the name of the Client-only PC.

13. If you are configuring the client GUI on the Server PC, in the Address field, where the current value is "localhost", change the value to the IP address of the PC, where the configuration is taking place.

If you are configuring the client GUI for a Client-only PC (not the Server PC), in the Address field, where the current value is "localhost", change the value to the IP address of the Client-only PC.

If there are additional client GUIs, click the **Add New GUI** button and repeat Step 12 and Step 13 until the list is complete.

14. Leave all other fields untouched and click **Save**. The information is saved to the services.xml file selected in Step 3.



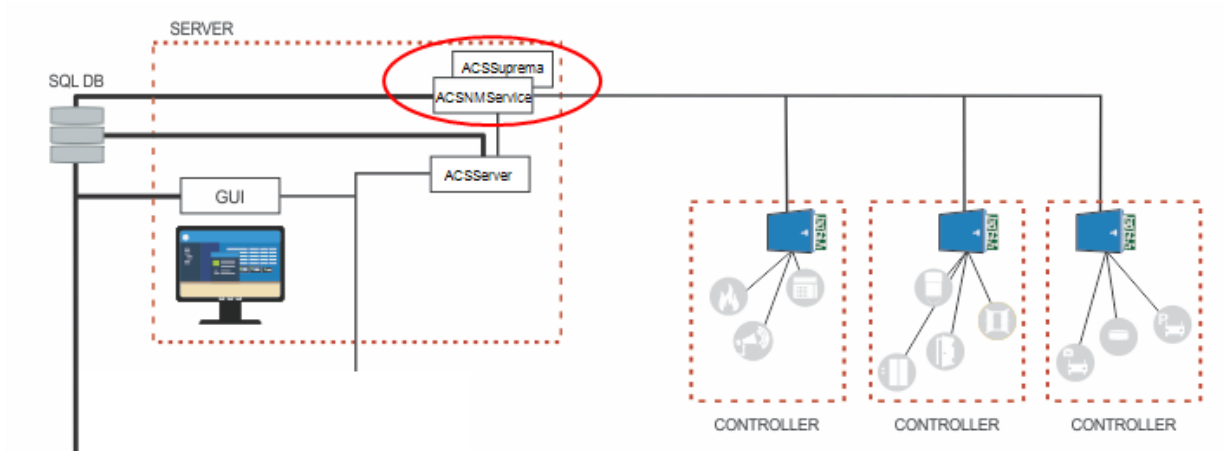
**Note:** The ports specified in the instructions and prerequisites are the default ports used by GuardPoint10. If your IT department or GuardPoint10 technical support directs you to use other ports, please change the values in the relevant fields.

A best practice is to click the **Check connection to server** button after completing a client or service entry. This will confirm that the data entered (PC name and IP address) is correct.

## How to record a Server PC - AcsNMService

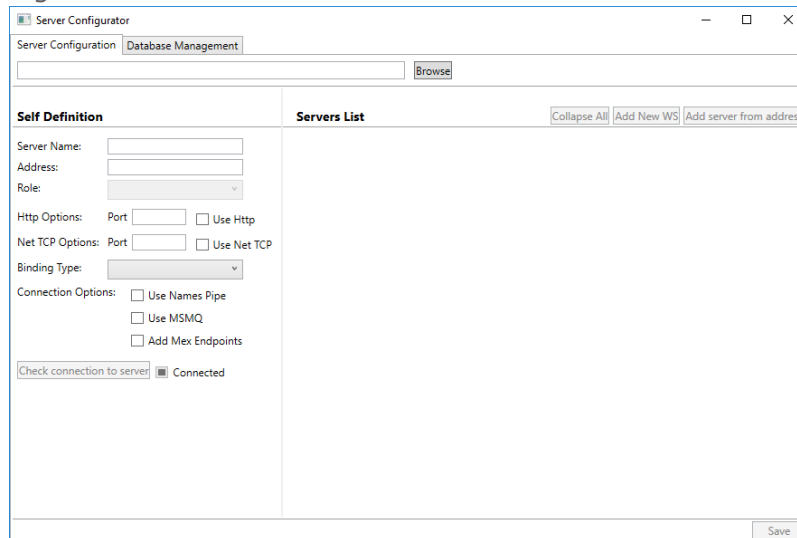
The Server PC's AcsNMService service communicates only with the GPPServer service. Therefore, the Configurator needs to record AcsNMService service information ("Who am I") and the GPPServer service information ("Who do I talk to").

Figure 1-22



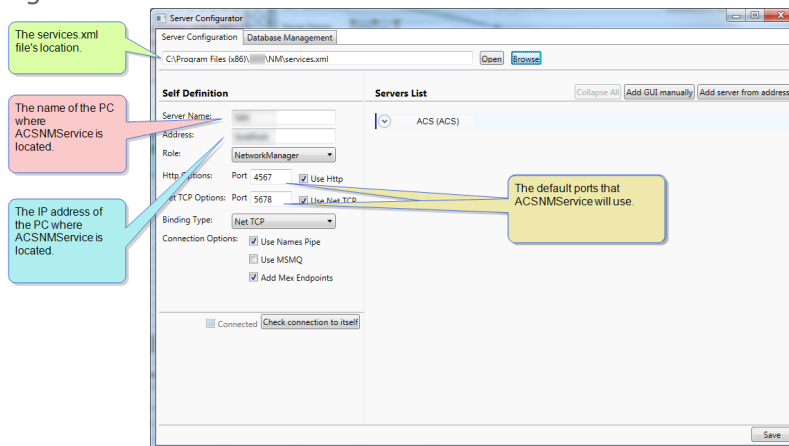
1. If the Configurator is not already opened, go to  
C:\Program Files (x86)\ACS\Configurator\  
and click **.ACS.Util.UI.exe**. The Configurator window is displayed.

Figure 1-23



2. Click **Browse** at the top of the window. A file Selection dialog is displayed.
3. Select  
`C:\Program Files (x86)\ACS\NM\services.xml`  
The path appears in the Open field and "NM" appears in the Server Name field.
4. In the Server Name field, change "NM" to the name of the PC where the configuration is taking place.
5. In the Address field, where the current value is "localhost", change the value to the IP address of the PC where the configuration is taking place.
6. Leave all other fields untouched and click **Save**. The configuration is saved in the services.xml file selected in Step 3.

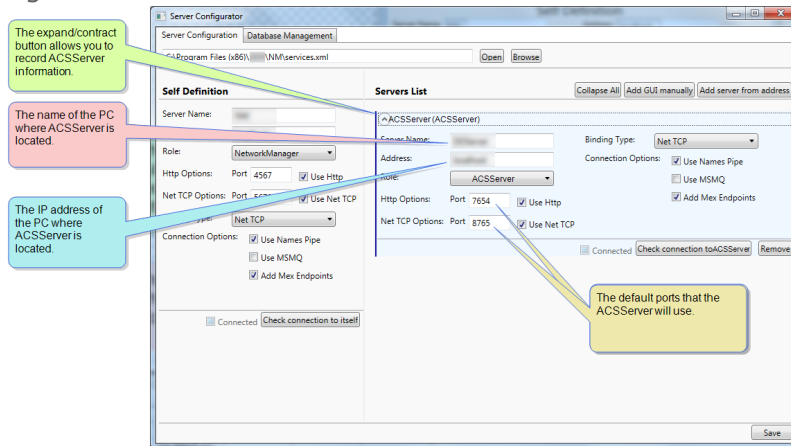
Figure 1-24



7. In the Servers List, below the Self-Definition area, click **GPPServer (GPPServer)**. Fields related to the GPPServer service appear.



Figure 1-25



This is done because the AcsNMService service needs to communicate with the GPPServer service; and for that to happen, the AcsNMService service needs to know where to find the GPPServer service.

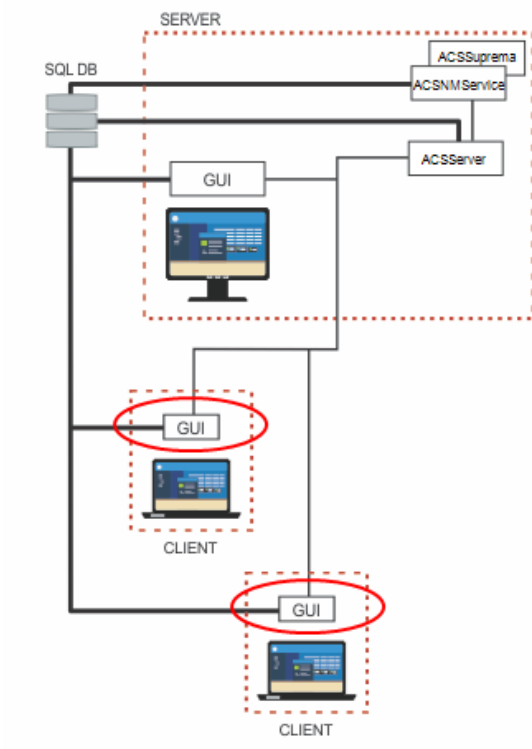
8. In the Server Name field, change "GPPServer" to the name of the PC where the configuration is taking place.
9. In the Address field, where the current value is "localhost", change the value to the IP address of the PC where the configuration is taking place.
10. Leave all other fields untouched and click **Save**. The configuration is saved in the services.xml file selected in Step 3.

**Note:** The ports specified in the instructions and prerequisites are the default ports used by GuardPoint10. If your IT department or GuardPoint10 technical support directs you to use other ports, please change the values in the relevant fields.

A best practice is to click the **Check connection to server** button after completing a client or service entry. This will confirm that the data entered (PC name and IP address) is correct.

# How to record a Client-only PC

Figure 1-26

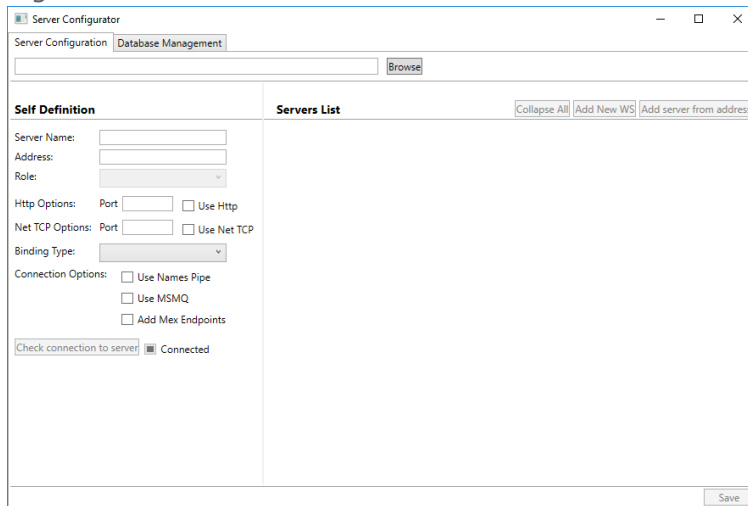


A Client-only PC only has a client GUI, the client GUI only communicates with the Server PC's GPPServer service. Therefore, the Configurator only needs to record the client information ("Who am I") and the GPPServer service information ("Who do I talk to").

**Note:** This operation must be performed on each PC where a Client only installation exists.

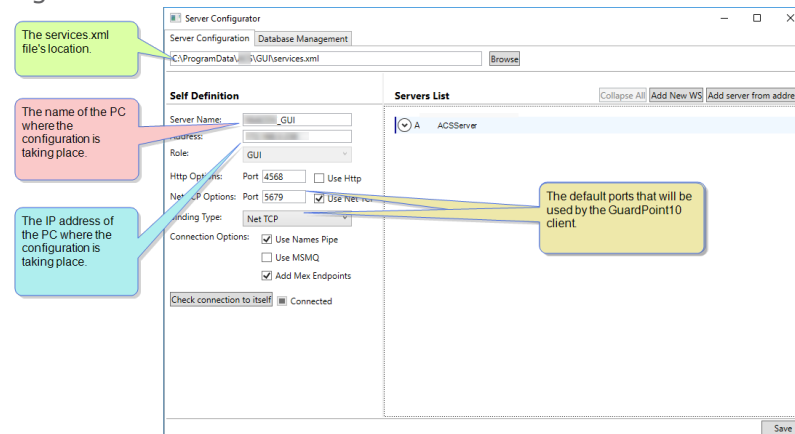
1. If the Configurator is not already opened, go to  
C:\Program Files (x86)\ACS\Configurator\  
and click **.ACS.Util.UI.exe**. The Configurator window is displayed.

Figure 1-27



2. Click **Browse** at the top of the window to Configure the GUI. A file Selection dialog is displayed.
3. Select  
`C:\ProgramData\ACS\GUI\services.xml`  
The path appears in the Open field and "GUI" appears in the Server Name field.
4. In the Server Name field, change "GUI" to the name of the Client-only PC, where the configuration is taking place.
5. In the Address field, where it currently says "localhost", enter the IP address of the Client-only PC.
6. Leave all other fields untouched and click **Save**. The information is saved to the services.xml file selected in Step 3.

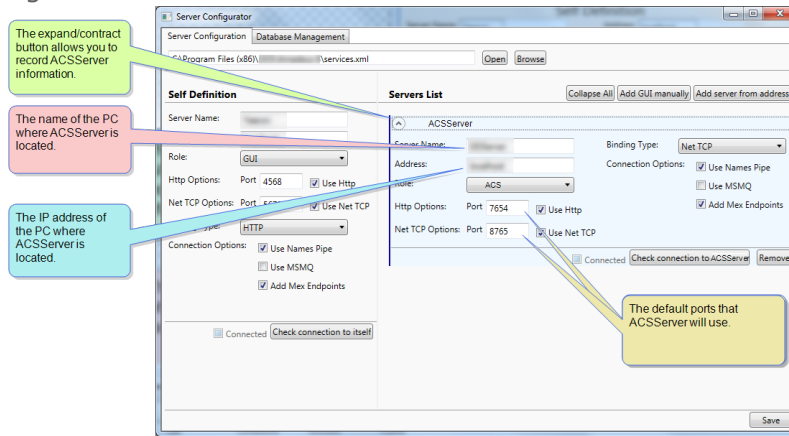
Figure 1-28



7. In the Servers List, below the Self-Definition area, click **GPPServer**. Fields related to the GPPServer service appear.  
This is done because the client GUI needs to communicate with the GPPServer service; and for that to happen, the client GUI needs to know where to find the GPPServer service.

8. In the GPPServer's Server Name field, change " GPPServer" to the name of the PC, where the GPPServer service is located.
9. In the GPPServer's Address field, where the current value is "localhost", change the value to the IP address of the PC, where the GPPServer service is located.

Figure 1-29



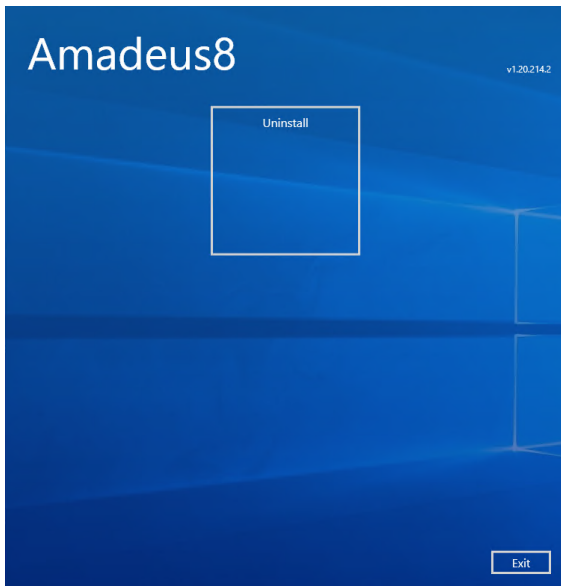
10. Leave all other fields untouched and click **Save**. The configuration is saved in the Client-only PC's services.xml file selected in Step 3.

**Note:** The ports specified in the instructions and prerequisites are the default ports used by GuardPoint10. If your IT department or GuardPoint10 technical support directs you to use other ports, please change the values in the relevant fields.

A best practice is to click the **Check connection to server** button after completing a client or service entry. This will confirm that the data entered (PC name and IP address) is correct.

# Uninstalling GuardPoint10

1. From the machine where the GuardPoint10 installation exists, launch the same EXE file used for the installation. The uninstall wizard begins.



2. Click **Uninstall** and wait for the uninstall process to successfully complete, and then restart the machine.



**Note:** After the uninstall process is completed, the folders and files created during the installation still exist on the machine where the uninstall process took place.

# GuardPoint10 Troubleshooting Best Practice

On rare occasions, environmental factors may cause GuardPoint10 system anomalies. A best practice to resolve the anomalies is to initialize your controllers and check that GuardPoint10 is in your anti-virus' exception list. If the anomalies persist, contact your GuardPoint10 provider.

## Getting familiar with the GuardPoint10 console

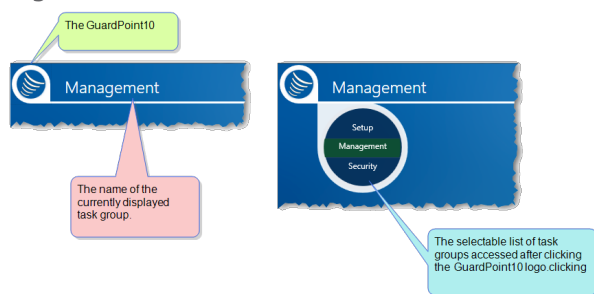
This is an introduction to the fundamental elements of the GuardPoint10 console layout. Besides the usual PC window components (close box, title bar, scrollbars, etc.), a typical GuardPoint10 console has other elements, as shown below.

### Non-Editable elements

At the top of the console, there are three items:

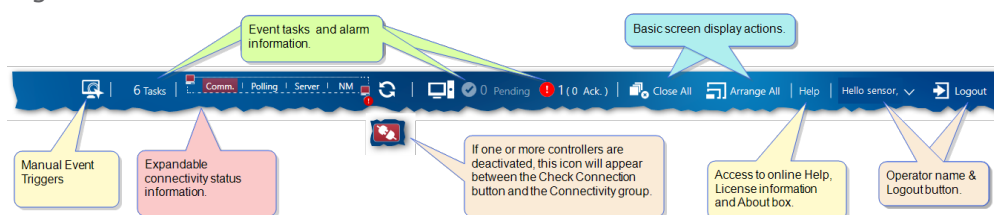
- » **Task group selector and indicator:** Specifies the task group where the currently displayed screen is grouped. For example, the Cardholders screen is part of the Management task group. To go to a different task group, click the GuardPoint10 logo to the left of the task group name currently displayed and select the task group where you want to go.

Figure 1-30



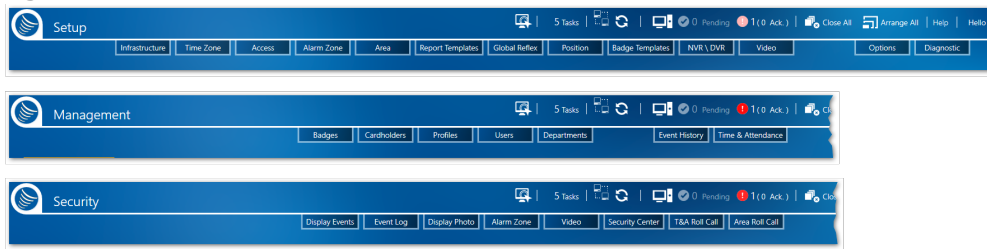
- » **Dashboard:** Contains information that is not specific to any one task. The dashboard includes real-time information that is updated at set intervals. The dashboard includes information about event tasks that require an operator's abstention, connectivity, basic screen display actions, the logged-in operator's name, and access to the logout action. For additional information, see "[Dashboard Content & Actions](#)" on page 334.

Figure 1-31



- » **Primary menu bar:** Provides access to a task group's related screens. The menu bar changes according to the task group selected via the Task group selector and indicator, described at the top of this list.

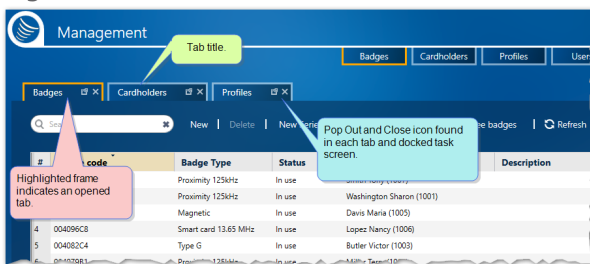
Figure 1-32



## Editable task screen views: tab stack, docking, and popout

When you're regularly dealing with multiple task screens (i.e. Cardholders, Video Security, Security Center, etc.), each with their own, the GuardPoint10 Tab Stacks feature lets you group the screens together into a single tab stack, where each task screen can be displayed by clicking the tasks tab title.

Figure 1-33

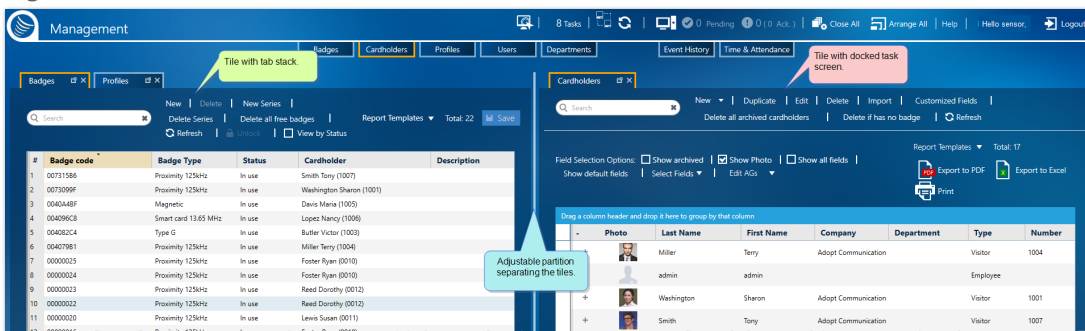


While this is a very nice feature to manage multiple screen views, it is not the only screen layout feature available.

If you find yourself constantly using a specific task screen, try the GuardPoint10 docking feature, which allows you to dock a task screen to a sidebar tile for convenient access.

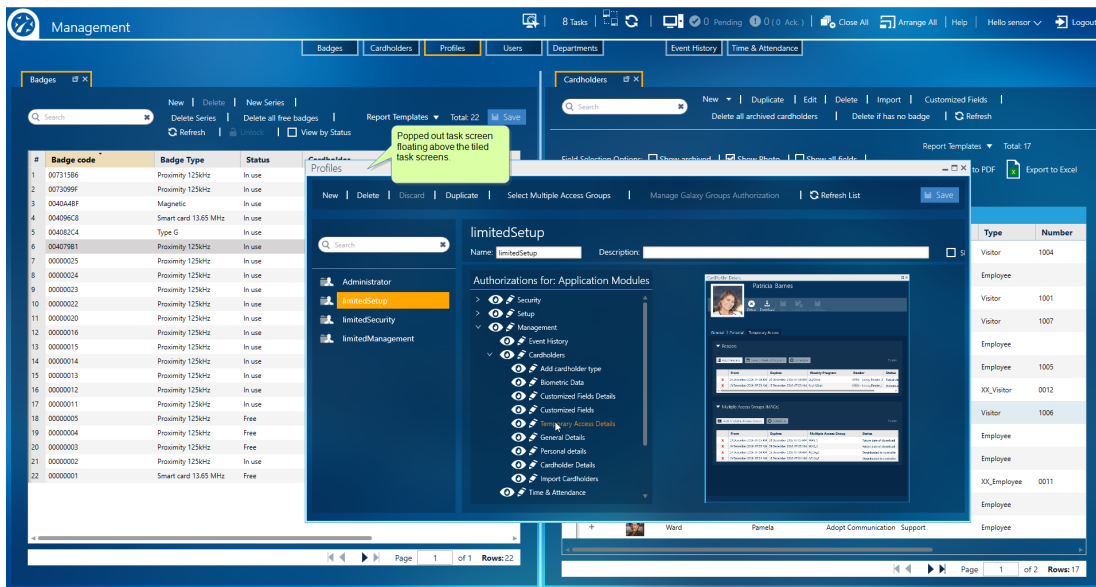
Tile view allows you to partition the GuardPoint10 console. Each partitioned area (tile) may contain a stack of task screens or a single docked task screen.

Figure 1-34



There is one more screen view best used for immediate task operation or when transitioning to another tile in the console called a popout. A task screen in popout view is layered on top of the console; it is not in a tile. It floats on top of the other displayed screens. A popped-out screen can be identified by its gray title bar. A popped-out screen may be added to a tab stack or docked in a tile at any time.

Figure 1-35



What do these task screen view options mean for you?

They provide a highly customizable console layout, where you can place task screens in tab stacks or dock them in tiles on the top, right, bottom, and left sides of the console.

With a series of gesture actions, you can perform by holding down the left mouse button and moving the mouse pointer to a specific tab stack, tile, or docking station indicator, you can create an intuitively organized layout for GuardPoint10 system task access and monitoring.

### Some information about docking station indicators:

There are two types of docking station indicators, a tile docking station indicator, and a console docking station indicator.

#### A tile docking station indicator

A tile docking station indicator drops a dragged task screen into a sidebar of the tile. Which sidebar, depends on the arrow in the docking station indicator where you drag the task screen. A gray, semi-transparent box will appear while you hover the mouse pointer over an arrow in the docking station indicator. The box indicates the area that will be occupied by the task screen if it would be dropped on that arrow.



The docking station located in the center of a tile.

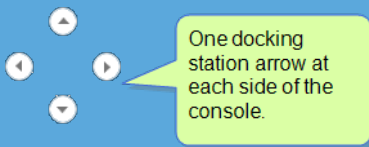
If you drop a task screen onto the center dot of the docking station indicator, the tile's content will turn into a tab stack, if it wasn't a tab stack before, and append the task screen to the end of the stack.

The tabs of a tab stack may appear at the top or bottom of a tile.

#### A console docking station indicator



A console docking station indicator places a dragged task screen into a sidebar of the console. There are four console docking station indicators, one on each side of the console. A gray, semi-transparent box will appear while you hover the mouse pointer over an indicator arrow. The box indicates the area that will be occupied by the task screen if it would be dropped on that arrow.



The following operations are used to manage your console layout and tab stacks. Expand an operation title to see the steps.

### Creating a tab stack

1. From the GuardPoint10 logo rollout, select the task group where the task that will be opened is found in the primary menu.
2. Select the task from the Primary menu bar. The task screen is displayed. This is the first screen of a potential tab stack (stack of task screens).
3. Repeat steps 1 and 2 to build the stack from a primary menu.

If multiple stacks are displayed on the console, any additional screens opened from a primary menu bar will automatically be added to the first stack created.

### Creating a popout task screen

» From a tab stack:

1. Display a task screen that is currently in a tab stack, and then do one of the following:
  - » In the tabs title area, click the small popout icon. The task screen is popped-out and floated on top of the other screens in the console.
  - » Drag and drop the tab title of the task screen that will be popped-out to a free area in the console (not occupied by another tab or docking station indicator).

» From a docked task screen (not tabbed):

- » On the right side of the title bar of the docked task screen, click the small popout icon. The task screen is popped-out and floated on top of the other screens in the console.

A popout may contain a tab stack or an individual screen.


A popout may also be minimized to the Windows task bar, where it can be reopened as required.

### Re-ordering a tab stack

1. From a tab stack, open the tab that will be moved to a different location in the same stack.
2. Drag and drop the tab title of the opened task screen over the tab title of the task screen that the selected tab title will appear in front of. The tab title appears in its new location.

### Creating a subsequent tab stack

- » If a subsequent tab stack does not already exist, drag a popped-out task screen or a tab from a previously created tab stack, to a docking station where the task screen will be displayed. The console is partitioned and the dragged task screen appears in the sidebar tile where the docking station arrow was pointing. After docking the initial task screen, follow the instructions in the next bullet to add a task screen to the subsequent tab stack.
- » If a subsequent tab stack already exists, drag a popped-out task screen or a tab from a previously created tab stack to the center docking station of the tile where the task screen will be stacked. The task screen's tab is appended to the tab stack.



**Note:** The tab titles in a subsequent tab stack may appear at the top or bottom of the stack.

### **Adding a task screen to an existing tab stack (not from the primary menu bar)**

- » Drag a popped-out task screen or a tab from a different tab stack to the center docking station where the task screen will be stacked. The task screen's tab is appended to the tab stack.

### **Closing a popped-out task screen, a stacked task screen, or a docked task screen**

Click the **X** in the title bar or tab title of the task screen. If there are unsaved changes on the task screen, you will be asked if you want to save your changes before the close operation is completed.

### **Docking a task screen**

If the task screen that will be docked is not opened yet, select it from the relevant primary menu bar. The task screen is appended to an existing tab stack. If there is no existing tab stack, the task screen appears as the initial task screen for a new tab stack.

After displaying the task screen, drag it to a docking station that includes an arrow. The task screen is displayed docked to the sidebar where the docking station arrow was pointing. For example, if the docking station arrow was pointing down, the task screen will dock to the sidebar at the bottom of the console.

# Roadmap to Site Building

This topic provides you with a general overview that guides you through the site-building process.

## Personnel

- » An administrator for GuardPoint10. This person will be the primary operator responsible for the system software interface.

The administrator should receive minimum training on the GuardPoint10 system.

- » An GuardPoint10 vendor-approved installer. This person will be responsible for the hardware installation, network database, and possibly the initial GuardPoint10 setup.

## Steps to build your system

### Hardware

1. Configure controller hardware and connect cables (see installation manuals).
2. In each controller, set the **dipswitch**<sup>1</sup> address.
3. If a TCP module will be used in the controller, configure the IP address and **baudrate**<sup>2</sup>. This is done via a computer link to the module. The exact operation varies, depending on the brand of the TCP module.
4. Set the badge technology on the controller's dipswitch via the technology selection jumpers.

### Software

1. Install GuardPoint10. The software is available via your GuardPoint10 system vendor.
2. Change the admin operator's username and password.  
Though you can change the username and password, you cannot change the authorizations set for this operator.
3. In GuardPoint10 go to Setup > Infrastructure and create your site structure. This can be done manually or via the Setup Wizard. The setup includes networks, controllers, readers, inputs, relays, and local reflexes (see ["Initial Setup" on page 38](#)).
4. Rename the various parts of the infrastructure to make it more intuitive and operator-friendly.
5. Add operators (see, ["Operators \(Users\)" on page 103](#)).
6. Configure time zones (see, ["Daily Program Time Zones" on page 114](#)).
7. Configure Access Groups (see, ["Access Groups" on page 140](#)).
8. Configure badges and cardholders (see, ["Badges" on page 175](#) and ["Cardholders" on page 193](#)).
9. Configure Alarm Zones, Video Setup, Position, etc., depending on the components available in your installation. Check out the online Help (press F1).

---

<sup>1</sup>A series of tiny switches built into circuit boards. The housing for the switches has the same shape as a chip and is usually red.

<sup>2</sup>The rate at which information (signal or symbol changes) is transferred per second.

# GuardPoint10 API Center

Just like GuardPoint10's cutting-edge user interface makes it possible for operators to manage the GuardPoint10 system. The GuardPoint10 API makes it possible for a third-party application to communicate with the GuardPoint10 system to their mutual benefit.

Sometimes businesses want to share data between application ecosystems. For example, a human resource application may have employee / cardholder information that would be beneficial to GuardPoint10, or vice versa. With GuardPoint10 APIs, computer automation rather than people can cohesively manage the work environments resulting in a quicker, flexible, and more productive unified environment.

The GuardPoint10 API Center is an add-on feature and not part of GuardPoint10's core solutions.

Contact your GuardPoint10 provider for more information about the GuardPoint10 API Center.

## MultiSite Implementation also includes a MultiCompany solution



**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

The MultiSite module partitions the security ecosystem of individual organizations, with separate **sites**, under one umbrella GuardPoint10 server installation and a single database.

GuardPoint10 also lets you share assets, with other sites in your GuardPoint10 system. Sharing assets is a convenient way of making resources available to other sites. The primary advantages of the sharing approach are as follows:

- » Eliminates the possibility of cross-site data conflicts.
- » Saves time creating individual security ecosystems.
- » Creates a cohesive group of assets while still supporting the unique security needs of each site.

A user's workflow will not radically change in day-to-day operations. MultiSite creates an environment where the user may have authorization to more than one site.

## MultiSite Terminology

- » **Assets:** Resources that affect the behavior of a site's security ecosystem. For example, readers, inputs, and relays.
- » **Owner:** The site whose users manage the sharing status of an asset and have Edit and Delete rights for an asset. In addition to site users, super users have been added and are owners of all assets on all sites.
- » **Sharing:** Method used to create a site-to-site relationship for assets. The asset owner site may choose to share, not share or, stop sharing an asset at their discretion.
- » **Super user:** The Root site's built-in administrator, as well as a site-to-site administrator. A super user can do anything a site admin can do. The difference is the scope. A super user is an

administrator for each site in the system. For example, a super user may add new sites to the system as well as add users to any site.

- » **Root site:** The first site of the infrastructure. The Root site not only includes its own site's assets, but also includes networks and controllers shared by other sites, where the ownership is changed to the Root site.

If the assets of a controller are shared, the controller's ownership is not moved to the Root site. But, if the controller itself is shared, the controller's ownership is moved to the Root site.

- » **Site:** The infrastructure element that partitions an organization with its own security ecosystem in the GuardPoint10 system.

## Architecture:

There is only one GPPServer and AcsNMService that polls the controllers of all sites and manages all the events. In addition, there is only one database server to which all sites must have access. Each site user can access the system from any workstation connected to the GPPServer.

A workstation is not owned by a site. The logged-in user's authorization determines the content available from the workstation. This means that a user can log into the system from any GuardPoint10 workstation, regardless of the user's owner site.



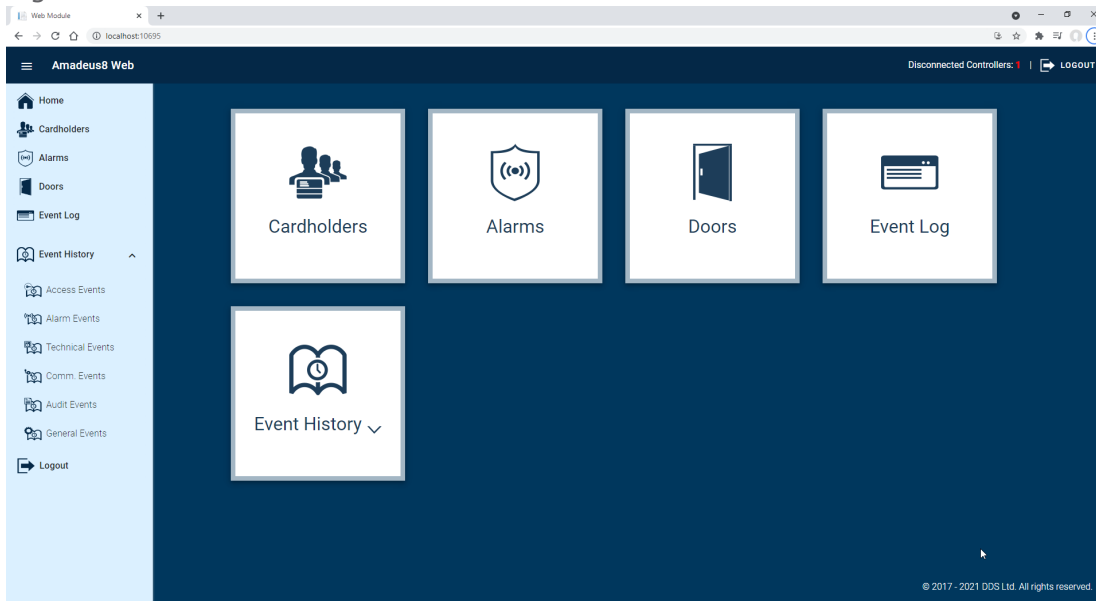
**Warning:** After setting MultiSite to **Yes** in the Options screen, **you cannot undo it.**

## MultiSite related topics

Many screens will be altered by enabling MultiSite. To see the scope of the screen changes perform a search in the Help for "MultiSite impact".

# GuardPoint10 WebApp

Figure 1-36



The GuardPoint10 WebApp is a user interface that allows you to oversee high-demand Management and Security data from a limited version of the GuardPoint10 interface. The GuardPoint10 WebApp is accessible to any authorized user via a Web browser.

For example, when you use the WebApp to add cardholders and badge codes, acknowledge & confirm alarms, as well as Open and close doors.

The features included are as follows:

- » Open / Close doors
- » View event histories of various types (i.e. Access, Alarm, Tech., Comm., Audit, General)
- » View / Add / Edit / Delete cardholders
- » Monitor controller communication status
- » View live events / Alarms
- » No special installation is required
- » Acknowledge / Confirm Alarms

The GuardPoint10 WebApp is available on any device that supports HTML5 web browser.

Connecting to the system is similar to entering a website, in the browser's address bar type the name of the machine where the GuardPoint10 server is installed followed by a colon and port number (i.e. "ACS\_ServerName:10695").

Enter your GuardPoint10 username and password, and start working.

To make the WebApp available to users:

- » In the Options screen General tab, set **Pass Events To API** to **Yes**.
- » For each user who will work with the WebApp, in the Users screen, set **Allow API** to **Yes**.

The maximum number of users who can be connected to the GuardPoint10 WebApp at the same time is restricted by the license that includes a **WebApps** item.

# CHAPTER 2:

## Infrastructure

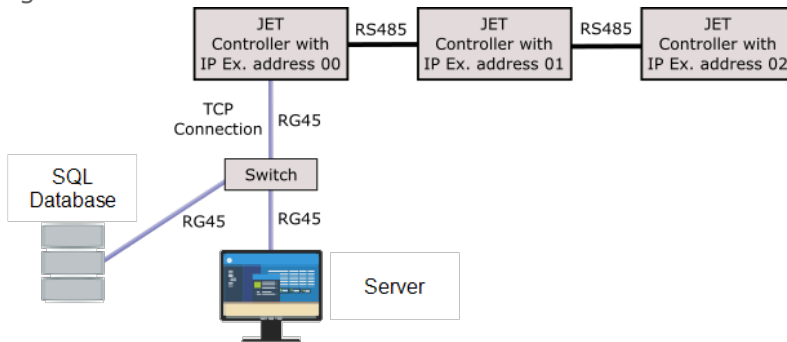


Site building and configurations are performed through the Infrastructure screens. When completed, the infrastructure tree represents a virtual roadmap of your physical system. It includes details about your system's controllers, readers, inputs, and other entities. This section covers the various methods for building your virtual system. While building the site, it may be necessary to consult with hardware installation personnel and your IT department. Once you've set up your virtual site and explored the parameters, you will want to continue the setup process by adding profiles, operators, time zones, etc.

# Initial Setup

For simplicity, we will document a setup scenario where we have three controllers, two connected to the network via COM ports and one with a TCP connection.

Figure 2-1

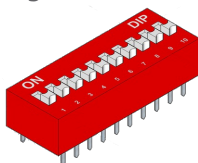


A best practice is for the initial setup to be performed by the primary GuardPoint10 operator together with the hardware installer.

## How to perform an initial setup of the infrastructure

1. Before getting started, the person responsible for the hardware installation should provide answers to the following questions about each controller:
  - » On which network will the controller be located?
  - » What is the controller type?
  - » Which COM port is the network connected to?
  - » Is this a TCP enabled controller? If the answer is yes, what is the IP Address and Port number?
  - » Is there a slave reader and if so, which reader is the master?
  - » What is the site **baudrate**<sup>1</sup>?
  - » What is the ID address of the controller (this is determined by the **Dipswitch**<sup>2</sup> setting on the controller panel)?

Figure 2-2



For information about the dipswitch settings see the Controller Installation Manual.

2. Open the GuardPoint10 application, go to the Setup Task group, and click **Infrastructure**. The Setup Wizard automatically starts.

<sup>1</sup>The rate at which information (signal or symbol changes) is transferred per second.

<sup>2</sup>A series of tiny switches built into circuit boards. The housing for the switches has the same shape as a chip and is usually red.



3. If the Setup Wizard does not start automatically, from the Infrastructure action bar, click **Setup Wizard**. The first dialog of the Setup Wizard is displayed. For a detailed explanation about the various parts and parameters in the setup Wizard, see "[Setup Wizard: Site -> Network -> Controllers](#)" on page 440.
4. If MultiSite exists in your GuardPoint10 system and it has been set to **Yes** in the Options screen, select a site from a drop-down list, where you are permitted (by virtue of your Users settings). Otherwise, skip to the next step.
5. In part B of the first wizard dialog, enter the number of COM networks and TCP networks that will be installed on your site, and then click **Next**. The Wizard's Networks dialog is displayed.

Figure 2-3

6. From the Wizard's Networks dialog, populate each network with controller information provided by the hardware installer (i.e. IP address, port, controller type, etc.).

Figure 2-4

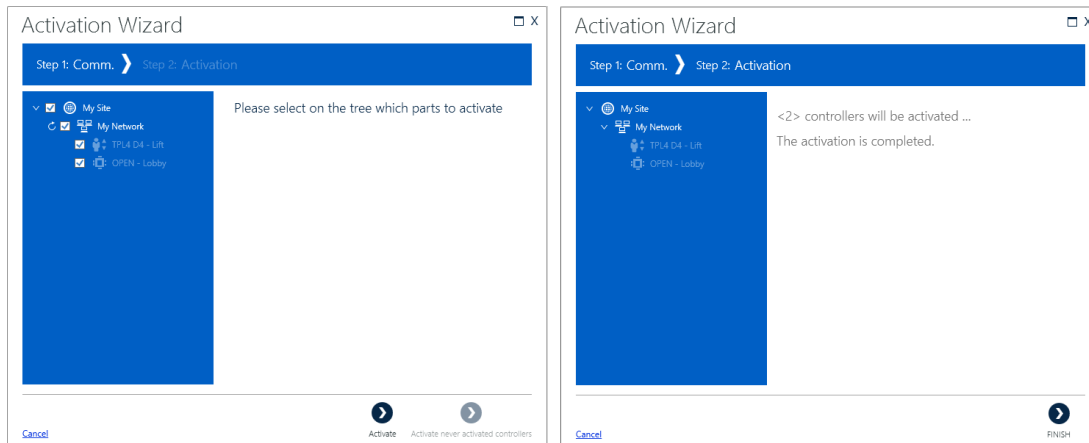


**Note:** Where the same IP address will be used multiple times in the dialog, a context menu has been provided for each IP address field that will allow you to copy an IP and paste it in multiple locations.

7. Click **Next**. The Wizard's Summary dialog is displayed. Click **Finish** to complete the installation. The site tree on the Infrastructure screen is updated to reflect the network and controller information you have entered in the Setup Wizard. The default number of readers, inputs, and relays are automatically created, according to the controller type's capacity.

After the Setup Wizard has finished, a message asking if you would like to proceed to the next stage and activate the controllers you have just set up is displayed. An activated controller shares information with the system database via polling. If you click **Yes**, see "[Controller Activation Wizard](#)" below.

## Controller Activation Wizard



The Activation Wizard guides you through the controller activation process for your site.

When a controller is activated, it shares information with the system database via polling. Controllers that are not activated, still gather information from devices connected to it, but no polling takes place. This means that the information is not shared with the system database and some of the data stored in the controller's local database may be lost (i.e. local database overflow) while the controller is deactivated.

During the initial installation, the Activation Wizard will start immediately after you complete the Setup Wizard.



**Note:** The Activation Wizard is optional. An alternative is to right-click a controller in the infrastructure tree and select **Activate** from the context menu to activate the controller in focus.

A controller may be deactivated by right-clicking an active controller in the infrastructure tree and selecting **Deactivate** from the context menu. An operator would deactivate a controller for testing purposes or to prevent polling.

## How to activate a controller

1. If the Activation Wizard was not automatically started, go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the action bar, click **Activation Wizard**. The first dialog of the Activation Wizard is displayed.
3. From the site tree, expand and select the controller(s) that you would like to activate.

If MultiSite exists in your GuardPoint10 system and it has been set to **Yes** in the Options screen, all controllers, where you are permitted (by virtue of your Users settings), will be available.

All controllers are selected by default.

Selecting a controller that is already active will not adversely affect the controller.

4. Click **Activate** the second dialog in the wizard is displayed. This dialog shows a breakdown of the activation results.
5. Click **Finish**. The wizard is closed.

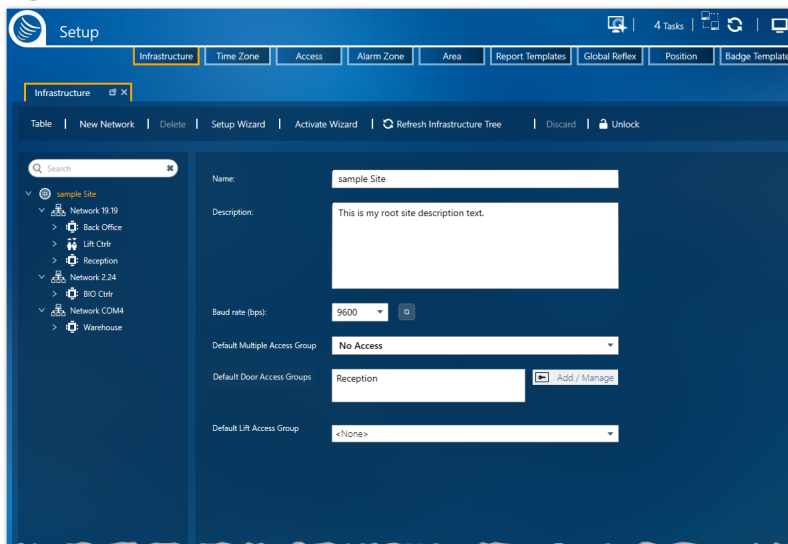
## Edit/Delete a Site Item

Use the following steps to edit or delete a site.

### How to edit site details

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the site item that you want to edit. The site's details are displayed.

Figure 2-5



3. Edit the site parameters as required (see "Site Details" on page 443).
4. After editing the site parameter values, do one of the following:
  - » Click **Discard**. The site parameters revert to their previously saved values.
  - » Click **Save**. The site parameter values are saved in the system database.

### How to delete a site (the root site cannot be deleted)

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the site item that you want to delete. The site's details are displayed.

If the site has a network connected to it, the network has to be deleted before you can delete the site (see "Edit/Delete a Network" on page 50).

3. Do one of the following:

- » Click **Delete** in the action bar and then confirm the operation. The empty site is deleted from the system database and the infrastructure tree.
- » Right-click the selected site and select **Delete** from the context menu, and then confirm the operation. The empty site is deleted from the system database and the infrastructure tree.

# Installing a MultiSplit

MultiSplit makes the GuardPoint10 system elastic by using distributed computing to split the workload between multiple machines or servers on the same machine.

MultiSplit is best used for large or growing GuardPoint10 systems. Imagine you have an GuardPoint10 server installation machine that generates a lot of data. This data must go through some processing, which unfortunately takes longer than to generate. For the processing to catch up with real-time, a slave machine (or server on the same machine) can be designated to handle some of the processing. Use the following steps to install a MultiSplit in an existing infrastructure.

## How to install a MultiSplit on an existing infrastructure

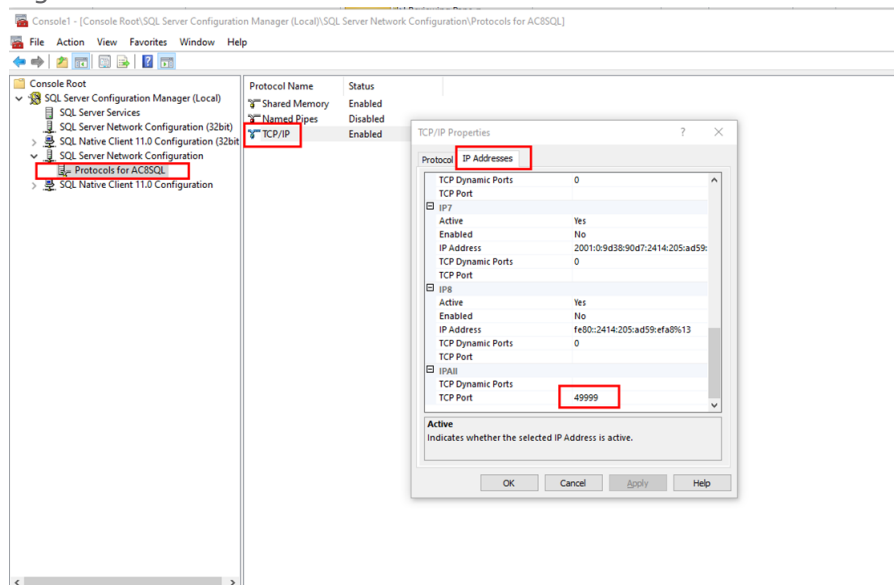
There are two parts to the MultiSplit installation.

- » **PART 1:** Adds a Communication Service via the GuardPoint10 GUI.
- » **PART 2:** Adds and edits folders and files to support a Communication Service that was added via the GuardPoint10 GUI.

### PART 1:

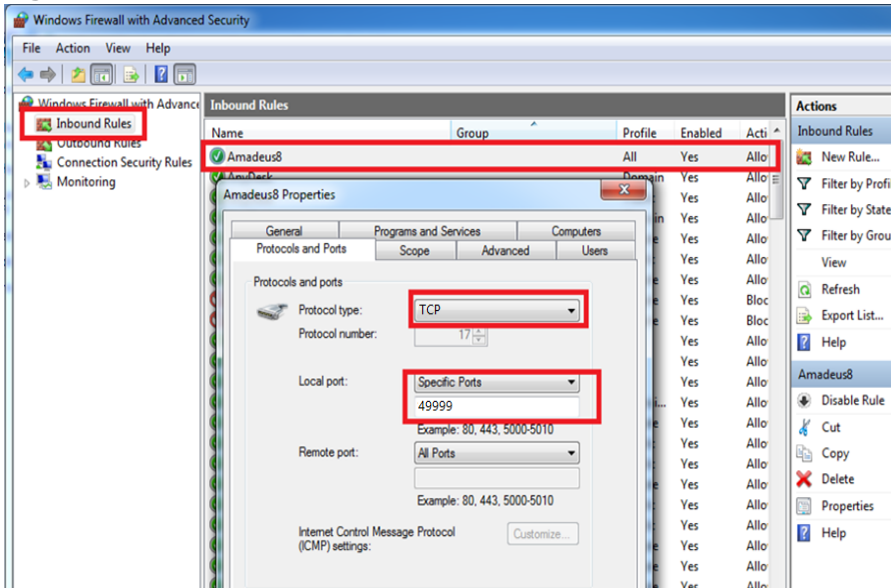
1. On the machine where the SQL server is installed, open the **Microsoft Management Console (MMC)**. Make sure that the TCP Port used by the SQL server = **49999**.
  - a. Open the MMC window via the **Start** button.
  - b. From the menu, click File > Add Remove Snap-in.
  - c. Add the **SQL Server Configuration Manager** to the Selected Snap-in list.
  - d. From the tree, select **Protocols for AC8SQL**.
  - e. Double-click on the **TCP/IP**.
  - f. Display the **TCP Port** value.

Figure 2-6



- If the TCP Port value is not 49999, change it to **49999** and restart the machine where the SQL server is installed.
- On the machine where the SQL server is installed, create an exception in the Firewall to allow the TCP Port **49999** in Inbound Rules.

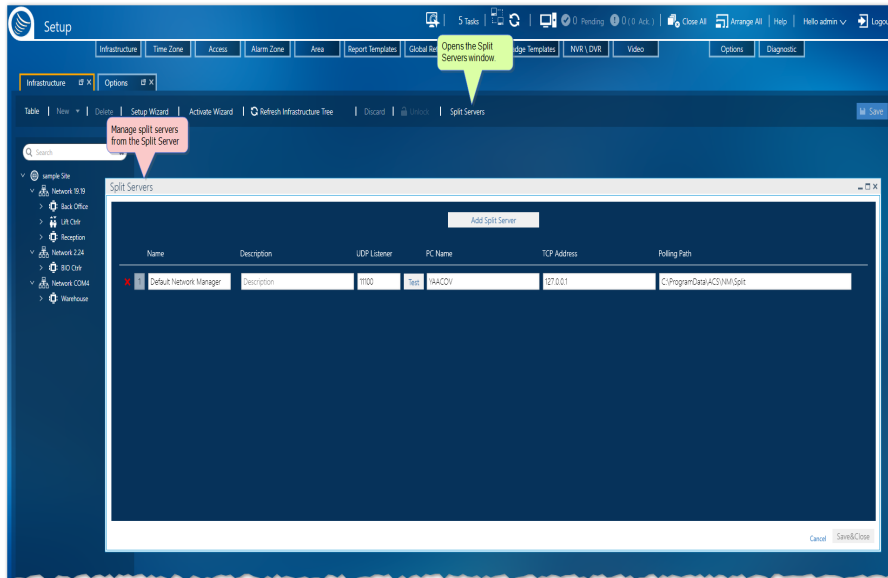
Figure 2-7



- On the GuardPoint10 Server machine, create an exception in the Firewall to allow the UDP Port **12100** in Inbound Rules.
- On the GuardPoint10 Server machine, open the `C:\ProgramData\ACS\NM\Split` folder, and then open the **SecComService.ini** file in a text editor.
- Create another exception to allow the TCP Port **49999**.
- In both **SQL\_Connect** and **SQL\_Connect\_Main** entries, change the **Data Source** value so it contains the full SQL server name (e.g. Replace **Data Source=.\AC8sql** with **Data Source=e=A8Server\AC8sql,49999**).
- Save and close the **SecComService.ini** file.
- From any GuardPoint10 installation, go to the Options > General screen.
- Set **Display MultiSplit** to **Yes**, and then click **Save**.
- Open the Infrastructure screen.
- Click the **Split Servers** button in the action bar. The Split Servers window is displayed.

The Split Servers window is where Communication Services are added to the system. The first row in the Split Servers window is the default Communication Service for each network in the infrastructure.

Figure 2-8



13. Click **Add Split Server**. A new row appears in the Split Servers window.
  14. Enter information in the new row.
- Each row contains the following:

Table 2-1 Split Server row information

Name	Description
ID	The read-only number identifies a Communication Service. This number is used in <b>PART 2</b> of the installation.
Name	A Communication Service’s selectable name that appears in a network’s details.
Description	(Optional) A free text field where information about the Communication Service is entered.
UDP Listener	Ensures that commands sent to the Communication Service are executed immediately. A UDP message is only reachable by machines that share the same network (i.e. it will not cross over a switch). This value should be unique.
Test (button)	Checks the communication between the <b>AcsNMService</b> and the Communication Service is successful. Test only after completing the steps in <b>PART 2</b> of the installation.
PC Name	The name of the third-party machine where a Communication Service will be placed. The field is not case-sensitive.
TCP Address	The address of the machine specified in the <b>PC Name</b> field.

Name	Description
Polling path	The network path, determined in <b>Part 2 (step 4)</b> , to the folder that will be shared (e.g. <code>\\NewPC\SecComService2</code> ). Initially, set the default folder (e.g. <code>C:\ProgramData\ACS\NM\Split</code> ) as a placeholder for the polling path until the actual network path exists.

- After a new Communication Service is defined, click **Save** in the Split Servers window.
- Take note of the **Communication Service ID** that has been assigned, this will be used in **PART 2** of the installation. Then click the **X** at the top right of the Split Servers window.



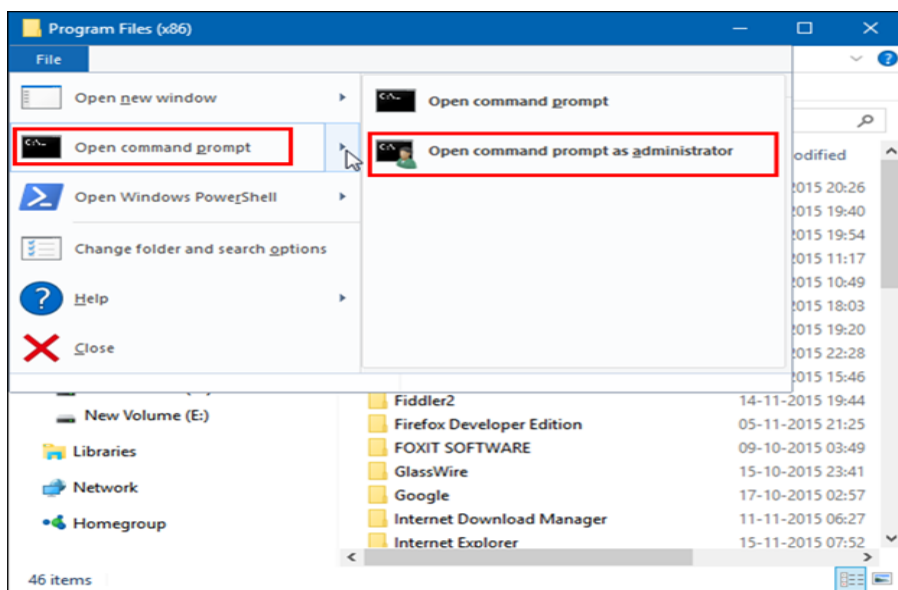
**Note:** Split Servers working on the same machine will not be allowed to share the same UDP listener port and TCP Address.

## PART 2:

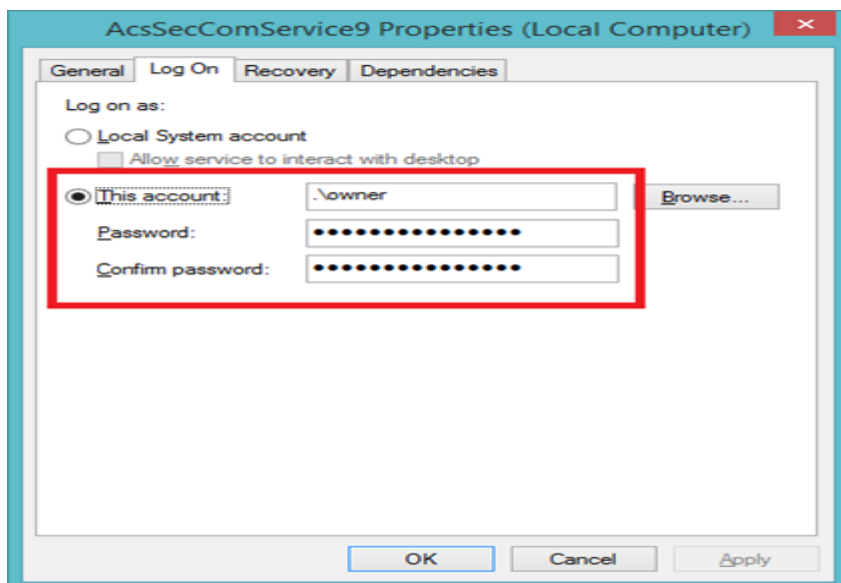
- On the machine where the GuardPoint10 server is installed, open the File Explorer, and then go to `C:\Program Files (x86)\GuardPoint10\NM`.
- Copy the **SecComService** folder and paste it into a folder on the third-party machine.
- On the third-party machine, rename the **SecComService** folder to **SecComService##**, where **##** is the **ID** number described in the **PART 1** table.
- Share the **SecComService##** folder so that any user from the GuardPoint10 server can write to this folder.
- Take note of the network path to the **SecComService##** folder (e.g. `\\NewPC\SecComService2`).
- On the same third-party machine, in the new **SecComService##** folder, open the **SecComService.exe.Config** file with a text editor.
- Change the **myNetGroupID** value so it contains the **ID** number found in the parent **SecComService##** folder name (e.g. Replace `value= "1"` with `value= "2"`).
- Change the **applicationPath** value so it contains the network path to the folder that has been shared previously (e.g. Replace `value= "C:\ProgramData\ACS\NM\Split"` with `value= "\\NewPC\SecComService2"`).
- Change the **serviceCorIP** value to match the IP address as the application server.
- Save and close the .Config file.
- In the same **SecComService##** folder, open the **SecComService.ini** file with a text editor.
- In both **SQL\_Connect** and **SQL\_Connect\_Main** entries, change the Data Source value so it contains the full SQL server name (e.g. Replace `Data Source=.\AC8sql` with `Data Source=A8Server\AC8sql,49999`).
- Save and close the .ini file.
- On the same third-party machine, in the new **SecComService##/MultiSplit** folder, open the **InstallSecComServiceSvc.bat** file with a text editor.
- Change the service name to **AcsSecComService##**, where **##** is the same **ID** number found in the parent **SecComService##** folder name.
- Save and close the .bat file.



17. In the **SecComService##/MultiSplit** folder, open Command Prompt as administrator from the File Explorer's **File** menu, and then click **Open command prompt as administrator**.



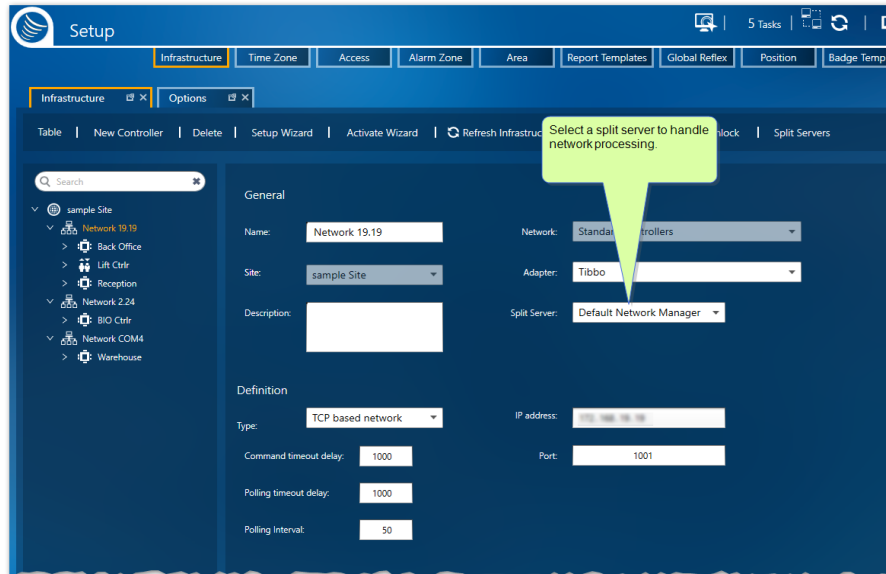
18. In the command prompt, type **InstallSecComServiceSvc.bat**. The .bat file launches in Administrator mode. This installs and starts the new service on the third-party machine.
19. On the 3rd party machine, create an exception in the Firewall to allow in Inbound Rules the UDP Port defined in the Split Servers window in **PART 1**.
20. In the Properties of the new service, open the **Log On** tab and add the relevant account credential details.



21. Press **OK**, and then restart the service.
22. On the GuardPoint10 server, open the Properties popup of the **AcsNMService** service and repeat steps **20** and **21**.

23. After all services are running, on GuardPoint10, click the **Split Servers** button in the action bar of the Infrastructure screen. The Split Servers window is displayed.
24. Enter the Polling path with the network path to the folder that has been shared previously on the third-party machine (e.g. \\NewPC\SecComService2).
25. Click **Save** in the Split Servers window.
26. Click the **Test** button in the relevant row (see the **PART 1** table) to make sure the communication between the AcsNMService and the Split Service is successful. Then click the **X** at the top right of the Split Servers window.
27. In the GuardPoint10 network's details, select the new Split Service from the **Split Server** drop-down list where the network will be hosted, and then click **Save**.

Figure 2-9



28. Restart the Split service previously assigned to the network to complete the communication switch to the new Split Service.

# Adding a New Network

Use the following steps to add a new network to an existing infrastructure.

## How to add a new network to an existing infrastructure

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the site item to place it in focus. The site parameters appear and the first action bar item changes to **New Network**.
3. Do one of the following:
  - » From the action bar, click **New Network**. Network details appear; the details include some default values.
  - » Right-click the site item in the infrastructure tree, and then select **New Network** from the context menu. Network details appear; the details include some default values.

Figure 2-10



4. Complete the detail fields, and then do one of the following:
  - » Click **Discard**, and then confirm the operation. The details are not saved and are removed from the screen.
  - » Click **Save**. The new network is saved in the system database and appears in the infrastructure tree.

Some of the information needed to complete the network details may be available from your hardware installation personnel.

Most network detail fields, including **Type** (Serial Based Network or TCP), can be edited at any time

For information about the network parameters, see ["Network Details" on page 445](#)

# Edit/Delete a Network

Use the following steps to edit or delete a network.

## How to edit network's details

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the network item that you want to edit. The network's details are displayed.
3. Edit the network parameters as required (see ["Network Details" on page 445](#)).



**Note:** Not all network parameter values will be editable.

4. After editing the network parameter values, do one of the following:
  - » Click **Discard**. The network parameters revert to their previously saved values.
  - » Click **Save**. The network parameter values are saved in the system database.

## How to delete a network

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the network item that you want to delete. The network's details are displayed.

If the network has a controller connected to it, the controller has to be deleted before you can delete the network (see ["Edit/Delete a Controller" on page 59](#)).

3. Do one of the following:
  - » Click **Delete** in the action bar and then confirm the operation. The empty network is deleted from the system database and removed from the infrastructure tree.
  - » Right-click the selected network and select **Delete** from the context menu, and then confirm the operation. The empty network is deleted from the system database and removed from the infrastructure tree.

# Adding a New Controller to a Network

Use the following steps to add a new controller to a network. These steps apply to both **Access Door** controllers and **Lift** controllers.

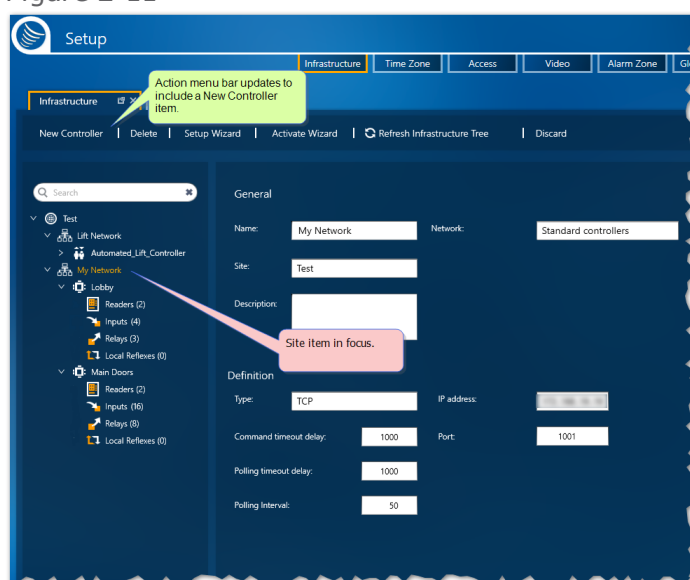
For information about Door and Lift controllers, see "[Controller Details](#)" on page 450 and "[Reader Details](#)" on page 453.

For information about Lift setup, see "[Understanding the Lift Setup concept in GuardPoint10](#)" on page 53.

## How to add a new controller to a network

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the network item where the new controller will be embedded. The network parameters appear and the first action bar item changes to **New Controller**.

Figure 2-11



3. Do one of the following:
  - » From the action bar, click **New Controller**. Controller details appear; the details include some default values.
  - » Right-click the site item in the infrastructure tree, and then select **New Controller** from the context menu. Controller details appear; the details include some default values.
4. Complete the detail fields, and then do one of the following:
  - » Click **Discard**, and then confirm the operation. The details are not saved and are removed from the screen.
  - » Click **Save**. The new controller is saved in the system database and appears in the infrastructure tree as a sub-item of the selected network.

Some of the information needed to complete the controller details may be available from your controller installation personnel.

After saving a controller, the controller's address and network can be changed from the controller details at any time.

For information about the controller parameters, see ["Controller Details" on page 450](#).

5. Because the saved controller has not been activated yet, the controller and its entities appear dimmed in the infrastructure tree. To activate the controller, do one of the following:
  - » From the action bar, click **Activation Wizard**. The first dialog of the Activation Wizard is displayed.
    - a. From the site tree, expand and select the controller(s) that you would like to activate. All controllers are selected by default.  
Selecting a controller that is already active will not adversely affect the controller.
    - b. Click **Activate** the second dialog in the wizard is displayed. This dialog shows a breakdown of the activation results.
    - c. Click **Finish**. The wizard is closed and the controller, with its entities, is activated and appears brighter in the infrastructure tree. The controller is also in focus and its details appear on the screen.
  - » Right-click the controller item in the infrastructure tree, and then select **Activate** from the context menu. The controller and its entities are activated and appear brighter in the infrastructure tree. The controller is also in focus and its details appear on the screen.

The difference between using the Activation Wizard and the context menu's Activate item is that in the wizard you can activate multiple controllers in one operation.



**Note:** After saving the new controller, it appears in the infrastructure tree with its supported entities (readers, inputs, relays, and local reflexes). The type of controller selected and installed determines the number of entities that will appear in the infrastructure tree as sub-items of the controller item. For more information about controller types and their supported entities, see ["Controller Support for Readers, Inputs, and Outputs" on page 711](#).

# Understanding the Lift Setup concept in GuardPoint10

A controller defined with a Purpose set to Lift, in the Infrastructure screen's controller details, represents a group of lifts. A group of lifts work together to manage destination control. A destination, within the context of lift control, refers to the floors of a building where a lift may stop to pick up or drop off passengers. A lift group may consist of one or more lifts.

Each lift has one reader installed in its passenger compartment. Each lift controller's reader represents one lift in a lift group.

Each floor button on the lift panel is connected to a controller relay. This means each lift controller's relay represents a floor button.

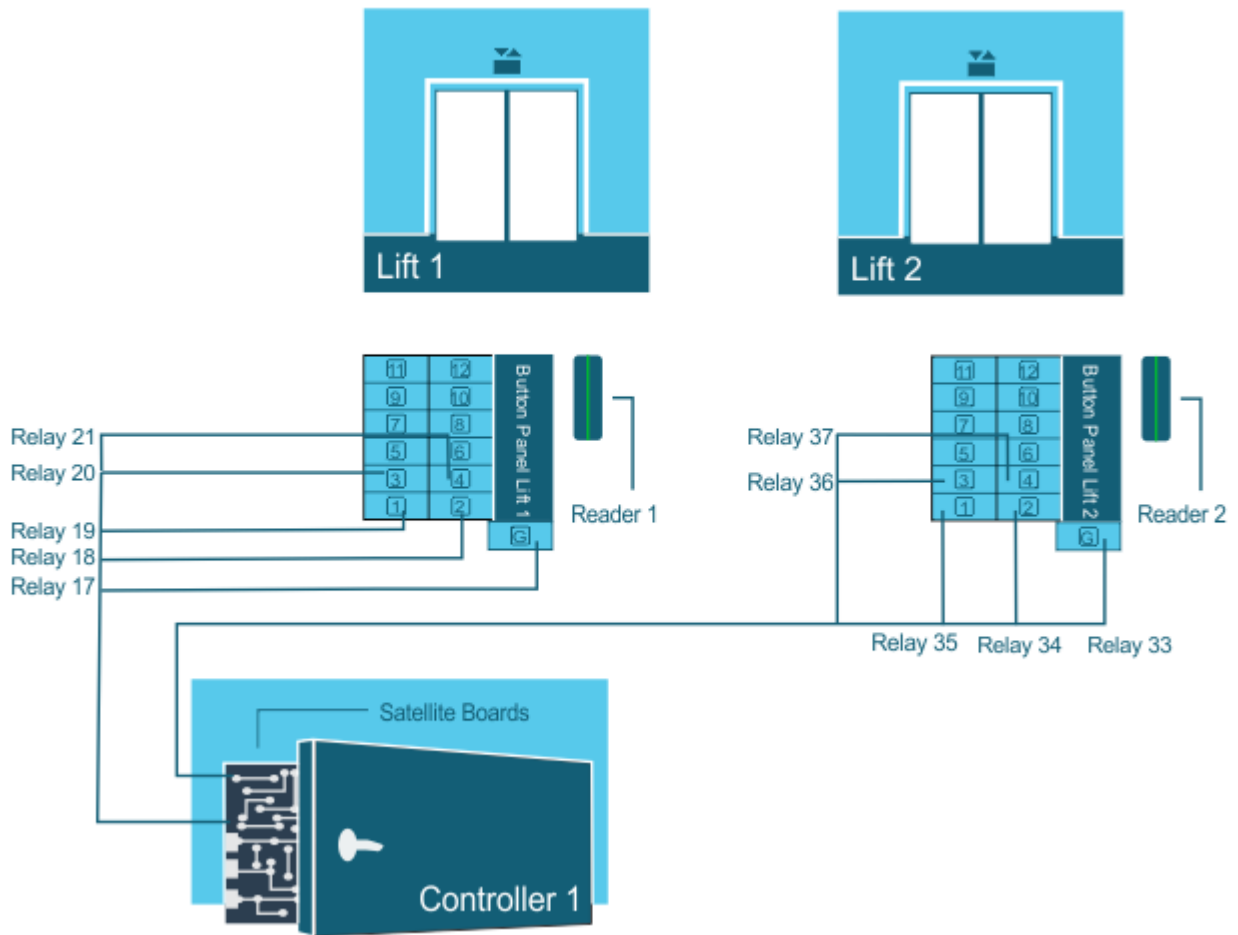
For clarity, a best practice is to rename the readers and the relays of a lift controller to better identify the physical relationship to a particular lift and floor (e.g. 'Lift1-Floor1', 'Lift1-Floor2', 'Lift2 -Floor1', etc.).

## Applying the Lift concept in a nutshell

A lift controller (IC2001, IC2000) may have up to 4 readers (i.e. lifts) and 64 relays (i.e. floor buttons).

When following the steps in this section, use the image below as a reference.

Figure 2-12



### Step\_1

1. Open GuardPoint10 and add the Lift controller to the system via the Infrastructure screen.
2. Rename the relays according to the Relay - Floor Correspondence table (e.g. Relay17 > Lift1-Ground Floor, Relay18 > Lift1-Floor1, etc.)
3. Installation personnel mount the controller, usually with a satellite board, at the top of a lift shaft, near the lift's I/O board, with a reader mounted in the passenger car, near the elevator button panel. The reader should be physically connected to the controller at this time.
4. After the hardware is in place, installation personnel physically connect the satellite board relays to the lift's I/O board.

A best practice is to fill out a Relay - Floor Correspondence table in a spreadsheet to track the connections.

### Step\_2

5. Determine the cardholder groups that will need specific floor access points via a lift. For example, cardholders in the Marketing team would need access to Floors 1 and 2, where the marketing department has their offices. The Development team would need access to Floors 3 and 4 where their offices are located.



- With the previous example in mind, open GuardPoint10 and go to the Setup > Access screen. Add a lift access group (LAG) for each lift and department combination as follows:

LAG Name	Relays Assignment
LAG_Marketing Reader 1	Relay17 Lift1-Ground Floor, Relay19 Lift1-Floor1, Relay18 Lift1-Floor2
LAG_Development Reader 1	Relay17 Lift1-Ground Floor, Relay20 Lift1-Floor3, Relay21 Lift1-Floor4
LAG_Marketing Reader 2	Relay33 Lift2-Ground Floor, Relay35 Lift2-Floor1, Relay36 Lift2-Floor2
LAG_Development Reader 2	Relay33 Lift2-Ground Floor, Relay36 Lift2-Floor3, Relay37 Lift2-Floor4

- After populating the LAGs with relevant relays, add the Development LAGs to the Multiple Access Group (MAG) dedicated to the Development team and the Marketing LAGs to the MAG dedicated to the Marketing team. These MAGs will eventually be assigned to cardholders in the Marketing team and Development team, respectively.

## How the cardholder experiences it

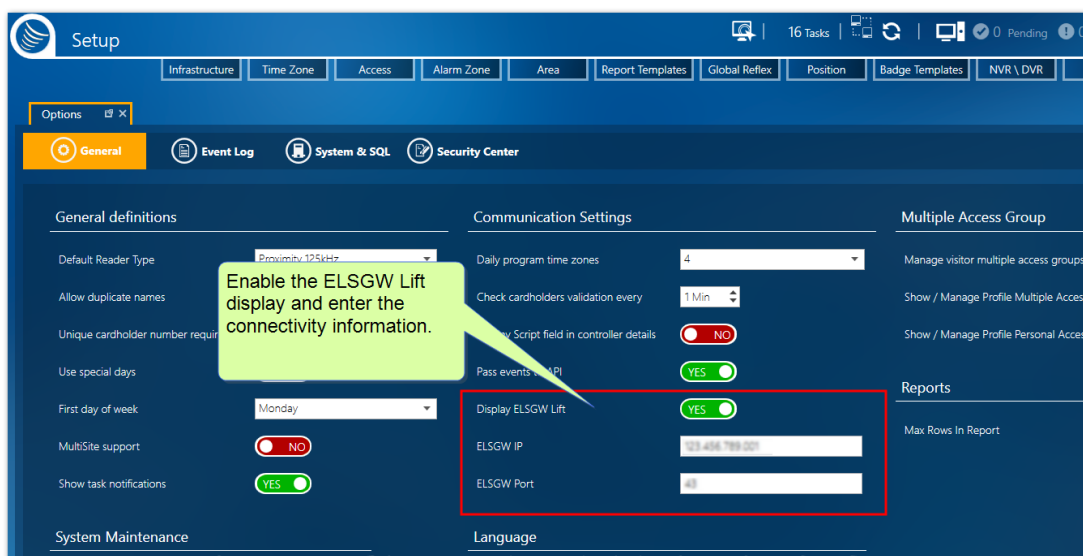
After a cardholder enters a lift car, they would swipe their badge at the badge reader. Only the floor buttons where the cardholder has access authorization are available. The other buttons will not function and therefore the floors will not be accessible.

# Understanding and setting up an ELSGW Lift in GuardPoint10

It is assumed the reader of this topic is familiar with the ELSGW Mitsubishi Lift. This topic describes the setup required to send data to the lift. The setup is not difficult, but it does cross over multiple GuardPoint10 screens.

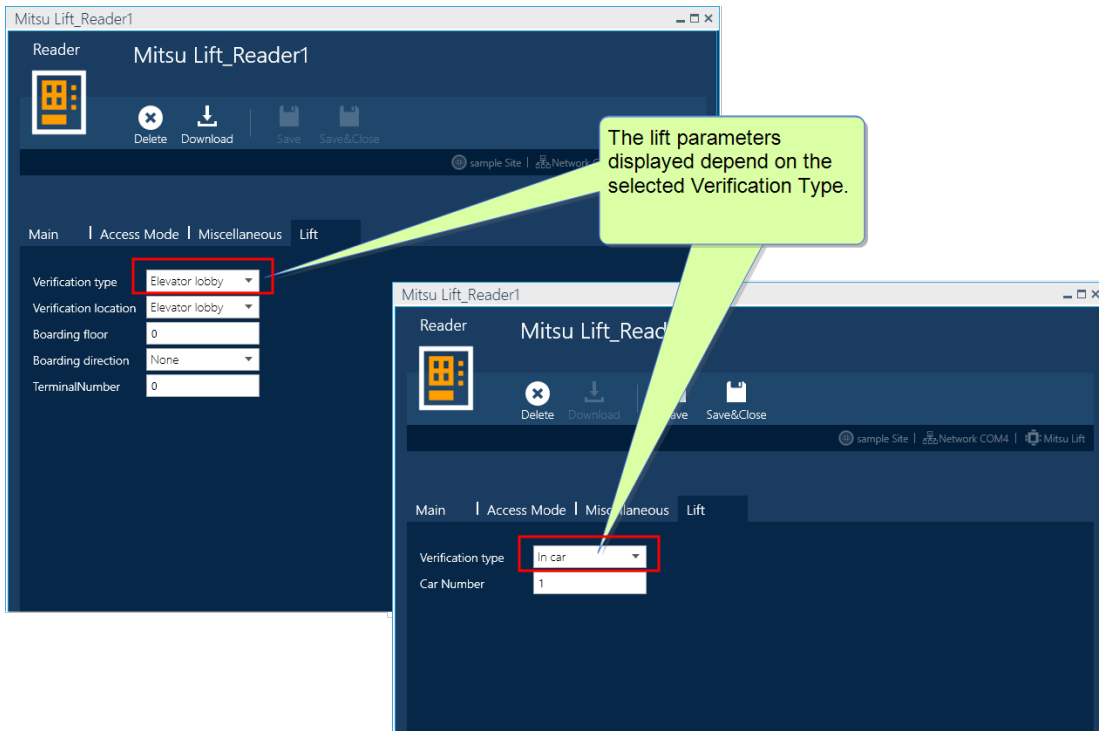
## Enter ELSGW Lift connection information and display ELSGW parameters in the GuardPoint10 GUI

1. Go to the Setup Task group and click **Options**. The Options screen is displayed.
2. In the Options category General, set **Display ELSGW Lift** to **Yes**. The **ELSGW IP** field and the **ELSGW Port** field are enabled.
3. Enter the **ELSGW IP** address and **ELSGW Port** number, and then click Save. Fields related to the ELSGW lift are now available in the **Infrastructure** and the **Access** screens.



## Add an ELSGW Lift controller to the infrastructure

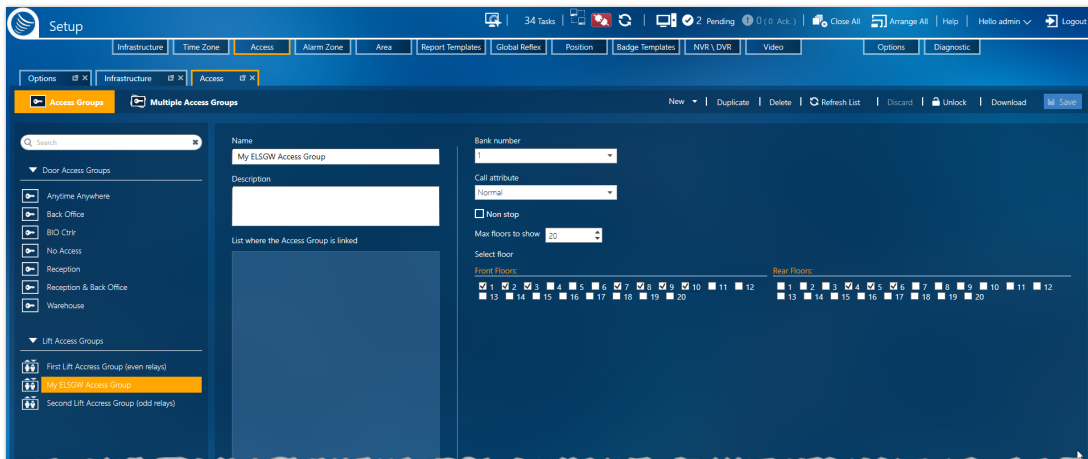
1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. Add a new network or select an existing network and add a controller with a **Purpose** Lift.
3. Open the Readers screen, and then open a reader's details. Each reader corresponds to a Lift car. An ELSGW specific **Lift** tab is displayed in the Reader details.
4. Open the Lift tab and complete the information in the displayed fields.



5. Save the reader. The corresponding relay (i.e. Reader1 to Relay1) will be automatically renamed. Do not change any information in the corresponding relay.

## Add an ELSGW Lift Access Group

1. Go to the Setup Task group and click **Access**. The Access screen is displayed.
2. On the left side of the action bar, select **Access Group**. The Access' Access Group screen is displayed.
3. From the action bar, click the **New** down arrow and select **ELSGW Access Group**.



4. Enter Access Group information as required for the ELSGW Lift:

- » Enter a new name for the Access Group.
  - » Select a bank number.
  - » Select Call attribute.
  - » Select the maximum number of floors to show.
  - » Choose the doors that will open on each floor. To prevent access to a floor, leave the check-boxes for that floor empty.
5. **Save** the ELSGW Lift Access Group, and assign it to a cardholder as you would any other access group.

# Edit/Delete a Controller

Use the following steps to edit or delete a controller.

## How to edit a controller

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the controller you want to edit. The controller's parameters appear.
3. Edit the controller parameters as required (see "[Controller Details](#)" on page 450), and then do one of the following:
  - » Click **Discard**, and then confirm the operation. The details revert to their previously saved values.
  - » Click **Save**. The new parameter values are saved in the system database and are also sent to the controller's local database.

In case of changing a controller's network, you may also have to change the controller's address to an available address in the new network. After saving the network change, the controller will automatically initialize.

## How to activate/deactivate a controller

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, right-click the controller you want to activate/deactivate. A context menu appears.
3. Do one of the following:

### If the controller is deactivated and you want to activate it:

- a. Click **Activate** in the context menu. A Controller Activation dialog is displayed.
- b. From the Controller Activation dialog, decide on the type of data transfer that will occur upon activation:
  - Load the pending events recorded since the controller was deactivated.
  - Load all controller-specific data from the system database on the controller's local database.
- c. Click **OK**. The controller is activated and the data transfer specified is performed.



**Note:** If the data in the system database and the data in the controller's local database are sync-ed at activation time, the Controller Activation dialog will be replaced with a message asking if you would like to load the pending events recorded since the controller was deactivated.

### If the controller is activated and you want to deactivate it:

Click one of the following deactivation options in the context menu:

- » Deactivate without clearing memory
- » Deactivate and clear memory to prevent access

The controller is deactivated and the data in the controller's local database may be altered to reflect the deactivation method selected.

## How to delete a controller

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the controller you want to delete. The controller parameters appear.
3. Do one of the following:
  - » Click **Delete** in the action bar and confirm the operation. The controller and any sub-entities are deleted from the system database.
  - » Right-click the controller and select **Delete** from the context menu, and then confirm the operation. The controller and any sub-entities are deleted from the system database.

## Adding a New Reader to a Controller

Use the following steps to add a new reader to a controller.

If the controller cannot support an additional reader, a message stating, "The maximum number of readers already exists", will appear and the Add New Reader operation will be aborted. However, if your technology permits, a reader already added to a controller may have a slave reader connected to it. To add a slave reader, see ["Adding a Slave Reader to a Controller" on page 64](#).

If the controller's **Purpose** is set to **Access**, the reader represents the device at a door where a scan (badge swipe) takes place.

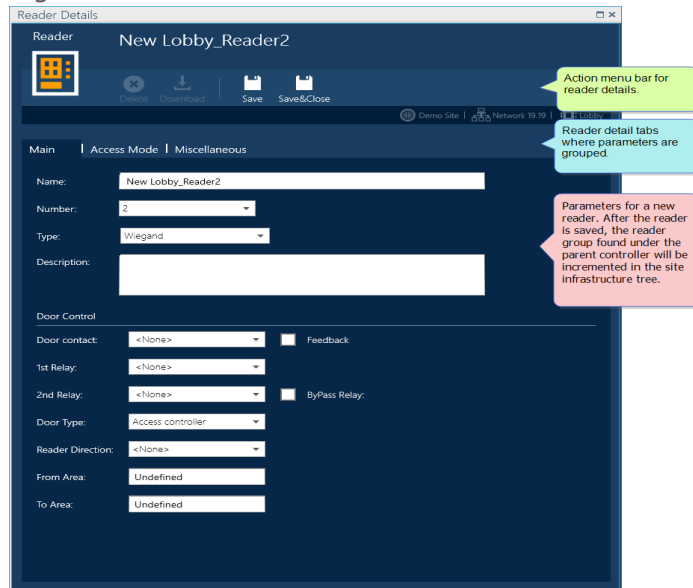
If the controller's **Purpose** is set to **Lift**, the reader represents the passenger compartment of a lift (elevator) where a scan takes place. For more information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10" on page 53](#).

## How to add a new reader to a controller

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the controller item where the new reader will be connected. The controller parameters appear and the first action bar item changes to a **New** drop-down list.
3. Do one of the following:
  - » From the action bar, click **New > Reader**. Reader details appear; the details include some default values.
  - » Right-click the controller item in the infrastructure tree, and then select **New > Reader** from the context menu. Reader details appear; the details include some default values.

If the maximum number of readers for the controller already exists, this context menu item will not be available.

Figure 2-13



4. Complete the detail fields (see ["Reader Details" on page 453](#)), and then click **Save**. The new reader is saved in the system database and is added to the infrastructure tree as a sub-item of the selected controller.

Some of the information needed to complete the reader details may be available from your hardware installation personnel.

5. Click **Download**. The reader data is sent to the controller's local database.

**Note:** The reader can be physically connected to the controller after you perform this operation.

If the physical connection is made before you perform the operation, the reader will automatically be added to the controller in the infrastructure tree, eliminating the need to perform the Add New Reader operation. However, you may still need to edit the details of the reader (see ["Edit/Delete a Reader" on page 67](#)).

# Adding a New Biometric Reader to a Controller

Use the following steps to add a new biometric reader to a controller.

If the controller cannot support an additional reader, a message stating, "The maximum number of readers already exists", will appear and the Add New Reader operation will be aborted. However, if your technology permits, a reader already added to a controller may have a slave reader connected to it as long as the master reader and slave reader are of the same type (Biometric). To add a slave reader, see ["Adding a Slave Reader to a Controller" on page 64](#).

If the controller's **Purpose** is set to **Access**, the reader represents the device at a door where a biometric scan takes place.

If the controller's **Purpose** is set to **Lift**, the reader represents the passenger compartment of a lift (elevator) where a biometric scan takes place.

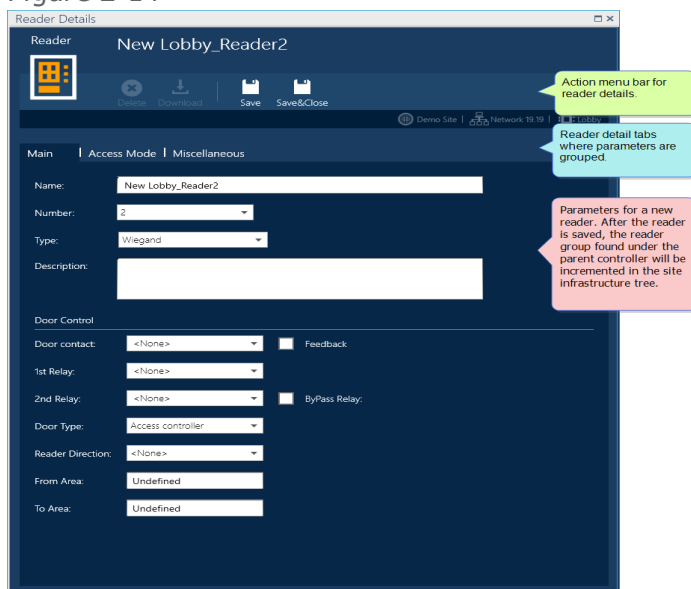
## How to add a new biometric reader to a controller

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the controller item where the new reader will be connected. The controller parameters appear and the first action bar item changes to a **New** drop-down list.
3. Do one of the following:

- » From the action bar, click **New > Reader**. Reader details appear; the details include some default values.
- » Right-click the controller item in the infrastructure tree, and then select **New > Reader** from the context menu. Reader details appear; the details include some default values.

If the maximum number of readers for the controller already exists, this context menu item will not be available.

Figure 2-14

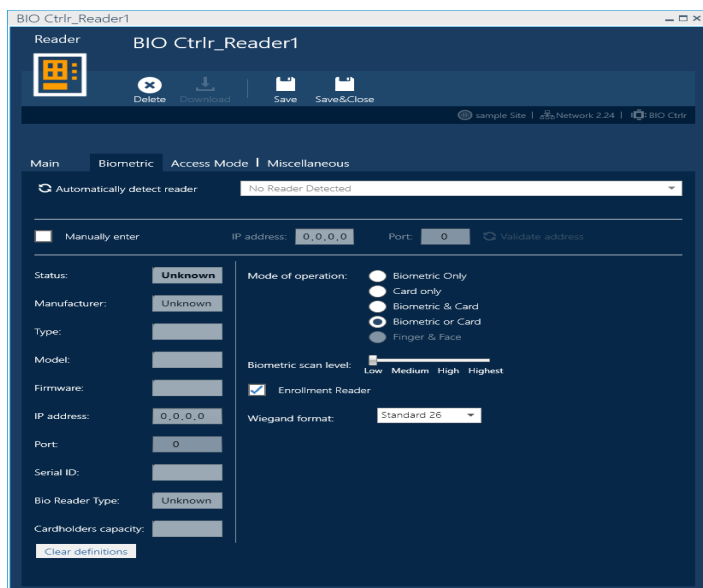


4. In the Main tab, select **Biometric** from the Type list. A Biometric tab appears in the reader details. **Biometric** and **Proximity 125kHz** are selected.



If the Biometric reader will also read smart cards, do not add **Smart Card 13.56 MHz** to the selected types. Instead, select **Mifare 32** in the Biometric tab's **Wiegand format** field.

5. Open the Biometric tab and do one of the following:



- » Click the **Automatically Detect Reader** button.

After the detection process is completed, all biometric readers in your system's LAN network will be listed in the **Automatically Detect Reader** drop-down list.

If a reader is already added to your system, the entry in the drop-down list will be disabled.

Select an available reader from the drop-down list. The fields below the drop-down list and on the left side of the partition are automatically filled with information gathered from the selected reader. These fields are read-only.

- » Select the **Manually Enter** checkbox and enter a known **IP Address** and **Port** number in the relevant biometric fields at the right of the checkbox.

Click the **Validate Address** button. The fields on the left side of the partition, below the **IP Address** and **Port** fields, are automatically filled with information gathered from the biometric reader using the information gathered from the manually entered IP Address and Port values. These fields are read-only.

6. In the **Mode of Operation** area, on the right side of the partition, select the cardholder input requirements necessary to determine the authentication of the cardholder at the selected reader (i.e. Card only, Biometric & Card, etc.).
7. After a biometric requirement was selected in the **Mode of Operation** area, select a Scan Level (Low, Medium, High, or Highest).

The Biometric scan level determines the degree of detail used when comparing a scanned biometric sample to biometric samples stored in the system database.

8. If the selected biometric reader will be used to add cardholder biometric samples to the system database, select the **Enrollment Reader** checkbox.

Badge code enrollment may also be performed from a biometric reader that can scan cards. This will require that the Mode of operation be set to **Card only** or **Biometric or Card**, and from the Main tab, select the **Enrollment reader** checkbox.

9. Select a biometric reader **Wiegand format**.

If the selected format is **Mifare 32-bit**, the Badge format in the Miscellaneous tab will be automatically set to Hexadecimal. **Do not change this setting unless specifically instructed.**

If the selected format is **Proximity 125kHz (Standard 26)**, the Badge format in the Miscellaneous tab can be set to Hexadecimal or Decimal.

10. Complete the non-biometric specific detail fields in the reader details tabs (see "[Reader Details](#)" on page 453), and then click **Save**. The new biometric reader is saved in the system database.

Some of the information needed to complete the reader details may be available from your hardware installation personnel.

11. Click **Download**. The reader data is sent to the controller's local database.



**Note:** If the IP address of a biometric reader is changed, go to the Infrastructure screen and delete the reader. After the reader is deleted, add it back to the infrastructure with the new IP address.

## Adding a Slave Reader to a Controller

A slave reader is a reader that uses parameter data from its master reader. The only slave reader parameters that are independent of the master reader are the slave's name and description. This means that the master reader and slave reader must be the same type (i.e. Regular, License Plate Recognition, or Biometric).

However, like any other reader, a slave reader's Weekly Program can be changed via the Access Group's Readers table (see "[Editing an Access Group](#)" on page 148).



**Note:** Whether or not a slave reader option is available, depends on the controller connected to the reader. If a slave reader is not an available option the **Has slave reader** checkbox will not appear in the reader's details.

### A common scenario where you would use a slave reader is as follows:

#### Brief:

The brief states that your controller is designated for three readers, one on each side of the same door and the third on a fire door.

Two readers are required to scan a cardholder's badge when entering or exiting from either side of the same door.

The fire door will have only one exit reader.

#### Issue:

The controller only supports two readers.

## Solution:

The entrance door (not the fire door) will have a standard reader installation (master) on one side, and a slave reader on the other side of the same door. This is done via the master reader's reader details.

Most of the slave reader's details will be linked to its master reader's details. This means that in the slave reader's details, some fields will be read-only. But, for example, the **T&A Reader** field will be enabled in both reader details so entrance and exit may be set individually.

About the physical connection to the controller:

IC2000: Master J1 --> Slave J1a, Master J2 --> Slave J2a

IC2001: Master J1 --> Slave J3, Master J2 --> Slave J4

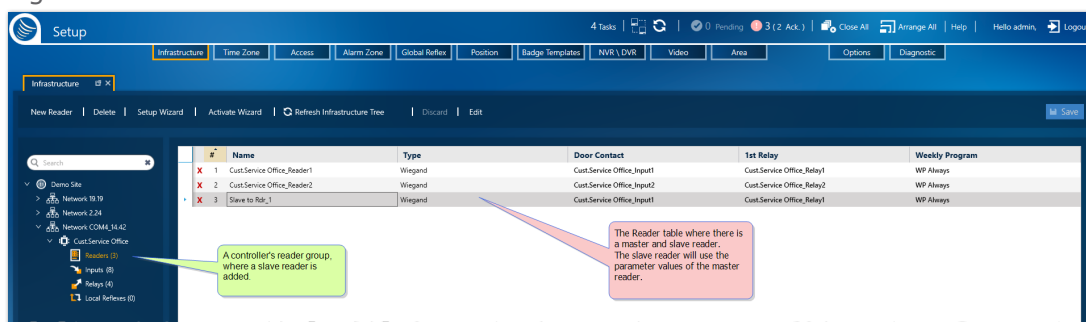
Use the following steps to add (define) a new slave reader.

## How to add a slave reader to a controller

This operation assumes that a standard reader already exists and is connected to the controller.

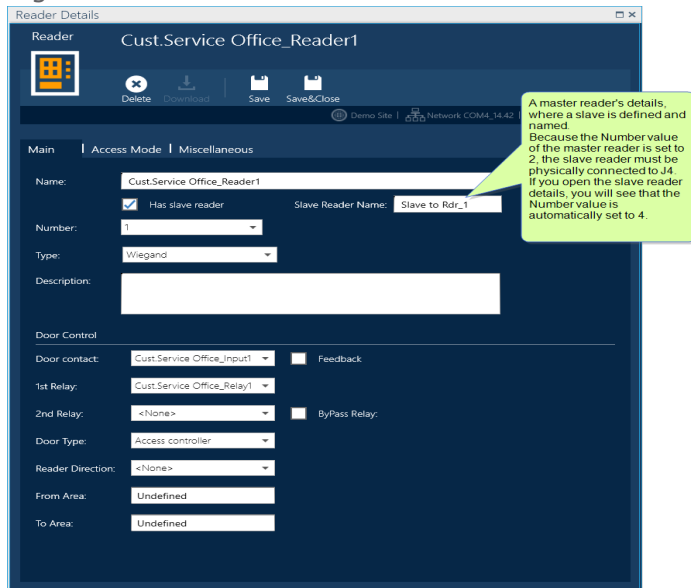
1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the reader item in the controller item where the slave reader will be connected. The Reader table is displayed.

Figure 2-15



3. Choose the reader that will be the master to the slave reader and click **Open details**. The reader's details are displayed.  
Keep in mind that the slave will be the same type as the selected master reader (i.e. Regular, License Plate Recognition, Biometric)
4. In the reader's details, select the **Has slave reader** checkbox. A Slave Reader Name parameter appears.

Figure 2-16



5. Enter a name for the slave reader and click **Save**. The slave reader data is saved in the system database and has its own set of reader details.
6. Click **Download**. Slave reader data is sent to the controller's local database.

**Note:** Not all controllers can support a slave reader. If a slave cannot be supported, the master reader details will not include a **Has slave reader** checkbox.


**Note:** A master reader can have only one slave reader.

# Edit/Delete a Reader

Use the following steps to edit or delete a reader.

## How to edit a reader's details

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the reader item in a controller parent item (i.e. Readers (2)). A Readers table is displayed.
3. Click the **Open details** button in a reader row where you want to edit parameter values. The reader's details are displayed.  
Alternatively, double-click the reader row where you want to edit parameter values. The reader's details are displayed.
4. Edit the reader parameters as required (see "[Reader Details](#)" on page 453).
5. Click **Save**. The new parameter values are saved in the system database.
6. Click **Download**. The new parameter values are sent to the relevant controller's local database.
7. Close the reader's details.




**Note:** If the reader has a slave reader, the slave reader's parameter values are also changed. If the reader being edited is a slave, you can only change the reader's name and description.

## How to only edit reader details visible in the Reader table

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the **Reader** item in a controller parent item (i.e. Readers (4)). A Readers table is displayed.
3. From the action bar, click **Edit** and then select a reader from the table. The details in the table are editable.
4. Edit the reader as required, and then click **Save**. The reader details are updated throughout the system.
5. As a precaution, right-click the **Readers** item in the infrastructure tree and click **Download Readers** in the context menu. The reader parameter values are sent to the relevant controller's local database and will overwrite any previously saved reader data in the local database.

To get out of Edit mode without saving your changes, click **Discard** in the action bar and confirm the don't save action.

Alternatively, press **Esc** on the keyboard. Edit mode is stopped and the non-saved reader name will appear with red text until it is saved or discarded.



**Note:** If the reader being edited is a biometric reader that is connected to the system, the **Status** of the reader, in the Biometric tab, will appear to be **Not Connected** when the tab is opened -this is not the true value. After the reader details are saved, the **Status** display will change to **Connected**.

## How to delete a reader

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the reader item in a controller parent item (i.e. Readers (2)). A Readers table is displayed
3. Click the **Delete** icon (red **x**) in the reader row that will be deleted, and then confirm the operation. The reader is deleted from the system database and the relevant controller's local database.
4. As a precaution, right-click the **Readers** item in the infrastructure tree and click **Download Readers** in the context menu. The new parameter values are sent to the controller's local database.



**Note:** If the deleted reader had a slave reader, the slave reader is also deleted from the system database and the controller's local database.

# Managing a Mantrap

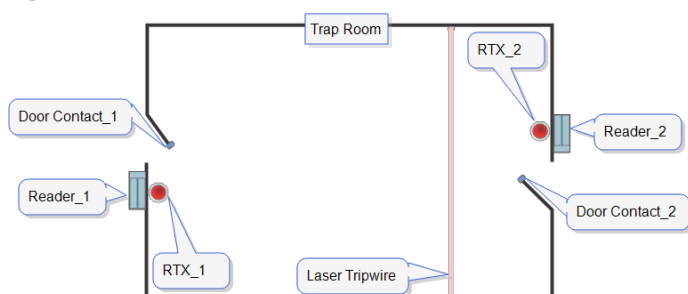
## What's a mantrap

A mantrap is a small room with a door on one wall and another door on the opposite wall. One door of a mantrap cannot be unlocked and opened until the opposite door has been closed and locked. These are called interlocking doors.

Mantraps are often used to separate non-secure areas from secure areas and prevent unauthorized access. They can also be found in hitech manufacturing to provide an entry and exit chamber for a cleanroom.

The following illustrates the general layout of a mantrap.

Figure 2-17



There are three types of mantrap. Each type of mantrap will have variations, but the concept is the same. The following is a description of each type of mantrap (mantrap 2 does not exist):

- » **Mantrap 1:** A door is opened after access is granted via its reader or RTX button (the door status is given by the door contact defined for that door), a second access cannot be granted from the same reader until the opposite door is opened and then closed. This opposite door may be opened either through its reader (if it is located inside the mantrap) or with its RTX button.

### How it works, step-by-step (follow along with the illustration above):

1. A cardholder swipes their badge at reader\_1, input 1 activates, which unlocks Door Contact\_1 and the cardholder enters. The cardholder is now in the mantrap.
2. After Door Contact\_1 is closed and relocked, input 4 activates RTX\_2 and the cardholder presses the RTX\_2 button to unlock Door Contact\_2.
3. After the RTX\_2 button is pressed by the cardholder, input\_2 unlocks Door Contact\_2 and the cardholder can open the door and exit the mantrap.

- » **Mantrap 3:** A door is opened after access is granted via its reader or RTX button (the door status is given by the door contact defined for that door), a second access cannot be granted from the same reader until the opposite door is opened and then closed. After the initial door is closed, the opposite door is automatically opened.

### How it works, step-by-step (follow along with the illustration above):

1. A cardholder swipes their badge at reader\_1, input\_1 activates, which unlocks Door Contact\_1 and the cardholder enters. The cardholder is now in the mantrap.

2. After Door Contact\_1 is closed and relocked, input\_2 **automatically** unlocks Door Contact\_2 and the cardholder can open the door and exit the mantrap.

» **Mantrap 4:** A door is opened after access is granted via its reader or RTX button (the door status is given by the door contact defined for that door), a second access cannot be granted from the same reader until the opposite door is opened and then closed. This opposite door is opened automatically when a controller input is triggered (i.e. a laser tripwire is crossed as a cardholder approaches the opposite door. In the example of the laser tripwire, the tripwire input would be defined in the reader details' **Controlled By** field (see "[Controlled By \(may not be visible\)](#)" on [page 458](#)).

**How it works, step-by-step (follow along with the illustration above):**

1. A cardholder swipes their badge at reader\_1. Activates input 1, which unlocks Door Contact\_1 and the cardholder enters. The cardholder is now in the mantrap.
2. After Door Contact\_1 is closed and relocked, the input selected in the reader details' **Controlled by** field **automatically** activates its connected device (i.e. a laser tripwire).
3. After the tripwire is triggered by the cardholder, input\_2 unlocks Door Contact\_2 and the cardholder can open the door and exit the mantrap.

A 2-door controller may manage one mantrap with readers 1 and 2. A 4-door controller may manage 2 mantraps, one with readers 1 and 2, and the other with readers 3 and 4.

For information about implementing a mantrap, see "[Adding a Mantrap](#)" on [page 72](#).

## How to Prevent a cardholder from being stranded in a mantrap

While in operation, a mantrap will have a default timeout delay. This means that when a cardholder is granted access to a mantrap, the mantrap doors are locked until the cardholder exits the mantrap from the opposite door. However, if the cardholder remains inside the trap for more than 60 seconds, a timeout will occur. This means both doors will be automatically unlocked.

To override the timeout's 60 seconds delay, select the **Relay Open During All Open Time** checkbox in the reader details' Miscellaneous tab.



**Warning:** If you override the timeout delay, as described above, the readers will stay **locked** until the cardholder exits the mantrap or until the readers are manually unlocked.

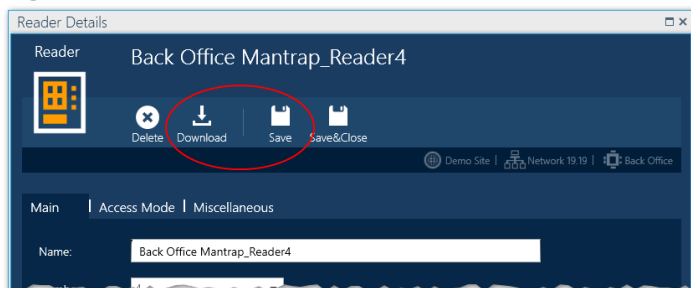
## How to manually unlock a mantrap reader

Mantrap readers are unlocked as soon as one of the reader's details is downloaded to the controller. Reader details are downloaded by doing one of the following:



- » Click **Save** or **Download** in the reader's details.

Figure 2-18



- » From the Diagnostic screen, select the Controller with the mantrap in the tree, and then click **Download > Send Reader Definitions** or **Initialization**.

# Adding a Mantrap

## How to add and test a mantrap

It is recommended that you review "[Managing a Mantrap](#)" on page 69 before you add a mantrap to your system.

The mantrap described in this topic is bi-directional. The controller must be able to support more than one door.

1. After setting up a controller, open the **Reader** details for **Reader1** and **Reader2** from the same controller.
2. Make the following field settings:
  - » Reader1 Main tab:
    - Door contact: input\_1
    - 1st Relay: Relay1
    - 2nd Relay: Relay2
    - Door type: Man Trap 1
    - Controlled by: Input1
  - » Reader1 Access Mode:
    - Door remote input: Input3
  - » Reader2 Main tab:
    - Door contact: input\_2
    - 1st Relay: Relay2
    - 2nd Relay: Relay1
    - Door type: Man Trap 1
    - Controlled by: Input2
  - » Reader2 Access Mode:
    - Door remote input: Input4

## Mantrap 1: Behavior test

Add two cardholders with badges that are authorized at **Reader1** and **Reader2**.

1. Swipe Badge1 at Reader1. Door1 is unlocked. An Access granted event occurs.
2. Trigger Input1. Simulates Door1 is opened and closed. The cardholder is in the mantrap room.
3. Swipe Badge2 at Reader1. Access denied because one cardholder is already in the mantrap room.
4. Press Input4 (RTX). Door2 is unlocked. An Access granted event occurs.
5. Trigger Input2. Simulates Door2 is opened and closed. The cardholder has exited the mantrap room.

6. Swipe Badge2 at Reader1 again. This time, Door1 is unlocked. Access granted event occurs for the second cardholder.

Because we set up both readers, the mantrap will work in both directions (starting from Door1 or Starting from Door2).

## Adding a New Input Device to a Controller

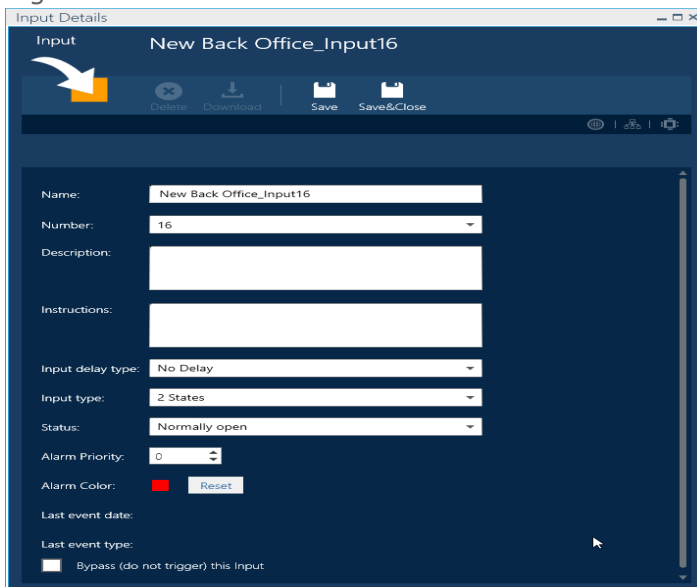
Use the following steps to add a new input device to a controller.

If the controller cannot support an additional input device, a message stating, "The maximum number of input devices already exists", will appear and the Add New Input operation will be aborted.

### How to add a new input device to a controller

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the controller item where the new input device will be connected. The controller parameters appear and the first action bar item changes to a **New** drop-down list.
3. Do one of the following:
  - » From the action bar, click **New > Input**. Input details appear; the details include some default values.
  - » Right-click the controller item in the infrastructure tree, and then select **New Input** from the context menu. Input details appear; the details include some default values.

Figure 2-19



4. Complete the detail fields (see "Zone Details" on page 499), and then click **Save**. The new input is saved in the system database and appears in the infrastructure tree as a sub-item of the selected controller.

Some of the information needed to complete the input details may be available from your hardware installation personnel.

5. Click **Download**. The input data is sent to the relevant controller's local database.

For information about an input device's physical connection to a controller, see ["Default Connections for Inputs, Relays, and RTX" on page 712](#).

## Edit/Delete an Input Device

Use the following steps to edit or delete an input device.

### How to edit an input device's details

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the **Input** item in a controller parent item (i.e. Input (8)). An Inputs table is displayed.
3. Click the **Open details** button in the input row where you want to edit parameter values. The input's details are displayed.
4. Edit the input parameters as required (see ["Input Device Table" on page 480](#)).



**Note:** Not all input parameter values will be editable.

5. Click **Save**. The new parameter values are saved in the system database and the relevant controller's local database.
6. As a precaution, right-click the input item in the infrastructure tree and click **Download Inputs** in the context menu. The new parameter values are sent to the relevant controller's local database.

### How to only edit an input device's details visible in the Inputs table

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the **Inputs** item in a controller parent item (i.e. Input (8)). An Inputs table is displayed.
3. From the action bar, click **Edit**. The input details in the table are now editable and then select an input name from the table. The name is in edit mode.
4. Rename the input, or perform any other edits, as required, and then click **Save**. The input name is changed throughout the system.

Not all fields in a table row are editable using this method.


5. As a precaution, right-click the **Inputs** item in the infrastructure tree and click **Download Inputs** in the context menu. The input parameter values (including the newly named input) are sent to the relevant controller's local database and will overwrite any previously saved input data in the local database.

To get out of Edit mode without saving your changes, click **Discard** in the action bar and confirm the don't save action.


Alternatively, press **Esc** on the keyboard. Edit mode is stopped and the non-saved input name will appear with red text until it is saved or discarded.

## How to delete an input

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the input item in a controller parent item (i.e. input (8)). An Inputs table is displayed.
3. Click the **Delete** icon (red **x**) in the input row that will be deleted, and then confirm the operation. The input is deleted from the system database and the relevant controller's local database.

Alternatively, double-click an input row to display the input's details, and then click  and confirm.

4. As a precaution, right-click the **Input** item in the infrastructure tree and click **Download Inputs**

in the context menu. If you are working from the input's details, click . The input parameter values are sent to the relevant controller's local database and will overwrite any previously saved input data.

## Adding a New Relay to a Controller

Use the following steps to add a new relay to a controller.

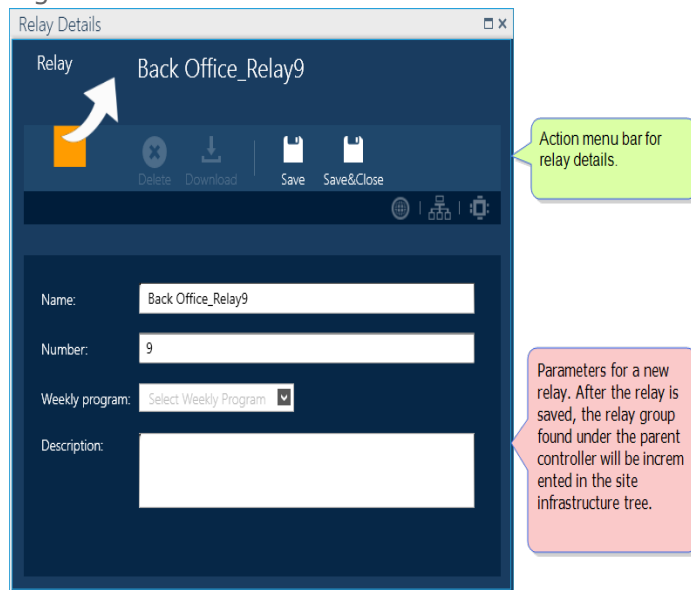
If the controller cannot support an additional relay, a message stating, "The maximum number of relays already exists", will appear and the Add New Relay operation will be aborted.

If the controller, where the relay is being added has its **Purpose** parameter set to **Lift**, the reader represents the passenger compartment of the lift (elevator) and the relay represents a floor where the lift may stop for passengers. For more information about Lift setup, see "[Understanding the Lift Setup concept in GuardPoint10](#)" on page 53.

## How to add a new relay to a controller

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the controller item where the new relay will be connected. The controller parameters appear and the first action bar item changes to **New**.
3. Do one of the following:
  - » From the action bar, click **New > Relay**. Relay details appear; the details include some default values.
  - » Right-click the controller item in the infrastructure tree, and then select **New > Relay** from the context menu. Relay details appear; the details include some default values.

Figure 2-20



4. Complete the detail fields (see ["Relay Details" on page 485](#)), and then click **Save**. The new relay is saved in the system database and is added to the infrastructure tree as a sub-item of the selected controller.

Some of the information needed to complete the relay details may be available from your hardware installation personnel.

5. Click **Download**. The relay data is sent to the relevant controller's local database.

For information about a relay's physical connection to a controller, see ["Default Connections for Inputs, Relays, and RTX" on page 712](#).

## Edit/Delete a Relay

Use the following steps to edit or delete a relay.

### How to edit a relay's details

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the relay item in a controller parent item (i.e. Relay (4)). A Relays table is displayed.
3. Click the **Open details** button in the relay row where you want to edit parameter values. The relay's details are displayed.
4. Edit the relay parameters as required (see ["Relays Table" on page 488](#)).
5. Click **Save**. The new parameter values are saved in the system database and the relevant controller's local database.
6. As a precaution, right-click the relay item in the infrastructure tree and click **Download Relays** in the context menu. The new parameter values are sent to the relevant controller's local database.

## How to only edit relay details visible in the Relays table


1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the **Relay** item in a controller parent item (i.e. Relay (8)). A Relays table is displayed.
3. From the action bar, click **Edit**. The relay details in the table are now editable.
4. Edit the relay details as required, and then click **Save**. The relay details update throughout the system.
5. As a precaution, right-click the **Relays** item in the infrastructure tree and click **Download Relays** in the context menu. The relay parameter values (including the newly update relay) are sent to the relevant controller's local database and will overwrite any previously saved relay data.

To get out of Edit mode without saving your changes, click **Discard** and confirm the don't save action.


Alternatively, press **Esc** on the keyboard. Edit mode is stopped and the non-saved relay name will appear with red text until it is saved or discarded.

## How to delete a relay

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the relay item in a controller parent item (i.e. Relay (4)). A Relays table is displayed.
3. Click the **Delete** icon (red **x**) in the relay row that will be deleted, and then confirm the operation. The relay is deleted from the system database and the relevant controller's local database.

Alternatively, double-click a relay row to display the relay's details, and then click  and confirm.

4. As a precaution, right-click the **Relays** item in the infrastructure tree and click **Download**

**Relays** in the context menu. If you are working from the relay's details, click . The relay parameter values are sent to the relevant controller's local database and will overwrite any previously saved relay data in the local database.

## Adding a New Local Reflex to a Controller

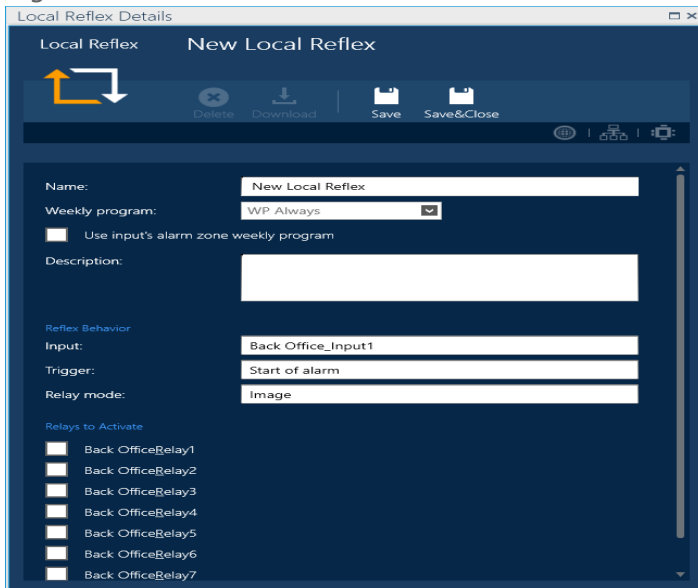
Use the following steps to add a new local reflex to a controller.

### How to add a new local reflex to a controller

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the controller item where the new local reflex will be located. The controller parameters appear and the first action bar item changes to a **New** drop-down list.
3. Do one of the following:

- » From the action bar, click **New > Local Reflex**. Local reflex details appear; the details include some default values.
- » Right-click the controller item in the infrastructure tree, and then select **New Local Reflex** from the context menu. Local reflex details appear; the details include some default values.

Figure 2-21



4. Complete the detail fields (see "[Local Reflex Details](#)" on page 490), and then click **Save**. The new local reflex is saved in the system database and appears in the infrastructure tree as a sub-item of the selected controller.
5. Click **Download**. The local reflex data is sent to the relevant controller's local database.

## Edit/Delete a Local Reflex

Use the following steps to edit or delete a local reflex.

### How to edit a local reflex's details

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the local reflex item in a controller parent item (i.e. Local Reflex (2)). A Local Reflex table is displayed.
3. Click the **Open details** button in the local reflex row where you want to edit parameter values. The local reflex's details are displayed.

Alternatively, double-click the local reflex row where you want to edit parameter values. The local reflex's details are displayed.

4. Edit the local reflex parameters as required (see "[Local Reflex Details](#)" on page 490).
5. Click **Save**. The new parameter values are saved in the system database.
6. Click **Download**. The new parameter values are sent to the relevant controller's local database.
7. Close the local reflex's details.



## How to delete a local reflex

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the local reflex item in a controller parent item (i.e. Local Reflex (2)). A Local Reflex table is displayed
3. Click the **Delete** icon (red **x**) in the local reflex row where you want to delete the local reflex, and then confirm the operation. The local reflex is deleted from the system database and the relevant controller's local database.
4. As a precaution, right-click the local reflex item in the infrastructure tree and click **Download** in the context menu. The new parameter values are sent to the relevant controller's local database.

## After the Infrastructure is Setup, What's Next?

After the initial infrastructure is completed, a best practice is to do the following:

1. Rename the various parts of the infrastructure to make it more intuitive and user-friendly. Examine details of the various elements in the infrastructure and use the corresponding Help topics as a reference.
2. Add operators (see ["Operators \(Users\)" on page 103](#)).
3. Configure time zones (see ["Daily Program Time Zones" on page 114](#)).
4. Configure Access (see ["Access" on page 139](#)).
5. Configure badges and cardholders (see ["Badges" on page 175](#) and ["Cardholders" on page 193](#)).
6. Configure Alarm Zones, Video, Position, etc., depending on the components available in your installation.
7. Update the infrastructure as required. Updates can be performed at any time during a session as long as the operator has authorization via their assigned profile.

# Understanding Anti-passback in GuardPoint10

Anti-passback is designed to prevent misuse of the access control system. It establishes a specific sequence in which badges must be used for the system to grant access.

There are three Anti-passback variations available in GuardPoint10:

- » Anti-passback (APB): Entry and exit readers connected to the same controller are set in a way to deter any cardholder from gaining access if the specified pattern is disturbed. For example, if a cardholder bypasses an entry/exit reader without swiping their badge and tries to access the subsequent reader, the rule is enforced and access is denied.
- » Timed AntiPassBack (TAPB): A cardholder can re-use their badge after a specified time since the last access event at the same reader. Generally, TAPB is used where there is no exit reader connected to the same controller, and the security administrator wants to stop multiple badge swipes by a single badge in quick succession.
- » Global Anti-PassBack( GAPB): Requires that readers be used in a designated sequence to enter or leave an GuardPoint10 defined area. This means that GAPB rules are centered on predefined areas. GAPB forces a cardholder to take a particular path to a destination via one or more areas.

After a cardholder swipes their badge at an area's entrance reader, where they are granted access, the cardholder will be denied access at any other reader except for the area's anti-passback exit reader.

The readers in a GAPB area do not have to be on the same controller as in APB or TAPB.

The GAPB can be extended to include multiple areas connected by the same reader. The exit reader of one area set to GAPB can be an entrance to another area set to GAPB.

All readers participating in a GAPB must be set to Anti-Passback in the reader's details.

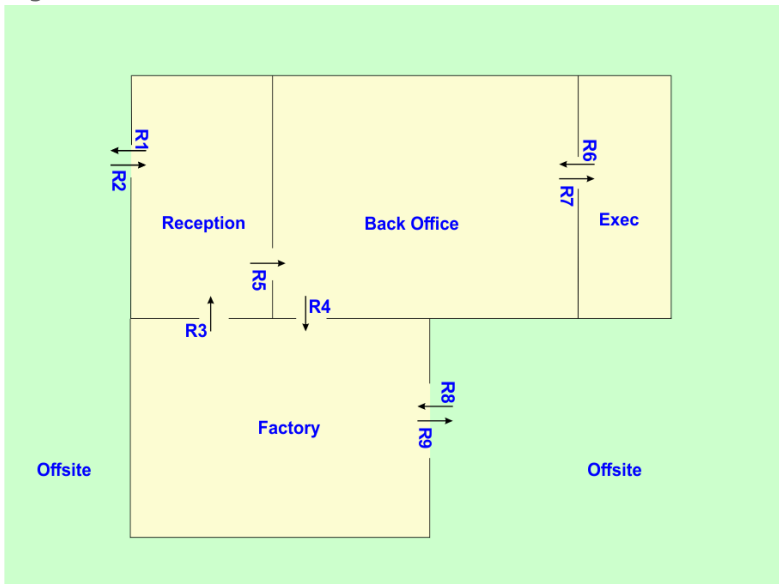
## Anti-Passback rule impact on cardholders

- » There are two ways a cardholder can be excluded from all types of Anti-Passback rule enforcement:
  - » If a cardholder's **Clear Area** button is clicked, the cardholder is automatically moved to offsite and they will receive one free Access Granted event at the next badge swipe regardless of the reader where the swipe takes place, This will also synch the Area value and the GAPB level value and automatically move the cardholder to the reader's area (assuming the reader is in an area). This free Access Granted event is sometimes called a *Soft Anti-Passback*. The system accepts the Access Granted event, even though it violates the Anti-Passback rules.
  - » If a cardholder's details have the 'No APB, No Timed Anti-Passback, and No GAPB rule enforcement' checkbox selected, Access will be granted where a cardholder without the checkbox selected will be denied access due to Anti-Passback rule enforcement.
- » It is important to understand that Anti-Passback rules, which determine a cardholder's level, are different than the rules that determine a cardholder's physical location in an area.

For example, using the floorplan image below, a cardholder is in Anti-Passback level Offsite and they swipe at reader R4 to get from Back Office to Factory. This will result in an Access Denied event due to the Anti-Passback rule. However, there is another rule for Area that is also in play.

Because the badge swipe took place at reader R4 in Back Office, the cardholder's Area value is automatically moved to Back Office. The system assumes that the cardholder must physically be in Back Office to perform the badge swipe. As a result, the cardholder's GAPB value remains Offsite and their Area value is Back Office. The Area rules and the Anti-Passback rules act independently.

Figure 2-22



## GAPB communication and commands

**Note:** Each controller in a network must have firmware dated 1/10/2019 or later to read the badge codes and apply GAPB rules. A controller's firmware date can be found in the Diagnostic screen.

- » **Command 26:** After access is granted to a cardholder, the controller, where the event took place, broadcasts an update to the cardholder's GAPB level with the cardholder's badge codes. This command broadcasts to networks in the system. Every time the cardholder moves from an area with GAPB. Command 26 is sent to all other networks where there is a reader with a GAPB level and where the cardholder can access (i.e. via MAG or Personal DAG).
- » **Command 76:** This command is sent with command 26 and includes all of the cardholder's badge codes.
- » **Command 79:** is sent at each badge swipe. If access is not granted to the cardholder, this is the only command sent.

In the Options screen, there is a GAPB setting called **Allow feature without PC**. When set to **Yes**, a controller will send the command 26 to all relevant controllers on the same network as the broadcasting controller.

# Integrating a Galaxy System into the Infrastructure

The Galaxy system's panel(s) must be configured before the Galaxy system can be integrated into the GuardPoint10 infrastructure. For more information about Galaxy panel configuration, see ["Configuring a Galaxy system panel" on the facing page](#).

Use the following steps to integrate an existing Galaxy system into your infrastructure.

## How to add an existing Galaxy system into your infrastructure

### The Network

1. Go to the Setup Task group and click **Infrastructure**. The Infrastructure screen is displayed.
2. From the infrastructure tree, click the site item to place it in focus. The site parameters appear and the first action bar item changes to **New Network**.
3. Do one of the following:
  - » From the action bar, click **New Network**. Network details appear; the details include some default values.
  - » Right-click the site item in the infrastructure tree, and then select **New Network** from the context menu. Network details appear; the details include some default values.

Figure 2-23



4. In the **Network** field select **Galaxy Panel** from the drop-down list.
5. Complete the detail fields, and then do one of the following:
  - » Click **Discard**, and then confirm the operation. The details are not saved and are removed from the screen.

- » Click **Save** and confirm. The Galaxy network is saved and appears in the infrastructure tree. Some of the information needed to complete the Galaxy network details may be available from your hardware installation personnel.
- For information about the network parameters, see ["Galaxy Panel Details" on page 494](#).

### The Galaxy Panel

1. After adding the Galaxy network, do one of the following:
  - » From the action bar, click **New Controller**. Galaxy panel details appear; the details include some default values.
  - » Right-click the Galaxy network item in the infrastructure tree, and then select **New Controller** from the context menu. Galaxy panel details appear; the details include some default values.
2. Complete the panel details, and then click **Save** and confirm. The Galaxy integration is completed and appears in the infrastructure tree with a Zone item under the panel.

The Zones item includes a table of zones found in the panel. A Galaxy zone is the equivalent of an GuardPoint10 input.

For more information about Galaxy zones, see ["Galaxy Zone Table" on page 496](#) and ["Zone Details" on page 499](#).

## Configuring a Galaxy system panel

This is a prerequisite before integrating a Galaxy system into the GuardPoint10 infrastructure.

Use the following steps to configure an existing Galaxy system before integrating it into your GuardPoint10 infrastructure.

The configuration of the Galaxy IP interface and its port is done via the LCD/Keypad unit of the panel, or

the Galaxy Frontshell program at its RSS / Ethernet screen.

(The default user / password of the "Frontshell" is **manager/password**).

### How to configure an existing Galaxy system panel via a Galaxy panel's LCD/Keypad

1. In the Galaxy Panel, set the DIP Switch number **8** switch to **OFF**.
2. Set the panel to **Engineer Mode** via the keypad as follows:

**Table 2-2** Change to **Engineer Mode**

Step	Press Keys	Display Shows
1	12345 [ent] [ent] [ent]	10=SETTINGS [ent] to Select

Step	Press Keys	Display Shows
2	48 [ent] [ent] [ent]	Engineer 0=DISABLED
3	1	Engineer 1=ENABLED
4	[ent]	System Access 1=Engineer
5	[esc] [esc] [esc] [esc]	"Galaxy" or "Engineer Mode" hh:mm DDD dd MMM (Time&Date)

3. While in **Engineer Mode**, set the panel **Ethernet configuration** via the keypad as follows:

Table 2-3 Change the **Ethernet configuration**

Step	Press Keys	Display Shows
1	112233 [ent] [ent]	10=SETTINGS [ent] to Select
2	56 [ent]	[ent] to Select 1=INT TELECOMS
3	4	[ent] to Select 4=ETHERNET
4	[ent]	01=MODULE CONFIG

4. At this point, type in numbers or use the arrows on the keypad to browse between the ten menus available in MODULE CONFIG:

- » **01=MODULE CONFIG**
- » **02=ALARM REPORT**
- » **03=REMOTE ACCESS**
- » 04=AUTOTEST
- » 05=ENGINEER TEST
- » 06=FAIL TO COMM
- » 07=LINE FAIL
- » **08=SIA CONTROL**
- » **09=ENCRYPT**
- » 10=BACKUP MODULE

The menu items relevant for GuardPoint10 integration are in **bold** text.

5. For GuardPoint10 integration, the relevant Galaxy panel MODULE CONFIG menu items are as follows:

Table 2-4 01=MODULE CONFIG

Sub-menu Item	Keypad Action
CONFIG 1=IP ADDRESS]	Type the IP of the Galaxy panel

Sub-menu Item	Keypad Action
4=NETWORK MASK	Set the subnet mask (default 255.255.255.0)

02=ALARM REPORT

Sub-menu Item	Keypad Action
1=FORMAT	<p>Set all 20 Trigger Events to ON, follow the example diagram for the first two:</p> <p>Figure 2-24</p> <pre> graph TD     A[1=Format] --&gt; B[SIA]     B --&gt; C[4]     C --&gt; D[TRIGGER EVENT]     D --&gt; E[01]     D --&gt; F[02]     E --&gt; G[Status]     F --&gt; H[Status]     G --&gt; I[1=ON]     H --&gt; J[1=ON]           </pre>
2=PRIMARY IP	<p>1=IP ADDRESS: Type 2=PRIMARY IP the IP of the GuardPoint10 Full Installation (Server) machine</p> <p>2=PORT NO.: 10002 (default) must be unique for each panel</p>
4=ACCOUNT NO.	<p>Set to: 4444 (for example)</p> <p>Set to: 1=TCP</p>

03=REMOTE ACCESS

Sub-menu Item	Keypad Action
1=ACCESS PERIOD	Set to: 4=ANY TIME
2=MODE	Set to: 1=DIRECT ACCESS

08=SIA CONTROL

Sub-menu Item	Keypad Action
	Type the IP of the GuardPoint10 Full Installation (Server) machine.

## 09=ENCRYPT

Sub-menu Item	Keypad Action
1=ALARM REPORT	Set to: OFF
2=REMOTE ACCESS	Set to: OFF
3=SIA CONTROL	Set to: OFF
4=ALARM MON.	Set to: OFF

Configuring an existing Galaxy system panel via the Galaxy Frontshell program at its RSS / Ethernet screen is outside the scope of this topic. Consult your Galaxy documentation for this information.



# Infrastructure: MultiSite Impact

All Infrastructure screens and details, except for Local Reflex, include a new field called **Owner**. This field identifies the site that owns that asset.

All Infrastructure details, except for Site, include a **Select site to share with** drop-down list. This list allows the user to select other sites to share the selected asset. Sites may be selected or unselected from the list by a user owned by the same site as the asset.

## Add a new site

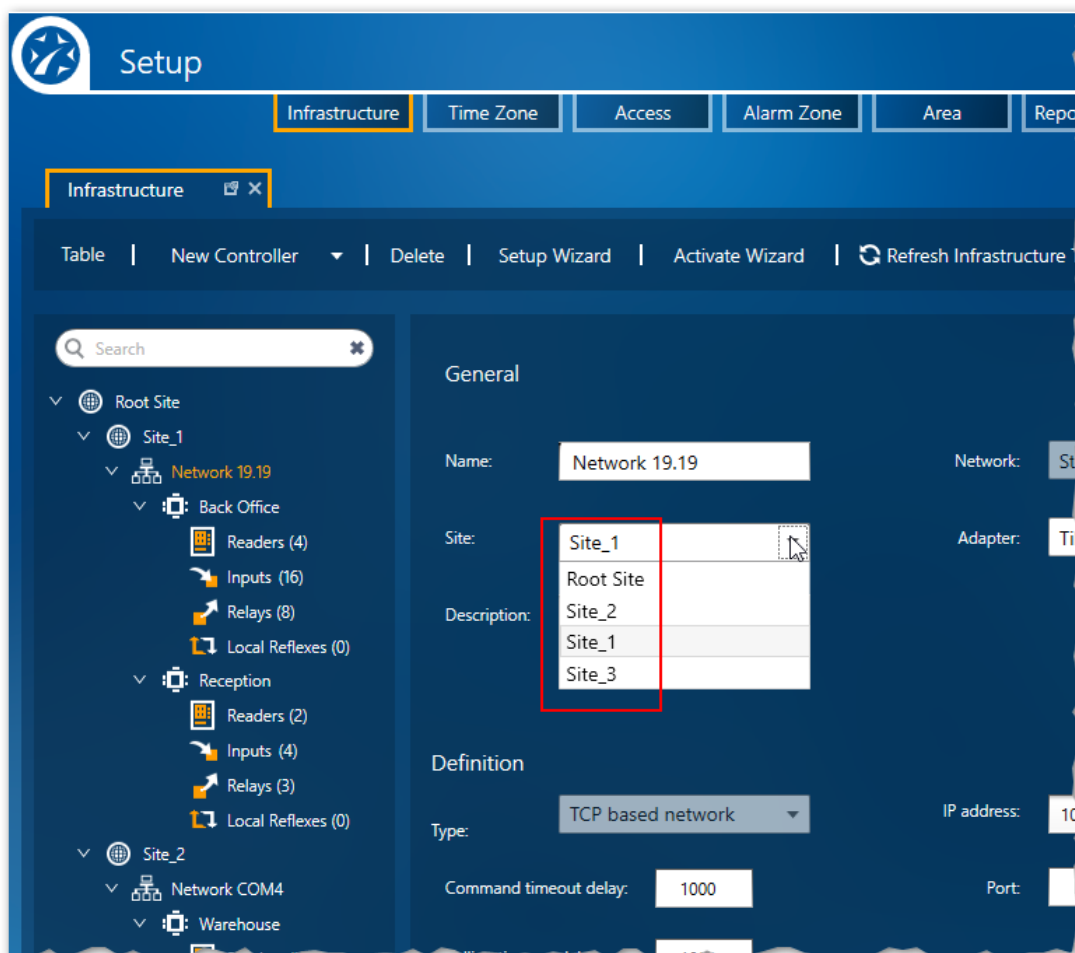
With the Root site in focus, you can add a new site to the infrastructure or a new network owned by the Root site via the Action menu or the Root site context menu.

Each site has a **Baud rate** value and **Default Multiple Access Group** value.

## Change the ownership of a network

1. With the network in focus, open the **Site** drop-down list and select the site where ownership will be transferred.

Figure 2-25



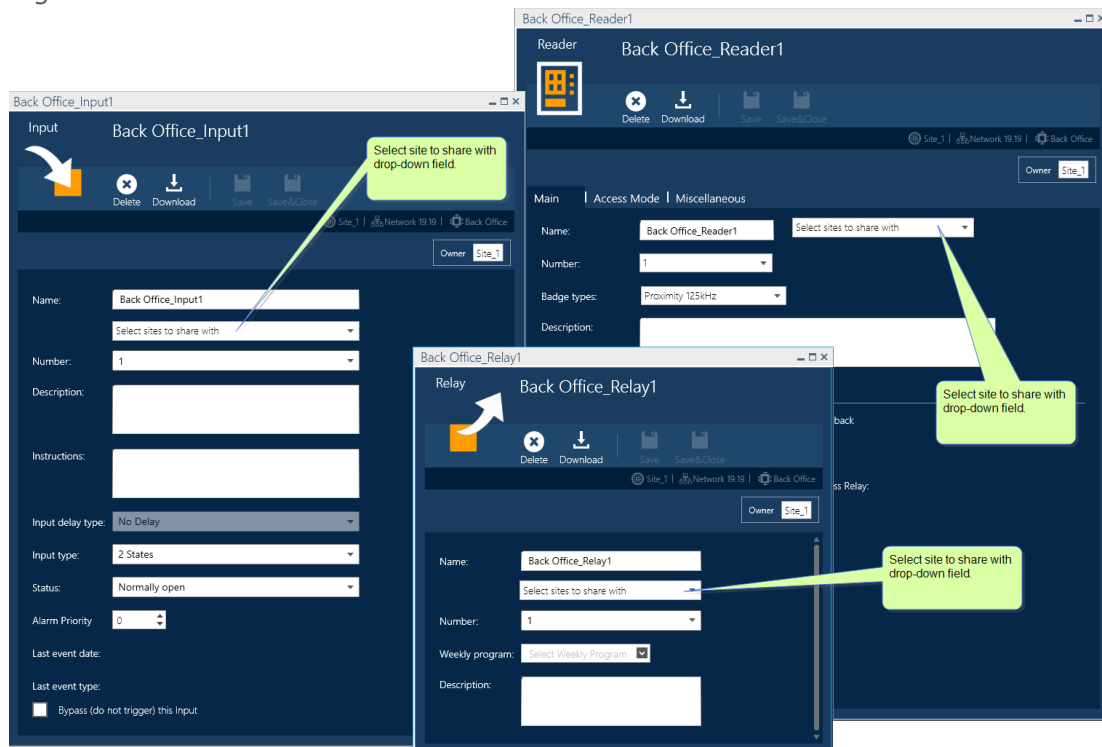
2. Click **Save**. Ownership is changed and the infrastructure tree is updated.

If all assets in the network are owned by the same site as the network, their ownership will also change to the site selected for the network. If there is an asset owned by a different site, the asset's ownership will not change even though the asset will appear in the network's new owner site. This means that the infrastructure tree may not always be accurate. However, if you go to the infrastructure's Table view an accurate presentation can be seen.

## Share an asset (network, controller, reader, input or, relay) with another site

1. Display the details of the relevant asset (controller, reader, input or, relay).
2. Open the **Select site to share with** a drop-down list.

Figure 2-26



3. Select the site where the asset will be shared.
4. Click **Save**. A user from the shared site will now be able to use the shared asset in their site.

If a network is shared with another site, the ownership of the network is changed to the Root site, and the previous network owner now shares the network with the other selected shared sites.

If a controller is shared with another site, the ownership of the controller and its network changes to the Root site, and the previous controller and network owner now share the controller and network with the other selected shared sites.

## Table View support for MultiSite

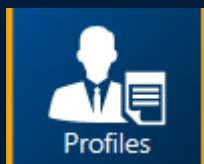
In the Select Fields list, found in Field Selection Options, three new column headings have been added to the Shared group: Owner, Shared with, and Site. This provides an infrastructure overview as it pertains to MultiSite.

Report Templates added in Table View are owned by the site that owns the logged-in user. The templates will not be available to users owned by other sites.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**







# CHAPTER 3:

## Profiles



The Profiles screen adds and manages profiles. A profile governs the authorizations assigned to operators. The authorization settings determine whether an operator can see a particular screen or, see and edit the data on a particular screen.

There are three types of authorization:

- » **Hidden:** The screen or element(s) are hidden from an operator. Click a module or element's white eye icon until it is dull . After the eye icon is dulled, the pencil icon will automatically change to dull .
- » **Read-only:** An operator may only see the screen or element(s) on the screen without being able to alter it. Click a module or element's white pencil icon until it is dull . Verify that the eye icon is white .
- » **Read and Write:** An operator may see and edit the element(s) on the screen. Click a module or element's eye icon and pencil icon until they are both white  .



**Note:** For you to make authorization changes or even to see the Profile screen, you will need the authorization to edit profiles.

Authorizing an operator to edit an element will automatically authorize them to see it. Any changes made to a profile will be applied to an assigned operator upon their next GuardPoint10 session login.

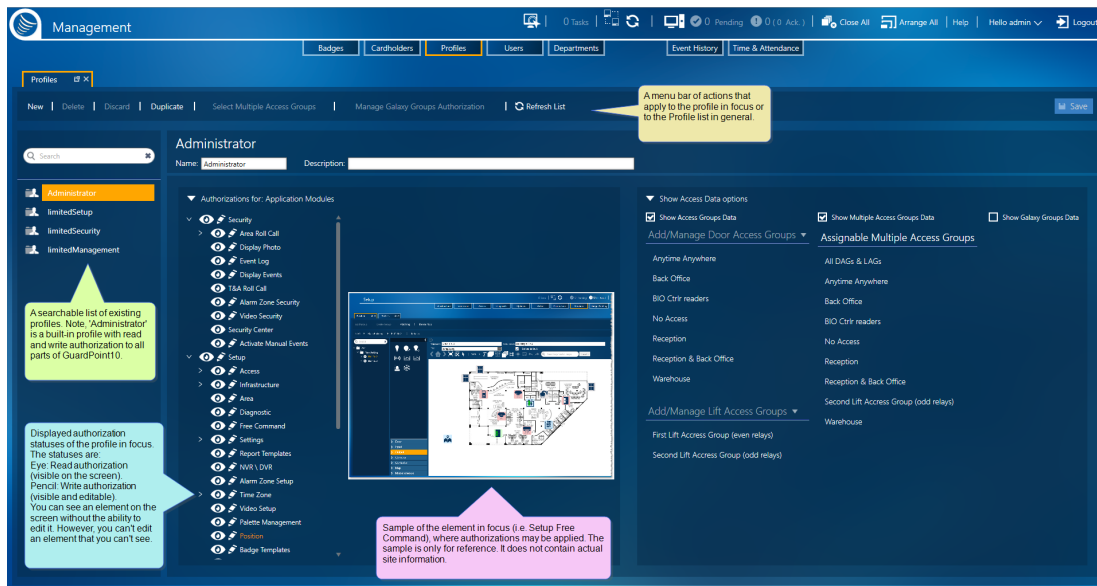
# Adding a New Profile

Use the following steps to create a new profile in the Profiles screen.

## How to create a new profile

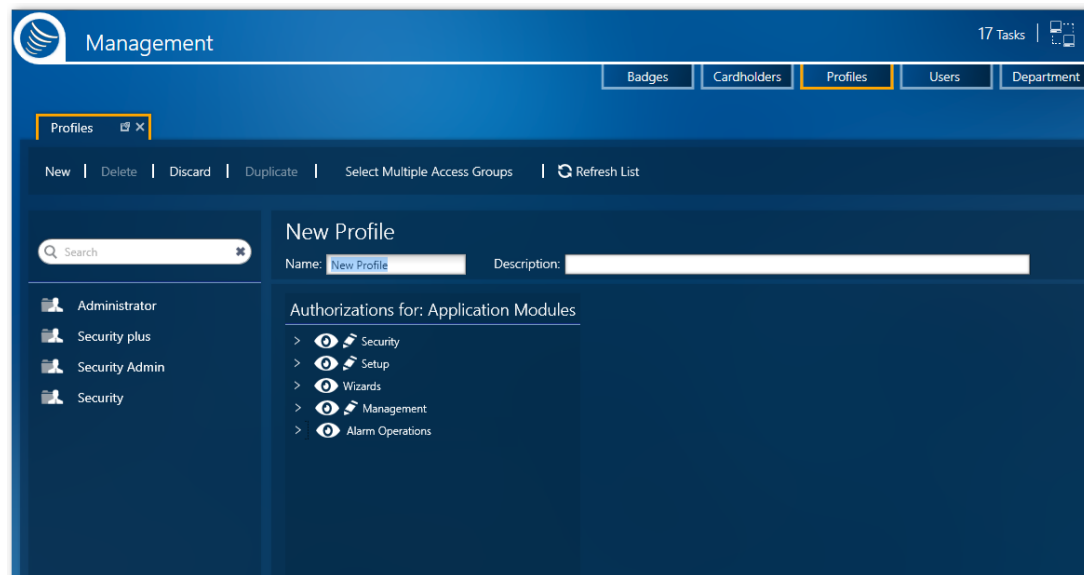
1. Go to the Management Task group and click **Profiles**.

Figure 3-1



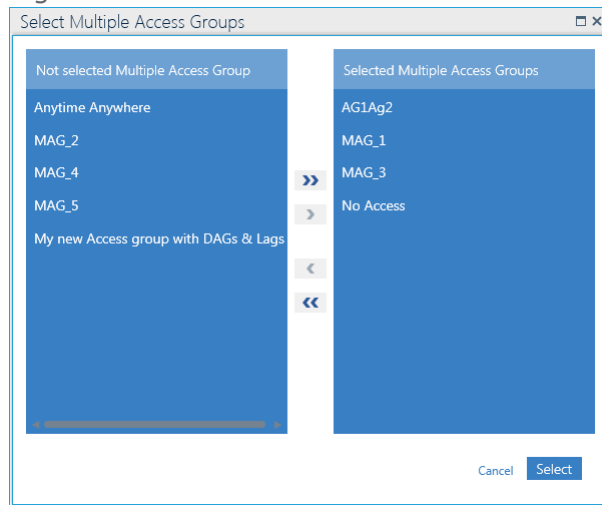
2. From the action bar, click **New**. New profile parameters and an expandable authorization tree are displayed.

Figure 3-2



3. Enter a profile name in the **Name** field. The default name is "New Profile".  
(Optional) Enter a description that provided more information about the profile.
4. Click **Select Multiple Access Groups**. The Select Multiple Access Groups dialog is displayed.

Figure 3-3



Add or Remove Multiple Access Groups to or from the Selected Multiple Access Group column via the buttons between the columns.







After you are satisfied with the content of the Selected Multiple Access Group column, click **Select**. The Multiple Access Groups selected are now available to operators, with the new profile, for assignment to cardholders.

5. Expand the GUI authorization tree. The tree can have as many as three levels of authorization.
6. Choose the authorization setting for each GUI module or element.

A module is the parent element in the tree (i.e. a screen). You can set the authorization on the module level, which will apply the same authorization to each subelement in the module or, you can set the authorization for each element in the module.

To assist in the selection process, click on the name of a module or element, an image representing the module or element is displayed to the right of the tree.

The GUI authorization types are as follows:

- » **Hidden:** The screen or element(s) are hidden from an operator with this profile. Click a module or element's white eye icon until it is dull . After the eye icon is dulled, the pencil icon will automatically change to dull .
- » **Read-only:** An operator, with this profile, may only see the screen or element(s) on the screen without being able to alter it. Click a module or element's white pencil icon until it is dull . Verify that the eye icon is white .
- » **Read and Write:** An operator may see and edit the module or element(s) on the screen. Click a module or element's eye icon and pencil icon until they are both white  .

7. After setting the authorizations, click **Save**. The profile is stored in the system database and the profile name is displayed in the Profiles list to the left of the tree.

After a profile is saved to the database, it can be assigned to an operator. For information about assigning a profile to an operator, see "[Operators \(Users\)](#)" on page 103.

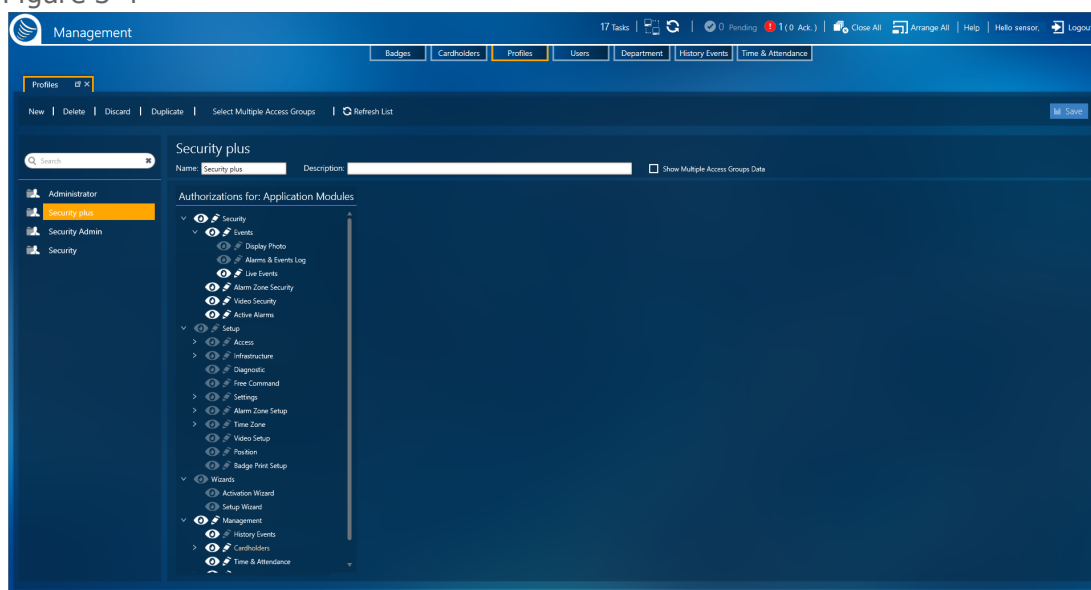
## Duplicating a Profile

If you want to add a profile to the system that is identical or almost identical to an existing profile, use the duplicate feature to perform this task quickly and accurately.

### How to duplicate a profile's details & authorizations

1. Go to the Management Task group and click **Profiles**.
2. From the list of existing profiles on the left, select the profile that will be duplicated. The profile's parameters and authorization tree are displayed.

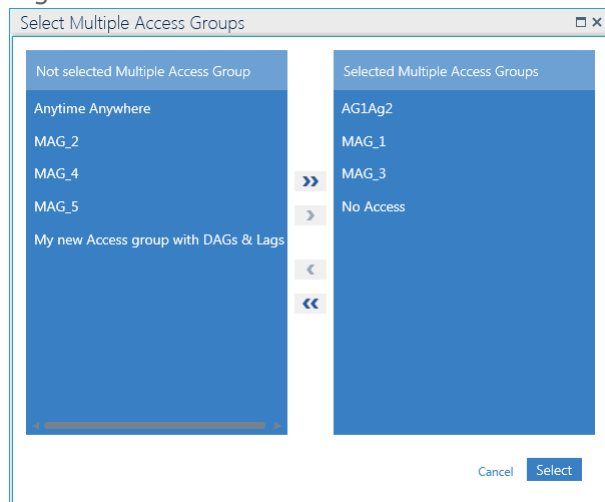
Figure 3-4



3. From the action bar, click **Duplicate**. A new profile, identical to the profile in focus is displayed to the right of the list of existing profiles. The only differences between the original and the duplicate profile are:
  - » The duplicate profile's name is appended with "\_Duplicate" (i.e. a profile named "SecurityStaffMember" would have a duplicate named "SecurityStaffMember\_Duplicate").
  - » The duplicate profile has not been saved in the system database and does not appear in the Profile list.
  - » The duplicate profile has not been assigned to an operator.
4. (Optional) A best practice is to rename the duplicate profile to something more identifiable.
5. (Optional) Enter a description that provided more information about the profile.
6. Click **Select Multiple Access Groups**. The Select Multiple Access Groups dialog is displayed.



Figure 3-5



Add or Remove Multiple Access Groups to or from the Selected Multiple Access Group column via the buttons between the columns.







After you are satisfied with the content of the Selected Multiple Access Group column, click **Select**. The Multiple Access Groups selected are now available to operators, with the new profile, for assignment to cardholders.

7. Expand the authorization tree. The tree can have as many as three levels of authorization.
8. Change the authorization setting for each module or element as required.

A module is the parent element in the tree. You can set the authorization on the module level, which will apply the same authorization to each subelement in the module or, you can set the authorization for each element in the module.

To assist in the selection process, click on the name of a module or element, an image representing the module or element is displayed to the right of the tree.

The authorization types are as follows:

- » **Hidden:** The screen or element(s) are hidden from an operator with this profile. Click a module or element's white eye icon until it is dull . After the eye icon is dulled, the pencil icon will automatically change to dull .
- » **Read-only:** An operator, with this profile, may only see the screen or element(s) on the screen without being able to alter it. Click a module or element's white pencil icon until it is dull . Verify that the eye icon is white .
- » **Read and Write:** An operator, with this profile, may see and edit the modules (screens) or element(s) on the screen. Click a module or element's eye icon and pencil icon until they are both white  .

9. After changing the duplicate profile, do one of the following:
  - » Click **Discard**. The duplicate profile is removed.
  - » Click **Save**. The profile is stored in the system database and appears in the Profiles list.

# Assigning Multiple Access Groups to a Profile

**Note:** This feature is only available when the Options screen General tab's **Profile Multiple Access Groups** field is set to Yes.

When you assign a Multiple Access Group to a profile, it means that an operator, with the profile, can only assign cardholders a Multiple Access Group from the list created for their operator profile.

## A simple example

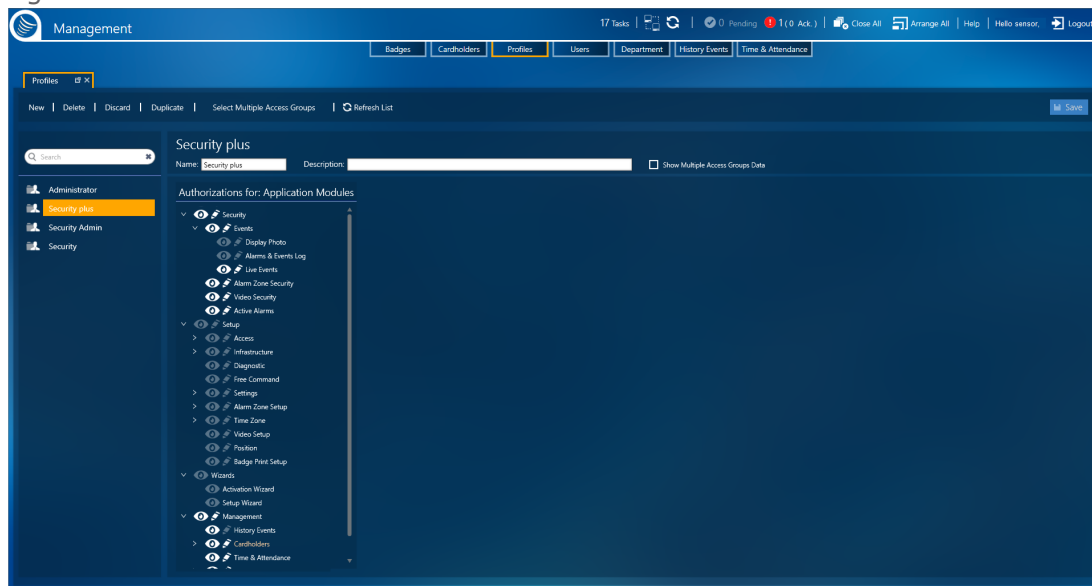
A secretary on floor 2 should only be able to assign cardholders access to zones on the second floor and not to zones on the third floor.

Use the following steps to assign Multiple Access Groups to a profile.

## How to assign a Multiple Access Group to a profile

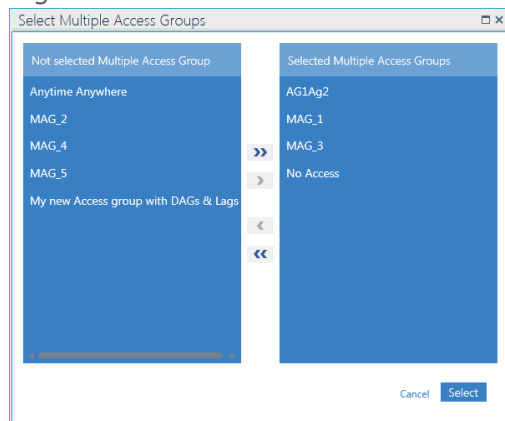
1. Go to the Management Task group and click **Profiles**.
2. From the list of existing profiles on the left, select the profile that will be assigned Multiple Access Groups. The profile's parameters and authorization tree are displayed.

Figure 3-6



3. From the action bar, click **Select Multiple Access Groups**. The Select Multiple Access Groups dialog is displayed.

Figure 3-7



The variability of the **Select Multiple Access Groups** button (show or hide) is determined by an Options screen setting. For more information see ["General Tab Options" on page 568](#).

Add or Remove Multiple Access Groups to or from the Selected Multiple Access Group column via the buttons between the columns.

After you are satisfied with the content of the Selected Multiple Access Group column, click **Select**. The Multiple Access Groups selected are now available to operators, with this profile, for assignment to cardholders.

4. Click **Save** in the Profiles screen to save the Profile in focus with its updated Multiple Access Groups.

For more information about Multiple Access Groups, see ["Multiple Access Groups" on page 156](#).



**Note:** Multiple Access Groups may also be assigned based on a cardholder's Department and Visitor status. However, if there is a conflict, in a cardholder's details, an operator assigns a Multiple Access Group takes priority over the Department assigned Multiple Access Group.

## Editing a Profile's Details & Authorizations

In a profile, there are two editable groups:

- » Details
- » Authorizations

Think of a profile as a container, the details include information about the container itself and the authorizations include information about the contents of the container.

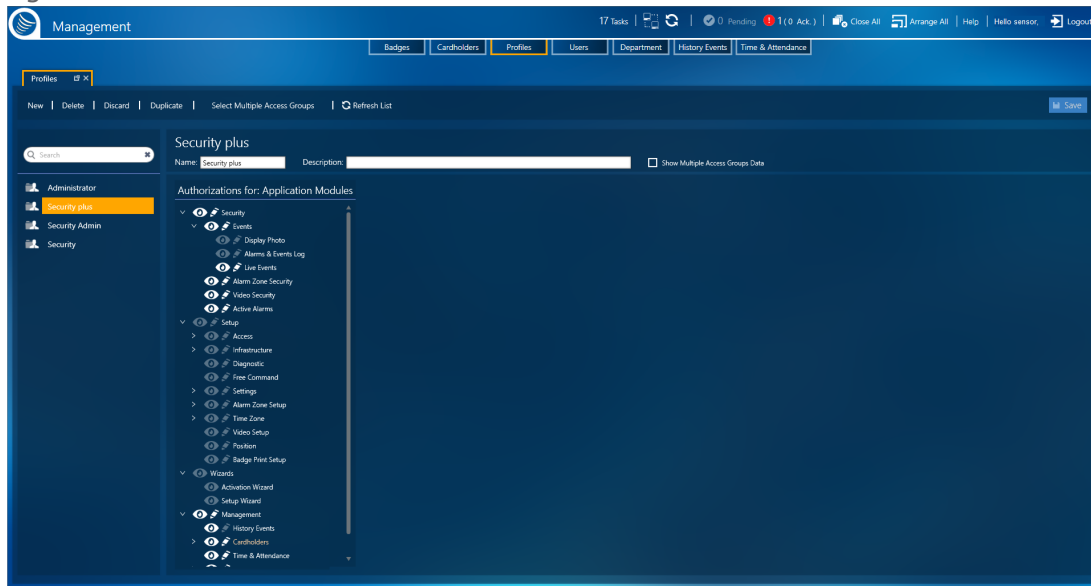


**Note:** The Administrator profile is built into the system and cannot be edited or deleted.

### How to edit a profile's details & authorizations

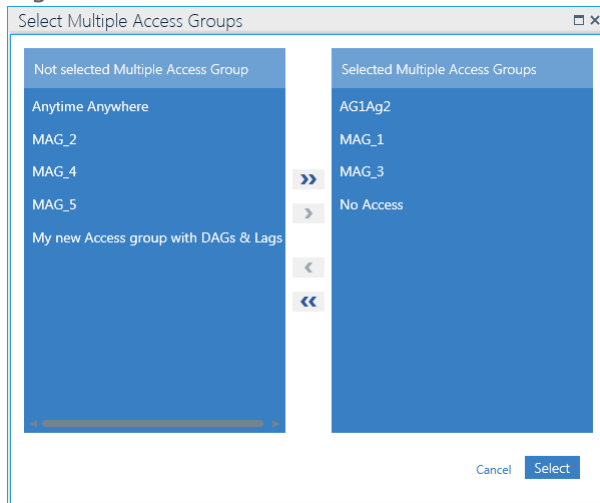
1. Go to the Management Task group and click **Profiles**.
2. From the list of existing profiles on the left, select the profile that will be edited. The profile's parameters and authorization tree are displayed.

Figure 3-8



3. Change the profile name as required.  
The name should identify the type of authorizations set in the profile.  
(Optional) Enter a description that provided more information about the profile.
4. Click **Select Multiple Access Groups**. The Select Multiple Access Group dialog is displayed.

Figure 3-9



Add or Remove Multiple Access Groups to or from the Selected Multiple Access Group column via the buttons between the columns.







After you are satisfied with the content of the Selected Multiple Access Group column, click **Select**. The Multiple Access Groups selected are now available to operators, with the new profile, for assignment to cardholders.

5. Expand the authorization tree. The tree can have as many as three levels of authorization.
6. Change the authorization settings for each module or element as required.

A module is the parent element in the tree. You can set the authorization on the module level, which will apply the same authorization setting to each subelement in the module or, you can set the authorization for each element in the module.


To assist in the selection process, click on the name of a module or element, an image representing the module or element is displayed to the right of the tree.

The authorization types are as follows:

- » **Hidden:** The screen or element(s) are hidden from an operator with this profile. Click a module or element's white eye icon until it is dull . After the eye icon is dulled, the pencil icon will automatically change to dull .
- » **Read-only:** An operator, with this profile, may only see the screen or element(s) on the screen without being able to alter it. Click a module or element's white pencil icon until it is dull . Verify that the eye icon is white .
- » **Read and Write:** An operator, with this profile, may see and edit the modules (screens) or element(s) on the screen. Click a module or element's eye icon and pencil icon until they are both white  .

7. After changing the profile, do one of the following:

- » Click **Discard**. The details or authorizations return to their previously saved values.
- » Click **Save**. The new profile information is stored in the system database.

 **Note:** After a profile is updated and saved in the system database, all operators with the profile are governed by the updated authorizations.

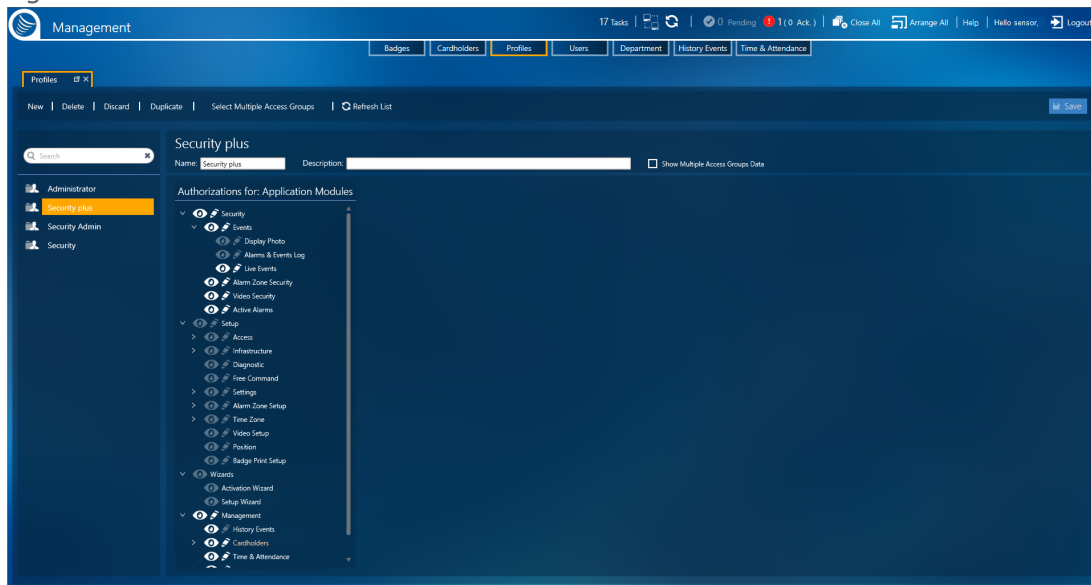
# Deleting a Profile from the System

Before you can delete a profile, it must be detached from any operator currently assigned to the profile. For information about attaching a different profile to an operator, see ["Editing an Operator's Details" on page 105](#).

## How to delete a profile from the system

1. Go to the Management Task group and click **Profiles**.
2. From the list of existing profiles on the left, select the profile that will be deleted. The profile's parameters and authorization tree are displayed.

Figure 3-10



3. From the action bar, click **Delete**, and then confirm the operation. The profile is removed from the system and no longer appears in the Profile list.

**Note:** The Administrator profile is built-in to the system and cannot be edited or deleted.

# Profiles: MultiSite Impact

Each site has its own profiles. Profiles cannot be shared with other sites. The name of the site that owns a profile appears in the profile's details.

When a site is added via the infrastructure screen, an Administrator profile owned by the new site is automatically added to the system. The Administrator profile name is prefixed with the name of the site that owns it.

A profile is attached to a user and applied to all sites where the user has authorization.

The list of saved profiles will only show those profiles owned by sites where the logged-in user has authorization.

## Add a Profile

1. From the Action menu, click **New**.
  - » If the logged-in user is only authorized in their owner site, the new profile will have the same owner site as the logged-in user.
  - » If the logged-in user is authorized in multiple sites, select the site that will own the new profile from the **New** button's drop-down list.
2. Complete new profile's details, and then click **Save**.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**



# CHAPTER 4:

## Operators (Users)



The Users screen is where GuardPoint10 operators are defined. An operator, also known as a user, is a person entrusted with security system operations. An operator is identified in the system by their GuardPoint10 login credentials (user name and password).

An operator is bound to a set of authorizations, which allows an operator to read or read & write to various parts of the interface. The authorizations are grouped into profiles.

Operators saved in the system database are identified as cardholders with or without a badge code assignment. If you look at the Cardholder screen, you will find cardholder-operators created in the Operators screen.

# Adding a New Operator

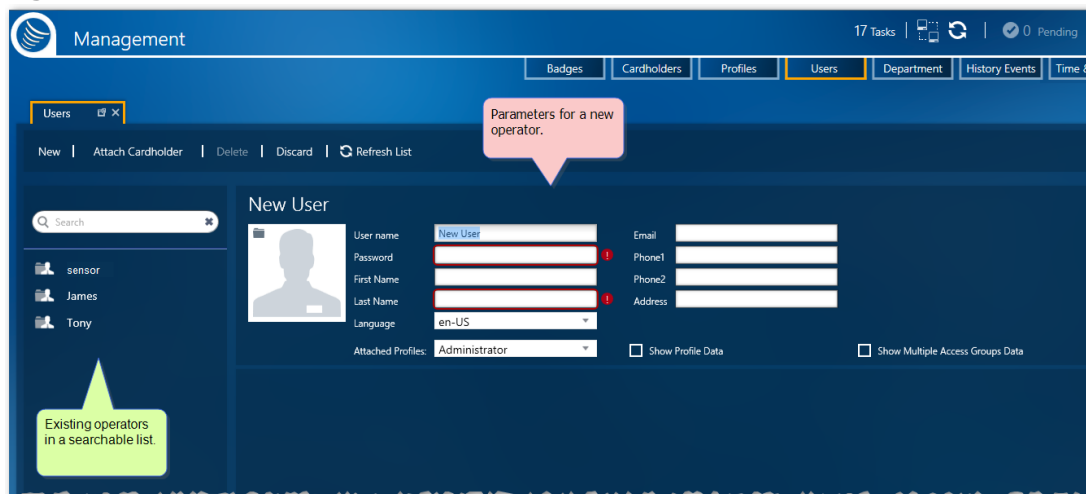
**Note:** Operators (with their parameter information) saved in the system database are identified as cardholders without a badge assignment. If you look at the Cardholder screen, you will find operators who have been added via the Operators screen.

Use the following steps to add a new operator via the Operator screen.

## How to add a new operator

1. Go to the Management Task group and click **Users**. The Users screen is displayed.
2. From the action bar, click **New**. New operator parameters are displayed.

Figure 4-1



3. Enter operator information in the parameter fields. The required parameters are as follows:
  - » **User Name:** The name that is part of the operator's credentials and is required when logging in to GuardPoint10.
  - » **Password:** The confidential password that is the second half of the operator's credentials and is required when logging in to GuardPoint10.
  - » **Should Password be replaced:** Forces the user to change their password the next time they log in to GuardPoint10.
  - » **Last Name:** The last name of the operator. This name will appear in the Operators list to the left of the New Operator parameters.
  - » **Language:** After the operator is logged in, this is the language of the text that will appear on the screen.
  - » **Attached Profile:** More about this in Step 4.

For more information about the parameters, see "[Users Screen](#)" on page 627.

4. Select a profile from the **Attached Profile** drop-down list.

Profiles are defined in the Profiles screen. A profile contains authorizations such as:

- » Hide information from an operator with the selected profile.
- » Show information to an operator, with the selected profile.
- » Allow an operator with this profile to edit information on a particular screen.

For more profile information, see ["Profiles" on page 91](#).

5. (Optional) Select the **Show Profile Data** checkbox to see the selected profile's expandable tree of authorizations.
6. (Optional) Select the **Show Multiple Access Groups Data** checkbox to see the Multiple Access Groups that an operator, with the selected profile, can choose from when assigning a Multiple Access Group to a cardholder.
7. Click **Save**. The operator information is stored in the system database and the operator's name is displayed in the Operators list to the left of the parameters.

## Editing an Operator's Details

An GuardPoint10 operator has two categories of details:

- » Authorization details
- » Operator details

### Authorization details

Authorizations are stored in profiles. Profiles are defined in the Profiles screen. You can designate the following authorization types to screens and some screen elements:

- » Hide information
- » View information without the ability to edit it
- » View and edit information

For more information about profiles, see ["Profiles" on page 91](#).

### Operator details

Operator details have more to do with the operator's identity in the system than authorizations. The following is the operator information you may enter via the Users screen:

- » **User Name:** The name that is part of an operator's credentials and is required when logging in to GuardPoint10.
- » **Password:** The confidential password that is the second half of an operator's credentials and is required when logging in to GuardPoint10.
- » **Should Password be replaced:** Forces the user to change their password the next time they log in to GuardPoint10.
- » **Last Name:** The last name of an operator. This name will appear in the Operators list to the left of the New Operator parameters.
- » **Language:** After the operator is logged in, this is the language of the text that will appear on the screen.

- » **Attached Profile:** Assigns the system authorizations to an operator by attaching a profile. A profile is a collection of authorizations.
- » **First name:** (Optional) The first name of an operator. This name will precede an operator's last name in the Operators list to the left of the Operator parameters.
- » **Email:** (Optional) The email address where an operator may be contacted.
- » **Phone1/Phone2:** (Optional) The primary and secondary phone numbers where an operator may be contacted.
- » **Address:** (Optional) The home address of an operator.

## How to edit the details of an operator

1. Go to the Management Task group and click **Users**. The Users screen is displayed.
2. From the list of existing operators on the left, select the operator whose details will be edited. The operator's parameters are displayed.

Figure 4-2



3. Change any of the details that pertain to the identity of the operator or switch the operator's profile.
4. After changing the details, do one of the following:
  - » Click **Discard**. The unsaved operator parameter values return to their previously saved values.
  - » Click **Save**. The operator information is stored in the system database.

## Attaching a Cardholder to Operator Details

An operator does not have to be a cardholder. For example, if your system is monitored off-site, there may not be a need for the GuardPoint10 operator to access the premises; therefore, they do not need a badge. However, there are many cases where you would want your GuardPoint10 operator to be on-site and have a badge.

A single cardholder may be attached to multiple operator details.

**Note:** Operators (with their parameter information) saved in the system database are identified as cardholders without badge assignments. If you look at the Cardholder screen, you will find operators listed that have been previously added and saved via the Operators screen.

## How to attach a cardholder to operator details

1. Create a cardholder and assign the cardholder a badge.

For information on how to perform this task, see ["Adding Customized Fields to Cardholder Details"](#) on page 199.

2. Go to the Management Task group and click **Users**. The Users screen is displayed.
3. Do one of the following:
  - » From the list of existing operators on the left, select the operator whose details will be attached to a cardholder. The operator's parameters are displayed.
  - » Add a new operator (see ["Adding a New Operator"](#) on page 104) and select the operator's name from the Operators list on the left, if it's not already on focus. The operator's parameters are displayed.

Figure 4-3



4. With the operator details displayed, click **Attach Cardholder** in the action bar, and then confirm the operation. A Select Cardholder dialog is displayed with a cardholder table inside.

Figure 4-4

The screenshot shows a 'Select Cardholder' dialog box with a search bar and a table of cardholders. The table has columns for Photo, Last Name, First Name, Company, Department, Type, and Number. Callouts highlight the search field and column filter options.

Photo	Last Name	First Name	Company	Department	Type	Number
	admin	admin			Employee	
	Anderson	Julie	Microsox	Management	Visitor	
	Butler	Victor	ConnectMe	Sales	Employee	1003
	Davis	Maria	ConnectMe	Support	Visitor	1005
	ITguy	ITguy			Employee	
	John	Johnsom			Freelancer	
	Lee	Judith	IT Energize	Management	Employee	
	Lopez	Nancy	ConnectMe	Support	Employee	1006
	Miller	Terry	Adopt Communication	Executive	Employee	1004
	Smith	Tony		Executive	Employee	1007

Callout 1: Narrow your view of visible cardholders with the Search field or column filter options available via a column heading.

Callout 2: A list of existing cardholders to choose from. The list includes filter and sort options available through the column headings.

For information about table filters, see **"Table Filters"** on page 695.

5. Choose a cardholder from the Select Cardholder dialog, and then click **Select**. The selected cardholder is now an operator and details that identified the operator are replaced by the cardholder's details.



**Note:** The original saved operator details still exist and can be found in the Cardholder screen.

## Attach Active Directory Credentials to User

An Active Directory (AD) sits on a domain controller Server machine. Among other things, an AD authenticates and authorizes all users and computers in a Windows domain type network. When you log in to Windows with a Username and Password the Username and Password credentials are validated via the AD.

When attaching an GuardPoint10 user to an AD user, you are allowing that GuardPoint10 user to log in to GuardPoint10 with the same credentials used when they logged in to Windows.



- Note:** To attach a user to an AD user, the following prerequisites must be performed:
- Install the GuardPoint10 Full installation (Server installation) on a machine in the domain network.
  - GuardPoint10 workstation installations also have to be on machines in the same domain network.
  - In the Options screen's General tab, set **Enable Active Directory** to **Yes** and then enter the **Domain name**. You may have to get the name from the organization's IT staff.

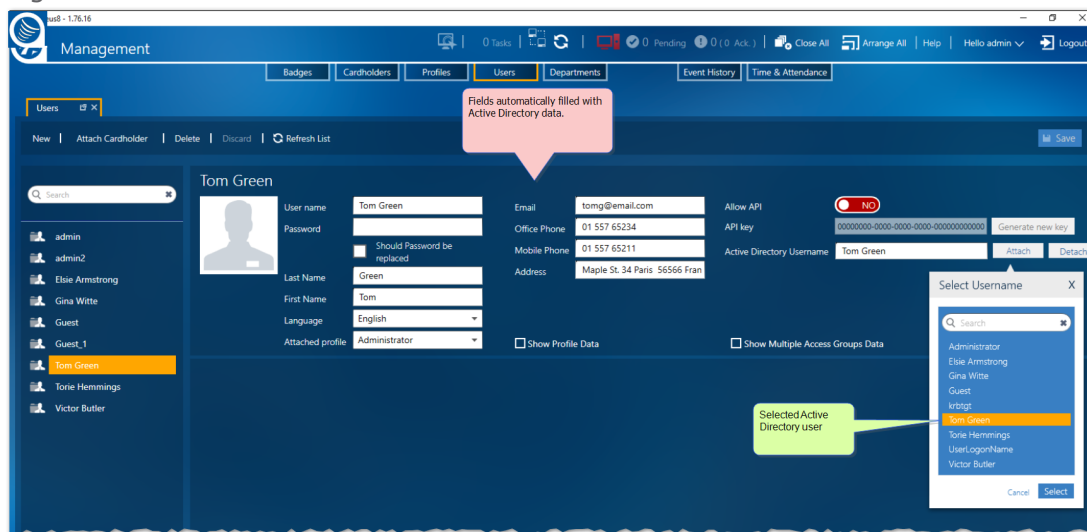
# How to attach an AD user to an GuardPoint10 user

1. Go to the Management Task group and click **Users**. The Users screen is displayed.
2. From the action bar, click **New**, or select an existing user. User details are displayed.
3. In **Active Directory Username**, click **Attach**. A Select Username dialog is displayed.
4. Choose the AD user logon name that will be attached to the GuardPoint10 user, and then click **Select**. The AD user logon name will appear in the field to the left of the **Attach** button.

Other User fields will be automatically filled with information found in the AD credentials. The fields are editable and can be changed as required.

However, the **Password**, **Language**, and **Attached Profile** fields will remain empty or unchanged. These field values must be manually entered or selected before the user details can be saved.

Figure 4-5



5. Click **Save**. The user will now be able to log in to GuardPoint10 with their GuardPoint10 user name and password, or just by clicking the **Login with Windows Credentials** button without entering a user name or password.



**Note:** If AD user information is changed, GuardPoint10 will not automatically update the information in the user's details. The AD user will have to be detached and then reattached to the GuardPoint10 user to update the information.

# To detach an AD user from an GuardPoint10 user

1. Go to the Management Task group and click **Users**. The Users screen is displayed.
2. Select a saved user who is attached to an AD user.
3. In **Active Directory Username**, click **Detach**, and then **Save**.

The AD user is detached from the GuardPoint10 user. However, the information in the user's details remains unchanged.

# Deleting an Operator from the System

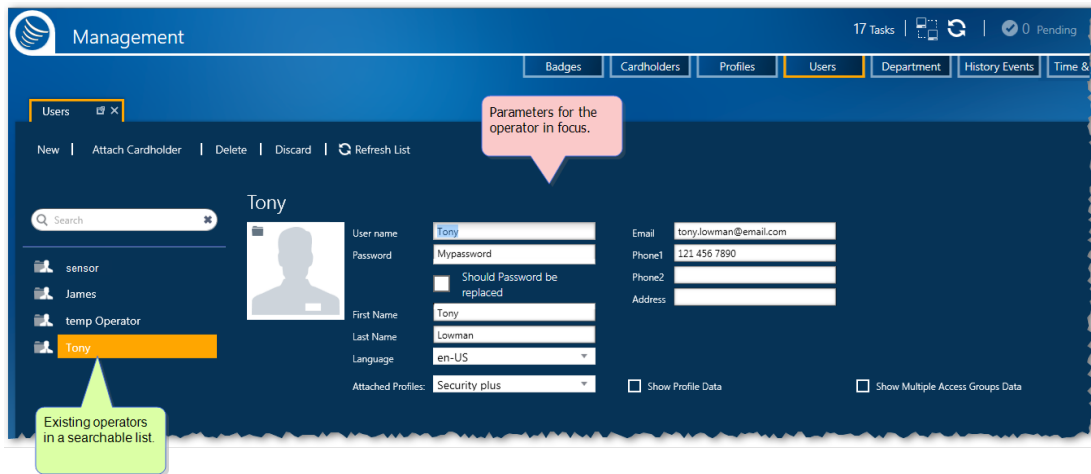
After you delete an operator from the system, you cannot undo the operation.

**Note:** Remember an operator is also a cardholder. If you delete an operator, only the operator information is deleted; the cardholder details remain intact.

## How to delete an operator from the system

1. Go to the Management Task group and click **Operators**. The Operators screen is displayed.
2. From the list of existing operators on the left, select the operator whose details will be deleted. The Operator's parameters are displayed.

Figure 4-6



3. From the action bar, click **Delete**, and then confirm the operation. The operator is removed from the system and the operator's name no longer appears in the Operators list. However, the cardholder data about the deleted operator remains intact and can be found in the Cardholders screen.



# Operator (User): MultiSite Impact

A user's details include the following new fields:

- » **Owner:** Identifies the site that owns the user and where the user has authorization.
- » **Sites:** A drop-down list of sites where a user's authorization can be extended to other sites.
- » **Super User:** When selected, the user has authorizations to all sites including the Root site. In addition, the API Center is only available to super users.

Figure 4-7



A user's corresponding cardholder will by default be owned by the same site as the user and have the share type of **Local**, regardless of the user's super user status or additional site authorizations.

A user's super user status or additional site authorizations can be changed at any time.

Only a logged-in super user can change another user's status to super user.

A user's attached profile is applied to all sites where the user is authorized even though the profile is owned by one site and cannot be shared.

The list of saved users is filtered to show only those users owned by a site where the currently logged-in user has authorization.

## Add a User

1. From the Action menu, click **New**.

If the logged-in user is only authorized in their owner site, the new user will have the same owner site as the logged-in user.

If the logged-in user is authorized in multiple sites, select the site that will own the new user from the **New** button's drop-down list.

2. Complete new user's details including the new MultiSite field, and then click **Save**.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 5:

## Time Zones



A Time Zone determines the behavior of various entities in the system. A Time Zone is made up of a range of times set to green or white. This white or green setting governs an entity's behavior and permissions.

All event behaviors connected to a system entity (actions and reactions) have timestamps. A timestamp is an actual time which an event takes place. As soon as an event is stamped, its timestamp is checked against the current period (green or white). Based on the period where the timestamp falls, a set of rules are applied.

A Time Zone is applied to a system entity through an assigned Weekly Program (WP). A WP is made up of one or more Daily Programs and, optionally, one or more Holidays and Special days.

# Daily Program Time Zones



**Note:** Defining Time Zones, Daily Programs, and Weekly Programs is very important. Properly defining the green and white periods in Daily Programs is essential for the system to work optimally.

A best practice is to successively specify the Daily and Weekly programs, as well as Holiday and Special Days, before defining the other parameters of the system.

A Time Zone determines the behavior of various entities in the system, this includes Cardholders, Readers, Inputs devices & Relays, and Reflexes. That's the simple definition. Now, let's look at what makes up a Time Zone and what's needed to apply a Time Zone.

A **Time Zone** is made up of a range of times set to green or white. This white or green setting governs an entity's behavior and permissions.

All event behaviors connected to a system entity (actions and reactions) have timestamps. A timestamp is the time at which an event takes place. As soon as an event is stamped, its timestamp is checked against the current period (green or white). Based on the period where the timestamp falls, a set of rules are applied.

To apply a Time Zone to a system entity or cardholder requires a Daily Program and a Weekly Program (WP).

There is an additional option that allows you to add rule exception *dates* to a WP. These date exceptions are Holidays and Special Days.

In this topic, we will cover the Daily Program, which is a building block for creating Weekly Programs.

## Daily Program

A Daily Program is a 24-hr segment of time during which a particular set of green and white periods may exist. A Daily Program supports a maximum of 4 green periods.

The system has two predefined Daily Programs:

- » **Always:** A green period all day long (Default).
- » **Never:** A white period all day long.

A Daily Program is not directly assigned to an entity. A Daily Program is assigned to one or more Weekly Programs (WPs). The WP is the object assigned to an entity.

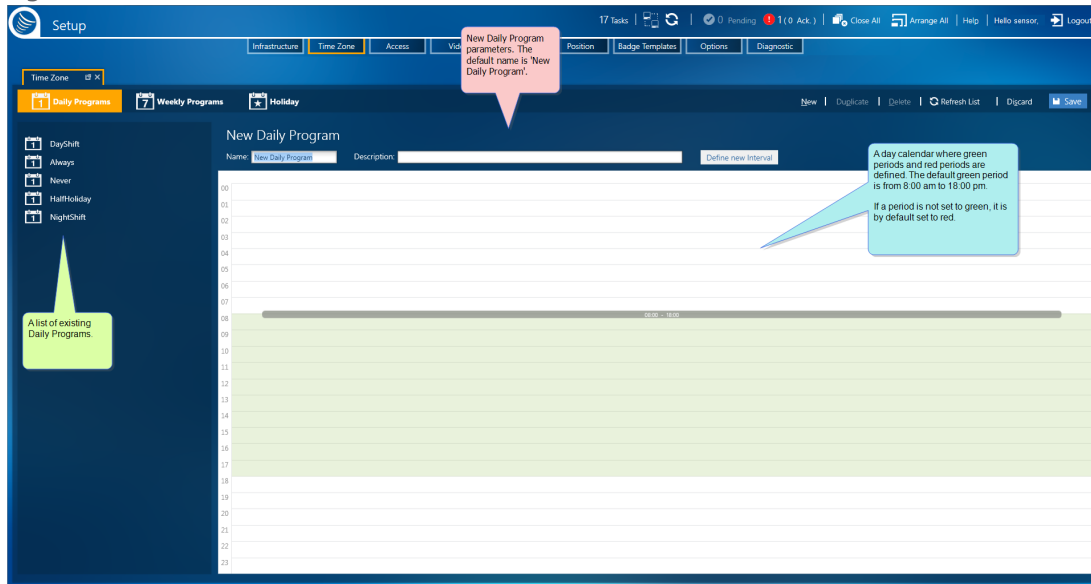
## Adding a New Daily Program

Use the following steps to create a new Daily Program in the Time Zone screen.

## How to create a new Daily Program

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Daily Program**. The Time Zones' Daily Program screen is displayed.
3. From the action bar, click **New**. New Daily Program parameters and a default day calendar are displayed.

Figure 5-1



4. Enter a new name for the Daily Program.

The name should identify the use of the program (when it would be applied in a Weekly Program).

(Optional) Enter a description that provided more information about the program.

5. In the day calendar area, you have the following edit options:

- » Drag the top or bottom border of the default green period to adjust the time in 15-minute intervals.
- » Double-click on the default green period to open a dialog and make precise adjustments to the time in the default green period.
- » Click the **Define new interval** button to set a precise time for an additional green period within the displayed 24 hour day.

Alternatively, right-click on a white period (colored white) on the day calendar, and then click **Define new interval** in the context menu. A new green period, within the displayed 24 hour day, is added.

- » Right-click on a green period on the day calendar and then click **Remove region** in the context menu. The region is removed.

6. After changing the default settings in the new Daily Program, do one of the following:
  - » Click **Discard**. The unsaved Daily Program is removed.
  - » Click **Save**. The new Daily Program is stored in the system database and can be applied to a WP.

**Note:** A Daily Program can support a maximum of 2 or 4 green periods. The maximum number of green periods is set in the Options screen.

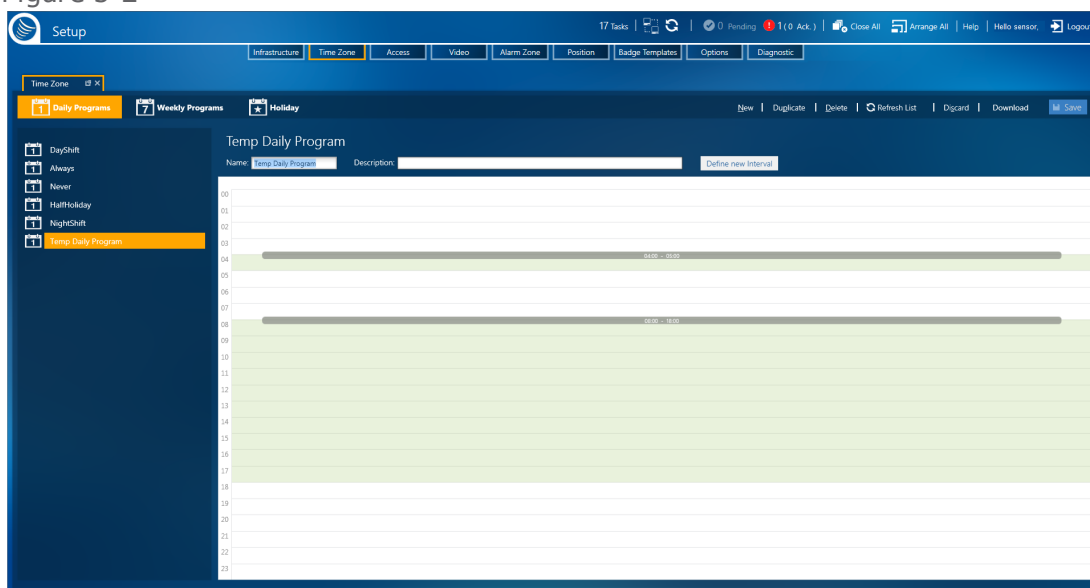
## Duplicating a Daily Program

If you want to add a Daily Program to the system, which is identical or almost identical to an existing Daily Program, use the Duplicate feature to perform this task quickly and accurately.

### How to duplicate a Daily Program

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Daily Program**. The Time Zones' Daily Program screen is displayed.
3. From the list of existing Daily Programs on the left, select the Daily Program that will be duplicated. The Daily Program's parameters and day calendar are displayed.

Figure 5-2



4. From the action bar, click **Duplicate**. A new Daily Program, identical to the Daily Program in focus, is displayed to the right of the list of existing Daily Programs. The only differences between the original and the duplicate are:
  - » The duplicate's name is appended with "\_Duplicate" (i.e. a Daily Program named "Temp Daily Program" would have a duplicate named "Temp Daily Program\_Duplicate").
  - » The duplicate has not been saved in the system database and will not appear in the list of existing Daily Programs.
  - » The duplicate has not been used in a WP.

A best practice is to rename the duplicate to something more identifiable.

5. Change the day calendar as required.

In the day calendar area, you have the following edit options:

- » Drag the top or bottom border of a green period to adjust the time in 15-minute intervals.
- » Double-click on a green period to open a dialog and make precise adjustments to the time in the default green period.
- » Click the **Define new interval** button to set a precise time for an additional green period within the displayed 24 hour day.

Alternatively, right-click on a white period (colored white) on the day calendar, and then click **Define new interval** in the context menu. A new green period, within the displayed 24 hour day, is added.

- » Right-click on a green period on the day calendar and then click **Remove region** in the context menu. The region is removed.

6. After modifying the duplicate Daily Program, do one of the following:

- » Click **Discard**. The unsaved, duplicate Daily Program is removed.
- » Click **Save**. The Daily Program is stored in the system database and is added to the list of existing Daily Programs.

## Editing a Daily Program

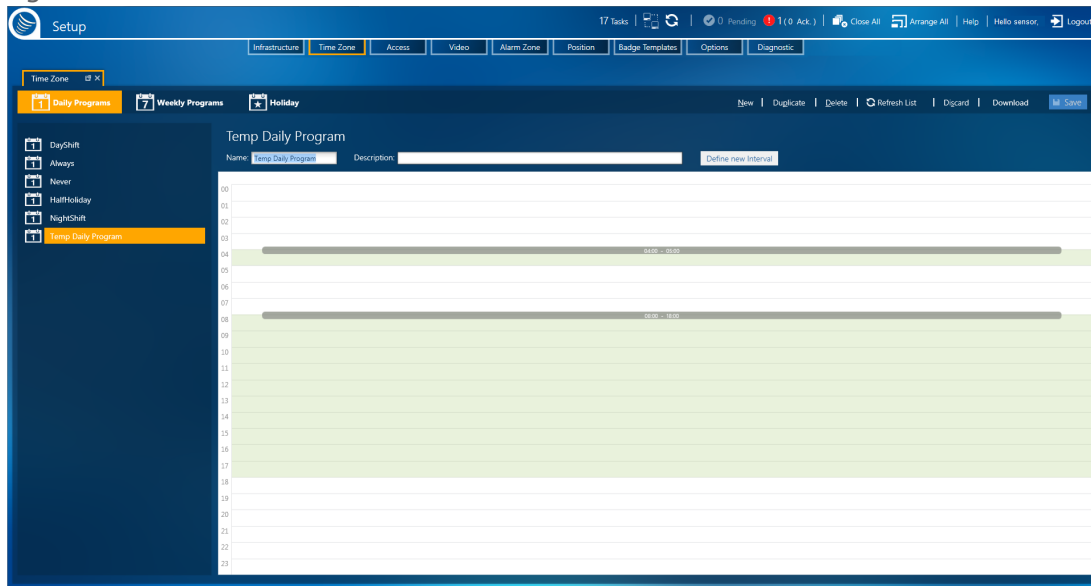
In a Daily Program, there are two editable groups:

- » Details (the Daily Program's name and description)
- » Day calendar periods (graphically displayed green and white periods)

## How to edit a Daily Program

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Daily Program**. The Time Zones' Daily Program screen is displayed.
3. From the list of existing Daily Programs on the left, select the Daily Program that will be edited. The Daily Program's parameters and day calendar are displayed.

Figure 5-3



4. Change the name, description, and day calendar as required.  
In the day calendar area, you have the following edit options:
  - » Drag the top or bottom border of a green period to adjust the time in 15-minute intervals.
  - » Double-click on a green period to open a dialog and make precise adjustments to the time in the default green period.
  - » Click the **Define new interval** button to set a precise time for an additional green period within the displayed 24 hour day.  
Alternatively, right-click on a white period (colored white) on the day calendar, and then click **Define new interval** in the context menu. A new green period, within the displayed 24 hour day, is added.
  - » Right-click on a green period on the day calendar and then click **Remove region** in the context menu. The region is removed.
5. After changing the Daily Program, do one of the following:
  - » Click **Discard**. The unsaved details and day calendar return to their previously saved values.
  - » Click **Save**. The updated Daily Program is stored in the system database and can be applied to a Weekly Program.

**Note:** After a Daily Program is updated and saved in the system database, all WPs that previously used the Daily Program are now governed by the updates.

**Note:** The **Always** and **Never** Daily Programs are built into the system and cannot be edited or deleted.



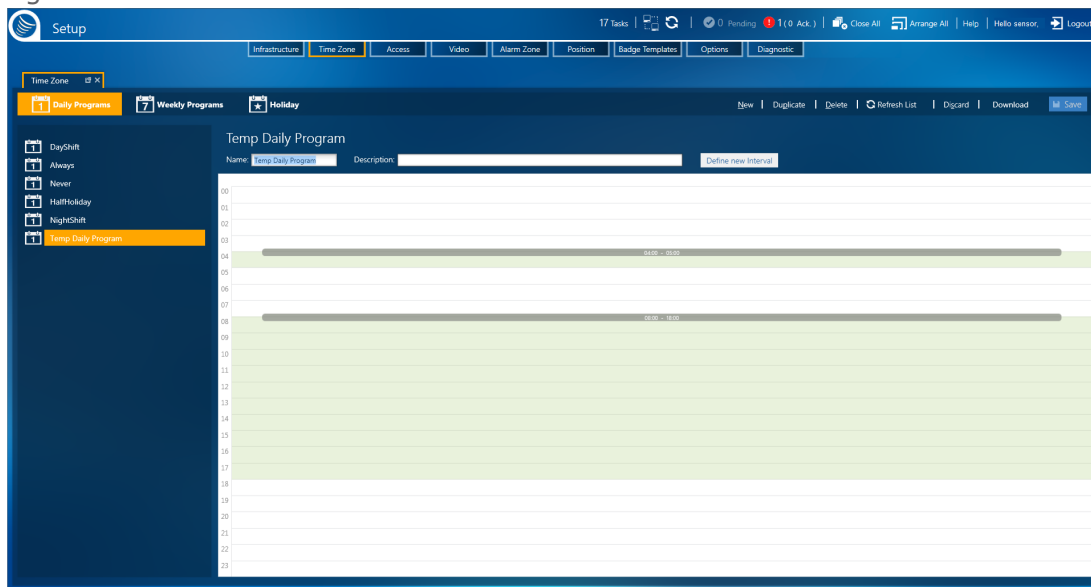
# Deleting a Daily Program from the System

Before you can delete a Daily Program, it must be detached from any Weekly Program (WP) currently using the Daily Program. For information about replacing a Daily Program used in a WP, see ["Editing a Weekly Program"](#) on page 125.

## How to delete a Daily Program from the system

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Daily Program**. The Time Zones' Daily Program screen is displayed.
3. From the list of existing Daily Programs on the left, select the Daily Program that will be deleted. The Daily Program's parameters and day calendar are displayed.

Figure 5-4



4. From the action bar, click **Delete**, and then confirm the operation. The Daily Program is removed from the system database and no longer appears in the Daily Program list.

**Note:** The **Always** and **Never** Daily Programs are built into the system and cannot be edited or deleted.

# Weekly Program Time Zones



**Note:** Defining Time Zones, Daily Programs, and Weekly Programs is very important. Properly defining the green and white periods in Daily Programs is essential for the system to work optimally.

A best practice is to successively specify the Daily and Weekly programs, as well as Holiday and Special Days, before defining the other parameters of the system.

A Time Zone determines the behavior of various entities in the system, this includes Cardholders, Reader, Inputs, Relays, and Reflexes. That's the simple definition. Now, let's look at what makes up a Time Zone and what's needed to apply a Time Zone to a system entity.

A **Time Zone** is made up of a range of times (periods) set to green or white. This white or green setting governs an entity's behavior and permissions.

All event behaviors connected to a system entity (actions and reactions) have timestamps. A timestamp is the time at which an event takes place. As soon as an event is stamped, its timestamp is checked against the current period (green or white). Based on the period where the timestamp falls, a set of rules are applied.

To apply Time Zones to a system entity requires a Weekly Program (WP).

In this topic, we will cover the WP, which is made up of one or more Daily Programs and may include a Holiday or Special days.

## Weekly Program (WP)

A WP consists of one Daily Program for each day in the weekly calendar. In addition to the standard seven-day weekly calendar, there is a Holiday option appended to the week and two Special Days (Special Day 1 and Special Day 2). For more information about Holidays and Special Days, see ["Time Zones Holiday & Special Day" on page 130](#).

**Note:** The Special Days will only appear when the Options screen's **Use Special days** is set to Yes.

Daily Programs may be assigned to each day of a WP.

The system has two predefined WPs. These WPs are as follows:

- » **WP Always:** Associates each day of the week and holidays to the Daily Program **Always**.
- » **WP Never:** Associates each day of the week and the holidays to the Daily Program **Never**.

**Note:** There is a third WP. However, it is only available via Access management. The third WP is called **WP Personal**. For more information about the **WP Personal** Weekly Program, see the ["General Tab" on page 608](#).

## Demonstration model of green and white period applications

The following table illustrates the influence of green and white periods on the system.

Entity	Green Period	White Period
<p><b>Cardholder Access</b></p> <p>A WP, attributed to a cardholder, defines when a cardholder may be granted access. It is attributed via an Access Groups (see <a href="#">"Access Groups Screen" on page 506</a>) or, if applicable, the cardholder's Personal WP (see the <a href="#">"General Tab" on page 608</a>).</p>	Access may be granted	Access denied
<p><b>Readers</b></p> <p>A WP, assigned to a reader, defines the reader's Access Mode rules. It is attributed via the Reader details' Access Mode tab (see <a href="#">"Access Mode Tab" on page 462</a>).</p>	Security Level 1	Security Level 2
<p><b>Alarm Zones (Input Groups) or individual Input devices</b></p> <p>A WP, attributed to an alarm zone or an input device, defines when it is armed or disarmed. It is attributed via the Security Task group's Events screen (see <a href="#">"Overriding an Alarm Zone's Status" on page 366</a>).</p>	Armed	Disarmed
<p><b>Relays</b></p> <p>A WP, attributed to a relay, defines when it is automatically activated. It is attributed via the Relays table and Relay details (see <a href="#">"Relays Table" on page 488</a> or <a href="#">"Relay Details" on page 485</a>).</p>	Armed	Disarmed
<p><b>Local Reflexes</b></p> <p>A WP, attributed to a Local Reflex, defines when it can be triggered. It is attributed via the Local Reflexes dialog (see <a href="#">"Local Reflex Details" on page 490</a> and <a href="#">"Local Reflex Table" on page 492</a>).</p>	May be triggered	Not triggered

## Adding a New Weekly Program

Use the following steps to create a new Weekly Program (WP) in the Time Zone screen.

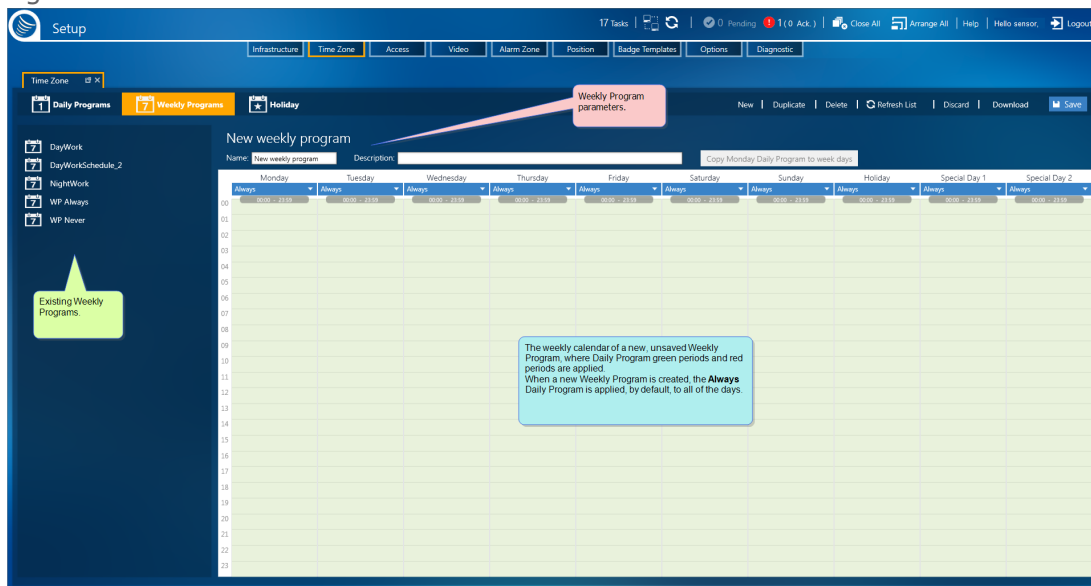
### How to create a new WP

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Weekly Program**. The Time Zones' Weekly Program screen is displayed.

- From the action bar, click **New**. New WP parameters with a default weekly calendar are displayed.

The default weekly calendar has the **Always** Daily Program applied to each day in the WP's weekly calendar.

Figure 5-5



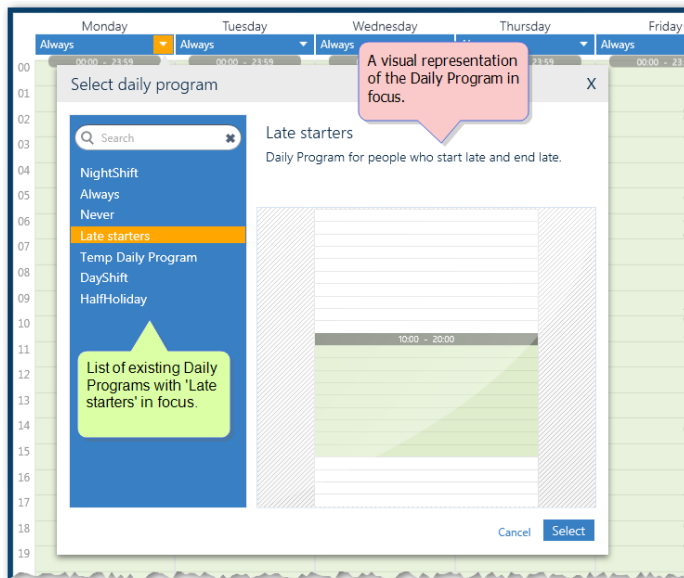
- In the Name field, enter a new name for the WP.

The name should identify the use of the program (where or when it would be applied).

(Optional) Enter a description that provided more information about the WP.

- In the weekly calendar area, where required, replace the **Always** Daily Program with another previously defined Daily Program:
  - Click the down arrow in the drop-down list at the top of a day column. The Select Daily Program dialog is displayed.

Figure 5-6



- b. Select a Daily Program from the list of existing Daily Programs. For information about the selection, refer to the image of the selected program's green period to the right of the Daily Programs list.
- c. Click **Select**. The day column now shows the selected Daily Program with its green period (s).

Alternatively, create and add a new daily Program from inside the WP (see "[Adding a Daily Program from inside a Weekly Program](#)" on page 126).

6. Repeat Step 5 for each day in the weekly calendar until you are satisfied with the WP's weekly calendar.

Alternatively, assign a Daily Program to the first day of the workweek in the WP, and then click the **Copy Daily Program to weekdays** button. The Daily Program will be applied to each day of the defined workweek in the weekly calendar.

7. After changing the default settings in the WP, do one of the following:
  - » Click **Discard**. The unsaved WP is removed.



**Note:** If you created a new Daily Program from inside the new WP, and then discard the WP, the new Daily Program will remain in the system and is available for assignment.

- » Click **Save**. The new WP is stored in the system database and appears in the Existing Weekly Programs list.

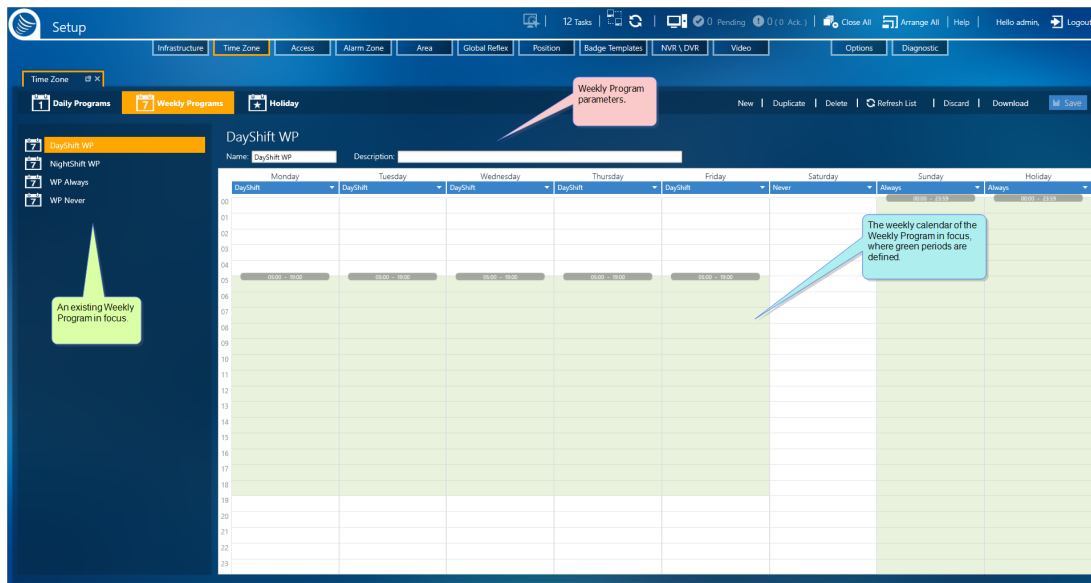
## Duplicating a Weekly Program

If you want to add a Weekly Program (WP) to the system that is identical, or almost identical, to an existing Daily Program, use the duplicate feature to perform this task quickly and accurately.

## How to duplicate a WP

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Weekly Program**. The Time Zones' Weekly Program screen is displayed.
3. From the list of existing WPs on the left, select the WP that will be duplicated. The WP's parameters and weekly calendar are displayed.

Figure 5-7



4. From the action bar, click **Duplicate**. A new WP, identical to the WP in focus is displayed to the right of the list of existing WPs. The only differences between the original and the duplicate are:
  - » The duplicate's name is appended with "\_Duplicate" (i.e. a WP named "DayWork" would have a duplicate named "DayWork\_Duplicate").
  - » The duplicate has not been saved in the system database and does not appear in the list of existing Weekly Programs.
  - » The duplicate has not been attached to any system entity.

A best practice is to rename the duplicate to something more identifiable.

5. Change the WP description and weekly calendar as required. In the weekly calendar area, you have the following edit options:
  - » Change the Daily Program of a day in the weekly calendar by creating a new Daily Program from inside the WP (see ["Adding a Daily Program from inside a Weekly Program" on page 126](#)).
  - » Change the Daily Program of a day in the weekly calendar by selecting an existing Daily Program from the drop-down list at the top of a day column in the weekly calendar.
  - » Change the Daily Program of the first day in the workweek, and then click the **Copy Daily Program to week days** button. The Daily Program will be applied to all of the other days in the predefined workweek.

6. After changing the duplicate WP, do one of the following:
  - » Click **Discard**. The unsaved, duplicate WP is removed.



**Note:** If you created a new Daily Program from inside the duplicate WP, and then discard the WP, the new Daily Program will remain in the system and is available for assignment.

- » Click **Save**. The duplicate WP is stored in the system database and can be applied to a system entity.

## Editing a Weekly Program

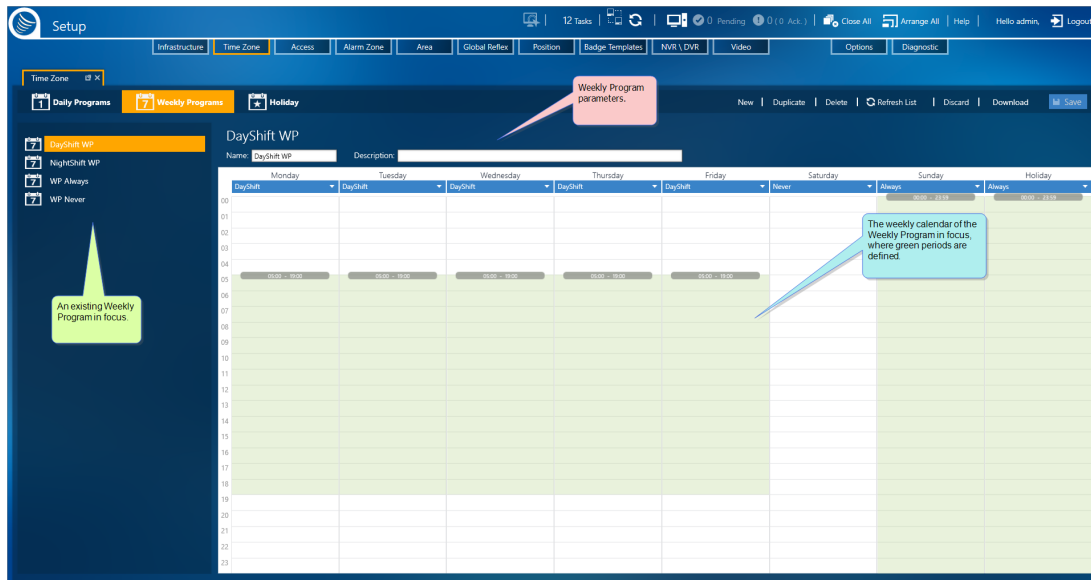
In a Weekly Program (WP), there are two editable groups:

- » Details (the WP's name and description).
- » Weekly calendar the area where green and white periods are assigned.

### How to edit a WP

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Weekly Program**. The Time Zones' Weekly Program screen is displayed.
3. From the list of existing WPs on the left, select the WP that will be edited. The WP's parameters and weekly calendar are displayed.

Figure 5-8

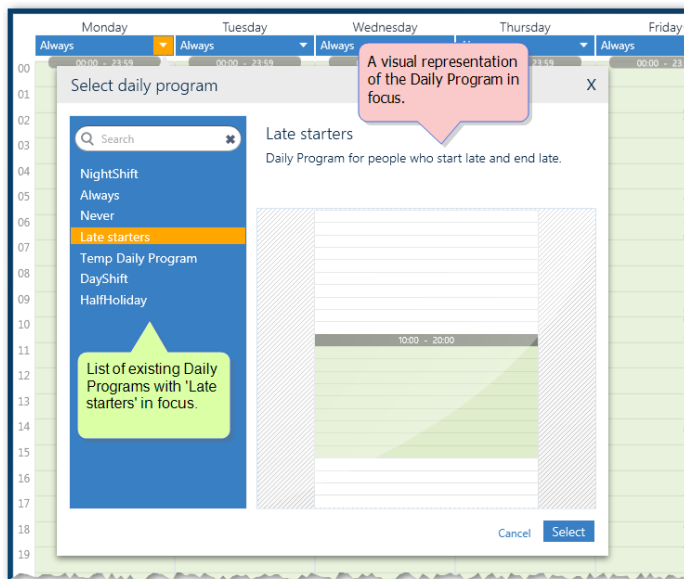


4. Change the WP as required.
  - In the details area, you can change the name or description.
  - In the weekly calendar area, you have the following edit options:

#### **Assign An existing Daily Program to a day in the weekly calendar**

- a. Click the down arrow in the drop-down list at the top of a day column. The Select Daily Program dialog is displayed.

Figure 5-9



- b. Select a Daily Program from the list of existing Daily Programs. For information about the selection, refer to the image of the selected program's green period to the right of the Daily Programs list.
- c. Click **Select**. The day column now shows the selected Daily Program with its green period (s).

### Create and add a new daily Program from inside the WP

See "[Adding a Daily Program from inside a Weekly Program](#)" below.

### Automatically populate a weekly calendar's workweek

Assign a Daily Program to the first day of the workweek in the WP, and then click the **Copy Daily Program to weekdays** button. The Daily Program will be applied to each day of the defined workweek in the weekly calendar.

5. After changing the WP, do one of the following:
  - » Click **Discard**. The unsaved details and weekly calendar return to their previously saved values.
  - » Click **Save**. The updated WP is stored in the system database and can be applied to a system entity. If the WP was previously assigned to an entity, the entity will now be governed by the updated WP data.



**Note:** If you created a new Daily Program from inside the WP, and then discard the WP changes, the new Daily Program will remain in the system and is available for assignment.

## Adding a Daily Program from inside a Weekly Program

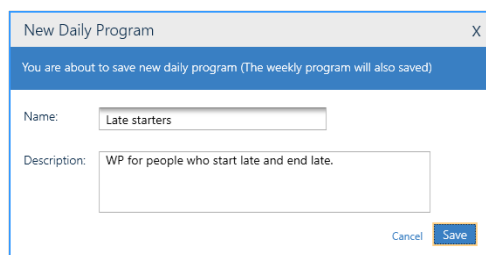
Use the following steps to create a new Daily Program from inside a Weekly Program (WP).



## How to add a Daily Program from inside a Weekly Program (WP)

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Weekly Program**. The Time Zones' Weekly Program screen is displayed.
3. From the Time Zones Weekly Program screen, select a WP from the list of existing Weekly Programs. The WP's parameters and the weekly calendar are displayed.
4. In the weekly calendar, choose the day where you would like the new Daily Program to appear, and then do one or both of the following:
  - a. Drag the top or bottom border of an existing green period and adjust the time. This will only adjust in 15-minute intervals.
  - b. Double-click a green period to open a dialog where you can adjust the times of the period more precisely.
  - c. Right-click on a non-green period area and select **Add New Region**. A new green area will appear in the area of the initial right-click. Now adjust the borders as instructed in Step "a" or "b".
  - d. Repeat either Step "a", "b" and or "c" until satisfied with the green period(s).
5. Click on another day on the calendar. A New Daily Program dialog is displayed.
6. Enter a name, and if required a description, for the Daily Program, and then click **Save**.

Figure 5-10



New Daily Program

You are about to save new daily program (The weekly program will also saved)

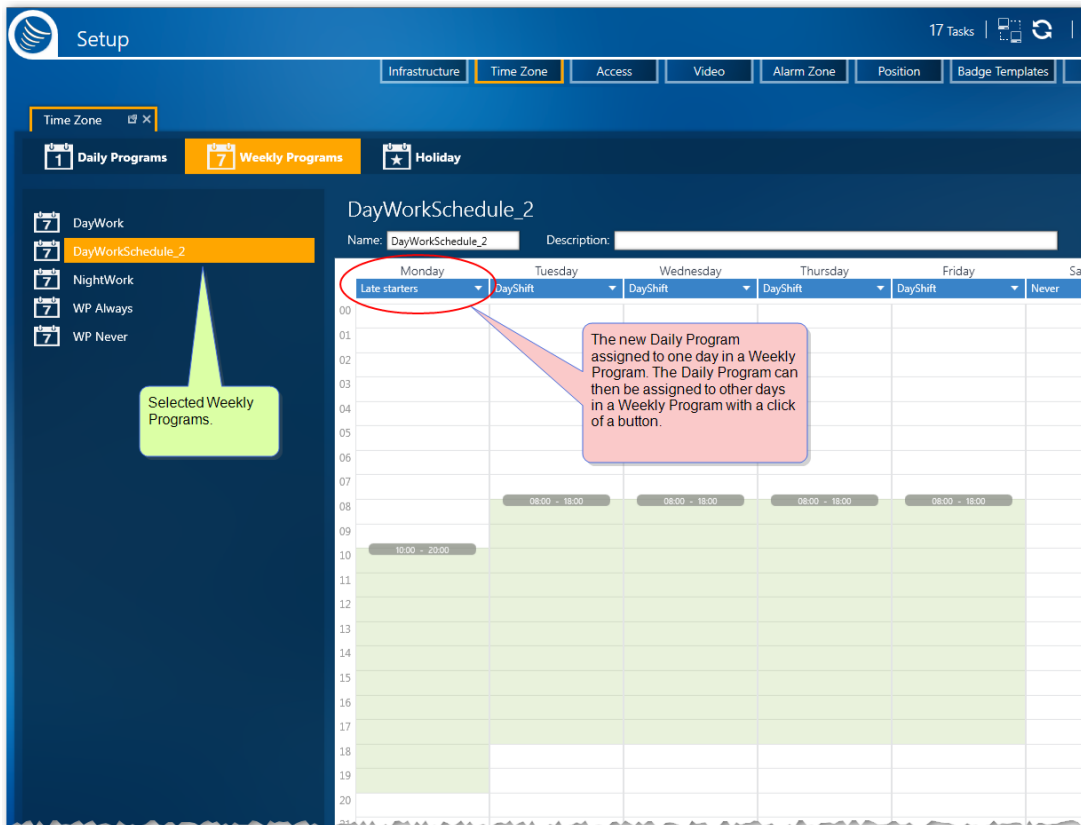
Name:

Description:

Cancel Save

The new Daily Program name appears at the top of the day's column and in the Time Zones' Daily Program screen. The new Daily Program can then be assigned to other days in the WP and days in other WPs.

Figure 5-11



7. After changing the WP, do one of the following:

- » Click **Discard**. The unsaved details and weekly calendar return to their previously saved values.
- » Click **Save**. The updated WP is stored in the system database, displayed in the Existing Weekly Programs list, and can be applied to a system entity.

**Note:** Part of the Adding a New Daily Program from inside a WP is an automatic save. If you add a new Daily Program from a WP as part of a general WP edit, the **Discard** command will undo any changes made after adding the new Daily Program from inside a WP (assuming you didn't click **Save**), but it will not undo any changes made before adding the new Daily Program from inside a WP.

If you delete a WP, where a Daily Program was added from inside the WP, the Daily Program will remain in the Time Zones' Daily Program list.

**Note:** The WP Always and WP Never Weekly Programs are built into the system and cannot be edited or deleted.

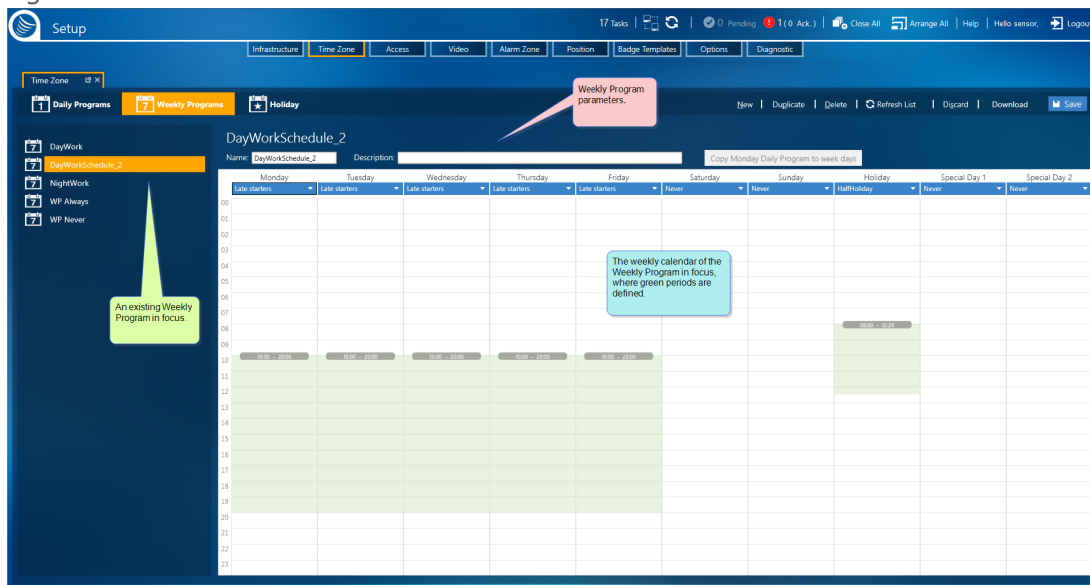
# Deleting a Weekly Program from the System

Before you can delete a Weekly Program (WP), it must be detached from any entity in the system currently using the WP. For information about replacing a WP with another WP, see ["Editing a Weekly Program"](#) on page 125.

## How to delete a WP from the system

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Weekly Program**. The Time Zones' Weekly Program screen is displayed.
3. From the list of existing WPs on the left, select the WP that will be deleted. The WP's parameters and weekly calendar are displayed.

Figure 5-12



4. From the action bar, click **Delete**, and then confirm the operation. The WP is removed from the system and no longer appears in the Existing Weekly Program list.

**Note:** The WP Always and WP Never Weekly Programs are built into the system and cannot be edited or deleted.

If you delete a WP, where a new Daily Program was created and added from inside the WP (see ["Adding a Daily Program from inside a Weekly Program"](#) on page 126), the Daily Program will remain in the Time Zones' Daily Program list.

# Time Zones Holiday & Special Day



**Note:** Defining Time Zones, Daily Programs, and Weekly Programs is very important. Properly defining the green and white periods in Daily Programs is essential for the system to work optimally. Holidays and Special days are date exceptions to a Weekly Program. A best practice is to successively specify the Daily, Weekly programs as well as Holiday and Special days before defining the other parameters of the system.

A Time Zone determines the behavior of various entities in the system, this includes Cardholders, Readers, Inputs, Relays, and Reflexes. That's the simple definition. Now, let's look at what makes up a Time Zone and what's needed to apply a Time Zone to a system entity.

A **Time Zone** is made up of a range of times set to green or white. This white or green setting governs an entity's behavior and permissions.

All event behaviors connected to a system entity (actions and reactions) have timestamps. A timestamp is an actual time in which an event takes place. As soon as an event is stamped, its timestamp is checked against the current period (green or white). Based on the period where the timestamp falls, a set of rules are applied.

To apply Time Zones to a system entity requires a Weekly Program (WP), which is made up of one or more Daily Programs and may include one or more Holidays and Special days.

In this topic, we will cover the optional Holiday & Special days, which may be used as a building block for creating a Weekly Program.

## Holidays and Special Days

**Note:** For Special Days to be available in a WP, the Options screen's **Use Special days** must be set to Yes. For more information, see "[Options Screen](#)" on page 567.

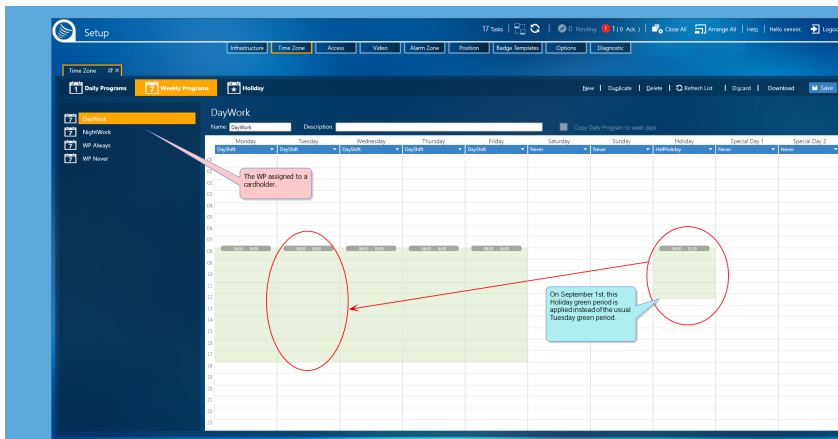
The Holiday and Special Days options allow you to specify *dates* on which the system will use a different set of Daily Program rules (green and white periods). During these dates, green and white periods defined in the Daily Program, and assigned to Holiday, Special Day 1, or Special Day 2, are applied regardless of the Daily Program assigned to that particular day of the week in the WP.

### For example:

Let's say September 1<sup>st</sup> is the first day of the school year and it's a national holiday (parents are celebrating all over the country).

This year, September 1<sup>st</sup> falls out on a Tuesday.

According to our cardholder's WP, Tuesday's green period is from 8:00 until 18:00. However, because it is also September 1<sup>st</sup>, the Daily Program assigned to the Holiday option in the WP (the green period from 8:00 until 12:30) is applied instead of the regular Tuesday Daily Program.



The scenario in this example could just as easily be applied to one of the Special Days instead of the Holiday.

## Adding a Holiday or Special Day

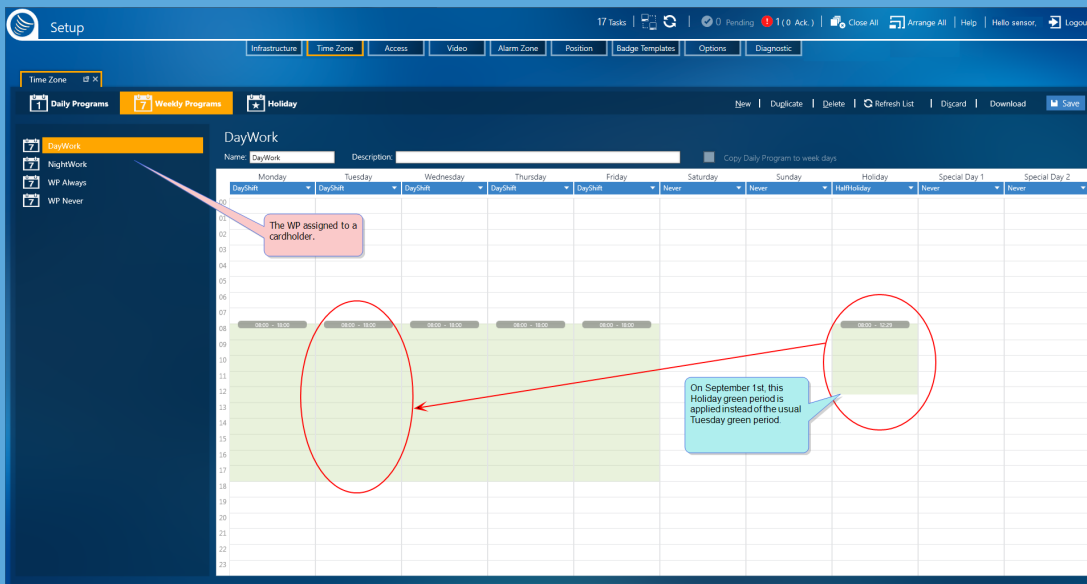
The Holiday and Special Day options allow you to specify dates on which the system should use a different set of Daily Program rules (green or white periods). During these dates, green and white periods defined in the Daily Program, and assigned to Holiday, Special Day 1, or Special Day 2, are applied regardless of the Daily Program assigned to that particular day or days of the week in the Weekly Program (WP).

### For example:

Let's say September 1<sup>st</sup> is the first day of the school year and it's a national holiday (parents are celebrating all over the country).

This year, September 1<sup>st</sup> falls on a Tuesday.

According to our cardholder's WP, Tuesday's green period is from 8:00 until 18:00. However, because it is also September 1<sup>st</sup>, the Daily Program assigned to the Holiday option in the WP (the green period from 8:00 until 12:30) is applied instead of the regular Tuesday Daily Program.



The scenario in this example could just as easily be applied to one of the Special Days instead of the Holiday.

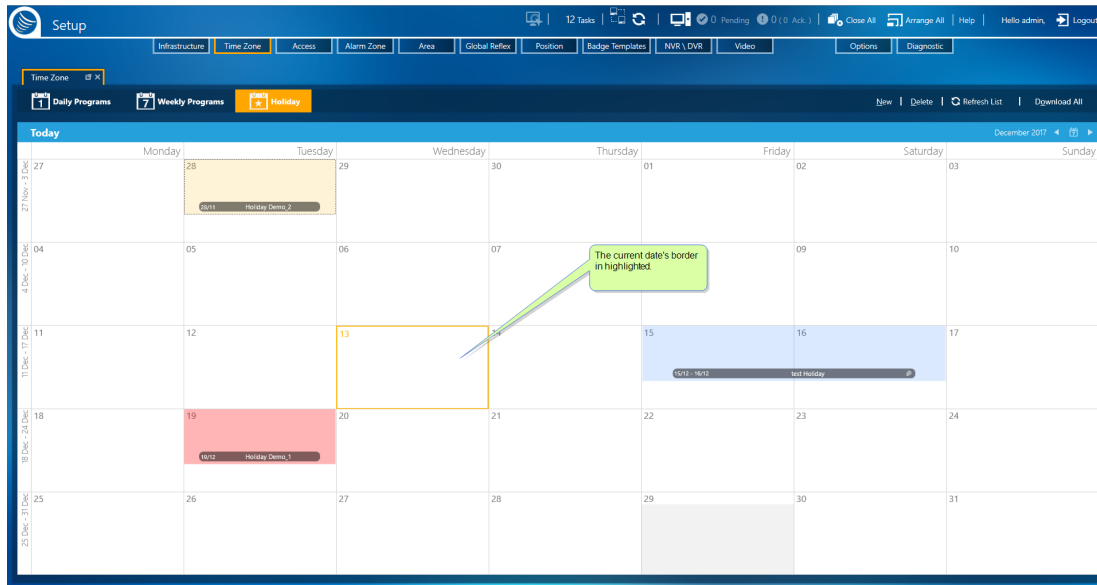
**Note:** For Special Days to be available in the WP, the option **Use Special days** must be set to Yes (see "Options Screen" on page 567).

The instructions that follow take for granted that **Use Special days** is set to Yes.

## How to create a Holiday or Special Day

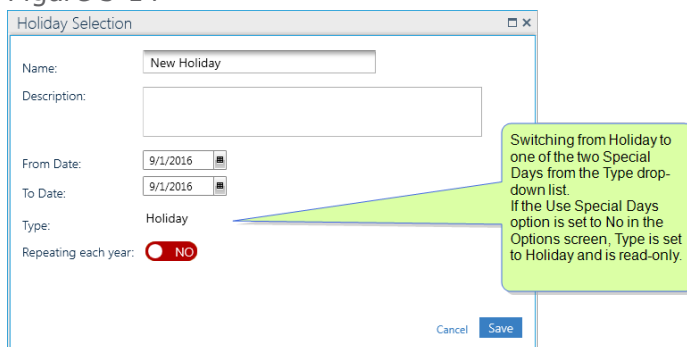
1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Holiday Program**. The Time Zones' Holiday Program screen is displayed.

Figure 5-13



3. Click on the date when the Holiday or Special Day will occur.  
If necessary, use the month navigation buttons on the right side of the calendar title bar.
4. From the action bar, click **New**. The Holiday Definition dialog is displayed.  
Alternatively, right-click on the selected date, and then click the **Add Holiday** command. The Holiday Definition dialog is displayed.

Figure 5-14



5. Enter a new name for the Holiday/Special Day.  
(Optional) Enter a description that provided more information about the Holiday/Special day.
6. Specify the **To** and **From** dates of the Holiday/Special day.  
The date selected in Step 3 is entered by default.
7. If you want the Holiday/Special day to repeat every year on the same date(s), drag the **Repeat each year** button to Yes.
8. From the Type drop-down list, select Holiday, Special day 1, or Special day 2. In the WP, the green period assigned to the selected day(s) will be applied to the weekday when the Holiday/Special day occurs.
9. Click **Save**. The Holiday/Special day is stored in the system database and is applied to all WPs.

**Note:** On rare occasions, where there may be a data conflict in the system database, click **Unlock** in the Holiday action bar to resolve the conflict. Clicking **Unlock**, where no data conflict exists, will not adversely affect your system or data.

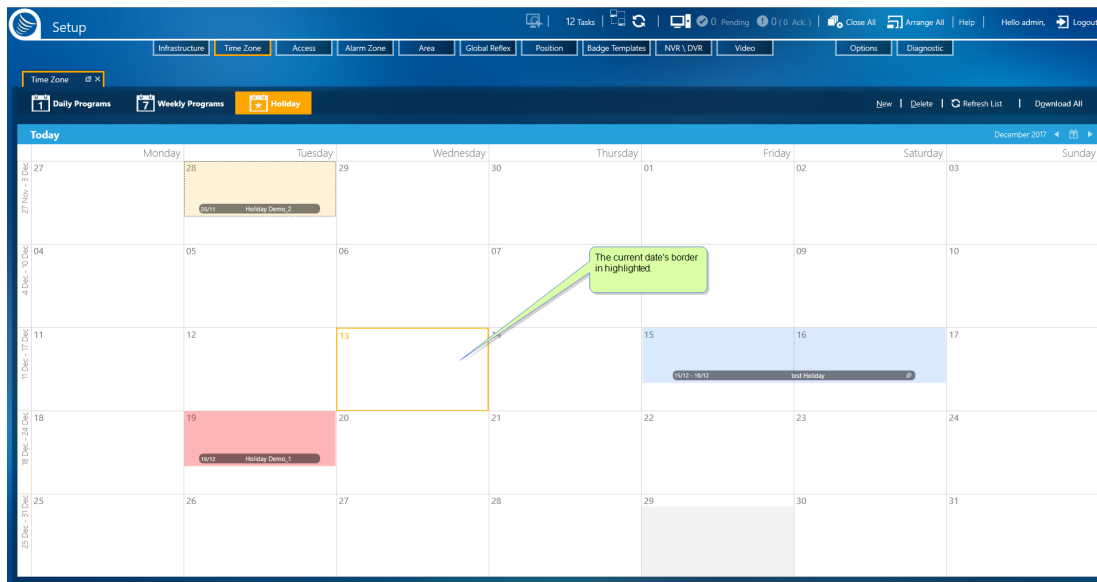
Whether or not **Unlock** appears in the action bar, is determined by the Options setting. For more information, see "[System & SQL Options](#)" on page 577.

## Editing or Deleting a Holiday or Special Day

### How to edit a Holiday / Special day

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Holiday Program**. The Time Zones' Holiday Program screen is displayed.

Figure 5-15



3. Click on the date when the Holiday or Special day occurs.  
If necessary, use the month navigation buttons on the right side of the calendar title bar.
4. Right-click on the selected date, and then click the **Edit Holiday** command. The Holiday Definition dialog is displayed.



Figure 5-16

The screenshot shows a 'Holiday Selection' dialog box with the following fields and values:

- Name: New Holiday
- Description: (empty)
- From Date: 9/1/2016
- To Date: 9/1/2016
- Type: Holiday
- Repeating each year:  NO

A callout box points to the 'Type' field with the following text: "Switching from Holiday to one of the two Special Days from the Type drop-down list. If the Use Special Days option is set to No in the Options screen, Type is set to Holiday and is read-only."

5. Make the required changes to the Holiday/Special day information, and then click **Save**. The Holiday/Special day is stored in the system database and is applied to all WPs.

Alternatively, to add additional days to an existing holiday, drag the left or right border of the holiday entry to another date in the same row of the calendar. confirm the operation and the calendar updates accordingly.


## How to delete a Holiday / Special Day

1. Go to the Setup Task group and click **Time Zones**. The Time Zones screen is displayed.
2. On the left side of the action bar, select **Holiday Program**. The Time Zones' Holiday Program screen is displayed.
3. Click on the date when the Holiday or Special day occurs.

If necessary, use the month navigation buttons on the right side of the calendar title bar.

4. From the action bar, click **Delete**, and then confirm the operation. The Holiday/Special day is removed from the calendar and the database.

Alternatively, right-click on the selected date, and then click the **Delete Holiday**. The Holiday/Special day is removed from the calendar.

 **Note:** On rare occasions where there may be a data conflict in the system database, click **Unlock** in the Holiday action bar to resolve the conflict. Clicking **Unlock**, where no data conflict exists, will not have any adverse effects on your system or data.

# Time Zones: MultiSite Impact

Each site has its own Daily Programs (DP) and Weekly Programs (WP). These DPs and WPs cannot be shared with other sites. The built-in DP and WP, named **Always** and **Never**, are accessible to all sites.

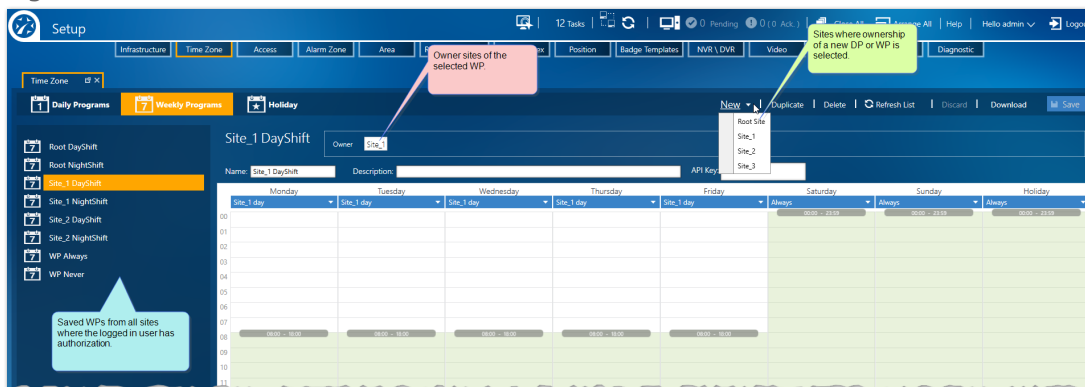
If a user is adding a new DP or WP they must select the site that will own the DP or WP via the **New** button's drop-down list. This is especially relevant for users who have authorization to more than one site.

When adding a new WP, you can only select a DP owned by the same site.

The list of saved DPs and WPs will display all site DPs and WPs where the user has authorization.

The site owner of a selected DP or WP appears above the Hours or Week table. Ownership of a DP and WP cannot be changed.

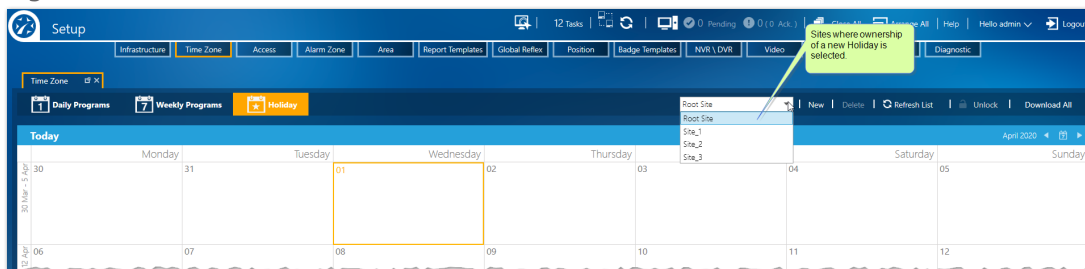
Figure 5-17



# Holiday support for MultiSite

Holidays, like DPs and WPs, need to be owned by a site at the time it is added to the system.

Figure 5-18



If the selected site is the Root site, the Holiday Selection dialog has an **Add Holiday to other sites** field that does not exist for other sites.

When **Add Holiday to other sites** is set to **YES**, the holiday is copied to all other sites in the system. If one of the other sites already has a holiday on the same date, the copy of the Root holiday will not be added to that site.

Figure 5-19

Holiday Selection

Name:

Description:

From Date:

To Date:

Type:

Repeating each year:  NO

Add Holiday to other sites:  YES

Owner:

Cancel Save

Only available when the holiday is owned by the root site. Puts a copy of the holiday on all sites.

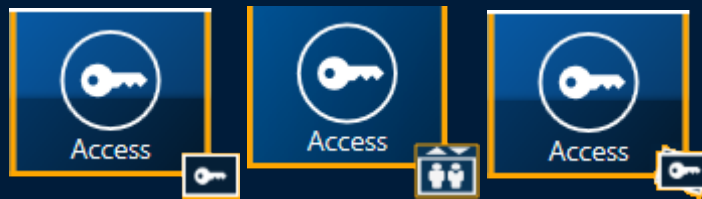
If the Root holiday is edited in the Root site, the holiday will be updated on other sites where it was copied.

If a Root holiday copy is edited in a non-Root site, the holiday in the non-Root site will no longer be updated from the Root holiday.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 6:

## Access

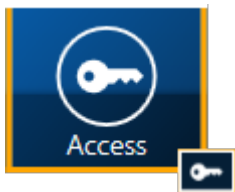


The Access screens manage a cardholder's access routes and time authorization as determined by assigned Access Groups. A Door Access Group (DAG) includes the "where and when" a cardholder may gain access via door readers.

A Lift Access Group (LAG) includes the "where and when" a cardholder may gain access to an elevator's passenger cabin and/or which floor buttons in the cabin's control panel are enabled. For more information about Lift setup, see "[Understanding the Lift Setup concept in GuardPoint10](#)" on page 53.

Door and Lift Access Groups may be grouped in containers called Multiple Access Groups (MAGs). A MAG is assigned to cardholders to provide authorizations to the cardholders. Alternatively, an Access Group can be assigned to a cardholder directly via a Persona Door Access Group or a Personal Lift Access Group.

# Access Groups



Defining Access Groups and the method used to assign them (Personal Access Group, Multiple Access Group or, Temporary Access) is very important. Properly defining the access options for a cardholder is essential for the system to work optimally.

A best practice is, after defining Weekly Programs, specify the Access Groups and/or Multiple Access Groups. Access Groups and Multiple Access Groups can be added or edited at any time.

Access Groups determine which doors or elevators are accessible, via reader device, to a cardholder during a cardholder's Weekly Program (WP) green period.

From a technical standpoint, an Access Group determines the badge codes that will be saved in a controller. For example, a cardholder assigned an Access Group, which includes Controller1\_Reader1, will have the cardholder's badge code saved in Controller1's local database.

There are two types of Access Group:

- » **Door Access Group:** Includes the "where and when" a cardholder may gain access via door readers.
- » **Lift Access Group:** Includes the "where and when" a cardholder may gain access to an elevator's passenger cabin and/or which floor buttons in the cabin's control panel are enabled. For more information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10" on page 53.](#)

## Methods available to assign an Access Group listed by priority

### » **Temporary Access**

Associates a cardholder with a scheduled reader or Multiple Access Group that can be scheduled and a Weekly Program that is applicable only in the Temporary Access event. Another Temporary Access advantage is that a Temporary Access reader does not have to be in an Access Group.

### » **Personal Access Groups (Personal Door Access Group and Personal Lift Access Group)**

Associates a cardholder with a Door Access Group list and /or a Lift Access Group. This method eliminates the need to create an unusually large number of Multiple Access Groups.

Personal Access Groups are best applicable, in a school-like environment where very few students would have the same class schedule, you would assign Access Groups directly for each student.

### » **Multiple Access Group**

Associates a cardholder with a collection of Door Access Groups and /or a Lift Access Group. Reduces the overall number of Access Groups necessary in a system.

A Multiple Access Group is best applicable, in an office-like environment where all of the cardholders in a department would generally have access authorization to the same spaces.



**Note:** A cardholder can be assigned a combination of any of the three methods listed above. If there is a conflict between a cardholder's assigned methods, the method with the higher priority will override the other method assigned to the cardholder. The priority order is: Temporary Access, Personal Access Group, and then Multiple Access Group.

## Built-in Access Groups

GuardPoint10 includes two built-in Access Groups. These groups cannot be deleted or modified. The built-in Access Groups are as follows:

- » **Anytime Anywhere:** Provides free access to all doors at all times.
- » **No Access:** (default) Denies access to all doors at all times. This group may be used for an employee who is temporarily separating from an organization. They still have their badge and the security system still has their details in its database. In the **Personal Door Access Groups list**, **No Access** is not available.

## MultiSite Impact

When **MultiSite** is set to **Yes**:

- » **Anytime Anywhere:** Available only to super users. It applies access authorization to all spaces at all times on all sites (except for elevators).
- » **Prefixed Anytime Anywhere:** Each site in the system has its own **Anytime Anywhere** access group and is prefixed with the name of the site. It allows access to all spaces at all times within the site.

## Adding a New Access Group

Use the following steps to create a new Access Group in the Access screen.

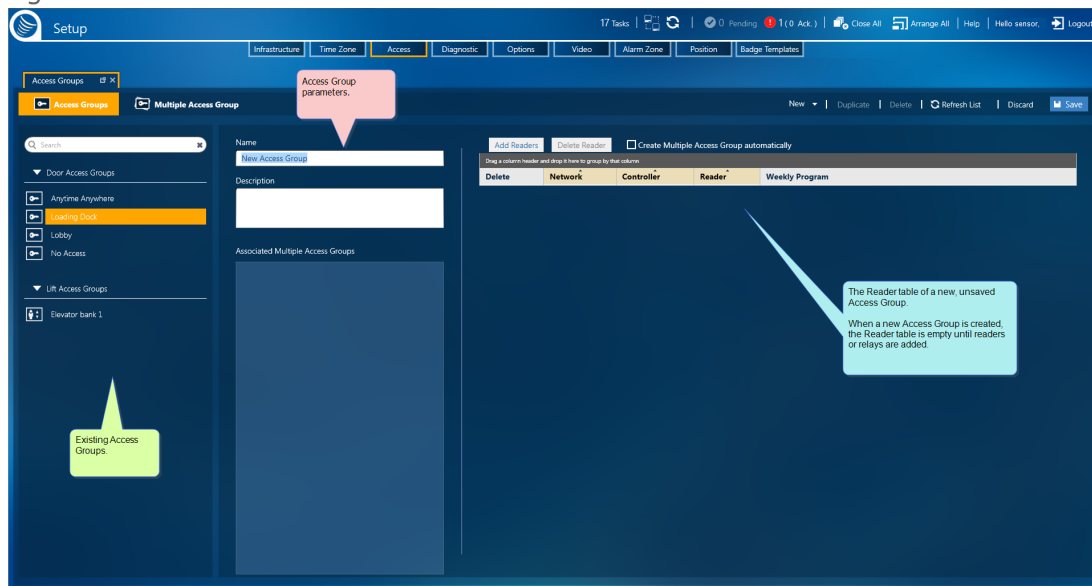
### How to create a new Access Group

1. Go to the Setup Task group and click **Access**. The Access screen is displayed.
2. On the left side of the action bar, select **Access Group**. The Access' Access Group screen is displayed.
3. From the action bar, click the **New** down arrow and select the type of Access Group you want to create:
  - » **Door Access Group:** Includes most all doorways that allow cardholders to move from one location to another.
  - » **Lift Access Group:** This type of group is designated for lift (elevator) doors. It allows cardholders to move from one floor in a building into an elevator passenger car. For more

information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10"](#) on page 53.

Access Group parameters, about the Access Group selected, are displayed along with an empty Readers / Relays table, depending on the type of Access Group in focus (Door or Lift).

Figure 6-1



#### 4. Enter Access Group information as required:

- » Enter a new name for the Access Group.

The name should identify how the group will be used.

- » (Optional) Enter a description that provided more information about the group you are creating.

- » The **Assigned Multiple Access Groups** list is read-only and is initially empty. If the **Create Multiple Access Group Automatically** checkbox is selected, a Multiple Access Groups with the same name as the new Access Group will appear in the **Assigned Multiple Access Groups** list, after the Access Group is saved.

The **Create Multiple Access Group Automatically** checkbox only appears when a new Access Group is being created. After you click **Save**, the checkbox is hidden.

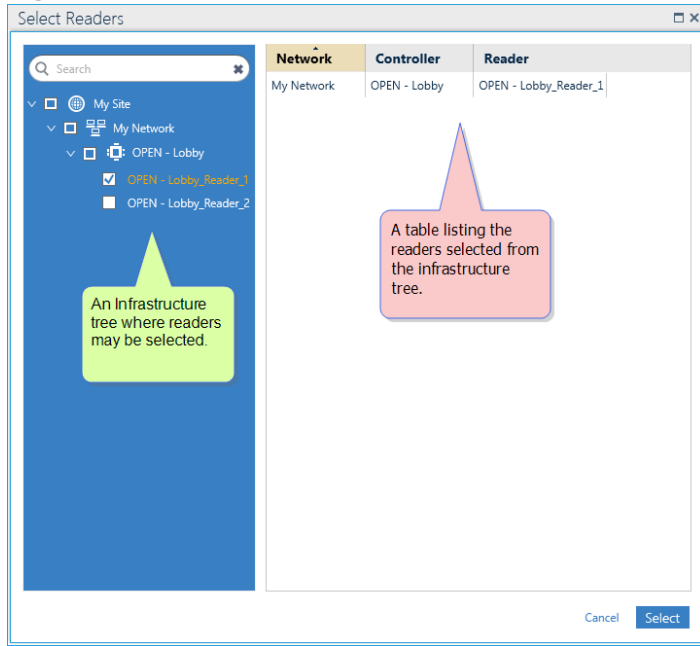
For more information about the Access Group information, see ["Access Groups Screen"](#) on page 506.

#### If you are creating a new Door Access Group, continue from here.

1. In the Readers table, click **Add Reader**. The Select Readers dialog is displayed.



Figure 6-2



- Choose readers, and then click **Select**. The readers are added to the Door Access Group's Readers table.

Figure 6-3



- (Optional) Switch the Weekly Program if necessary.

Besides the operator-defined Weekly Programs (WPs), the system has three predefined WPs in Access management:

- » **WP Always:** Associates each day of the week and the Holidays to the Daily Program **Always**.
- » **WP Never:** Associates each day of the week and the Holidays to the Daily Program **Never**.

» **WP Personal**: Applies the Weekly Program selected in the cardholder details of the person requesting access. If the cardholder details do not specify a personal weekly program, **WP Never** will be associated by default.

4. After defining your Door Access Group and adding readers, do one of the following:

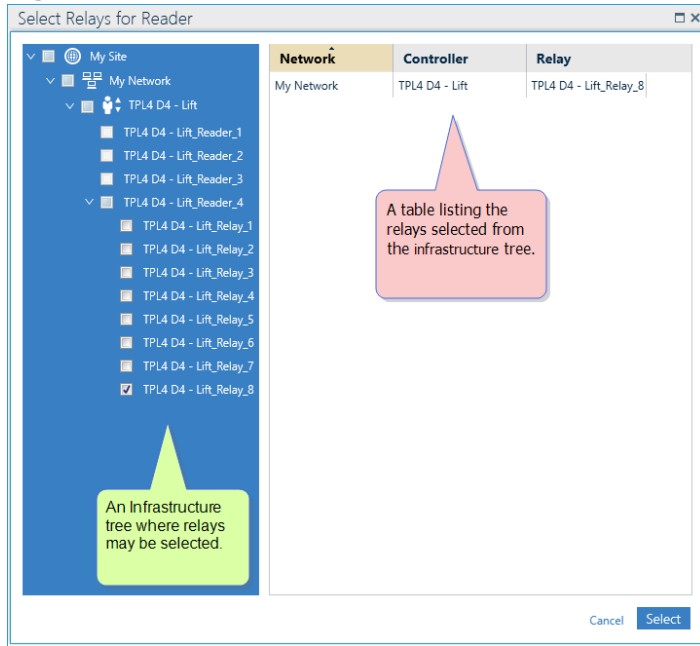
» Click **Discard**. The unsaved Door Access Group is removed.

» Click **Save**. The new Door Access Group is stored in the system database and can be assigned to a cardholder via a Multiple Access Group.

**If you are creating a new Lift Access Group, continue from here.**

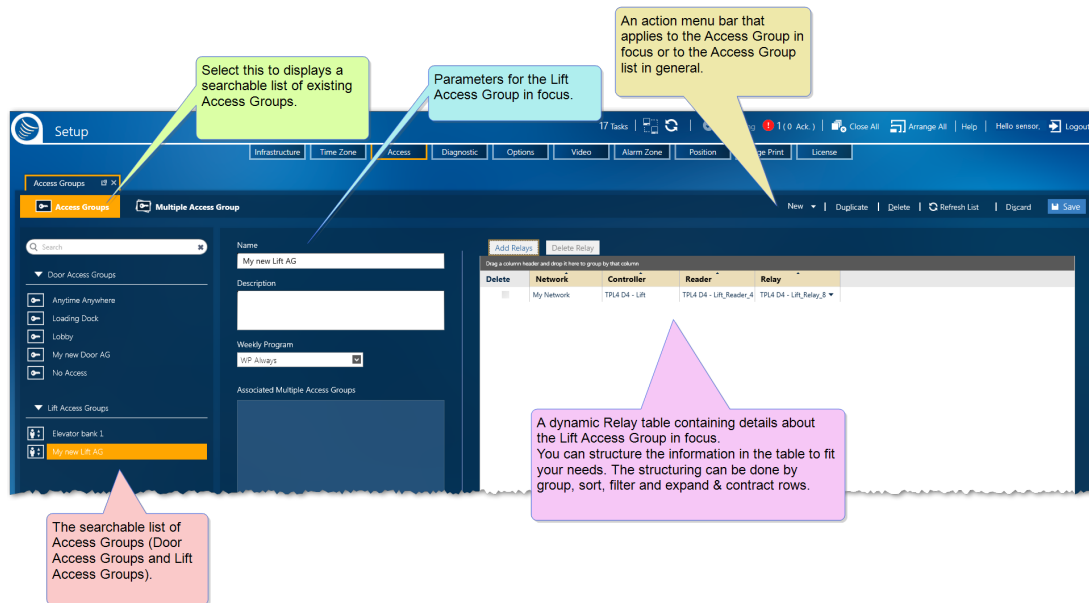
1. In the Readers table, click **Add Relay**. The Select Relay dialog is displayed.

Figure 6-4



2. Choose relays, and then click **Select**. The relays are added to the Lift Access Group's Readers table.

Figure 6-5



3. From just below the **Description** field, select the **Weekly Program** that will be assigned to the group.

Besides the operator-defined Weekly Programs (WPs), the system has three predefined WPs in Access management:

- » **WP Always:** Associates each day of the week and the Holidays to the Daily Program **Always**, where access is always granted.
- » **WP Never:** Associates each day of the week and the Holidays to the Daily Program **Never**, where access is never granted.
- » **WP Personal:** Applies the Weekly Program selected in the cardholder details of the person requesting access. If the cardholder details do not specify a personal weekly program, **WP Never** will be applied by default.

4. After defining your Lift Access Group and adding relays, and a WP, do one of the following:

- » Click **Discard**. The unsaved Lift Access Group is removed.
- » Click **Save**. The new Lift Access Group is stored in the system database and can be assigned to a cardholder via a Multiple Access Group.

#### MultiSite impact on Access Groups

You may have to choose a site where the new Access Group will be added. Only readers owned by that site or shared with that site will be available to add to the new Access Group.

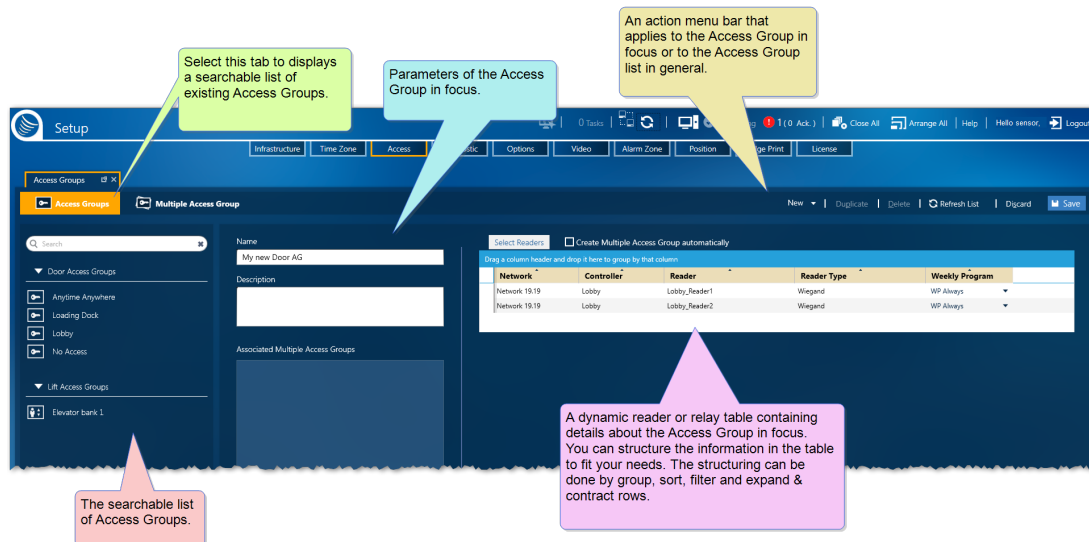
## Duplicating an Access Group

Use the following steps to duplicate an Access Group.

## How to duplicate an Access Group

1. Go to the Setup Task group and click **Access**. The Access screen is displayed.
2. On the left side of the action bar, select **Access Group**. The Access' Access Group screen is displayed.
3. From the list of existing Access Groups on the left, select the Access Group that will be duplicated. The Access Group's parameters and Readers table or Relays table are displayed.

Figure 6-6



4. From the action bar, click **Duplicate**. A new Access Group, identical to the Access Group in focus, is displayed to the right of the list of existing Access Groups. The only differences between the original and the duplicate are:
  - » The duplicate's name is appended with "\_Duplicate" (i.e. An Access Group named "My new AG" would have a duplicate named "My new AG\_Duplicate").
  - » The duplicate has not been saved in the system database and therefore has a **Create Multiple Access Group automatically** checkbox displayed. If the **Create Multiple Access Group Automatically** checkbox is selected, a Multiple Access Groups with the same name as the new Access Group will appear in the **Assigned Multiple Access Groups** list, after the Access Group is saved.
  - » The duplicate has not been assigned to a Multiple Access Group.

A best practice is to rename the duplicate to something more identifiable.

5. Change the name, description, and Readers table or Relays table as required (see "[Access Groups Screen](#)" on page 506).

The **Assigned Multiple Access Groups** list is read-only and is initially empty.

6. Depending on the type of Access Group created, do one of the following:

### For Door Access Groups

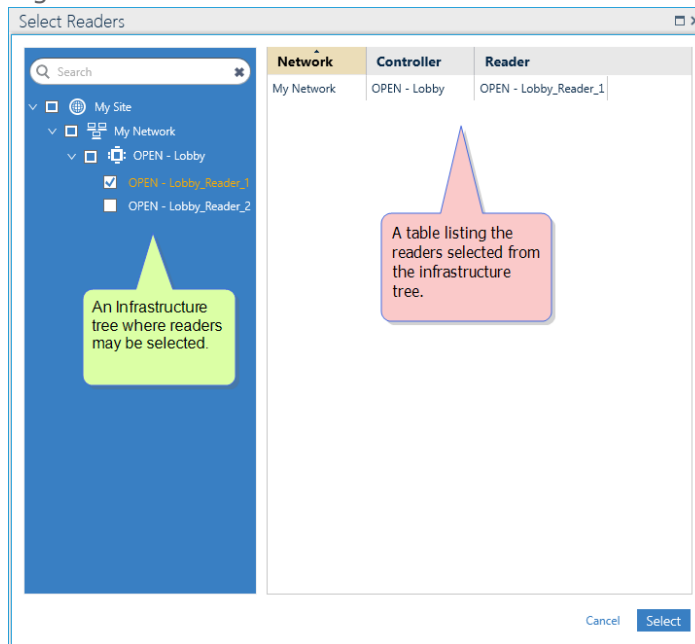
In the Readers table, you have the following edit options:

#### Add readers to the table

- a. In the Readers table, click **Add Reader**. The Select Readers dialog is displayed.

- b. Select one or more readers from the infrastructure tree on the left side of the dialog. The reader will appear in the table on the right of the dialog.

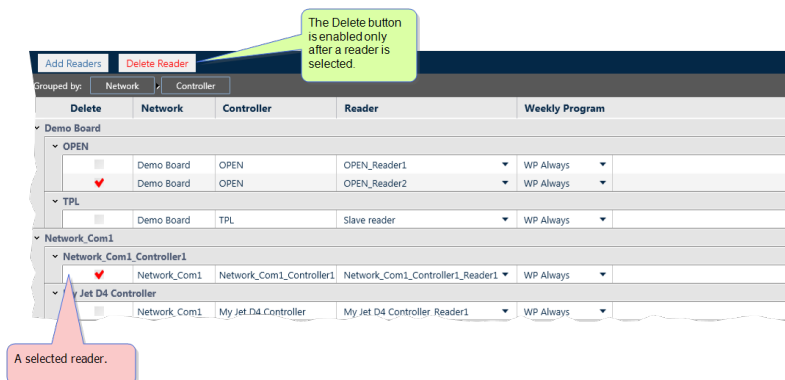
Figure 6-7



- c. Click **Select**. The readers are added to the Access Group's Readers table.

### Delete readers from the table

- a. In the Readers table, select the Delete checkbox for the reader(s) that will be deleted.



- b. Click **Delete Reader**. The reader(s) are removed from the Access Group.

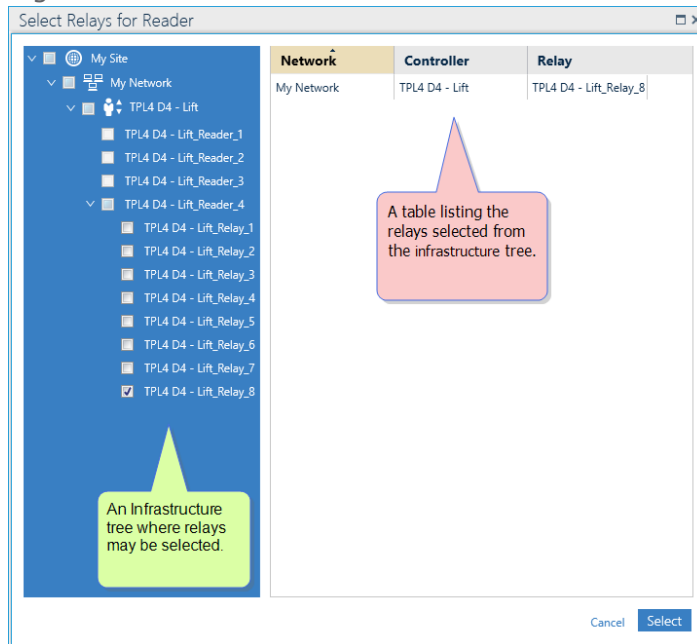
### For Lift Access Groups

In the Relays table, you have the following edit options:

#### Add Relays to the table

- a. In the Relays table, click **Add Relays**. The Select Relays from Reader dialog are displayed.
- b. Select one or more relays from a reader in the infrastructure tree on the left side of the dialog. The relay will appear in the table on the right of the dialog.

Figure 6-8

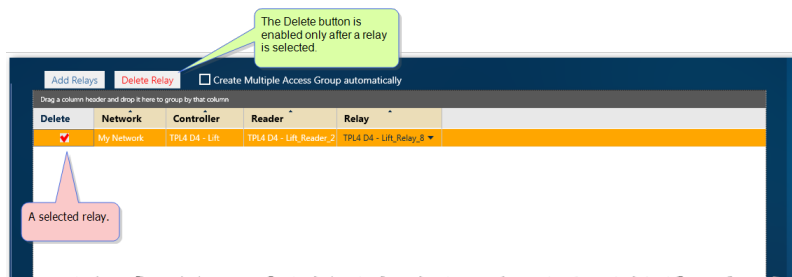


c. Click **Select**. The readers are added to the Access Group's Readers table.

For more information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10"](#) on page 53.

### Delete Relays from the table

a. In the Relay table, select the Delete checkbox for the relay(s) that will be deleted.



b. Click **Delete Relay**. The relay(s) are removed from the Access Group.

7. After modifying your Duplicate Access Group, do one of the following:

- » Click **Discard**. The unsaved Access Group is removed.
- » Click **Save**. The Access Group is stored in the system database and can be assigned via a Multiple Access Group.

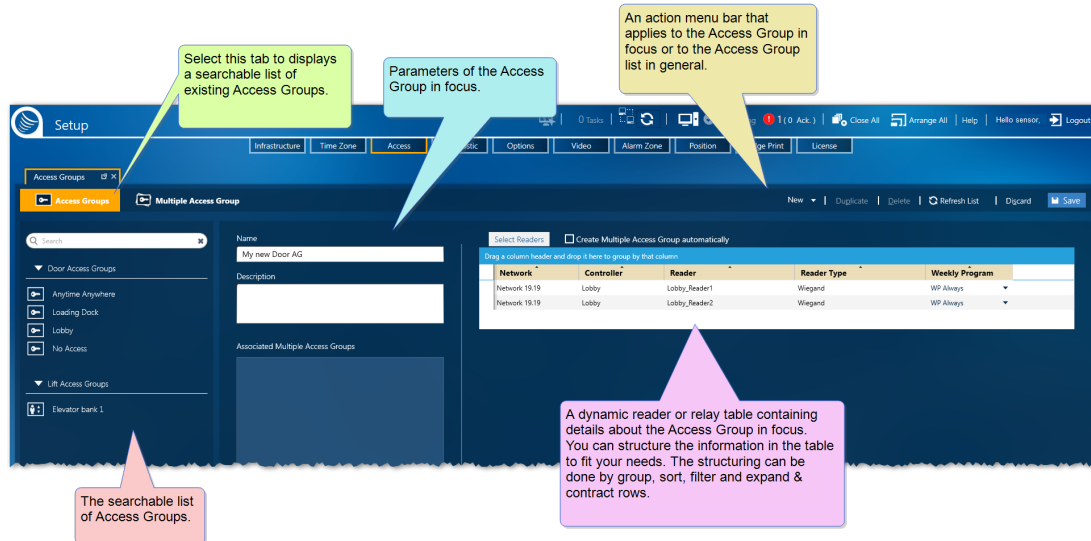
## Editing an Access Group

Use the following steps to edit an Access Group.

# How to edit an Access Group

1. Go to the Setup Task group and click **Access**. The Access screen is displayed.
2. On the left side of the action bar, select **Access Group**. The Access' Access Group screen is displayed.
3. From the list of existing Access Groups on the left, select the Access Group that will be edited. The Access Group's parameters and Readers table (for Door Access Groups) or Relays table (for Lift Access Groups) are displayed.

Figure 6-9



4. Change the name or description. and Readers table and or Relays table as required (see "Access Groups Screen" on page 506).

To change the content of a Reader or Relay table, click the select button above the table and edit the list of previously selected readers or relays as required. Click Select in the dialog, and the table updates.

The **Assigned Multiple Access Groups** list is read-only and is initially empty. If the **Create Multiple Access Group Automatically** checkbox was selected when the Access Group was created, a Multiple Access Groups with the same name as the Access Group being edited will appear in the Assigned Multiple Access Groups list. This list can be edited via the Multiple Access Group screen. For more information, see "cardholderEditing a Multiple Access Group" on page 163.

5. Depending on the type of Access Group created, do one of the following:

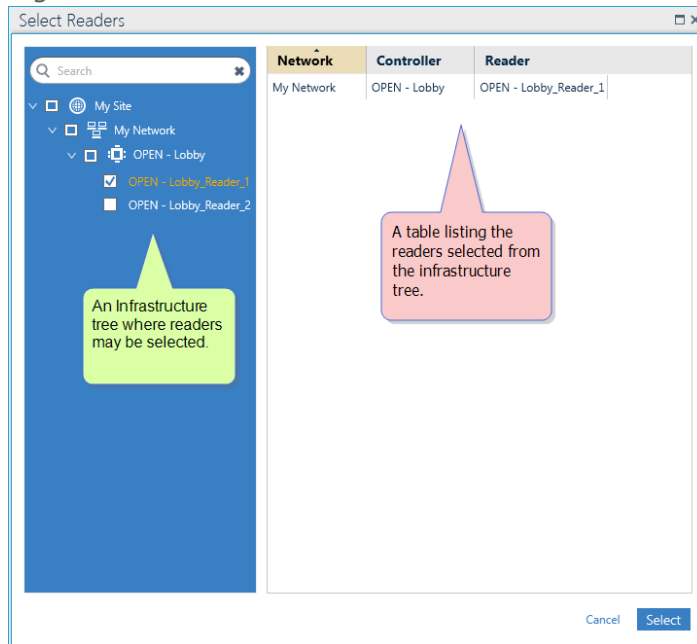
### For Door Access Groups

In the Readers table, you have the following edit options:

#### Add readers to the table

- a. In the Readers table, click **Select Reader**. The Select Reader dialog is displayed.
- b. Select one or more readers from the infrastructure tree on the left of the dialog. The reader will appear in the table on the right of the dialog.

Figure 6-10



**Note:** If the reader is a slave reader, it will inherit its Access Group from its master reader and will not be available for selection.

- c. Click **Select**. The readers are added to the Access Group's Readers table.

#### Delete a reader from the table

- a. Above the Readers table, click **Select Reader**. The Select Reader dialog is displayed.
- b. Remove items from the Selected list in the dialog via the red **X** at the beginning of each row. Click **Select**. The reader(s) are removed from the Access Group's Readers table.

#### Replace the Weekly Program of a listed reader



**Note:** A slave reader's Weekly Program is inherited from its master reader.

- a. In the Readers table's Weekly Program column, click the drop-down list arrow of the reader that will be assigned a different Weekly Program. A Select Weekly Program dialog is displayed.
- b. From the Select Weekly Program dialog, select a Weekly Program for the reader in focus. A graphic representation of the Weekly Program will appear to the right of the Weekly Program list.
- c. Click **Select**. The new Weekly Program will appear in the Readers table.

The system has three predefined WPs in Access management:

- » **WP Always:** Associates each day of the week and the Holidays to the Daily Program **Always**.
- » **WP Never:** Associates each day of the week and the Holidays to the Daily Program **Never**.



- » **WP Personal**: Applies the Weekly Program selected in the cardholder details of the person requesting access. If the cardholder details do not specify a personal weekly program, **WP Never** will be applied by default.

## Replace the Weekly Program of multiple readers listed via a context menu



**Note:** A slave reader's Weekly Program is inherited from its master reader.

- From the Readers table, press the **Shift** or **Alt** key and click one or more reader rows to place the rows in focus.
- Right-click a reader row that is in focus. A context menu appears.
- From the context menu, select **Change Weekly Program**. A Select Weekly Program dialog is displayed.
- From the Select Weekly Program dialog, select a Weekly Program for the readers in focus. A graphic representation of the Weekly Program will appear to the right of the Weekly Program list.
- Click **Select**. The new Weekly Program will appear in the Readers table.

The system has three predefined WPs in Access management:

- » **WP Always**: Associates each day of the week and the Holidays to the Daily Program **Always**.
- » **WP Never**: Associates each day of the week and the Holidays to the Daily Program **Never**.
- » **WP Personal**: Applies the Weekly Program selected in the cardholder details of the person requesting access. If the cardholder details do not specify a personal weekly program, **WP Never** will be applied by default.

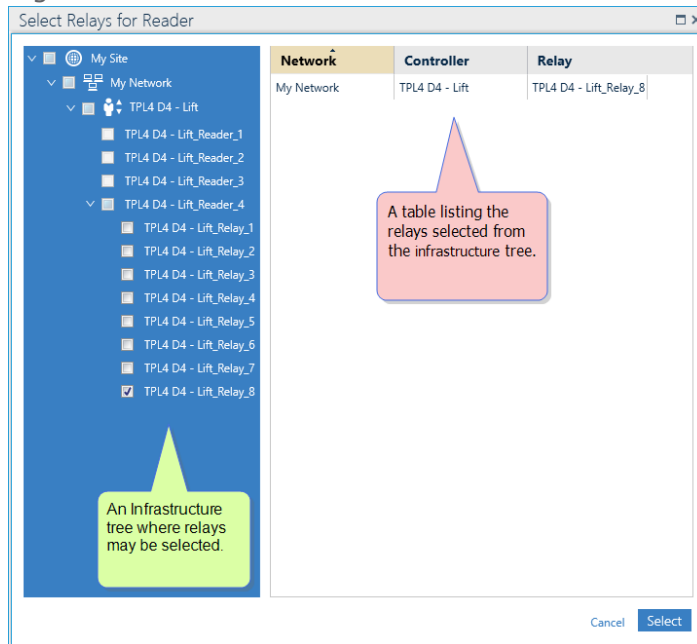
### For Lift Access Groups

In the Relays table, you have the following edit options:

#### Add relays to the table

- In the Relays table, click **Select Relay**. The Select Relays for Reader dialog is displayed.
- Select one or more relays from the infrastructure tree on the left of the dialog. The relays will appear in the table on the right of the dialog.

Figure 6-11



- c. Click **Select**. The relays are added to the Access Group's Readers table.

For more information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10"](#) on page 53.

### Replace a relay already in the Relays table

- a. In a Relays table row, select the drop-down list arrow in the **Relay** column. A list of available relays is displayed.
- b. From the list, click a Replacement relay's name. The new relay now appears in the Relays table.
- c. Click **Save**. The Lift Access Group is updated with the replacement relay.

A relay can also be replaced by the Select Relays button and opening the Select Relays for Reader dialog.

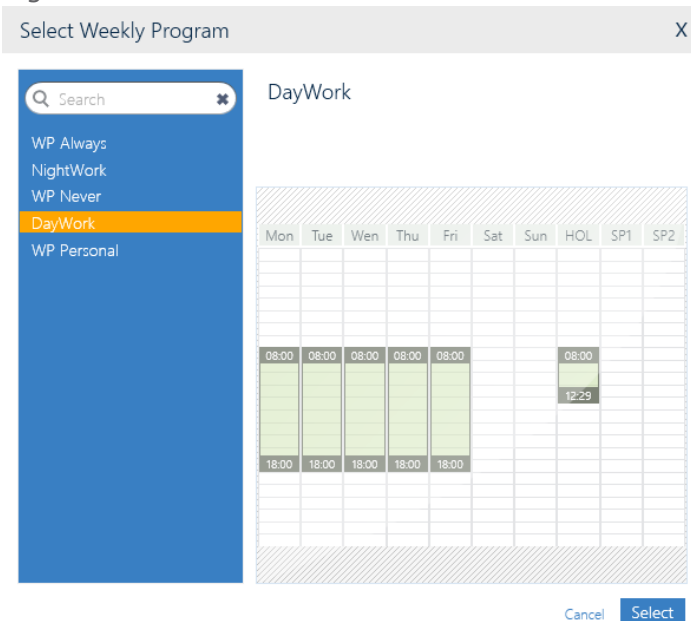
### Delete a relay from the table

- a. In the Relays table, click **Select Relay**. The Select Relays for Reader dialog is displayed.
- b. Remove items from the Selected list in the dialog via the red **X** at the beginning of each row. Click **Select**. The relay(s) are removed from the Access Group's Relay table.

### Replace the Weekly Program of a Lift Access Group's Relay

- a. In a Relays table row, select the drop-down list arrow in the **Weekly Program** column. A Select Weekly Program dialog is displayed.
- b. From the Select Weekly Program dialog, select the new Weekly Program for the relay in focus. A graphic representation of the Weekly Program in focus will appear to the right of the Weekly Program list.

Figure 6-12



- c. Click **Select**. The new Weekly Program will appear in the relay's **Weekly Program** field for all relays assigned the same reader as the relay where the Weekly Program was changed.

Besides the operator-defined Weekly Programs (WP), the system has three predefined WPs in Access management:

- » **WP Always:** Associates each day of the week and the Holidays to the Daily Program **Always**.
- » **WP Never:** Associates each day of the week and the Holidays to the Daily Program **Never**.
- » **WP Personal:** Applies the Weekly Program selected in the cardholder details of the person requesting access. If the cardholder details do not specify a personal weekly program, **WP Never** will be associated by default.

The selected Weekly Program is applied to all of the relays in the group that is assigned to the same reader. The Lift Access Group may include relays from more than one reader.

For more information about Lift setup, see "[Understanding the Lift Setup concept in GuardPoint10](#)" on page 53.

6. After updating your Access Group, do one of the following:
  - » Click **Discard**. The unsaved details return to their previously saved values.
  - » Click **Save**. The updated Access Group is stored in the system database and can be assigned to a cardholder via a Multiple Access Group.

**Note:** After an Access Group is updated and saved in the system database, all cardholders that were assigned the Access Group, via a Multiple Access Group, or directly via a cardholder details **Door Access Groups** or **Personal Lift Access Group** field are now governed by the updates. Click **Download** to manually download all data related to cardholders assigned to a Multiple Access Group that includes the edited Access Group.

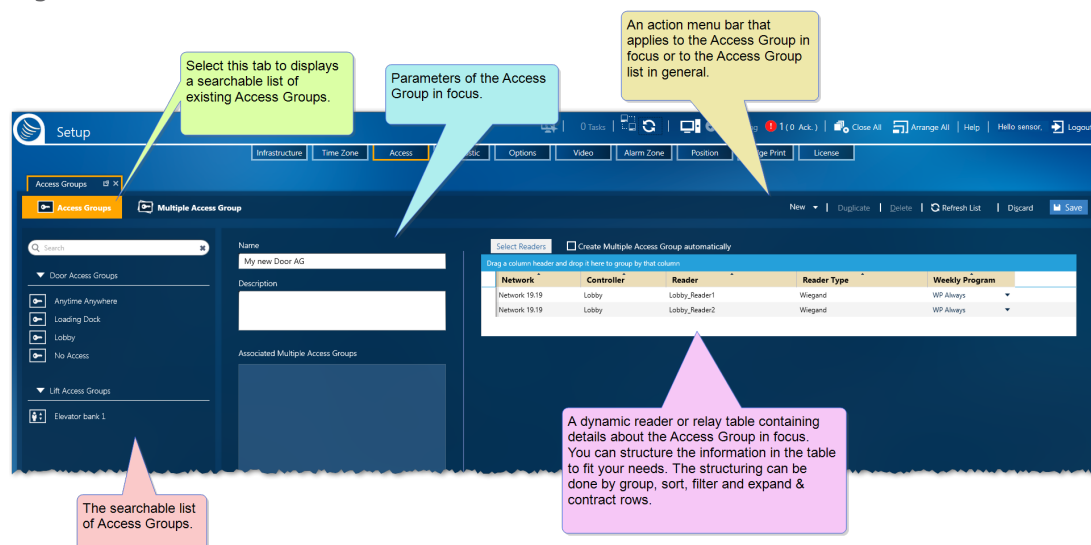
# Deleting an Access Group

Use the following steps to delete an Access Group.

## How to edit an Access Group

1. Go to the Setup Task group and click **Access**. The Access screen is displayed.
2. On the left side of the action bar, select **Access Group**. The Access' Access Group screen is displayed.
3. From the list of existing Access Groups on the left, select the Access Group that will be deleted. The Access Group's parameters and Readers table are displayed.

Figure 6-13



4. From the action bar, click **Delete**, and then confirm the operation. The Access Group is removed from the system and is no longer assigned to a Multiple Access Group(s).

If the Access Group (Door or Lift) was assigned to a cardholder directly via the cardholder details **Personal Door Access Groups** or **Personal Lift Access Group** fields, the Access group will automatically be removed from the cardholder details.

**Note:** The **Anytime Anywhere** and **No Access** Access Groups are built into the system and cannot be edited or deleted.

## MultiSite impact on Anytime Anywhere and No Access

An **Anytime Anywhere** is automatically added for each site when the site is added to the infrastructure and cannot be edited or shared. The **Anytime Anywhere** is automatically deleted after the site is deleted from the system.

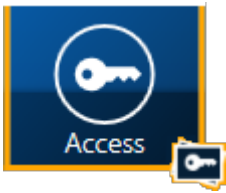
A site's **Anytime Anywhere** is prefixed with the name of the site.

There is only one instance of **No Access** and it is available to any site in the infrastructure.

The Root site has an additional **Anytime Anywhere** without a prefix. This **Anytime Anywhere** contains all readers from all sites in the infrastructure.



# Multiple Access Groups



**Note:** Defining Access Groups and Multiple Access Groups is very important. Properly defining the access options for a cardholder is essential for the system to work optimally. A best practice is, after defining Weekly Programs, specify the Access Groups and Multiple Access Groups.

Access Groups determine a cardholder's access routes.

A Multiple Access Group is a container that holds individual Access Groups. An Access Groups association to a cardholder must go through a Multiple Access Group. This means that for an Access Group to be associated with a cardholder, the Access Group must be a member of a Multiple Access Group associated with the cardholder. Multiple Access Groups allow access rules to be determined by a combination of existing Access Groups, rather than having to create a single, complex Access Group for each access scenario.

**Note:** An individual Access Group can be a member of more than one Multiple Access Group.

## Built-in Multiple Access Groups

GuardPoint10 includes two built-in Multiple Access Groups. These groups cannot be deleted or modified. The built-in Multiple Access Groups are as follows:

- » **Anytime Anywhere:** Contains the **Anytime Anywhere** Access Group. It provides free access to all doors.
- » **No Access:** (default) Contains the **No Access** Access Group. It denies access to all doors. This Multiple Access Group may be used for an employee who is temporarily separating from an organization. They still have their badge and the system database still has their details.

These Multiple Access Groups were created to allow a cardholder to associate with one of the built-in Access Groups. As stated earlier, the only way to associate an Access Group with a cardholder is via a Multiple Access Group, even if that Multiple Access Group has only one Access Group member.

## MultiSite Impact

When **MultiSite** is set to **Yes**:

- » **Anytime Anywhere:** Available only to super users. It includes the **Anytime Anywhere** access group, where all spaces at all times in all sites (except for elevators) are accessible.
- » **Prefixed Anytime Anywhere:** Each organization in the system has its own **Anytime Anywhere** Multiple Access Group which is prefixed with the name of the site. It includes the prefixed **Anytime Anywhere** access group that allows access to all spaces at all times within the organization.

# Adding a New Multiple Access Group

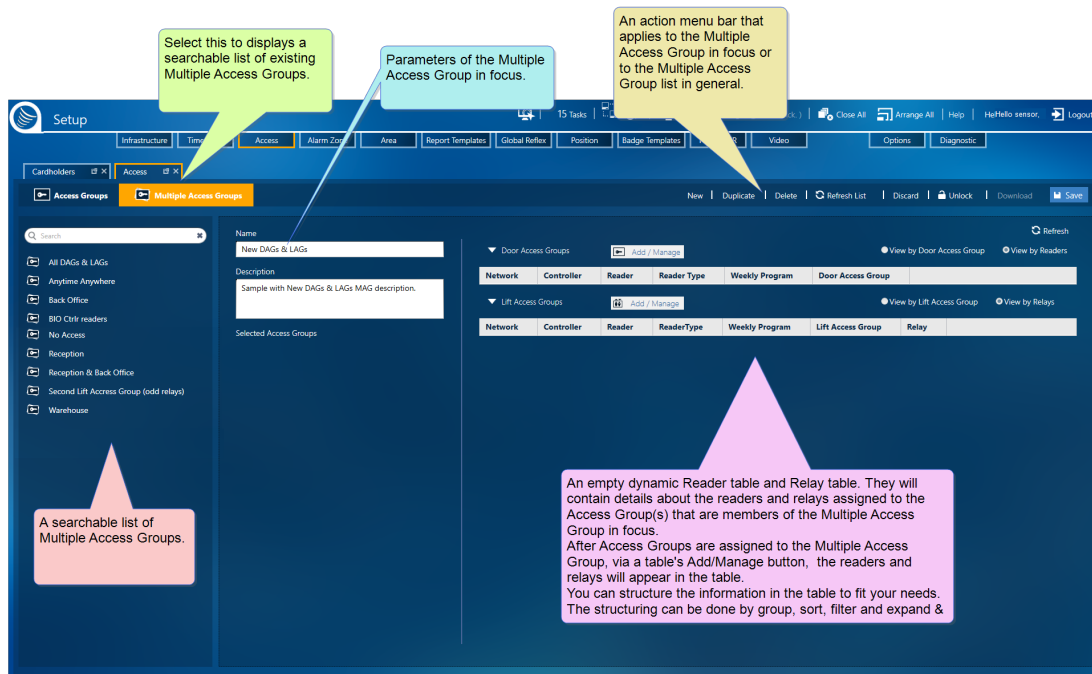
Use the following steps to create a new Multiple Access Group in the Access screen.

## How to create a new Multiple Access Group

1. Go to the Setup Task group and click **Access**. The Access screen is displayed.
2. On the left side of the action bar, select **Multiple Access Group**. The Access' Multiple Access Group screen is displayed.
3. From the action bar, click **New**. New Multiple Access Group parameters and an empty dynamic Readers table (for Door Access Groups) and Relays table (for Lift Access Groups) are displayed.

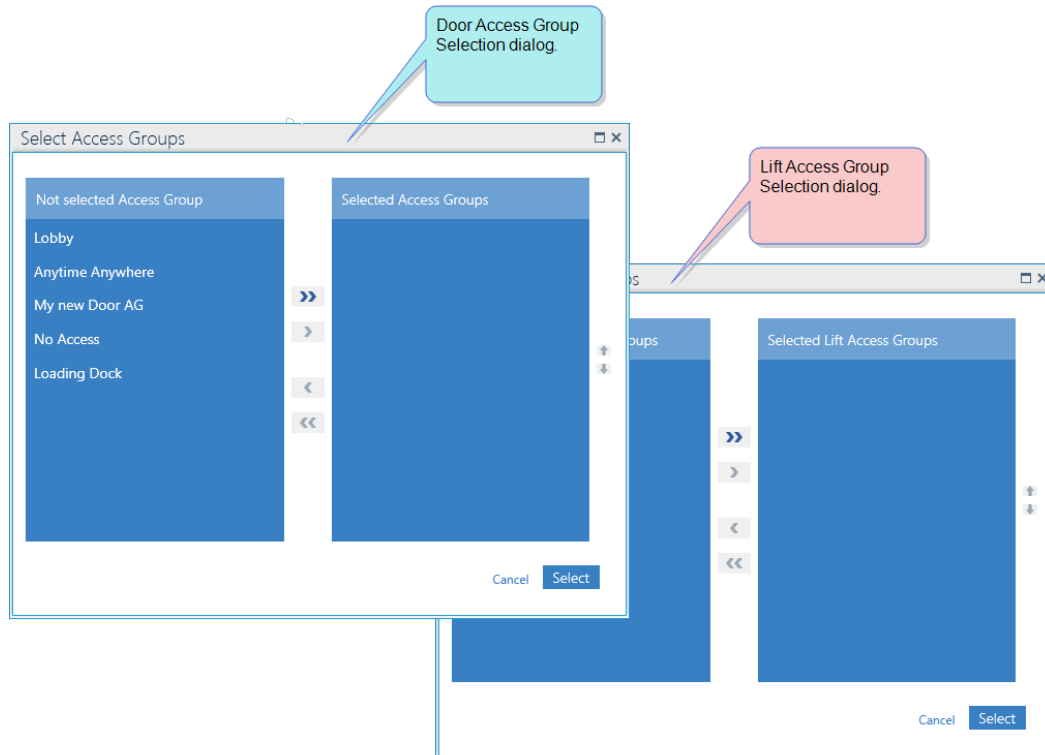
MultiSite Impact: When clicking **New**, you may have to choose a site that will own the new Multiple Access Group.

Figure 6-14



4. Enter a new name for the Multiple Access Group.  
The name should identify the use of the group.  
(Optional) Enter a description that provided more information about the group.
5. From just above either the Door Access Group table or the Lift Access Group table, click **Add/Manage**. A Select Access Group dialog is displayed listing the available Access Groups of the selected type (Door or Lift).  
The **Selected Access Groups** list is read-only and is initially empty. The list will include the Access Groups assigned to the Multiple Access Group. An Access Group may be assigned to more than one Multiple Access Group.

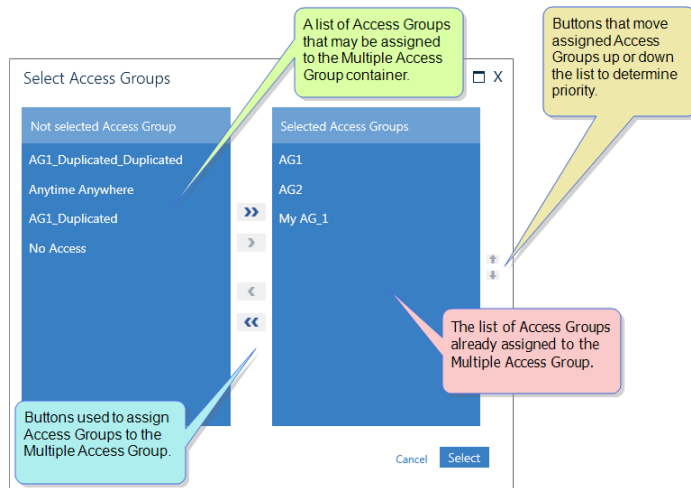
Figure 6-15





6. Use the following buttons to assign Access Groups from the list of **Not Selected Access Groups** on the left of the dialog to the **Selected Multiple Access Group** list:
  - » Assigns all of the Access Groups from the **Not Selected Access Groups** list to the **Selected Multiple Access Group** list.
  - « Revokes the assignment of all Access Groups in the **Selected Multiple Access Group** list and returns them to the **Not Selected Access Groups** list.
  - » Assigns selected Access Groups from the **Not Selected Access Groups** list to the **Selected Multiple Access Group** list.
  - « Revokes the assignment of selected Access Groups in **Selected Multiple Access Group** list and returns them to the **Not Selected Access Groups** list.
7. After compiling the list of Access Groups that will be assigned to the Multiple Access Group, order the list by priority. The Access Group at the top of the list will have the highest priority and will take precedence over any conflicting rules from an Access Group found lower on the list.



Figure 6-16



Use the following buttons to set the priority order of the list of assigned Access Groups.

-  Moves a selected Access Group higher on the list.
-  Moves a selected Access Group lower on the list.

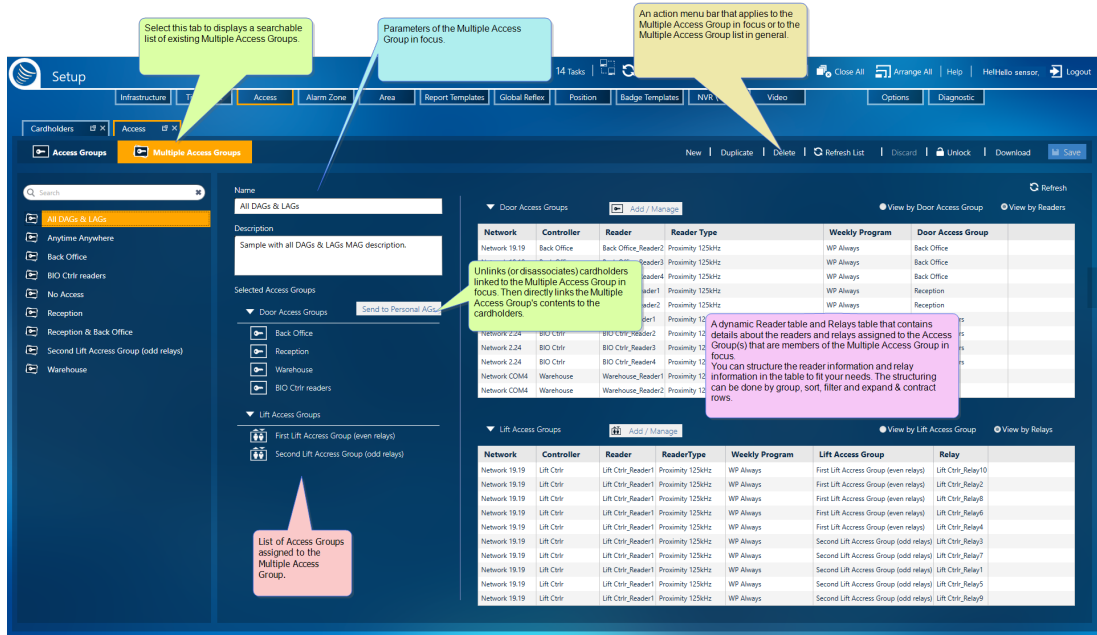


**Note:** **Anytime Anywhere** and **No Access** are built-in Access Groups that cannot be edited. These groups can be assigned to a Multiple Access Group, but because of their pervasive rules, it is a best practice not to place either group at the top of a priority list.

MultiSite impact on **Anytime Anywhere** and **No Access** Access Groups are automatically added when the site is added to the system and cannot be edited. The name of the **Anytime Anywhere** will be prefixed with the name of the site. The **Anytime Anywhere** is automatically deleted after the site is deleted from the infrastructure.

8. After prioritizing the Access Groups assigned to the Multiple Access Group, click **Select**. The assigned Access Groups appear in the **Selected Access Groups** list and the dynamic Readers table and Relays table.
9. Expand the Access Groups in the table to see reader/relay information.

Figure 6-17



- After defining your Multiple Access Group and assigning Access Groups to the Multiple Access Group, do one of the following:
  - Click **Discard**. The unsaved Multiple Access Group is removed.
  - Click **Save**. The new Multiple Access Group is stored in the system database and can be assigned to a cardholder.

**Note:** The **Send to Personal AGs** button does not appear until a Door Access Group or Lift Access Group is added to a new Multiple Access Group

A displayed **Send to Personal AGs** button will be disabled in a new Multiple Access Group until it is assigned to a cardholder.

## Duplicating a Multiple Access Group

Use the following steps to duplicate a Multiple Access Group in the Access screen.

### How to duplicate a Multiple Access Group

- Go to the Setup Task group and click **Access**. The Access screen is displayed.
- On the left side of the action bar, select **Multiple Access Group**. The Access' Multiple Access Group screen is displayed.
- From the list of existing Multiple Access Groups on the left, select the Multiple Access Group that will be duplicated. The Multiple Access Group's parameters and dynamic Readers / Relays tables are displayed.
- From the action bar, click **Duplicate**. A new Multiple Access Group, identical to the Multiple Access Group in focus, is displayed to the right of the list of existing Multiple Access Groups. The only differences between the original and the duplicate are:

- » The duplicate's name is appended with "\_Duplicate" (i.e. a Multiple Access Group named "MAGDay Shift Bld 3" would have a duplicate named "MAGDay Shift Bld 3\_Duplicate").
- » The duplicate has not been saved in the system database.
- » The duplicate has not been assigned to a cardholder.

MultiSite Impact: When clicking **Duplicate**, you may have to choose a site that will own the new Multiple Access Group.

A best practice is to rename the duplicate to something more identifiable.

5. Change the name of the Multiple Access Group.

The name should identify the type of cardholder who would be associated with the Multiple Access Group.

(Optional) Enter a description that provided more information about the group.

The **Selected Access Groups** list is read-only and is initially filled with the Access Groups that are assigned to the original Multiple Access Group. An Access Group may be assigned to more than one Multiple Access Group.

6. Change the **Selected Access Groups** list as follows:





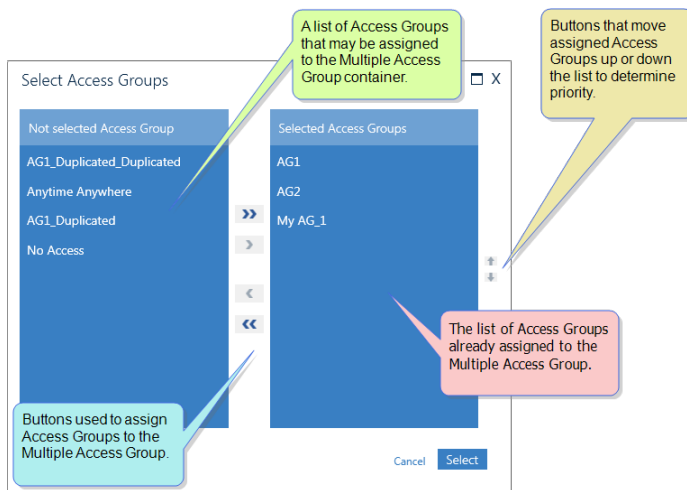
- a. From just above either the Door Access Group table or the Lift Access Group table, click the **Add/Manage** button. A Select Access Group dialog is displayed.
- b. Use the following buttons to assign Access Groups from the list of **Not Selected Access Groups** on the left of the dialog to the Multiple Access Group:
  -  Assigns all of the Access Groups from the **Not Selected Access Groups** list to the Multiple Access Group.
  -  Revokes the assignment of all Access Groups in the Multiple Access Group and returns them to the **Not Selected Access Groups** list.
  -  Assigns selected Access Groups from the **Not Selected Access Groups** list to the Multiple Access Group.
  -  Revokes the assignment of selected Access Groups in the Multiple Access Group and returns them to the **Not Selected Access Groups** list.
- c. After compiling the list of Access Groups that will be assigned to the Multiple Access Group, order the list by priority. The Access Group at the top of the list will have the highest priority and will override any conflicting rules from an Access Group found lower on the list.

Figure 6-18



Use the following buttons to set the priority order of the list of assigned Access Groups.

- ↑ Moves a selected Access Group higher on the list.
- ↓ Moves a selected Access Group lower on the list.

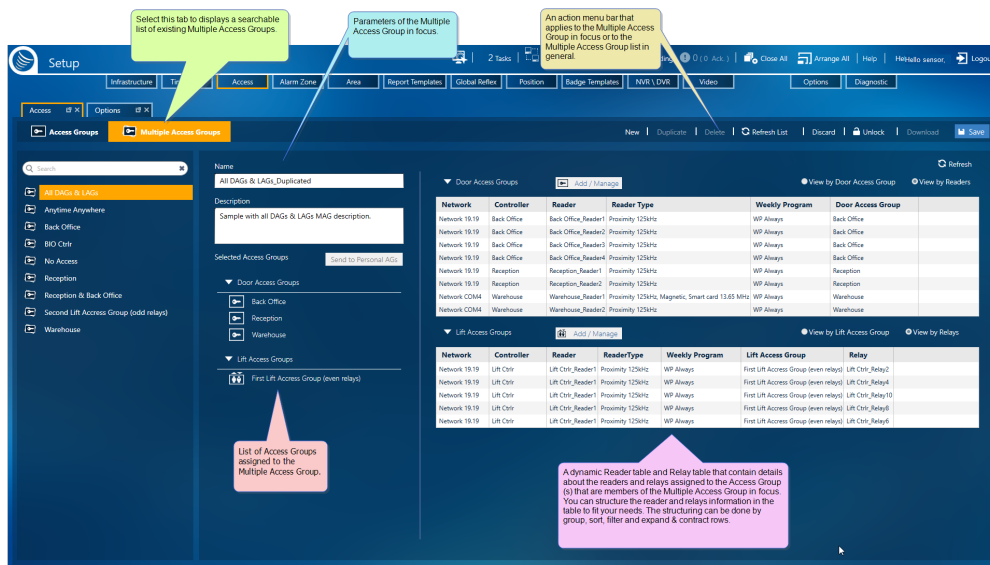


**Note:** **Anytime Anywhere** and **No Access** are built-in Access Groups that cannot be edited. These groups can be assigned to a Multiple Access Group, but because of their pervasive rules, it is a best practice not to place either group at the top of a priority list.

- After prioritizing the Access Groups assigned to the Multiple Access Group, click **Select**. The assigned Access Groups appear in the **Selected Access Groups** list and the dynamic Readers table or Relays table respectively.

Expand the Access Groups in a table to see reader/relay information.

Figure 6-19



- After modifying your duplicate Multiple Access Group and assigning Access Groups, do one of the following:
  - Click **Discard**. The unsaved Multiple Access Group is removed.
  - Click **Save**. The new Multiple Access Group is stored in the system database and can be assigned to a cardholder.

**Note:** The **Send to Personal AGs** button is disabled in a duplicate Multiple Access Group until it is assigned to a cardholder.

## Editing a Multiple Access Group

Use the following steps to edit a Multiple Access Group.

### How to edit a Multiple Access Group

- Go to the Setup Task group and click **Access**. The Access screen is displayed.
- On the left side of the action bar, select **Multiple Access Group**. The Access' Multiple Access Group screen is displayed.
- From the list of existing Multiple Access Groups on the left of the screen, select the Multiple Access Group that will be edited. The Multiple Access Group's parameters and dynamic Readers table and Relays table are displayed.

Figure 6-20

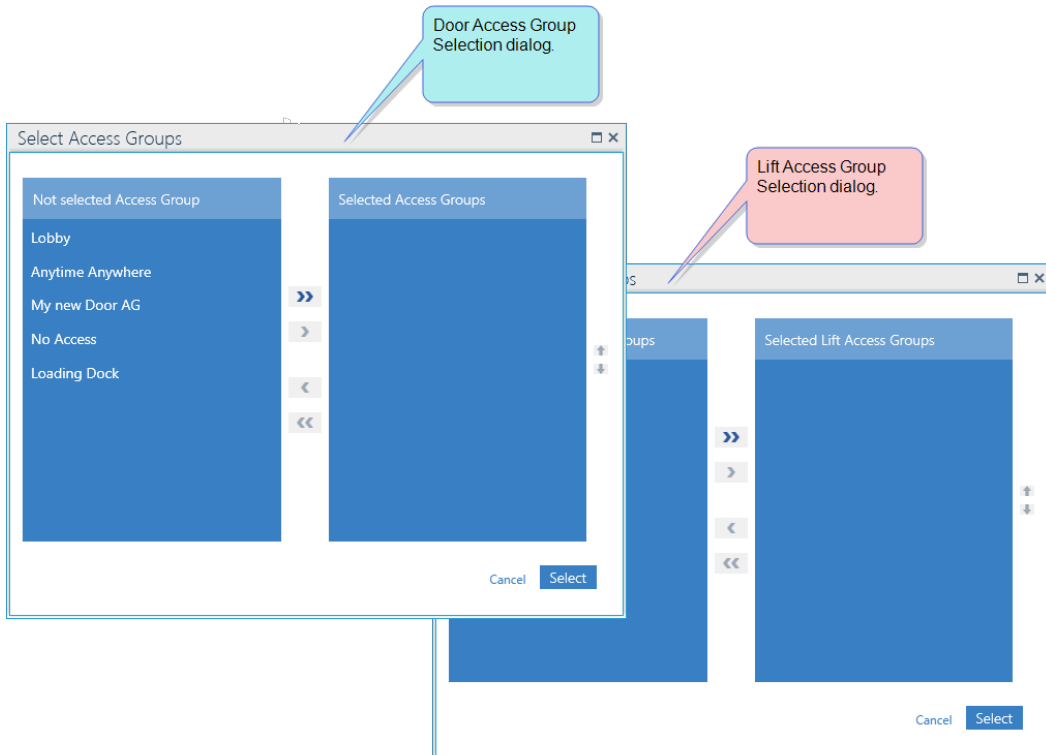
The screenshot shows the 'Setup' interface for 'Access' configuration. The left sidebar contains a search bar and a list of 'All DAGs & LAGs' including 'Anytime Anywhere', 'Back Office', 'BIO Ctrl readers', 'No Access', 'Reception', 'Reception & Back Office', 'Second Lift Access Group (odd relays)', and 'Warehouse'. The main area displays the 'Multiple Access Groups' configuration for a selected group. It includes a 'Name' field, a 'Description' field, and a 'Selected Access Groups' section with a 'Send to Personal AGs' button. Below this are two tables: 'Door Access Groups' and 'Lift Access Groups'. The 'Door Access Groups' table has columns for Network, Controller, Reader, Reader Type, Weekly Program, and Door Access Group. The 'Lift Access Groups' table has columns for Network, Controller, Reader, Reader Type, Weekly Program, Lift Access Group, and Relay. Callout boxes provide additional context for various UI elements.

- Enter a new name for the Multiple Access Group as required. The name should identify the use of the group. (Optional) Enter a description that provided more information about the group.

5. Change the **Selected Access Groups** list as required:

- a. From just above either the Door Access Group table or the Lift Access Group table, click the **Add/Manage** button. A Select Access Group dialog is displayed listing the available Access Groups of the selected Access Group type.

Figure 6-21



- b. Use the following buttons to assign Access Groups from the list of **Not Selected Access Groups** on the left of the dialog to the **Selected Multiple Access Group** list:

**>>** Assigns all of the Access Groups from the **Not Selected Access Groups** list to the **Selected Multiple Access Group** list.

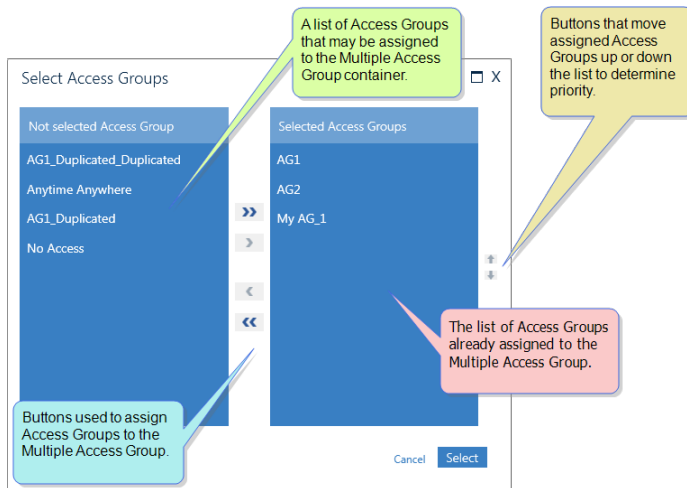
**<<** Revokes the assignment of all Access Groups in the **Selected Multiple Access Group** list and returns them to the **Not Selected Access Groups** list.

**>** Assigns selected Access Groups from the **Not Selected Access Groups** list to the **Selected Multiple Access Group** list.



**<** Revokes the assignment of selected Access Groups in the **Selected Multiple Access Group** list and returns them to the **Not Selected Access Groups** list.


- c. After compiling the list of Access Groups that will be assigned to the Multiple Access Group, order the list by priority. The Access Group at the top of the list will have the highest priority and will override any conflicting rules from an Access Group found lower on the list.

Figure 6-22



Use the following buttons to set the priority order of the list of assigned Access Groups.

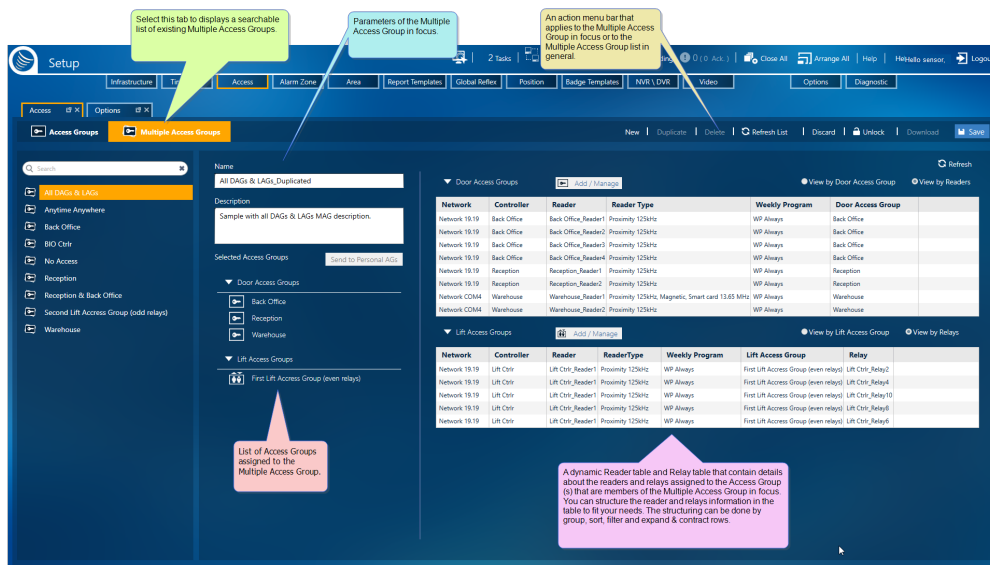
-  Moves a selected Access Group higher on the list.
-  Moves a selected Access Group lower on the list.

 **Note:** **Anytime Anywhere** and **No Access** are built-in Access Groups that cannot be edited. These groups can be assigned to a Multiple Access Group, but because of their pervasive rules, it is a best practice not to place either group at the top of a priority list.

- d. After prioritizing the Access Groups assigned to the Multiple Access Group, click **Select**. The assigned Access Groups appear in the **Selected Access Groups** list and the dynamic Readers / Relays table.

Expand the Access Groups type in the table to see reader and relay information.

Figure 6-23



6. After editing your Multiple Access Group, do one of the following:

- » Click **Discard**. The unsaved Multiple Access Group details and Access Group assignments return to their previously saved values.
- » Click **Save**. The edited Multiple Access Group is stored in the system database and can be assigned to a cardholder.

If the Multiple Access Group was previously assigned to a cardholder, the cardholder's access authorizations update to reflect the changes made in the Multiple Access Group.

Click **Download** to manually download all data related to cardholders assigned to the Multiple Access Group to the relevant controller(s).

**Note:** The **Send to Personal AGs** button is disabled in a Multiple Access Group until it is assigned to a cardholder.

## Deleting a Multiple Access Group

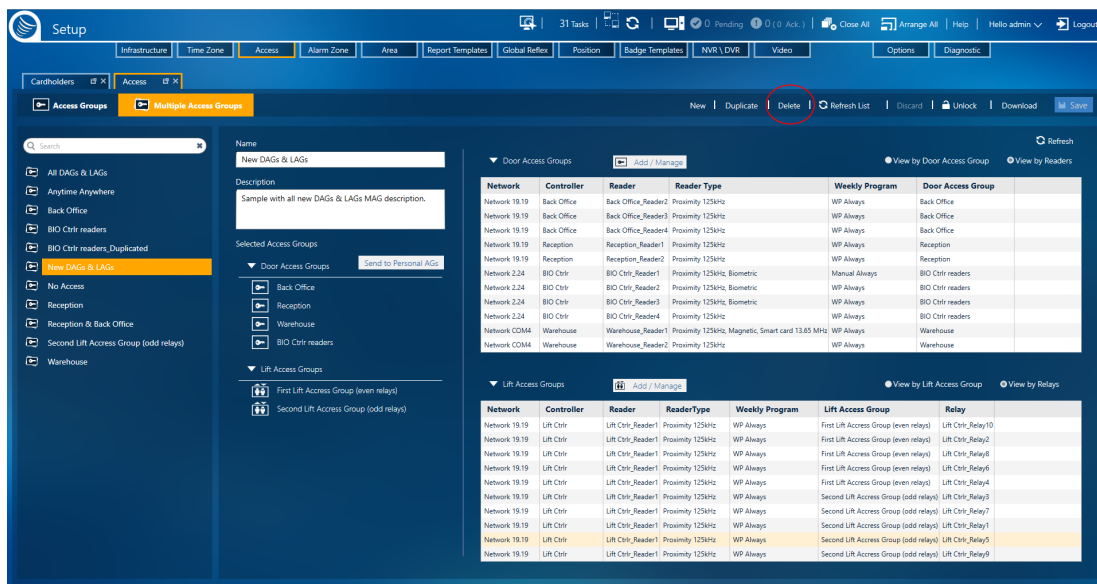
Use the following steps to delete a Multiple Access Group.

### How to delete a Multiple Access Group

A Multiple Access Group cannot be deleted if it is still assigned to a cardholder or department.

1. Go to the Setup Task group and click **Access**. The Access screen is displayed.
2. On the left side of the action bar, select **Multiple Access Group**. The Access' Multiple Access Group screen is displayed.
3. From the list of existing Multiple Access Groups on the left, select the Multiple Access Group that will be deleted. The Multiple Access Group's parameters and dynamic Readers table and Relays table are displayed.

Figure 6-24





4. From the action bar, click **Delete**, and then confirm the operation. The Multiple Access Group is removed from the system and is no longer associated with a cardholder.

The Access Groups that were in the Deleted Multiple Access Group still exist and can be seen in the Access Group screen.



**Note:** The **Anytime Anywhere** and **No Access** Multiple Access Groups are built into the system and cannot be edited or deleted.

MultiSite impact on the **Anytime Anywhere** and **No Access** Multiple Access Groups are automatically added when the site is added to the infrastructure and cannot be edited. However, they are automatically deleted after the site is deleted from the system.

# Temporary Access

## Providing a Cardholder with Temporary Access

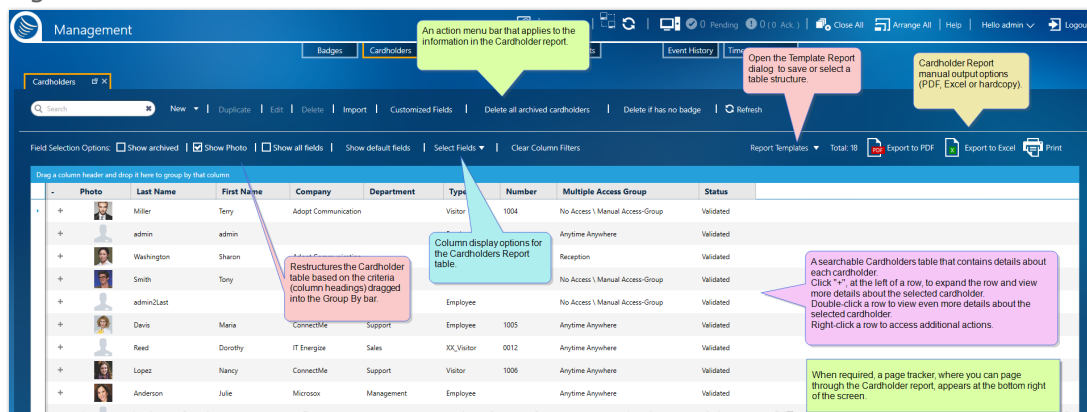
Use the following steps to provide a cardholder with temporary access, via Multiple Access Groups and/or individual readers.

If there is a conflict between a temporary access item and a cardholder's existing Multiple Access Group, Door Access Group or, Lift Access Group, the Temporary Access item will have priority.

## How to provide temporary access to a cardholder

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.

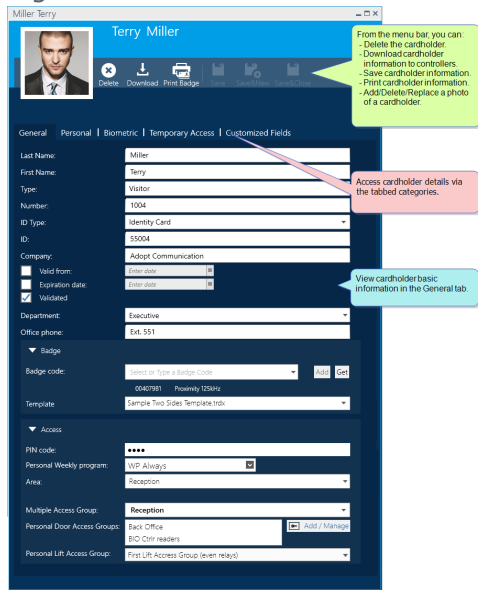
Figure 6-25



2. From the Cardholder Report table, find the cardholder who you will provide temporary access to and do one of the following:
  - » Double-click the cardholder's row.
  - » Expand the cardholders' row and click **Open** in the expanded view.

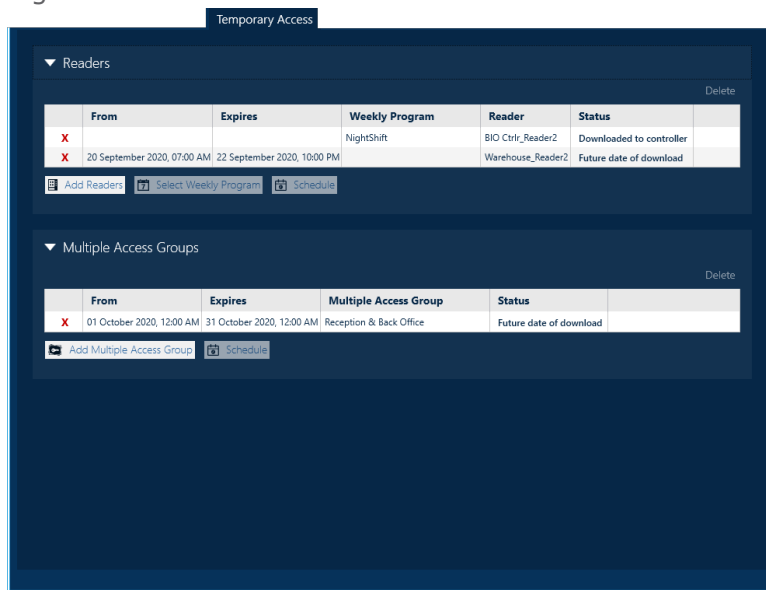
The cardholder's details are displayed.

Figure 6-26



- From the cardholder's details, open the Temporary Access tab. A Reader area and a Multiple Access Group area appear in the tab.

Figure 6-27



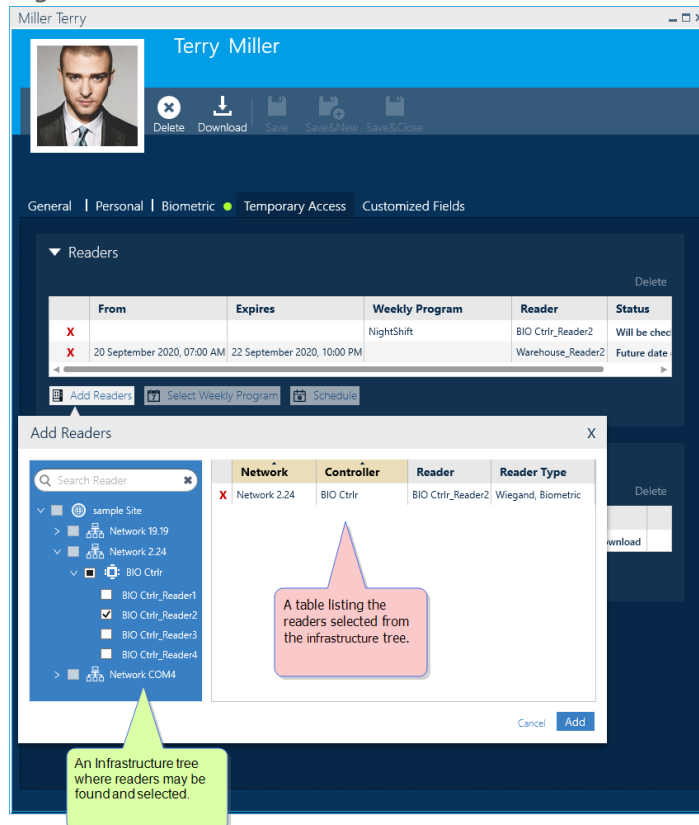
- Decide which temporary assignment type to provide the cardholder with, and then do one of the following:
  - » Temporarily assign a reader to a cardholder
  - » Temporarily assign a Multiple Access Group to a cardholder

# Temporarily assign a reader to a cardholder

A temporarily assigned reader is added to the list of readers where a cardholder may already gain access to a space.

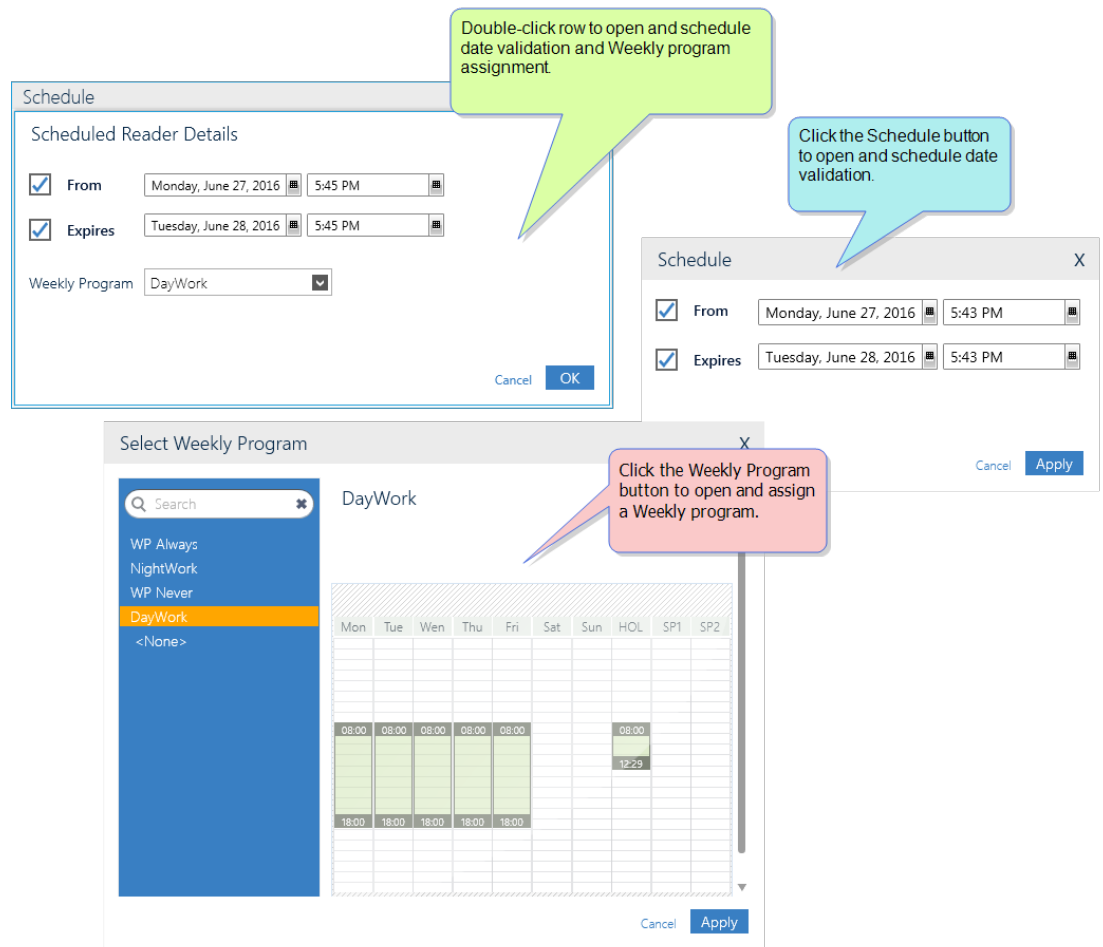
1. Click **Add Readers**. The Add Readers dialog is displayed.

Figure 6-28



2. Expand the tree and select the reader that will be added to the Readers area table
3. Click **Add**. The reader appears in the Readers area table.
4. (Optional) Set a specific Weekly Program for a temporary access instance in focus and/or set a range of time for the temporary access to be valid as follows:
  - a. Double-click a temporary access reader row or click the **Schedule** button. A Schedule Reader Details dialog is displayed.
  - b. Set a date and time when temporary access to the space will be valid (**From** and **Expire**), and then select a Weekly Program from the Select Weekly Program dialog. Alternatively, click **Apply** or **OK** as stated in Step **c** below, and then select a Weekly Program via the **Select Weekly Program** button.

Figure 6-29



- c. Click **Apply** or **OK**. The new parameter settings appear in the Reader area table.
  5. Repeat Step 4 for each reader in the Readers area table as required.
- Alternatively, set the Weekly Program and time range for multiple rows in the Reader area table via a batch process as follows:
- a. Drag your mouse through multiple rows or use the **Ctrl** key and mouse pointer to cherry-pick the rows you want to include in the batch.
  - b. Click the **Select Weekly Program** button above the Reader area table. The Select Weekly Program dialog is displayed.
  - c. Select a Weekly Program, and then click **Apply**. The dialog is closed and the selected Weekly Program appears in each of the rows in focus.
  - d. With the rows still in focus, click **Schedule**. A Schedule dialog is displayed.
  - e. Drag the Apply From and the Apply Expires switches to Yes (green). Select the checkboxes and then choose your dates and times.
  - f. Click **Apply**. The dialog is closed and the values appear in each of the rows in focus.
6. Click one of the **Save** options in the cardholder detail's menu bar. The Status in the reader row will change to **Down Loaded to Controller**.

To delete any of the rows, click the red **x** at the beginning of the row, and then click one of the **Save** options again.



**Note:** If you don't enter a range of time for a reader to be valid, the reader validation will start when the temporary access parameters are saved and there will be no expiration date (open-ended).

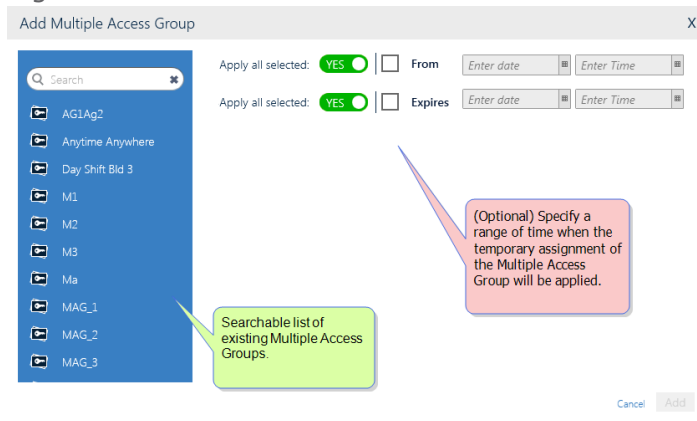
If you don't enter a Weekly Program for a reader, the reader's predefined or default Weekly Program will be used.

## Temporarily assign a Multiple Access Group to a cardholder

This action will temporarily replace a cardholder's previously assigned Multiple Access Group. The rules governing access to spaces via the previously assigned Multiple Access Group will be suspended until the temporary Multiple Access Group is no longer valid.

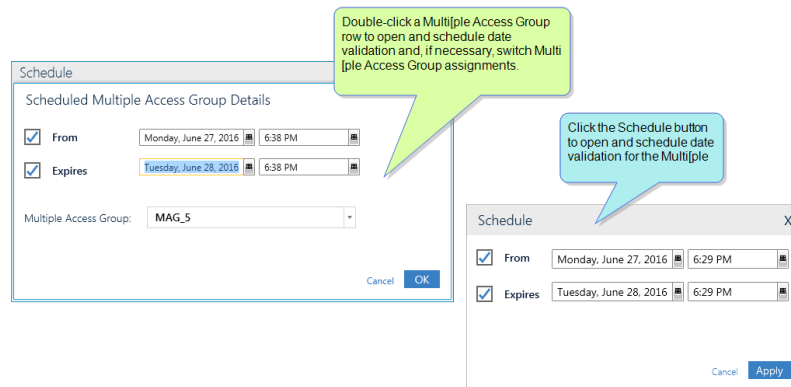
1. Click **Add Multiple Access Group**. The Add Multiple Access Group dialog is displayed.

Figure 6-30



2. Select a Multiple Access Group you want to add to the Multiple Access Group area table. From the same dialog, you can also select the dates when the Multiple Access Group assignment will be valid.
3. Click **Add**. The Multiple Access Group appears in the Multiple Access Group area table.
4. (Optional) Set the dates, or change the dates, when the Multiple Access Group assignment will be valid as follows:
  - a. Double-click a temporary access Multiple Access Group row, or select a row and click **Schedule**. A Schedule dialog is displayed.

Figure 6-31



- b. Set a date and time when the temporary access Multiple Access Group will be valid.
  - c. (Optional) Switch Multiple Access Groups by selecting a different Multiple Access Group from the dialog's drop-down list (only when the row was double-clicked).
  - d. Click **Apply** or **OK**. The new parameter settings appear in the Multiple Access Group area table.
5. Repeat Step 4 for each Multiple Access Group in the area table as required.
  6. Click one of the **Save** options in the cardholder detail's menu bar. The Status in the Multiple Access Group row will change to **Down Loaded to Controller**.

To delete any of the rows, click the red **x** at the beginning of a row, and then click one of the **Save** options again.



**Note:** If you don't enter a range of times for a Multiple Access Group to be valid, the Multiple Access Group validation will start when the temporary access parameters are saved and there will be no expiration date (open-ended).

If a reader has been selected for temporary access, and that reader also exists in a Multiple Access Group that has also been selected for temporary access, the reader settings in the Readers area table have priority.

# Access: MultiSite Impact

When a site is added to the infrastructure, GuardPoint10 will automatically add an **Anytime Anywhere** Access Group and an **Anytime Anywhere** Multiple Access Group for that site. The Anytime Anywhere item names will be prefixed with the name of the site; for example, "Site\_1\_Anytime Anywhere".

If the logged-in user is a super user, they will have the Access Group **Anytime Anywhere**, with no prefix, available. This group will include all readers from all sites in the system.

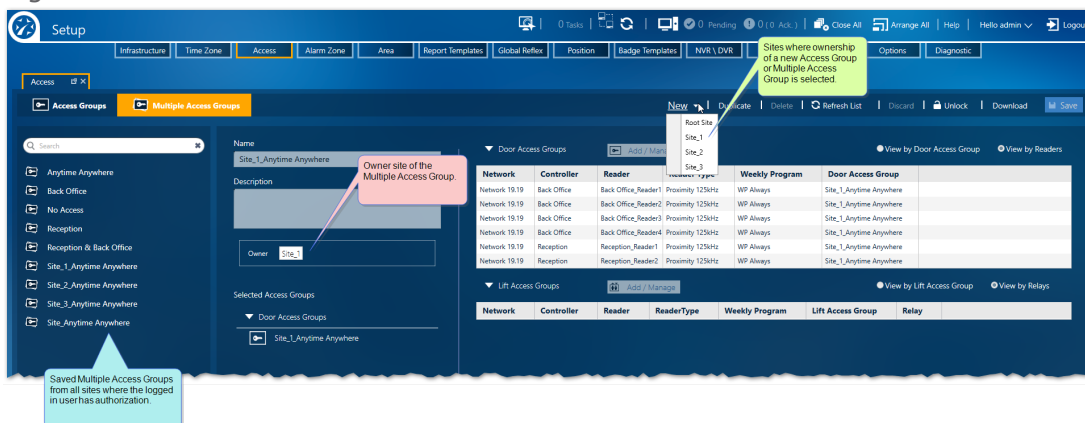
A site's Access Group may include readers owned by another site and shared with the Access Group's site owner. If the reader is later unshared, the reader will be automatically removed from the group where it was shared.

For example, an Access Group owned by Site\_1 can include a reader owned by Site\_2 and shared with Site\_1.

When adding a new Multiple Access Group, you can only include Access Groups owned by the same site as the Multiple Access Group.

The list of saved Access Groups and Multiple Access Groups will display all Access Groups and Multiple Access Groups from sites where the logged-in user has authorization.

Figure 6-32





# CHAPTER 7:

## Badges



The Badge screen adds badges to the system database, manages the status of existing badges, and is one of the access points where a badge may be assigned to a cardholder.

A badge is a physical device that has a unique code by which the system can identify it, by scanning the badge at a reader device. Each badge code must be in the system database. After a badge is added to the database, it can be assigned to a cardholder. During this process, the system assigns a cardholder an *internal system card number*. This number is a cardholder's internal system ID. Generally, the badge code and the internal system card number are unknown to the assigned cardholder.

When a badge is swiped at a reader, the controller to which the reader is attached first checks if the badge is known (i.e. its badge code is in the controller's local database) and if so, to whom it is assigned. This is required to check the access authorization of the cardholder.

The reading technology is defined in the "[Reader Details](#)" on page 453 and badge technology is defined in the "[Badges Screen](#)" on page 597. The badge technology must be the same as the one selected on the controller's electronic board through its **Technology Selection Jumpers**<sup>1</sup>.

---

<sup>1</sup>The WebApp is a limited version of the GuardPoint10 interface. It is available on any device that supports HTML5. To learn how to connect to the module, contact your provider.

Because badge and cardholder tasks are usually bound together, many of the cardholder operations can also be performed via the Badges screen and many of the badge operations can be performed via the Cardholders screen.

**Note:** Where a site uses more than one badge type, a badge with the same code may exist for each technology type.

## Changing the Badges Table View

Because the Badges table can be very large and difficult to manage, two additional view options have been added to the standard group of filters and sorts available in most other GuardPoint10 tables (see "Badges Screen" on page 597). The additional view options are:

- » **View by Status:** The table is grouped by status. There are five statuses:
  - » **In use:** The badge is assigned to a cardholder.
  - » **Free:** The badge is available for assignment.
  - » **Canceled:** The badge is no longer accepted by the system.
  - » **Lost:** The physical badge is unrecoverable and is no longer accepted by the system.
  - » **Stolen:** The physical badge is unrecoverable due to theft and is no longer accepted by the system.

## How to change the Badges Table View

1. Go to the Management Task group and click **Badges**. The Badges screen is displayed.
2. From the action bar, select the **View by Status** checkbox. The table changes and is now grouped by status.

Figure 7-1

Badge code	Type	Status	Cardholder	Description
Free				
002222000222	Wiegand	Free		
In Use				
Canceled				
5971A829	Wiegand	Canceled	Thompson Adam	
Lost				
FCD390A0	Wiegand	Lost	Flores Deborah	
Stolen				
2A573008	Wiegand	Stolen	Martinez Benjamin	
357BEDFF	Wiegand	Stolen	Richardson Angela	
16ECF584	Wiegand	Stolen	Jones Ashley	

In the screen example above, the In Use group is collapsed and only the group title is visible.

If there were no stolen badges in the database, the Stolen group would not appear in the **View by Status** display.

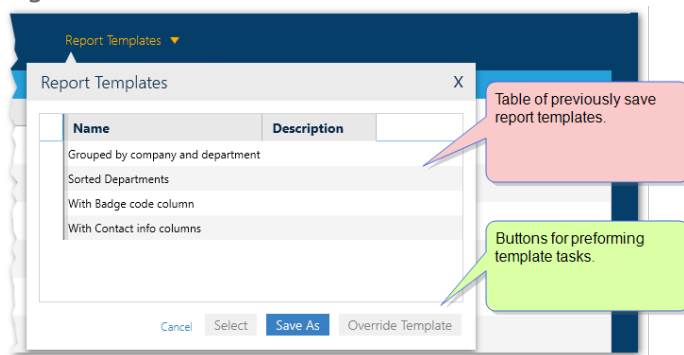
# Manage the Badges Table Layout with Templates

## Report Template dialog

The structure of the screen table can be saved in a template so it can be applied later, either to the screen display or a global reflex "[Create Template-based report](#)" on [page 548](#) action. The data in a template is dynamic and will change to reflect the environment.

To start using templates click the **Report Templates** button.

Figure 7-2



The table in the Report Template dialog contains the names and descriptions of previously save templates, which are specific to the screen displayed.

From the screen's Report Template dialog you can click:

- » **Save As:** Opens the "[Report Template Screen](#)" on [page 529](#), where the current structure of the displayed table can be saved.
- » **Override:** Opens the "[Report Template Screen](#)" on [page 529](#), where the current structure of the displayed table can override the last selected template with the current structure of the displayed table.
- » **Select:** Displays current data in the template selected from the dialog's table.

# Adding New Badges

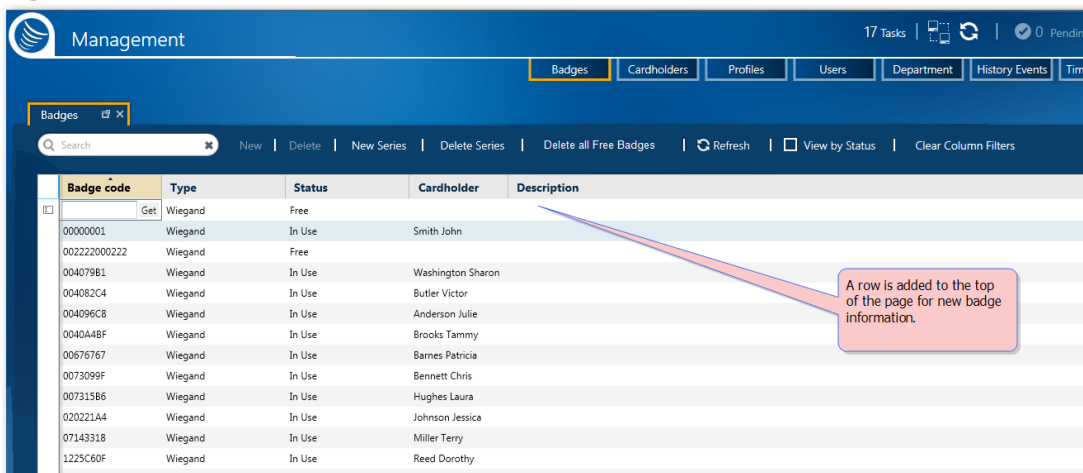
Use the following steps to create a new badge via the Badges screen.

**Note:** A badge may be added and assigned through cardholder management or through the Badges screen. For information about badge options via cardholder management, see ["Cardholders"](#) on page 193.

## How to add new badges

1. Go to the Management Task group and click **Badges**. The Badges screen is displayed.
2. From the action bar, click **New**. A new row is added to the top of the Badges table, where information about the new badge is entered.

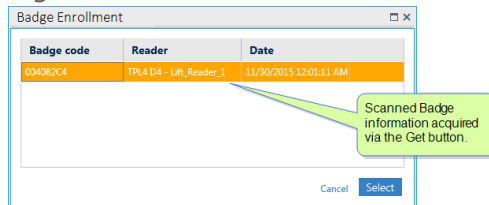
Figure 7-3



Badge code	Type	Status	Cardholder	Description
00000001	Wiegand	Free		
002222000222	Wiegand	Free		
004079B1	Wiegand	In Use	Washington Sharon	
004082C4	Wiegand	In Use	Butler Victor	
004096C8	Wiegand	In Use	Anderson Julie	
0040A4BF	Wiegand	In Use	Brooks Tammy	
00676767	Wiegand	In Use	Barnes Patricia	
0073099F	Wiegand	In Use	Bennett Chris	
007315B6	Wiegand	In Use	Hughes Laura	
020221A4	Wiegand	In Use	Johnson Jessica	
07143318	Wiegand	In Use	Miller Terry	
1225C60F	Wiegand	In Use	Reed Dorothy	

3. Enter new badge information in the parameter fields. The parameters are as follows:
  - » **Badge Code:** Code attached to a badge. The code may be expressed in decimal or hexadecimal values. Where applicable, leading zeros will be entered automatically to the default code length. If the badge code is not known, use the **Get** button alongside the field.The **Get** button allows you to acquire one or more badge codes via a reader device scan.
  - a. Click **Get**. The Badge Enrollment dialog is displayed.

Figure 7-4



Badge code	Reader	Date
004082C4	TPL4 D4 - Lift_Reader_1	11/30/2015 12:01:31 AM

- b. Scan the new badge(s) at a reader. The badge information, including the badge code, appears in the dialog.

If a scanned badge does not have a status of **Free**, the badge information will not appear in the dialog.

- c. Place a badge code in focus, and then click **Select**. The Badge Enrollment dialog is closed and the badge code appears in the **Badge Code** field.

Alternatively, in the Badge Enrollment dialog, place multiple badge rows in focus and click **Select**. The dialog closes, and a new row is added to the Badges table for each new badge code. The badge codes appear in a new row's **Badge Code** field.



**Note:** The new badge code must be entered before you can proceed to the next field. Otherwise, the New Badge operation will stop.

- » **Type:** Technology of a badge. The default badge type is defined in the Options screen's, General tab, in the **Default Badge Technology** parameter. To select a different technology type, click on the field and select a new type from the drop-down list.
- » **Status:** A Badge has one of the following statuses:
  - » **Free:** Available until the badge is allocated to a cardholder or is given another status.
  - » **In Use:** Badge is assigned to a cardholder.
  - » **Canceled:** Automatically invalidates the badge, but the badge still exists in the system. If someone attempts to use a canceled badge, the Event Table Log will document the attempt and security personnel may take action based on a predefined protocol.
  - » **Lost:** Automatically invalidates the badge, but the badge still exists in the system. If someone attempts to use a lost badge, the Event Table Log will document the attempt and security personnel may take action based on a predefined protocol.
  - » **Stolen:** Automatically invalidates the badge, but the badge still exists in the system. If someone attempts to use a stolen badge, the Event Table Log will document the attempt and security personnel may take action based on a predefined protocol.
- » **Owner:** (Optional) The name of the cardholder assigned to the badge. A badge can exist in the system without an owner.
- » **Description:** (Optional) A free text field that describes the badge; this may include how it is used and the type of cardholder who would be assigned the badge. For example, a range of badges may be designated only for visitors, another range only for freelancers, etc. This information would be added to the badge's description.

4. Click **Save**. The badge appears in the Badges table and is added to the system database.

# Adding Multiple Badges where the Badge Code is Sequential

Use the following steps to create a series of badges with sequential badge codes.

**Note:** A badge may be assigned through cardholder management or through the Badges screen. For more information about badge options in cardholder management, see ["Cardholders" on page 193](#).

## How to create a series of new badges

1. Go to the Management Task group and click **Badges**. The Badges screen is displayed.
2. From the action bar, click **New Series**. The Create Series of Badges dialog is displayed.

Figure 7-5

The screenshot shows a 'New Badge Group' dialog box with the following fields and options:

- First badge code: 00000010
- Quantity: 20
- Type: Wiegand
- Position to increment: 8
- Create also cardholders: YES (selected)
- Select Multiple Access Group: Anytime Anywhere (selected)
- Set parameters as: Select Cardholder

Callout boxes indicate that the top section contains 'Badge series specific information' and the bottom section contains '(Optional) Cardholder and assignment information'.

There are two parts to the Create Series of Badges dialog:

- » The **badge series information**
- » The **optional cardholder information**

3. Enter new badge series information in the parameters at the top of the dialog. The parameters are as follows:

- » **First Badge Code:** The code attached to the first badge in the series.

The code may be expressed in decimal or hexadecimal values. Where applicable, leading zeros will be entered automatically to the default length of the code.

- » **Quantity:** The number of badges in the series.

If an existing badge has a code that falls within the code series you are creating, GuardPoint10 will notify you that a badge with the code already exists and skips the code during the badge generation process (after you click **OK** in the dialog).

### For example:

You are creating a series of 10 badges, where the first badge has the code 01 and where a badge with the code 05 already exists in the system database. The end result will be badge codes 01 - 04, skip 05 because it's already in the database, and continue with badge codes 06 - 11 to complete the series of 10 badges.



**Note:** Two badges can have the same badge code as long as the badges use different technology types.



**Note:** If a previously deleted badge had a code that fell within the code series you are creating, the code still exists in the system database and will be skipped during the badge generation process.

- » **Type:** Technology of the badges in the series. If you want to enter a type other than the default type that appears in the field, click the field and select a different type from the drop-down list.
- » **Position to increment:** Determines which digit in the code will be incremented during the badge code generation process.

### For example:

You are creating a series of 5 badges, where the first badge code is set to 00000800 and the **Position to increment** value is set to 7. The end result are badges with the following codes:

00000810  
00000820  
00000830  
00000840  
00000850

Because the 7th digit from the left is set to increment (the previous code number +1).

4. (Optional) If you want to create the same number of cardholders as badges, where the cardholder's last name is the same as the badge code:
  - a. Drag the button for **Also create cardholders** to Yes (green).
  - b. Select a Multiple Access Group for the cardholders by doing one of the following:
    - » Select the button for **Select Multiple Access Group for basic parameters**, and then choose a Multiple Access Group from the drop-down list. The **No Access** Multiple Access Group is chosen by default.
    - » Select the button for **Set parameters as**, and then click **Select Cardholder**. A Select Cardholder dialog is displayed.

Figure 7-6

The screenshot shows a 'Select Cardholder' dialog box with a search bar and a table of cardholders. The table has columns for Photo, Last Name, First Name, Company, Department, Type, and Number. Callouts explain that the search bar and column headings can be used to narrow the view, and that the table includes filter and sort options.

Photo	Last Name	First Name	Company	Department	Type	Number
	admin	admin			Employee	
	Anderson	Julie	Microsox	Management	Visitor	
	Butler	Victor	ConnectMe	Sales	Employee	1003
	Davis	Maria	ConnectMe	Support	Visitor	1005
	ITguy	ITguy			Employee	
	John	Johnsom			Freelancer	
	Lee	Judith	IT Energize	Management	Employee	
	Lopez	Nancy	ConnectMe	Support	Employee	1006
	Miller	Terry	Adopt Communication	Executive	Employee	1004
	Smith	Tony		Executive	Employee	1007

Select the cardholder whose Multiple Access Group assignment you would like to assign to the new cardholders that will be created during the badge code generation process.

c. Click **Select**. The Select Cardholder dialog is closed and the selected cardholder's last name appears under the **Select Cardholder** button.

5. Click **OK** in the Create Series of Badges dialog. The badges and (if selected) cardholders are generated and added to the system database and the respective tables.

**Note:** When creating a series of badge codes with cardholders, besides the badge codes and cardholder last names matching, the badge is automatically assigned to the corresponding cardholder.

## Assigning a Badge to an Existing Cardholder from the Badges Screen

Use the following steps to assign a badge to an existing cardholder.

**Note:** A badge may be assigned to an existing cardholder through the Badges screen or through cardholder management. For more information about badge options in cardholder management, see "[Cardholders](#)" on page 193.

### How to assign a badge to an existing cardholder

1. Go to the Management Task group and click **Badges**. The Badges screen is displayed.
2. From the Badges table, select the row that contains the badge information that will be assigned to a cardholder. The badge status must be set to **Free**.



To change the status of a badge, right-click on the Status field and select the relevant context menu command.


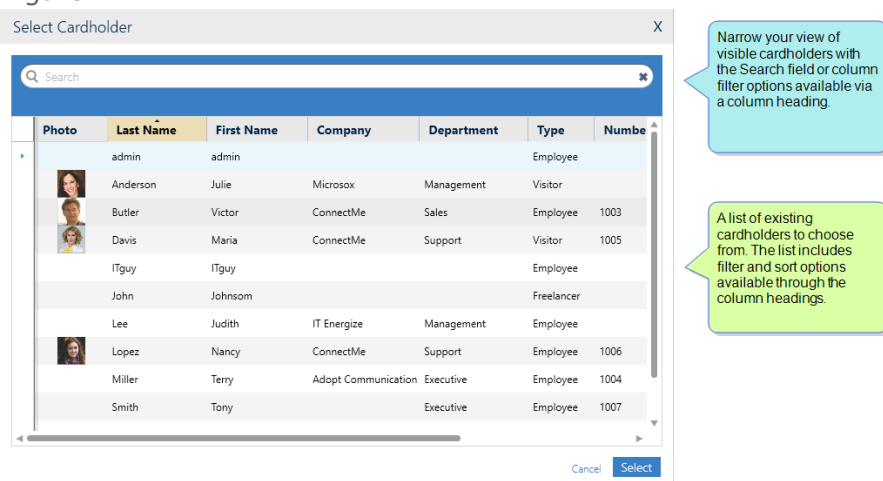
3. After putting a badge row, with a **Free** status, in focus, do one of the following:
  - » Right-click on the Free status cell, and then select **Attach to Cardholder** from the context menu. A Select Cardholder dialog is displayed.
  - » Double-click on the Cardholder cell, and then click the three ellipses . A Select Cardholder dialog is displayed.

Figure 7-7




The Select Cardholder dialog will only list the cardholders who are available for badge assignment (i.e. not archived cardholders).

4. Select the cardholder who will be assigned the badge in focus.
5. After selecting a cardholder, click **Select**. The Select Cardholder dialog is closed. The selected cardholder's name appears in the Cardholder cell of the badge in focus and the status of the badge is changed from **Free** to **In Use**. In addition, the badge assignment is automatically added to the system database.

## Assigning a Badge to a New Cardholder

Use the following steps to assign a badge to a new cardholder. This process allows you to add a cardholder to the system database and assign the cardholder a badge at the same time via the Badges screen.

 **Note:** A badge may be assigned to a new cardholder through the Badges screen or through cardholder management. For more information about badge options in cardholder management, see "Cardholders" on page 193.

# How to assign a badge to a new cardholder

1. Go to the Management Task group and click **Badges**. The Badges screen is displayed.
2. From the Badges table, select the row that contains the badge that will be assigned to a cardholder. The badge status must be set to **Free**.

To change the status of a badge, right-click on the Status cell and select the relevant context menu command.

3. After putting a badge row, with a Free status, in focus, right-click on the row, and then select **Attach to new Cardholder**. New cardholder details, with a minimum of default values, are displayed with the badge code already assigned.

Figure 7-8



4. Enter new cardholder detail information in the parameter fields. For information about the cardholder details fields, see "[Operator \(User\): MultiSite Impact Cardholder Details](#)" on page 607.
5. After entering all of the relevant information, in the action bar, click **Save & Close**. The following happens:
  - » The cardholder detail information is saved in the system database.
  - » The cardholder details are closed.
  - » The cardholder's name appears in the **Cardholders** cell of the Badges table.
  - » The new cardholder appears on the Cardholders screen.



**Note:** To make changes to the cardholder's details after you click **Save & Close**, use cardholder management (see "[Cardholders](#)" on page 193).

## Changing the Status of a Badge

### How to change the status of a badge

1. Go to the Management Task group and click **Badges**. The Badges screen is displayed.
2. Right-click on the badge the will change statuses.
3. Click **Change Status** and then choose a new status (**Free**, **Lost**, **Stolen**, or **Canceled**).

If a badge has a status of **Lost**, **Stolen**, or **Canceled**, The operator can detach the cardholder from the badge via the badge's context menu item **Change Status**.

# Manually Assigning a Cardholder a Badge Template via the Badges Screen

Use the following steps to override a Type's default template assignment for an individual cardholder via the Badges screen. The template determines the layout and cardholder details that will appear on a cardholder's printed badge.

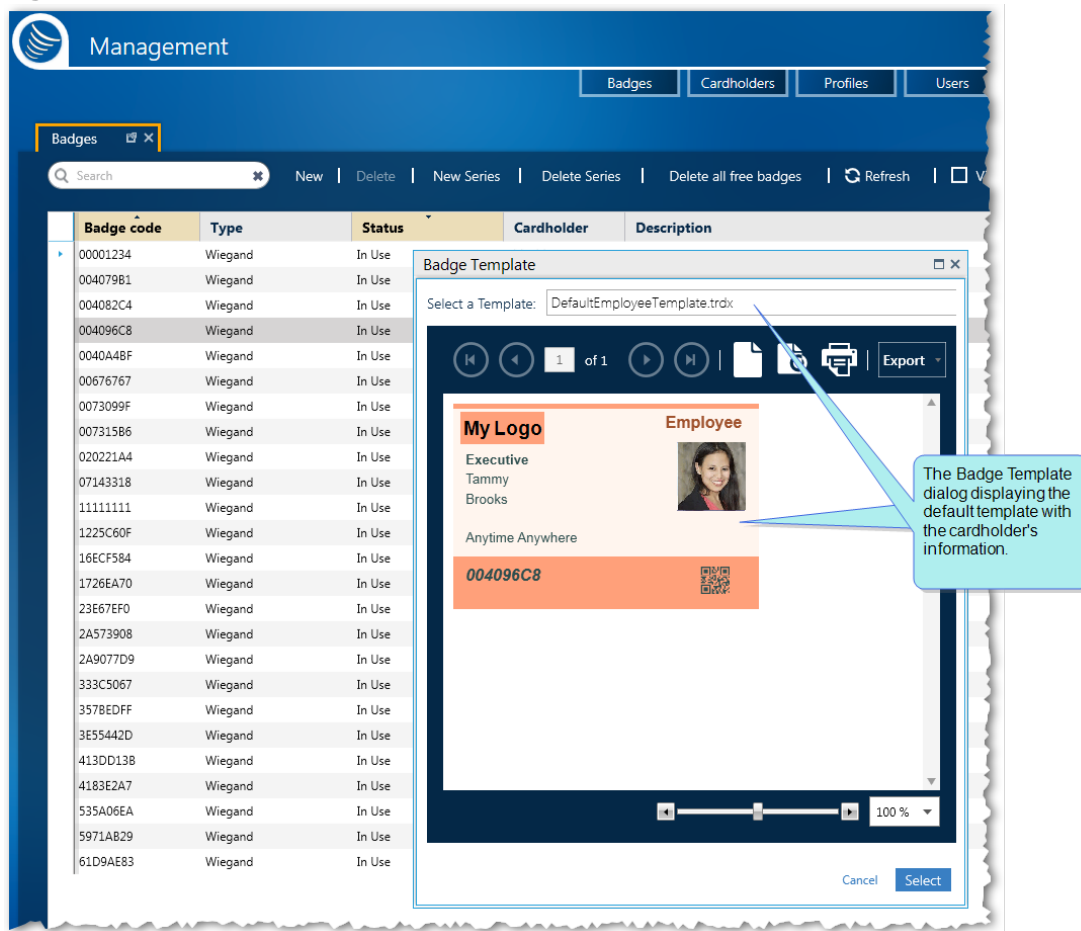


**Note:** These instructions are only relevant for GuardPoint10 installations that include the Badge Template module. For information about the Badge Template module, see "[Badge Templates](#)" on [page 293](#).

## How to assign a badge template to an individual cardholder (regardless of the cardholder Type) via the Badges screen

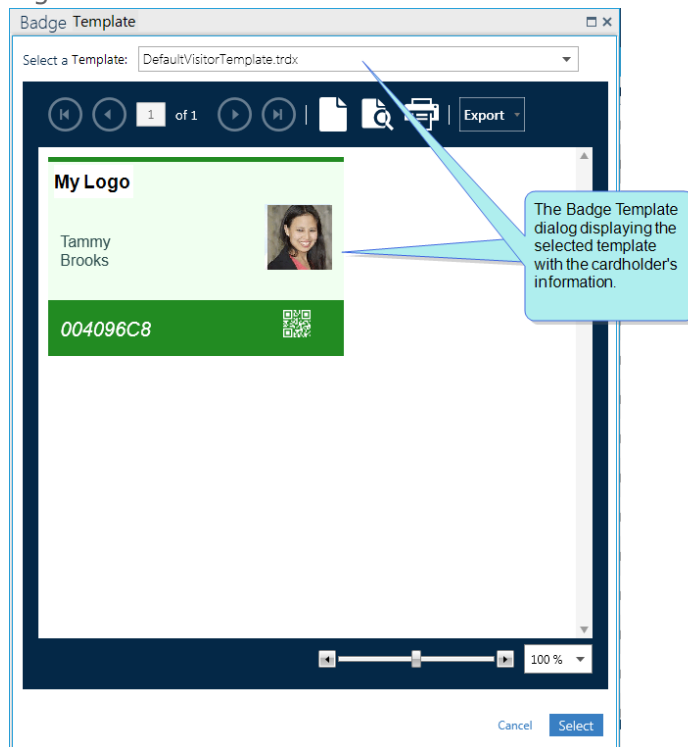
1. Go to the Management Task group and click **Badges**. The Badges screen is displayed.
2. In the Badges table, right-click on the badge row's Cardholder column where you are going to change the cardholders template assignment. A context menu appears.
3. In the context menu click **Print Badge**. The Badge Template dialog is displayed with the cardholder's badge appearing in the currently assigned template.

Figure 7-9



4. From the **Select Template** drop-down list, select the template that will replace the currently assigned template. The cardholder's badge appears in the dialog with the new template layout.

Figure 7-10



For more information about the template dialog, see ["Badge Templates Screen"](#) on page 564.

5. After selecting the new template, click **Select**. The dialog is closed and the name of the new template appears in the Cardholders screen's Template column.

The cardholder's badge template assignment will be retained regardless of any changes made to the Type assignment or the default template of the cardholder's Type.

# Printing a Cardholder Badge via the Badges Screen

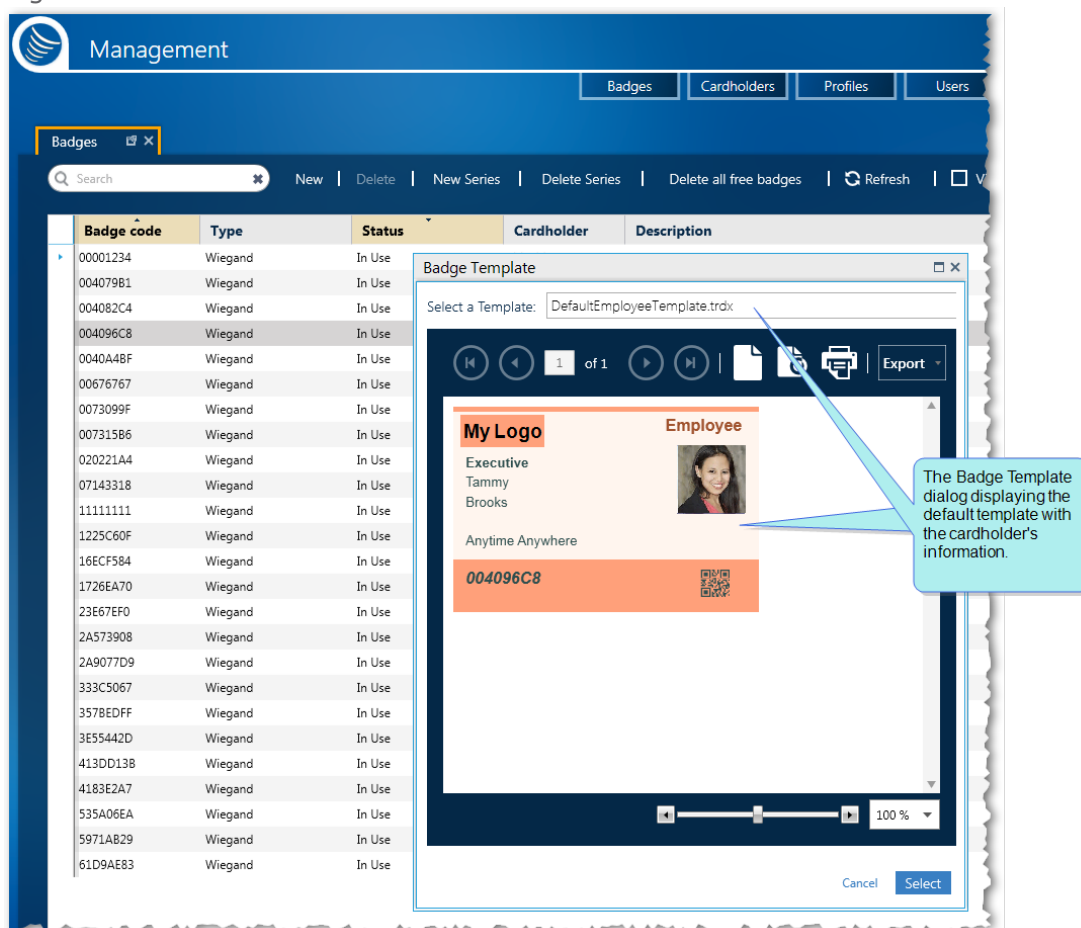
A badge can be printed from the Badges screen and the Cardholders screen. Use the following steps to print a cardholder's badge via the Badges screen.

**Note:** These instructions are only relevant for GuardPoint10 installations that include the Badge Template module. For information about the Badge Template module, see "[Badge Templates](#)" on page 293.

## How to print a badge via the Badges screen

1. Go to the Management Task group and click **Badges**. The Badges screen is displayed.
2. In the Badges table, choose the cardholder whose badge will be printed and right-click on the badge row's Cardholder column. A context menu appears.
3. In the context menu click **Print Badge**. The Badge Template dialog is displayed with the cardholder's badge in view.

Figure 7-11



- From the Badge Template dialog toolbar, click the printer icon. The Windows Print dialog is displayed.
- Complete the Print dialog and click **Print**. The Badge is printed on the designated printer.

## Deleting a Badge

When you delete a badge, it's erased from the system database. After being deleted, the badge information may only be recovered from a third-party backup solution.

You can only delete badges that have a **Free** status.

### How to delete selected badges

- Go to the Management Task group and click **Badges**. The Badges screen is displayed.
- Select the rows of one or more badges that will be deleted.  
To select multiple rows, either drag the mouse over through the rows or press **Ctrl** and click on each row.
- From the action bar, select **Delete**, and then confirm the operation. All of the selected badges are deleted from the system database.

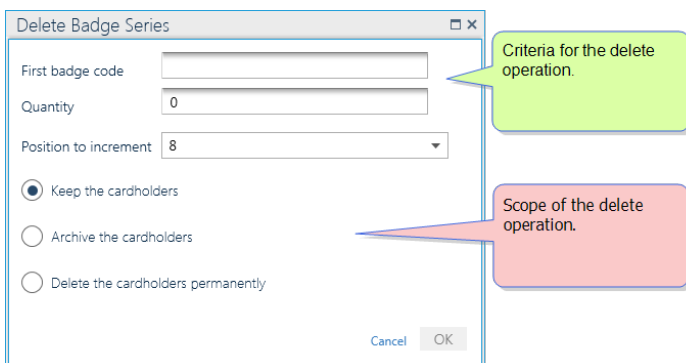
### How to delete all free badges

- Go to the Management Task group and click **Badges**. The Badges screen is displayed.
- From the action bar, select **Delete All Free Badges**, and then confirm the operation. All free badges are deleted from the system database.

### How to delete a range of badges with sequenced badge codes (badge series)

When deleting a series of badges, the status of the badges must be **Free**. If a badge in the specified series is set to something other than **Free**, it will not be deleted during the Delete Series operation.

- Go to the Management Task group and click **Badges**. The Badges screen is displayed.
- From the action bar, click **Delete Series**. The Delete Series of Badges dialog is displayed.



There are two parts to the Delete Series of Badges dialog:



» the **badge criteria information**

» the **delete scope information**

3. Enter badge series information in the parameters at the top of the dialog. The parameters are as follows:

» **First Badge Code:** The code attached to the first badge in the series.

The code may be expressed in decimal or hexadecimal values.

» **Quantity:** The number of badges in the series.

» **Increment position:** Determines which digit in the code will be incremented during the badge code deletion process.

#### For example:

You are deleting a series of 5 badges, where the first badge code is set to 00000800 and the **Increment position** value is set to 7. The end result will be that the badges with the following codes are deleted:

00000810

00000820

00000830

00000840

00000850

Because the 7th digit from the left is set to increment (the previous code number +1).

4. (Optional) Set the scope of the deletion process. The scope options are as follows:

5. **Keep the cardholders:** When selected, cardholders assigned a badge in the selected series will remain in the system database, but without a badge assignment.

**Archive the cardholders:** When selected, cardholders assigned a badge in the selected series will be archived during the Delete Series operation.

**Delete the Cardholder Permanently:** When selected, cardholders assigned a badge in the selected series will be deleted from the system database during the Delete Series operation.

6. After setting the criteria and scope, click **OK**. The badges are deleted, and their assigned cardholders, are Archived / Deleted / Unassigned, depending on the scope selected.



**Note:** After deleting a series of badges and possibly cardholders, you will not be able to undelete them later, unless they are recovered via a third-party backup solution.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 8:

## Cardholders



A cardholder is an individual, registered in the system database, as a person who may be assigned a badge and badge code.

Managing cardholders is one of the main purposes of the system. Through cardholder management, an operator may do the following:

- » Define cardholder's personal information (Name, Address, photos, vehicle license plate number, etc.).
- » Define where, when, and how a cardholder may access a space monitored by the system.

All of this information is recorded via the Cardholders screen.

A cardholder's unique identification is a combination of a cardholder's first name last name and internal system identification number.

Cardholder authorizations linked to access points are downloaded to the controllers that manage these access points.

When a reader device scans a badge, the controller to which the reader is attached uses the badge code to search its local database to find the cardholder's access information. Using this information and the authorizations of this cardholder (time zones, cardholder parameters, etc.), the controller determines whether to grant or deny the access request. Because all of the data used to make a determination is stored locally in the controller, the determination is performed immediately.

Once a request has been granted or denied, the controller stores this as a transaction in its **Event Buffer**<sup>1</sup>, which will be read by the system.

If the scanned badge code is not found in the controller's local database, the controller records an **unknown badge** transaction and checks the system database for relevant information about the badge.

## Changing Cardholder Report Table View

The Cardholder table is treated as a report and is therefore referred to as the Cardholder Report table. Because the Cardholder Report table can be very large and difficult to manage, additional view options have been added to the standard group of filters and sorts available in most other GuardPoint10 tables. For more information, see ["Cardholders Screen" on page 600](#).

After making a Cardholder Report table view, the view can be saved as a Report template. For information about Report templates, see ["Handling Report Template" on page 322](#) and ["Manage the Cardholder Table Layout with Templates" on page 196](#).

The additional view options are as follows:

- » **Show Archived:** When selected, cardholders that were previously archived are visible in the Cardholder Report table.



**Note:** An archived cardholder is frozen and cannot be assigned a badge or granted authorizations. However, an archived cardholder is still in the system database and may be restored at any time.

- » **Show Photo:** When selected, a Photo column is added to the cardholder table. The column contains a photo of each cardholder in their respective rows.  
If a cardholder doesn't have a photo in the system database, an avatar is displayed as a placeholder.
- » **Show Report Default Fields:** When selected, the columns most commonly exported in the Cardholder Report table are shown.
- » **Show All Fields:** When selected, all available columns are shown in the Cardholder Report table.
- » **Show Default Fields:** When selected, the columns most commonly displayed in the Cardholder Report table are shown.
- » **Select Fields:** When selected, a drop-down list of available columns is displayed. By selecting a column's checkbox in the list, you can cherry-pick the columns that will be shown in the Cardholder Report table. If Custom Fields exist, the columns linked to the fields will be listed.

## How to change the Cardholder Report Table View

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. From the Field Selection Options row, just above the report table, select any of the view options described above. The report table changes appearance according to the selection. The image below illustrates just one of the possible view options.

---

<sup>1</sup>A temporary storage area in a controller. The buffer contains system events involving entities attached to the controller. An Event buffer is read and cleared by the system during polling (a query as to whether a controller has any data to transmit).

Figure 8-1

The screenshot displays the 'Management' interface for 'Cardholders'. At the top, there are navigation tabs: Badges, Cardholders (selected), Profiles, Users, Department, History Events, and Time & Attendance. Below the tabs, there are search and action buttons: Search, New, Duplicate, Edit, Delete, Import, Delete all archived cardholders, Delete if has no badge, and Refresh. A 'Field Selection Options' bar includes checkboxes for 'Show archived', 'Show Photo', 'Show report default fields', 'Show all fields', and 'Show default fields', along with a 'Select Fields' dropdown. The main area is a table of cardholders. A 'Select Fields' dropdown menu is open over the table, listing fields with checkboxes: Photo, Last Name, First Name, Company, Department, Type, Number, Badge code, Photo, Last Name, First Name, Company, Department, Type, Number, Multiple Access Group, Status, From Date, Expire Date, Temporal, Last pass reader, Last pass date, Badge code, and Car license plate. The table below has columns: Photo, Last Name, First Name, Company, Department, Type, Number, and Badge code. The data rows include cardholders like Jones, Brooks, Barnes, Thompson, Reed, sensor, Rogers, Washington, Taylor, Bennett, Gray, White, Johnson, Smith, Cooper, and Price.

Photo	Last Name	First Name	Company	Department	Type	Number	Badge code
	Jones	Ashley	IT Energize	Development	Visitor		166CF384
	Brooks	Tammy		Executive	Employee	12345	004096C8
	Barnes	Patricia	IT Energize	Support	Employee	12350	00076767
	Thompson	Adam	FL5	Development	Employee		5971A829
	Reed	Dorothy	Microsox	Marketing	Visitor		1225C60F
	sensor	sensor			Employee		
	Rogers	Martin	IT Energize	Support	Employee		CD3C6026
	Washington	Sharon	Microsox	Support	Employee	AG1Ag2	004079E1
	Taylor	Donna	Adopt Communication	Marketing	Visitor	MA0_3	9205A033
	Bennett	Chris		Development	Employee	12349	Anytime Anywhere
	Gray	Anne	Adopt Communication	Development	Employee	AG1Ag2	23657EFD
	White	Kenneth	Adopt Communication	Admin	Employee	AG1Ag2	248077D9
	Johnson	Jessica	Microsox	Marketing	Employee	MA0_4	020221A4
	Smith	John	ConnectMe	Management	Employee	AG1Ag2	11111111
	Cooper	Joshua	FL5	Management	Visitor	12347	MA0_3
	Price	Julia	Adopt Communication	Management	Employee	AG1Ag2	4188E207

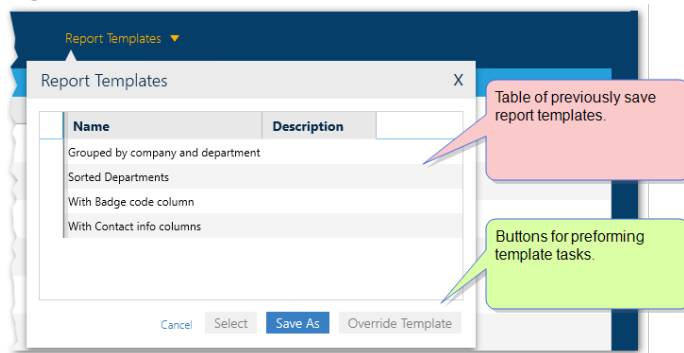
# Manage the Cardholder Table Layout with Templates

## Report Template dialog

The structure of the screen table can be saved in a template so it can be applied later, either to the screen display or a global reflex "[Create Template-based report](#)" on page 548 action. The data in a template is dynamic and will change to reflect the environment.

To start using templates click the **Report Templates** button.

Figure 8-2



The table in the Report Template dialog contains the names and descriptions of previously save templates, which are specific to the screen displayed.

From the screen's Report Template dialog you can click:

- » **Save As:** Opens the "[Report Template Screen](#)" on page 529, where the current structure of the displayed table can be saved.
- » **Override:** Opens the "[Report Template Screen](#)" on page 529, where the current structure of the displayed table can override the last selected template with the current structure of the displayed table.
- » **Select:** Displays current data in the template selected from the dialog's table.

## Adding a New Cardholder

Use the following steps to create a new cardholder via the Cardholders screen.

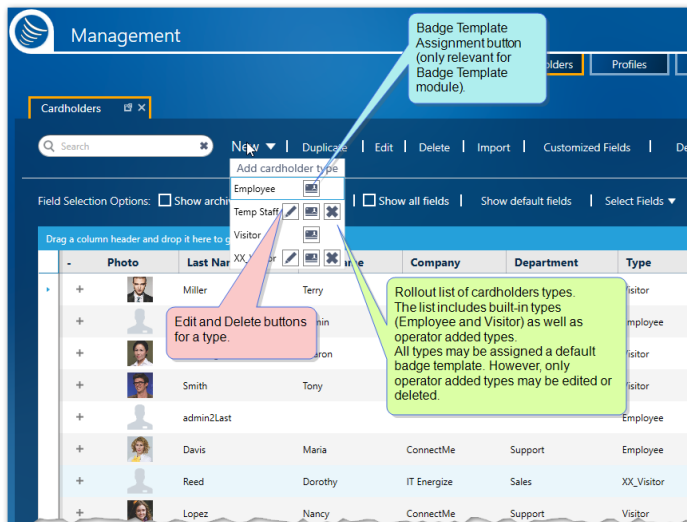


**Note:** A cardholder may be added and assigned a badge through the Cardholders screen or through badge management. For more information about cardholder options in badge management, see [Assigning a Badge to a New Cardholder](#) and "[Adding Multiple Badges where the Badge Code is Sequential](#)" on page 180.

# How to add a new cardholder to the system

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. From the action bar, click **New**. A rollout list of existing Types appears. At the top of the list is an action item that allows you to create a new Type. For more information about managing Types, see "Add/Edit/Delete a Cardholder Type" on page 205.

Figure 8-3



3. Select a Type from the rollout list. A new cardholder's details are displayed with the selected Type and other default values already entered.

If the **Visitor** cardholder type is selected, the **Anytime Anywhere** Multiple Access Group will not be available in the cardholder's details.

Figure 8-4

The screenshot shows a 'Cardholder Details' form with the following sections and fields:

- General:** Last Name, First Name, Type (Temp Staff), Number, ID Type (Identity Card), ID, Company.
- Valid from:** Enter date
- Expiration date:** Enter date
- Validated:**
- Department:** Please select an item.
- Office phone:**
- Badge:**
  - Badge code: Select or Type a Badge Code (with Add and Get buttons)
  - Template: No Template Selected (Using Default)
- Access:**
  - PIN code:
  - Personal Weekly program: Select Weekly Program
  - Area: Not located
  - Multiple Access Group: No Access \ Personal Access-Group
  - Personal Door Access Groups: Reception (with Add / Manage button)
  - Personal Lift Access Group: <None>

Callouts:

- Green callout: "New cardholder's details with the type already selected. A different type may be selected from the Type drop-down list." (points to the Type dropdown)
- Pink callout: "Multiple Access Group, Personal Door Access Groups, and Personal Lift Access Group may appear with default values set in the Infrastructure screen's Site details." (points to the Multiple Access Group dropdown)

4. Enter additional cardholder information in the parameter fields as required for each tab in the cardholder's details.

For information about each field, see "[Operator \(User\): MultiSite Impact Cardholder Details](#)" on page 607.



**Note:** When selecting an initial Department for a new cardholder and the department has a Multiple Access Group designation, The Multiple Access Group will be used as a default for the cardholder and will appear in the detail's Multiple Access Group field. You can change the group at any time from the Multiple Access Group drop-down list.

If the badge code that will be assigned to a cardholder is already in the system (in the Badges screen) and is free, a filter will be used in the Badge code field drop-down list. The filter is applied to a partially typed badge code or a partially typed description text linked to a badge code in the Badges screen.

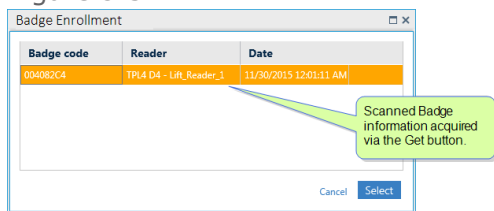
If the badge code is unknown to the system and the physical badge is available, use the **Get** button to the right of the Badge Code field.

The **Get** button allows you to acquire a badge code via a reader device swipe.



- a. Click **Get**. The Badge Enrollment dialog is displayed.

Figure 8-5



- b. Swipe the new badge at an enrollment reader. The badge information, including the badge code, appears in the dialog.

If the swiped badge does not have a status of **Free**, the badge information will not appear in the dialog.

If the cardholder requires a biometric sample enrollment, see ["Enrolling / Deleting a Cardholder's Biometric Sample" on page 214](#).

- c. Place the badge code in focus, and then click **Select**. The badge code appears in the Cardholder detail's **Badge Code** field.



**Note:** Not all cardholders require a badge. An example of a cardholder who doesn't need a badge code is a system operator who works offsite.

5. If a cardholder requires temporary access to a particular space see ["Temporary Access" on page 168](#). If not, leave the Temporary Access tab closed and go to Step 6.
6. Click one of the **Save** options in the action bar. The cardholder appears in the Cardholder Report table and is added to the system database.



**Note:** If the Cardholder Report table is more than one page, click **Refresh** to see the new cardholder row.

## Adding Customized Fields to Cardholder Details

Customized fields appear in all cardholder details' Customized Fields tab, this tab is only visible when a customized field exists. There are multiple types of customized fields that may be added to the Customized Fields tab (i.e. Free text, Yes/No slider, Number, and Date).

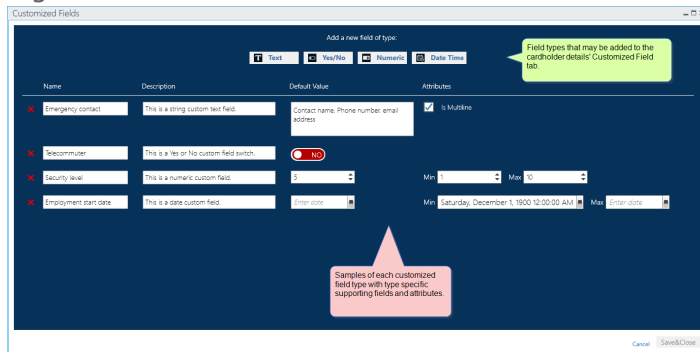
Customized Fields may be added to the Cardholder table via the **Select Fields** drop-down list found in the Cardholders screen. These field columns can be filtered and sorted like any other column in the table. There is one limitation, only five of each field type may be selected from the **Select Fields** drop-down list.

Use the following steps to add customized fields to cardholder details via the Cardholders screen.

### How to add customized fields to the cardholder details

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. From the action bar, click **Customized Fields**. The Customized Fields window is displayed.

Figure 8-6



3. Select the Type of field that will be added from the top of the window. A new row is added to the window with fields specific to the selected Type.
4. Enter a Name that will appear in the cardholder details' Customized Field tab and any other additional information.
5. Repeat Steps 3 and 4 until all customized fields are listed in the window.
6. In the list of customized field rows, drag and drop a row in the list to change the order in which the fields will appear in the cardholder details' Customized Field tab.
7. Click **Save**. The customized fields appear in all of the cardholder details' Customized Field tab.

## More about Customized Fields

Edits to a customized field row are immediately displayed in the cardholders details' Customized Field tab as soon as you click **Save** in the Customized Field window.

Customized fields may be deleted at any time by clicking the red "x" at the left of a row).



**Warning:** When you delete a customized field, any cardholder information previously entered in the field, via cardholders details' Customized Field tab, is lost.

# Importing Cardholder Data

Use the following steps to import cardholder data into the system via the Cardholders screen.



**Note:** The GuardPoint10 Cardholder Data Import process supports Excel (XLS and XLSX) formats. A purpose-built Excel Import spreadsheet must be populated with cardholder data (i.e. from an external database) before the import process can be started.

If the spreadsheet includes departments that do not currently exist in the system database, they are added to the database and the Departments screen during the import process.

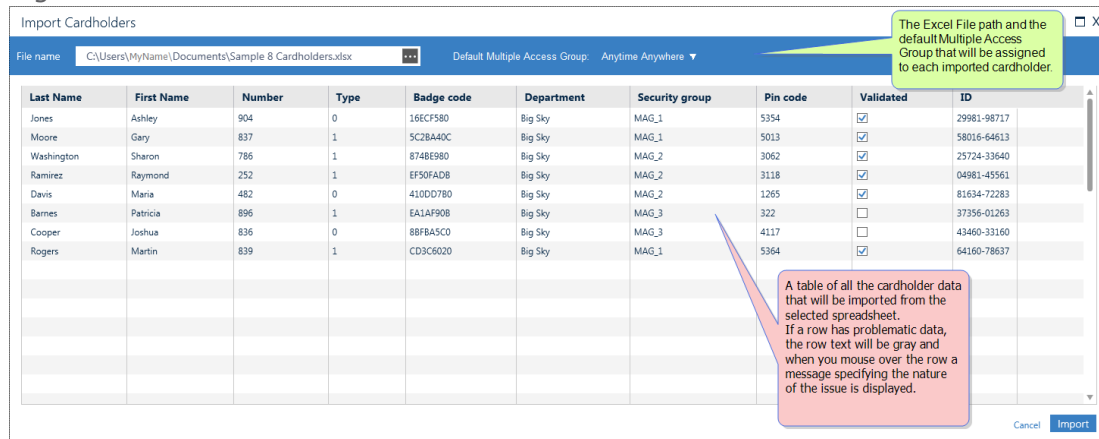
## How to import cardholder data into the system

1. Open your Excel Import spreadsheet with any application that supports the XLS file format.  
The spreadsheet, in a standard installation, can be found in:  
C:\Program Files (x86)\GuardPoint10\Gui\FormatFiles\Hr1.xls
2. Populate your spreadsheet template with cardholder data and save it.  
In the Import table, a Type can be entered by name or by the number assigned to an existing type in the database. If a user enters a new type, the type will be added to the database during the import process.
3. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
4. From the action bar, click **Import**. An Import Cardholders dialog is displayed.
5. From the top of the Import Cardholders dialog, click the three ellipses, and then browse and select your Excel spreadsheet file. The table in the dialog is then automatically populated with cardholder data from the spreadsheet.  
The maximum number of cardholders that can be imported from one Excel file is 1,500.
6. Immediately to the right of the Excel spreadsheet path field, select a **Default Multiple Access Group** from the drop-down list. The selected Multiple Access Group will be assigned to all of the cardholders that will be imported.

If **Default Multiple Access Group** is set to **Anytime Anywhere**, a cardholder, of type visitor, will bypass the default setting and initially be set to **No Access**.

The default value is **No Access**. Where applicable, the default site is the Root site.

Figure 8-7



If a cardholder row has problematic data, the row text will be gray and when you mouseover the row a message specifying the nature of the issue is displayed.

Data loaded into the Import Cardholder table may be edited at any time before clicking the Import button.

4. Click **Import**. The Import Cardholders dialog is closed; the cardholder data appears in the Cardholder Report table and is saved in the system database.

Data loaded into the Import Cardholder table may be edited at any time before clicking the **Import** button.

A cardholder **Type** value can be entered as text (i.e. "Freelancer") or, as the numeric value of a type already in the GuardPoint10 database (i.e. "0" for Employee or "1" for Visitor).

Currently, the maximum number of cardholders that can be imported at one time **with photos** is 1000.

## Updating cardholder information via the cardholder import process

When importing cardholders who are already in the system, the following fields will not update during the import process:

- » **Site**
- » **Shared status**
- » **Badge code** where **Is Additional Card** set to zero
- » **Valid From** and **To** dates
- » **Badge type**
- » **Cardholder photo**
- » **Custom fields**

# Duplicating a Cardholder

Use the following steps to create a duplicate of an existing cardholder via the Cardholders screen.



**Note:** When initially created, the duplicate cardholder will only copy general information from the selected cardholder. All other information must be added to the duplicate cardholder's details (i.e. First name, Last Name).

## How to duplicate the general data of an existing cardholder

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Select the row of an existing cardholder that will be duplicated.
3. From the action bar, click **Duplicate**. New cardholder details appear containing duplicate general information from the cardholder previously selected in Step 2.

Figure 8-8

4. Enter missing cardholder information in the parameter fields as required or, change duplicate information copied from the original cardholder.

5. Click one of the **Save** options in the action bar. The new cardholder appears in the Cardholder Report table and is added to the system database.

# Add/Edit/Delete a Cardholder Type

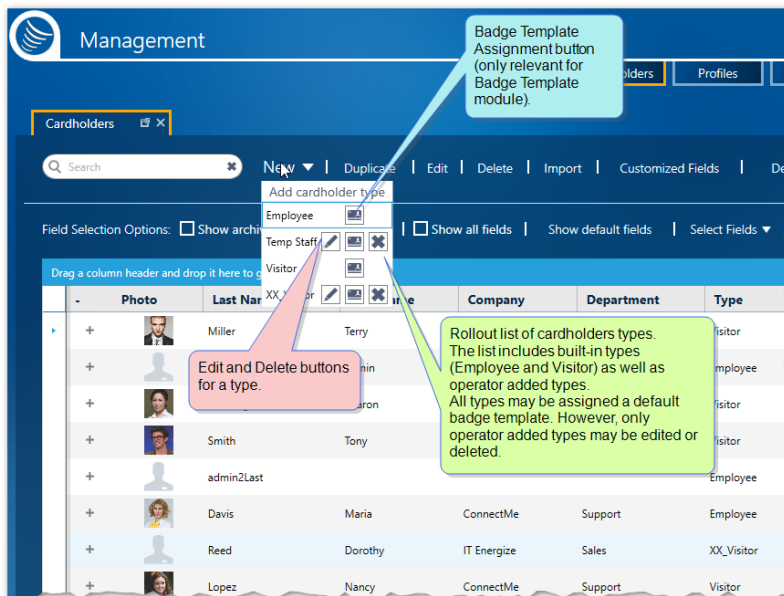
Use the following steps to create a new cardholder Type via the Cardholders screen.

**Note:** These instructions include information about badge templates. The information about the templates is only relevant for GuardPoint10 installations that include the Badge Template module. For information about the Badge Template module, see "[Badge Templates](#)" on page 293.

## How to add a new cardholder Type to the system

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. From the action bar, click **New**. A rollout list of existing Types appears. At the top of the list is an action item called **Add Cardholder Type**. This item allows you to create a new Type and assign it a badge template.

Figure 8-9






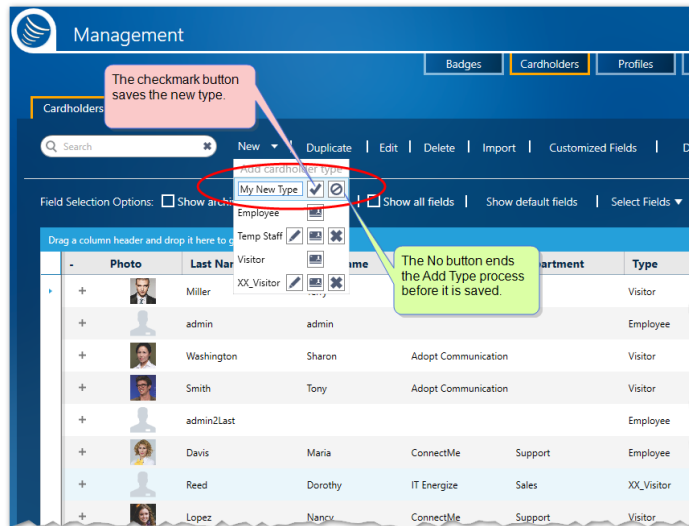

3. Click **Add Cardholder Type**. A new field appears just below the **Add Cardholder Type** action item.
4. Enter the name of the new Type and then click the checkmark  to the right of the field to save the Type. The Type is now available for assignment and appears in the rollout with an **Edit** button , **Delete**  button, and a **Badge Template Assignment**  button.

Figure 8-10



To cancel the Add New Type operation, click  before you click the checkmark.

## How to assign a default badge template to a cardholder Type

**Note:** This section is only relevant for installations that include the Badge Template module.

This means that any new cardholder with this Type assignment will automatically be assigned the selected badge template.


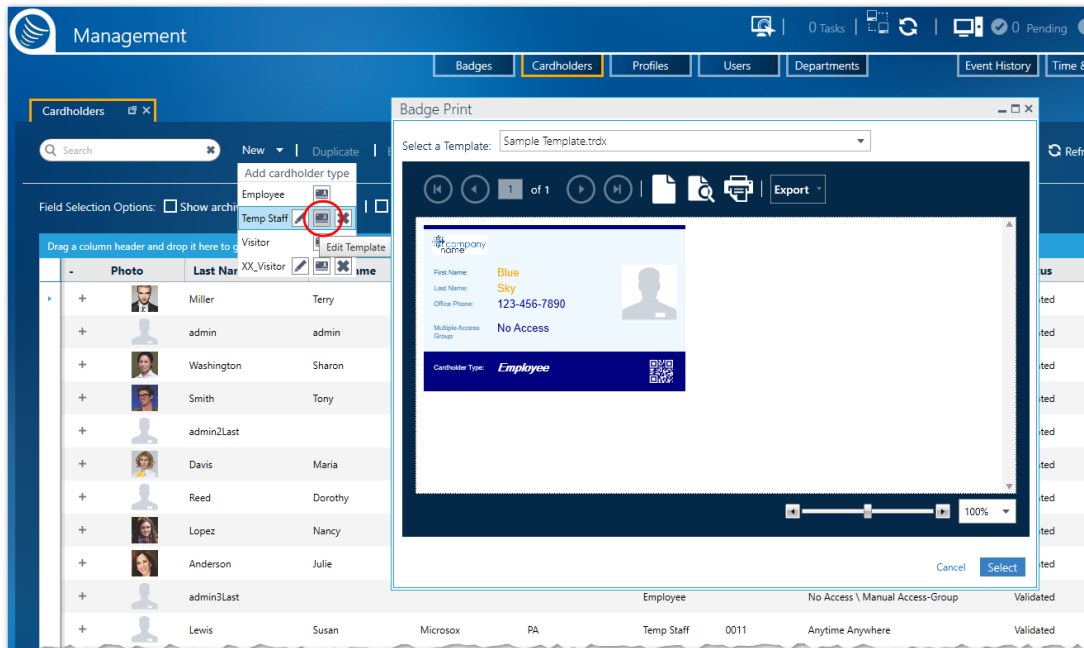
1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. From the action bar, click **New**. A rollout list of existing Types appears.
3. Scroll to the Type that will be assigned a default template and click the **Badge Template**  button. A Badge Template dialog is displayed.



Figure 8-11



4. From the **Select a Template** drop-down list, select a default template for the Type. The template layout appears in the dialog.
5. After selecting the template, click **Select**. The dialog is closed and the name of the template appears in the Cardholders screen's, Template column for each cardholder of the selected Type.

Assigning a default template means that all cardholders with the specified Type will automatically be assigned the selected template. However, an individual cardholder previously assigned a different template, with no connection to their assigned Type, will retain their previously assigned template and will not be assigned the default template.

6. If a cardholder is using the cardholder type's default badge template, the cardholder's details will not display the badge template name in the relevant field, even though the default badge template is assigned to the cardholder.


For information about assigning an individual cardholder a badge template other than the default template, see ["Manually assigning a Cardholder a Badge Template via the Cardholders Screen" on the next page.](#)

## How to Edit/Delete an operator defined cardholder Type

1. Go to the Management Task group and click Cardholders. The Cardholders screen is displayed.
2. From the action bar, click **New**. A rollout list of existing Types appears.
3. Scroll to the Type that you will edit or delete and do one of the following:

» To the right of the Type name, click . The Type Name field is now editable.

Changing the name of a Type in this field does not change the Type name in a cardholder details where the Type has already been assigned.

- » To the right of the Type name, click . The Type is deleted from the rollout list of existing Types.

Deleting the name of a Type prevents the Type from being used in the future, or until it is added to the Type list again. It does not delete the Type name in cardholder details where the Type was previously assigned.

## Manually assigning a Cardholder a Badge Template via the Cardholders Screen

Use the following steps to override a cardholder's Type default template assignment via the Cardholders screen.



**Note:** These instructions are only relevant for GuardPoint10 installations that include the Badge Template module. For information about the Badge Template module, see "[Badge Templates](#)" on page 293.

### How to assign a badge template to a cardholder, regardless of the cardholder's Type.

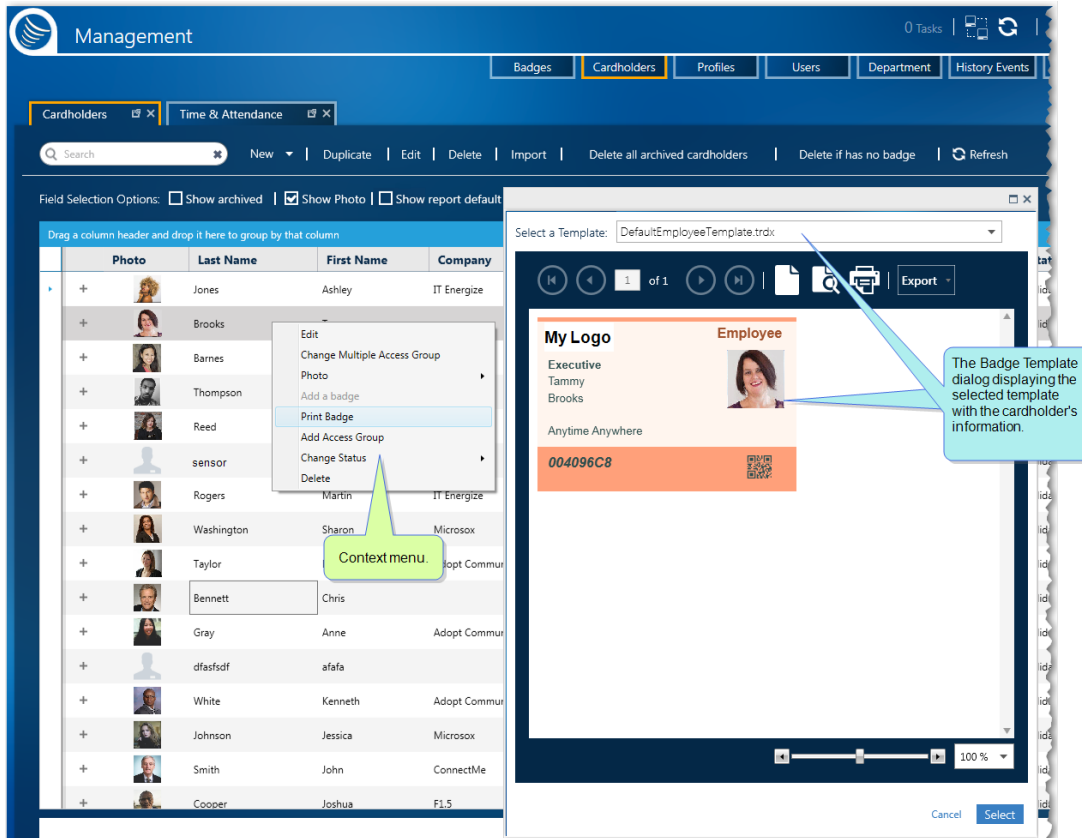
#### Via the Cardholders screen

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. In the Cardholder Report table, right-click on a cardholder's row where the template assignment will be changed. A context menu appears.
3. In the context menu click **Print Badge**. A Badge Template dialog is displayed with the cardholder's badge appearing with the currently assigned template.

For **Print Badge** to be enabled in the context menu, the cardholder must have a badge code already assigned.

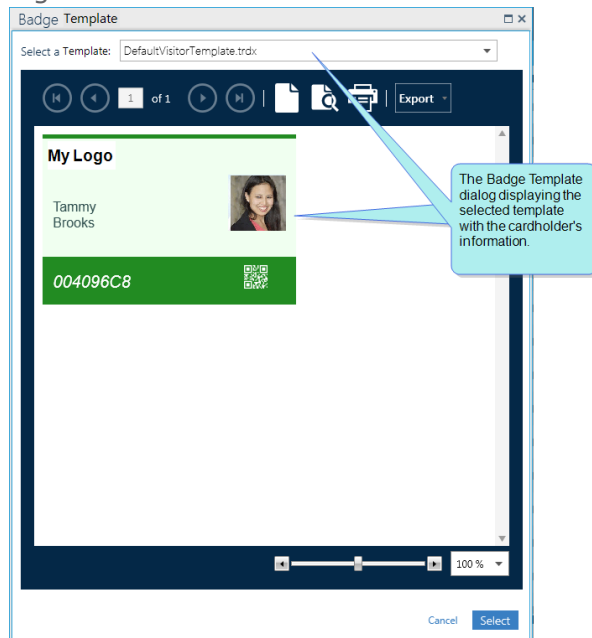
Alternatively, click the **Print Badge** button in the Cardholder's details. A Badge Template dialog is displayed with the cardholder's badge appearing with the currently assigned template.

Figure 8-12



4. From the **Select a Template** drop-down list, select the template that will replace the currently assigned template. The cardholder's badge appears in the dialog with the new template.

Figure 8-13



For more information about the template dialog, see "Badge Templates Screen" on page 564.

5. After selecting the new template, click **Select**. The dialog is closed and the name of the new template appears in the cardholder's Template column.

The cardholder's manually assigned badge template will be retained regardless of any changes made to the Type assignment or the default template of the cardholder's Type.

## Via a cardholder's details

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. In the Cardholder Report table, double-click on a cardholder's row where the template assignment will be changed. The cardholder's details are displayed.
3. In the **Template** field, select a new template from the field's drop-down list.
4. Click one of the **Save** options in the cardholder details' action bar. The cardholder's badge template assignment is saved in the system database.

The new badge template assignment is cardholder-specific and does not rely on the default template assignment of the cardholder's Type assignment.

# Assigning a Preexisting Multiple Access Group to a Cardholder via the Cardholders Screen

Use the following steps to assign a preexisting Multiple Access Group to a cardholder without opening the cardholder's details.

If the cardholder already has a Personal Door Access group list or, Personal Lift Access Group, and there is a conflict between a selected Multiple Access Group and a Personal Access Group, the Personal Access Group will have a higher priority than the Multiple Access Group.



**Note:** A Multiple Access Group cannot be assigned to an archived cardholder.

## How to assign a Multiple Access Group to a cardholder in a single operation

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Right-click a cardholder. A context menu appears.  
Alternatively, to select multiple cardholders (batch selection), press **Alt** on the keyboard and click multiple cardholder rows, and then right-click. A context menu appears.
3. From the context menu, select **Change Multiple Access Group**. A Select Multiple Access Group dialog is displayed.
4. Select an existing Multiple Access Group from the drop-down list, and then click **Save**. The Multiple Access Group is assigned to the previously selected cardholder(s).
5. (Optional) Verify the cardholder has been assigned the selected Multiple Access Group by opening the cardholder's details and in the General tab confirm that the **Multiple Access Group** parameter value is the same.

If you would like to change the value in the **Multiple Access Group** parameter again, you can select a Multiple Access Group value from the parameter's drop-down list in the cardholder's details.

# Manage a Cardholder's Door Access Group assignment from the Cardholders screen - Without a Multiple Access Group

This topic covers the management of Door Access Groups assigned to a cardholder outside of the Multiple Access Group container, via the Personal Door Access Group field.



**Note:** If a conflict exists between an assigned Multiple Access Group, a Personal Access Group, or a Temporary Access item (reader or Multiple Access Group), the priority order is (from top to bottom) Temporary Access item followed Personal Access Group, and then Multiple Access Group.

Use the following steps to Manage a Cardholder's Personal Door Access Group assignment from the Cardholders screen.

## How to Add/Manage a Cardholder's Personal Door Access Group assignments via the Cardholders screen

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Select one or more cardholders from the Cardholders table.
3. Right-click the selected cardholder(s). A context menu appears. Select **Add Personal Door Access Groups to Cardholders**.
4. From the displayed Select Door Access Groups dialog, Move Door Access Groups to the Selected Access Groups column as required.
5. Click **Override** or **Add**.

If **Override** is clicked, the selected Door Access Groups will replace any previously listed Personal Door Access Groups in the cardholder's details.

If **Add** is clicked, the selected Door Access Groups will be added to the top of the Personal Door Access Groups list in the cardholder's details. All previously added Personal Door Access Groups will remain on the list.

If **Add** is clicked, the selected Door Access Groups will be added to the top of the Personal Door Access Groups list in the cardholder's details. All previously added Personal Door Access Groups will remain on the list.

The **Add** button will appear in the dialog in case:

- » One or more of the selected cardholders currently do not have any Personal Door Access Groups.
- » The selected cardholders do not have matching lists of Personal Door Access Groups.

## How to Remove a Cardholder's Door Access Group assignments via the Cardholders screen

1. Go to the Management Task group and click Cardholders. The Cardholders screen is displayed.
2. Select one or more cardholders from the Cardholders table.
3. Do one of the following:
  - » Click the **Add / Manage Door Access Group** button found in the Action menu.  
From the displayed Add / Manage dialog, Move Door Access Groups to the Not Selected Access Groups column as required, and then click **Override**.
  - » Right-click the selected cardholder(s). A context menu appears. Select **Remove All Door Access Groups**.

The list of assigned Personal Door Access Groups in each cardholder's details is updated.

## How to place a cardholder's assigned Personal Door Access Groups with a New Multiple Access Group via the Cardholders screen

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Select a cardholder from the Cardholders table.
3. Right-click the selected cardholder and select **Convert Door Access Groups to a Multiple Access Group**. A Convert Door Access Groups to a Multiple Access Group dialog is displayed.
4. Enter a name for the new Multiple Access Group.
5. Select the checkbox in the dialog to apply the new Multiple Access Group to all cardholders who are using the same Personal Door Access Group list. Otherwise, the new Multiple Access Group will only be applied to the selected cardholder.
6. Click **Save**. A new Multiple Access Group containing the Door Access Groups in the selected cardholder's details is added to the Access screen's Multiple Access Group tab and is assigned to the relevant cardholder(s).

# Enrolling / Deleting a Cardholder's Biometric Sample

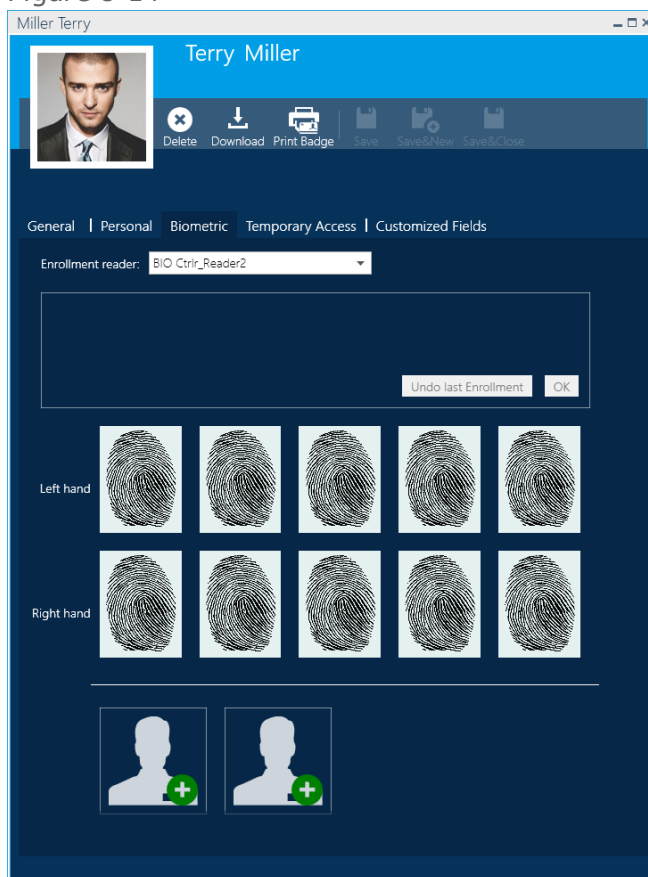
Before you can enroll a cardholder's biometric sample, verify that a biometric reader is set as an Enrollment reader in the system (see ["Reader Details" on page 453](#)).

Use the following steps to enroll the biometric sample of a cardholder.

## How to enroll a cardholder's biometric sample

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Click the row of an existing cardholder who will enroll a biometric sample. The cardholder's details are displayed.
3. Open the Biometric tab in the cardholder's details.

Figure 8-14



4. From the **Enrollment Reader** drop-down list, select a previously defined biometric enrollment reader.
5. Choose to enroll a fingerprint or a face



» Fingerprint:

- a. Mouseover an image (white fingerprint). A green plus sign appears.
- b. Click the green plus sign. The reader is now in scan mode.
- c. Quickly, have the cardholder place their finger on the reader's scanner and wait for a beep. The fingerprint is scanned.
- d. Repeat Step 7. Two consecutive scans are required to enroll a fingerprint.
- e. Click the **OK** button to confirm the enrollment and make the other fingerprint images accessible. The color of the fingerprint image, where you enrolled the cardholder's biometric data (fingerprint), changes to green.

At this point, you can enroll additional fingerprints (Steps 5 - 9) or delete biometric data (a fingerprint) previously enrolled.

- f. Click one of the **Save** options in the cardholder details' action bar. The cardholder's biometric data (a fingerprint) is saved in the system database and downloaded to the local database of relevant biometric readers.

» Face:

- a. Mouseover an image (a white silhouette of a person).
- b. Click the green plus sign. The reader is now in scan mode.
- c. Quickly, have the cardholder step in front of the reader's scanner and wait for the scan to complete. The scanned image will appear in the same group box as the **OK** button and the **Undo last Enrollment** button.
- d. Evaluate the scanned image for use as a biometric sample.
- e. Click the **OK** button to confirm the enrollment, or click **Undo last Enrollment** to reject the image.

If **OK** was clicked the biometric sample will replace the framed white silhouette and includes a red X overlay to delete the biometric sample.

- f. Click one of the **Save** options in the cardholder details' action bar. The cardholder's biometric sample is saved in the system database and downloaded to the local database of relevant biometric readers.

## How to delete a cardholder's enrolled biometric sample

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Click the row of an existing cardholder where an enrolled biometric sample will be deleted. The cardholder's details are displayed.
3. Open the Biometric tab in the cardholder's detail and mouseover a biometric sample. A red minus sign appears over the image.
4. Click the red minus sign and confirm the operation. The biometric sample changes to white.
5. Click one of the **Save** options in the cardholder details' action bar. The cardholder's biometric sample is removed from the system database and the local database of relevant biometric readers.

# Editing Cardholder Details

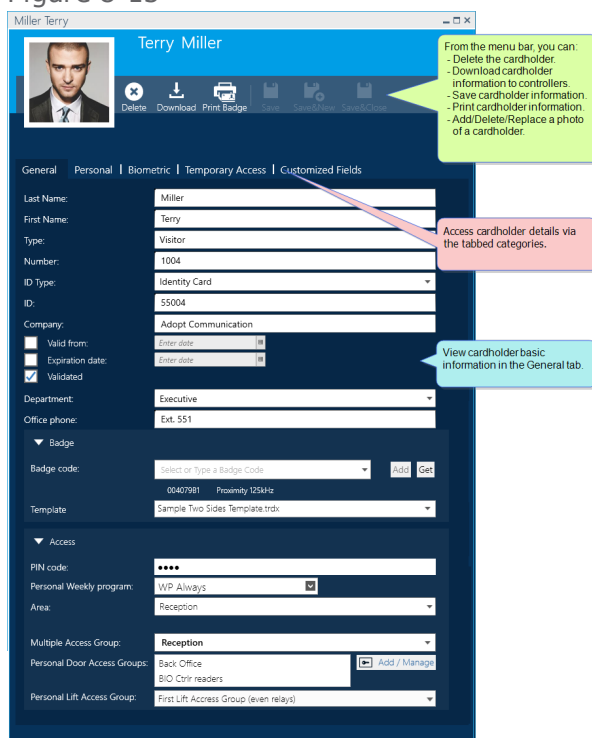
Use the following steps to edit an existing cardholder's details via the Cardholders screen.

## How to edit the details of an existing cardholder

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Double-click the row of an existing cardholder where the details will be edited. The details are displayed.
3. Edit/Add/Delete information in the relevant parameter fields. If necessary, refer to "[Operator \(User\): MultiSite Impact Cardholder Details](#)" on page 607, for more information about each field.

If you are going to change the information in the Temporary Access tab, see "[Temporary Access](#)" on page 168.

Figure 8-15



4. Changing a cardholder's validation setting may be performed from the cardholder's details or from a cardholder's context menu in the Cardholders Report table.

To access the validation setting in a cardholder's context menu, right-click a cardholder row and select Validate or Invalidate (depending on the current setting). Verify the change from the cardholder details General tab's **Validated** parameter setting.




**Note:** If the validation setting is date-dependent (**Valid From** and **Expiration Date** values exist in the cardholder's detail), changing the values from the cardholder context menu will override these values.


5. Changing a cardholder photo is not quite as straightforward as the other parameter fields. To Switch/Add/Delete a cardholder photo, which is located over the left side of the action bar of the details, do the following:

**Mouseover**<sup>1</sup> the current image in the cardholder's details and:

**If you are going to take a picture with a digital camera connected to the PC, where GuardPoint10 is running:**

- a. Click . A Take Photo dialog is displayed.  
Alternatively, in the Cardholder screen, right-click a cardholder row and select the Photo > Take Photo item from the context menu.
- b. Take the picture; when the image appears in the dialog, click **Save**. The image appears in the cardholder's details and in the Cardholder Report table.


**If you are going to use a previously saved photo:**

- a. Click . A file browser is displayed.  
Alternatively, in the Cardholder screen, right-click a cardholder row and select Photo > Browse from the context menu.
- b. In the browser, find the file you want to use in the cardholder details, and then click **Save**. The image appears in the cardholder's details and in the Cardholder Report table.

**If you are going to delete a photo that is already in the cardholder's details:**

- » Click . The image is deleted from the cardholder's details and from the Cardholder Report table.

Alternatively, in the Cardholder screen, right-click a cardholder row and select Photo > Delete from the context menu.

The  button appears (and the Delete context menu option is enabled) only when a photo is already in the cardholder's details.

5. After you have finished editing the details, click one of the **Save** options in the action bar. The cardholder details are updated in the Cardholder Report table and saved in the system database.

## How to edit the details of multiple cardholders from a single set of cardholder details

This operation allows you to change common data in multiple cardholder details via a specially designed **Select Multi** cardholder details.

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Select the rows of existing cardholders where the details will be edited. The rows are in focus.

To select multiple rows, hold down the left mouse button and drag across multiple rows. Alternatively, hold down the **Ctrl** key while selecting individual rows out of sequence.

---

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

3. Right-click a selected cardholder row and select **Edit** from the context menu. A cardholder's details, titled "Select Multi", is displayed.

Figure 8-16

The screenshot shows a web application window titled "Multi Select" with a sub-header "Select Multi". The interface includes a navigation bar with icons for Delete, Download, Print Badge, Save, Save&New, and Save&Close. Below the navigation bar are tabs for General, Personal, Biometric, Temporary Access, and Customized Fields. The form fields are organized into sections: General (Last Name: Multi, First Name: Select, Type: XX\_Employee, Number: xxxxxx, ID Type: Identity Card, ID: xxxxxx, Company: [dropdown]), Valid from and Expiration date (date pickers), Validated (checked), Department (dropdown), Office phone (Ex. 223), Badge (dropdown, Add, Get), and Template (No Template Selected (Using Default)). The Access section includes PIN code (masked), Personal Weekly program (dropdown), Area (The Area field is not available in Select Multi), Multiple Access Group (Reception), Personal Door Access Groups (Back Office, BIO Ctrlr readers, Add / Manage), and Personal Lift Access Group (First Lift Access Group (even relays)).

4. Make the required changes to the "Select Multi" details.

Only the fields that are logically able to share information will be enabled. For example, the **ID** field will not be enabled because it must be a unique value for each cardholder.

The Select Multi details' Temporary Access tab is disabled.

5. After you have finished editing the details, click one of the **Save** options in the action bar. Any change you made will be applied to all of the cardholders selected in Step 2.

# Creating and Assigning a New Multiple Access Group in a Single Cardholder Operation

The operation used to create and assign a new Multiple Access Group is simple. However, the process is relatively complex. To understand the results of this operation you should understand the logic behind it.

## Logic flow:

After selecting an Access Group from the Selected Access Group dialog (more about this dialog in the instructions below), the system examines each cardholder in focus to determine if the Multiple Access Group currently assigned to the cardholder includes the new selected Access Group.

The examination results in one of the following actions:

If the cardholder's currently assigned Multiple Access Group does include the Access Group selected in the Select Access Group dialog, the cardholder's Multiple Access Group assignment is left unchanged.

If the cardholder's currently assigned Multiple Access Group does **not** include the Access Group selected in the Select Access Group dialog, a new Multiple Access Group is automatically created. The new Multiple Access Group will include the Access Group selected in the Select Access Group dialog and all of the Access Groups in the Multiple Access Group currently assigned to the cardholder.

After the new Multiple Access Group is created it will be assigned to the cardholder and the previously assigned Multiple Access Group will be discarded.

The previously assigned Multiple Access Group still exists. The only change to it is its assignment to the cardholder who fits the conditions described above.

If the cardholder does not have a previously assigned Multiple Access Group, a new Multiple Access Group will be created and assigned to the cardholder. The new Multiple Access Group will contain only the selected Access Group.



**Note:** This operation may add a new Multiple Access Group to the Access screen, see "[Access](#)" on [page 139](#). Multiple Access Groups created via the Cardholders screen behave the same way as any other Multiple Access Group. The only difference is the method used to create it.

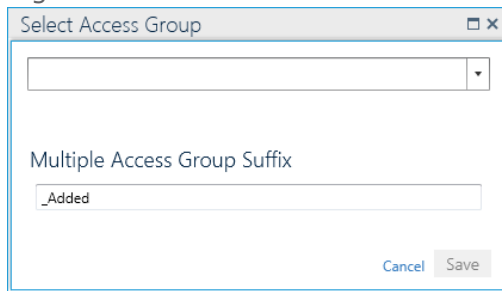
This operation is especially useful when assigning a batch of cardholders to a new Multiple Access Groups based on the same logic.

Use the following steps to creating and assigning a new Multiple Access Group via the Cardholders screen.

# How to create a new Multiple Access Group and assign it to a cardholder in a single operation

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Right-click a cardholder. A context menu appears.  
Alternatively, select multiple cardholders (batch selection), press Alt on the keyboard and click multiple cardholder rows, and then right-click. A context menu appears.
3. From the context menu, select **Add Access Group**. A Select Access Group dialog is displayed.

Figure 8-17



4. Select an existing Access Group from the drop-down list.
5. Enter a unique suffix in the Multiple Access Group Suffix area if the default suffix doesn't work for you, and then click **Save**.
6. Using the logic flow described above, the system will (or won't) create and assign a new Multiple Access Group as required. The Multiple Access Group column in the Cardholders screen is updated to reflect any changes to the Multiple Access Group assignments.

# Assigning a Badge Code to an Existing Cardholder from the Cardholders Screen

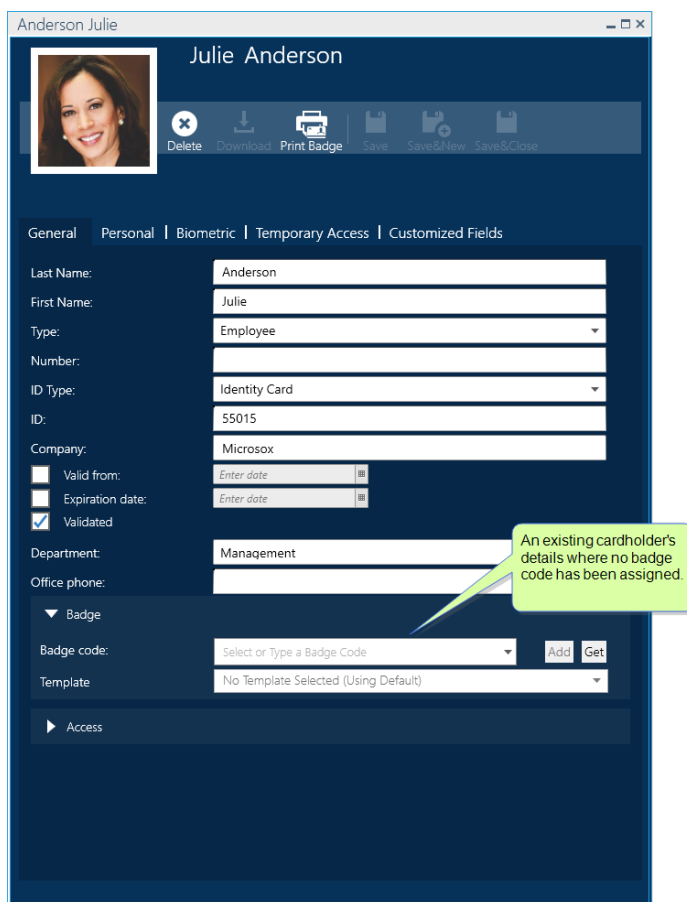
Use the following steps to assign a badge to an existing cardholder.

**Note:** A badge may be assigned to an existing cardholder through the Cardholder screen or through badge management. For more information about cardholder options in badge management, see ["Badges" on page 175](#).

A badge cannot be assigned to an archived cardholder.

## How to assign a badge to an existing cardholder

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Click the row of an existing cardholder where the badge will be assigned. The cardholder's details are displayed.



Anderson Julie

Julie Anderson

Delete Download Print Badge Save Save&New Save&Close

General Personal Biometric Temporary Access Customized Fields

Last Name: Anderson

First Name: Julie

Type: Employee

Number:

ID Type: Identity Card

ID: 55015

Company: Microsox

Valid from: Enter date

Expiration date: Enter date

Validated

Department: Management

Office phone:

Badge

Badge code: Select or Type a Badge Code Add Get

Template: No Template Selected (Using Default)

Access

An existing cardholder's details where no badge code has been assigned.

**Note:** One active badge code can be assigned per cardholder. This means that if the selected cardholder already has a badge code assignment, they cannot be assigned a new badge code until the first badge code's assignment is changed.

To free a badge code already assigned to a cardholder, open the cardholder's details and click the **Badge Code** field. From the field's drop-down list, select <None>.

3. In the **Badge code** field, enter a free badge code known to the system

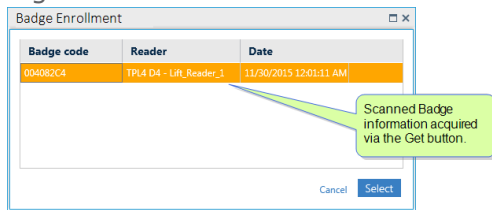
A filter will be used in the Badge code field drop-down list. The filter is applied to a partially typed badge code or a partially typed description text linked to a badge code in the Badges screen.

If the badge code is not known to the system, but the physical badge is available, use the **Get** button to the right of the **Badge Code** field.

The **Get** button allows you to acquire a badge code via a reader device scan.

- a. Click **Get**. The Badge Enrollment dialog is displayed.

Figure 8-18



- b. Scan the new badge at a reader. The badge information, including the badge code, appears in the dialog.

If the scanned badge does not have a status of **Free**, the badge information will not appear in the dialog.

- c. Place the code in focus, and then click **Select**. The badge code appears in the cardholder's **Badge Code** field.



**Note:** Cardholders do not require a badge assignment. An example of a cardholder who doesn't need a badge code is a system operator who works offsite.

4. Click **Add**, and then one of the **Save** options in the cardholder details' action bar. The cardholder's badge code assignment is saved in the system database.



# Printing a Cardholder Badge via the Cardholders Screen

A badge can be printed from the Badges screen and the Cardholders screen. Use the following steps to print a cardholder's badge via the Cardholders screen.

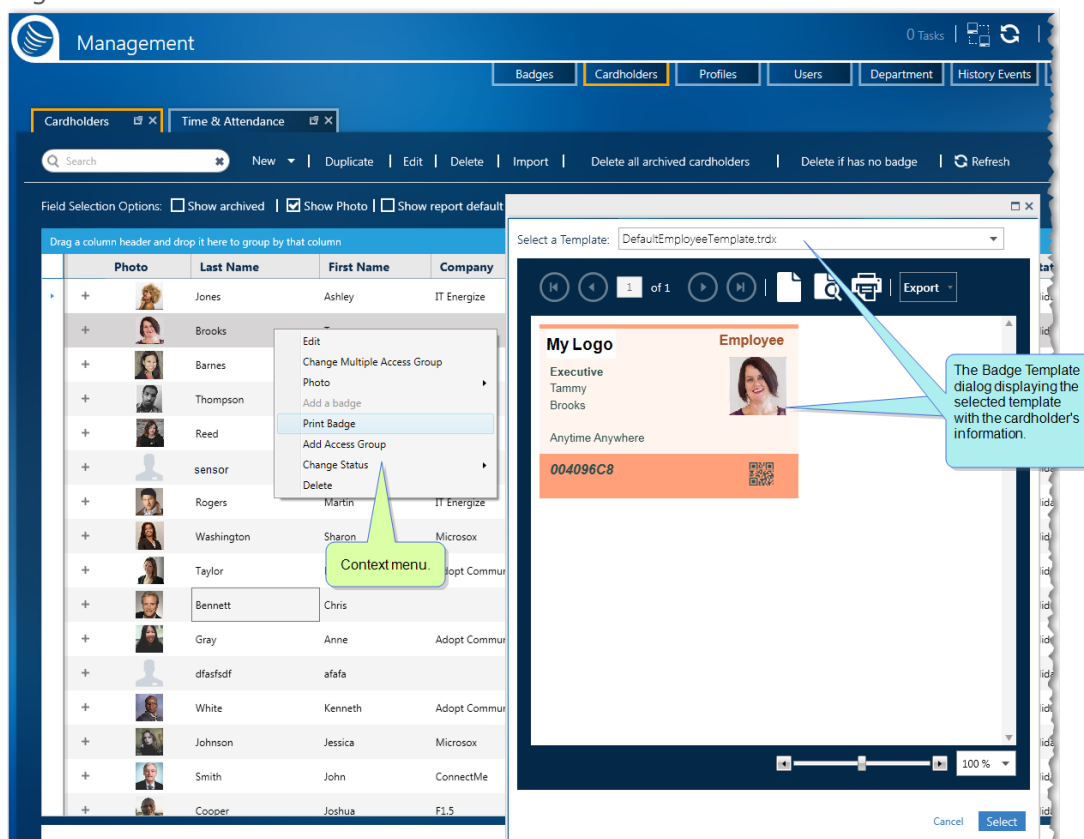
**Note:** These instructions are only relevant for GuardPoint10 installations that include the Badge Template module. For information about the Badge Template module, see ["Badge Templates" on page 293](#).

## How to print a badge via the Badges screen

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. In the Cardholder Report table, choose the cardholder whose badge will be printed and right-click on the cardholder's row. A context menu appears.
3. In the context menu click **Print Badge**. A Badge Template dialog is displayed with the cardholder's badge appearing with the currently assigned template.

For **Print Badge** to be enabled in the context menu, the cardholder must have a badge code already assigned.

Figure 8-19



4. From the Badge Template dialog toolbar, click the printer icon. The Windows Print dialog is displayed.
5. Complete the Print dialog and click **Print**. The Badge is printed on the designated printer.

## Changing the Status of Cardholders

Use the following procedures to change the status of cardholders from the Cardholders screen.

### How to archive a single cardholder



**Note:** After archiving cardholders, you will always have the option of restoring them later. However, deleting cardholders from the system database is permanent.

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Select the row of a cardholder that will be archived. The row is placed in focus.
3. Right-click the row and select **Change Status > Archive** from the context menu, and then confirm the operation. The cardholder is archived. If the cardholder was assigned a badge code, the code assignment is withdrawn and the code will have a status of **Free**.

To see archived cardholders in the Cardholder Report table, select the **Show Archived** checkbox above in the Cardholder Report table.

### How to archive a batch of cardholders

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. From the Cardholder Report table, do one of the following:
  - » Press the **Ctrl** key and click on the cardholder rows you want to archive. The rows are placed in focus.
  - » Drag the mouse pointer through the cardholder rows you want to archive. The rows are placed in focus.
3. Right-click one of the rows in focus and select **Change Status > Archive** from the context menu, and then confirm the operation. The cardholders are archived. If a cardholder was assigned a badge code, the code assignment is withdrawn and the code will have a status of **Free**.
4. To verify that the cardholders are archived, from above the Cardholder Report table select **Show Archived**. The archived cardholders will appear in the table with a Status of **Archived**.

### How to restore one or more archived cardholders Cardholder Report Table

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. From the action bar, select the **Show archived** checkbox. Archived cardholders appear in the Cardholder Report table.
3. Select one or more rows of archived cardholders (use the **Ctrl** key or mouse drag technique).

4. Right-click on a selected row, and then select **Change Status > Restore** from the context menu. The cardholder(s) are no longer frozen and may be assigned badge codes.

## How to validate/Invalidate one or more cardholders from the

You can only validate/Invalidate cardholders that are not archived.

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. From the Cardholder Report table, do one of the following:
  - » Select the row of a single cardholder that will have its validity status changed.
  - » Press the **Ctrl** key and click on the cardholder rows where you want to change the cardholder's validity status.
  - » Drag the mouse pointer through the cardholder rows where you want to change the cardholder's validity status.
3. Right-click one of the rows in focus and select **Change Status > Validate** or **Change Status > Invalidate** from the context menu, and then confirm the operation. The cardholders' validity status changes.

This is the equivalent of opening a cardholder's details and selecting or clearing the Validated checkbox.



**Note:** To validate a cardholder for a specific range of time, open a cardholder's details and complete the **Valid From** field and the **Expiration Date** field.

## How to delete cardholders from the system database via Cardholder Report Table

You can delete cardholders regardless of their archive status or validity.

Proceed with caution, a deleted cardholder cannot be undeleted.

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Do one of the following:
  - » From the action bar, select **Delete All Archived Cardholders**, and then confirm the operation. Archived cardholders are erased from the system database.
  - » From the action bar, select **Delete if has no badge**, and then confirm the operation. Cardholders that are not assigned badges (this includes all archived cardholders) are erased from the system database.
  - » Select one or more cardholders from the Cardholder Report table, and then click **Delete** in the action bar. The cardholder(s) is erased from the system database.

# Generating a Cardholders Report Output (PDF, Excel, or Print)

A Cardholders Report consists of the displayed columns in the Cardholders screen's table.

You can generate a standard or customized Cardholder Report by selecting Cardholders Report table columns in the Cardholders screen. Before you generate a report, decide on the format that best satisfies your requirements. GuardPoint10 can generate reports in PDF and XLS formats. There is an additional option to print a hardcopy of your report via a selected printer.

After generating a report file or printing a hardcopy, you can distribute the report to the relevant personnel.



**Warning:** Some data in the Cardholder Report may be confidential and should be distributed responsibly.

## How to generate a Cardholder Report

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Display the Cardholder Report table columns in the order in which you would like them to appear in the report. To change the view of the table, see ["Changing Cardholder Report Table View" on page 194](#) and ["Cardholders Screen" on page 600](#).
3. After adjusting the Cardholder Report table view, do one of the following:

### Export to PDF

- a. Click **Export to PDF**. A Print Report dialog is displayed.
- b. Enter a report title name and click **Export**. A file browser opens.
- c. Enter a file name and select a location for your PDF file, and then click **Save**. The file is generated and saved in the specified location.

### Export to Excel

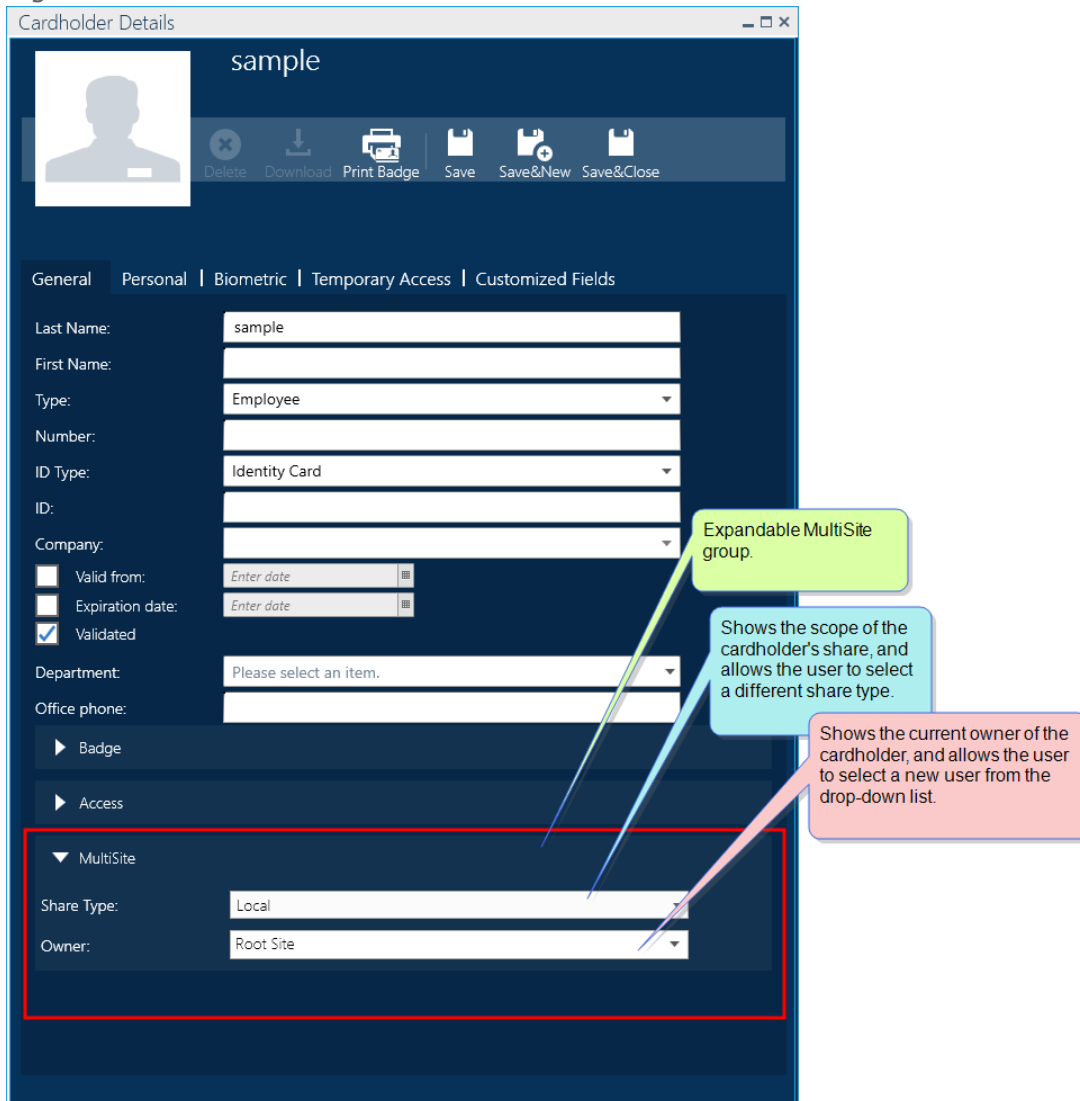
- a. Click **Export to Excel**. A Print Report dialog is displayed.
- b. Enter a report title name and click **Export**. A file browser opens.
- c. Enter a file name and select a location for your XLS file, and then click **Save**. The file is generated and saved in the specified location.

### Print a Hardcopy

- a. Click **Print**. A Print Report dialog is displayed.
- b. Enter a report title name and click **Print**. A Print Preview window opens.
- c. Review the pages of the report and; if necessary, change the page orientation.
- d. Click the **Print** button. A Printer Preference dialog is displayed.
- e. Select your preferences and click **Print**. A hardcopy of the report is printed at the specified printer.

# Cardholder: MultiSite Impact

Figure 8-20



The cardholder details includes a MultiSite expandable group at the bottom of the General tab. In this group there are the following fields:

- » **Owner:** Displays the name of the site where the cardholder is owned.
- » **Share Type:** indicates the share level of the cardholder. These levels are as follows:
  - » **Local:** Allows access only via readers owned by the same site as the cardholder. Cardholder details may be edited by a user owned by the same site and a super user.
  - » **Shared:** Allows access via readers owned by the same site as the cardholder as well as readers owned by other sites. Users owned by other sites may see the cardholder's details in a read-only view except for the Temporary Access tab where the user may add a temporary access reader or Multiple Access Group rule.
  - » **Global:** Allows access via readers owned by the same site as the cardholder as well as readers owned by other sites. Users owned by other sites may edit the cardholder's details as required including deleting the cardholder from the system.

A cardholder's **Number** no longer needs to be unique in the system, instead, it has to be unique to the site owner. For example, a cardholder owned by Site\_1 can have the same **Number** as a cardholder owned by Site\_2. But two cardholders in Site\_1 cannot have the same **Number**.

## Add a cardholder

When a cardholder is added to the system they are automatically assigned the same owner as the logged-in user who added the cardholder. The **Share type** will default to **Local**.

## Change the ownership of a cardholder

From the cardholder's details, select an owner site from the **Owner** drop-down list, and then click one of the save options. The cardholder's **Multiple Access Group** will automatically change to **No Access** and if there was a **Personal WP. Personal Door Access Groups**, and/or **Personal Lift Access Group**, it will reset to **<None>**.

## Consideration to make a cardholder MultiSite accessible

1. The cardholder must have a **Share type** of **Shared** or **Global**.
2. The other sites must share readers with the cardholder's owner site.
3. The cardholder's **Multiple Access Groups** must include the shared readers from the other sites.

# CHAPTER 9:

## Departments



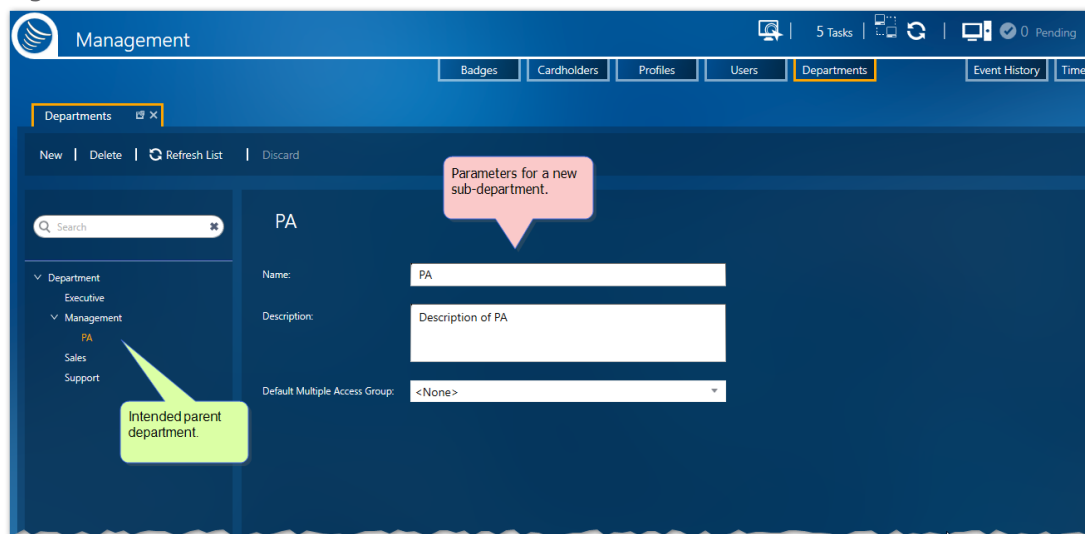
The Departments screen divides a company into various departments. A department can stand alone or be a sub-group of another department. In addition, a department may be used as a criteria for screen table layouts and report generation.

### Adding a New Department

Use the following steps to create a new department via the Departments screen.

# How to add a new department to the system

Figure 9-1



2. Enter a department name. The default name is "New Department".  
A department name must be unique.
3. (Optional) In the Description field, enter information specific to the department as it pertains to security.
4. (Optional) From the Default Multiple Access Group drop-down list, select the initial Multiple Access Group assigned to cardholders who are also assigned to the department in focus.

If a cardholder is assigned a Multiple Access Group via their cardholder details, the setting in the details will have a higher priority and override the department's **Default Multiple Access Group**.

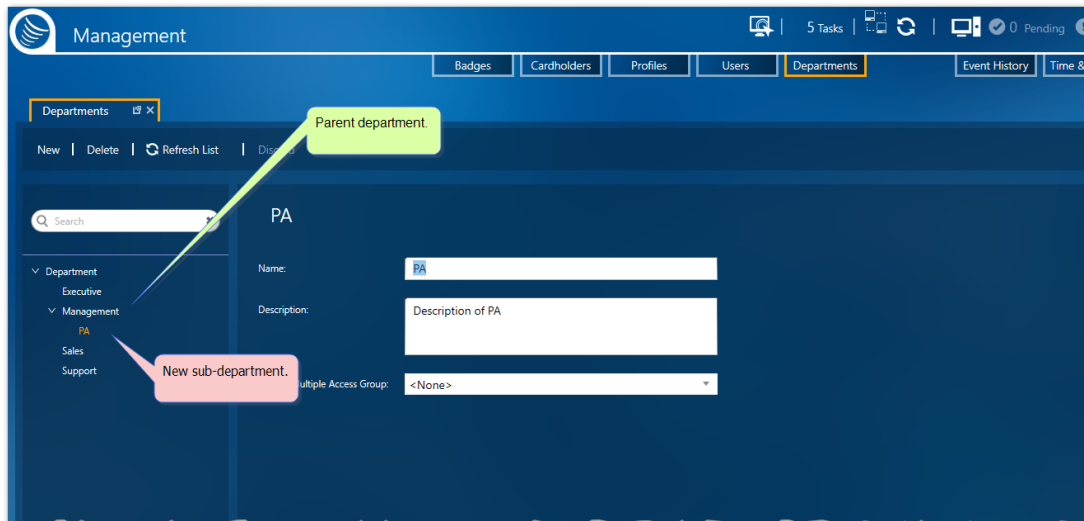
If **Default Multiple Access Group** is set to **Anytime Anywhere**, a cardholder, of type visitor, will bypass the default setting and initially be set to **No Access**.

For more information about Multiple Access Groups, see "[Multiple Access Groups](#)" on page 156.

5. Click **Save**. The department data is saved in the system database, it is added to the list of existing departments and it's available in a cardholder details' Department drop-down list.



Figure 9-2



# Editing Department Details

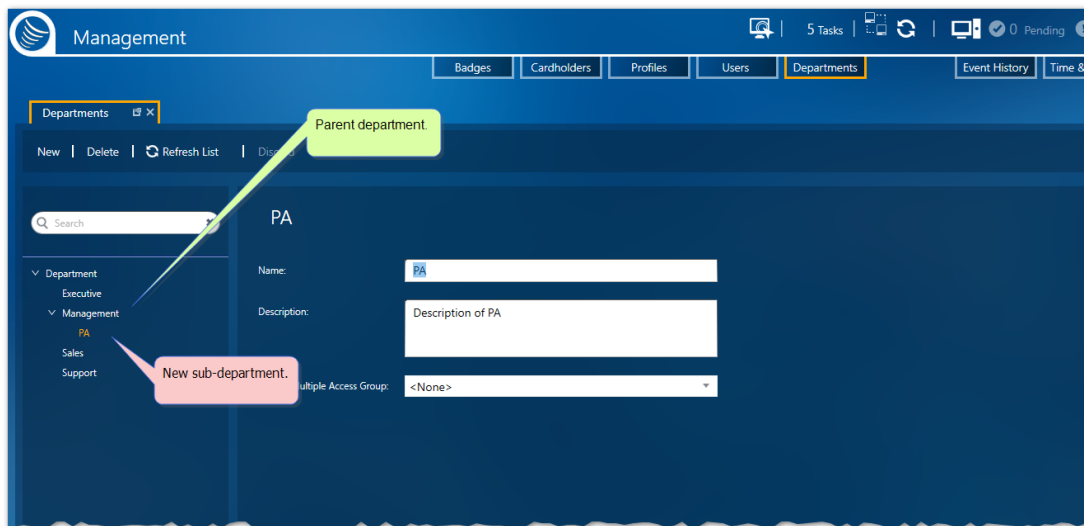
Use the following steps to edit the details of an existing department via the Departments screen.

**Note:** A department cannot be redesignated as a sub-department or vice versa through the editing process. You must delete the existing department and recreate it as a sub-department to redesignate it. For more information, see ["Deleting a Department" on page 234](#) and ["" on page 229](#).

## How to edit the details of a department

1. Go to the Management Task group and click **Departments**. The Departments screen is displayed.
2. From the list of existing departments on the left, select the department whose details will be edited. The department's parameters are displayed.

Figure 9-3



3. Change the department name, description, or default Multiple Access Group. A department name must be unique.
4. After editing department data, do one of the following:
  - » Click **Discard**. The system reverts to the previously saved department data.
  - » Click **Save**. The updated department data is saved in the system database and is updated in the details of a previously assigned cardholder.

# Assigning a Department to a Cardholder

Use the following steps to assign an existing department to a cardholder.

## How to assign a department to a cardholder

1. Go to the Management Task group and click **Cardholders**. The Cardholders screen is displayed.
2. Double-click the row of an existing cardholder where a department will be assigned. The cardholder's details are displayed.

Figure 9-4

The screenshot shows the 'Terry Miller' cardholder details form. The form is divided into several sections: General, Personal, Biometric, Temporary Access, and Customized Fields. The General tab is active, showing fields for Last Name (Miller), First Name (Terry), Type (Visitor), Number (1004), ID Type (Identity Card), ID (S5004), Company (Adopt Communication), Valid from, Expiration date, Validated, Department (Executive), Office phone (Ext. 551), Badge code (00407981), Template (Sample Two Sides Template.trdx), PIN code (\*\*\*\*), Personal Weekly program (W/P Always), Area (Reception), Multiple Access Group (Reception), Personal Door Access Groups (Back Office, BIO Cross readers), and Personal Lift Access Group (First Lift Access Group (even relays)). The form also includes a menu bar with options like Delete, Download, and Print Badge. Three callout boxes provide additional information: a green box lists actions available from the menu bar, a red box points to the tabbed categories, and a blue box points to the General tab.

If you want to change the Department setting of multiple cardholders in a single batch process, see ["How to edit the details of multiple cardholders from a single set of cardholder details" on page 217](#).

3. In the General tab, **Mouseover**<sup>1</sup> the Department field and select a department from the drop-down list.
4. After selecting a department, click one of the **Save** options in the action bar. The cardholder details are updated in the Cardholder Report table and saved in the system database.

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

# Deleting a Department

Use the following steps to delete an existing department via the Departments screen.



**Note:** When you delete a department, you are deleting it from the system database.

Before you can delete a department from the system, you must first change any cardholder's Department setting, where the cardholder's assigned department is the one that will be deleted. For more information, see ["How to edit the details of multiple cardholders from a single set of cardholder details" on page 217](#).

In addition, if the department intended to be deleted has a sub-department, the sub-department must be deleted before the parent department can be deleted.

## How to delete a department

These instructions assume that the department is not assigned to a cardholder.

1. Go to the Management Task group and click **Departments**. The Departments screen is displayed.
2. From the list of existing departments on the left side of the screen, select the department that will be deleted. The department's parameters are displayed.
3. Click **Delete** and confirm the operation. The department is removed from the screen and the system database.

# Departments: MultiSite Impact

Each site has its own departments. Departments cannot be shared with other sites. The name of the site that owns a department appears in the department's details.

The built-in Root site department is not accessible and cannot be assigned to a cardholder by any user. All other departments appear below the Root site department in the Department tree.

The Department tree shows all departments where the logged-in user has authorization.

If the user is a super user and the department is owned by the Root site, the user will be able to select the department and edit it. This Root site department cannot be shared. A non-super user can add departments where they have authorization. The Default Multiple Access Groups available to a department must be owned by the same site as the department.

## Add a Department

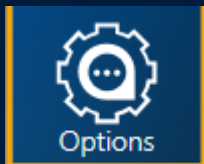
1. Select an existing department (i.e. the Root Departments).
2. From the Action menu, click **New**.
  - » If the built-in Root "Departments" is in focus, select the site that will own the new department. This is especially relevant for users who have authorization to more than one site.
  - » If the Area in focus is not the root Departments, the new department will have the same owner as the department in focus and will appear as a sub-department of the department in focus.
3. (Optional) Select a **Default Multiple Access Group** for the department and click **Save**.

If **Default Multiple Access Group** is set to **Anytime Anywhere**, a cardholder, of type visitor, will bypass the default setting and initially be set to **No Access**.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 10:

## Options



The Options screen manages GuardPoint10's appearance, behaviors, and file location preferences. All operators share the same options regardless of who is logged in or which workstation is running the GuardPoint10 GUI.

## Changing Option settings

Use the following steps to change an option setting via the Options screen.



**Note:** Changes made to the option settings are comprehensive. They will be applied to all instances of GuardPoint10 regardless of the operator logged in or the workstation running GuardPoint10.

## How to change option settings

1. Go to the Setup Task group and click **Options**. The Options screen is displayed.
2. Select an option category and make your changes. For information about the various settings available, see "[Options Screen](#)" on page 567.

To restore a single option setting to GuardPoint10's built-in default configuration, right-click the current setting, and then select **Restore Default** from the context menu.

3. After making your changes, click **Save**. The changes will be applied to all future GuardPoint10 sessions.

## Restoring Default Options Settings

Option settings are stored in the system database and are restored to a previous point by restoring an entire system database, however, this will restore everything in the database, not just the options.

Alternatively, you can restore all options settings to those found after the initial installation of GuardPoint10 -the default settings.

### How to restore all default options settings

1. Go to the Setup Task group and click **Options**. The Options screen is displayed.
2. Click **Restore Default** in the action bar, and then confirm the operation. The options settings revert to GuardPoint10's default initial option settings.



# System Database and Journal Management Options

System database journal and management includes the following options from the **SQL Server Options** drop-down list, found at the top of the Options screen's System & SQL tab:

- » Backup Database
- » Backup Journal
- » Restore Database
- » Restore Journal



**Warning:** The Restore Database and Restore Journal actions are only available on the GuardPoint10 Server installation where the SQL Server is installed on the same machine as the GuardPoint10 Server installation. However, you may backup a database or journal to a remote SQL Server.

## Backup a system database or journal to a Backup folder

Use the following steps to backup a system database or journal to the SQL Server's Backup folder, via the Options screen.

## How to backup a system database or journal to the SQL Server's Backup folder

1. Go to the Setup Task group and click **Options**. The Options screen is displayed.
2. Open the System & SQL tab.
3. At the top of the tab, click **SQL Server Options**. A drop-down list is displayed.
4. Do one of the following:
  - » Click **Backup Database**. The current system database is backed up in the SQL Server's Backup folder with the following naming convention:  
AC8\_<suffix><date of backup> <time of backup>.BAK
  - » Click **Backup Journal**. The current journal is backed up in the SQL Server's Backup folder with the following naming convention:  
AC8Journal\_<suffix><date of backup> <time of backup>.BAK

## Restore system database or journal from a Backup folder

Use the following steps to restore a system database or journal from the SQL Server's Backup folder, via the Options screen.

# How to restore a system database or journal from the SQL Server's Backup folder

1. Go to the Setup Task group and click **Options**. The Options screen is displayed.
2. Open the System & SQL tab.
3. At the top of the tab, click **SQL Server Options**. A drop-down list is displayed.
4. Do one of the following:

## Select Restore Database:

A File Explorer opens and displays the content of the SQL Server's Backup folder. Select the database that will be restored, and click Open. The database restore process begins.

The database restore process will automatically close or stop all opened GuardPoint10 instances (Server and Workstation) and restart the GuardPoint10 services.

The GuardPoint10 services can be monitored from the GuardPoint10 Watchdog application found on the GuardPoint10 Server machine. When the last line in the Watchdogs log reads "UI can be relaunched.", the database is restored and GuardPoint10 can be relaunched.

To determine which file to restore, take advantage of the backup naming conventions. The naming convention is:

AC8\_<suffix><date of backup> <time of backup>.BAK



**Note:** Option settings are stored in the database and will be restored along with other system data.



**Note:** After restoring a database, a best practice is to initialize controllers. This will resolve any residual data issues that may be in a controller's memory from before the restore operation.

## Select Restore Journal:

A File Explorer opens and displays the content of the SQL Server's Backup folder. Select the journal that will be restored, and click Open. The journal restore process begins.

The journal restore process will automatically close all opened GuardPoint10 instances (Server and Workstation) and restart the GuardPoint10 services.

The GuardPoint10 services can be monitored from the GuardPoint10 Watchdog application on the GuardPoint10 Server machine. When the last line in the Watchdogs log reads "UI can be relaunched.", the database is restored and GuardPoint10 can be relaunched.

To determine which file to restore, take advantage of the backup naming conventions. The naming convention is:

AC8Journal\_<suffix><date of backup> <time of backup>.BAK



**Note:** Part of the restore process includes an automatic backup of the current journal or system database. The automatic backup will have the following naming convention:

AC8Journal\_<suffix>\_ BeforeRestore\_<date of backup> <time of backup>.BAK

or

```
AC8_<suffix>_BeforeRestore_<date of backup> <time of backup>.BAK
```

## Automatically archive the GuardPoint10 journal

Use the following steps to set up the automatic archive process for the current journal. The automatic archive process starts when the GPPServer service is restarted. The GuardPoint10 services are restarted atmospherically as part of the system maintenance process. The system maintenance process time is set in the Options > General screen.

### How to set up the journal's automatic archive process

1. Go to the Setup Task group and click **Options**. The Options screen is displayed.
2. Open the **System & SQL** tab.
3. Set **Archive Journal** to **Yes**. The related fields are enabled.
4. In **For Events Older Than (in Days)**, enter the number of days that the entry must be older than to include in an archive.
5. In **Max Rows per Archive (in Millions)**, enter the maximum number of entry rows allowed per archive. After the limit is reached, a new archive will be automatically started.
6. Click **Save**.
7. Go to the **Options > General** tab and set **Restart Services every night** to **Yes**, and then specify a **restart time**.
8. Click **Save** again.

An archived journal name includes a timestamp indicating the date and time the archive was created (YYYYMMDDHHMM).

To learn how to view an archived journal, see "[Changing Event History Report Table View](#)" on [page 254](#).

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 11:

## Video (Setup) and NVR/DVR



The Video Setup screen is used to construct a logic tree. A logic tree is a representation of the GuardPoint10-linked NVR/DVR's structure, as it pertains to a camera's relationship to a space, reader, or input within the GuardPoint10 ecosystem. Operators use the logic tree in the Video Security screen and the Security Center screen to display video streams from a selected camera. The Video Security screen is GuardPoint10's CCTV client.

The NVR/DVR screen is where connections between GuardPoint10 and third-party NVR/DVR systems are defined. In addition, the NVR/DVR screen is where the rules governing the behavior established by the connection to the NVR/DVR systems and the Video Security screen are configured.

Through GuardPoint10's user interface, the Video module works hand-in-hand with the NVR/DVR to provide the following:

- » Live and playback video records
- » Video/Picture side by side comparison
- » Snapshots
- » PTZ control
- » Access-based video monitoring
- » Alarm-based video monitoring

### For example:

After an intrusion is detected (alarm), security personnel (an GuardPoint10 operator) monitoring the situation via the Video Security screen can investigate the alarm event from the screen, with the available cameras, and determine if a genuine break-in is taking place.

If a break-in is in progress, the operator may lock/unlock doors or arm/disarm the corresponding alarm zone to stall the intruder and allow roaming security personnel to detain them.

These, and other, actions such as monitoring the real-time status of each door (opened/closed, locked/unlocked) may be performed via the Video Security screen and the Security Center screen.

To make operator supervision easy and intuitive, readers, inputs, cameras are organized in a logic tree structure via the Video Setup screen. The logic tree is provided as a framework for selecting views in the Video Security screen and camera icon links in the Position screen.

## Configuring a Video NVR/DVR connection



**Note:** The configuration information needed to integrate an NVR or DVR into your GuardPoint10 system should be acquired from your network administrator.

### How to configure or edit a Video Logic tree

1. Go to the Setup Task group and click **NVR/DVR**. The NVR/DVR screen is displayed (see "[Video NVR/DVR Screen](#)" on page 678).  
If an NVR/DVR connection is already configured, it will be listed on the left side of the screen.
2. Click **New**. Fields appear to the right of the list of existing NVR/DVR connections.
3. In the Name field, enter a name that best describes the NVR/DVR.
4. Enter the information provided by your network administrator in the remaining fields.

The Active button, when set to YES, will enable cameras in the logic tree to interact with GuardPoint10 in the Video Security screen.

If you are using (Onssi) Ocularis version 5.4 or older:

- a. Install the Ocularis client on each GuardPoint10 workstation.
- b. In the NVR/DVR screen create the NVR and select the **Onssi** type.
- c. Close GuardPoint10 GUI.
- d. Open a command prompt as an administrator, go to the `./GuardPoint10/Gui` folder and launch the `Onssi.bat` file.

If you are using Seetec, Cayuga, or (Onssi) Ocularis version 6:

- a. In the NVR/DVR screen create the NVR and select the **Qognify** type.
- b. Close GuardPoint10 GUI.

- c. Open a command prompt as an administrator, go to the `./GuardPoint10/Gui` folder and launch the `Qognify.bat` file.

## Delete/Duplicate NVR/DVR connection

1. Go to the Setup Task group and click **NVR/DVR**. The NVR/DVR screen is displayed.
2. From the list of saved NVR/DVR, select an NVR/DVR connection that will be deleted or duplicated.
3. Do one of the following:
  - » Click **Delete** and confirm the operation. The NVR/DVR connection is deleted from the system database.
  - » Click **Duplicate**. The NVR/DVR connection is duplicated on the right side of the list.  
The name of the NVR/DVR connection is appended with "\_Duplicated" and the **IP address** field is blanked.

## Discard NVR/DVR connection

1. Go to the Setup Task group and click **NVR/DVR**. The NVR/DVR screen is displayed.
2. From the list of saved NVR/DVR, select an existing NVR/DVR connection or add a new NVR/DVR connection.
3. Change a value in the fields to the right of the list of existing NVR/DVR connections.
4. Click **Discard**. The NVR/DVR connection settings revert to their last saved version.

# Configuring & Editing the Video Logic Tree



**Note:** It is important to understand that the Video Module is not an NVR or DVR, but rather interfaces with your existing NVR or DVR to integrate its functionality into GuardPoint10 features, via the Video Security screen and the Security Center screen.

Before configuring Video Setup, contact the SENSOR support team for instructions on establishing connectivity between your particular NVR/DVR and GuardPoint10.

## How to configure or edit a Video Logic tree

1. Go to the Setup Task group and click **Video Setup**. The Video Setup screen is displayed (see "[Video Setup Screen](#)" on page 519).  
If this is the first time the logic tree is being configured, the logic tree will only have a Root element.  
If a configuration already exists, it will be visible on the left side of the screen.
2. From the logic tree, place Root in focus and click **New**. Fields appear to the right of the logic tree.
3. From the **Type** field, select **Area**, and in the **Name** field enter the name of the area where the reader(s) input(s) camera(s) will be located.

The name should be descriptive. An operator monitoring the Video Security screen should be able to recognize the location from the name alone.



**Note:** The area item is optional. At any point, you can add a reader, input or, camera to the Root.

4. (Optional) Enter a description of the area.

Generally, the description identifies the borders of the area and something about the cardholders who work in the area.

5. Click **Save**. The Area appears in the logic tree with an identifying icon.
6. After saving the area add one or more of the following to the area:

#### **Add a sub-area (a subset of the previously created area).**

- a. From the logic tree, place what will be the parent area in focus and do one of the following:
  - » Click **New**. Fields appear to the right of the logic tree.
  - » Right-click an area and select **Add** from the context menu. Fields appear to the right of the logic tree.
- b. From the **Type** field, select **Area**, and in the **Name** field enter the name of the new sub-area where the reader(s), input(s), or camera(s) will be located.

The name should be descriptive and recognizable.
- c. (Optional) Enter a description of the sub-area.

Generally, the description identifies the borders of the sub-area and something about the cardholders who work there.
- d. Click **Save**. The sub-area appears in the logic tree, under its parent area with the same identifying icon as the parent.

#### **Add a reader to an area**

- a. From the logic tree, place the area where the reader will be located in focus and do one of the following:
  - » Click **New**. Fields appear to the right of the logic tree.
  - » Right-click the area and select **Add** from the context menu. Fields appear to the right of the logic tree.
- b. From the **Type** field, select **Reader**, and in the **Reader** field drop-down list, select a reader.

The list of readers is generated from the NVR or DVR connected to GuardPoint10.
- c. (Optional) Enter a description of the reader.

Generally, the description identifies the reader's location and purpose.
- d. Click **Save**. The reader appears in the logic tree under its parent area with an identifying icon.

#### **Add an input device to an area**

- a. From the logic tree, place the area where the input will be located in focus and do one of the following:



- » Click **New**. Fields appear to the right of the logic tree.
  - » Right-click the area and select **Add** from the context menu. Fields appear to the right of the logic tree.
- b. From the **Type** field, select **Input**, and from the **Input** field's drop-down list, select an input.

The list of inputs is generated from the NVR or DVR connected to GuardPoint10.
  - c. (Optional) Enter a description of the input.

Generally, the description identifies the input's location and purpose.
  - d. Click **Save**. The input appears in the logic tree under its parent area with an identifying icon.

### Add a camera to an area

- a. From the logic tree, place the area, reader, or input where the camera will be located in focus and do one of the following:
  - » Click **New**. Fields appear to the right of the logic tree.
  - » Right-click the area, reader, or input and select **Add** from the context menu. Fields appear to the right of the logic tree.
- b. From the **Type** field, select **Camera**. A Provider field appears.
- c. Select the NVR/DVR provider where the camera is connected, and in the **Camera** field drop-down list, select an existing camera recognized by GuardPoint10.

The list of cameras is generated from the NVR or DVR connected to GuardPoint10.
- d. (Optional) Enter a description of the camera.

Generally, the description identifies the camera's location and purpose (i.e. "Behind the tree and pointed at the front door.").
- e. Click **Save**. The camera appears in the logic tree under its area with an identifying icon.



**Note:** A camera that is not a subelement of a reader or an input in the logic tree is constantly on and has no activations triggers.

7. Repeat the steps above to add additional elements.



**Note:** You can only add an area to the Root or other areas.

If multiple cameras are connected (subelements) to a reader, the first camera listed will be the primary camera. This means that in the Video Security screen the primary camera's video stream will display in a tile if triggered by an event (i.e. a badge swipe). A secondary camera's video stream may be displayed by selecting it from the tile's context menu.

The configured logic tree will appear on the left side of the Video Security screen.

## Deleting elements

1. Go to the Setup Task group and click **Video Setup**. The Video Setup screen is displayed.
2. From the logic tree, select the camera, reader, input, or area that will be deleted.

3. Do one of the following:

- » Click **Delete** and confirm the operation. The element and any subelements are deleted from the system database and the logic tree.
- » Right-click the element in the logic tree and select **Delete** from the context menu, and then confirm the operation. The element and any subelements are deleted from the system database and the logic tree.

# Video Setup: MultiSite Impact

This topic will address NVRs/DVRs and the Logical tree.

## NVRs/DVRs

Each site has its own NVRs/DVRs. These NVRs/DVRs cannot be shared with other sites. However, the same NVR/DVR can be added to multiple sites.

The name of the site that owns an NVRs/DVRs appears below the NVR/DVR name.

## Add an NVR/DVR

If the logged-in user has authorization to more than one site, they must select the site that will own the new NVR/DVR via the **New** button's drop-down list.

## Logical tree

When a site is added via the infrastructure screen, a corresponding site element is automatically added to the Logical tree. A user sees all sites in the Logical tree where they have authorization.

## Add assets to the Logical tree

A user can only add assets, including cameras, to a site in the logical tree where the site owns the asset or, in the case of readers and inputs, the asset is shared with the site.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 12:

## Event History



The Event History screen shows each event that takes place in the GuardPoint10 ecosystem that was recorded in the system database. The Event History screen manages these events and creates a concise, legible Event History report that can be shared with relevant personnel.

Through Event History management, you may do the following:

- » Choose the type of event(s) that will appear in the Event History report. The available types are:
  - » Access
  - » Alarms
  - » Tech. Alarms
  - » Comm. Alarms
  - » Audit
  - » Galaxy Audit (relevant where a Galaxy panel is incorporated into the GuardPoint10 ecosystem)
  - » General Events
- » Group, filter, or sort data in the Event History Report table.
- » Determine the columns that will appear in an Event History Report table.
- » Export an Event History Report table to Excel, PDF or print a hardcopy of a report via a printer on your network.

# Load and View a Previously Archived Journal

This topic assumes that automatically archived journals already exist in GuardPoint10's SQL Server. To learn how to set up the journal's automatic archive process, see ["Automatically archive the GuardPoint10 journal" on page 241](#).

## How to load and view a previously archived journal

1. Go to the Management Task group and click **Event History**. The Event History screen is displayed.
2. To the right of the Event Type bar there is a drop-down field showing the currently displayed journal's name.
3. Click the down arrow in the drop-down field. A list of previously archived journals appears each journal name includes a timestamp indicating when the archive was made.
4. Select the journal that will be loaded in the Even History screen. The journal is loaded in the Even History table.

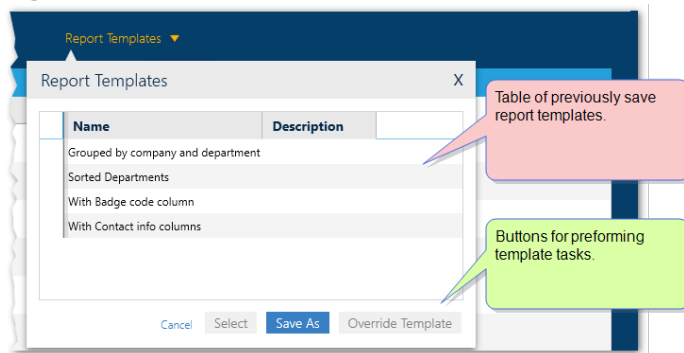
# Manage the Cardholder Table Layout with Templates

## Report Template dialog

The structure of the screen table can be saved in a template so it can be applied later, either to the screen display or a global reflex ["Create Template-based report" on page 548](#) action. The data in a template is dynamic and will change to reflect the environment.

To start using templates click the **Report Templates** button.

Figure 12-1



The table in the Report Template dialog contains the names and descriptions of previously save templates, which are specific to the screen displayed.

From the screen's Report Template dialog you can click:

- » **Save As:** Opens the ["Report Template Screen" on page 529](#), where the current structure of the displayed table can be saved.
- » **Override:** Opens the ["Report Template Screen" on page 529](#), where the current structure of the displayed table can override the last selected template with the current structure of the displayed table.
- » **Select:** Displays current data in the template selected from the dialog's table.

# Changing Event History Report Table View

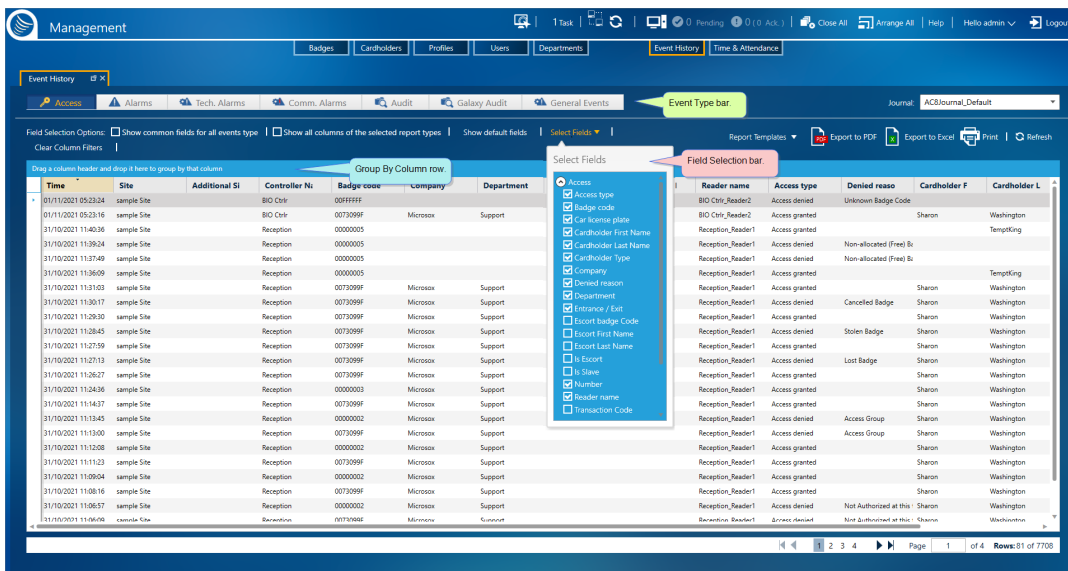
The Event History table is handled as a report and is therefore referred to as the Event History Report table.

Because the Event History Report table can be very large and difficult to manage, additional view options have been added to the standard group of filters and sorts available in most other GuardPoint10 tables (see "Event History Screen" on page 631).

## How to change the Event History Report Table View

1. Go to the Management Task group and click **Event History**. The Event History screen is displayed.
2. From the Event Type bar, select the type(s) of events you would like to include in the Event History report (Access, Alarms, Tech. Alarms, Comm. Alarms, General Events, or Audit). The Event History Report table change to reflect your selection.
3. From the Field Selection Options bar, just above the report bar table, select the required view options. The report table columns change appearance according to your selection. The image below illustrates just one of the view options available in the Field Selection Options bar.

Figure 12-2



## Generating Event History Report Output (PDF, Excel, or Print)

You can generate a standard or customized Event History Report by changing the view of the table. Before you generate a report, decide on the format that best satisfies your requirements. GuardPoint10 can generate reports in PDF and XLS formats. There is an additional option to print a hardcopy of your report via a selected printer.

After generating a report file or printing a hardcopy, you can distribute the report to the relevant personnel.





**Warning:** Some of the data in the Event History Report may be confidential.

## How to generate an Event History Report

1. Go to the Management Task group and click **Event History**. The Event History screen is displayed.
2. Display the Event History Report table columns the way in which you would like them to appear in the exported report. To change the view of the table, see "[Load and View a Previously Archived Journal](#)" on page 252 and "[Event History Screen](#)" on page 631.
3. After adjusting the Event History Report table view, do one of the following:

### Export to PDF

- a. Click **Export to PDF**. A Print Report dialog is displayed.
- b. Enter a report title name and click **Export**. A file browser opens.
- c. Enter a file name and select a location for your PDF file, and then click **Save**. The file is generated and saved in the specified location.

### Export to Excel

- a. Click **Export to Excel**. A Print Report dialog is displayed.
- b. Enter a report title name and click **Export**. A file browser opens.
- c. Enter a file name and select a location for your XLS file, and then click **Save**. The file is generated and saved in the specified location.

### Print a Hardcopy

- a. Click **Print**. A Print Report dialog is displayed.
- b. Enter a report title name and click **Print**. A Print Preview window opens.
- c. Review the pages of the report and; if necessary, change the page orientation.
- d. Click the **Print** button. A Printer Preference dialog is displayed.
- e. Select your preferences and click **Print**. A hardcopy of the report is printed at the specified printer.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 13:

## Time & Attendance



The Time & Attendance screen provides operators with a hassle-free, automated timesheet report generator. Each cardholder selected is included in the report file, as long as they had an access event within the selected date range. And if selected, that access event took place at an Entrance or Exit reader.

The report includes a cardholder's start and stop times per day, the total hours for their day, and any comments relevant to the day. In addition, a cardholder's individual report displays the total number of days and hours a cardholder worked, in the specified range, at the bottom of a report.

The Time & Attendance module produces an on-demand timesheet report based on selected criteria. After a report is generated and viewed online, it may be exported to one of many different formats and even printed via a networked printer.

# Generating a Timesheet Report & Exporting the Report

A Time & Attendance Timesheet report consists of a cardholder's name and a table row for each day that the cardholder was present at the workplace. Each row includes the time the cardholder first entered and last exited the workplace followed by the total hours for that day. Below the table is the total number of hours and days that a cardholder was at the workplace for the specified date range of the report.

A Timesheet report may contain information about one or more cardholders. Each cardholder's name is preceded by a page break in the screen view. This means that each cardholder's information starts on a new page.

For information about the Time & Attendance screen, see "[Time & Attendance Screen](#)" on page 641.

## How to generate a Timesheet report

1. Go to the Management Task group and click **Time & Attendance**. The Time & Attendance screen is displayed.
2. From the top left of the screen, select the date range that will be included in the report.
3. (Optional) If there are designated readers for entrance and exit events and you want to use the timestamps recorded from those respective readers, select the **Only Entrance/Exit Readers** checkbox. If not, the report will use the first and last reader entrance/exit events of each day, regardless of the reader they came from.
4. From the Truncated Cardholders table, select one or more cardholders to include in the report.

Use one of the following methods to select multiple cardholders:

- » Press **Alt** and click cardholder rows in no particular order. Each selected cardholder row will be included in the report.
  - » Drag the mouse across multiple rows. Each cardholder row covered by the drag action will be included in the report.
  - » Press **Ctrl + A** to select all rows in the table. All cardholders in the table will be included in the report.
5. After selecting cardholders, click the **Display Report for Select Cardholders** button. The report will be displayed in the Report View area to the right of the table.

At this point, you may page through the report or export the report as required.

## How to export a generated Timesheet report

A Timesheet report may be exported to a file in one of the following formats.

- » PDF
- » CSV (comma separated values)
- » Excel
- » RTF (Rich Text Format)

» TIF

» MHTML (Web Archive - saves as web page content and incorporates external resources)

1. After generating a Timesheet report, from the Report View area toolbar, click the Export button. A rollout listing of all the available formats is displayed.
2. Select a format. A File Save As dialog appears.
3. Select a folder location and name the file that will contain the report, and then click **Save**. The file is saved in the selected format.

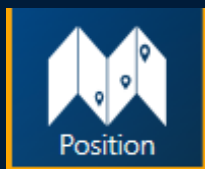
Alternatively, you can send the report to a networked printer and print a hardcopy.

1. From the Report View area toolbar, click the **Print Report** button and select a printer from the dialog.
2. After selecting a printer, click **Print**. A hardcopy is printed at the select printer.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 14:

## Position



The Position screen is where the Security Center environment is built.

The Position screen integrates your physical security system entities (i.e. alarm detectors, readers, etc.) with dynamic icons layered on top of maps, creating a virtual representation of the GuardPoint10 ecosystem. The maps present a geographic location (i.e. floorplan) within your environment where the icons, representing the different parts of your system, alert operators to the state of the element, represented by the icon, and events triggered from the element.

### **For example:**

A door icon shows if the door is physically open or closed, the state of the relays controlling it ('Normally Open' or 'Normally Closed'), if an override state is currently in place, and whether alarms associated with it have been acknowledged and confirmed.

Operators build layers of icons and link them to various parts of the system (controllers, readers, inputs, cameras, etc.) to approximate your system's physical layout. By placing each icon on a map layer in the same general location where the physical element linked to it is located in the real world, an operator can detect changes and patterns, and quickly take any required action based on the nature of an event and its proximity to sensitive spaces.

A predefined area may also be linked to an icon, shape, or textbox. This provides a method to track cardholder occupancy for the area.

A palette's dynamic icons are added to a map with a simple drag&drop. New palettes, and their content, can be added and customized to fit the needs of the ecosystem as needed via the Position screen and, for new icons, a third-party product called Inkscape.



# Managing a Map Tree

The map tree is made up of groups and maps. Groups are used to apply a layer of organization to the tree that may not be available with a standard map sub-map relationship model.

Use the following steps to manage the map tree via the Position screen.

## How to add a group to the map tree

The Position screen's map tree comes with a built-in group called Site\_1. You can change the name of the group at any time. The point is that there will always be an initial group to build out from.

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. In the map tree, select a preexisting group. The group's parameters appear to the right of the icon pallet. Above the map tree, the **Add Group** and **Delete Group** buttons are enabled.  
A folder icon precedes all group names.
3. Click **Add Group**. A new group appears in the map tree as a sub-group of the group previously in focus. In addition, parameters for the new sub-group appear to the right of the icon pallet.  
Alternatively, right-click on an existing group and select **Add Group** from the context menu. A new group will appear in the tree as a sub-group of the previously selected group.
4. Rename the new group to something recognizable by other operators and, if necessary, enter a description.



**Note:** The group name must be unique to all other groups.

5. Click **Save**. The group information is saved in the system database.  
After a group is saved it can be moved to a new location in the tree with a simple drag and drop mouse action. Any maps in the group will move with the group in this action.

## How to add a map page to the map tree

In the tree, a circle icon precedes all map page names.

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. In the map tree, select a preexisting group or map page.  
If you selected a group, the group's parameters appear to the right of the icon pallet. Above the map tree, the **Add Group** and **Delete Group** buttons are enabled.  
If you selected a previously added map page, the page's parameters and layout appear to the right of the icon pallet. Above the map tree, the **Add Map** and **Delete Map** buttons are enabled.
3. Click **Add Map**. A new map page appears in the map tree as a sub-group of the original group, or map page previously in focus. In addition, parameters for the new map page along with a blank page appear to the right of the icon pallet.  
Alternatively, right-click on the parent group or map page and select **Add Map** from the context menu.
4. Click The Browse button and select an image to use as a map (icons will be placed on top of the map).

The map image file size limit depends on the memory available on the machine. However, a very wide image, regardless of the file size, may have issues resizing and displaying on the screen.

5. Rename the new map page to something recognizable by other operators and, if necessary, enter a description.



**Note:** The map page name must be unique to all other map pages, regardless of their group.

6. Click **Save**. The map page information is saved in the system database.

After a map is saved it can be moved to a new location in the tree with a simple drag and drop mouse action.

## How to move a group or map in the tree

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. In the map tree, do one of the following:
  - » Select the group that will be moved. The group's parameters appear to the right of the icon pallet. Drag & drop the group on top of another group in the tree. The dragged group will be a sub-group of the group that it was dropped on.



**Note:** If a group has sub-groups (other groups or map pages), the sub-groups / sub-maps will move with the group in focus.

- » Select the map that will be moved. The map's page appears to the right of the icon pallet. Drag & drop the map on top of another map or group in the tree. The dragged map will be a sub-map of the map that it was dropped on or, put in the group it was dropped on.



**Note:** If a map has sub-maps, the sub-maps will move with the map in focus.

## How to delete a group from the map tree

In the tree, a folder icon precedes all group names.

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. In the map tree, select the group that will be deleted. The group's parameters appear to the right of the icon pallet. Above the map tree, the **Add Group** and **Delete Group** buttons are enabled.



**Note:** If a group has sub-groups or sub-map pages), the subgroups / maps have to be deleted before you can delete the group in focus.

3. Click **Delete Group** and confirm the operation. The group is deleted from the system database and no longer appears in the map tree.

Alternatively, right-click on the group, select **Delete Group** from the context menu and confirm the operation. The group is deleted from the system database and no longer appears in the map tree.

## How to delete a map page from the map tree

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.

2. In the map tree, select the map page that will be deleted. The page's parameters and content appear to the right of the icon pallet. Above the map tree, the **Add Map** and **Delete Map** buttons are enabled.

In the tree, a circle icon precedes all map page names.



**Note:** If a map page has sub-map pages, the sub-maps have to be deleted before you can delete the map page in focus.

3. Click **Delete Map** and confirm the operation. The map is deleted from the system database and no longer appears in the map tree.

Alternatively, right-click on the map page in the tree, select **Delete Map** from the context menu and confirm the operation. The map page is deleted from the system database and no longer appears in the map tree.

# Add and Manage Customized Palettes

GuardPoint10 comes with a built-in default pallet. However, you may want to add a new palette with icons specific to the needs of the environment. There are multiple ways to handle this task (i.e. new, duplicate, etc.).

Use the following steps to add and manage palettes.

## How to add and manage palettes in the Position screen

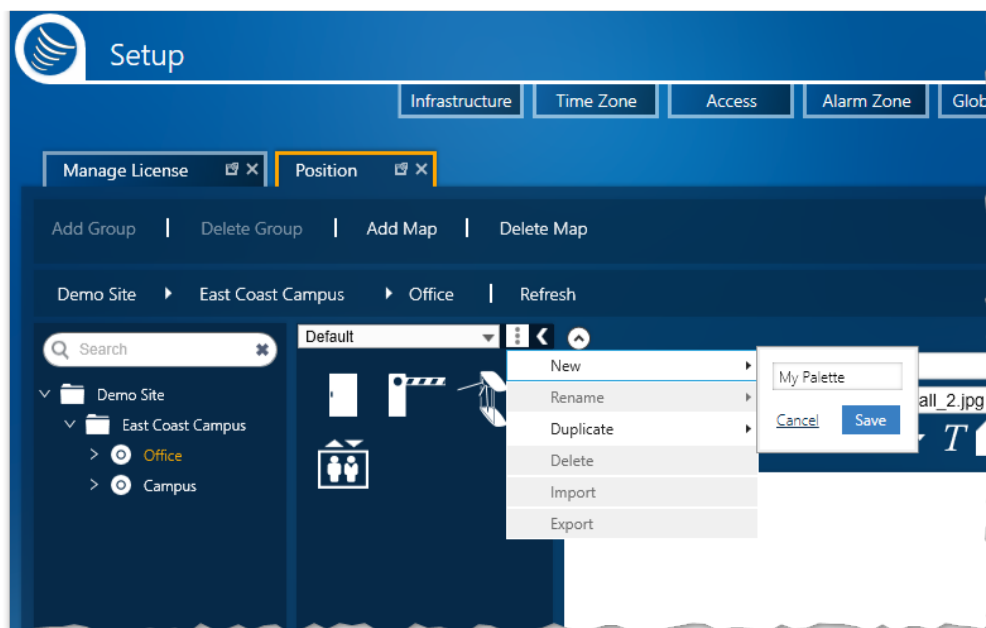
1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. At the top of the Palettes panel, select a preexisting palette from the drop-down list. The name of the built-in palette is **Default**, it cannot be deleted or customized, but it can be duplicated.
3. Expand the rollout menu to the right of the palette drop-down list and do one of the following:

### Add an empty palette

From the rollout menu, select **New**.

A field appears next to the menu item. Enter a name for the new palette, and then click **Save**. The new palette appears in the Palette drop-down list.

Figure 14-1



The palette's stencils are empty except for an **Add** icon.

### Rename a custom palette

Select a palette other than "Default" from the drop-down list, and then from the rollout menu, select **Rename**.

A field appears next to the menu item. Enter a new name for the palette, and then click **Save**. The palette appears in the Palette drop-down list with the new name.

## Duplicate the built-in palette or a custom palette

Select a palette from the drop-down list, and then from the rollout menu, select **Duplicate**.

A field appears next to the menu item. Enter a name for the new duplicate palette, and then click **Save**. The duplicate palette appears in the Palette drop-down list with the new name.

The palette's stencils contain all of the icons that are in the duplicate palette including an **Add** icon.

## Import a custom palette that was previously exported

Select a custom palette from the drop-down list, and then from the rollout menu, select **Import**. An Import XAML Palette File window is displayed.

Browse and select the palette file that will be imported. The palette will appear in the drop-down list.

If a palette with the same name already exists in the palette drop-down list, the imported palette will merge with the existing palette. This means that if an icon with the same name exists in both palettes, the icon in the imported palette will overwrite the icon in the existing palette. Other icons in the imported palette will be added to the relevant stencil in the existing palette.



**Note:** If an import process overwrites an existing icon, and the existing icon had already been placed on a map, the icon on the map will remain unchanged.

## Export a custom palette

Select a custom palette from the drop-down list, and then from the rollout menu, select **Export**. A Save As window is displayed.

Browse to the folder where the palette will be saved, and name the palette file (the file name and the palette name do not have to be the same).

Click **Save**. The palette is saved as an XML file.



**Note:** Icons from the exported palette that were previously placed on a map will remain on the map unchanged.

## Delete a custom palette

Select a custom palette from the drop-down list, and then from the rollout menu, select **Delete**. Confirm the Delete operation. The palette is removed from the drop-down list.



**Note:** Icons from the deleted palette that were previously placed on a map will remain on the map unchanged.



**Note:** The last palette added to the Palette panel will be the palette initially displayed in the panel.

After a new icon from a new pallet is added to a map, an operator may have to restart GuardPoint10 in other workstations to see an accurate display of the new icon.

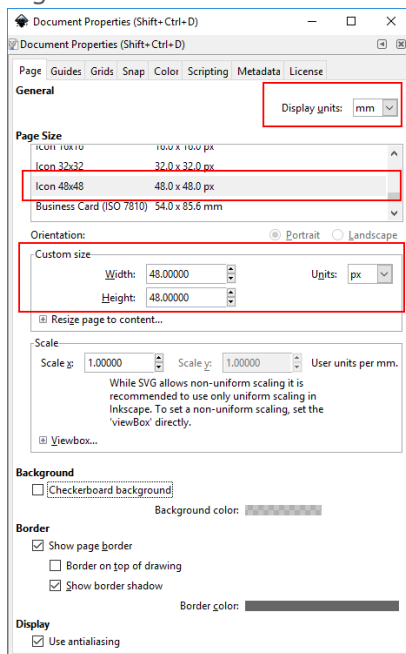
# Create XAML icons for Custom Palettes

To perform the actions in the topic, you will need the third-party free software called Inkscape.

## How to create a XAML icon for a custom palette's stencil

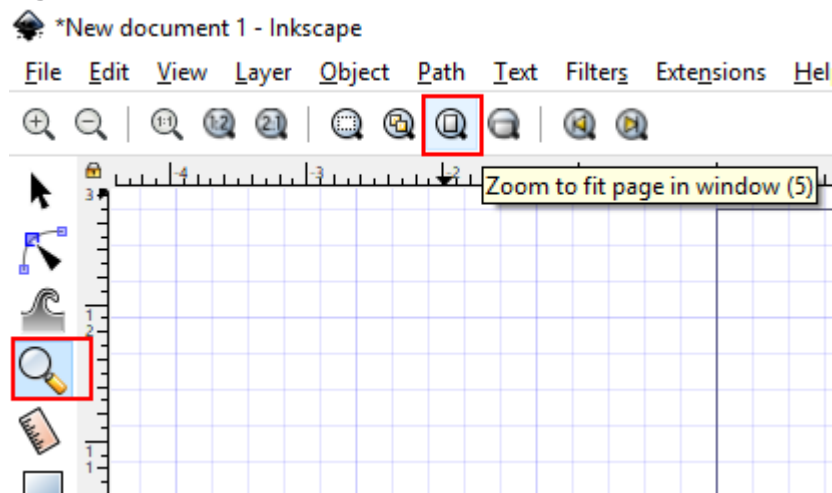
1. If necessary, download and install Inkscape from:  
[http://download.cnet.com/Inkscape/3000-6675\\_4-10527269.html](http://download.cnet.com/Inkscape/3000-6675_4-10527269.html)
2. Open Inkscape and select **File > Document Properties**. The Document Properties window is displayed.
3. In the Page tab, change the following:
  - » Display units to "px"
  - » Page size to "Icon 48x48"
  - » The Page tab should look like this:

Figure 14-2



4. Close the Document Properties window via the "X" at the top-right of the window.
5. From the Inkscape primary window, select the **Zoom** tool, and from the toolbar along the top, select the **Zoom to Fit Page in Window** option. The 48x48 px page now fills the Inkscape screen.

Figure 14-3



6. From the menu bar at the top of the window, select **View > Page Grid**. A grid appears over the page.
7. From the menu bar at the top of the window, select **View > Icon Preview**. A preview panel appears along the right side of the window.  
From the preview panel, select the 48x48 square.
8. Do one of the following:
  - » Draw an image for the icon using the available Inkscape tools.
  - » Import an existing image and resize it as required to fit the 48x48 page.
    - a. To import an image, select **File > Import**. A File Browser window is displayed.
    - b. Select the image file to import. The image appears on the page.

Best Practices:

- » When importing an image select an SVG file format for best results.
  - » Resize the image as required to fit the 48x48 page.
  - » Keep in mind the background of an icon is significant and will change color to reflect the state of the element the icon is linked to in GuardPoint10 (i.e. Armed, Disarmed, Acknowledged, etc.).
  - » Modify the image as required. You will need at least two variations of the image, depending on the palette stencil where the image will be saved.
  - » Use the Icon Preview panel to see how the icon will look when on a map in GuardPoint10.
9. When you are satisfied with the image, from the menu bar, select **File > Save as**. A File Browser window is displayed.
  10. Select a folder where the icon will be saved, and then name the file, and choose the Microsoft XAML **File type**.
  11. Click **Save**. The file is saved and the File Browser window is closed.

**Note:**

- A best practice is to save the icon image a second time as an SVG file. If you want to edit the



image in the future you will not be able to open the XAML file in Inkscape, but you will be able to open the SVG file.

- A best practice for overlay images is to reduce the size of the image to approximately 30 percent of the 48x48 pixel State icon size.

# Adding a New Icon to a Custom Palette

Before you start adding icons to your palette, verify that you have all of the variations of the icon already prepared. For example, if you're adding a new Door icon to the Door stencil (icon group) you may need seven variations of the same icon for the following states:

- » In Palette
- » Close
- » Close Under Alarm
- » Close Disconnect
- » Open
- » Open Under Alarm
- » Open Disconnected

For more information about creating icons, see ["Create XAML icons for Custom Palettes"](#) on page 269.

## How to add a new icon to a custom palette

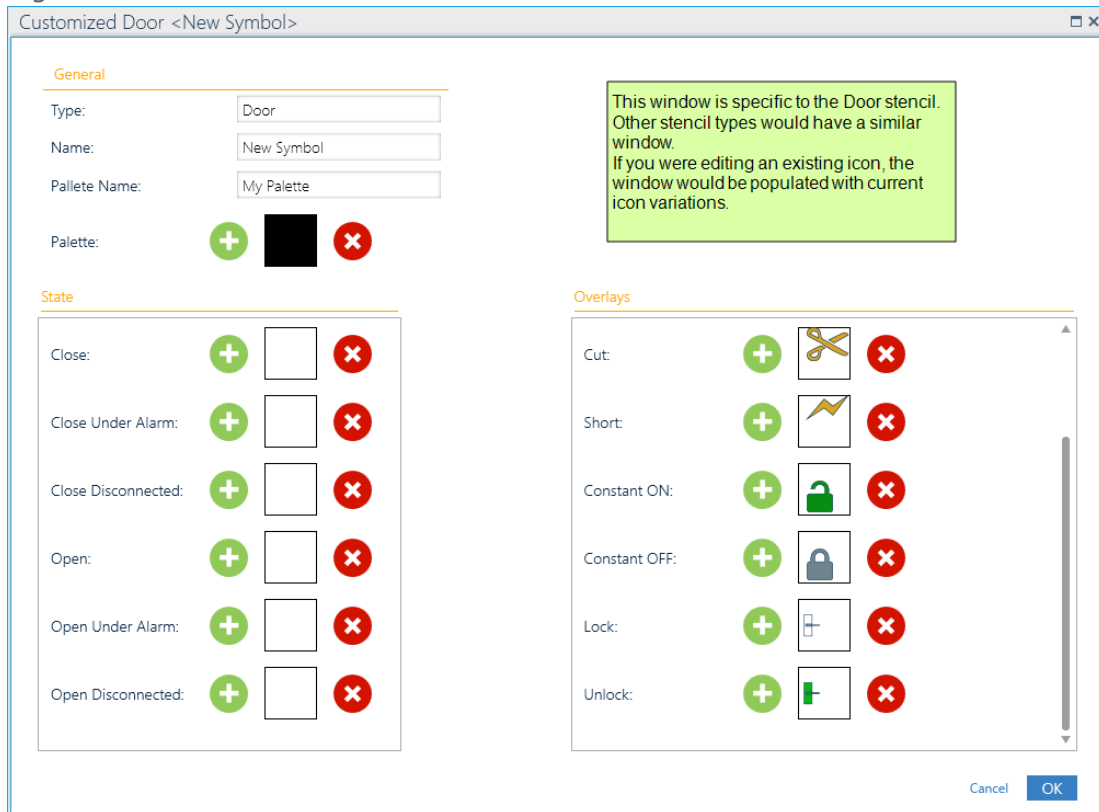
1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. Open a custom palette from the Palette drop-down list found at the top of the expandable palette panel.
3. Select the stencil (icon group) where the new icon will be placed (i.e. Door, Input, Map, etc.).



The last icon in the stencil is an **Add Icon** button. If the stencil does not have any icons in it, only the **Add Icon** button will appear in the stencil.

4. Click the **Add Icon** button. An Icon Management window is displayed.

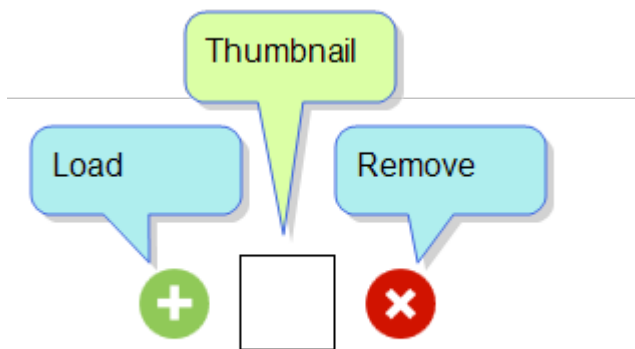
Figure 14-4



In the General area of the window, enter the icon's name in the **Name** field. This name will be used as a tooltip in the Position and Security Center screen.

5. Use the Load and Remove buttons on either side of the icon variation thumbnail to add a XAML icon file created with Inkscape. For information about creating XAML files, see "[Create XAML icons for Custom Palettes](#)" on page 269.

Figure 14-5

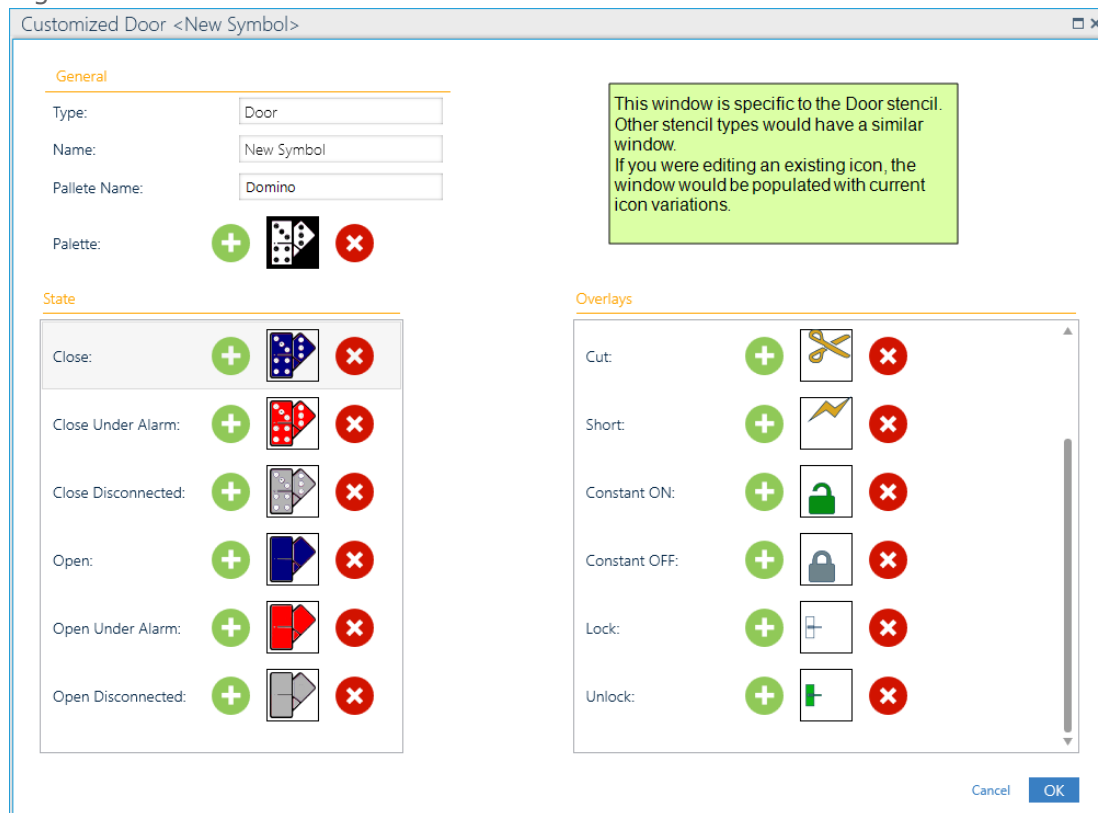


A best practice is to use the GuardPoint.ini built-in Default icon variations as a guide for your own icon variations.

If a thumbnail is left blank, the icon state will only appear with the background color and overlay -if required.

6. After loading the icon variations and making any changes to the overlay area, click **Save**. The Icon Management window is closed and the new palette icon appears in the relevant stencil.

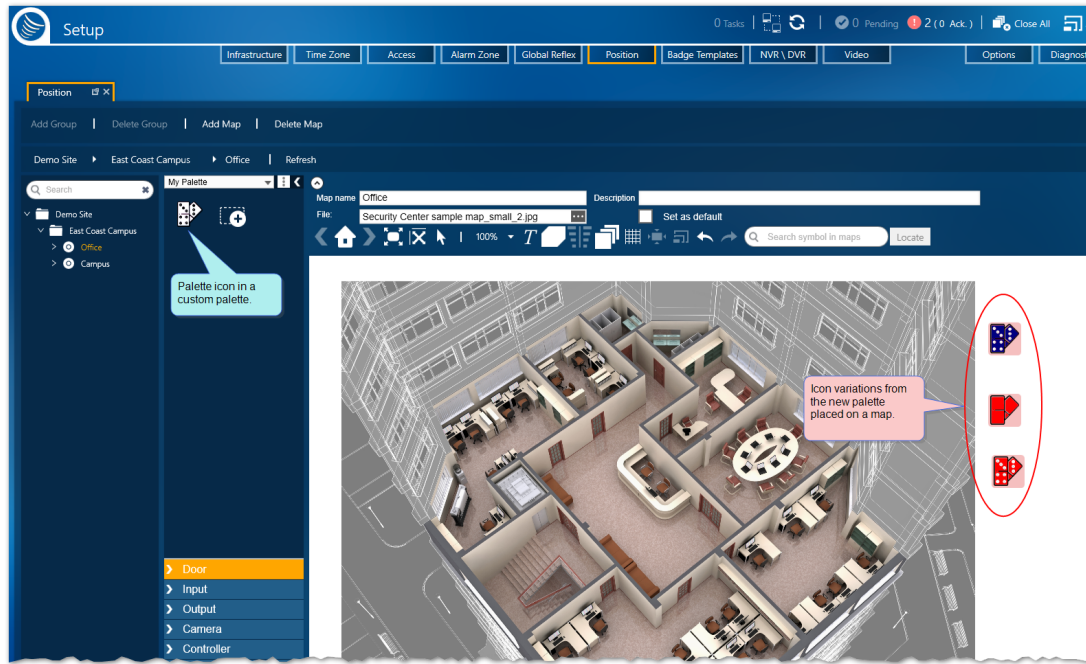
Figure 14-6



**Note:** Overlay placement and animation on an icon are fixed. For example, the default Alarm overlay is automatically placed at the top right of the icon and flashes. A replacement Alarm overlay will also be automatically placed at the top right of the icon and flash.

Position screen with the new icon.

Figure 14-7



# Edit or Delete an Icon in a Custom Palette

Icons that have already been placed on a map will remain on the map unchanged regardless of any edit or delete action taken on the icon in the palette.

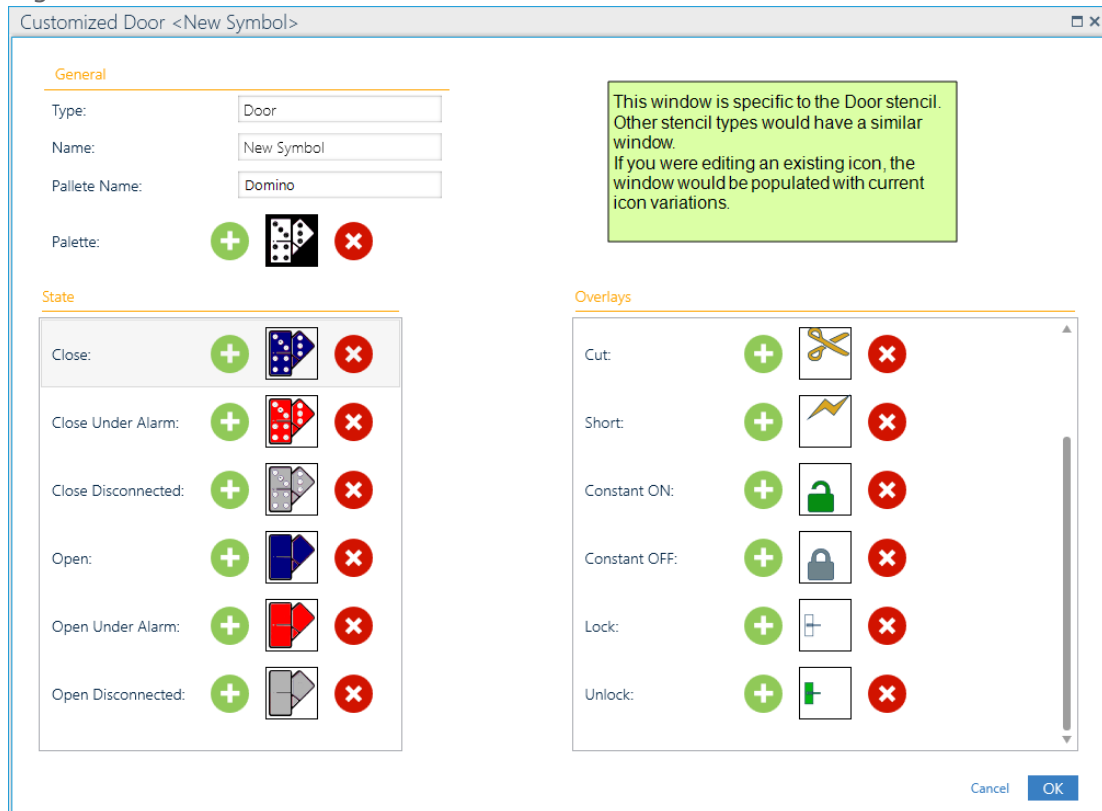
## How to edit / delete an icon in a custom palette

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. Open a custom palette from the Palette drop-down list found at the top of the expandable palette panel.
3. Select the stencil (icon group) where the icon that will be edited / removed is located(i.e. Door, Input, Map, etc.).
4. Right-click the icon in the palette and do one of the following:

### Edit an icon variation

- a. Select Edit from the icon's context menu. An Add /Edit Icon window is displayed with the icon's variations displayed as thumbnails.

Figure 14-8



- b. Replace any of the icons or change the name of the icon in the General area of the window.
- c. Click **Save**. The Add /Edit Icon window is closed and the icon is updated.

Any future drag&drop action taken with the icon will use the saved edited variation. If the icon was dropped on a map before it was edited, the icon and its variations will remain unchanged.

### **Delete an icon and its variations**

- a. Select Delete from the icon's context menu.
- b. Confirm the delete action. The icon is removed from the palette.

If the icon was dropped on a map before it was deleted from the palette, the icon and its variations will remain unchanged.

# Position: MultiSite Impact

Each site has its own Maps and Groups. These Maps and Groups cannot be shared with other sites. The name of the site that owns a Map or Group appears at the workspace, to the right of the Pallet Panel.

An icon shape, or textbox can link to assets owned by the same site as the map where it is placed, and link to assets (including Alarm Zones) that are shared with the site that owns the map.

If the logged-in user is a super user and the map in focus is owned by the Root site, the user will be able to link assets from other sites to icons, shapes or, textboxes.

## Add a Map or Group

1. Select an existing Map or Group (i.e. the Root Group).
2. From the Action menu, click **Add Group** or **Add Map**. Alternatively, click **Add Group** or **Add Map** from the context menu of the tree element in focus.

If the built-in Root Group is in focus, select the site that will own the new map or group. This is especially relevant for users who have authorization to more than one site.

If the map or group in focus is not the Root Group, the new element will have the same owner as the map or group in focus.

## Manage the tree

Maps and groups can be dragged and dropped in the tree. This means an element (map or group) can be a sub-element of another (parent) element. However, this is only allowed when the sub-element is owned by the same site as the parent element or if the parent element is the Root Group.



# What to Know About Designing a Map Page

When designing a map page, consider the operator who will be using it in the Security task group's Security Center screen. They need to easily recognize and access events and event information.

Maps or floorplans should include only the information needed to recognize a location, too much information may slow down a necessary response.

The icons, shapes or, textboxes placed on a map should be limited to those required by an operator for monitoring and analysis.

## The design process

The first step in designing a map page is loading a map image. The image can be an architectural drawing, a bird's-eye view photo, a rendering from a graphics program, etc.

After you have loaded an image on the map layer, add icons, shapes or, textboxes as required. You can link an icon / shape / textbox to a physical component in the system at the same time or you can place all of the icons / shapes / textboxes on the map and then link them to the relevant components. Use the viewing tools to make placement easier (see "[Changing the Map Page View](#)" below).

It is important to save frequently during the design stage. At any given time during the design stage, view the progress in the Security Center screen to evaluate what other operators will experience when using the Security Center screen. Keep in mind that the outcome of double-clicking an icon shape, or textbox in the Security Center screen may vary between operators. For example, the profile of some operators may not allow them to view the details of a component.

An authorized operator may edit a map page at any time. If a map page is being monitored on one PC and edited on another PC, after an operator clicks **Save** on the editing PC, the monitoring PC will refresh and display with the updates.

## Changing the Map Page View

Use the following tools to change a map page view via the Position screen.

### How to change a map page view

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. If a map page is not open on the screen, select a map page from the map tree **breadcrumbs**<sup>1</sup>. The map page parameters and map page are displayed.

When initially opened, a map page is displayed in Auto Fit view. This means that the map will zoom in or zoom out to display all elements on the map page.


3. To change the view, do one of the following:

» Click . The map moves to the top left of the page.

» Click . The zoom setting is changed to fit the map in the work area.

---

<sup>1</sup>A graphical control element used as a navigational aid in GuardPoint10' GUI. It allows operators to keep track of their current location.

- » Click . The map is displayed in full screen or exits full screen.
- » Click the magnification percentage to select a magnification setting from a drop-down list. The default magnification is 100%.

## Adding a Map Image to a Map Page

Use the following steps to add a map image to a page via the Position screen.

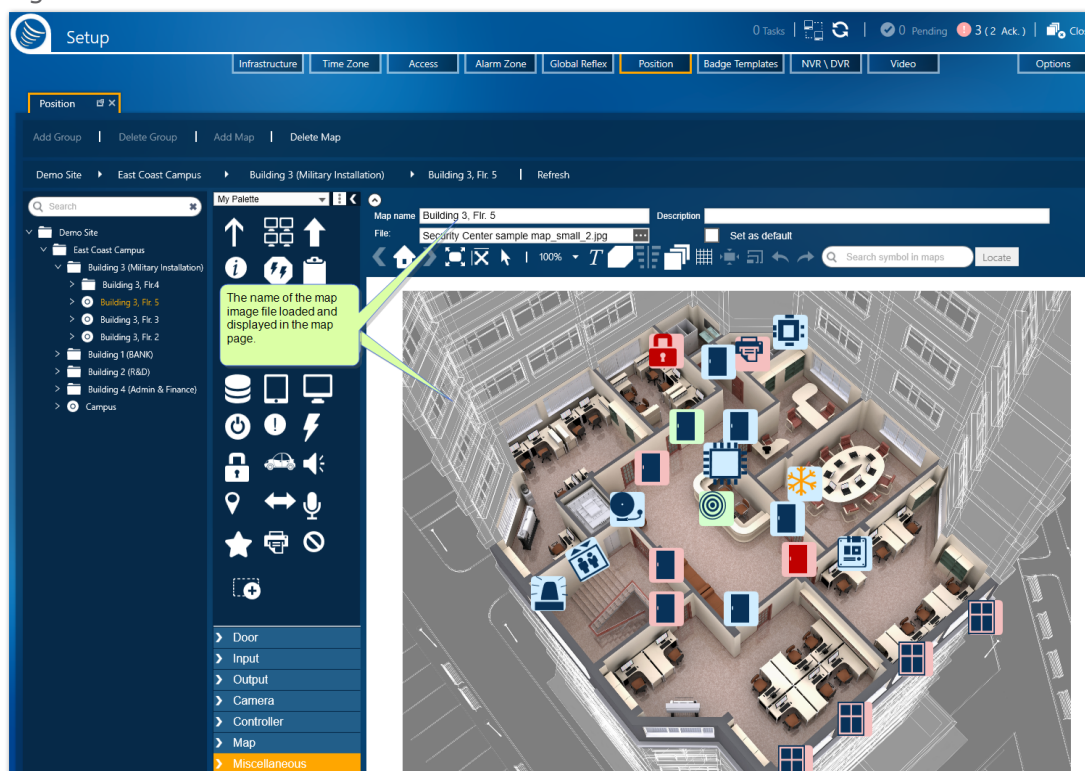
### How to add an image to the map layer of a map page

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. From the map tree or **breadcrumbs**<sup>1</sup>, select the map page where the image will be loaded. The map page parameters and page grid are displayed.

If the map page does not exist in the tree, see "[Managing a Map Tree](#)" on page 263.

3. Click the three ellipses button in the **File** parameter field. An Open File dialog is displayed.
4. Browse to the image file that you want to load onto the map page.
5. Click **OK**. The image appears on the map page and the image file name is in the File field.

Figure 14-9



<sup>1</sup>A graphical control element used as a navigational aid in GuardPoint10' GUI. It allows operators to keep track of their current location.

The map image file size limit depends on the memory available on the machine. However, a very wide image, regardless of the file size, may have issues resizing and displaying on the screen.

6. Click **Save**. The map page is saved in the system database. Map page design updates will not be visible on the Security Center screen unless it is saved.

## Adding an Icon, Shape or, Textbox to a Map Page

Use the following tools to add an icon, shape, or textbox to a map page via the Position screen.



**Note:** If your GuardPoint10 system includes an integrated Galaxy panel, elements from the panel can be placed on a map via a relevant stencil, like any GuardPoint10 element.

A Galaxy panel may be linked to a Controller stencil icon.

A Galaxy group may be linked to a Miscellaneous stencil icon, shape, or textbox.

A Galaxy zone may be linked to an Input stencil icon.

### How to add an icon, shape, or textbox to a map page

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. Open a map page, which already has a map image, via the map tree or **breadcrumbs**<sup>1</sup>.  
When initially opened, a map page is displayed in Auto Fit view. This means that the map will zoom in or zoom out to display all elements on the map page.
3. Do one of the following:

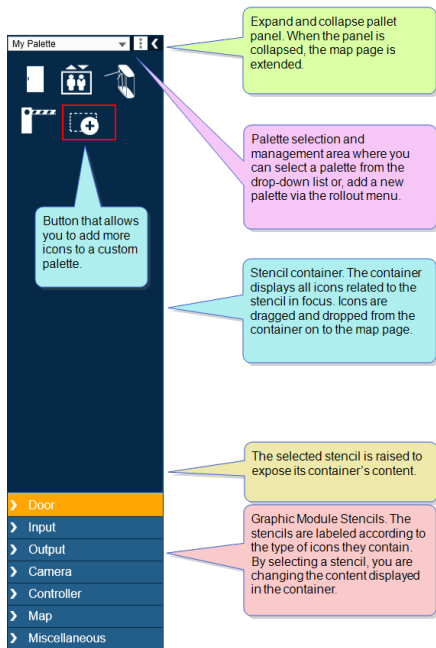
#### Add an icon

- a. Select the stencil type where the desired icon is located. The icons of the selected stencil are displayed in the icon pallet.

---

<sup>1</sup>A graphical control element used as a navigational aid in GuardPoint10' GUI. It allows operators to keep track of their current location.

Figure 14-10



- b. Drag and drop an icon from the pallet onto the map page. The icon will appear in a layer on top of the map image. An icon may be moved with the mouse pointer or nudged with the arrow keys on the keyboard.

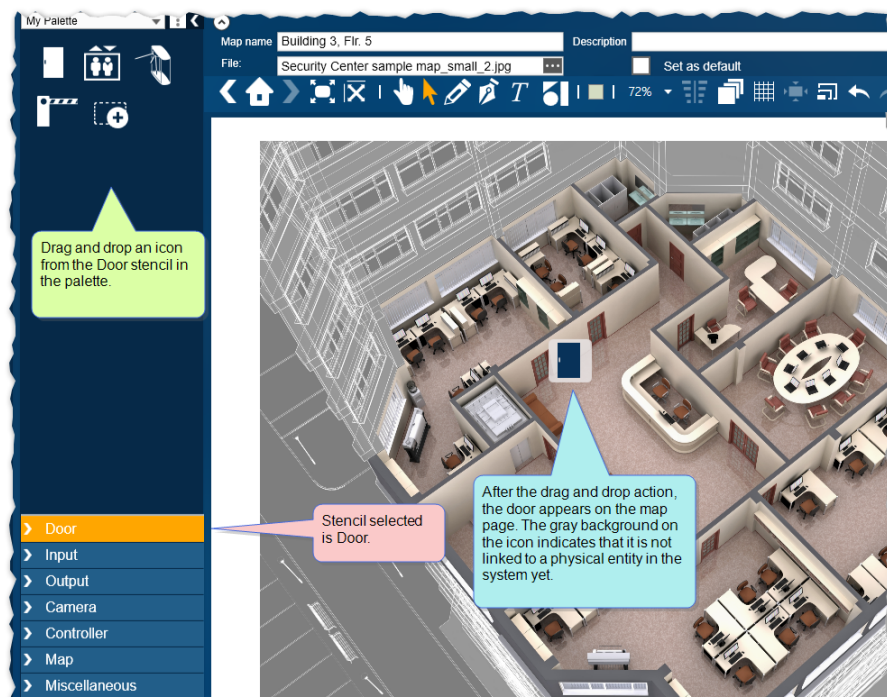


Figure 14-11

- c. After placing the icon on the map, do the following in whichever order you prefer:
- » "Linking an Icon, Shape, or Textbox" on page 284
  - » "Refining Icon, Shape or, Textbox Placement" on page 288

### Add a shape or textbox

- a. Click , , or  in the action bar above the map page.





If you select , a rollout containing available basic shapes appears. The shape color may be changed via the shape's context menu.

Figure 14-12




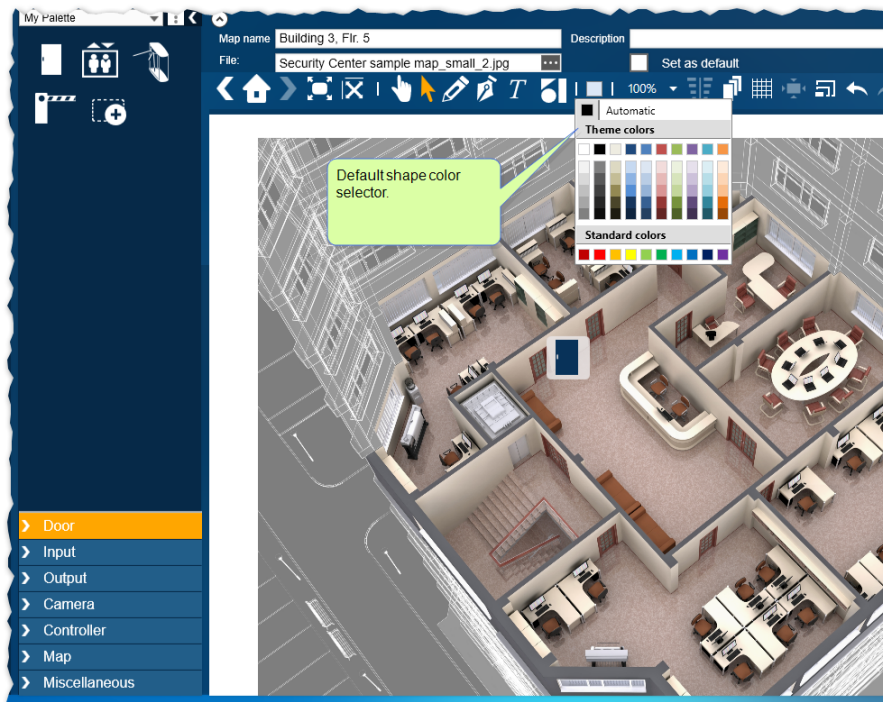
If you select  or , you will be able to draw a shape on the map. The shape color may be changed via the shape's context menu.

- b. Select a shape. A semi-transparent shape appears on the map with the default fill color.

Alternatively, click  on the action bar above the map page to place a textbox on the map. The textbox color may be selected via the box's context menu. Change the text in the box to fit your requirements and then move on to Step c.

A shape or textbox may be moved with the mouse pointer or nudged with the arrow keys on the keyboard.

- c. After placing a shape or textbox on the map, do the following in whichever order you prefer:
- » ["Linking an Icon, Shape, or Textbox" on the next page](#)
  - » ["Refining Icon, Shape or, Textbox Placement" on page 288](#)
- d. If you want to change the default color of future shapes that will be added to a map, click  and select a new default color from the displayed color palette.



Multiple icons, shapes or, textboxes on a map may be linked to the same element.

## Linking an Icon, Shape, or Textbox

Use the following tools to link an icon, shape, or textbox already placed on a map page to a component in the system.

### How to link an icon, shape, or textbox to a physical component

Multiple icons, shapes or, textboxes on a map may be linked to the same element.

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. Open a map page that already has a map image and icons, shapes or, textboxes, via the map tree or **breadcrumbs**<sup>1</sup>.

When initially opened, a map page is displayed in Auto Fit view. This means that the map will zoom in or zoom out to display all elements on the map page.

3. Do one of the following:

#### Link an icon

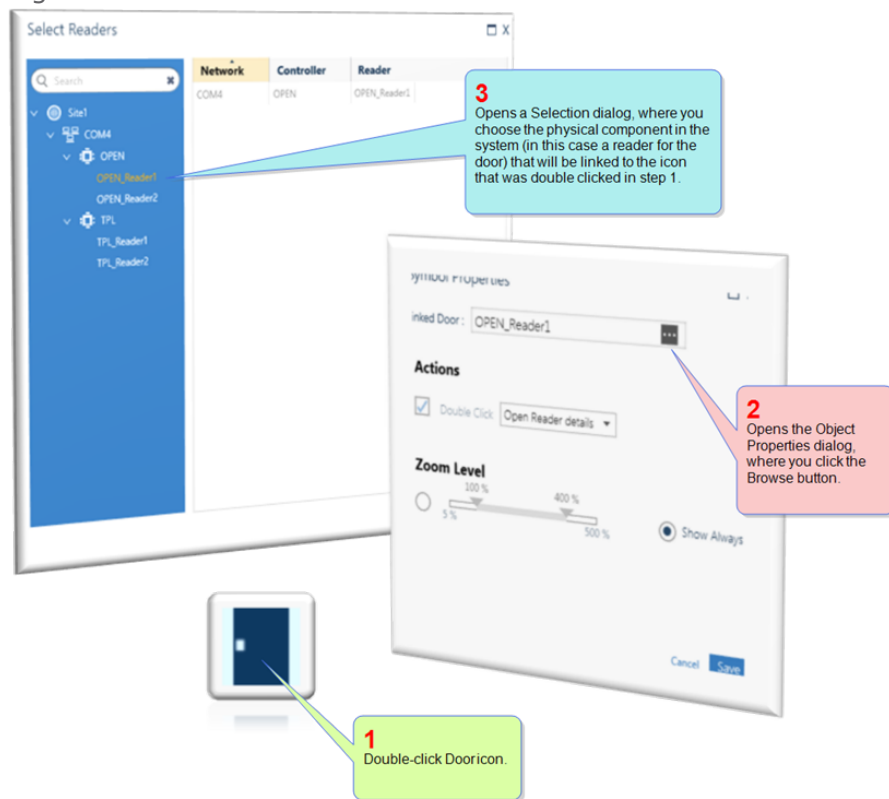
- a. Double-click an icon (object), An Symbol Properties dialog is displayed.

Depending on the type (stencil)of icon selected (i.e. Door, Input, Camera, etc.), a variation of the Linked field label appears in the Symbol Properties dialog. For example, a door icon will have a **Linked Door** field label, a relay icon will have a **Linked Relay** field label, etc.

<sup>1</sup>A graphical control element used as a navigational aid in GuardPoint10' GUI. It allows operators to keep track of their current location.

- b. Click the Browse button in the Linked field a Selection dialog is displayed where you can select the physical component or map where the icon will be linked.

Figure 14-13



**Note:** For a camera icon, instead of a Selection dialog, a drop-down list exists. The list includes all cameras belonging to NVRs or DVRs defined in the NVR/DVR screen. For information about the NVR/DVR screen, see "[Video NVR/DVR Screen](#)" on page 678.

- c. From the Selection dialog, double-click the component or put the component in focus and click **Select**. The Selection dialog is closed and the selected component's name appears in the Linked field.  
If a component is already linked to another object on the map, it cannot be selected in a Selection dialog. The only exception is a Map icon, shape, or textbox linked to a map.  
A component can only be linked to one object on the same map.
- d. The Double-click action drop-down list has the following functionality:
  - » If there are *no* manual events saved in the system, the only action available will be to open details of the linked icon, shape, or textbox.
  - » If there are manual events saved in the system, the actions available will be to open details of the linked icon, shape, textbox, or execute a global reflex that includes the selected manual event as a trigger.

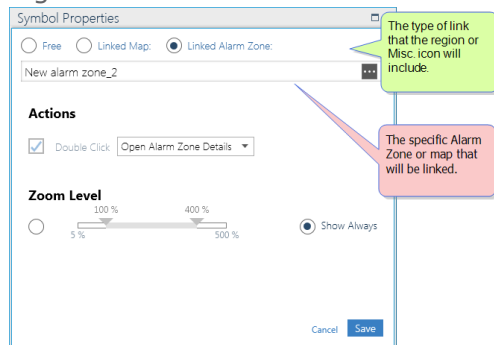
For more information about manual events, see "[Manual Events](#)" on page 532.

- e. Click **Save** in the Symbol Properties dialog. The Symbol Properties dialog is closed and the settings are assigned to the object in focus.
- f. Click **Save** in the Position screen. The map page information, with the new object settings, is updated in the system database.

### Link a shape or textbox

- a. Double-click a shape or textbox, An Symbol Properties dialog is displayed.

Figure 14-14



- b. Select the type of link you want for the object:

- » **Free**: The object is decorative and has no action associated with it.
- » **Linked Map**: When the object is clicked, a specified map page is opened.
- » **Linked Alarm Zone**: When the object is clicked, a specified Alarm Zone is opened, where Weekly Programs, inputs, and global reflexes can be specified. For information about Alarm Zones, see "[Alarm Zones \(Setup\)](#)" on page 301.
- » **Linked Area**: When the object is clicked, a specified Area's Roll Call window is opened.

Based on the link type selected, do one of the following:

- » If the **Free** link type is selected, click **Save**, as instructed in Step "c".
- » If the **Linked Map** link type is selected, click the Browse button in the **Linked** field. A Selection dialog is displayed where you select the map where the icon will be linked.
- » If the **Linked Alarm Zone** link type is selected, click the Browse button in the **Linked** field. A Selection dialog is displayed where you select the Alarm Zone where the icon will be linked.
- » If the **Linked Area** link type is selected, click the Browse button in the **Linked** field. A Selection dialog is displayed where you select the Area where the icon will be linked.

- c. The Double-click action drop-down list has the following functionality:

- » If there are *no* manual events saved in the system, the only action available will be to open details of the linked icon, shape, or textbox.
- » If there are manual events save in the system, the actions available will be to open details of the linked icon, shape, textbox or, execute a global reflex that includes the selected manual event as a trigger.

For more information about manual events, see "[Manual Events](#)" on page 542.



- d. Click **Save** in the Symbol Properties dialog. The Symbol Properties dialog is closed and the settings are assigned to the object in focus.



**Note:** Before closing the Symbol Properties dialog, you can select a show condition for the object (see "How to set an icon / shape / textbox's show condition" below).

- e. Click **Save** in the Position screen. The map page information, with the new object settings, is updated in the system database.

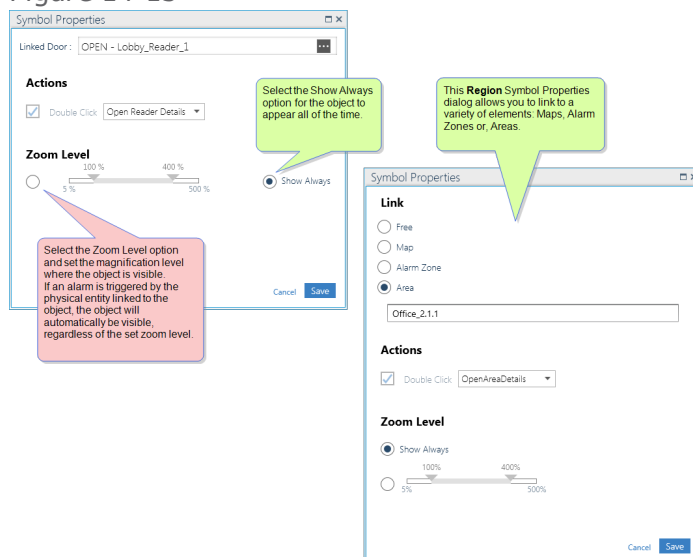
## How to set an icon / shape / textbox's show condition

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. Open a map page that already has a map image and icon, shape, or textbox.

When initially opened, a map page is displayed in Auto Fit view. This means that the map will zoom in or zoom out to display all elements on the map page.

3. Double-click icon, shape, or textbox, A Symbol Properties dialog is displayed. The dialog may vary depending on the item selected.

Figure 14-15



4. Do one of the following:
  - » Select **Show Always**: The object appears on the map page at all times.
  - » Select **Zoom Level**: The object only appears when the map page magnification is within the specified range, or if an alarm, linked to the icon, shape, or textbox, is triggered.


Change the range percentage in the Symbol Properties dialog as required.

5. Click **Save**. The show condition is saved.
6. Click **Save** in the Position screen. The object show settings are updated in the system database.

## Duplicating an Icon, Shape, or Textbox on a Map Page

Use the following tools to duplicate an icon, shape, or textbox that is already on a map page via the Position screen.

## How to duplicate an icon, shape, or textbox on a map page

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. Open a map page, which already has a map image, via the map tree or **breadcrumbs**<sup>1</sup>.  
When initially opened, a map page is displayed in Auto Fit view. This means that the map will zoom in or zoom out to display all elements on the map page.
3. Select an icon, shape, or textbox that is already on the map.
4. Click . A copy of the selected icon, shape, or textbox appears on the map.  
The copy is only in appearance, the Symbol Properties dialog parameters are not copied from the original.
5. After placing the duplicate on the map, do the following in whichever order you prefer:
  - » ["Linking an Icon, Shape, or Textbox" on page 284](#)
  - » ["Refining Icon, Shape or, Textbox Placement" below](#)

Multiple icons, shapes, or textboxes on a map may be linked to the same element.

## Refining Icon, Shape or, Textbox Placement

Use the following tools to refine an icon shape, or textbox already placed on a map page.

While performing a refinement operation, you may find the grouping tool useful. Grouping is used to apply any of the operations described in this topic to a group of icons, shapes, or textboxes as a single unit. Keep in mind that even if you group objects together they still remain as independent entities with their own links and display settings. A group of objects can be ungrouped at any time. For more information about groups, see ["Position Screen" on page 554](#).

## How to refine an icon, shape, or textbox on a map page

1. Go to the Setup Task group and click **Position**. The Position screen is displayed.
2. Open a map page that already has a map image and icons, shapes or, textboxes, via the map tree or **breadcrumbs**<sup>2</sup>.  
When initially opened, a map page is displayed in Auto Fit view. This means that the map will zoom in or zoom out to display all elements on the map page.
3. Do one of the following:
  - » **Resize an icon, shape, or textbox**
    - a. Select one or more icons, shapes or, textboxes (objects) that will be resized. Handles appear at the corners of the object.  
To select multiple objects, drag the mouse pointer over the objects or, hold down the **Ctrl** key and select each object individually. If more than one object is selected, the objects are surrounded by a dashed-lined rectangle with handles at the corners.

---

<sup>1</sup>A graphical control element used as a navigational aid in GuardPoint10' GUI. It allows operators to keep track of their current location.

<sup>2</sup>A graphical control element used as a navigational aid in GuardPoint10' GUI. It allows operators to keep track of their current location.

- b. With the mouse pointer, drag a handle in or out. The size and proportions of the selected object(s) change with the dragged handle.
- c. Release the handle and click **Save**. The object(s) remains resized and the map page information is updated in the system database.

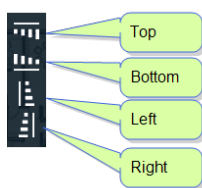
» **Align icon, shape, or textbox**

- a. Select two or more icons, shapes or, textboxes (objects).

To select multiple objects, drag the mouse pointer over the objects or, hold down the **Ctrl** key and select each object individually. If more than one object is selected, the objects are surrounded by a dashed-line rectangle with handles at the corners.

- b. After putting multiple objects in focus, click  on the action bar. A rollout appears with various alignment options.

Figure 14-16



- c. Click an alignment option. The selected objects align according to the option selected.
- d. Click **Save**. The map page information is updated in the system database.

» **Order icon, shape, or textbox**

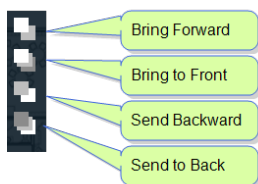
Each icon, shape, or textbox (object) placed on the icon layer has its own object layer. The Order option allows you to move one or more objects forward or backward in this object layer.

- a. Select one or more objects on a map page.

To select multiple objects, drag the mouse pointer over the objects or hold down the **Ctrl** key and select each object individually. If more than one object is selected, the objects are surrounded by a dashed-line rectangle with handles at the corners.

- b. Click  in the action bar. A rollout appears with various Order options.

Figure 14-17



- c. Select an Order option. The object(s) layer is moved forward or backward, according to the Order option selected.





**Note:** The best way to observe object layering is to overlap objects on a map and see which object overlaps the other.

- d. Click **Save**. The map page information is updated in the system database.

#### » Snap an icon, shape, or textbox to a grid line



**Note:** The Snap option is only available when the grid is visible. To make the grid visible, select  in the action bar.

- a. Select one or more icons, shapes or, textboxes (objects).  
To select multiple objects, drag the mouse pointer over the objects or hold down the **Ctrl** key and select each object individually. If more than one object is selected, the objects are surrounded by a dashed-line rectangle with handles at the corners.
- b. Click  in the action bar. The object(s) moves to the closest top and right grid lines.
- c. Click **Save**. The map page information is updated in the system database.

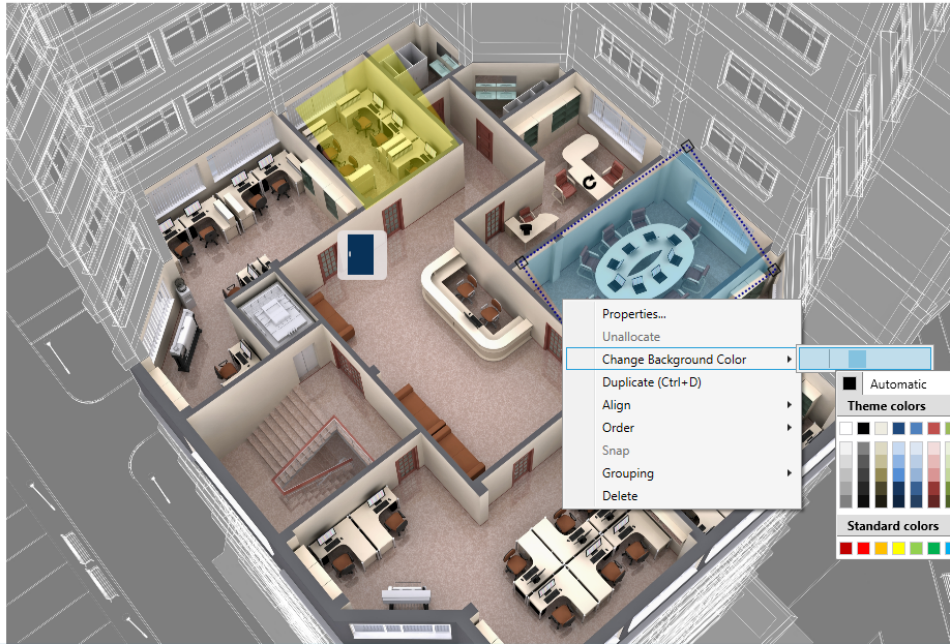
#### » Change the color of shape or textbox



**Note:** The Undo button does not apply to the Change Color action.

- a. Right-click a shape or textbox. A context menu appears.
- b. From the context menu, select the **Change Background Color** item.
- c. Click the current color to expand a pallet of available colors to select from.

Figure 14-18



- d. Click on a new color. The shape or textbox changes to the selected color.

To make the background of a shape or textbox transparent, select **Make Background Transparent** from the context menu.

#### » Change the default color of shapes



**Note:** The Undo button does not apply to the Change Default Color action.




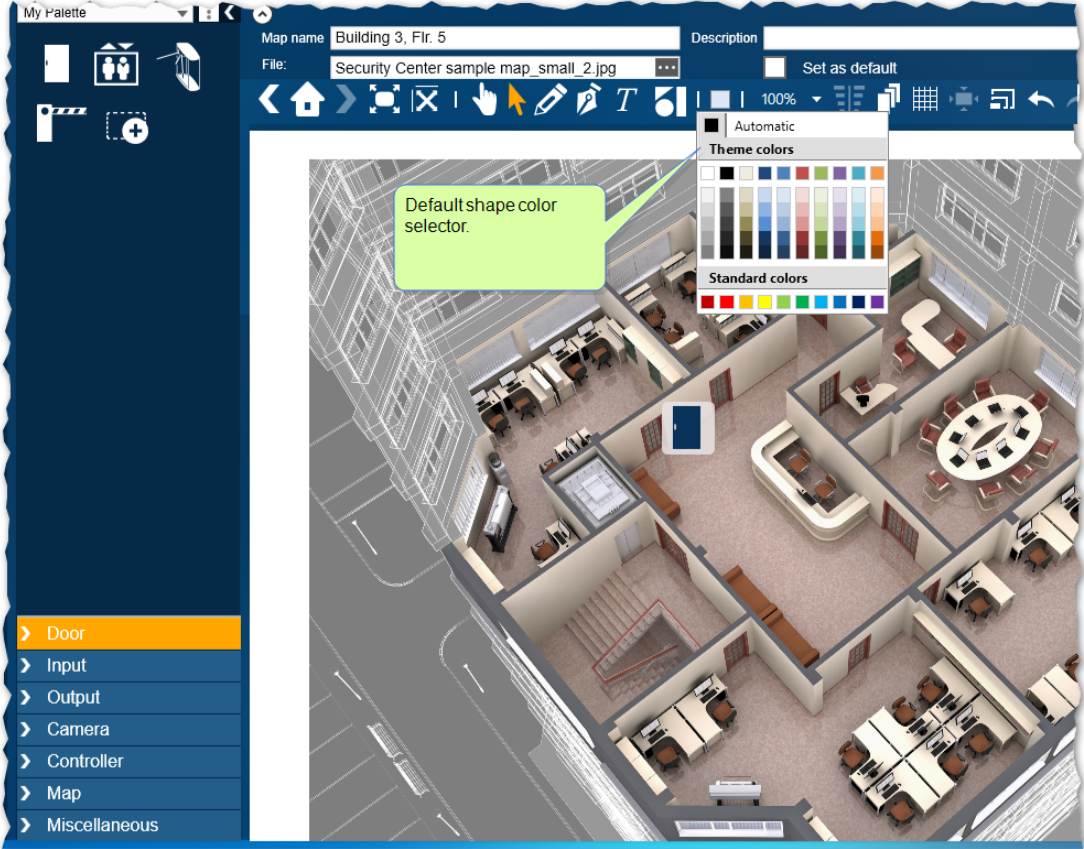
- a. Click  in the action bar. A color palette appears.
- b. From the palette, select the default color that will be applied to new shapes.  
A shape can be a Basic shape a Freehand shape or, a shape made one segment at a time.

Figure 14-19



Selected icons, shapes or, textboxes may be nudged with the arrow keys on the keyboard.

# CHAPTER 15:

## Badge Templates

The Badge Template module may be added to the GuardPoint10 core solutions upon request.

If you would like to purchase the Badge Template module, contact your GuardPoint10 provider.



The Badge Template module is used to design and produce personalized badges on demand. These badges may include company colors, logos, cardholder details with photo, etc. The Badge Template designer is accessed from the Setup task group and the Badge Print option is found in the Badges screen and Cardholders screen.

Template assignments are, by default, cardholder Type dependent (i.e. Employee, Visitor, etc.). However, an individual cardholder may be manually re-assigned a badge template that is non-Type dependent.

Template management takes place in the Setup task group, via the Badge Templates screen. Template design is done in a Telerik Report Designer. The Report Designer features an easy-to-use screen environment. The Report Designer is accessed via the Badge Templates screen.

Manual template assignment, which is not cardholder Type dependent, is performed via a cardholder's details or the Badges screen.

# Adding a Badge Template

Badge templates are part of the Badge Template module and may not be present in your current GuardPoint10 installation.

Use the following steps to design a new badge template via the Badge Templates screen.

## How to design and add a new badge template to the system

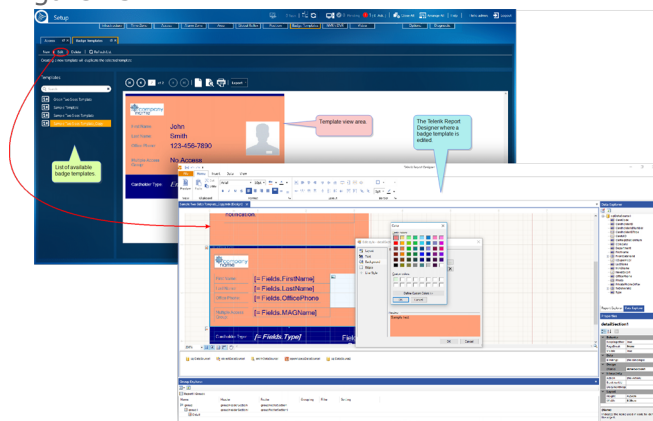
1. Go to the Setup Task group and click **Badge Templates**. The Badge Templates screen is displayed.
2. Select a template from the Template List on the left side of the screen that is most similar to the template you want to design. The template appears on the screen in the View area.
3. From the action bar, click **New**. A duplicate template is added to the Template list and appears in the View area. The duplicate is identical to the template previously selected except the name is appended to the text "\_Copy".



**Note:** If an operator-built template is linked to a cardholder manually and that template is later deleted, the cardholder will automatically be linked to the template designated for the cardholder's Type. Initially, a cardholder Type is linked to the Built-in sample template, though this link can be changed by an operator at any time.

4. Select the duplicate template, if not already selected, and change the name of the template to something that better describes its purpose (i.e. R&D, Marketing, Admin, Generic, etc.).
5. Click **Edit**. The new badge template is opened in the Telerik Report Designer window.

Figure 15-1



The Telerik Report Designer is a third-party application that allows you to customize your template. For basic badge design instructions, see ["Editing an Existing Badge Template" on the facing page](#).

For a detailed explanation of all of the tools available in the Telerik Report Designer window, go to <http://docs.telerik.com/reporting/standalone-report-designer>



# Editing an Existing Badge Template

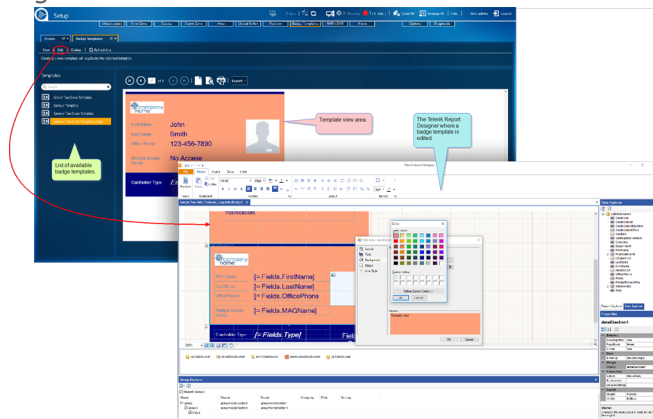
Badge templates are part of the Badge Template module and may not be present in your current GuardPoint10 installation.

Use the following information for basic badge template design via the Telerik Report Designer window.

## Basic badge template design

1. From the GuardPoint10 Badge Templates screen, select an operator-built badge template from the Template list, and then click **Edit**. The badge template is opened in the Telerik Report Designer window.

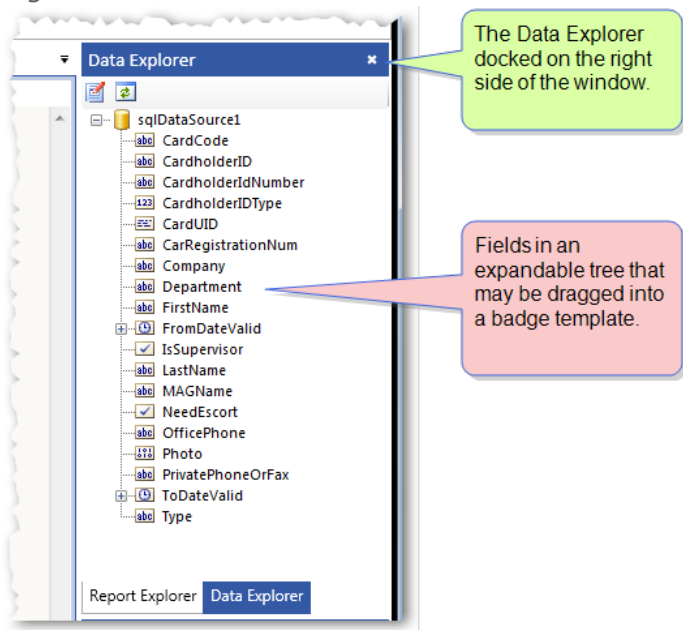
Figure 15-2



### » Add a field to a badge template:

Drag a field from the Data Explorer tree on the right side of the Telerik Report Designer window and drop it in the badge template. If necessary, change the position of a field by dragging the field in the template to a new location.

Figure 15-3

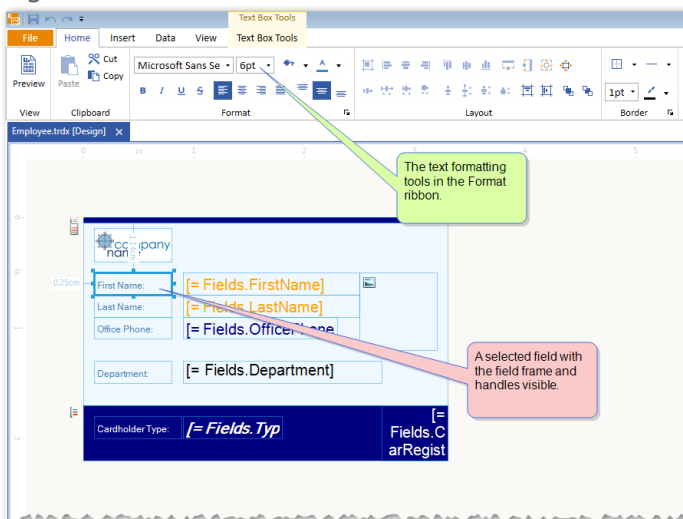


» **Resize a field already in a badge template:**

1. Select a field in the template. Handles appear around the frame of the field.
2. Drag a handle in any direction to resize the field.

If the field output will contain text, you may also want to adjust the point size of the text font via the toolbar at the top of the window to fit the designated frame size.

Figure 15-4



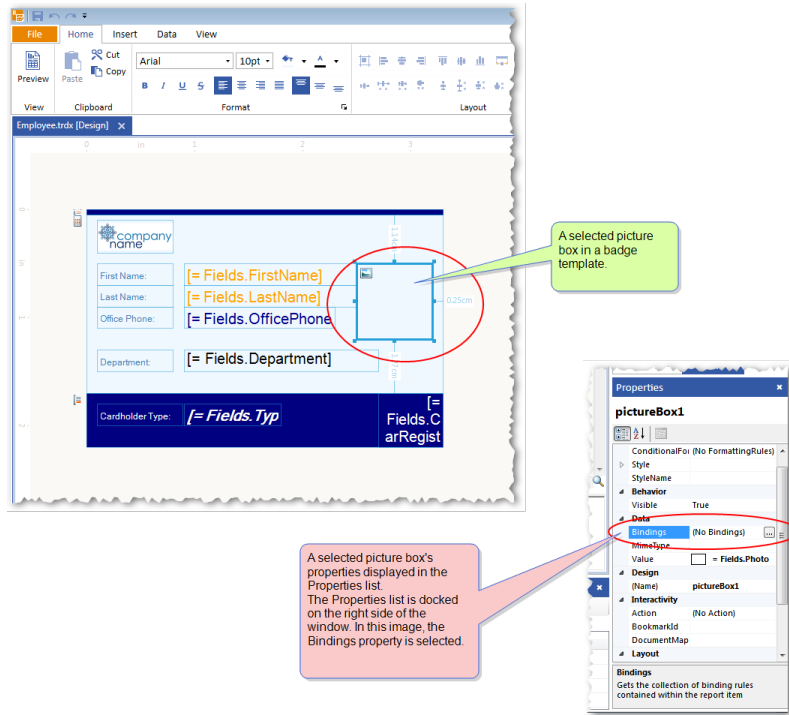
» **Add dynamic behavior to a picture box:**

A picture box that will contain a company logo may not need to be dynamic because the logo will remain the same in all badges. However, a picture box that will contain a cardholder's photo will need to be dynamic because the photo will depend on the cardholder for whom the badge is being made.

To make the content of a picture box dynamic:

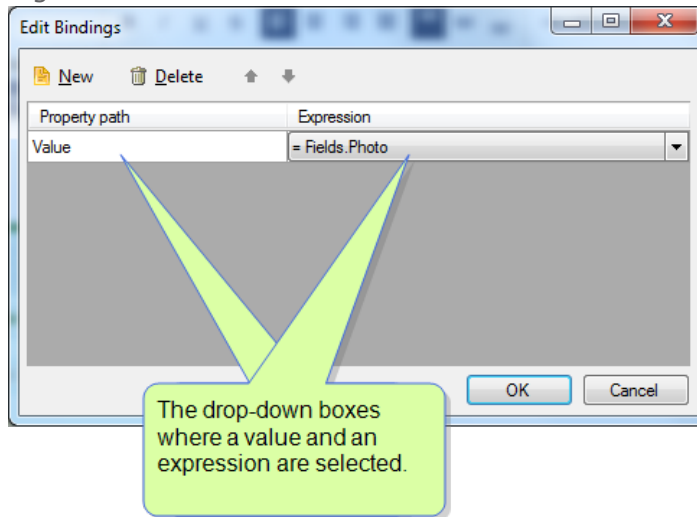
1. Select a picture box in the template. A frame appears around the box.  
Alternatively, add a picture box from the Insert ribbon's Report Items group.
2. In the Properties list, select Bindings and click the ... symbol. The Edit Bindings dialog is displayed.

Figure 15-5



3. Click **New** and select **Value** from the **Property path** drop-down list.
4. From the **Expression** drop-down list, select the field that represents the dynamic value. For example, to have the picture box contain the photo of a cardholder, select **= Fields.Photo**.

Figure 15-6



5. Click **OK** in the Edit Bindings dialog. The dialog is closed.
6. In the Properties list, select Sizing found at the bottom of the list and select ScaleProportional from the Sizing list. This will allow the image to fit properly in the picture box.
7. Save the template and that's it. Now when you use the template, the photo in the picture box will be dependent on the cardholder selected in the Cardholders screen or the Badges screen.

#### » Add dynamic QR item to a badge template:

A QR is the square image that looks a little bit like a crossword puzzle and is read as an access



code. The dynamic behavior assigned to the QR means the QR image changes based on the code linked to the QR (i.e. badge code).

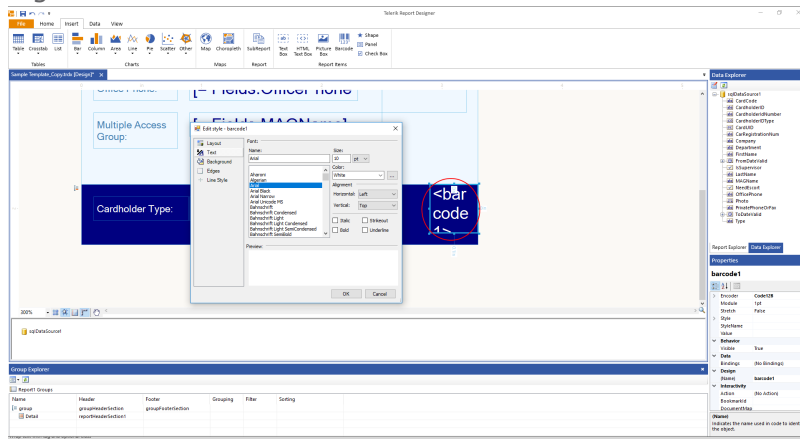


**Note:** Currently GuardPoint10 does not support QR access control, however by adding a QR to a badge template, a QR may be used with other applications.

To add a dynamic QR to a badge template:

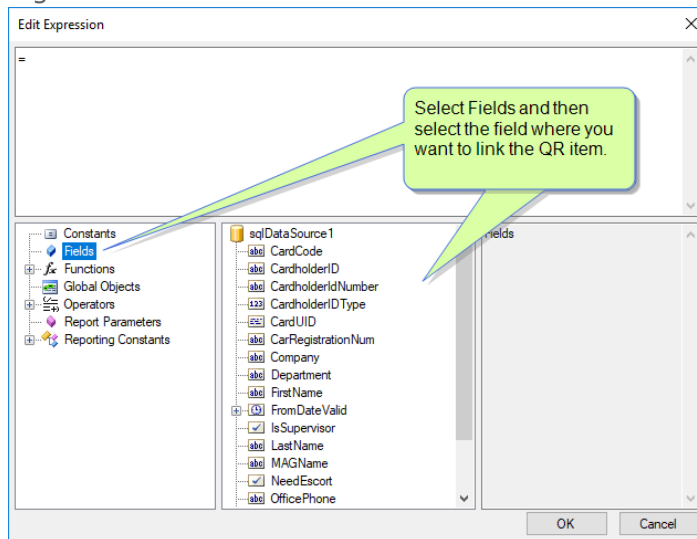
1. In the Telerik Report Designer, click on a badge template.
2. From the toolbar, select **Insert** > **Barcode** from the Report Items group.
3. Change the size via the frame around the QR item and change the style of the QR item as required via the context menu.

Figure 15-7



4. With the QR item selected, select **Encoder** from the Properties pane and select **QRcode** from the drop-down list.  
Other codes in the **Encode** property will display the code as a non-QR code (i.e. bar code).
5. With the QR item selected, select the **Value** property's ... button. The Edit Expression dialog is displayed.

Figure 15-8



6. Select **Fields** and then select the field that the QR code will dynamically change to represent when printed (i.e. **Cardcode**).
7. Save the template and that's it. Now when you use the template, the QR displayed will be dependent on the cardholder and badge code selected in the Badge Print window.

The Telerik Report Designer is a third-party application that allows you to customize your template. For a more detailed explanation of all of the tools available in the Telerik Report Designer window, go to <http://docs.telerik.com/reporting/standalone-report-designer>

# Deleting a Badge Template

Badge templates are part of the Badge Template module and may not be present in your current GuardPoint10 installation.

Use the following steps to delete a badge template via the Badge Templates screen.

## How to delete a badge template from the system

1. Go to the Setup Task group and click **Badge Templates**. The Badge Templates screen is displayed.
2. Select an operator-built badge template from the Template list. The template appears on the screen in the View area.
3. From the action bar, click **Delete**. The template is removed from the Template list and from the database.



**Note:** The badge template that is built-in to GuardPoint10 (Sample Template) cannot be deleted or edited.

If an operator-built template is linked to a cardholder manually and that template is later deleted, the cardholder will automatically be linked to the template designated for the cardholder's Type.

Initially, a cardholder Type is linked to the Built-in sample template, though this link can be changed by an operator at any time. If a template linked to a cardholder Type is deleted, the Type will automatically link to the Built-in sample template.

# CHAPTER 16:

## Alarm Zones (Setup)



The Alarm Zone Setup screen groups and manages the status of alarm detectors such as motion detectors that monitor a single physical space (i.e. lobby and hallway). The status of an Alarm Zone (armed or disarmed) is governed by a Weekly Program.

The following demonstrates a logical division of inputs by an Alarm Zone and how a WP would govern them.

### Example:

A company called Paper Pusher International (PPI) has an office building in France, where each floor in the building is designated for a different region in the world.

PPI employees keep the same standard work hours (i.e. 9:00 to 18:00) as the region where they are designated.

Each floor in the building has inputs (i.e. doors, windows, and motion sensors). The inputs of each floor are grouped into Alarm Zones (i.e. AZ Flr\_1, AZ Flr\_2, AZ Flr\_3, etc.).

A WP is defined for each floor, based on the time in the region where the floor is designated. The first floor is designated for Eastern Europe. The WP defined for the first floor will be based on **UTC<sup>1</sup> +3**.

Assigning the WPs to their respective Alarm Zones means that all of the inputs in an Alarm Zone are governed by the same WP. All of the inputs on the first floor will be in their green period from 9:00 (UTC +3) until 18:00 (UTC +3). When the business day is over in Eastern Europe (from 18:00 until 9:00 (UTC +3)), the first floor is closed and the inputs enter their white period.

## Adding a New Alarm Zone

Use the following steps to add a new alarm zone via the Alarm Zone screen.



**Note:** To save the alarm zone to a relevant local controller database, click **Download** in the action bar.

Operators creating or editing an alarm zone should have knowledge of the system in their workplace.

## How to add a new alarm zone to the system

### Create an alarm zone container

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. From the action bar, click **New** and select **Alarm Zone** from the drop-down list that appears under the **New** button. Two blank areas designed for different pieces of alarm zone information appear on the screen.

» Parameters

» Inputs table

These areas define the new alarm zone space. For more information about these areas, see "[Alarm Zone Setup Screen](#)" on page 521.

3. Replace the default alarm zone name with a more descriptive name.

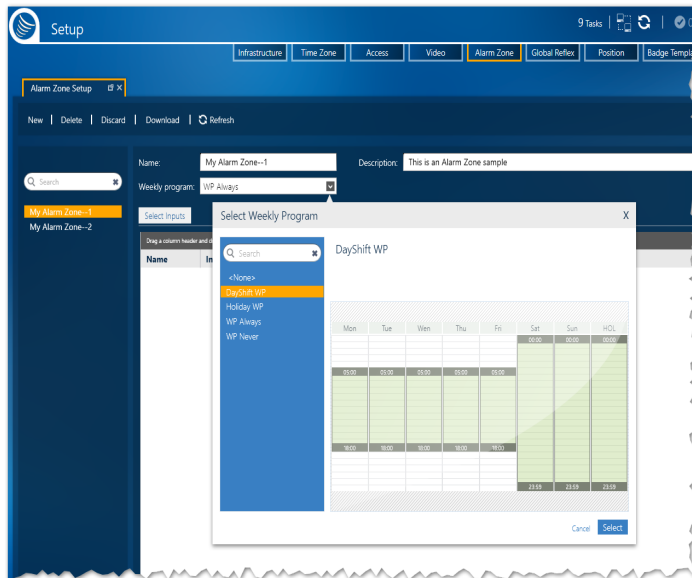
---

<sup>1</sup>Universal Coordinated Time (UTC) is the successor to Greenwich Mean Time (GMT). It is the basis for local times worldwide.



4. (Optional) Enter a description of the alarm zone. Generally, the description identifies the logic used to identify the inputs that are included in the alarm zone container (i.e. the space affected by the alarm zone).
5. Click the down arrow in the Weekly Program field. A Select Weekly Program dialog is displayed. If you select **None** from the Weekly Program list, the alarm zone will only be activated by a manual action (i.e. badge swipe, keypad code, Alarm Zone Security screen action).
6. From the dialog, select the Weekly Program that will be applied to all of the inputs in the alarm zone. An image representing the schedule configured for the selected Weekly Program will appear to the right of the selection.

Figure 16-1

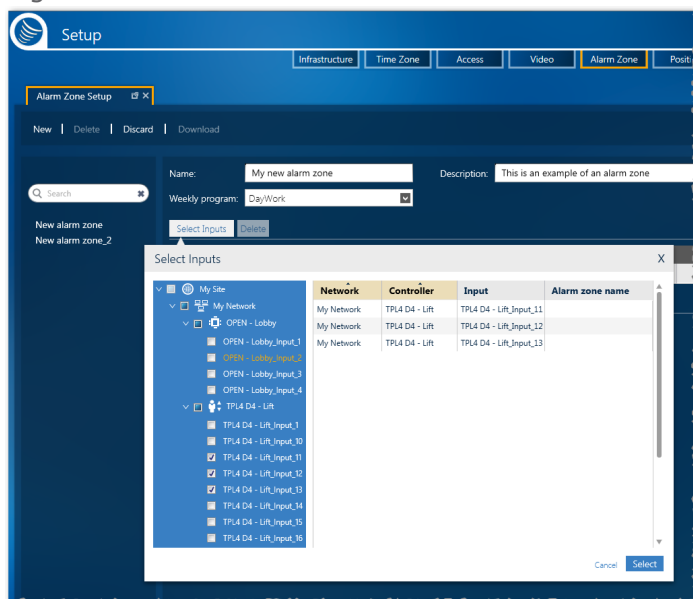


7. Click **Select**. The selected Weekly Program governs the alarm zone's green and white periods.

## Select input devices that will be put in the alarm zone

1. In the Inputs area, click **Select Inputs**. A Select Input dialog is displayed.
2. From the Select Input dialog, expand the infrastructure tree and select the input device(s) that will be added to the alarm zone container. The selected device(s) will appear in a table to the right of the tree.

Figure 16-2



An input can only be selected for one alarm zone. If you try to select an input that has already been selected for a different alarm zone, the entry in the dialog's table will have gray text and the **Select** button will be disabled or will not be applied to the input item.

3. Click **Select**. The selected inputs are added to the dynamic table in the Alarm Zone screen's Input area. For information about the dynamic table, see ["Alarm Zone Setup Screen" on page 521](#).

## Save the new alarm zone

1. In the Alarm Zone screen, click **Save** on the far right of the action bar. The alarm zone is saved in the system database.
2. Click **Download**. The alarm zone in focus is saved in the local database of the controller(s) where the selected input(s) is connected.

**Note:** The **Discard** button removes any changes made to the alarm zone since it was last saved.

# Editing / Deleting a Galaxy Group or Zone

Use the following steps to edit a previously saved Galaxy group or zone via the Alarm Zone Setup screen.



**Note:** Operators editing a Galaxy group or zone should have knowledge of the Galaxy system and GuardPoint10 system in their workplace.

## How to edit or delete a Galaxy group

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select a Galaxy group from the searchable and collapsible list of groups in the column on the left side of the screen. The following areas are populated with data related to the group in focus.
  - » Parameters
  - » Zone table

For information about these areas, see ["Alarm Zone Setup Screen" on page 521](#).

3. Make the required changes to the group's parameters. The available fields are Name, Description, and Group number (if there are other numbers available). The panel cannot be changed.
4. After making changes, do one of the following:
  - » Click **Discard** to revert to the last saved version of the group.
  - » Click **Save** on the far right of the action bar. The edited group is saved in the system database.

## How to delete a Galaxy group

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select a Galaxy group from the searchable and collapsible list of groups in the column on the left side of the screen.
3. Click **Delete** from the Action menu and confirm the delete action.
4. The group is removed from the list. However, the group with its zones still exists in the Galaxy panel.



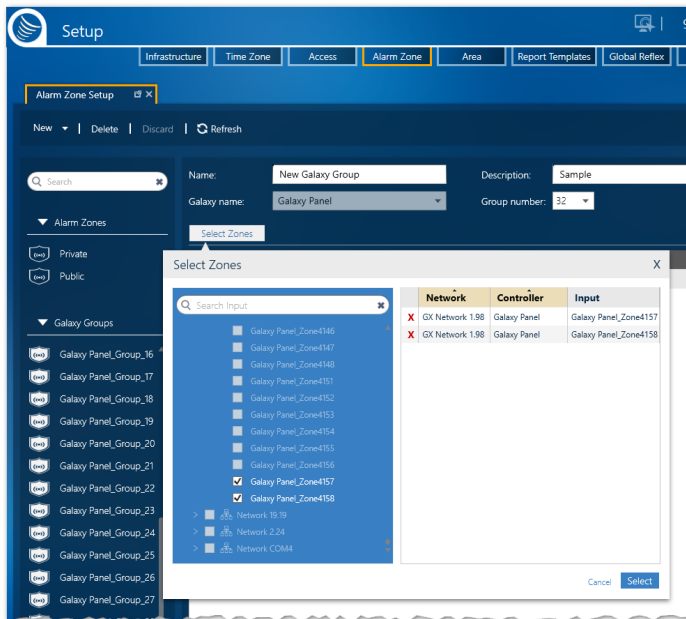
**Warning:** If a zone, which was in the now-deleted group, is triggered, the alarm will appear in GuardPoint10 and the group number is shown in the Event Log will be the number assigned to the zone in the Galaxy panel.

# How to delete a zone from a Galaxy Group

Use the following steps to delete a zone in a previously saved Galaxy group via the Alarm Zone Setup screen.

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select a Galaxy group from the searchable and collapsible list of groups in the column on the left side of the screen. The zones in the group will appear in the Zone table.
3. Click Select Zone. A Select Zone dialog is displayed.

Figure 16-3



4. From the table in the dialog, click the red **X** in the row of the zone(s) that will be deleted.
5. Click **Select**. The Select Zone dialog is closed and the zones are removed from the Zone table.
6. Click **Save**. The Galaxy group is saved without the deleted zone(s) in it.



**Note:** A deleted zone is only deleted from the Galaxy group in GuardPoint10. The zone still exists in a Galaxy panel group.

If the deleted zone is triggered, the zone will be automatically returned to the group where it was deleted in GuardPoint10.

# How to edit a zone in a Galaxy Group

Use the following steps to edit a zone in a previously saved Galaxy group via the Alarm Zone Setup screen.

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select a Galaxy group from the searchable and collapsible list of groups in the column on the left side of the screen.
3. The zones in the group will appear in the Zone table.
4. Double-click a zone row in the Zone table. The Zone details are displayed.
5. From the Zone details, add / change the zone's: name, description instructions, priority, and specify if an alarm from the zone should be ignored via the **Omit** checkbox.

## Deleting an Alarm Zone

Use the following steps to delete an alarm zone via the Alarm Zone screen.

### How to delete an alarm zone

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select an alarm zone from the searchable list of alarm zones in the column on the left side of the screen.
3. In the action bar, click **Delete**. The alarm zone is removed from the system database and the controllers, where the inputs that were placed in the alarm zone are connected.



**Note:** The **Discard** button removes any changes made to the alarm zone since it was last saved.

## Adding a New Galaxy Group

Use the following steps to add a new Galaxy group via the Alarm Zone screen.



**Note:** This topic assumes that a Galaxy panel has been integrated into your GuardPoint10 system infrastructure.

Operators creating or editing a Galaxy group should have knowledge of the GuardPoint10 system and the Galaxy system in their workplace.

Before adding a Galaxy group, it is important to understand the following:

- » When a Galaxy panel is added to the infrastructure, Galaxy groups are automatically added to the Alarm Zone Setup screen with all Galaxy zones placed in **Group\_1**.
- » The number of Galaxy groups automatically added to the Alarm Zone Setup screen depends on the Galaxy panel type added to the infrastructure.

- » A Galaxy group can only be added when the current number of groups in the Alarm Zone screen is less than the maximum allowed by the Galaxy panel type.

## How to add a Galaxy group to the GuardPoint10 system

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. From the action bar, click **New** and select **Galaxy Group** from the drop-down list that appears under the **New** button. Two blank areas designed for different pieces of alarm zone information appear on the screen.
  - » Parameters
  - » Zone table

These areas define the new Galaxy group space. For more information about these areas, see ["Alarm Zone Setup Screen" on page 521](#).

3. Replace the default Galaxy group name with a more descriptive name.
4. (Optional) Enter a description of the Galaxy group. Generally, the description identifies the logic used to identify the zones that are included in the Galaxy group.
5. From the **Galaxy name** drop-down list, select the Galaxy panel where the new group will be added.
6. From the **Group number** drop-down list, select the Galaxy group number that will be assigned to the new group.

If the maximum number of groups for the selected Galaxy panel already exists in the GuardPoint10 system, the Group number drop-down will be disabled and the new group will not be able to be saveable.

7. Click **Save**. The new, empty Galaxy group is added to the list of saved groups visible in the searchable and collapsible list of groups in the column on the left side of the screen.

To add a Galaxy zone to the Galaxy group, see ["Adding a Galaxy Zone to a Galaxy Group" below](#).



**Note:** The **Discard** button removes any changes made to the Galaxy group since it was last saved.

## Adding a Galaxy Zone to a Galaxy Group

Use the following steps to add a Galaxy zone to a Galaxy group via the Alarm Zone screen.



**Note:** This topic assumes that a Galaxy panel has been integrated into your GuardPoint10 system infrastructure.

Operators editing a Galaxy group should have knowledge of the GuardPoint10 system and the Galaxy system in their workplace.

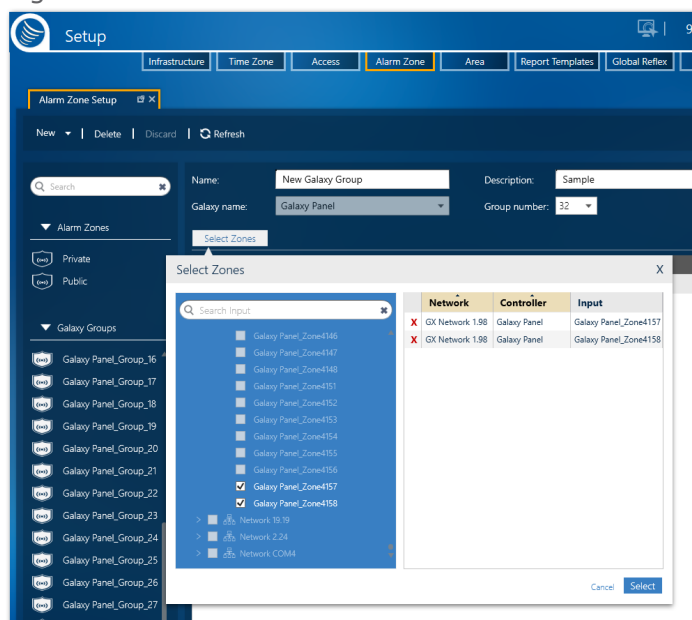
Before adding a Galaxy zone to a Galaxy group, be aware of the following:

- » When a Galaxy panel is added to the infrastructure, Galaxy groups are automatically added to the Alarm Zone Setup screen with all Galaxy zones placed in **Group\_1**.
- » For a Galaxy zone to be placed in a Galaxy group, the zone must be available; this means that the zone is not already placed in a different Galaxy group.

## How to Galaxy add a zone to a Galaxy Group

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select an existing Galaxy group from the list of saved groups visible in the searchable and collapsible list of groups in the column on the left side of the screen. The group's details and Zone table are displayed.
3. Above the Zone table, click **Select Zones**. A Select Zones dialog is displayed.

Figure 16-4



Zones that have already been placed in a Galaxy group are disabled in the dialog's table.

4. From the Select Zones dialog, expand the infrastructure tree and select a zone(s) that will be added to the Galaxy group. The selected zone(s) will appear in a table to the right of the tree.
5. Click **Select**. The selected zones are added to the Zone table in the Alarm Zone screen.
6. In the Alarm Zone screen, click **Save** on the far right of the action bar. The Galaxy group is saved in the system database.

**Note:** The **Discard** button removes any changes made to the Galaxy group since it was last saved.

# Editing / Deleting a Galaxy Group or Zone

Use the following steps to edit a previously saved Galaxy group or zone via the Alarm Zone Setup screen.



**Note:** Operators editing a Galaxy group or zone should have knowledge of the Galaxy system and GuardPoint10 system in their workplace.

## How to edit or delete a Galaxy group

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select a Galaxy group from the searchable and collapsible list of groups in the column on the left side of the screen. The following areas are populated with data related to the group in focus.
  - » Parameters
  - » Zone table

For information about these areas, see ["Alarm Zone Setup Screen" on page 521](#).

3. Make the required changes to the group's parameters. The available fields are Name, Description, and Group number (if there are other numbers available). The panel cannot be changed.
4. After making changes, do one of the following:
  - » Click **Discard** to revert to the last saved version of the group.
  - » Click **Save** on the far right of the action bar. The edited group is saved in the system database.

## How to delete a Galaxy group

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select a Galaxy group from the searchable and collapsible list of groups in the column on the left side of the screen.
3. Click **Delete** from the Action menu and confirm the delete action.
4. The group is removed from the list. However, the group with its zones still exists in the Galaxy panel.



**Warning:** If a zone, which was in the now-deleted group, is triggered, the alarm will appear in GuardPoint10 and the group number is shown in the Event Log will be the number assigned to the zone in the Galaxy panel.

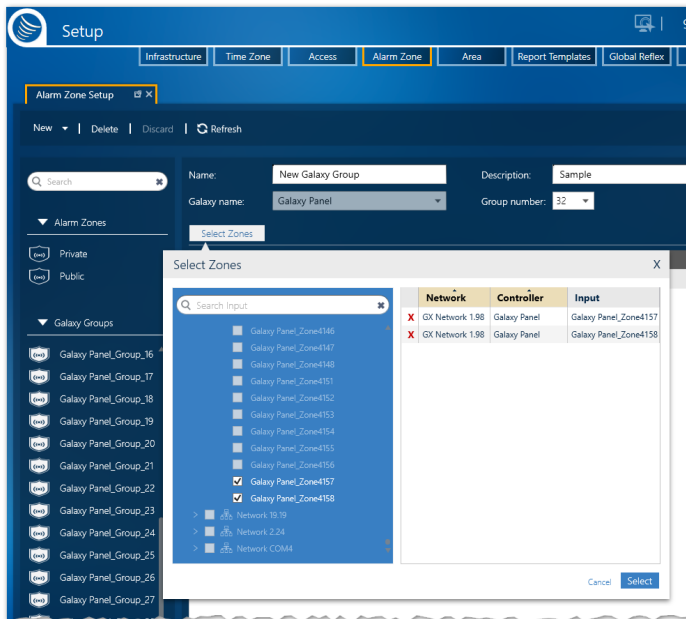


# How to delete a zone from a Galaxy Group

Use the following steps to delete a zone in a previously saved Galaxy group via the Alarm Zone Setup screen.

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select a Galaxy group from the searchable and collapsible list of groups in the column on the left side of the screen. The zones in the group will appear in the Zone table.
3. Click Select Zone. A Select Zone dialog is displayed.

Figure 16-5



4. From the table in the dialog, click the red **X** in the row of the zone(s) that will be deleted.
5. Click **Select**. The Select Zone dialog is closed and the zones are removed from the Zone table.
6. Click **Save**. The Galaxy group is saved without the deleted zone(s) in it.



**Note:** A deleted zone is only deleted from the Galaxy group in GuardPoint10. The zone still exists in a Galaxy panel group.

If the deleted zone is triggered, the zone will be automatically returned to the group where it was deleted in GuardPoint10.

# How to edit a zone in a Galaxy Group

Use the following steps to edit a zone in a previously saved Galaxy group via the Alarm Zone Setup screen.

1. Go to the Setup Task group and click **Alarm Zone**. The Alarm Zone Setup screen is displayed.
2. Select a Galaxy group from the searchable and collapsible list of groups in the column on the left side of the screen.
3. The zones in the group will appear in the Zone table.
4. Double-click a zone row in the Zone table. The Zone details are displayed.
5. From the Zone details, add / change the zone's: name, description instructions, priority, and specify if an alarm from the zone should be ignored via the **Omit** checkbox.

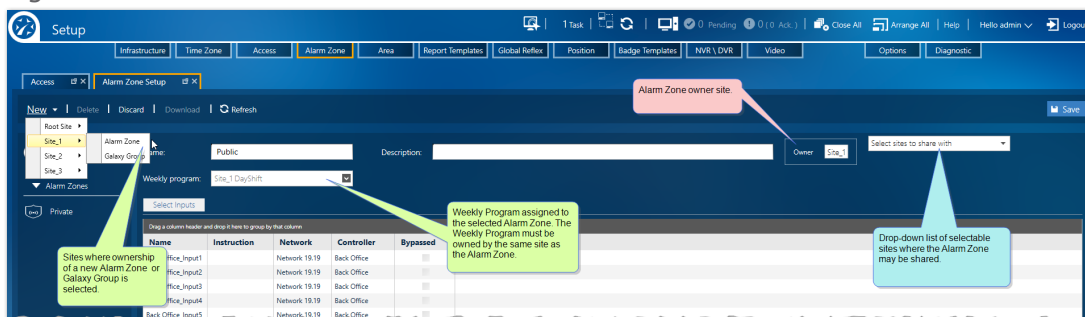
# Alarm Zone Setup: MultiSite Impact

The Alarm Zone Setup screen includes a new field called **Owner**. This field identifies the site that owns the Alarm Zone. An Alarm Zone also includes a **Select site to share with** a drop-down list. This list allows the user to select other sites where the Alarm Zone may be shared.

## Add a new Alarm Zone

1. With the Alarm Zone screen displayed, click the **New** button.
2. From the **New** button drop-down, select the site that will own the new Alarm Zone and then select either **Alarm Zone** or **Galaxy Group**.
3. When selecting a **Weekly Program** for the Alarm Zone, only those Weekly Programs owned by the same site as the Alarm Zone are available.
4. When selecting **inputs** for the Alarm Zone, only those inputs owned by the same site as the Alarm Zone are available. Shared inputs from other sites cannot be included in the Alarm Zone.

Figure 16-6



**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 17:

## Area



See how many cardholders are in a building, and how many are in each room in the building with the Area module.

Area is a highly configurable module where spaces (building, rooms, etc.) can be defined as named areas for monitoring cardholder occupancy. This allows GuardPoint10 to implement geotracking of cardholders within an access-controlled environment.

The Area screen is where an area is named and the entrance and exit readers are identified for an area. In addition, the cardholder capacity of an area is recorded.

After defining an area, occupancy monitoring takes place based on access events that occur via the identified readers. Monitored results may be easily viewed in the GuardPoint10 GUI via the Security Center screen and an area-centric Area Roll Call screen, and to a lesser extent, a cardholder's details.

Actions can be invoked on the condition of monitored area data via a powerful global reflex specifically designed to trigger based on an area condition.

# Adding a New Area

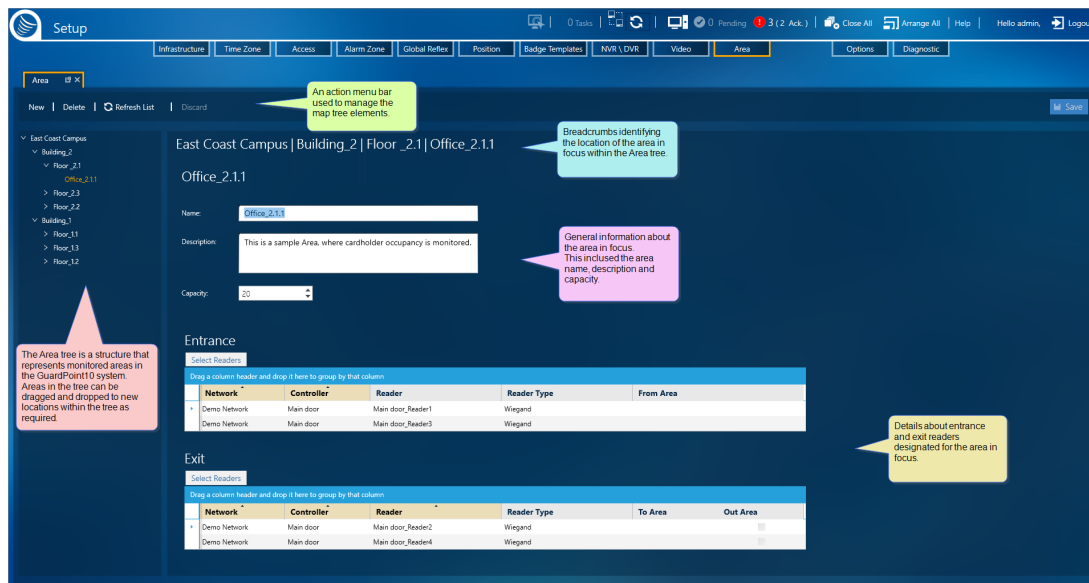
Use the following steps to add a new area via the Area screen.

## How to add a new area to the system

After an area is added to the GuardPoint10 system, it may be used in the Position and Security Center screens, and the Area Roll Call screen.

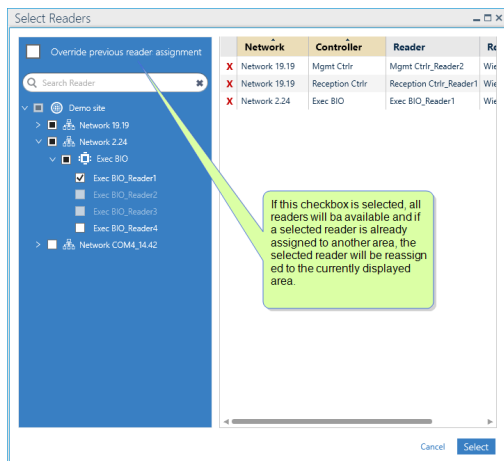
1. Go to the Setup Task group and click **Area**. The Area screen is displayed.

Figure 17-1



For information about the Area screen, see "Area Screen" on page 525.

2. In the Area tree, select the existing area where the new area will be a sub-area.
3. From the action bar, click **New**. Area details appear to the right of the Area tree.
4. Complete the general fields for the new area (i.e., **Name**, **Description**, and **Capacity**).
5. Click the **Select Readers** button above the **Entrance Readers** table. A Select Readers dialog is displayed.



- From the Select Readers dialog, select one or more readers that will be identified as entry points to the new area, and then click **Select**.

When the **Override previous reader assignment** checkbox in the Select Readers dialog is selected, readers that have been previously assigned to an area will be available in the Select Reader dialog for reassignment. If the checkbox is not selected, readers that have already been assigned to an area will be grayed out in the Select Reader dialog and unavailable for reassignment.

- Click the **Select Readers** button above the **Exit Readers** table. A Select Readers dialog is displayed.
- From the Select Readers dialog, select the readers that will be identified as exit points to the new area, and then click **Select**.

When the **Only readers that have no Area assignment are available** checkbox in the Select Readers dialog is selected, readers that have been previously assigned to an area will be available in the Select Reader dialog for reassignment. If the checkbox is not selected, readers that have already been assigned to an area will be grayed out in the Select Reader dialog and unavailable for reassignment.

- Click **Save** on the far right of the action bar. The area is saved in the system database and appears in the Area tree.

A reader can only have one area Entrance or Exit assignment.

# Adding a Global Anti-passback Area

Use the following steps to add a global anti-passback area via the Area screen.

**Note:** Before you start, the Options screen's **Apply global anti-passback** setting must be set to **Yes**.

## How to add a global anti-passback area

1. Go to the Setup Task group and click **Area**. The Area screen is displayed.
2. Add a new area, see ["Adding a New Area" on page 316](#).  
Alternatively, select an existing area from the Area tree on the left side of the screen. The area's details are displayed.  
For information about these details, see ["Area Screen" on page 525](#).
3. Set **Global Anti-Passback** to **Yes**.
4. The name of the area appears in the **Current GAPB Areas** list and the **Number of remaining Areas that may have the GAPB option** value is updated.
5. Double-click an entrance reader row (with reader data) to open the reader's details.
6. In the reader details > Access Mode tab, set **Anti-Passback** to **Yes**.
7. Click **Save&Close**.
8. Repeat steps 5 - 7 for each of the area's entrance and exit readers where the GAPB rule will be applied.
9. Click **Save** on the far right of the Area screen's action bar. The GAPB area is saved in the system database and downloaded to all relevant controllers.

To avoid a situation where a cardholder cannot gain access via a reader due to APB or GAPB, and a user is not available to assist, create a Global Reflex where the action will open the relay of the door where the cardholder would want to access. The trigger should be something the cardholder can do on their own (i.e. swipe the badge at the reader five consecutive times).

For more information about Global Anti-Passback, see ["Understanding Anti-passback in GuardPoint10" on page 80](#).

**Note:** The saved changes are immediately applied to any relevant item in the Area Roll Call screen and Security Center screen.




# Editing an Area

Use the following steps to edit a previously saved area via the Area screen.

## How to edit an area

1. Go to the Setup Task group and click **Area**. The Area screen is displayed.
2. Select an area from the Area tree on the left side of the screen. The area's details are displayed.  
For information about these details, see ["Area Screen" on page 525](#).
3. Make the required changes.
4. After making changes, do one of the following:
  - » Click **Discard** to revert to the last saved version of the area.
  - » Click **Save** on the far right of the action bar. The edited area is saved in the system database.




**Note:** The saved changes are immediately applied to any relevant item in the Area Roll Call screen and Security Center screen.

# Deleting an Area

Use the following steps to delete an area via the Area screen.

## How to delete an area

1. Go to the Setup Task group and click **Area**. The Area screen is displayed.
2. Select an area from the Area tree on the left side of the screen.
3. In the action bar, click **Delete**. The area is removed from the system database and the tree



**Note:** The deleted area is no longer available in the Area Roll Call screen. The area will be removed from any global reflex where the area was previously assigned. In the Position screen and Security Center screen, any icons, shapes or, textboxes that were previously linked to the now-deleted icon will be unallocated.

# Area Setup: MultiSite Impact

Each site has its own Areas. These Areas cannot be shared with other sites. The name of the site that owns an Area appears below the Area description.

The built-in Root site Area is accessible to super users and users owned by the Root site. All other Areas appear below the Root site Areas in the Area tree.

The Area tree shows the Root Area and all other Areas where the logged-in user has authorization.

If the user is a super user and the Area is owned by the Root site, the user will be able to select readers from other sites. This Root site Area will not be shareable. A non-super user can add Areas where they have authorization. The readers available to that Area must be owned by the same site as the Area (no shared readers).

## Add an Area

1. Select an existing Area (i.e. the Root Area).
2. From the Action menu, click **New**. Alternatively, click **Add Area** from the context menu of the Area in focus.

If the built-in Root Area is in focus, select the site that will own the new Area. This is especially relevant for users who have authorization to more than one site.

If the Area in focus is not the Root Area, the new Area will have the same owner as the Area in focus.

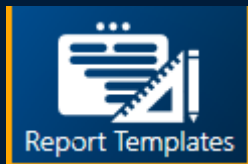
3. Select readers for the entrance and exit points of the Area.
4. (Optional) Add a capacity and description, and click **Save**.

## Manage the Area tree

Areas can be dragged and dropped in the Area tree. This means an Area can be a sub-Area of another (parent) Area. However, this is only allowed when the sub-Area is owned by the same site as the parent Area or if the parent Area is the built-in Root Area.

# CHAPTER 18:

## Report Templates



The Report Templates screen is where general information about a template is entered, and where information about a template's use in a global reflex ["Create Template-based report" on page 548](#) action is entered. A report template is saved and grouped by screen on the Report Templates screen. A report template can be used to quickly load a table structure that was previously saved instead of manually rebuilding the structure. A report template can also be used in a global reflex ["Create Template-based report" on page 548](#) action.

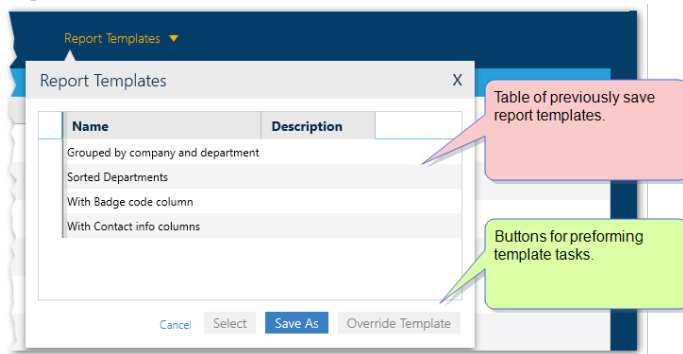
# Handling Report Template

Use the following steps to handle a report template via the Report Templates screen.

The Report Template screen is accessible from two places:

- » The Setup task group's primary menu bar.
- » The **Save As** button or **Override Template** button, found in a screen's Report Template dialog.

Figure 18-1



The Report Template dialog is accessible from the Infrastructure (Table view), Badges, Card-holders, and Event History screens. New templates are only added to the Report Templates screen via the Report Template dialog.

## How to handle existing report templates via the Report Templates screen

1. Open the Report Templates screen via the Setup task group or Report Templates dialog.
2. If necessary, select a report template from the Saved Templates list.
3. Do one of the following:
  - » Enter or change the information in the displayed parameters (i.e. **Name**, **Description**, **Title**, etc.) and save.
  - » Click **Display Reports**. The screen pertaining to the report template is displayed with the selected report template loaded.
  - » Click **Duplicate**. A copy of the selected report template is displayed. The name of the new report template copy has the text "\_Duplicate" appended to it.  
Edit the displayed parameters as required and save.
  - » Click **Delete**. The selected report template is removed from the system. If the report template is used in a global reflex "[Create Template-based report](#)" on page 548 action, it cannot be deleted.
  - » Click **Discard**. The report template reverts to its last saved version.

Figure 18-2 For more information about the report template parameters, see "[Report Template Screen](#)" on page 529.

# Report Templates: MultiSite Impact

Each site has its own Report Templates. These templates cannot be shared with other sites. The name of the site that owns a Report Template appears in the Report Templates screen.

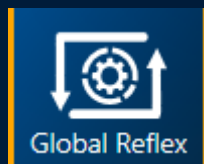
Assigning ownership to a template means that the template is only available to logged-in users who are owned by the same site as the template. This is relevant to:

- » The screen where the template can be applied.
- » The Global Reflex Action **Create Template-based report** where the templates available for the action must be owned by the same site as the Global Reflex where the action is added.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 19:

## Global Reflex



Meets the challenges of the twenty-first century where you can tailor condition triggers and actions to meet the needs of your organization. With a user interface designed to build, what could be a relatively complex scenario, with the skill set of a typical GuardPoint10 operator. Program your global reflexes with the power of a developer without writing code.

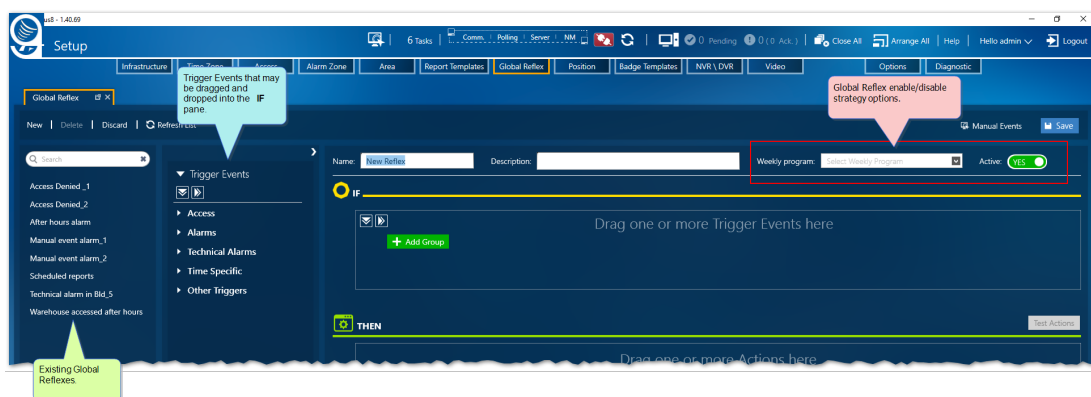
# Adding a New Global Reflex

Use the following steps to create a new global reflex via the Global Reflex screen.

## How to add a new global reflex to the system

1. Go to the Setup Task group and click **Global Reflex**. The Global Reflex screen is displayed.
2. From the action bar, click **New**. New global reflex parameters are displayed.

Figure 19-1



3. Enter a global reflex name. The default name is "New Reflex".  
A global reflex name must be unique.
4. (Optional) In the Description field, enter information specific to the global reflex as it pertains to security.

## Define the condition(s) that will trigger an action in the **IF** pane.

5. From the Trigger Events pane, drag and drop a trigger event from the list into the **IF** pane. The Trigger Event and its specifics are displayed.
6. (Option) Drag and drop additional trigger events into the Trigger Events pane as required.  
When there is more than one trigger event in the pane, it is considered an event trigger group and an OR operator is automatically added to connect the trigger events in the group. Click the OR to change the operator to an AND operator. The AND operator comes with the following:
  - » **Within field:** All event triggers in the event trigger group must be satisfied within the specified time to consider the event trigger group true.
  - » **Reset condition period every time checkbox:** When the checkbox is selected after the AND connected event trigger group is true (all event triggers in the group are satisfied), the group will reset and a new instance of the event triggers in the group will have to be satisfied).
7. Select the checkboxes of the Trigger Event specifics that will be used to define the condition.
8. Select values for each checkbox specified via its accompanying field(s).

For information about each Trigger Event, see "[Global Reflex Screen](#)" on page 532.



9. (Option) Click the **Add Group** button next to an operator (OR or AND), this will embed a new event trigger group to the parent group where the **Add Group** button was clicked.

## Define the action(s) that will be triggered by a Trigger Event.

10. From the Actions pane, drag an action from the list into the **THEN** pane and release the mouse button. the action and its specifics are displayed.
11. Drag additional action from the Actions pane list as required.



**Note:** To invoke an email action, the **SMTP Mail Server** settings must be completed. These settings are found in the Options > System & SQL screen.

12. Set the specifics of the selected action(s) as required.  
For information about each action, see ["Global Reflex Screen" on page 532](#).
13. Click **Save**. The global reflex is saved to the system database.

To test actions, click the **TEST** button. The selected actions are executed regardless of the trigger events added to the **IF** pane.



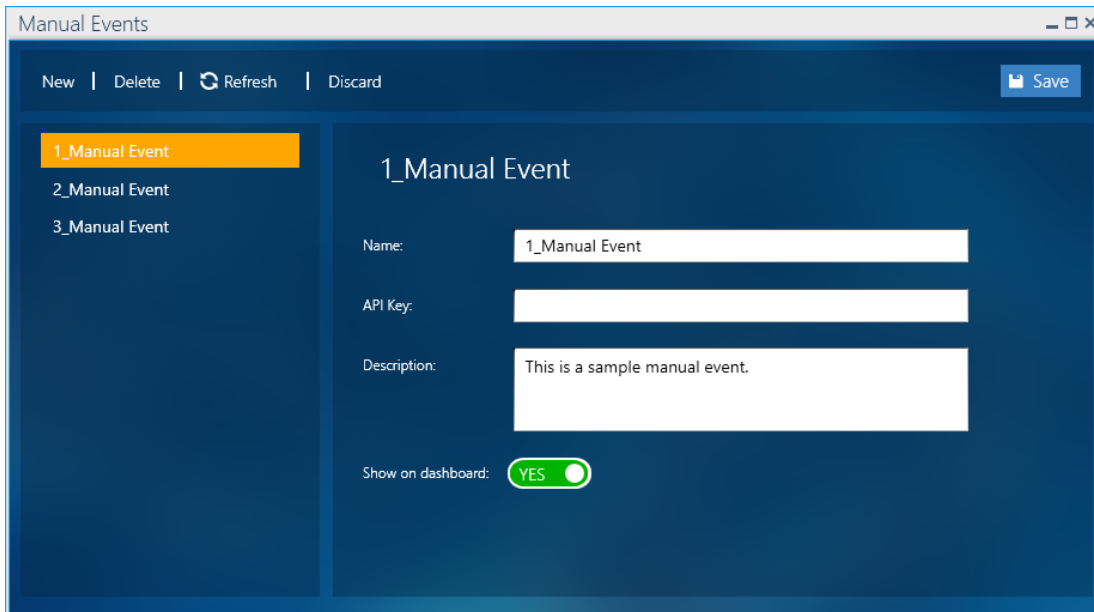
**Note:** To delete a condition in the **IF** pane or an action in the **THEN** pane, click the red **x** on the right side of the condition or action.

# Adding a Global Reflex Manual Event

Use the following steps to create a new Manual Event for a global reflex.

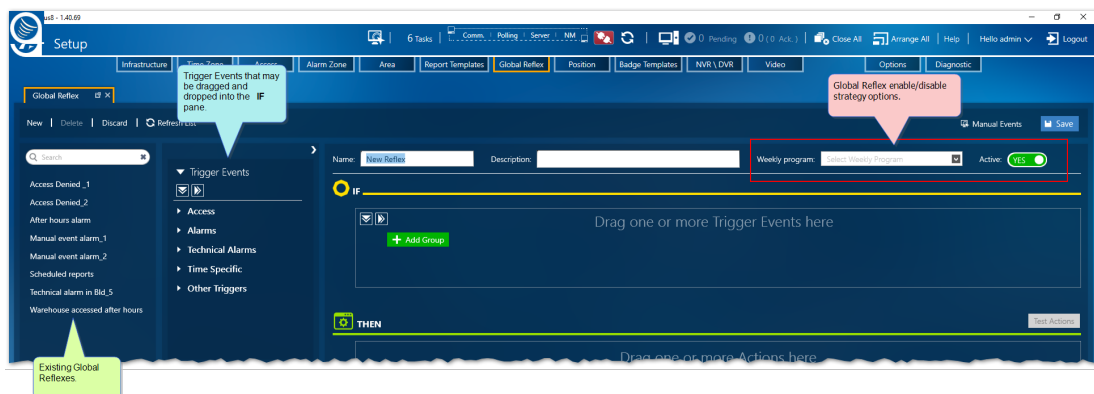
## How to add a new Manual Event to a global reflex

1. Go to the Setup Task group and click **Global Reflex**. The Global Reflex screen is displayed.
2. Click the Manual Events button found next to the Save button at the top right. The Manual Events window is displayed.



3. In the Manual Events window, click New. Fields about the new event appear.
4. Name the Manual Event and enter any other relevant event information as required.
5. Click Save, and then close the Manual Events window.
6. From the Global Reflex action bar, click **New** (or select an existing global reflex). New global reflex parameters are displayed.

Figure 19-2



7. Enter a global reflex name. The default name is "New Reflex".

A global reflex name must be unique.

8. (Optional) In the Description field, enter information specific to the global reflex as it pertains to security.

## Define the condition(s) that will trigger an action in the **IF** area.

9. From the Trigger Events pane, drag the Manual Event trigger from the list into the **IF** pane and release the mouse button. the Trigger Event and its specifics are displayed.
10. From the condition's drop-down list, select the manual event that was previously created in the Manual Events window.
11. Add action to the global reflex as required.

For information about each trigger condition or action, see ["Global Reflex Screen" on page 532](#).

12. Click **Save**. The global reflex is saved to the system database.

To test actions, click the **TEST** button. The selected actions are executed regardless of the trigger events added to the **IF** area.



**Note:** To delete a condition in the **IF** pane or an action in the **THEN** pane, click the red **x** on the right side of the condition or action.

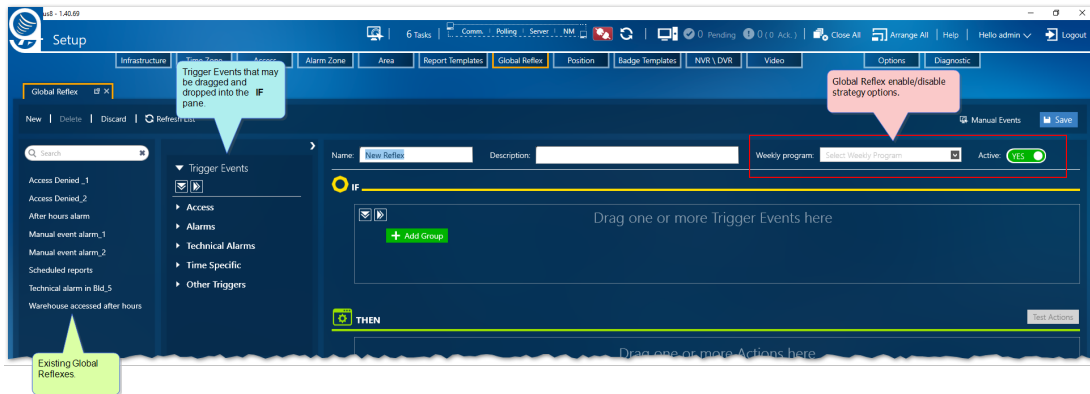
# Enable / Disable Strategy for a Global Reflex

Use the following steps to enable / disable a global reflex via the Global Reflex screen. A global reflex may be enabled or disabled *manually* via the Active setting (Yes No). A global reflex may also be enabled or disabled *automatically* via a selected Weekly Program.

## How to set a global reflex enable/disable strategy

1. Go to the Setup Task group and click **Global Reflex**. The Global Reflex screen is displayed.

Figure 19-3



2. Select an existing global reflex from the pane on the far left. The **IF** and **THEN** panes display the global reflex's Trigger Events and actions.
3. From above the **IF** pane, do one of the following:
  - » Manually enable or disable the global reflex in focus by changing the **Active** Yes or No setting, and click **Save**. The global reflex state changes.
  - » Automatically enable or disable the global reflex in focus by selecting a Weekly Program from the **Weekly Program** drop-down list, and click **Save**. The global reflex state is enabled during the Weekly Program's green period and disabled during the Weekly Program's white period.

**Note:** If the manual **Active** setting is **No**, The global reflex's Weekly Program setting is discarded.

## Deleting a Global Reflex

Use the following steps to delete a global reflex via the Global Reflex screen.

### How to delete a global reflex

1. Go to the Setup Task group and click **Global Reflex**. The Global Reflex screen is displayed.
2. Select an existing global reflex from the pane on the far left. The **IF** and **THEN** panes display the global reflex's Trigger Events and actions.
3. Click **Delete**, the global reflex is removed from the far left pane on the screen and the system database.

# Global Reflex: MultiSite Impact

Each site has its own Global Reflexes. These Global Reflexes cannot be shared with other sites. The name of the site that owns a Global Reflex appears below the **Save** button.

A Global Reflex owned by the Root site may use assets owned by the Root site as well as assets owned by other sites (this includes cardholders with a **Share Type** of **Shared** or **Global**). However, a Global Reflex owned by a non-Root site may only use assets and cardholders owned by the same site that owns the Global Reflex.

Each site has its own Manual Events. These Manual Events cannot be shared with other sites, except for a Global Reflex owned by the Root site.

The list of saved Global Reflexes will only show those Global Reflexes owned by sites where the logged-in user has authorization.

## Add a Global Reflex

1. From the Action menu, click **New**.

If the logged-in user is only authorized in their owner site, the new Global Reflex will have the same owner site as the logged-in user.

If the logged-in user is authorized in multiple sites, select the site that will own the new Global Reflex from the **New** button's drop-down list.

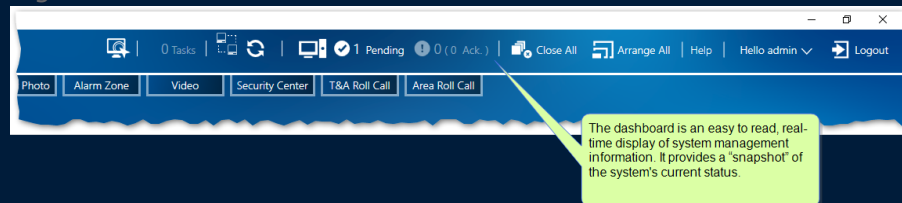
2. Complete new Global Reflex details (triggers and actions), and then click **Save**.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 20:

## Dashboard

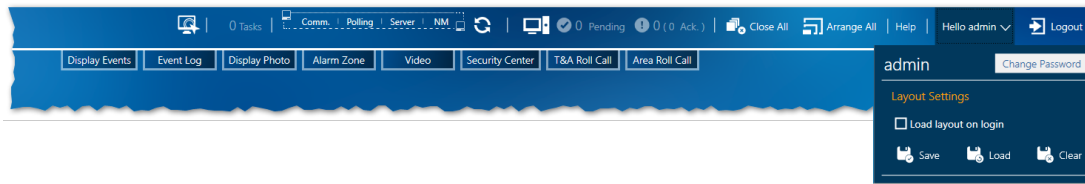
Figure 20-1



The dashboard is an easy-to-read, real-time display of system management information. It provides a "snapshot" of the system's current status and provides access to information that may require attention.


# Dashboard Content & Actions

Figure 20-2

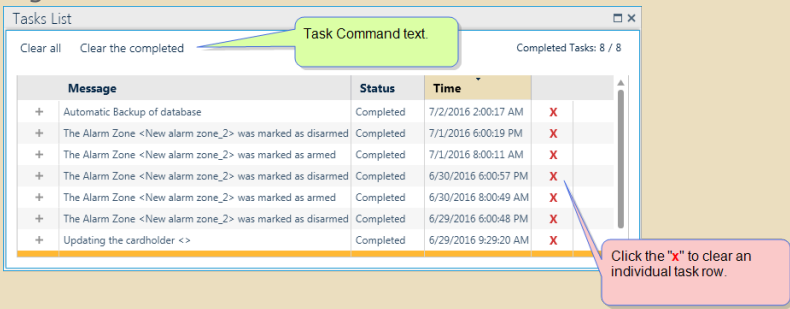





Use the following table to understand and respond to dashboard items.

Dashboard Item Details

Item	Details
<p>Activate Manual Events</p>	<ul style="list-style-type: none"> <li>» <b>Description:</b> A manual event is a global reflex trigger without conditions attached to it.  <div style="text-align: center; margin: 10px 0;"> <p>Figure 20-3</p>  </div> </li> <li>» <b>Operator Response:</b> If one or more manual events exist, click the Activate Manual Events icon on the dashboard. A list of manual events is displayed. Click a manual event to activate it. This means that all global reflex actions associated with the manual event will execute. For more information about manual events, see <a href="#">"Global Reflex Screen" on page 532</a> and <a href="#">"Adding a Global Reflex Manual Event" on page 328</a>.</li> <li>» If there are no manual events set to show on the Dashboard, the icon will be disabled.</li> <li>» The availability of the Activate Manual Events icon depends on the logged-in operator's profile.</li> </ul>



Item	Details
Tasks	<p>» <b>Description:</b> A task is an event that takes place in the system. An event can be technical (i.e. the transfer of data from the system database to a controller) or non-technical (i.e. after a cardholder scans their badge at a particular reader, the alarm zone, where the reader is located, is disarmed).</p> <p>Generally, tasks that appear in the Task List are those tasks that are transparent to the operator during normal GuardPoint10 operations.</p> <p>When a task event is started, the number next to the Task item is incremented. When the same task ends, that too is an event and the Task item increments again.</p> <p>» <b>Operator Response:</b> If a task exists, click <b>Tasks</b> on the dashboard. The Task List dialog is displayed.</p> <p>Figure 20-4</p>  <p>From the Task List dialog, you can see a description of each task along with their status and timestamp.</p> <p><b>Clear all</b> tasks or just <b>Clear completed</b> tasks via the command text above the dialog table.</p> <p>Select the <b>Keep list clean</b> checkbox to automatically limit the number of events in the list. The last 50 events that have been started and not yet completed will be listed. This will keep the list of events manageable for users to monitor.</p> <p>To clear an individual task from the table click the red <b>x</b> on the right side of the task row.</p>

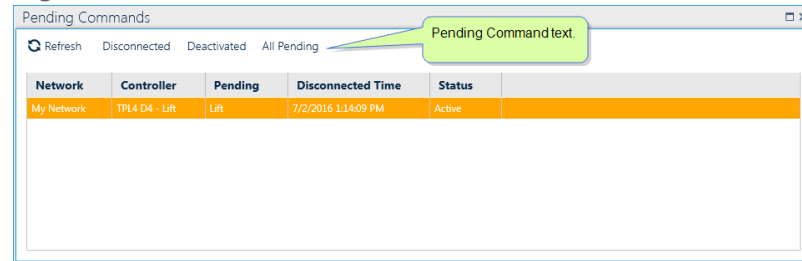
Item	Details
Connection Indicators	<p>» <b>Description:</b> An expandable icon that references the following indicators:</p> <ul style="list-style-type: none"> <li>» Controller communication status</li> <li>» Polling status</li> <li>» GPPServer (server) status</li> <li>» AcsNMService (Network Manager) service status</li> </ul> <p>» <b>Operator Response:</b> If a connection issue exists that requires attention, the icon will flash red. Click the icon to expand the connection indicators and discover the issue by placing the mouse pointer over the flashing text in the expanded view or clicking the indicators to display more information about the indicator-related issues.</p> <p>Click an expanded Comm icon again to contract it.</p>
Deactivated Controller (may not be visible)	<p>This indicator only appears when one or more controllers are deactivated. Click the indicator to display details about deactivated controllers.</p> 
Check Communication	<p>Pings the various controllers on the site.</p> 
System Hardware Pre-requisite status	<p>» <b>Description:</b> A flashing or non-flashing red icon appears when there is machine hardware that does not satisfy mandatory prerequisites.</p> <p>Figure 20-5</p>  <p>» <b>Operator Response:</b> If one or more hardware prerequisites are not met, click the red icon on the dashboard. A message displays listing hardware non-compliance issue details.</p> <p>The red icon only evaluates the machine where the icon is displayed. If there are no prerequisite compliance issues, the icon is white.</p> <p>The flashing behavior is set in the Options screen's <a href="#">"System &amp; SQL Tab"</a> on <a href="#">page 577</a>.</p>

**Item****Details**

Pending

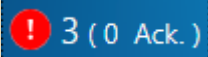
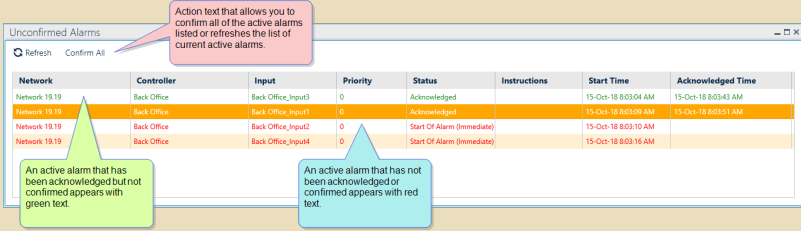
- » **Description:** Pending statuses are those statuses that require operator intervention.
- » **Operator Response:** If a pending status exists, click **Pending** on the dashboard. The Pending Commands dialog is displayed.

Figure 20-6



From the Pending Command window, you can see details about each status. To change the view of the table in the window, use the command text above the table.

Double-click a row in the table to open the GuardPoint10 screen about the pending command.

Item	Details																																								
<p>Active Alarm Indicators</p>	<p>» <b>Description:</b> The number of active alarms that require operator attention. These active alarms must be acknowledged by an operator and then confirmed. However, an operator may take a shortcut and confirm all active alarms which would bypass the acknowledgment operation.</p> <p>» <b>Operator Response:</b> If one or more active alarms exist, an exclamation mark in a flashing red circle appears on the dashboard followed by the number of active alarms that need to be confirmed. If alarms have been acknowledged, the number of acknowledged alarms followed by "Ack" appear in the parentheses.</p> <p>Click  on the dashboard. The Unconfirmed Alarms dialog is displayed.</p> <p>Figure 20-7</p>  <p>The screenshot shows a dialog titled "Unconfirmed Alarms" with a "Refresh" button and a "Confirm All" button. Below the buttons is a table with the following data:</p> <table border="1"> <thead> <tr> <th>Network</th> <th>Controller</th> <th>Input</th> <th>Priority</th> <th>Status</th> <th>Instructions</th> <th>Start Time</th> <th>Acknowledged Time</th> </tr> </thead> <tbody> <tr> <td>Network 18.19</td> <td>Back Office</td> <td>Back Office_Input3</td> <td>0</td> <td>Acknowledged</td> <td></td> <td>15-Oct-18 8:03:04 AM</td> <td>15-Oct-18 8:03:43 AM</td> </tr> <tr> <td>Network 18.19</td> <td>Back Office</td> <td>Back Office_Input1</td> <td>0</td> <td>Acknowledged</td> <td></td> <td>15-Oct-18 8:03:09 AM</td> <td>15-Oct-18 8:03:51 AM</td> </tr> <tr> <td>Network 18.19</td> <td>Back Office</td> <td>Back Office_Input2</td> <td>0</td> <td>Start Of Alarm (Immediate)</td> <td></td> <td>15-Oct-18 8:03:10 AM</td> <td></td> </tr> <tr> <td>Network 18.19</td> <td>Back Office</td> <td>Back Office_Input4</td> <td>0</td> <td>Start Of Alarm (Immediate)</td> <td></td> <td>15-Oct-18 8:03:16 AM</td> <td></td> </tr> </tbody> </table> <p>Callouts in the screenshot:</p> <ul style="list-style-type: none"> <li>A pink callout points to the "Confirm All" button: "Action text that allows you to confirm all of the active alarms listed or refreshes the list of current active alarms."</li> <li>A green callout points to the first row: "An active alarm that has been acknowledged but not confirmed appears with green text."</li> <li>A blue callout points to the last row: "An active alarm that has not been acknowledged or confirmed appears with red text."</li> </ul> <p>From the Unconfirmed Alarms dialog, you can see details about each alarm's status (you may have to drag the right side of the dialog to see all of the information).</p> <p>To resolve an active alarm, right-click on a row and select an action (<b>Acknowledge</b> or <b>Confirm</b>) from the context menu. Alternatively, click the <b>Confirm All</b> action text above the table to confirm all listed active alarms, regardless of their acknowledge status.</p> <p>If the alarms input is linked to an icon on a map in the Security Center, you have an additional <b>Navigate to map</b> context menu option. When selected the relevant map will automatically display on a Security Center screen.</p>	Network	Controller	Input	Priority	Status	Instructions	Start Time	Acknowledged Time	Network 18.19	Back Office	Back Office_Input3	0	Acknowledged		15-Oct-18 8:03:04 AM	15-Oct-18 8:03:43 AM	Network 18.19	Back Office	Back Office_Input1	0	Acknowledged		15-Oct-18 8:03:09 AM	15-Oct-18 8:03:51 AM	Network 18.19	Back Office	Back Office_Input2	0	Start Of Alarm (Immediate)		15-Oct-18 8:03:10 AM		Network 18.19	Back Office	Back Office_Input4	0	Start Of Alarm (Immediate)		15-Oct-18 8:03:16 AM	
Network	Controller	Input	Priority	Status	Instructions	Start Time	Acknowledged Time																																		
Network 18.19	Back Office	Back Office_Input3	0	Acknowledged		15-Oct-18 8:03:04 AM	15-Oct-18 8:03:43 AM																																		
Network 18.19	Back Office	Back Office_Input1	0	Acknowledged		15-Oct-18 8:03:09 AM	15-Oct-18 8:03:51 AM																																		
Network 18.19	Back Office	Back Office_Input2	0	Start Of Alarm (Immediate)		15-Oct-18 8:03:10 AM																																			
Network 18.19	Back Office	Back Office_Input4	0	Start Of Alarm (Immediate)		15-Oct-18 8:03:16 AM																																			
<p>Close All</p>	<p>Closes all screens visible in the console display (i.e. tabs, popout windows and tiles). There are some floating screens that may not close if they are in an editable state (i.e. Cardholder details).</p>																																								
<p>Arrange All</p>	<p>Arranges all opened screens, into their own individual tiles as tabs. This allows you to view different parts of the system on the console at the same time.</p>																																								
<p>Help</p>	<p>A drop-down menu where the operator can open the <a href="#">"License screen "</a> on <a href="#">page 435</a>, online Help (or, press F1), About GuardPoint10 window.</p>																																								
<p>Session Details</p>	<p>Displays the name of the operator currently logged in to GuardPoint10, which is immediately followed by a button that allows the operator to log out.</p> <p>The "Hello &lt;operator name&gt;" includes a drop-down list where the operator can Save, Load or, Clear a screen layout</p>																																								

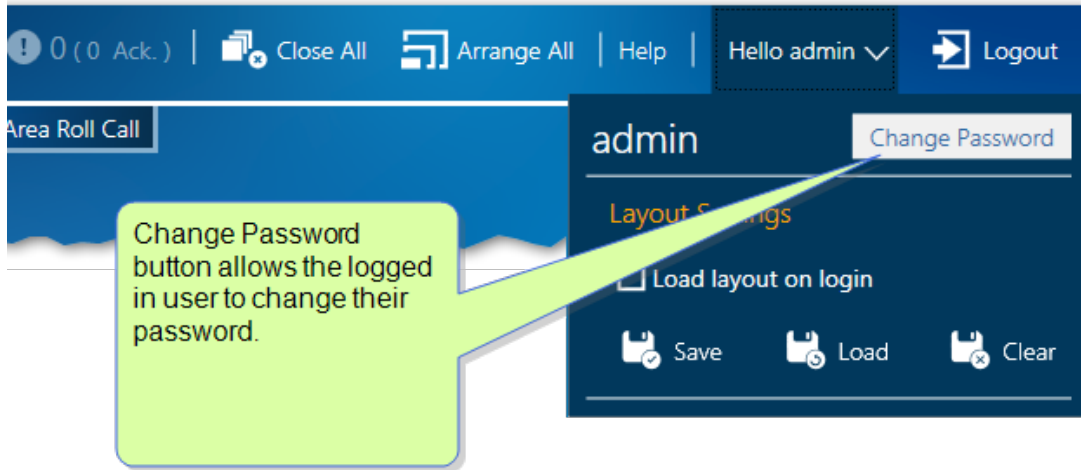
# Operator password management

This feature allows an operator to change their password.

## To change the password

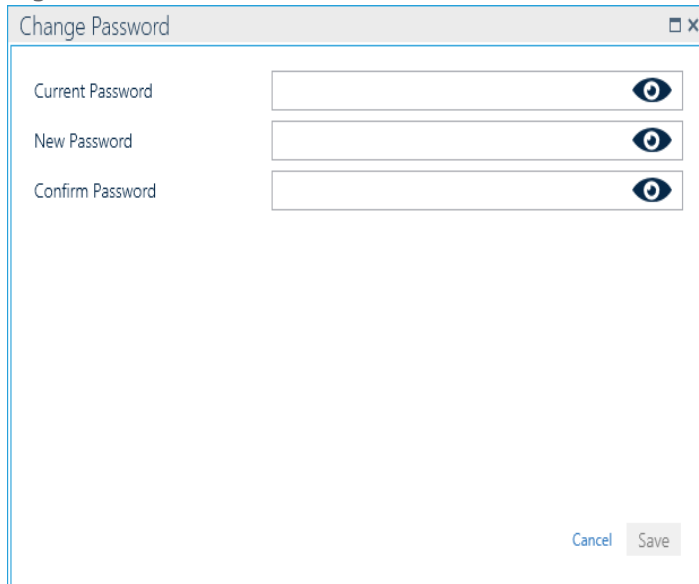
1. From the dashboard click the Down Arrow immediately following the operator name. The Layout settings are displayed along with a **Change Password** button.

Figure 20-8



2. Click **Change Password**. A Change Password dialog is displayed.

Figure 20-9



3. Enter information in the dialog and click **Save**. The next time the user logs in, they will need to enter the new password.

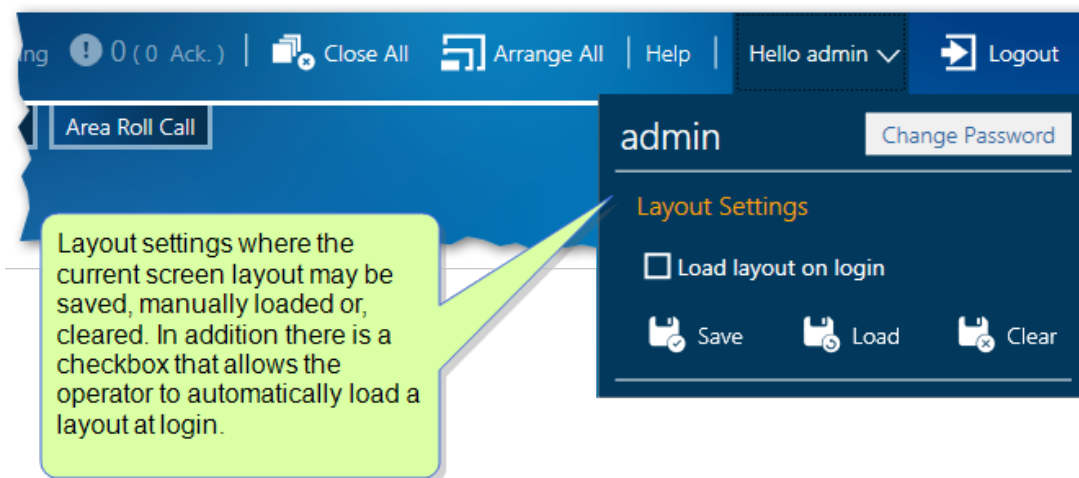
# Operator specific screen layout management Save / Load / Clear

This feature allows an operator to save a layout for their specific use. Each operator has their own unique layout load option. A layout is a stack of GuardPoint10 screens saved as a snapshot. This saved snapshot will be available for automatic loading at login or, manual loading via a Load button.

## To save a layout

1. Open the screens that will be included in the layout snapshot.
2. From the dashboard click the Down Arrow immediately following the operator name. The Layout settings are displayed.

Figure 20-10



3. Do one of the following:
  - » Click **Save**: A snapshot of the current screen layout is saved and available for loading. Only one layout may be saved at any given time per operator.
  - » Click **Load**: The saved layout snapshot is loaded.
  - » Click **Clear**: A previously saved layout snapshot is removed from the system.
  - » Select the **Load layout on login** checkbox: The layout snapshot will be automatically loaded every time the operator logs in to GuardPoint10.

**Note:** If a layout snapshot is particularly complex, the load may be unusually slow. The operator can always unselect the **Load layout on login** checkbox to disable the automatic load option.

# CHAPTER 21:

## Diagnostics



The Diagnostics screen provides sophisticated diagnostic tests and solution tools for both the typical operator and the operator with advanced system knowledge (a system troubleshooter). The Diagnostic tools not only provide an on-screen status and efficiency report. They also provide solution-based tasks to resolve system issues.

Because many of the solution-based tasks are very powerful and irreversible, it is a best practice that, unless stated otherwise, only operators with advanced system knowledge perform the solution-based tasks available via the Diagnostic screen.

# Checking Controller Communications

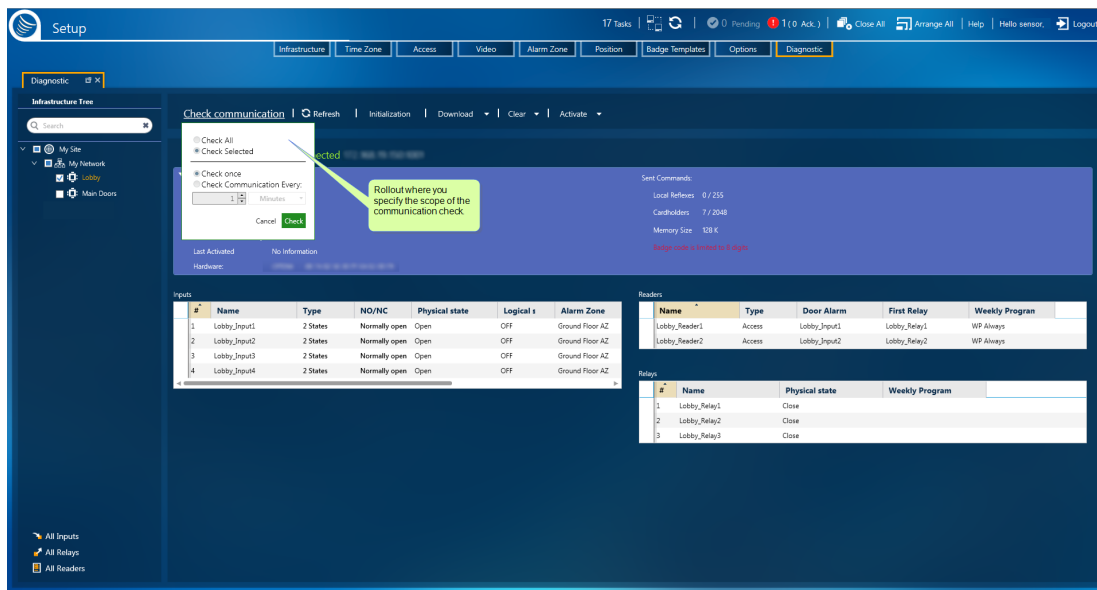
Use the following steps to check the communication between one or more controllers in the system.

**Note:** The communication check is passive and can be performed by operators of any skill level.

## How to check controller communication

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. From the action bar, click **Check Communication**. A rollout appears where you specify the scope of the communication check.

Figure 21-1



3. In the communication rollout, choose from the following options:
  - » If one or more controllers are selected (a controller checkbox contains a checkmark). You can select:
    - » **Check All:** All of the controllers on the site are checked, regardless of the state of the controllers checkbox.
    - » **Check Selected:** Only the selected controllers are checked.If none of the controllers are selected, **Check All** will be the only available option.
  - » In the second half of the communication rollout, specify the frequency of the communication check. The available options are as follows:
    - » **Check once:** A single check is performed.
    - » **Check Communication Every:** Checks are performed at intervals, The intervals are based on time units entered below the option.
4. Click **Check**. If successful, a checkmark with a green background temporarily appears to the right of the controller in the infrastructure tree. If the communication check fails, a checkmark with a red background temporarily appears.



# Reset a Controller

Use the following steps to reset a controller. Reset means that you are powering off and then powering on a selected controller. There is no data transfer.



**Note:** The reset task can be performed by operators of any skill level.

## How to reset a controller

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more controllers that will be reset (a controller checkbox contains a checkmark).
3. From the action menu, click **Download > Reset Controller**. The selected controller(s) are powered off and then powered on again.


Until the reset task is completed, readers and other entities attached to the selected controller may be offline.

# Activate/Deactivate a Controller

An activated controller will receive polling-related messages from the system. The controller, and its connected entities, will perform tasks -including polling- as expected.

A deactivated controller will not send polling-related messages and the controller's event buffer will likely overflow. Besides the loss of data, due to the buffer overflow, a deactivated controller and its connected entities operate normally.

Use the following steps to activate or deactivate a controller.



**Note:** The task described in this topic can have far-reaching implications. Critical data may be inadvertently lost. A best practice is for this task to be performed by an operator with advanced system knowledge.

## How to activate or deactivate a controller

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more active controllers and do one of the following:
  - » If the controller(s) will be deactivated (a controller checkbox contains a checkmark), click **Activate > Deactivate** from the action bar. The controller(s) that was active is now deactivated and appear dulled in the infrastructure tree.
  - » If the controller(s) will be activated (a controller checkbox contains a checkmark), and then click **Activate > Activate** from the action bar. The controllers are activated and appear brighter white in the infrastructure tree.

Alternatively, a controller may be activated or deactivated from the Infrastructure screen by right-clicking a controller in the Infrastructure tree and selecting one of the activate or deactivate context menu items. For more information, see "[Edit/Delete a Controller](#)" on page 59.

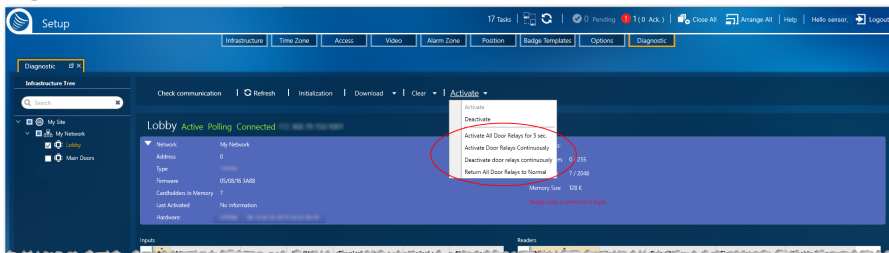
# Override a Normal Door Relay State

Use the following steps to override the normal state of a controller's relay(s). This override would be especially useful in case of fire. You would activate all relays, which would open all of the doors and allow personnel to escape.

**Note:** Operators of any skill level can perform the door relay override operations.

The override options are in the following action menu. They allow you to do the follows:

Figure 21-2



## How to activate a controller's door relay(s)

This task will leave all of the doors connected to a selected controller, open continuously, regardless of any other change (i.e. controller reset).

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more active controllers where the door relay(s) will be overridden (a controller checkbox contains a checkmark).
3. From the action bar, click **Activate > Activate Door Relays Continuously**. The doors connected to a selected controller will remain open until the state is changed by another action in the Diagnostic screen's **Activate** action menu.

## How to deactivate a controller's door relay(s)

This task will leave all of the doors connected to the selected controllers, locked continuously, regardless of any other change (i.e. controller reset).

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more active controllers where the door relay(s) will be overridden (a controller checkbox contains a checkmark).
3. From the action menu, click **Activate > Deactivate Door Relays Continuously**. The doors connected to a selected controller will remain locked until the state is changed by another action in the Diagnostic screen's **Activate** action menu.

## How to return a controller's door relays to their normal state

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more active controllers where the door relay(s) will be returned to its normal state (a controller checkbox contains a checkmark).
3. From the action bar, click **Activate > Return All Door Relays to Normal**. The doors connected to a selected controller will return to their normal state.

## How to temporarily activate a controller's door relays

This task will leave all of the doors connected to a selected controller open for 5 seconds, regardless of any other change (i.e. controller reset).

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more active controllers where the door relays will be temporarily overridden (a controller checkbox contains a checkmark).
3. From the action bar, click **Activate > Activate All Door Relays for 5 sec.** The doors connected to a selected controller will remain open for 5 seconds, and then return the relays to their normal state.

## Overwrite a Controller's Local Data

Use the following steps to overwrite data on a selected controller's local database with data stored in the system database.



**Note:** These tasks are severe and far-reaching. Critical data may be inadvertently lost. A best practice is for this task to be performed by an operator with advanced system knowledge.

## How to overwrite all local controller data with data from the system database

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more controllers where data will be overwritten (a controller checkbox contains a checkmark).
3. From the action bar, click **Initialization**. Data, which was previously acquired from each of the selected controllers' local databases, is downloaded from the system database to the respective controller's local database, where it will overwrite preexisting local data.

## How to overwrite all local controller data, except for cardholder definitions, with data from the system database

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more controllers where data will be overwritten (a controller checkbox contains a checkmark).
3. From the action bar, click **Download > Initialization (Except for Cardholder Definitions)**. Data, which was previously acquired from each of the selected controllers' local databases, is downloaded from the system database to the respective controllers, where it will overwrite preexisting local data. The only data that will remain intact in the controller's local database is the cardholder definitions.

# Send Selective Data to a Controller's Local Database

Use the following steps to overwrite selective data in a controller's local database with data stored in the system database.



**Note:** Except for **Send Time and Date**, the tasks described in this topic can have far-reaching implications. Critical data may be inadvertently lost. A best practice is for these tasks to be performed by an operator with advanced system knowledge.

## How to overwrite selective data in a controller's local database

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more controllers where selective data will be overwritten (a controller checkbox contains a checkmark).
3. From the action bar, click **Download**, and then choose the system data that you want to send and overwrite on a controller's local database. The options are as follows:
  - » **Send Time and Date:** Synchronizes the time and date in the controller with the time and date on the server, where the system database is located.
  - » **Send Daily and Weekly Programs:** Overwrites Daily Programs and Weekly Programs stored in a controller's local database with Daily Programs and Weekly Programs stored in the system database.
  - » **Send All Cardholders:** Overwrites cardholder data stored in a controller's local database with cardholder data stored in the system database.
  - » **Send Reader Definitions:** Overwrites reader data stored in a controller's local database with reader data stored in the system database.
  - » **Send Controller Definitions:** Overwrites information that identifies the controller with controller information stored in the system database.

# Clearing Memory in a Controller

Use the following steps to clear all or selective data in a controller's local database.



**Note:** The tasks described in this topic can have far-reaching implications. Critical data may be inadvertently lost. A best practice is for these tasks to be performed by an operator with advanced system knowledge.

## How to clear all data in a controller's local database

This is the equivalent to reformatting a controller's memory.

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more active controllers where data will be cleared (a controller checkbox contains a checkmark).
3. From the action bar, click **Clear > Clear Memory**, and then confirm the operation. The controller's memory is reformatted.

## How to clear selective data in a controller's local database

1. Go to the Setup Task group and click **Diagnostic**. The Diagnostic screen is displayed.
2. Select one or more active controllers where data will be cleared (a controller checkbox contains a checkmark).
3. From the action bar, click **Clear**, and then choose the controller data that you want to clear. The options are as follows:
  - » **Clear All (Except Cardholder Definitions)**: Removed all of the data from a controller's database, except for cardholder definitions.
  - » **Clear Event Buffer**: Removed all event data from a controller's **Event Buffer**<sup>1</sup>.
  - » **Clear Cardholder Definitions**: Only removes cardholder information from a controller's database. All other data remains intact.

---

<sup>1</sup>A temporary storage area in a controller. The buffer contains system events involving entities attached to the controller. An Event buffer is read and cleared by the system during polling (a query as to whether a controller has any data to transmit).

## Diagnostic: MultiSite Impact

Diagnostic actions on a selected controller can only be performed by a logged-in user whose owner site also owns the controller where the action will take place.

A super user can perform all Diagnostic actions on any controller in the system.

# SECURITY TASKS

Through a well designed and properly configured system, GuardPoint10 assists your team of security professionals with performing their duties. The following modules provide security personnel with monitoring tools and access to protocol instructions for required actions.

- » ["Display Events Screen" on page 353](#)
- » ["Event Log Screen" on page 357](#)
- » ["Display Photo" on page 361](#)
- » ["Alarm Zones \(Security\)" on page 365](#)
- » ["Video \(Security\)" on page 373](#)
- » ["Security Center" on page 389](#)
- » ["Area Roll Call" on page 401](#)
- » ["Visitor Control Management" on page 409](#)
- » ["From the Dashboard: License, Help, and About" on page 435](#)



**Setup**  
**Management**  
**Security**

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**



# CHAPTER 22:

## Security Tasks: MultiSite Impact

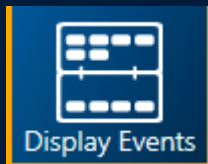
All Security Task screens allow the logged-in user to work within the scope of the sites where the user has authorization. For example, if a user has authorization to Site\_1 and Site\_2 and the user is owned by Site\_1:

- » Only Access events taking place in Site\_1 and Site\_2 will be visible to the user in the relevant screens.
- » If an Access event occurs at a shared reader owned by Site\_1 or Site\_2 and the cardholder is not known in either site, the user will see the event, but will not have access to the cardholder's details.
- » The Event Log will show all events that take place at assets owned by Site\_1 and Site\_2.
- » If an alarm even starts in Site\_1 or Site\_2, the user will see it in the relevant screens and the Dashboard where it can be acknowledged or confirmed. However, if an alarm event is triggered at an input **shared** with Site\_1 or Site\_2, the user will see the alarm but, will not be able to acknowledge or confirm it.
- » The user will be able to perform all alarm zone action for Alarm Zones owned by Site\_1 or Site\_2.
- » The user will be able to observe and perform all map and icon-related actions on maps owned by Site\_1 or Site\_2.
- » In the Area Roll Call screen, the user will be able to manage and move cardholders from Area to Area within the scope of Site\_1 and Site\_2.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 23:

## Display Events Screen



The Display Events screen provides operators with a quick and convenient single point of reference to see various types of events recorded in a real-time in a graphic display.

The interface shows:

- » Alarms and failed attempts to perform an operation.
- » Cardholder activity.
- » A real-time updated table of all events (physical and virtual) that take place within the Sensor Access system.

# Managing Events from an Event Card in the Display Events Screen

The top of the Display Events screen contains alarms that may require an operator's attention and failed cardholder access attempts as well as other system events that qualify as alarms. Just below these events is an area where successful cardholder access events are displayed.

Each event, regardless of type, appears in a card-like graphic. Click a card to flip it and reveal more information about the event. To display the front of the card, click the card again.

## Alarm events

Some alarms require management. These alarm cards have the following management context menu options:

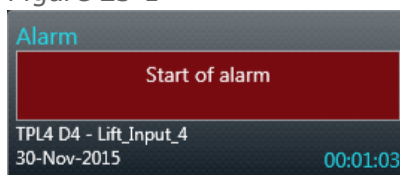
- » **Acknowledge:** The alarm is recognized by the operator. An acknowledgment is reflected on a new alarm card and in the pending area of the dashboard. An alarm must be acknowledged before it can be confirmed. The acknowledged event can be seen in the Event log (see ["Display Events Screen" on the previous page](#)).
- » **Confirm:** Opens a Confirmation dialog where you may enter a description of the alarm and details that confirm your observation of the alarm. Click **Confirm** in the dialog to complete the confirmation process. After an alarm is confirmed, a new confirmation card appears in the Events screen. The confirmed event can also be seen in the Event log (see ["Display Events Screen" on the previous page](#)).
- » **Navigate to Map:** If an alarm's input is linked to an icon that appears on a map in the Security Center, the map will be automatically displayed.

Use the following steps to manage an alarm event via the Display Events screen.

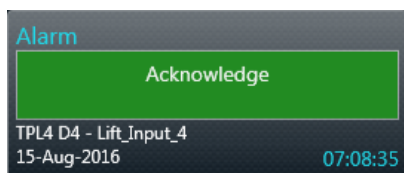
## How to manage an alarm event from an event's card

1. Go to the Security Task group and click **Display Events**. The Display Events screen is displayed.
2. After an alarm is triggered and appears in the top half of the screen, right-click the alarm card and do one of the following:

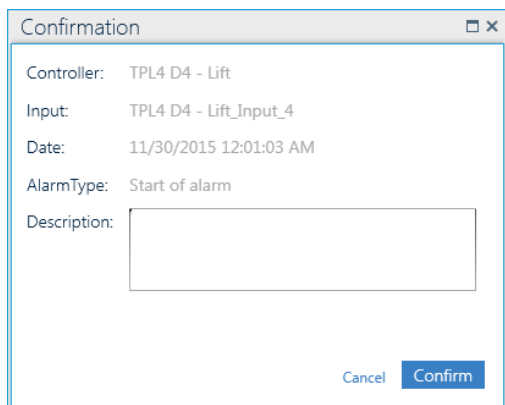
Figure 23-1



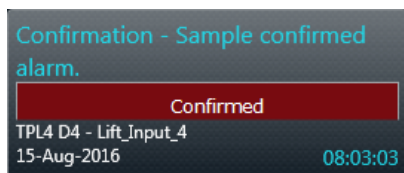
- » Click **Acknowledge** in the card's context menu. A new acknowledge card about the alarm event appears. The background of the new card's alarm text is green and the status text reads "Acknowledged". In addition, the system database is updated and the Events' Log table displays the acknowledgment in a new row.



- » Click **Confirm** in an acknowledged alarm card's context menu. An Alarm Confirmation dialog is displayed.



In the dialog, enter a comment if necessary, and then click **Confirm**. A new confirm card about the alarm event appears. The background of the card's alarm text is red and the status text reads "Confirmed"; if a comment was entered in the dialog, the comment will also appear on the card. In addition, the system database is updated and the Events' Log table displays the Confirm event in a new row.



- » Click **Navigate to map** in the card's context menu. If an alarm's input is linked to an icon that appears on a map in the Security Center, the map will be automatically displayed. For more information about alarms in the Security Center, see "[Addressing Alarms via a Security Center Icon](#)" on page 391.

## Access events (Access Granted, Access Denied)



**Note:** An Access Denied event will appear inline with the other non-access granted event cards.

The **Access Denied** type appears with a simple clear explanation why access was denied (i.e. "Unknown Badge Code"). However, there is one **Access Denied** type called **Inhibited Cardholder** that may require some more information.

The **Inhibited Cardholder** type may occur in the following two cases:

- A reader has the weekly program **WP Personal** selected in the access group of the cardholder, and the cardholder does not have a Personal Weekly Program selected in their details.

- A reader assigned **Badge Type** does not match the badge type of a cardholder's swiped badge.

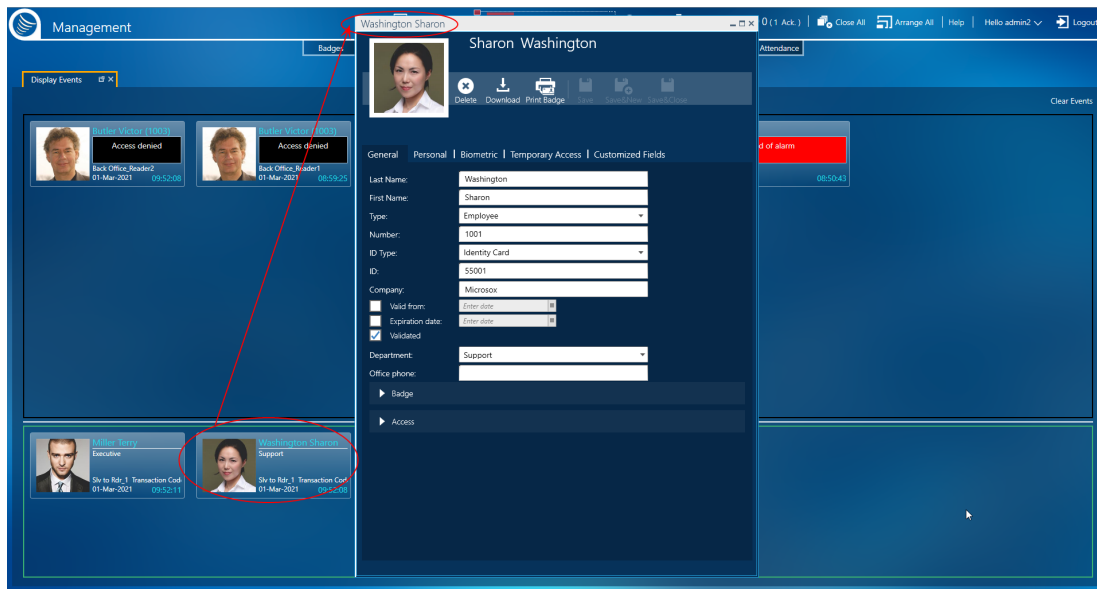
## How to display and possibly edit cardholder details from an access event's card

1. Go to the Security Task group and click **Display Events**. The Display Events screen is displayed.
2. After an access event is triggered and the card appears in the top half of the screen, double-click the card. The card flips and the cardholder's details are displayed.



**Note:** An access event may take the form of an access granted event or an access failed event (denied or unsuccessful). If an access granted event took place, the card will appear just below the alarm card / denied access card area. Drag the partition line up or down to automatically resize the areas.

Figure 23-2



3. At this point, you can flip the card back to the front and edit the cardholder's details as required. For information about editing a cardholder's details, see ["Editing Cardholder Details" on page 216](#).

# CHAPTER 24:

## Event Log Screen



The Event Log screen provides operators with a quick and convenient view of real-time events in a simple table format. The advantages of tabular format are as follows:

- » Filter by column.
- » Sort by column.
- » Restructure the table via the Group By bar.

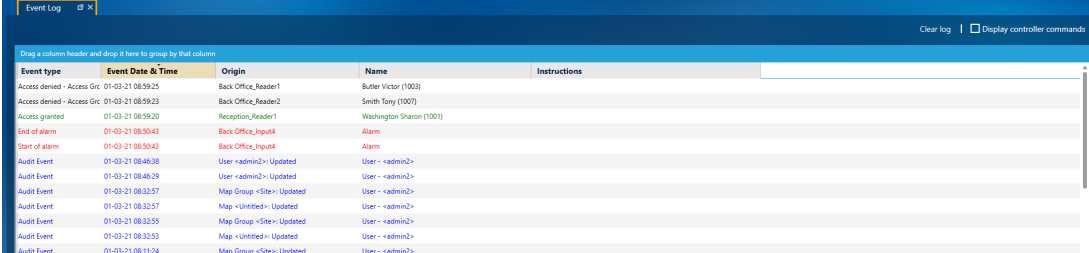
# Managing the Events Table Log

Use the following steps to manage the data displayed in the Event Table Log table via the Events screen.

## How to manage the data displayed in the Event Log Table

1. Go to the Security Task group and click **Event Log**. The Event Log screen is displayed.

Figure 24-1



Event type	Event Date & Time	Origin	Name	Instructions
Access denied - Access Gri	01-03-21 08:59:25	Back Office_Reader1	Butler Victor (1003)	
Access denied - Access Gri	01-03-21 08:59:23	Back Office_Reader2	Smith Tony (1007)	
Access granted	01-03-21 08:59:30	Reception_Reader1	Washington Sharon (1001)	
End of alarm	01-03-21 08:50:43	Back Office_Input4	Alarm	
Start of alarm	01-03-21 08:50:43	Back Office_Input4	Alarm	
Audit Event	01-03-21 08:46:38	User <admin2> Updated	User - <admin2>	
Audit Event	01-03-21 08:46:29	User <admin2> Updated	User - <admin2>	
Audit Event	01-03-21 08:32:57	Map Group <Site> Updated	User - <admin2>	
Audit Event	01-03-21 08:32:57	Map <Untitled> Updated	User - <admin2>	
Audit Event	01-03-21 08:32:55	Map Group <Site> Updated	User - <admin2>	
Audit Event	01-03-21 08:32:53	Map <Untitled> Updated	User - <admin2>	
Audit Event	01-03-21 08:11:24	Map Group <Site> Updated	User - <admin2>	

2. From the action bar, above the Event Log table, do one of the following:

- » Click **Clear Log**. Event data is erased from the log table and new event data will populate the table as the events occur.



**Note:** The record of the events erased from the table still exists in the system database and may be viewed in the Events screen (see "[Event History](#)" on page 251).

- » Select the **Display Controller Commands** checkbox. The Event Log table is filtered to show Controller type events in addition to other event types.



**Note:** The Controller type event filter is not available in the tables Event Type heading filter.

Right-clicking on a Controller type event displays a context menu command that allows you to copy the event data (the data in the Cardholder Name column) to the PC's clipboard. At some point, a technician may request this data to troubleshoot your system.



# How to manage alarms via the Event Log Table

1. Go to the Security Task group and click **Event Log**. The Event Log screen is displayed.

Figure 24-2

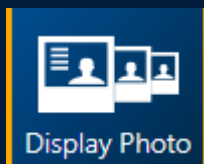
Event type	Event Date & Time	Origin	Name	Instructions
Access denied - Access Grc	01-03-21 08:59:25	Back Office_Reader1	Butler Victor (1003)	
Access denied - Access Grc	01-03-21 08:59:23	Back Office_Reader2	Smith Tony (1007)	
Access granted	01-03-21 08:59:20	Reception_Reader1	Washington Sharon (1001)	
End of alarm	01-03-21 08:59:20	Reception_Reader1	Alarm	
Start of alarm	01-03-21 08:59:20	Reception_Reader1	Alarm	
Audit Event	01-03-21 08:59:20	Reception_Reader1	Alarm	
Audit Event	01-03-21 08:46:29	User <admin2>: Updated	User - <admin2>	
Audit Event	01-03-21 08:32:57	Map Group <Site>: Updated	User - <admin2>	
Audit Event	01-03-21 08:32:57	Map <Untitled>: Updated	User - <admin2>	
Audit Event	01-03-21 08:32:55	Map Group <Site>: Updated	User - <admin2>	
Audit Event	01-03-21 08:32:53	Map <Untitled>: Updated	User - <admin2>	
Audit Event	01-03-21 08:11:24	Map Group <Site>: Updated	User - <admin2>	

2. Right-click an alarm event row. A context menu appears.
3. From the context menu, you can **Acknowledge** or **Confirm** the alarm. If the alarm's input is linked to an input icon on a map, you can click **Navigate to map** to open the relevant map in the Security Center screen. For more information about the Security Center, see "[Security Center](#)" on page 389.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 25:

## Display Photo



The Display Photo screen provides operators with a quick and convenient view of access events with an emphasis on visual recognition via a large photo of the cardholder initiating the event.

Each access event is displayed in a scrollable chronology.

A displayed access event shows:

- » Cardholder details.
- » Cardholder photo (if available).
- » Information about the access event (i.e. accepted, denied, timestamp, and the reader's name).

# Working with the Display Photo Window

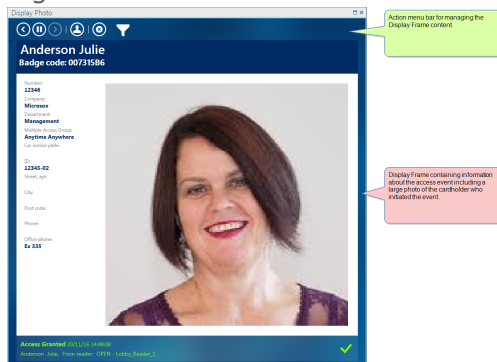
Use the following steps to manage the data displayed in the Display Photo window via the Events Log Table tab.

Multiple Display Photo windows may be opened at the same time simply by clicking the **Display Photo** button. Each instance of the Display Photo window works independently.

## How to manage the Display Photo window


1. Go to the Security Task group and click **Display Photo**. The Display Photo screen is displayed. The initial content of the Display Photo window includes information about the most recent access event.

Figure 25-1



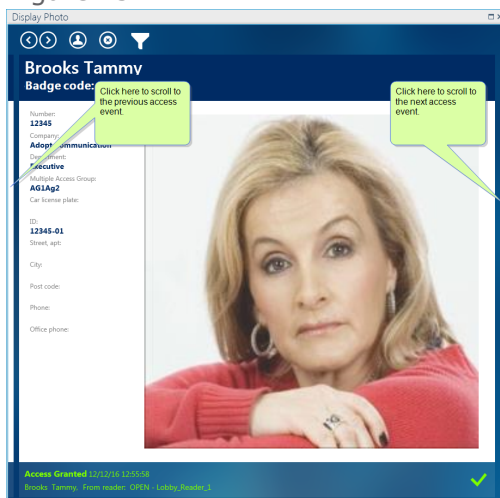
2. From the Display Photo window's action bar, do one of the following:





- » Click  to scroll access events displayed in the Display Photo window's display frame.

Alternatively, click outside the left or right side of the frame of the currently displayed access event to scroll to the next or previous event.


Figure 25-2





- » Click  to show the cardholder details of the cardholder who initiated the currently displayed access event.

- » Click  to clear the Display Photo window's display frame of all access event information logged at that time.

This action will not delete the events from the system log, but will only remove them from the Display Photo window.

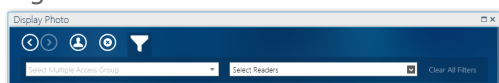
- » Click  to pause the Display Photo window's live update action to the display frame.

- » Click  to restart a paused Display Photo window's live update action.

- » Click  to show the filter fields where you can narrow the range of access events scrollable in the Display Photo window.

The filters available are **Filter by Multiple Access Group** and **Filter by Reader**. The filters can work independently or together.

Figure 25-3

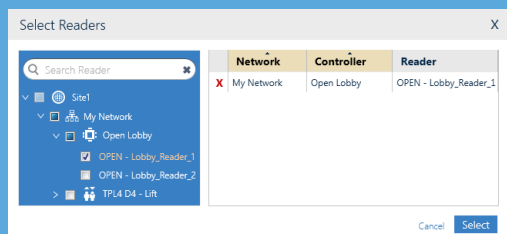


If scrollable access events are filtered, the funnel in the Filter button will turn yellow .

### Filter Examples:

To only display access event information, where the cardholder who initiated an event is assigned a particular Multiple Access Group, select the Multiple Access Group from the **Filter by Multiple Access Group** field.

To only display access event information that took place at a specific reader, select the reader from the **Filter by Reader's** Select Reader dialog and click **Select**.



The reader name will appear in the **Filter by Reader** field and the **Filter by Multiple Access Group** will be disabled.

To use both fields together, first, select a Multiple Access Group and then select a reader. Only the readers accessible via the selected Multiple Access Group will be available in the Select Reader dialog.

After selecting a filter, the scrollable display frame will automatically update and only show the access events that satisfy the selected filter.

To remove a filter, click **Clear All Filters** found at the right of the **Filter by Reader** field.

## Escort display options in the Display Photo window

If an access event includes an escort, this means the access event requires two badge swipes one from the cardholder who requires an escort and one from the cardholder who is doing the escorting, a **View Escort** checkbox appears over the image of the initial access badge swipe event.

Select the **View Escort** checkbox to display access information about both cardholders involved in the access event side-by-side.

Clear the **View Escort** checkbox to display access information about a single access event where escort information is not displayed.

For information about escort rules, see "[Escort Rules for Access Events](#)" on page 697.

# CHAPTER 26:

## Alarm Zones (Security)



The Alarm Zone Security screen enables an operator to override an Alarm Zones state (governed by a Weekly Program or reflex defined in the Alarm Zones' Setup), via a simple straightforward screen interface.

For information about the Alarm Zones (Setup) screen, see "[Alarm Zones \(Setup\)](#)" on page 301.

# Overriding an Alarm Zone's Status

Use the following steps to manually override an alarm zone's status via the Alarm Zone Security screen.

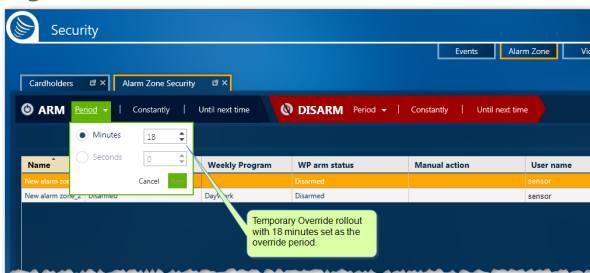
## How to manually override the current status of an alarm zone

1. Go to the Security Task group and click **Alarm Zone**. The Alarm Zone Security screen is displayed.
2. Select the row of an alarm zone where the status will be manually overridden.
3. Decide if you are going to override with an ARM command or a DISARM command.
4. If you are going to override with a DISARM command, go to Step 5. If you are going to override with an ARM command, do one of the following:

### Temporarily arm the alarm zone in focus

- a. Click **Period** in the Arm part of the override menu. A Temporary Override rollout appears.

Figure 26-1



- b. Select an amount of time, in minutes or seconds, that the override ARM status will be in place.
- c. Click **ARM** in the rollout. The temporary arm data is sent to the relevant controllers. A relevant controller is a controller connected to an input that is also grouped in the alarm zone container where the temporary override command was applied.

In addition:

- » The Manual Action column value changes to reflect the override time.
- » If the Real Time Status value was not set to Arm before the manual override, it is now.
- » The name of the operator who performed the override appears in the Operator Name column.

### Arm the alarm zone in focus indefinitely

Click **Constantly** in the Arm part of the override menu. The alarm zone is armed until another manual override operation is performed.

In addition:



- » The Manual Action column value changes to reflect the override time.
- » If the Real Time Status value was not set to Arm before the manual override, it is now.
- » The name of the operator who performed the override appears in the Operator Name column.

**Arm the alarm zone until the next Weekly Program period (green or white) starts.**

Click **Until Next Time** in the Arm part of the override menu. The alarm zone is armed until the next Weekly Program period (green or white) starts.

In addition:

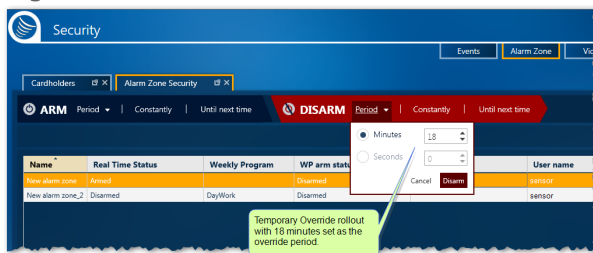
- » The Manual Action column value changes to reflect the override time.
- » If the Real Time Status value was not set to Arm before the manual override, it is now.
- » The name of the operator who performed the override appears in the Operator Name column.

5. If you are going to override with a DISARM command, do one of the following.

**Temporarily disarm the alarm zone in focus**

- a. Click **Period** in the Disarm part of the override menu. A Temporary Override rollout appears.

Figure 26-2



- b. Select an amount of time, in minutes or seconds, that the override DISARM status will be in place.
- c. Click **DISARM** in the rollout. The temporary disarm data is sent to the relevant controllers. A relevant controller is a controller connected to an input that is also grouped in the alarm zone, where the temporary override command was applied.
- d. In addition:
  - » The Manual Action column value changes to reflect the override time.
  - » If the Real Time Status value was not set to Disarm before the manual override, it is now.
  - » The name of the operator who performed the override appears in the Operator Name column.

**Disarm the alarm zone in focus indefinitely**

Click **Constantly** in the Disarm part of the override menu. The alarm zone is disarmed until another manual override operation is performed.

In addition:

- » The Manual Action column value changes to reflect the override time.
- » If the Real Time Status value was not set to Disarm before the manual override, it is now.
- » The name of the operator who performed the override appears in the Operator Name column.

**Disarm the alarm zone until the next Weekly Program period (green or white) starts.**

Click **Until Next Time** in the Disarm part of the override menu. The alarm zone is disarmed until the next Weekly Program period (green or white) starts.

In addition:

- » The Manual Action column value changes to reflect the override time.
- » If the Real Time Status value was not set to Disarm before the manual override, it is now.
- » The name of the operator who performed the override appears in the Operator Name column.

6. (Optional) Click **Download**. The override command is re-sent to the relevant controller(s). This may be necessary if there is a network issue. If the override command was sent automatically, after performing the override operation, clicking **Download** will not adversely affect the command execution.

## Canceling a Temporary Override

Use the following steps to cancel a temporary manual override of an alarm zone's status via the Alarm Zone Security screen.

### How to cancel a temporary manual override of an alarm zone

1. Go to the Security Task group and click **Alarm Zone**. The Alarm Zone Security screen is displayed.
2. Select the row of an alarm zone whose status is currently being overridden.
3. In the action bar, click **Cancel Temporary Action**. The command is recorded in the system database and sent to the relevant controllers, where the manual override is stopped.

A relevant controller is a controller connected to an input that is also grouped in the alarm zone container where the temporary override command was applied.

# Canceling Any Override, Where the Alarm Zone Is Assigned a Weekly Program (WP)

Use the following steps to cancel any manual override command applied to an alarm zone's status via the Alarm Zone Security screen.

## How to cancel a manual override of an alarm zone where the alarm zone is controlled by a WP

1. Go to the Security Task group and click **Alarm Zone**. The Alarm Zone Security screen is displayed.
2. Select a row of an alarm zone that is assigned a WP (check the content of the Weekly Program column in the table).
3. In the action bar, click **Return to Weekly Program**. The command is recorded in the system database and then sent to the relevant controllers, where the manual override is stopped and the WP, assigned to the alarm zone, starts to govern the inputs based on the WP's configured green and white periods.

A relevant controller is a controller connected to an input that is also grouped in the alarm zone container where temporary override command was applied.

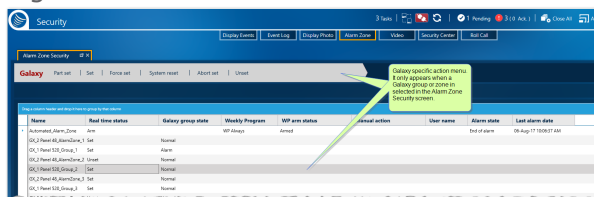
# Changing the setting of a Galaxy Group or Zone

Use the following steps to change the setting of a Galaxy group or zone via the Alarm Zone Security screen.

## How to change the settings of a Galaxy group or zone via the Alarm Zone Security screen

1. Go to the Security Task group and click **Alarm Zone**. The Alarm Zone Security screen is displayed.
2. Select a Galaxy group or zone row. The setting toolbar change to accommodate Galaxy actions.

Figure 26-3



3. Click on a setting command. The Galaxy group or zone changes.
4. (Optional) Right-click a Galaxy row and select a setting command from the context menu. The same context menu options available in the toolbar are also available in the context menu.

The availability of the Galaxy settings depends on the **Real Time Status** and the **Galaxy Group state** values of the group or zone.

# Managing a Galaxy Zone Alarm

Use the following steps to handle a Galaxy zone alarm.

A Galaxy zone's details may include instructions related to the particular alarm. This topic includes general information on Galaxy zone alarm handling and assumes there are no instructions in the zones details.

A best practice is to incorporate these steps into your organization's alarm protocol.

## How to handle a Galaxy zone alarm

1. After an alarm is triggered, Confirm and Acknowledge the alarm from the GuardPoint10 interface; this can be done via the dashboard, Security Center screen, Display Events screen, etc.
2. Open the Alarm Zone Security screen.
3. Select the Galaxy group where the zone under alarm is located.
4. From the group's row context menu or the Action menu above the table, Click Reset System. It may be necessary to also click Rest after Reset System is completed.

The Confirm and Acknowledge operation address the alarm in the GuardPoint10 database. However, the alarm still exists in the Galaxy panel. The Reset System operation, which may be performed via the GuardPoint10 interface or the panel's keypad, addresses the alarm on the Galaxy panel.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 27:

## Video (Security)



The Video Security screen is an GuardPoint10 CCTV client that is far from passive. An operator can link a camera from the logic tree to a specific tile, where they can perform the following camera-related monitoring operations:

- » View live feed and playback video records
- » Compare Videos/Pictures side by side
- » Take a Snapshot from a video
- » Control a PTZ enabled camera
- » Monitor Access-based video
- » Monitor Alarm-based video

### For example:

After an intrusion is detected (alarm), security personnel (an GuardPoint10 operator) monitoring the situation via the Video Security screen can investigate the alarm event from the screen, with the available cameras, and determine if a genuine break-in is taking place.

If a break-in is in progress, the operator may lock/unlock doors or arm/disarm the corresponding alarm zone to stall the intruder and allow roaming security personnel to detain them.

These, and other, actions such as monitoring the real-time status of each door (opened/closed, locked/unlocked) may be performed via the Video Security screen.

Screen views are created and managed in the Video Security screen to allow an operator to customize their own tab and panel configuration. This allows an operator to effectively respond to a security-related event.






## Configuring the Video Panel

Each video tab (Access Monitoring and Alarm Monitoring) has its own independent video panel. A video panel consists of tiles. Each tile can potentially display a video or still image (snapshot). In addition, a layer of content-related information can be displayed on top of the video or snapshot.

Use the following procedures to configure a video panel and the tiles in the video panel.

### How to configure a video panel

1. Go to the Security Task group and click **Video**. The Video Security screen is displayed.
2. Choose to open either an Access or Alarm monitoring tab.
3. From the configuration bar, select a tile layout. The available options are:

	The video panel will display a single tile where a video or snapshots may be viewed.
	The video panel will display four tiles where videos or snapshots may be placed and viewed. (Default)
	The video panel will display nine tiles where videos or snapshots may be placed and viewed.
	The video panel will display sixteen tiles where videos or snapshots may be placed and viewed.
	In the video panel, all tiles are emptied.

The tiles reconfigure to the selected layout.

**Note:** The selected configuration is only applied to the video panel in the opened video tab. The video panels in any other video tab remain unchanged.



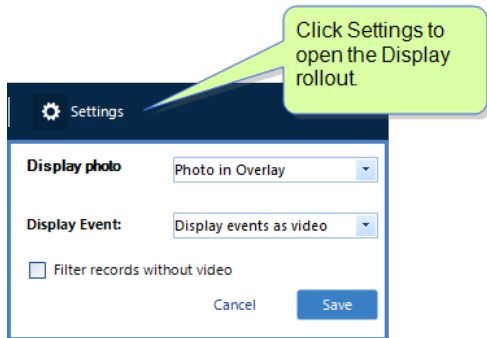
# How to configure the tiles in a video panel

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.

Four empty tiles are displayed in the control panel by default.

3. From the configuration bar, click **Settings**. A Display rollout appears.

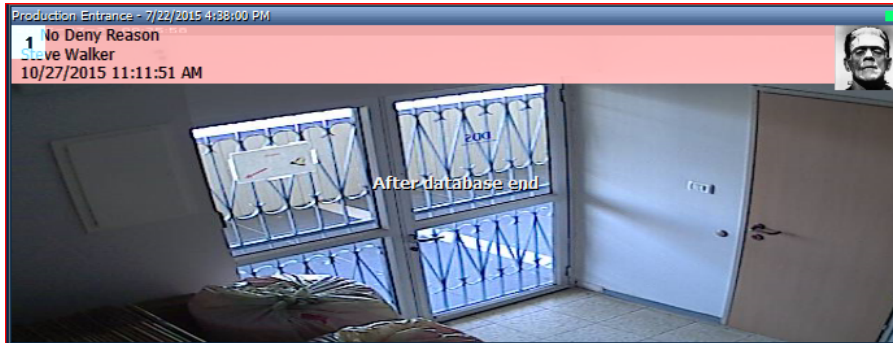
Figure 27-1



4. In the rollout, select an option from the **Display Photo** drop-down list. A cardholder's photo appears in a tile as dictated by the selected option. The available photo positioning options are as follows:

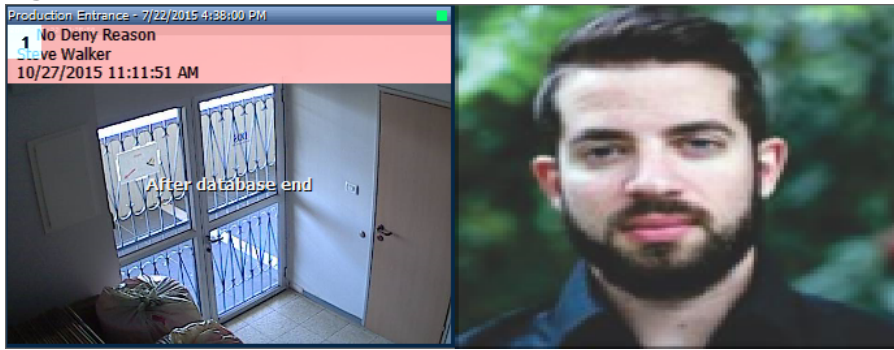
» **Photo in overlay**: The cardholder's photo will appear on top of the event image. This is the default option.

Figure 27-2



» **Side-by-side**: The event image will be cropped and the cardholder's photo will appear alongside the event image.

Figure 27-3



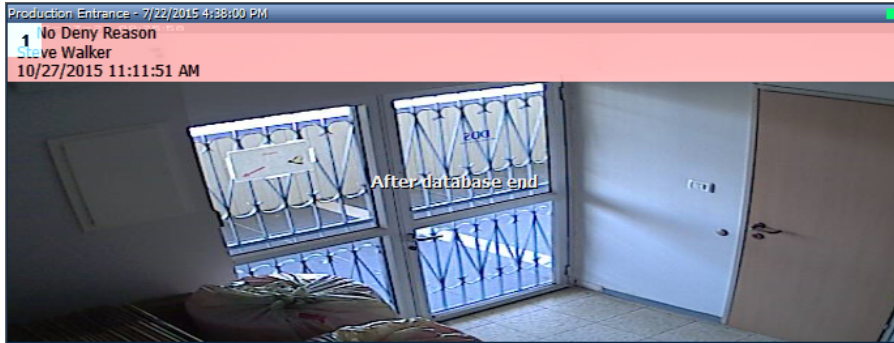
- » **Photo only:** The event image will be hidden and only the cardholder's photo will appear in the tile.

Figure 27-4



- » **Hide photo:** The event image will appear in the tile without the cardholder's photo.

Figure 27-5



5. In the same rollout, select an option from the Display Event drop-down list. This setting determines how an image in a tile will be presented

The available options are as follows:

- » **Display event as snapshot:** A still image of an event appears in a designated tile.
- » **Display event as video:** A 30 sec delay is applied to the event video. When the video does appear in the tile, you can use the player controls in the virtual remote to rewind 30 seconds and see the event as it happened. This is the default option.

For information about the virtual remote, see ["Video Security Screen" on page 667](#).

» **Display event as live:** A live video stream appears in the designated tile where you can see the event take place in real time.

6. Click **Save**, the Display rollout selections are immediately applied to the tiles in the video panel.



**Note:** The Display Photo drop-down list pertains only to Access video tabs.

If a cardholder does not have a photo in the system, an avatar will be used as a placeholder.

Because access attempts and alarms are both considered events, the Display Event drop-down list applies to both video tab types.

## Managing Tile Content

Tile management allows you to designate one or more cameras to a particular tile in a tab. This means that all events related to a designated camera will always be displayed in the same tile.

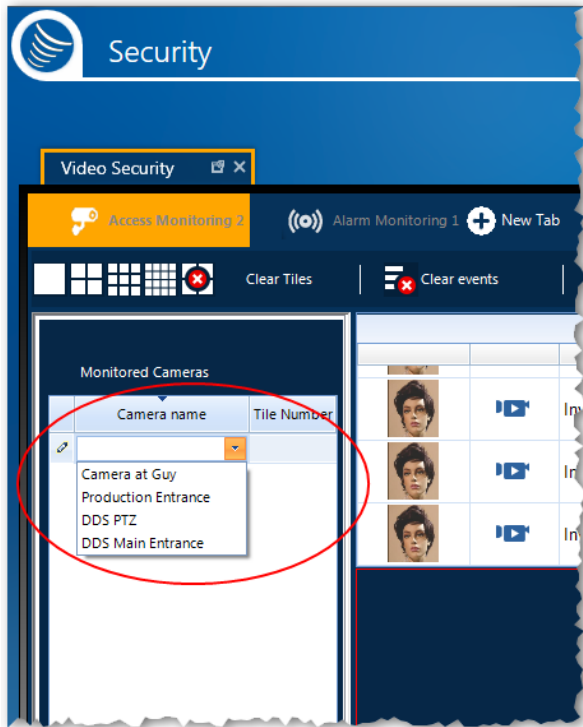
A camera designation is identified in the system as a combination of tile number and video tab name. In other words, tile management is video tab specific and cannot be linked to another video tab.

Use the following steps to designate a camera to a tile in the video panel.

### How to designate a camera to a tile

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. If the logic tree is displayed, go to the bottom of the pane and click the Tile management tab. The camera designation table is displayed.
4. In the Camera Name column's drop-down list, select a camera.

Figure 27-6



5. In the Tile Number column's drop-down list, select a tile number. The camera is designated to the selected tile.

Each tile is numbered. This number appears in a tile, whether it's empty or playing a video. Tile numbers range from 1 to 16.

A tile does not have to be visible in the video panel to be assigned to a camera.

6. To designate another camera to a tile, click the pencil icon in the first column of the previously edited row and repeat Step 3 and Step 4.

**Note:** If you select **None** as a Tile Number for a camera, the camera will not be displayed in the video panel at all. Consequently, if a new access or alarm event occurs, nothing will be displayed in the video panel, unless other cameras are associated with the same event.

This display restriction extends to actions such as drag and drop an event from a log table to a video panel's tile or, right-clicking a displayed event and selecting a camera that is not allowed to be displayed (designated **None**).

To delete a camera-tile designation, in the Tile management table, select a row and click the trash pail button. The row is deleted.

Alternatively, right-click on the Tile management table row and select **Delete row** from the context menu.

# Managing Access/Alarm Event Log

The Video Security screen displays logs in a table format. The logs are automatically updated in real time by the system.

In an Access Monitoring video tab, the displayed log shows all access events such as 'Access Granted', 'Access Denied'.

In the Alarm Monitoring video tab, the displayed log shows all active alarms.

If a camera has been associated with a reader or an input, it can be configured to automatically display in a designated tile when an event occurs on the reader/input device (see ["Managing Tile Content" on page 377](#)). The video corresponding to the event can also be recalled and played at a later time as required (see ["Perform a Playback from a Specific Date and Time" on page 388](#)).

Use the following information to manage the Access and Alarm log tables.

## How to restructure a log table

1. Go to the Security Task group and click **Video**. T
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From either an Access log table or Alarm log table, drag and drop a labeled column heading into the Group By bar, just above the table. The table heading is now also a criteria for the Group By bar.

The table automatically groups the table content by the selected criteria.

4. Edit the content of the Group By bar as required by doing the following:
  - » Drag and drop additional column headings to the Group By bar.
  - » Click the **x** in a Group by criteria frame to remove it from the Group By bar.
  - » Change the order of the criteria in the Group By bar.

After editing the content of the Group By bar, the table structure is automatically updated.

## How to sort a log table

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From either an Access log table or Alarm log table, click on the heading of a labeled column. A small arrow will appear at the top of the column.

The arrow serves two purposes:

- » It indicates the column content that the sort is based on.
  - » From the direction in which the arrow is pointing, you can determine whether the sort is ascending or descending.
4. If necessary, click on the column a second time to change the direction of the arrow. The sort is automatically updated.

# Managing a Video Tab & Tab Bar

Each video tab (Access Monitoring and Alarm Monitoring) has its own context menu. The items in the context menu are broken down into three categories:

- » Items that only apply to the video tab where the context menu was opened
- » Items that apply to all video tabs visible in the tab bar
- » Items Show/Hide different areas of the video tab where the context menu was opened

Use the following information to manage a video tab or tab bar.

## How to manage a single video tab

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From a tab bar, right-click on a video tab. A context menu appears.
4. From the context menu, do one of the following:
  - » Click **Close tab**. One of the following actions takes place:
    - If the video tab, where the context menu was opened, was the only visible tab, an empty Video Security screen is displayed.
    - If there are multiple video tabs visible in the tab bar, where the context menu was opened, the next tab in the tab bar is opened.
    - If the video tab, where the context menu was opened, was the only visible tab in the tab bar and the screen was previously split (horizontally or vertically), the split side, where there are still tabs visible in the tab bar, will display in full screen.
  - » Click **Rename tab**. A Rename Tab dialog is displayed.

Enter a new video tab name and click **OK**. The tab name is replaced with the name entered in the dialog.

## How to manage a tab bar

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From a tab bar, right-click on a video tab. A context menu appears.
4. From the context menu, do one of the following:
  - » Click **Close all other tabs**. All video tabs in the tab bar, except for the tab where the context menu was opened, are closed.
  - » Click **Close all**. All video tabs in the tab bar, including the tab where the context menu was opened, are closed.
  - » Click **New horizontal tab group**. The Video Security screen is split into panes (horizontal). The video tab, where the context menu was opened, is moved to the new pane.

- » Click **New vertical tab group**. The Video Security screen is split into panes (vertical). The video tab, where the context menu was opened, is moved to the new pane.
- » Click **Move to previous tab group** or **Move to next tab group**. The video tab, where the context menu was opened, is moved to another pane in the split-screen.



**Note:** The **New horizontal tab group** and **New vertical tab group** operations may also be performed with a drag and drop action similar to the one described in "[Editable task screen views: tab stack, docking, and popout](#)" on page 29.

## How to show/hide areas in a video tab

The advantage to hiding the areas described below is to make more room for your video panel and provide operators with fewer distractions.

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From a tab bar, right-click on a video tab. A context menu appears.
4. From the context menu, do one of the following:
  - » Click **Hide Logic Tree**. The logic tree is hidden and the **Hide Logic Tree** context menu item is preceded by a checkmark.  
Click **Hide Logic Tree** again to show (unhide) the logic tree.  
Alternatively, drag the splitter, which separates the logic tree from the rest of the pane to the right or left to adjust the size allocated to the logic tree.
  - » Click **Hide event/alarm table**. The log table is hidden and the **Hide event/alarm table** context menu item is preceded by a checkmark.  
Click **Hide event/alarm table** again to show (unhide) the log table.



**Note:** Depending on the type of video tab opened, the log table may be an Access Event log table or an Alarm log table.

- » Click **Hide virtual remote**. The virtual remote is hidden and the **Hide virtual remote** context menu item is preceded by a checkmark.  
Click **Hide virtual remote** again to show (unhide) the virtual remote.


# Sharing a Video Tab Configuration

A tab is an independent interface in the Video Security screen. After you configure a tab to fit your work environment, you can save the configuration for reuse in future GuardPoint10 sessions or share it with other operators.

A tab configuration is saved in an XML file. As long as you, or another operator, have access to that XML file, the tab configuration can be reused.

Use the following steps to save a tab configuration and open a previously saved tab configuration.


## How to save a tab configuration

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. Select the tab that will be saved.
4. In the tab area of the configuration bar, click . A Save As dialog is displayed.
5. Select a file location and enter a name for the tab configuration file, and then click **Save**. The XML file containing the tab configuration data is saved.



**Note:** If you intend to share the tab configuration with others, place the XML file in a folder accessible to the other operators.

## How to open a saved tab configuration

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. In the tab area of the configuration bar, click . An Open File dialog is displayed.
4. Select the XML file, and then click **Open**. The tab opens in your tab bar.



**Note:** After you have opened the previously saved tab, you can change the configuration without affecting the XML file where the configuration data originated.

You cannot open the same XML file twice on the same Video Security screen.




# Overriding a Door's Lock/Unlock State

Use the following steps to override the status of a door lock via the Video Security screen.

These options are applied to the relays of the relevant reader associated with a selected tile's camera feed. The relationship is depicted in the logic tree on the left side of the screen.

## How to lock an unlocked door via the Video override options

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From the video panel, select a tile with a live video stream. The live stream is in focus.
4. From the virtual remote, click . A list of lock options appears.
5. Select one of the following lock options:
  - » **Close <reader name> constantly**: Locks the door until another action from the Video Security screen unlocks it. The reader name is the name as it appears in the logic tree.
  - » **Close <reader name> for 5 seconds**: Locks the door for 5 seconds and then performs the Return <reader name> relays to normal mode command described later in this list of options.




**Note:** 5 seconds is the default temporary time to keep a door locked. The value can be changed to better suit your needs (i.e. 10 sec, 15 sec, etc.).

- » **Close 'All' associated doors at the same time**: This option is only available when multiple readers are associated with the camera feed current displayed in the tile in focus. It is similar to the **close constantly** option, but on a larger scale. It locks all of the relevant doors until another action from the Video Security screen locks it.
- » **Return <reader name> relays to normal mode**: Return the relays, controlling the door's lock, to their normal status for that particular time period (green or white). For more information about green and white periods, see "[Weekly Program Time Zones](#)" on page 120.

After selecting an override option, the override is applied and governs the door's lock state.

## How to unlock a locked door via the Video override options

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From the video panel, select a tile with a live video stream. The live stream is in focus.
4. From the virtual remote, click . A list of unlock options appears.
5. Select one of the following unlock options:

- » **Open <reader name> constantly:** Unlocks the door until another action from the Video Security screen locks it. The reader name is the name as it appears in the logic tree.
- » **Open <reader name> for 5 seconds:** Unlocks the door for 5 seconds and then performs the Return <reader name> relays to normal mode command described later in this list of options.



**Note:** 5 seconds is the default temporary time to keep a door locked. The value can be changed to better suit your needs (i.e. 10 sec, 15 sec, etc.).

- » **Open 'All' associated doors at the same time:** This option is only available when multiple readers are associated with the camera feed current displayed in the tile in focus. It is similar to the open constantly option, but on a larger scale. It unlocks all of the relevant doors until another action from the Video Security screen locks it.
- » **Return <reader name> relays to normal mode:** Return the relays, controlling the door's lock, to its normal status for that particular time -as determined by its green or white period. For more information about green and white periods, see "[Weekly Program Time Zones](#)" on page 120.

After selecting an override option, the override is applied and governs the door's lock state.

# Overriding an Alarm Zone's Status from the Video Security Screen

Use the following steps to override an alarm zone's status via the Video Security screen.

These options are applied to the alarm zone where the input associated with a selected tile's camera stream is grouped. The group relationship between the input and the alarm zone can be seen in the Alarm Zone Setup screen (see "[Alarm Zones \(Setup\)](#)" on page 301). The relationship between an input and a camera is depicted in the logic tree on the left side of the Video Security screen.

## How to arm an alarm zone via the Video override options

1. Go to the Security Task group and click **Video**. The Video Security screen is displayed.
2. From the video panel, select a tile with a live video stream. The live stream is in focus.

The camera streaming to the tile must be connected to an input device that is grouped in an alarm zone.

3. From the virtual remote, click . A list of arm options appears.
4. Select one of the following arm options:

- » **ARM <alarm zone name> for 5 seconds**: Arms the alarm zone for 5 seconds and then return the alarm zone to its normal status for that particular time (as determined by its green or white period). For more information about green and white periods, see "[Weekly Program Time Zones](#)" on page 120.



**Note:** The default temporary time to keep an alarm zone armed is 5 seconds. The value can be changed to better suit your needs (i.e. 10 sec, 15 sec, etc.). This logic also applies to the next arm options, which have a default value of 1 minute.

- » **ARM <alarm zone name> for 1 minute**: Arms the alarm zone for 1 minute and then return the alarm zone to its normal status for that particular time (as determined by its green or white period). For more information about green and white periods, see "[Weekly Program Time Zones](#)" on page 120.
- » **ARM <alarm zone name> constantly**: Arms the alarm zone until another action from the Video Security screen disarms it.
- » **ARM <alarm zone name> until next time zone**: The alarm zone will remain armed until the associated time zone switches from a green period to a white period or vice versa.
- » **ARM 'All' associated alarm zones at the same time**: This option is only available when multiple inputs are associated with the selected camera. It's similar to the arm constantly option, but on a larger scale.

After selecting an override option, the override is applied and governs the input's alarm zone status.

## How to disarm an alarm zone via the Video override options

1. Go to the Security Task group and click **Video**. The Video Security screen is displayed.
2. From the video panel, select a tile with a live video stream. The live stream is in focus.

The camera streaming to the tile must be connected to an input device that is grouped in an alarm zone.

3. From the virtual remote, click . A list of disarm options appears.
4. Select one of the following disarm options:

- » **DISARM <alarm zone name> for 5 seconds:** Disarms the alarm zone for 5 seconds and then return the alarm zone to its normal status for that particular time (as determined by its green or white period). For more information about green and white periods, see "[Weekly Program Time Zones](#)" on page 120.



**Note:** The default temporary time to keep an alarm zone armed is 5 seconds. The value can be changed to better suit your needs (i.e. 10 sec, 15 sec, etc.). This logic also applies to the next arm options, which have a default value of 1 minute.

- » **DISARM <alarm zone name> for 1 minute:** Disarms the alarm zone for 1 minute and then return the alarm zone to its normal status for that particular time (as determined by its green or white period). For more information about green and white periods, see "[Weekly Program Time Zones](#)" on page 120.
- » **DISARM <alarm zone name> constantly:** Disarms the alarm zone until another action from the Video Security screen arms it.
- » **DISARM <alarm zone name> until next time zone:** The alarm zone will remain disarmed until the associated time zone switches from a green period to a white period or vice versa.
- » **DISARM 'All' associated alarm zones at the same time:** This option is only available when multiple inputs are associated with the selected camera. It's similar to the Disarm Constantly option, but on a larger scale.

After selecting an override option, the override is applied and governs the input's alarm zone status.

# Handling an Alarm Event in the Video Security Screen

There are two steps in handling an active alarm, first acknowledge it and then confirm it. Use the following steps to handle an alarm via the Video Security screen.

## How to handle an active alarm

1. Go to the Security Task group and click **Video**.
2. Open an Alarm Monitoring video tab. The Video screen is displayed with an Alarm monitoring tab.  
If an active alarm event exists, it will appear in the log table with red text and the Status column text will be 'Active'.
3. Select an active alarm row.
4. Click **Acknowledge** in the alarm-specific action bar, just above the table. The text in the alarm row changes to green and the Status text now reads "Acknowledged".
5. If the acknowledged alarm row is no longer in focus, select it again and click **Confirm** in the action bar. An Alarm Confirm dialog is displayed.
6. Enter a comment if necessary, and then click **OK**. The alarm event is removed from the log table, the system database is updated and the Events Log table displays the Confirm event.



**Note:** If multiple alarm rows have been acknowledged, they can all be confirmed at the same time by clicking **Confirm All** instead of **Confirm**. However, the Confirm All option does not allow you to append a comment to the acknowledged alarms.

**Confirm All** may also be clicked without the need to acknowledge the alarms.


If multiple cameras are connected (subelements) to a reader, where an event is triggered, the first camera listed will be the primary camera. This means that in the Video Security screen the primary camera's video stream will display in a tile if triggered by an event (i.e. a badge swipe). A secondary camera's video stream may be displayed by selecting it from the tile's context menu item **Show on other cameras** and select the second camera.

# Play a Playback from a Log Entry

Each log entry is detailed in a log table row. If the entry event (access or alarm) was recorded by a camera listed in the logic tree, the video may be accessed via the log entry.

Use the following steps to perform a playback via a log entry.

## How to perform a playback via a log entry




1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From either an Access log table or Alarm log table, find the required event and verify that it includes a playback icon  in the event row.
4. Drag and drop the playback icon into a tile. The video will start to play.

# Perform a Playback from a Specific Date and Time


Video records may be archived by your NVR/DVR system. An archived video record is called a playback. If a playback exists, it can be called and viewed via the GuardPoint10 Video Security screen.

Use the following steps to call and play a playback from a specific date and time.

## How to call and play a playback from a specific date and time

1. Go to the Security Task group and click **Video**.
2. Choose to open either an Access or Alarm monitoring tab. The Video Security screen is displayed.
3. From either an Access log table or Alarm log table, click  in the virtual remote. A Calendar & Date dialog is displayed.
4. Specify the date and time where you would like to start viewing the playback.
5. Click **OK**. The dialog is closed, the video starts to play in the tile currently in focus, and the Playback button's background  changes to orange .

Use the player **Playback Controls** in the virtual remote to go to a specific point in a playback.



**Note:** If the camera where the playback was recorded is designated as **None** in the tab's Tile Management table (see "[Managing Tile Content](#)" on page 377), you will not be able to play the playback. However, if the camera has a designation other than **None** in another video tab, the playback is viewable from the other tab.

# CHAPTER 28:

## Security Center



The Security Center screen provides access to virtual maps of your GuardPoint10 ecosystem and includes actionable supporting features based on animated indicators placed on the map in the Position screen.

The icons, representing the different parts of your system, alert you to the state of the element, linked to the icon, and events triggered from the element.

### **For example:**

A door icon shows if the door is physically open or closed, the state of the relays controlling it ('Normally Open' or 'Normally Closed'), if an override state is currently in place, and whether alarms associated with it have been acknowledged and confirmed.

The Security Center screen brings your system to life where an operator can monitor multiple locations and identify a real-time status change, alarms and access events, as they occur.



Multiple Security Center screens can be open at the same time in a single stack or in individual tiles in the console. Each Security Center screen instance may have a different map displayed.

When the Security Center screen is initially opened the map that is automatically displayed is the last map that was closed.

# Opening a Map Page

Use one of the following steps to open a map page via the Security Center screen.




## How to open a map page in the Security Center screen

1. Go to the Security Task group and click **Security Center**. The Security Center screen is displayed with the last map that was previously opened.
2. Do one of the following:
  - » From the map tree:
    - » Find the map you want to display by expanding tree elements (groups or parent maps) until you find the desired map, and then click it (put it in focus). The map page is displayed.
    - » Enter the name or part of the name (min. 3 characters) of a map in the Search field above the tree. The first map in the tree, which includes the search text in its name, is placed in focus and displayed.
  - » From a map page that is already displayed:
    - » If a map icon  is on the page, click it. The map linked to the icon is displayed.
    - » If a shape, textbox or, Miscellaneous icon, which is linked to a map, is on the page, click it. The map linked to the shape / textbox / icon is displayed.
    - » From the menu above the map page, use the navigation buttons  to go to map pages that have previously been displayed during the current session.

# Changing the Map Page View

Use the following steps to change the map page view via the Security Center screen.

## How to change a map page view in the Security Center screen

1. If the Security Center screen is not already opened, go to the Security Task group and click **Security Center**. The Security Center screen is displayed with the last map that was previously opened.
2. Do one of the following:
  - » Click . The map zoom item will automatically change to "Fit to Page".
  - » Click . The map aligns to the left-top corner of the map page.
  - » Click . Pans from one area of the map to another.
  - » Click **Layers**. Opens a drop-down list where you select the type of icons to show or hide on the map page.



- » Click a magnification level from the drop-down list, the zoom changes to the selected magnification.

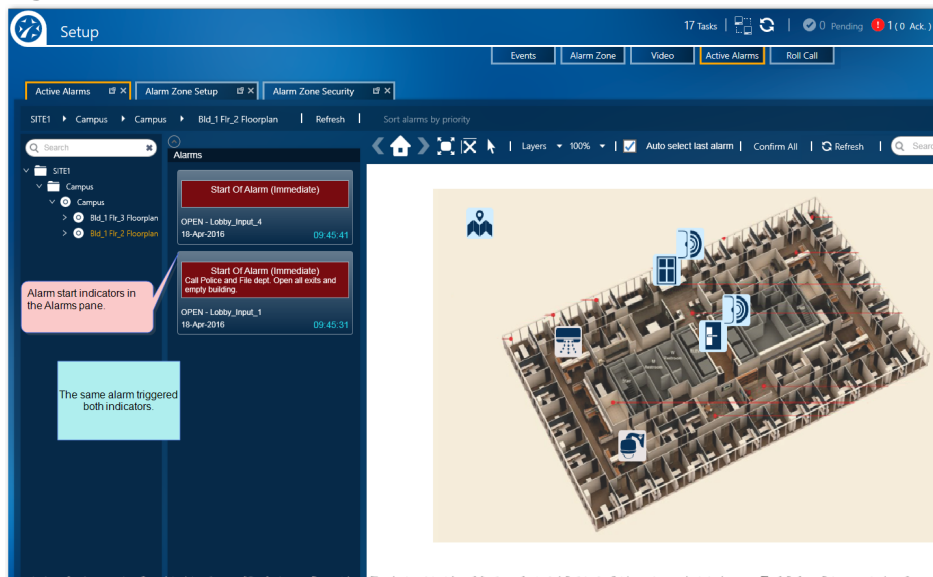
## Addressing Alarms via a Security Center Icon

### How to identify an alarm in the Security Center screen

When an alarm is triggered, the following indicators may appear on the Security Center screen:

- » An alarm message appears in the alarm pane to the right of the map tree.

Figure 28-1



- » An icon, linked to the system component where the alarm was triggered, flashes red and change




- » If a map icon on the currently displayed map page is linked to another map, where an icon indicates that its system component triggered an alarm, the map icon flashes red and changes appear-



- » If a shape or textbox on the currently displayed map page is linked to a map, where an icon indicates that its system component triggered an alarm, the shape or textbox flashes red and has a red



- » If the **Auto select last alarm** checkbox is selected when an alarm is triggered, the map page, where an icon indicating the alarm exists, is displayed automatically.



**Note:** icons, shapes, and textboxes can indicate more than just alarms, for a comprehensive list of indicators, see ["Security Center Screen" on page 680](#).

## How to manage an alarm from the Security Center screen

Use the following procedures to manage alarms via the Security Center screen's Alarm pane. These procedures exclude any alarm-specific instructions that may have been configured during a setup operation (i.e. "Contact police and fire departments, and then call your shift supervisor").

Shapes and Textboxes cannot be linked to inputs, but they can be linked to alarm zones. This means that an alarm cannot be managed from a shape or textbox. If the shape, or textbox is linked to the alarm zone that contained the input that is under alarm, the shape or textbox will have an under alarm overlay, and a context menu that will allow you to manage the alarm zone.

1. After an alarm is triggered, acknowledge the individual alarm. An icon's background color changes to green and stops flashing. The alarm message in the Alarm pane includes the text "Acknowledged" and the text background changes to green.

To acknowledge an alarm, do one of the following:

- » From the Alarm pane, right-click an alarm card and from the context menu, click **Acknowledge**.

Alternatively, click **Navigate to Map** in the context menu. The map where the alarm icon is located opens. Click **Acknowledge** in the icon's context menu.

- » Click **Acknowledge** in the relevant icon's context menu.
- » From a map icon, where an alarm is indicated, click **Navigate to Map** in the context menu. The map where the alarm icon is located opens. Click **Acknowledge** in the icon's context menu.

2. Confirm the alarm. The alarm indicators are removed from the relevant objects (the alarm pane card, icons). The alarms, and how they were dealt with, will appear in the Event Table Log (see ["Display Events Screen" on page 353](#)).

An alarm must be acknowledged before it can be confirmed.

To confirm an alarm, do one of the following:

- » From the Alarm pane card's context menu, click **Confirm**. A Confirm dialog appears. If necessary, enter a description of the circumstances surrounding the alarm, and then click **Confirm**. The card is removed from the Alarm pane.
- » Click **Confirm** in the relevant icon's context menu. A Confirm dialog appears. If necessary, enter a description of the circumstances surrounding the alarm, and then click **Confirm**. The icon returns to its normal status.
- » From a map icon, shape, or textbox context menu, click **Navigate to Map**. The map where the alarm icon is located opens. Click **Confirm** in the icon's context menu. A Confirm dialog appears. If necessary, enter a description of the circumstances surrounding the alarm, and then click **Confirm**. The icon indicating the alarm, and the map icon, return to their normal status. If an icon, shape, or textbox is linked to the alarm zone where the now confirmed alarmed input is located, it also returns to a normal status.

Alternatively, you can take a shortcut and skip the Acknowledge step and the step where you would confirm each alarm individually. If one or more alarms exist, you can click the **Confirm**

**All** button in the menu above the map page. All of the alarms will be confirmed and removed from the Security Center screen. The one drawback to this method is that you will not be able to enter a description of the circumstances surrounding an alarm.

# Accessing Alarm Zone Details Via a Miscellaneous Icon, Shape, and Textbox

Use the following steps to reconfigure an alarm zone's details via a Miscellaneous icon, shape, or textbox in the Security Center screen.

## How to access an alarm zone's details for a Miscellaneous Icon, Shape, and Textbox

1. Go to the Security Task group and click **Security Center**. The Security Center screen is displayed with the last map that was previously opened.
2. Select the Miscellaneous icon, shape, or textbox linked to the alarm zone that will be accessed. The object was linked to the alarm zone in the Setup tasks' Position screen (see "[Linking an Icon, Shape, or Textbox](#)" on page 284).
3. Double-click the Miscellaneous icon, shape, or textbox, the Alarm Zone details are displayed.

Figure 28-2

Parameters of the alarm zone linked to the object in focus. These include the Weekly Program that governs the zone.

A dynamic table that shows the contents of the alarm zone in focus. These inputs are selected via the Select Inputs button above the table.

Name	Instruction	Network name	Controller Name	Bypassed
Main Doors_Input_1		My Access Network	Main Doors	<input type="checkbox"/>
Main Doors_Input_2		My Access Network	Main Doors	<input type="checkbox"/>
Main Doors_Input_3		My Access Network	Main Doors	<input type="checkbox"/>
Main Doors_Input_4		My Access Network	Main Doors	<input type="checkbox"/>
Main Doors_Input_5		My Access Network	Main Doors	<input type="checkbox"/>
Main Doors_Input_6		My Access Network	Main Doors	<input type="checkbox"/>
Main Doors_Input_7		My Access Network	Main Doors	<input checked="" type="checkbox"/>
Main Doors_Input_8		My Access Network	Main Doors	<input type="checkbox"/>

If a manual event was selected for the Double-click on the Positions screen, a global reflex that includes the manual event will execute the global reflex's action(s).

4. View or edit the current alarm zone configuration as required.

To see or edit the alarm zone details, you must have the relevant Alarm Zone Setup authorization (see "[Profiles](#)" on page 91).

An alarm zone's details can also be accessed from the Alarm Zone screen in the Setup task group.

For more information about the different Alarm Zone details, see "[Alarm Zone Setup Screen](#)" on page 521.

5. After the configuration is completed, close the dialog. A message asking if you would like to save your alarm zone changes is displayed.
6. Click **Yes**. The Configuration is saved in the system database and the relevant controller's local database.

## Managing an Object's Status from a Map Page

Use the following steps to manage map page objects via the Security Center screen.

### How to locate a specific object in the Security Center screen's maps

This operation is used to find objects on map pages as well as map images.

1. If the Security Center screen is not already opened, go to the Security Task group and click **Security Center**. The Security Center screen is displayed with the last map that was previously opened.
2. From the menu above the map page, click the **Search symbol in maps** field.
3. Enter all or part of an object's name. The name, in this case, refers to the name of the system component where an icon is linked, or the name of a map page defined in the map tree.
4. Click the down arrow, to the right of the field. A list of objects, which fit the text criteria entered in the field, is displayed.
5. Click a listed object, and then click **Locate**. The map where the object is located opens and the object is put in focus.



**Note:** All objects have a unique internal system name. The name is a combination of the map page name and the name of the linked component. If objects with the same name appear in the drop-down list, they are preceded by the map name where they are located.

### How to change the status of an object via its context menu

A change to the status of an object may change the object's look and feel on a map page. In addition, if an object has associated or connected objects, those objects may consequently change their status. For example, deactivating a controller object will deactivate all components physically connected to the controller.

1. If the Security Center screen is not already opened, go to the Security Task group and click **Security Center**. The Security Center screen is displayed.
2. Right-click an object on the page. A context menu appears.
3. Choose a context menu item. The context menu items are as follows:
  - » **Acknowledge:** Affects alarm handling (see "[Addressing Alarms via a Security Center Icon](#)" on page 391).
  - » **Confirm:** Affects alarm handling (see "[Addressing Alarms via a Security Center Icon](#)" on page 391).

- » **Input Deactivation (Bypass):** The icon does not reflect the status of the physical component.
- » **Input Activation:** The current status of the input is displayed via the icon look and feel.
- » **Activate Relay Duration 5 seconds:** The doors will be unlocked for 5 seconds.
- » **Activate Relay Continuously (Constant ON):** The doors will be unlocked until an operator changes the action via another context menu item selection, or the Alarm Zone Security screen (see ["Overriding an Alarm Zone's Status" on page 366](#)).
- » **Deactivate Relay Continuously (Constant OFF):** The doors will be locked until an operator changes the action via another context menu item selection, or the Alarm Zone Security screen (see ["Overriding an Alarm Zone's Status" on page 366](#)).
- » **Return to Normal Mode:** The doors will be in their defined normal state. The Weekly Program assigned to the relay determines the normal state.
- » **Open <object type> Details:** Displays detail information about the linked component (i.e. reader, alarm zone, controller, etc.).
- » **Navigate to Map:** Opens the map page linked to the selected map icon, shape, or textbox with a map link.

The content of an object's context menu depends on the object type and the type of component linked to the object.

## How to view an object's details via its context menu

1. If the Security Center screen is not already opened, go to the Security Task group and click **Security Center**. The Security Center screen is displayed.
2. Right-click an object on the page. A context menu appears.
3. Click **Open <object type> Details**. Infrastructure information about the physical component linked to the icon is displayed.



**Note:** The logged-in operator must have the authorization to see the details for the **Open <object type> Details** context menu item to be enabled.



**Note:** Shapes, textboxes, and Miscellaneous or Map icons can only link to maps, alarm zones, or areas. For more information about the unique properties of shapes, textboxes, and Miscellaneous icons, see ["Linking an Icon, Shape, or Textbox" on page 284](#).

# Managing an Alarm from an Alarm Card

The Security Center screen's Alarm pane contains a filtered list of alarms. These alarms appear in the form of a card-like graphic. An alarm card is listed in the pane after the alarm is triggered. Unlike the Events screen, the card filter in the Alarm pane only allows those cards that require an operator's attention to appear in the pane. For example, an access denied card or a technical alarm card will not appear in the pane; even a confirmed alarm card will be prevented from appearing in the pane.

Click a listed card to flip it and reveal more information about the alarm. To display the front of the card, click the card again.

## Alarm events

Alarms require management. The listed alarm cards have the following management context menu options:

- » **Acknowledge:** The alarm is recognized by the operator. An acknowledgment is reflected on the existing alarm card and in the pending area of the dashboard. An alarm must be acknowledged before it can be confirmed.
- » **Confirm:** Opens a Confirmation dialog where you may enter a description of the alarm and details that confirm your observation of the alarm. Click **Confirm** in the dialog to complete the confirmation process. After an alarm is confirmed, the card is removed from the Alarm pane.
- » **Navigate to map:** If an alarm's input icon appears on a map in the Security Center, the map will be displayed.



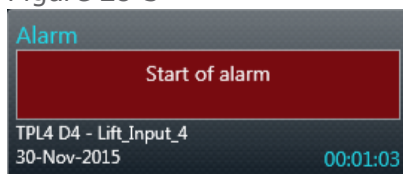
**Note:** Alarms may also be managed (acknowledged or confirmed from the animated alarm's icon via the icons context menu.

Use the following steps to manage an alarm event via the Alarm pane.

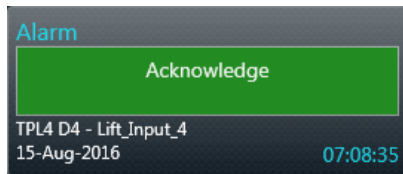
## How to manage an alarm event from an alarm card

1. Go to the Security Task group and click **Security Center**. The Security Center screen is displayed.  
Initially, the alarm pane is empty. The Security Center screen must be open before an alarm event is triggered for the alarm card to appear in the pane.
2. After an alarm is triggered and appears in the pane, right-click the alarm card and do one of the following:

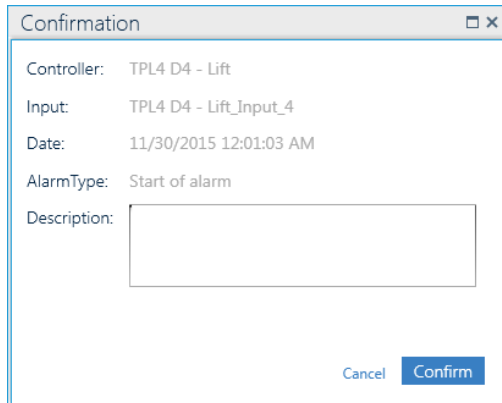
Figure 28-3



- » Click **Acknowledge** in the card's context menu. The background of the card's alarm text changes to green and the status text reads "Acknowledged".



- » Click **Confirm** in an acknowledged alarm card's context menu. An Alarm Confirmation dialog is displayed.



In the dialog, enter a comment if necessary, and then click **Confirm**. The card is removed from the pane. If a comment was entered in the dialog, the comment will appear on a confirmation card on the Events screen and on a confirmation event row in the Events' Log table.



# Monitoring Areas on a Map Page

Use the following steps to monitor areas on a map page via the Security Center screen.

The following assumes that there are areas linked to a Miscellaneous icon, shape, or textbox.

## How to monitor areas on a map page via the Security Center screen

1. If the Security Center screen is not already opened, go to the Security Task group and click **Security Center**. The Security Center screen is displayed with the last map that was previously opened.

2. Select a map that includes linked areas. The following appears:

» **If an area is linked to a Miscellaneous icon:** The default background color is blue as long as the number of cardholders in the area is below a defined capacity or, if there is no defined capacity. If the number of cardholders in the area is at capacity or above capacity, the default background color is red.

The number of cardholders in an area is displayed in an icon's tooltip. If the area has sub-areas, the cardholder occupancy number will also include the number of cardholders in the sub-areas. As long as there is a defined capacity, the capacity number will follow the occupancy number. For example, **6/20** means that there are **6** cardholders in an area with a capacity of **20** cardholders.

» **If an area is linked to a shape, or textbox:** The default shape, or textbox frame color is blue as long as the number of cardholders in the area is below a defined capacity or, if there is no defined capacity. If the number of cardholders in the area is at capacity or above capacity, the Miscellaneous icon background color is red and a shape, or textbox frame color is red.

The number of cardholders in an area is displayed at the bottom of the shape or textbox. If the area has sub-areas, the cardholder occupancy number will also include the number of cardholders in the sub-areas. As long as there is a defined capacity, the capacity number will follow the occupancy number. For example, **6/20** means that there are **6** cardholders in an area with a capacity of **20** cardholders.

The number of cardholders in an area and the area's capacity will also appear in an area linked Miscellaneous icon, shape, or textboxes tooltip.

## How to manage a linked area via the Security Center screen

1. If the Security Center screen is not already opened, go to the Security Task group and click **Security Center**. The Security Center screen is displayed with the last map that was previously opened.
2. Select a map that includes linked areas.
3. Right-click a shape, textbox or, Miscellaneous icon linked to an area. The context menu items available are:

- » **Open Area details:** Displays Area-specific information in a limited read-only Area screen.
- » **Open Area Roll Call details:** Displays Area-specific information in an instance of the Area Roll Call screen.

For information about the Area screen, see ["Area Screen" on page 525](#). For information about the Security Center screen, see ["Security Center Screen" on page 680](#).

# CHAPTER 29:

## Area Roll Call



The Area Roll Call screen automatically gathers selected area entry point readers and exit point readers and determines if a cardholder is inside or outside the selected area. Based on this determination, the Area Roll Call screen displays a cardholder card on the relevant side of the screen's partition. The screen can be displayed in a graphical format or tabular format (with or without cardholder photos).

The gathered information is presented to an operator in two groups:

- » **Inside:** Displays information about cardholders who are in the selected area. This means that a cardholder has been granted access to the area and has not exited.

Alternatively, an operator can set the cardholder's area location from the **Area** field in a cardholder's details. For information about area settings in a cardholder's details, see ["Operator \(User\): MultiSite Impact Cardholder Details" on page 607](#).

- » **Outside:** Displays information about cardholders whose last access action was a badge swipe at a reader with an Exit Area designation.

For information about a reader's designation as an area's entrance or exit points, see ["Reader Details" on page 453](#) and ["Area Screen" on page 525](#).



**Note:** If the site does not have a reader with a designated area setting other than **Area\_Undefined**, the Area Roll Call screen will not display

information about cardholders using the reader.

The Inside group title includes the total number of cardholders in the group along with the capacity of the area.

Each group has its own view option. A group may be displayed in a Table view Graphic view (as cards). Regardless of the view selected (table view graphic), the operator may drill down to the cardholder details of any cardholder with a simple double-click on the cardholder's row or card.

## Manually Change a Cardholder's Area

You can manually change a cardholder's area from the Area Roll Call screen or from a cardholder's details.

### Via the Area Roll Call screen

Use the following steps to change a cardholder's area via the Area Roll Call screen.

### How to change a cardholder's area via the Area Roll Call screen

1. Go to the Security Task group and click **Area Roll Call**. The Area Roll Call screen is displayed.
2. From the Area tree, select the area currently occupied by the cardholder. The details of the selected area are displayed.
3. From the Inside or Outside side of the partition, select a cardholder.
4. Drag and drop the cardholder into a different area in the Area tree. The cardholder is now found in the area where they were dropped and the system database is updated to reflect the change.

**Note:** If the area where the cardholder is dropped from is also a GAPB area, the cardholder's GAPB level will also change.

### Via a cardholder's details

Use the following steps to change a cardholder's area via a cardholder's details.

### How to change a cardholder's area via a cardholder's details

1. Open a cardholder's details from any screen where it is accessible (i.e. double-click a cardholder's information in the **Area Roll Call** screen).
2. In the General tab, go to the **Area** field's drop-down list and select a different area.
3. Save and close the cardholder's details. The cardholder is now found in the area selected in the cardholder's details and the system database is updated to reflect the change.

To avoid a situation where a cardholder cannot gain access via a reader due to APB or GAPB, and a user is not available to assist, create a Global Reflex where the action will open the relay of the door where the cardholder would want to access. The trigger should be something the cardholder can do on their own (i.e. swipe the badge at the reader five consecutive times).

## Area Roll Call MultiSite Impact

In the Area Roll Call screen, a user will be able to manage and move cardholders from Area to Area within the scope of the user's authorization. For example, a user owned by Site\_1 and has authorization in Site\_2, the user will be able to manage a cardholder's Area in both sites.

## Generating Area Roll Call Report Output

An Area Roll Call Report consists of two tables. The first table includes information about cardholders displayed in the Outside area of the Area Roll Call screen. The second table includes information about cardholders displayed in the Inside area of the Area Roll Call screen.

Before you generate a report, decide on the format that best satisfies your requirements. GuardPoint10 can generate reports in the following file formats, PDF, CSV, Excel, RTF, TIFF, and MHTML (Web Archive). There is an additional option to print a hardcopy of your report via a selected printer.

After generating a report file or printing a hardcopy, you can distribute the report to the relevant personnel.



**Warning:** Some data in the Area Roll Call report may be confidential and should be distributed responsibly.

## How to generate an Area Roll Call Report

1. Go to the Security Task group and click **Area Roll Call**. The Area Roll Call screen is displayed.
2. (Optional) Use the Search field to narrow the range of cardholders you would like to appear in the report.

Only the cardholders in the Outside and Inside areas at the time the report is generated will appear in the report.

3. Click **Print/Export...** to open the Print Report window, and then do one of the following:

### Print a Hardcopy

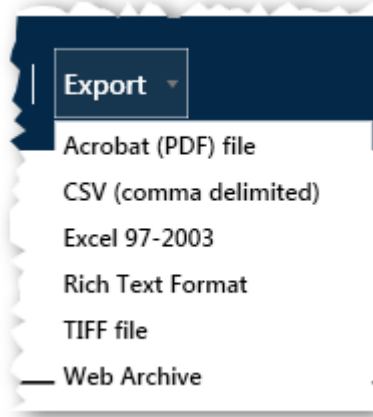


- a. In the Print Report window, click . A standard Windows Print dialog is displayed.
- b. Complete the dialog and click **Print**. A hardcopy of the report is printed at the specified printer.

### Export to File

- a. In the Print Report window, click **Export**. A drop-down list of available file formats appears.

Figure 29-1



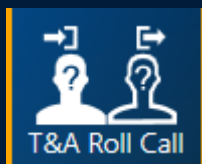
- b. Select a format. A standard Windows Save As dialog is displayed.
- c. Enter a file name and select a location for your file, and then click **Save**. The file is generated and saved in the specified location.



**Note:** If the file format selected does not support images, the cardholder photos will be excluded from the report.

# CHAPTER 30:

## T&A Roll Call



The T&A Roll Call screen automatically gathers information from designated entrance and exit readers and determines if a cardholder is inside or outside. The entrance and exit information is used in the Time & Attendance report generation via the Time & Attendance screen.

The T&A Roll Call screen displays a cardholder's information on the relevant side of the screen's partition. Each side of the partition can be displayed in a graphical (card) format or tabular format.

The gathered information is presented to an operator in two groups:

- » **Inside:** Displays information about cardholders who are on the premises. This means that a cardholder has swiped their badge an odd number of times.

Alternatively, a cardholder's last badge swipe was at a reader with an Entrance designation.

- » **Outside:** Displays information about cardholders who are *not* on the premises. This means that a cardholder has swiped their badge an even number of times.

Alternatively, a cardholder's last badge swipe was at a reader with an Exit designation.

For information about a reader's **T&A Reader** field, see "[T&A Reader](#)" on [page 459](#).



**Note:** If the site does not have a reader with a **T&A Reader** designation other than **None**, the T&A Roll Call screen will place all cardholders in the Outside group with "No Reader Info". In addition, if a cardholder does not have an entrance exit history ("No Reader Info" appears on the card in T&A Roll Call's Outside area), swiping their badge at a reader with a **T&A Reader** set to **Entrance/Exit** will have no impact on the T&A Roll Call screen.

The Inside and Outside group titles include the total number of cardholders in each group.

Each group has its own view option. A group may be displayed in a Table view Graphic view (as cards). Regardless of the view selected, the operator may drill down to the cardholder details of any cardholder with a simple double-click on the cardholder's row or card.

## Generating T&A Roll Call Report Output

A T&A Roll Call Report consists of two tables. The first table includes information about cardholders displayed in the Outside area of the T&A Roll Call screen. The second table includes information about cardholders displayed in the Inside area of the T&A Roll Call screen.

Before you generate a report, decide on the format that best satisfies your requirements. GuardPoint10 can generate reports in the following file formats, PDF, CSV, Excel, RTF, TIFF, and MHTML (Web Archive). There is an additional option to print a hardcopy of your report via a selected printer.

After generating a report file or printing a hardcopy, you can distribute the report to the relevant personnel.



**Warning:** Some data in the T&A Roll Call report may be confidential and should be distributed responsibly.

## How to generate a T&A Roll Call Report


1. Go to the Security Task group and click **T&A Roll Call**. The T&A Roll Call screen is displayed.
2. (Optional) Use the **Search** field to narrow the range of cardholders you would like to appear in the report.

Only the cardholders in the Outside and Inside areas at the time the report is generated will appear in the report.

3. Click **Print/Export...** to open the Print Report window, and then do one of the following:

### Print a Hardcopy



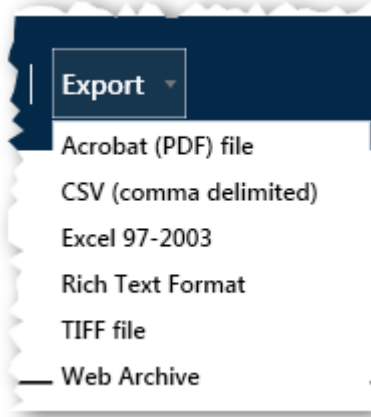
- a. In the Print Report window, click . A standard Windows Print dialog is displayed.
- b. Complete the dialog and click **Print**. A hardcopy of the report is printed at the specified printer.

### Export to File

- a. In the Print Report window, click **Export**. A drop-down list of available file formats appears.



Figure 30-1



- b. Select a format. A standard Windows Save As dialog is displayed.
- c. Enter a file name and select a location for your file, and then click **Save**. The file is generated and saved in the specified location.

**Note:** If the file format selected does not support images, the cardholder's photos will be excluded from the report.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 31:

## Visitor Control Management



The Visitor Control screen, accessed from any web browser that supports HTML 5, provides you with a flexible meeting and visit management solution and report generator. At any time, you can access a list of visits and meetings in your ecosystem; create a new visit or meeting, view/edit details about an existing visit or meeting, including meeting participants or a visit/meeting status. And, generate reports based on a record of visits or meetings in the system.

An overview or patterns can be seen via the Visitor Control's reports generator. A report can be filtered, sorted, and exported as required by the operator.

A visit / meeting status identifies the current stage of the event in its lifecycle. A lifecycle has four stages. A lifecycle starts after a visit is defined (see "[VM Visitor](#)" on page 411). The stage of a visit lifecycle appears in the Visitor Control log's Status column on the left side of the screen. The lifecycle stages are as follows:

1. Enrollment: A visit has been created and saved in the database, but has not progressed beyond that (i.e. the visitor has not checked in).
2. Checked In: The visitor arrives and a badge may be issued to them. The badge provides access to the area where the visit will take place.

3. Visit Started: An acknowledgment that the visit has started and the visitor is with the visit's host or on the way to the host.
4. Visit Ended: The badge is returned (if required) and the visitor leaves the premises.

To display the Visitor Control screen, open a web browser and enter the relevant web address:

- » If you are opening the Visitor Control screen on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
- » If you are opening the Visitor Control screen on a machine with a Client workstation installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`

Ideally, you would want to bookmark the page in your browser for future reference.

## Visit

A visit is a meeting between an employee-cardholder (host) and a single temporary visitor-cardholder visitor) on the premises where access and security are monitored and managed through the system database.

Visitors are identified, security risks are flagged, badges are assigned (if necessary), access to a visit location is authorized and visitors are tracked while their visit is still active (i.e. has a status value other than **Ended**).

## Meeting

A meeting is an encounter between a cardholder (meeting host) and multiple temporary cardholders (meeting participants) on the premises where access and security are monitored and managed through the system database.

Participants are identified, security risks are flagged, badges are assigned (if necessary), access to a meeting location is authorized, and participants, are tracked while on the premises.

## Reports

Each report type provides a breakdown of the visits and meetings in the system from a different perspective. Each report table includes its own set of filter fields to narrow the view of a report.

A displayed report can be exported to either CSV (Excel) or PDF.



**Note:** The Visitor Control module may be absent from your installation. If you would like to add the Visitor Control module, please contact your GuardPoint10 provider.

# VM Visitor

## Adding a New Visit

Use the following steps to create a new visit via the Visitor Control screen. The visitor-cardholder who will participate in the visit will be added to the GuardPoint10 system after the visit is saved. If the visitor-cardholder will be assigned a badge code later, during the check in operation, the badge code's status will be changed to **In Use** in the GuardPoint10 system, this means that the badge code cannot be assigned to another visitor-cardholder until the first visitor-cardholder's visit is done.

## How to add a new visit to the system

1. Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter  
`localhost/Visitors/`
  - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter  
`http://<GuardPoint10 Server machine name>/Visitors/`

Figure 31-1



2. From the Visitor Control page, click **New Visit**. A New Visit page is displayed on the right side of the browser over the day calendar.

Figure 31-2

For information about each field on the New Visit page, see ["Visitor Control Web Application" on page 645](#).

3. Enter the first name and last name of the visitor-cardholder in the heading (the colored area at the top of the page) of the New Visitor page. The name not only identifies the visitor, but is also used as the title of the visit. For example, in the day calendar, the visitor name is used in the visit event label).
4. Just below the name fields, in the **Start Date** and **End Date** fields, schedule a time for the visit. You can change the visit's start time and end time values at any time as required. The name and date fields are mandatory. The visit cannot be saved until these fields are filled.
5. From the Access Authorization drop-down list, select a Multiple Access Group that provides access to the location where the visitor-cardholder will require admittance. A Multiple Access Group allows a collection of access rules to determine a cardholder's authorization to one or more spaces on the premises. For more information about Multiple Access Groups, see ["Multiple Access Groups" on page 156](#). For example, if the visitor-cardholder is meeting someone in Room 512, select the Multiple Access Group that includes access to Room 512 and all of the zones that lead to the room (i.e. the elevator and Floor 5).
6. Enter optional information regarding the visitor:
  - » **Photo:** Image to identify the visitor-cardholder.
  - » **Company:** Where the visitor is affiliated.

- » **Phone:** The phone number where the visitor may be contacted.
- » **Visit Location:** Where the visit will take place.
- » **Car License Plate:** Identifies the vehicle belonging to the visitor.
- » **Security checkboxes:** Does the visitor require someone to accompany them (**Accompany**). Does the visitor require a supervisor cardholder to accompany them and comply with GuardPoint10 [escort rules](#) (**GuardPoint10 Escort**). Does the visitor need to be cleared by the security department before they can access the premises (**Security Clearance**).

7. (Optional) The host's details are automatically entered by the system based on the logged-in operator's data found in the system database.

The host may be changed to any valid employee-cardholder at any time by typing a few letters of the new host name in one of the host name fields. A list of potential hosts that include the typed letters will appear below the field. Select the new host's name from the list.

A host must be listed as an **Employee** in the GuardPoint10 Cardholders screen. For more information about cardholders, see ["Cardholders" on page 193](#).

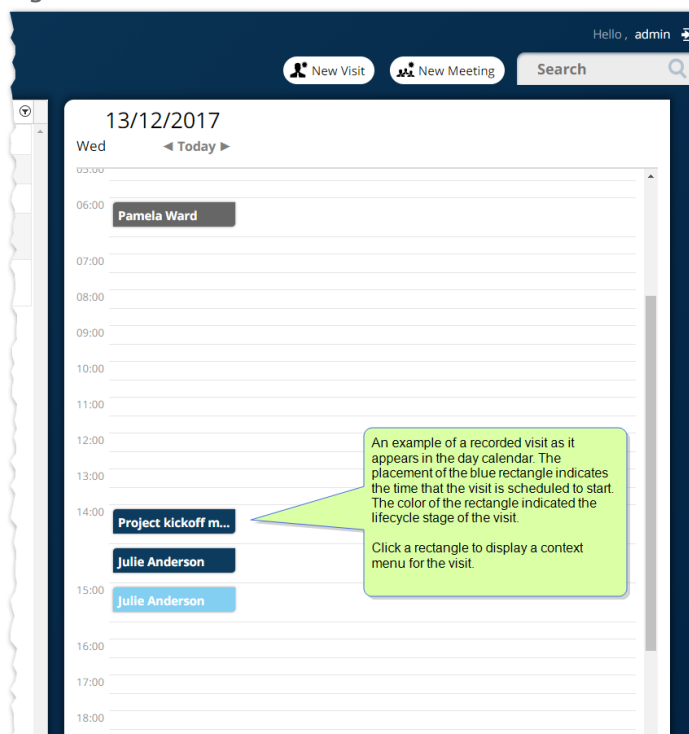
8. (Optional) In the **Comments** field, enter information about the visit that may be relevant to the visit's success (i.e. agenda, preparatory reading material, request for refreshments, etc.).

9. Click **Save** in the heading. The visit is recorded in the log to the left of the details page with an **Enrollment** status.

After you click **Save**, the **Save** button changes to an **Edit** button and the details will be in Read-Only mode. Click **Edit** to continue entering data or to update existing data.

10. After you have saved the details, click the white **x** in the heading (top right). The New Visit page is closed and the visit appears in the day calendar on the page corresponding to the visit's start date and time.

Figure 31-3



For information about the day calendar, see ["Visitor Control Web Application" on page 645](#).

## Advancing the Lifecycle of a Visit Event

Use the following steps to advance the lifecycle of a visit. The lifecycle starts after the visit is defined (see "VM Visitor" on page 411). The stage in a visit lifecycle appears in the Visitor Control log's Status column on the left side of the screen. The lifecycle stages are as follows:

1. **Enrollment:** A visit has been created and saved in the database, but has not progressed beyond that (i.e. the visitor has not checked in).
2. **Checked In:** The visitor arrives and a badge may be issued to them. The badge provides access to the area where the visit will take place at the time the visit is scheduled to start. Though the visitor-cardholder may have their badge in-hand, it will not work until the visit is started.
3. **Visit Started:** An acknowledgment that the visit has started and the visitor may access authorized areas (i.e. is with the visit's host or on the way to the host).
4. **Visit Ended:** The badge is returned (if required) and the visitor leaves the premises.

The following instructions walk you through each progression in a visit's lifecycle stages starting from "Check In".



**Note:** You cannot turn back the clock. Once the lifecycle of a visit has been advanced, it cannot be reversed.

### How to check in a visitor

1. Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
  - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`
2. After opening the Visitor Control page in your web browser, do one of the following:
  - » Find an **Enrolled** visit in the log on the left side of the screen and click on the row. The visit's details are displayed over the day calendar.
  - » Navigate to the day calendar page where the enrolled visit is scheduled to start and scroll to the visit's scheduled start time. The visit entry is displayed in a **Light blue** rectangle in the line of the scheduled time.

Click the **Light blue** rectangle to display a drop-down list of actions, and do one of the following:

- » Select **Check In** in the drop-down list.
- » Select **Edit** from the drop-down list.

After selecting **Check In** or **Edit** in the drop-down list, the visit's details are displayed over the day calendar.



Figure 31-4

Scott Marshal

17/01/2017 14:39 18/01/2017 16:52

\* Start date \* End date

Check In Edit Delete

Schodan Company +44 7700 900030 Phone Any Group Anytime Ar Access Authorization

Room 14 Location 232544 Car license plate

**Host details**

John Smith

First Name Last Name

Anet

Company	Department	Office phone	Private phone / Fax
---------	------------	--------------	---------------------

**Comments**

This is a sample visit

For information about the visit detail's field, see "[Visitor Control Web Application](#)" on page 645.

3. If **Edit** was selected from the day calendar's drop-down list or the details were opened from the log on the left side of the screen, click **Check In** in the visit details heading. The **Check In** button changes to a **Start Visit** button and a Check In Details area appears below the previously entered basic visit information.

If **Check In** was selected from the drop-down list, the **Start Visit** button and the Check In details are already displayed.

The Check In Details area primarily deals with the exchange of the visitor's ID for a badge that provides access.

Figure 31-5

▼ Check in details

0040A4BF Identity Card 3564 2  
Badge ID Type ID Number Rack number

Host details

John Smith  
First Name Last Name

Anet  
Company Department Office phone Private phone / Fax

Comments

This is a sample visit

The Check In Details area includes the following fields:

» **Badge:** The badge code assigned to the visitor. A **Free** badge code may be selected from the Badge field by entering a character from a **Free** code and selecting the code from the field's drop-down list.

Alternatively, a badge code may be assigned via the GuardPoint10 Cardholders screen or the Badges screen. If a badge has not been assigned to a participant before the Check In Details area is opened, the **Badge** field will be empty.

» **ID Type:** The ID that the visitor will exchange for a badge (i.e. Driver license).

» **ID Number:** The unique number on the ID exchanged by the visitor.

» **Rack Number:** The partition or box number where the visitor's ID will be stored while they have a badge.

4. Complete the Check In Details and exchange the visitor's ID for the assigned badge.

For more information about the Check In Detail area fields, see "[Visitor Control Web Application](#)" on page 645.

5. Click **Save** located in the visit details heading. The information entered since the previous Save operation is saved to the database and the visit's status, in the log on the left side of the screen, has changed to **Checked In**.

## How to record the start of a visit

**Note:** A visitor must be checked in before a visit can be started.

1. Open Visitor Control in your web browser.

» If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`

» If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`

2. After opening the Visitor Control page in your web browser, do one of the following.

- » Find a **Checked In** visit in the log on the left side of the screen and click on the row. The visit's details are displayed over the day calendar.
- » Navigate to the day calendar page where the visit is scheduled to start and scroll to the visit's scheduled start time. The visit entry is displayed in a rectangle in the line of the scheduled time.

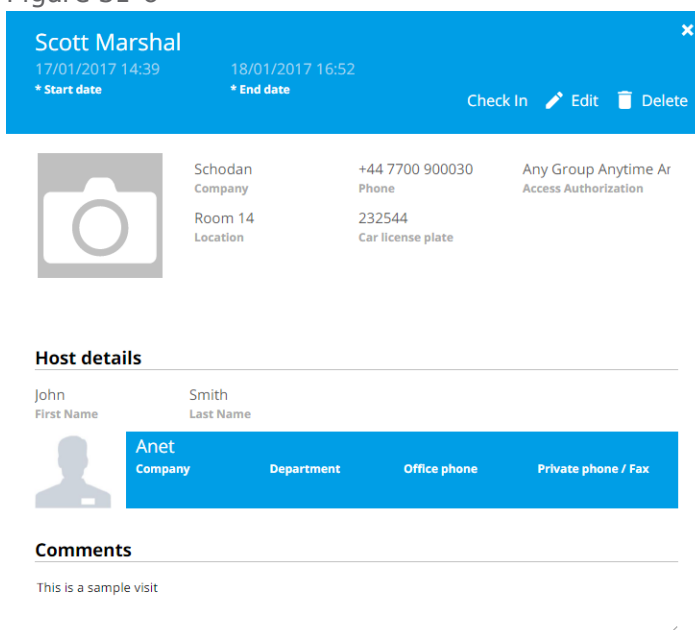
The background color of the rectangle is **Dark blue** to indicate the visit's stage in the life-cycle.

Click the **Dark blue** rectangle to display a drop-down list of actions, and do one of the following:

- Select **Start Visit** in the drop-down list.
- Select **Edit** from the drop-down list.

After selecting **Start Visit** or **Edit** in the drop-down list, the visit's details are displayed over the day calendar.

Figure 31-6



For information about the visit detail's field, see "[Visitor Control Web Application](#)" on page 645.

3. If **Edit** was selected from the day calendar's drop-down list or the details were opened from the log on the left side of the screen, click **Start Visit** in the visit details heading. The **Start Visit** button changes to an **End Visit** button.

If **Start Visit** was selected from the drop-down list, the **End Visit** button is already displayed in the heading. After the Start Visit operation is initiated, it is saved to the database and the visit's status, in the log on the left side of the screen, is changed to **Started Visit**.

## How to record the end of a visit



**Note:** A visit must be started before it can be ended.

1. Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
  - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`
2. After opening the Visitor Control page in your web browser, do one of the following.
  - » Find a **Started** visit in the log on the left side of the screen and click on the row. The visit's details are displayed over the day calendar.
  - » Navigate to the day calendar page where the visit is scheduled to start and scroll to the visit's scheduled start time. The visit entry is displayed in a rectangle in the line of the scheduled time.

The background color of the rectangle is **Dark blue** to indicate the visit's stage in the life-cycle.

Click the **Dark blue** rectangle to display a drop-down list of actions, and do one of the following:

- Select **End Visit** in the drop-down list.
- Select **Edit** from the drop-down list.

After selecting **End Visit** or **Edit** in the drop-down list, the visit's details are displayed over the day calendar.

For information about the visit detail's field, see "[Visitor Control Web Application](#)" on page 645.

3. If **Edit** was selected from the day calendar's drop-down list or the details were opened from the log on the left side of the screen, click **End Visit** in the visit details heading. The **End Visit** button is removed.

If **End Visit** was selected from the drop-down list, the **End Visit** button is already removed from the heading.

After the End Visit operation is initiated, it is saved on the database the visit's status, in the log on the left side of the screen, is changed to **Ended Visit**, and the visit rectangle color changes to **Brown** in the day calendar.

## Deleting a Visit Event

Use the following steps to delete a visit. A deleted visit means that the visit is removed from the Visitor Control log and the database. The visitor-cardholder who was added to the GuardPoint10 Cardholders screen because of the visit is archived and if they were assigned a badge code, the code's status is changed to **Free** in the GuardPoint10 Badges screen.



**Note:** You cannot undo a Delete Visit operation.

## How to delete a visit

Open Visitor Control in your web browser.

- » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
- » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`

After opening the Visitor Control page in your web browser, do one of the following:

- » Find a visit in the log on the left side of the screen and click on the row. The visit's details are displayed over the day calendar.
- » Navigate to the day calendar page where the enrolled visit is scheduled to start and scroll to the visit's scheduled start time. The visit entry is displayed in a rectangle in the line of the scheduled time.

Click the rectangle to display a drop-down list of actions, and do one of the following:

- » Select **Delete** in the drop-down list and confirm the operation. The visit entry is removed from the day calendar and from the log on the left side of the screen. The visit is also removed from the database.
- » Select **Edit** from the drop-down list. The visit's details are displayed over the day calendar. In the details heading, click **Delete**, and then confirm the operation. The visit's details page is closed. The visit entry is removed from the day calendar and from the log on the left side of the screen. The visit is also removed from the database.

Regardless of the method used to delete a visit, the visitor-cardholder created for the visit is archived in the GuardPoint10 Cardholders screen. If a badge code was assigned to the visitor for the visit, its status is changed to **Free** in the GuardPoint10 Badges screen.

## Duplicating a Visit

Use the following steps to duplicate a visit.



**Note:** A duplicate visit should be considered a starting point for a new visit. The visit details in the duplicate visit should be edited in some way to best describe the new visit.

### How to duplicate a visit

1. Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
  - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`

From the web browser, you can either enter the web address of the Visitor Control and press **Enter** or select it from a pre-assigned bookmark.

2. From the day calendar, navigate to the day when the original visit is scheduled to start and scroll to the visit's scheduled start time. The visit will appear in a colored rectangle in the line of the scheduled time.

The background color of the rectangle indicates the visit's stage in its lifecycle.

- » **Light blue**: A visit has been recorded (Enrolled), but not started.
- » **Dark blue**: A visitor has been checked in or a visit has been started.
- » **Brown**: A visit has ended.

3. Click the colored rectangle of a visit and select **Duplicate** from the drop-down list. A duplicate of the original visit's details is displayed over the day calendar with the following differences:
  - » The duplicate visit's lifecycle stage will be "Enrolled", regardless of the stage of the original visit.
  - » The duplicate visit and its details will not be recorded in the database until **Save** is clicked on the details page.
4. Change at least one detail in the duplicate visit (i.e. the visitor's name, the scheduled start time, the scheduled end times, etc.).

For information about the fields on the visit details page, see "[Visitor Control Web Application](#)" on page 645.

5. Click **Save** in the duplicate visit details heading at the top of the details page. The visit is saved. The visit details page is closed and the visit entry appears in the day calendar at the defined start time and in the log on the left side of the screen.



**Note:** Badge codes are excluded from the duplication operation. This means that if the visit that was duplicated includes a badge code assignment, the assignment will not be duplicated in the new visit.

## Editing a Visit Event

Visit information may be edited at any point in the visit's lifecycle.

Use the following steps to edit a visit.



**Note:** You can change the details of a visit (i.e. visitor name, schedule, check in information, etc.), but you cannot revert to an earlier point in the lifecycle of the visit.

## How to edit a visit

1. Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
  - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`
2. After opening the Visitor Control page in your web browser, do one of the following:
  - » Find a visit in the log on the left side of the screen and click on the row. The visit's details are displayed over the day calendar.

In the visit details heading, click **Edit**. The details are in edit mode.

- » Navigate to the day calendar page where the enrolled visit is scheduled to start and scroll to the visit's scheduled start time. The visit entry is displayed in a colored rectangle in the line of the scheduled time.

Click the rectangle to display a drop-down list of actions, and select **Edit**, the visit's details are displayed over the day calendar in Edit mode.

3. Change the visit's details as required, and click **Save** in the visit details heading. The details are updated in the database. Depending on the nature of the changes, updates may also occur in the Visitor Control page's log, and the GuardPoint10 Cardholder and Badges screens.

For information about the fields on the visit details page, see "[Visitor Control Web Application](#)" on page 645.



**Note:** While the visit details page is opened for editing, you may also advance the lifecycle stage of the visit (i.e. check in the visitor, start the visit, etc.). For information about advancing the lifecycle, see "[Advancing the Lifecycle of a Visit Event](#)" on page 414.

# VM Meetings

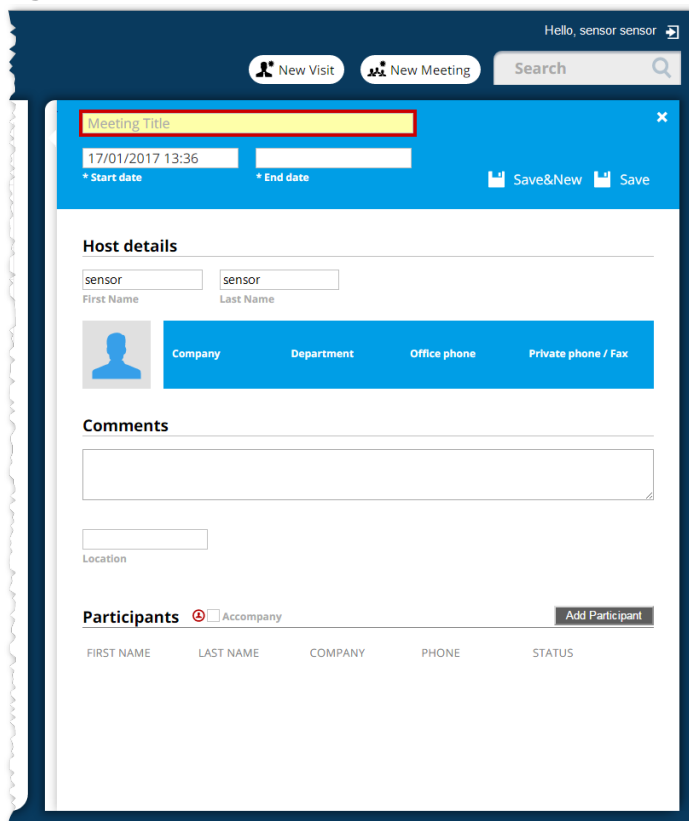
## Adding a New Meeting

Use the following steps to create a new meeting via the Visitor Control screen.

### How to add a new meeting to the system

1. Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
  - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`
2. From the Visitor Control page, click **New Meeting**. A New Meeting details page is displayed on the right side of the browser, over the day calendar.

Figure 31-7



The screenshot shows the 'New Meeting' details page in a web browser. The page has a dark blue header with 'Hello, sensor sensor' and navigation buttons for 'New Visit' and 'New Meeting'. A search bar is also present. The main content area is white with a blue header for the meeting details. It includes a 'Meeting Title' field, 'Start date' (17/01/2017 13:36) and 'End date' fields, and 'Save & New' and 'Save' buttons. Below this is the 'Host details' section with 'First Name' and 'Last Name' fields, a profile picture placeholder, and a table for 'Company', 'Department', 'Office phone', and 'Private phone / Fax'. There is also a 'Comments' section with a text area and a 'Location' field. At the bottom, there is a 'Participants' section with an 'Accompany' checkbox and an 'Add Participant' button. A table with columns for 'FIRST NAME', 'LAST NAME', 'COMPANY', 'PHONE', and 'STATUS' is partially visible.

For information about each field in the New Meeting details, see "[Visitor Control Web Application](#)" on page 645.

3. Enter the title of the meeting in the **Meeting Title** field found in the new meeting details page heading.
4. In the **Start Date** and **End Date** fields, schedule a time for the meeting. The meeting's **Start Date** and **End Date** values are required. The **End Date** must be later than the **Start Date**.



- (Optional) The host's details are automatically entered by the system based on the logged-in operator's data found in the system database. The host may be changed at any time by typing a few letters of the new host name in one of the host name fields. A list of potential hosts that include the typed letters will appear below the field. Select the new host's name from the list.

A host must be listed as an **Employee** in the GuardPoint10 Cardholders screen. For more information about cardholders, see ["Cardholders" on page 193](#).

- (Optional) In the **Comments** field, enter information about the meeting that may be relevant to the meeting's success (i.e. agenda, preparatory reading material, request for refreshments, etc.).
- In the **Meeting Location** field, enter a room number or name identifying where the meeting will take place.
- (Optional) Click **Save**.

You may click **Save** at any time to save data recorded since the previous save operation. If you clicked **Save**, the details will be in Read-Only mode. Click **Edit** in the heading to switch to Edit mode and continue to add participants or update existing information.

- Click **Add Participant**. Fields about an individual who will be invited to the meeting are displayed.

Figure 31-8

The screenshot shows a web application interface for adding a participant. At the top, there is a 'Meeting Location' input field. Below it is a 'Participants' section with a table header containing 'FIRST NAME', 'LAST NAME', 'COMPANY', 'PHONE', and 'STATUS'. To the right of this table is an 'Add Participant' button. Below the table is a 'Participant Details' form with several input fields: 'First Name', 'Last Name', 'Company', 'Phone', 'Access Authorization' (a dropdown menu with 'No Group Never Nowhere' selected), 'Car license plate', and a checkbox for 'Amadeus 8 Escort'. A 'Cancel' button is located at the bottom right of the form.

The **Accompany All** checkbox will apply to all participants in your list. When selected, the participants will require someone to accompany them while on the premises.

- Complete the following fields in a participant's area:

- » **First name**
- » **Last name** (required)
- » **Company**
- » **Phone**
- » **Access Authorization** (required)
- » **Car License Plate**
- » **GuardPoint10 Escort**

For information about the fields, see ["Visitor Control Web Application" on page 645](#).

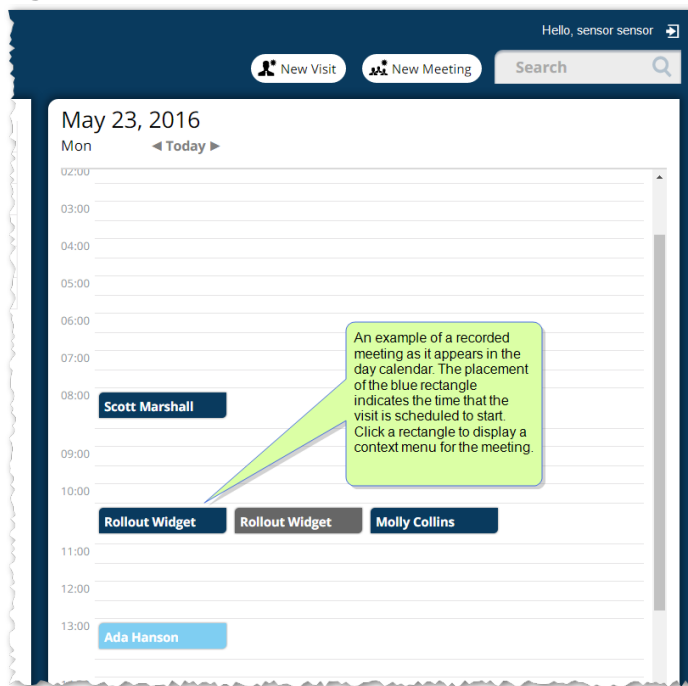
11. Click **Save&Close**. in the participant's area. The participant's details contract to reveal only the basic information in a single row.

You must save each participant's information before you click **Save** in the heading, where all meeting details are saved. To continue entering data, you must click **Edit** in the heading to return to Edit mode.

If you click **Add Participant** without saving the details of a previously added participant, the previously add participant's details are automatically saved and contracted, and a new set of participant details are displayed.

12. Repeat Steps 10 and 11 and for each meeting participant, except for the host.
13. In the heading of the meeting details page, click **Save**. The meeting is recorded in the log to the left of the details page with a status of **Enrolled**.
14. Click the white **x** at the top right of the meeting details heading. The meeting details are closed and the meeting appears in the day calendar on the page corresponding to the meeting's start date.

Figure 31-9



For more information about the day calendar, see "[Visitor Control Web Application](#)" on page 645.

## Advancing the Lifecycle of a Meeting

Use the following steps to advance an existing meeting's lifecycle via the Visitor Control screen.

These instructions walk you through each progression in a meeting's lifecycle. The lifecycle starts after a meeting is created (see "[VM Meetings](#)" on page 422).

**Note:** You cannot turn back the clock. Once the lifecycle of a meeting or a meeting participant has been advanced, it cannot be reversed.

# How to advance the lifecycle of a meeting

1. Open Visitor Control in your web browser.
    - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
    - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`
  2. After opening the Visitor Control page in your web browser, do one of the following:
    - » Find the meeting in the log on the left side of the screen and click the meeting row. The meeting details are displayed over the day calendar on the right side of the screen.
    - » Navigate to the day calendar page where the meeting is scheduled to start and scroll to the meeting's scheduled start time. The meeting title appears on the calendar in a rectangle. The background color of the meeting rectangle indicates the meeting's stage in its lifecycle.
      - » **Light blue**: A meeting has been recorded, but not started (Enrolled).
      - » **Dark blue**: At least one meeting participant has been checked in or has started their meeting.
      - » **Brown**: All meeting participants have ended their meeting.
- Click the rectangle and select **Edit** from the drop-down list. The meeting details are displayed in Edit mode over the day calendar.

Figure 31-10

Rollout Widget

23/01/2017 10:15 24/01/2017 00:00  
\* Start date \* End date Save Delete

**Host details**

John Smith  
First Name Last Name

Anet  
Company Department Office phone Private phone / Fax

**Comments**

The is a sample meeting.

Room 12  
Meeting Location

**Participants** Add Participant

Accompany all

FIRST NAME	LAST NAME	COMPANY	PHONE	STATUS
Tony	Johnson	Balda	346657234	Enrollment
Sheryl	Ford	Balda	67456358	Enrollment

For information about each field in a meeting's details, see "[Visitor Control Web Application](#)" on page 645.

# Check In a meeting participant

To advance an Enrolled meeting to Check in, you must advance one meeting participant to Check in. A meeting that has no participants cannot be advanced beyond enrollment.

After completing step 2 above, do the following.



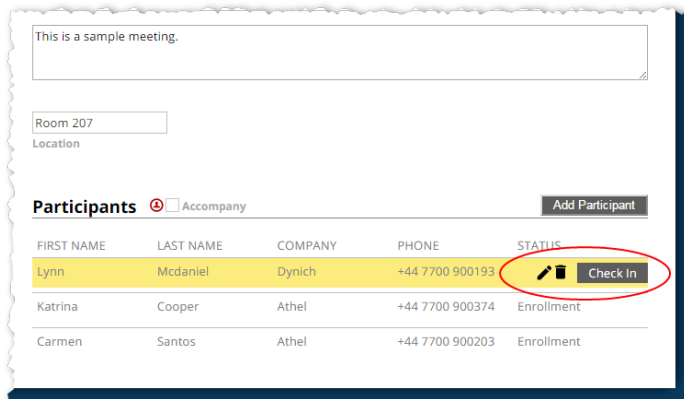
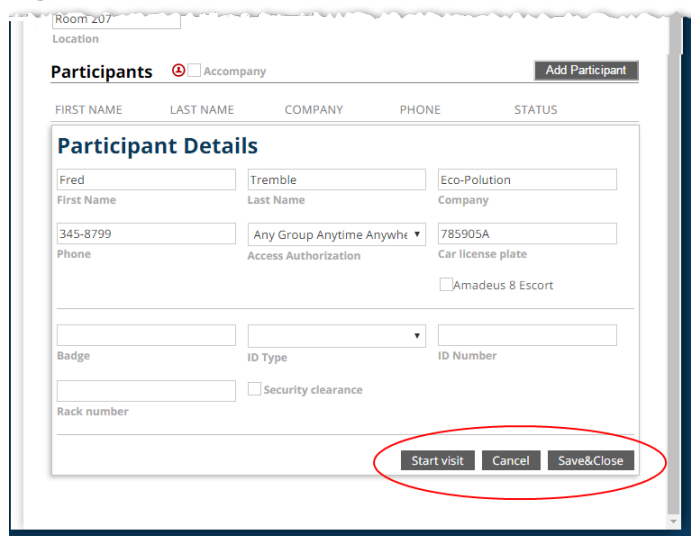
1. In the Participants table, mouseover an enrolled participant, an **Edit**  and **Delete**  icon along with a **Check in** button appears in the participant's row.

Figure 31-11



2. Click **Check in** for a participant as they arrive for the meeting. Check in details appear below the participant's basic information and the **Check in** button changes to a **Start visit** button that is followed by a **Cancel** button and **Save&Close** button.

Figure 31-12



A participant's check in details contains information about the exchange of a participant's ID for a badge that will provide access to the meeting location. The check in details are as follows:

- » **Badge**: The badge code assigned to the participant. A **Free** badge code may be selected from the Badge field by entering a character from a code and selecting the code from the field's drop-down list.

Alternatively, a badge code assignment may be performed via the GuardPoint10 Card-holders screen or the Badges screen. If a badge has not been assigned to a participant before the Check in details is opened, the **Badge** field will be empty.

- » **ID Type**: The ID that the participant will exchange for a badge (i.e. Driver license).
- » **ID Number**: The unique number on the ID exchanged by the participant.
- » **Rack Number**: The partition or box number where the ID will be stored until it is returned to the participant.
- » **Security clearance**: When selected, the participant has been approved to receive a badge.

3. Complete the Check in details and exchange the visitor's ID for the assigned badge.

For more information about the Check in details, see "[Visitor Control Web Application](#)" on page 645.

4. Click **Save&Close** located at the bottom of the Check in details. The Check in details are saved in the database, and the Visit Control log on the left side of the screen is updated (i.e. the Status column now displays Checked in).

## Start a meeting participant's visit

To advance a Checked in meeting to a started meeting, you must advance one meeting participant to Start visit.

After you have checked in a participant, do the following.



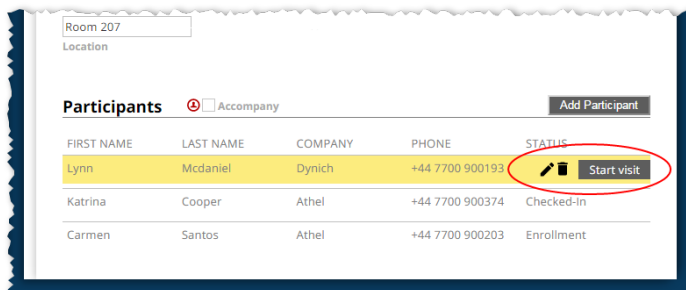
1. In the Participants table, mouseover a checked in participant, an **Edit**  and **Delete**  icon along with a **Start visit** button appears in the participant's row.

Figure 31-13



2. Click **Start visit** for a participant. The **Start visit** button changes to an **End visit** button. The change is saved in the database, and the Visit Control log on the left side of the screen is updated (i.e. the Status column now displays Started visit).

Alternatively:




1. In the Participants table, mouseover a checked in participant, an **Edit**  and **Delete**  icon along with a **Start visit** button appears in the participant's row.
2. Click . The participant's details appear.
3. At the bottom of the participant's details, click the **Start visit** button.

Figure 31-14

Room 207  
Location

**Participants**  Accompany Add Participant

FIRST NAME	LAST NAME	COMPANY	PHONE	STATUS
<b>Participant Details</b>				
Fred First Name	Tremble Last Name	Eco-Polution Company		
345-8799 Phone	Any Group Anytime Anywh Access Authorization	785905A Car license plate		<input type="checkbox"/> Amadeus 8 Escort
<input type="text"/> Badge	<input type="text"/> ID Type	<input type="text"/> ID Number		
<input type="text"/> Rack number	<input type="checkbox"/> Security clearance			
<input type="button" value="Start visit"/> <input type="button" value="Cancel"/> <input type="button" value="Save&amp;Close"/>				

The participant's details contract and, when you mouseover the participant, you will notice that the **Start visit** button has changed to an **End visit** button. The change is saved in the database, and the Visit Control log on the left side of the screen is updated (i.e. the Status column now displays Started visit).

Figure 31-15

Room 207  
Location

**Participants**  Accompany Add Participant

FIRST NAME	LAST NAME	COMPANY	PHONE	STATUS
Lynn	Mcdaniel	Dynich	+44 7700 900193	<input type="button" value="End Visit"/>
Katrina	Cooper	Athel	+44 7700 900374	Enrollment
Carmen	Santos	Athel	+44 7700 900203	Enrollment

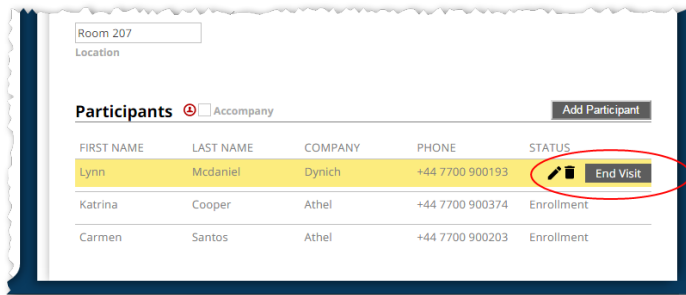
## End a meeting participant's visit

To advance a Started meeting to an Ended meeting, you must advance all meeting participants to End visit.

After advancing all meeting participants to **Started visit**, do the following to each participant's meeting status.

1. In the Participants table, mouseover a participant, an **Edit** and **Delete** icon along with an **End visit** button appears in the participant's row.

Figure 31-16



2. Click **End visit** for a participant. The **End visit** button changes to an **Ended** disabled button. The change is saved in the database.

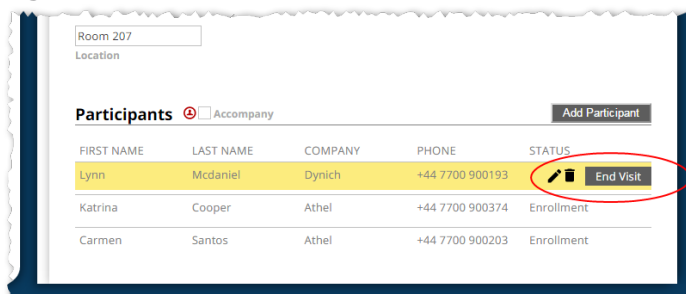
Even though a participant's meeting has ended, the participant's data can still be edited and the participant can still be deleted from the Participant list

3. Repeat steps 1 and 2 for all of the remaining meeting participants. After you have ended all of the participants' visits, the meeting status will be marked **Visit Ended**. The status will be saved in the database, and the Visit Control log on the left side of the screen is updated (i.e. the Status column now displays Visit ended).

Alternatively:

1. In the Participants table, mouseover a participant whose visit has already started, an **Edit** and **Delete** icon along with an **End visit** button appears in the participant's row.

Figure 31-17



2. Click the **Edit** icon. The participant's details appear.
3. At the bottom of the participant's details, click the **End visit** button.

Figure 31-18

Room 207  
Location

**Participants**  Accompany Add Participant

FIRST NAME LAST NAME COMPANY PHONE STATUS

**Participant Details**

Fred Tremble Eco-Polution  
First Name Last Name Company

345-8799 Any Group Anytime Anywh 785905A  
Phone Access Authorization Car license plate

Amadeus 8 Escort

Badge ID Type ID Number

Security clearance

Rack number

Start visit Cancel Save&Close

The participant's details contract and, when you mouseover it, the **End visit** button changes to an **Ended** disabled button. The change is saved in the database.

**Note:** Even though a participant's meeting has ended, the participant's data can still be edited and the participant can still be deleted from the Participant list.

- Repeat steps 1 - 3 for all of the remaining meeting participants. After you have ended all of the participants' visits, the meeting status will be marked **Visit Ended**. The status will be saved in the database, and the Visit Control log on the left side of the screen is updated (i.e. the Status column now displays Visit ended).

Participants who have ended a meeting are archived in the GuardPoint10 Cardholders screen. If a participant was assigned a badge code, the code has changed its status to **Free** in the Badges screen.

## Deleting a Meeting

Use the following steps to delete a meeting. A deleted meeting means that the meeting is removed from the Visitor Control log and the system database.

**Note:** You cannot undo a Delete Meeting operation.

### How to delete a meeting

There are two ways to delete a meeting, from the day calendar and from meeting details.

#### From the day calendar:

- Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`



- » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`
- 2. In the day calendar, navigate to the day when the meeting is scheduled to start and scroll to the meeting's scheduled time. The meeting entry is displayed in a colored rectangle in the line of the scheduled time.
- 3. Click the rectangle and select **Delete** from the drop-down list, and then confirm the operation. The meeting entry is removed from the day calendar, the log on the left side of the screen, and the database.

Participants of a deleted meeting are archived in the GuardPoint10 Cardholders screen. If a participant was assigned a badge code, the code has changed its status to **Free** in the Badges screen.

## From the meeting details:

1. Open Visitor Control in your web browser.  
From the web browser, you can either enter the web address of the Visitor Control and press **Enter** or select it from a pre-assigned bookmark.
2. From the log on the left side of the screen, find the meeting and click the row. The meeting details are displayed over the day calendar.  
Alternatively, click the meeting entry in the day calendar and select **View details** or **Edit** from the drop-down list. The meeting details are displayed over the day calendar.
3. In the meeting details heading, click **Delete**, and then confirm the Delete operation. The meeting details are closed. The meeting entry is removed from the day calendar, the log on the left side of the screen, and the database.

Participants who have ended a meeting are archived in the GuardPoint10 Cardholders screen. If a participant was assigned a badge code, the code has changed its status to **Free** in the Badges screen.

## Duplicating a Meeting

Use the following steps to duplicate a meeting.




**Note:** A duplicate meeting should be considered a starting point for a new meeting. The meeting details in the duplicate meeting should be edited in some way to best describe the new meeting.

In the duplicate meeting, The lifecycle of the meeting and the status of each participant in the meeting is set to Enrolled, regardless of the original meeting's status.

## How to duplicate a meeting

1. Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
  - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`


2. From the day calendar, navigate to the day when the original meeting is scheduled to start and scroll to the meeting's scheduled start time. The meeting will appear in a colored rectangle in the line of the scheduled time.
3. Click the colored rectangle of the original meeting and select **Duplicate** from the drop-down list. Duplicate details of the original meeting are displayed in Edit mode over the day calendar with the following differences:
  - » The duplicate meeting's lifecycle stage will be **Enrolled** and none of the participants will be checked in, regardless of their stage in the original meeting.
  - » In the duplicate meeting's details, "[copy]" will be added to the meeting title.
  - » The Duplicate meeting and its details will not be recorded in the database until **Save** is clicked in the details heading.
4. (Recommended) Change at least one detail in the duplicate meeting (i.e. the meeting title, the scheduled start time, the scheduled end time, the list of participants, etc.).
5. Click **Save** in the duplicate meeting's details heading at the top of the details page. The meeting is saved with the updated detail information. The meeting details page is no longer in Edit mode. The meeting entry appears in the day calendar at the defined start time and in the Visitor Control log, on the left side of the screen.



**Note:** Badge codes are excluded from the duplication operation. This means that if the meeting that was duplicated has participants with badge code assignments, the assignments will not be duplicated in the new meeting.

## Editing a Meeting

Use the following steps to edit a meeting.



**Note:** You can change the details of a meeting (i.e. meeting title, a participant's name, schedule, check in information, etc.), but you cannot revert to an earlier point in the lifecycle of the meeting.

## How to edit a meeting

1. Open Visitor Control in your web browser.
  - » If you are opening the Visitor Control on the machine with the server GuardPoint10 installation, enter `localhost/Visitors/`
  - » If you are opening the Visitor Control on a machine with a Client GuardPoint10 installation, enter `http://<GuardPoint10 Server machine name>/Visitors/`
2. From the day calendar, navigate to the day when the meeting is scheduled to start and scroll to the meeting's scheduled start time. The meeting will appear in a colored rectangle in the same line as the scheduled start time.


The background color of the meeting rectangle indicates the meeting's lifecycle stage.

- » **Light blue:** A meeting has been recorded, but not started (Enrolled).
  - » **Dark blue:** At least one meeting participant has been checked in or has started their meeting.
  - » **Brown:** All meeting participants have ended their meeting.
3. Click the meeting rectangle and select **Edit** from the drop-down list. The meeting details are displayed over the day calendar in edit mode.
  4. Change the meeting's details as required, and then click **Save**. The details are updated in the database.

For information about the fields on the meeting details page, see "[Visitor Control Web Application](#)" on page 645.

## How to edit a meeting's Participants table

Each entry in the Participants table initially appears with only a participant's basic information.

- » To add a participant to the Participants table, click the **Add Participant** button above the list. A new participant entry is appended to the bottom of the list. Enter the new participant's information, and then click the **Save** button found below the participant's detail fields. The new participant is saved in the database and appears in the list with their basic details visible.
- » To edit a participant's basic information, mouseover a participant's row and click the **Edit**  icon. Participant detail fields are displayed in edit mode. After editing the information in the fields, click the **Save&Close** button below the participant's detail fields. The participant's information is saved in the database and the Visitor Control screen is updated as required.

Click **Save** in the heading of the meeting details page to save all of the details.



**Note:** While the meeting details page is opened for editing, you may also advance the meeting's stage in its lifecycle (i.e. Check In a participant). For information about the lifecycle, see "[Advancing the Lifecycle of a Meeting](#)" on page 424.

A meeting or participant's lifecycle status cannot be reversed. For example, a participant's status that has been advanced to **Started visit** cannot be returned to a **Checked in** status. The participant would have to be deleted from the Participants table and added again.

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# CHAPTER 32:

## From the Dashboard: License, Help, and About

The following is accessible from the Help item in the dashboard:

- » License screen
- » HTML Help
- » About the software

The License screen presents the scope of the GuardPoint10 license, and what is currently in use. The license screen includes:

- » The scope of the current license
- » The capabilities currently in use on the system
- » The workstations running on the system
- » Instructions and tools required to change the license (must have a serial code provided by your provider).

For more information about the License screen, see "[License, Help, and About](#)" on page 693.

The GuardPoint10 Help is displayed in a web browser that supports HTML5. It includes:

- » General information about GuardPoint10 solution modules.
  - » A detailed description of each screen.
  - » Step-by-step instruction to perform the various tasks available.
- and more...

The About box includes the version number of your GuardPoint10 installation as well as copyright information.

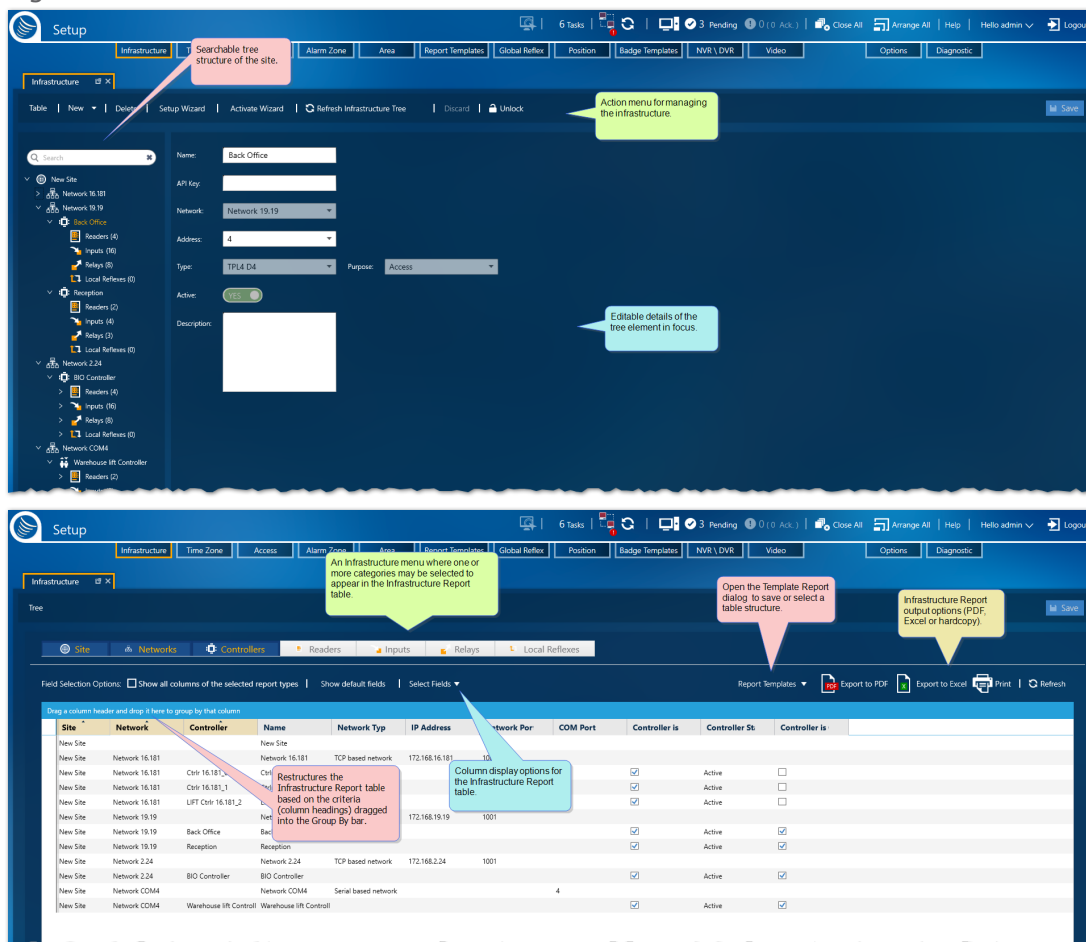
# APPENDIX A:

## Screen Descriptions

This section contains information about the screens and dialogs you may encounter while performing a task in GuardPoint10. Each topic contains the name of the screen or dialog followed by a picture and a table listing each parameter along with a brief description.

# Infrastructure Screen Views: Tree and Table

Figure A-1



The infrastructure screen has two views Tree and Table. In the Tree view, you can manage the infrastructure data via a selected tree element and related detail fields. In the Table view infrastructure data is presented in a read-only tabular format based on the category(s) selected above the table.

The system treats the Infrastructure's Table view screen as a report where information can be filtered, sorted, and grouped according to the needs of the operator.

A Table view report's manual output may be in a PDF format or an Excel format. In addition, the report may also be printed.

A Table view report may be saved as a Report Template via action bar **Report Template** button. The advantages of a report template are:

- » Display a complex report structure with a couple of clicks.
- » Automatically save a template report to file or email it to others via a global reflex "Create Template-based report" on page 548 action.

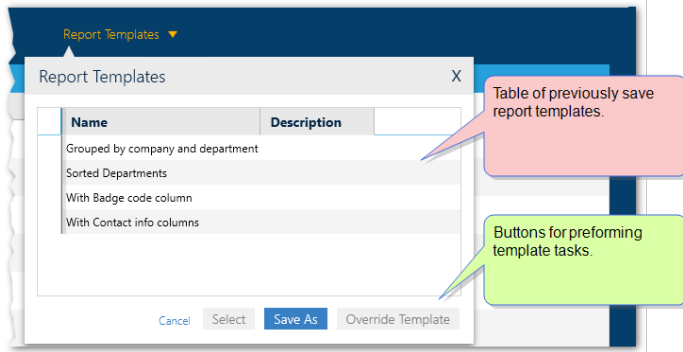


# Report Template dialog

The structure of the screen table can be saved in a template so it can be applied later, either to the screen display or a global reflex ["Create Template-based report" on page 548](#) action. The data in a template is dynamic and will change to reflect the environment.

To start using templates click the **Report Templates** button.

Figure A-2



The table in the Report Template dialog contains the names and descriptions of previously save templates, which are specific to the screen displayed.

From the screen's Report Template dialog you can click:

- » **Save As:** Opens the ["Report Template Screen" on page 529](#), where the current structure of the displayed table can be saved.
- » **Override:** Opens the ["Report Template Screen" on page 529](#), where the current structure of the displayed table can override the last selected template with the current structure of the displayed table.
- » **Select:** Displays current data in the template selected from the dialog's table.

The primary purpose of the Table view is to produce a comprehensive picture of the infrastructure in a tabular format where a report template may be saved or applied to the displayed table.

# Setup Wizard: Site -> Network -> Controllers

Figure A-3

**Step 1:** Name the site and specify the number of COM and TCP networks that will be in the site. This is not fixed. Additional networks may be added in the future.

**Step 2:** Enter information about the controllers in each network, and then click ADD. A drop-down list of controllers appears below the network name and information fields.

**Step 3:** A summary of your selections is displayed. To place the site, networks and controllers in your system, click FINISH.

**Note:** Some of the information required for this wizard is acquired from the controller hardware (i.e. COM Port, TCP IP address, controller ID). Before beginning the site setup, contact your hardware installer to get this information.

The Setup wizard guides you through the complex setup tasks for your site, networks, and controllers. The wizard collects information about the setup via a structured set of dialogs that the operator steps through using the navigation buttons at the bottom of each dialog.

In Step 1 and Step 2, enter information that defines the fundamental parameters of the site, networks, and controllers. In Step 3, a text and a tree structure describe what was created in Steps 1 and 2. If you are satisfied, click the **Finish** button to save the structure.

After completing the Setup wizard, a message is displayed asking if you would like to start the Activation wizard. The Activation wizard allows polling to take place between a controller and the server. The new network / controller structure appears in the Infrastructure tree, regardless of your choice to start the Activation wizard or not.

Additional information may be required for each element added to your site. These details can be specified, and existing details can be edited, in the relevant screens.

The following table includes descriptions of each element in the Setup wizard's steps.

## Setup Wizard Parameters

Parameter	Description
<b>Step 1: Basic details</b>	
Define required number of sites	<p>If MultiSite is set to <b>No</b> in the Options screen, only one site may be defined per system installation. Therefore, this field will be set to "1" and uneditable.</p> <p>If MultiSite is set to <b>Yes</b> in the Options screen, more than one site may be added via the wizard.</p> <hr/> <p><b>Note:</b> You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.</p>
Site name	<p>A free text field that identifies the site. The default name is "New Site".</p> <p>A best practice is to rename the site to something that identifies the site's location or purpose and allows you to recognize the site (i.e. "South Campus" or "Primary Site_1").</p> <p>The site name must be unique.</p>
Define required number of networks	The networks are broken down into two categories: COM and TCP. The number of networks for each category is entered below this title.
Total COM networks	The number of networks on the site that will operate using a COM protocol to communicate with other elements on the site.
Total TCP networks	The number of networks on the site that will operate using a TCP protocol to communicate with other elements on the site.
<b>Step 2: Networks</b>	
Network name	<p>An automatically generated name that identifies the network. The default name formats are as follows:</p> <ul style="list-style-type: none"> <li>» For COM networks: "Network_Com&lt;#&gt;", where '#' is a sequential number that makes the name unique.</li> <li>» For TCP networks: "Network_Tcp&lt;#&gt;", where '#' is a sequential number that makes the name unique.</li> </ul> <p>A best practice is after you have completed the wizard; rename each network to something that identifies the network's location or purpose via a network's details. The name must be unique.</p> <p>For more information about changing an existing network's parameters, see <a href="#">"Network Details" on page 445</a>.</p>
Type	The communication protocol type used by a network. The read-only values may be COM or TCP.

Parameter	Description
Connected to (Only visible for COM ports)	The communication port used by a COM network.
IP Address (Only visible for TCP ports)	Identifies a TCP network destination on the site. The site uses an IP address to route messages to a network.  <b>Note:</b> This particular field has a context menu that enables you to copy an IP address and paste it into other IP address fields.
Port (Only visible for TCP ports)	The communication port used by a TCP network.
Controller type	The type of controller(s) you are adding to a network. Select a type from the field's drop-down list.
Purpose	The expected behavior of the <b>Controller type</b> selected. For example, a controller connected to a reader at a lift (elevator) will not behave the same way as a controller at an office door. The system adjusts its handling of information received from a controller based on its purpose.
Amount	The number of controllers of the same type and subtype that you are adding to a network.
ADD button	Adds the controller(s) to a network. Whether or not the controller(s) has been physically installed is not a factor.

## MultiSite impact on the interface - Setup wizard

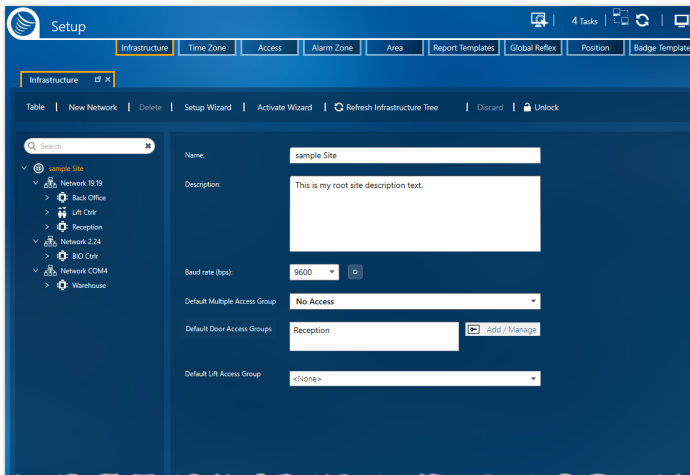
**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the Setup wizard is as follows:

- » Only operators who are super users may add sites with networks and controllers for those sites.
- » An operator, with access to the Setup wizard, may add networks and controllers only to their site.
- » An operator, with access to the Setup wizard, who is shared with other sites, may choose from all sites, where they are shared, to add networks and controllers.

# Site Details

Figure A-4



A site item in the Infrastructure tree has a unique context menu item called Stop Polling or Start Polling. This menu item will stop/start polling for your entire site. The menu item makes infrastructural maintenance more convenient.

## Site Parameters

Parameter	Description
Name	<p>A free text field that identifies the site.</p> <p>A best practice is to name the site to something that identifies the site's location or purpose and allows you to recognize the site (i.e. "South Campus" or "Primary Site_1").</p> <p>The site name must be unique.</p>
Description	<p>(Optional) A free text field where information about the site can be entered.</p>
<b>Baudrate</b> <sup>1</sup>	<p>The rate at which information is transferred in a communication channel to a controller. This rate is the same for all controllers on the site.</p> <p>Default rate: 9600 bd.</p> <p>This means that the serial port is capable of transferring a maximum of 9600 bits per second.</p> <p>To update all controllers to the selected rate in real time, click the icon next to the <b>Baudrate</b> field.</p>

<sup>1</sup>The rate at which information (signal or symbol changes) is transferred per second.

Parameter	Description
Default Multiple Access Group	<p>The Multiple Access Group that is initially assigned to a new cardholder, or an imported cardholder who has no Multiple Access Group setting. The default Multiple Access Group may be changed for an individual cardholder via the "<a href="#">Operator (User): MultiSite Impact Cardholder Details</a>" on page 607, or the Cardholders table context menu.</p> <p>The default Multiple Access Group will be available to all operators regardless of any profile limitation.</p> <p>If <b>Default Multiple Access Group</b> is set to <b>Anytime Anywhere</b>, a cardholder, of type visitor, will bypass the default setting and initially be set to <b>No Access</b>.</p> <p>The initial default is <b>No Access</b>.</p>
Default Door Access Groups	<p>A list of one or more Door Access Groups that are initially assigned to a new cardholder as a Personal Door Access Group. If there is a conflict between the assigned Multiple Access Group and an assigned Door Access Group, the Door Access Group has a higher priority.</p> <p>The Default is empty.</p>
Default Lift Access Group	<p>A Lift Access Group that is initially assigned to a new cardholder as a Personal Lift Access Group. If there is a conflict between the assigned Multiple Access Group and the assigned Lift Access Group, the Lift Access Group has a higher priority.</p> <p>The Default is <b>None</b>.</p>

## MultiSite impact on the interface - Site details



**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the site details is as follows:

- » The **New** button has two options, **Site** or **Network**.
- » There may be multiple sites in the infrastructure. In this case, each site has its own unique set of site parameters.
- » An operator who does not have authorization in the owner site, but whose own site is a sharer of the site will have read-only access to the site's details.
- » An operator who does not have authorization in the Root site and is a super user can add a new site as long as the number of sites already existing is not the maximum allowed by the license.

# Network Details

Figure A-5



## Network Parameters

Parameter	Description
Name	<p>A free text field that identifies the network.</p> <p>A best practice is to rename the network to something that identifies the network's location or purpose.</p> <p>The new network name must also be unique.</p>
API Key (may not be visible)	<p>A network URI that an API can use to identify it.</p> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this field value.</p>
Network	<p>Identifies the type of controllers that will be connected to the network. The options are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Standard Controllers:</b> Controllers, other than a Galaxy panel will be connected to the network.</li> <li>» <b>Galaxy<sup>1</sup> Panel:</b> A Galaxy panel will be connected to the network. Keep in mind that a Galaxy system is integrated into GuardPoint10. The Galaxy system must be installed and connected to your LAN before it can be integrated into GuardPoint10.</li> </ul>
Site	The name of the site where the network is located (read-only).

<sup>1</sup>A Honeywell alarm monitoring system where detectors are connected to a Galaxy panel. The panel manages various kinds of alarms (i.e. fire, intruder, etc.).

Parameter	Description
Adapter (Only visible for TCP networks)	<p>The data access and management solution used to collect data via TCP. The options are as follows:</p> <ul style="list-style-type: none"> <li>» Tibbo</li> <li>» Lantronix</li> </ul> <hr/> <p><b>Note:</b> If you are updating from an GuardPoint10 version that does not include this field, the default value will be Tibbo for all networks in the infrastructure after the update installation is completed.</p> <p>A best practice is after the installation, open the infrastructure details of each TCP network that uses Lantronix and set the Adapter field value to Lantronix.</p>
Description	(Optional) A free text field where information about the network is entered.
Type	Identifies the type of communication protocol used for the port (Serial Based Network or TCP).
COM Number (Only visible for Serial Based Networks)	<p>A COM port number, from 1 to 99. Each network, defined as type Serial Based Network, must have a separate corresponding port on the PC.</p> <hr/> <p><b>Note:</b> Not visible in a Galaxy type network.</p>
Split Server	The server where network processing takes place. The default value is the server installed with the GuardPoint10 server installation.
IP Address (Only visible for TCP ports)	Identifies a TCP network destination of the site. The site uses the IP address to route messages to the network.
Command Timeout Delay	<p>The maximum time within which a controller must reply to a command sent by the system (other than a polling command). If a controller does not reply within the specified time, the system will resend the command three more times or until an answer is received from the controller. If, after the third attempt, there is still no reply from the controller, the command will be put in Pending (see "<a href="#">Dashboard</a>" on page 333).</p> <p>Default: 1000ms – Do not change this value unless specifically instructed by SENSOR personnel.</p> <hr/> <p><b>Note:</b> Not visible in a Galaxy type network.</p>
Port (Only visible for TCP ports)	<p>The port used by the network's TCP protocol to communicate within the system. This information should be provided by hardware installation personnel.</p> <p>If you are configuring multiple Galaxy networks, the <b>Port</b> number must be unique for each Galaxy network.</p>



Parameter	Description
Polling Timeout Delay	<p>Polling a controller means the system (on the server side) asks a controller if any events occurred since the last poll, (i.e. either an access transaction (granted or denied) or an alarm).</p> <p>The system continuously polls all controllers, and if nothing happened since the previous polling event, a controller replies with an empty message. If events have taken place, a controller replies with the events that have occurred since the previous polling event.</p> <p>The Timeout polling value is the maximum amount of time, within which a controller must reply to a poll. If a controller does not reply within the specified time, the system will make three more attempts to poll the controller or until a reply is received from the controller. If there is still no reply from the controller, the system will flag this as a communication error (see "<a href="#">Dashboard</a>" on page 333) and jump to the next controller.</p> <p>The system will declare a communication problem if a controller does not reply to a polling query during a predefined <b>Polling error time-out</b> delay. The default delay time is 30 seconds.</p> <p>Default: 1000ms - Do not change this value unless specifically instructed by SENSOR personnel.</p>
<p><b>Note:</b> Not visible in a Galaxy type network.</p>	

Parameter	Description
Polling Interval	<p>The frequency of messages sent to a controller (polling or commands) in milliseconds.</p> <p>Slowing the frequency frees up server resources.</p> <div style="background-color: #4a90e2; color: white; padding: 10px; margin: 10px 0;"> <p><b>For example:</b></p> <p>A Waiting delay value of 50 msec means that in 1 second, the server will send 20 polling commands (<math>20\text{ms} \times 50\text{ms} = 1000\text{ms}</math>) to the same controller network.</p> <p>If 20 controllers are connected to a network, each controller will receive 1 command per second.</p> <p>If only one controller uses the network, the controller will receive a command 20 times per second. In this scenario, the communication on the network may be slowed down to 5 polling commands per second to free up server resources, without causing any significant communication delays.</p> <p>To adjust the system to this setting, the Waiting delay should be set to 200ms (<math>1000/5\text{ms} = 200\text{ms}</math>).</p> </div> <p>Default: 50ms</p> <hr/> <p><b>Note:</b> The communication <b>baudrate</b><sup>1</sup> between controllers and the system is defined in the Site details (see <a href="#">"Site Details"</a> on page 443).</p> <hr/> <p><b>Note:</b> Not visible in a Galaxy type network.</p>

## MultiSite impact on the interface - Network details

**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the network details is as follows:

- » The **New Controller** button has a drop-down list where the owner of the new controller is selected.
- » An **Owner** field appears which identifies the site that has ownership of the network. The owner has complete control of the network.
- » A **Share With** field displays a list of networks where an operator in the network's owner site can choose to share the input with another site.

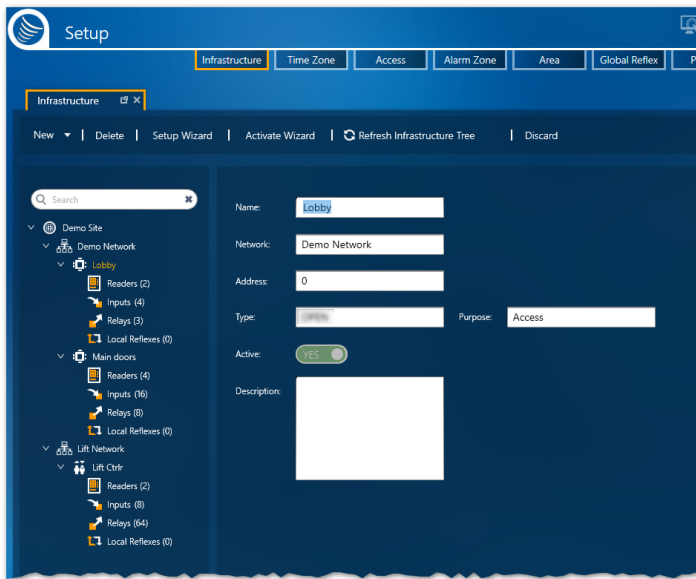
<sup>1</sup>The rate at which information (signal or symbol changes) is transferred per second.

When a network is shared, its ownership is automatically changed to the Root site. The previous owner is then a sharer of the network.

- » An operator who does not have authorization in the owner site, but whose own site is a sharer of the network will have read-only access to the network's details.
- » An operator, who does have authorization to the site that shares the network, can add (and own) a new controller to the network as long as the number of controllers already existing is not the maximum allowed by the license.

# Controller Details

Figure A-6



A controller is a microprocessor-based circuit board with large onboard memory for storing various groups of parameters, such as cardholders, time zones, reflexes, etc. Each controller is connected to the central system via a dedicated network.

The following describes the information found in a controller's details.

## Controller Parameters

Parameter	Description
Name	<p>A free text field that identifies a controller. The default name is "New Controller".</p> <p>A best practice is to rename a controller to something that identifies a controller's location or purpose and allows you to recognize the controller (i.e. "FrontEntrance01" or "FrontEntrance02").</p> <p>The new name must be unique to the site, not just the network where the controller resides.</p>
API Key (may not be visible)	<p>A controller URI that an API can use to identify it.</p> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this field value.</p>
Also Rename Readers, Inputs, and Relays  (Only visible when renaming an existing controller)	<p>When selected, all entities (readers, inputs, and relays) connected to the controller are renamed to their default name with the new controller name incorporated in the entity name.</p> <hr/> <p><b>Note:</b> If an entity has a custom name, the name will be overwritten with the new default name that includes the controller name.</p>

Parameter	Description
Network	The name of the network where a controller will be located.
Address	The physical address of the controller set on the controller Address Selection <b>Dipswitch</b> <sup>1</sup> . This information should be provided by hardware installation personnel.
Type	The type of controller that is being added to the network. To select a controller type, for a new controller installation, click on the field, and select the type from the drop-down list. This information should be provided by hardware installation personnel. After a new controller is saved, the <b>Type</b> value is fixed and cannot be changed.
Purpose	The plan or environment of a controller described in one word found in the parameter's drop-down list. The available drop-down list options are as follows: <ul style="list-style-type: none"> <li>» <b>Access</b>: The controller will be used for general arrivals and departures from premises via a door.</li> <li>» <b>Lift</b>: The controller will be used for a lift (elevator).</li> </ul> For more information about Lift setup, see " <a href="#">Understanding the Lift Setup concept in GuardPoint10</a> " on page 53. After a new controller is saved, the <b>Purpose</b> value is fixed and cannot be changed.
Active	If set to <b>Yes</b> , the controller has established communication with the system, and polling will be performed. If set to <b>No</b> , the controller gathers data locally (via entities), but polling is not performed. This will likely result in the loss of controller data due to an <b>event buffer<sup>2</sup> overflow (FIFO)<sup>3</sup></b> .
Description	(Optional) A free text field where information about the controller is entered.

<sup>1</sup>A series of tiny switches built into circuit boards. The housing for the switches has the same shape as a chip and is usually red.

<sup>2</sup>A temporary storage area in a controller. The buffer contains system events involving entities attached to the controller. An Event buffer is read and cleared by the system during polling (a query as to whether a controller has any data to transmit).

<sup>3</sup>A method of memory management for storing data that arrives at a controller (First In First Out). The oldest transactions are erased to make space for the newer transactions.

Parameter	Description
Script (may not be visible)	<p>A field where command code is entered. The code specifies a command that will be sent to the controller with specific parameters. To add a single line comment inside the script, place '/' in a line, like this:</p> <pre>//comment text</pre> <p>Text following the '/', until the end of the line, will not be evaluated during execution.</p> <p>The code is executed under the following conditions:</p> <ul style="list-style-type: none"> <li>» After the <b>Download Script</b> button is clicked.</li> <li>» After the controller is initialized.</li> </ul> <p>For more information about the command codes, contact your GuardPoint10 vendor.</p>

## MultiSite Impact on the interface - Controller details

**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the controller details is as follows:

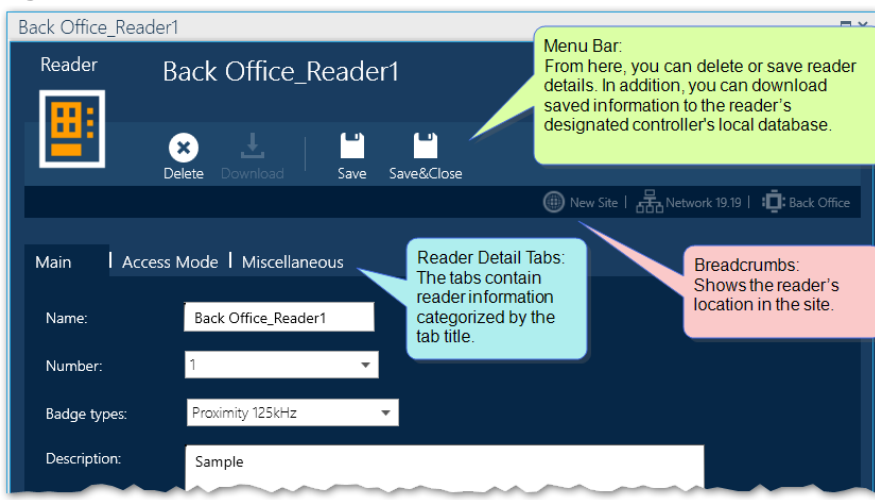
- » The **New** button has a drop-down list for **Reader**, **Input**, and **Relay**, where the owner of the new asset (reader, input, and relay) is selected.
- » An **Owner** field appears which identifies the site that has ownership of the controller. The owner has complete control of the controller.
- » A **Share With** field displays a list of sites where an operator in the controller's owner site can choose to share the input with other sites.

When a controller is shared, its ownership and its network ownership are automatically changed to the Root site. The previous owner is then a sharer of the controller and network.

- » An operator who does not have authorization in the owner site, but whose own site is a sharer of the controller will have read-only access to the controller's details.
- » An operator who does have authorization to the site that shares the controller can add (and own) a new asset (reader, input, and relay) as long as the number of assets already existing is not the maximum allowed by the controller.

# Reader Details

Figure A-7



A reader accepts credentials from cardholders, and usually sends the credential information (i.e. a number) to a controller. Credentials can come in many forms such as scanned badges, PIN codes, and scanned biometrics, depending on the type of reader installed.

If a reader is designated for a Lift controller (a controller for an elevator), the reader represents the elevator car. Each relay associated with the reader represents a floor where the elevator is authorized to stop. For more information about Lift setup, see "[Understanding the Lift Setup concept in GuardPoint10](#)" on page 53.

Each reader is defined in a detail area.

The top of the Reader Details includes the following:

» **Menu bar:**

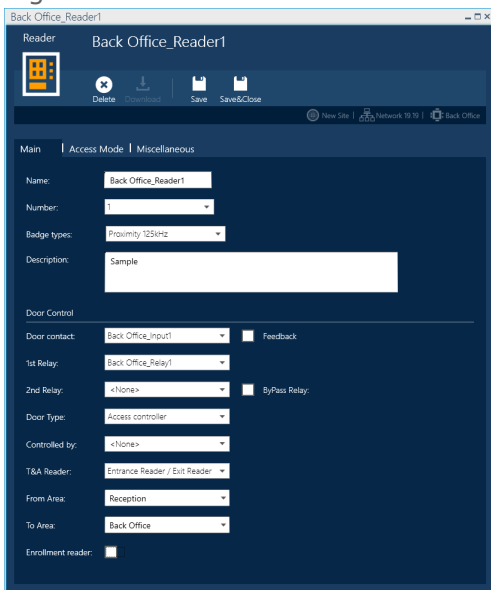
- **Delete:** Removes the reader's link to the controller. All data related to the reader is gone.
- **Download:** Sends the reader's information to the controller where it is saved.
- **Save:** Saves the reader's information in the system database.

» **Breadcrumbs:** A graphic representation of the reader's location on the site.

The rest of the dialog consists of four tabs. Each tab contains parameters affiliated with the tab title. The tabs and their parameter descriptions are as follows:

# Main Tab

Figure A-8



Main Tab Parameters

Parameter	Description
Name	<p>A free text field for naming the reader. The default device name for a new reader is "New Reader". Otherwise, the default name is &lt;controller name&gt;_Reader&lt;#&gt;.</p> <p>A best practice is to rename the reader to something that identifies the reader's location or purpose and allows you to quickly recognize the reader (i.e. "FrontEntrance01_Door01" or "FrontEntrance01_Door02").</p> <p>The name must be unique to the site, not just the network where the reader resides.</p>
API Key (may not be visible)	<p>A reader URI that an API can use to identify it.</p> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this field value.</p>



Parameter	Description
Has a Slave Reader (May not be visible)	<p><b>Note:</b> This parameter is only available when the controller, where the reader is connected, is an Access controller and not a Lift controller.</p> <p>In addition, the controller type must be able to support a slave reader.</p> <p>Select this checkbox when an additional reader is required but the controller cannot support it using conventional methods.</p> <p>When selected, a field appears that allows you to name the slave reader. After you name and save the slave reader, it will appear in the Reader table.</p> <p>If you open the slave reader's details you will notice that the slave reader is linked to the parameters of its master reader (where it was initially defined). The only parameters you will be able to change are:</p> <ul style="list-style-type: none"> <li>» Name</li> <li>» Description</li> <li>» Weekly Program</li> <li>» T&amp;A Reader (defaults to the opposite value of the parent reader, unless the parent is set to Entrance and Exit).</li> <li>» Access Group</li> </ul> <p>The <b>Number</b> assigned to the slave reader depends on the number assigned to its master reader. On the controller panel, if the master reader is connected to number <b>1</b> the slave reader is automatically connected to number <b>3</b>; and if the master reader is connected to number <b>2</b> the slave reader is automatically connected to number <b>4</b>.</p>
Number	<p>Drop-down shows the controller's available external connectors where the reader can be physically connected. The number of connectors varies between controller types. For more information about controller types and available connectors, see "<a href="#">Controller Support for Readers, Inputs, and Outputs</a>" on page 711.</p>

Parameter	Description
Badge Types	<p>A classification of a reader's scan options as determined by the recognition method or technology type(s) selected. There are four primary types:</p> <ul style="list-style-type: none"> <li>» <b>Proximity 125kHz:</b> Recognizes Proximity 125kHz badges and may include a keypad option (Default).</li> <li>» <b>Magnetic:</b> Recognizes magnetic badges and may include a keypad option.</li> <li>» <b>Biometric:</b> Recognizes unique physical characteristics (fingerprints or facial features) and may also include a badge scanner. When selected, a Biometric tab is added to the reader details' tab stack. For information about the Biometric tab, see <a href="#">"Biometric Tab" on page 459</a>.</li> </ul> <p>When <b>Biometric</b> is selected the reader only uses <b>Proximity 125kHz</b> technology and therefore displays <b>Biometric</b> and <b>Proximity 125kHz</b> as a recognized <b>Badge Types</b>. Also, the Miscellaneous tab's <b>Interface</b> and <b>Badge Format</b> values are read-only and automatically set to <b>Wiegand 8</b> digits and <b>Hexadecimal</b>. However, the first 2 digits of the biometric code must be <b>00</b>, and the maximum code value currently supported is <b>00FFFFFF</b>.</p> <ul style="list-style-type: none"> <li>» <b>License Plate Recognition:</b> Recognizes a scanned / photographed car license plate numbers.</li> </ul> <p>When the Main tab's <b>Badge Types</b> value is set to <b>License Plate Recognition</b>, the Miscellaneous tab's <b>Interface</b> and <b>Badge Format</b> values are read-only and automatically set to <b>Wiegand 8</b> digits and <b>Hexadecimal</b>.</p> <p>The plate number is recorded by the camera at an entrance, and then translated into an 8-digit Wiegand code. This code is sent to the reader's controller where it is treated like any other badge code.</p> <ul style="list-style-type: none"> <li>» <b>Smart Card 13.65 MHz:</b> Recognizes Smart Card badges and may include a keypad option.</li> <li>» <b>Variable Types (Type A...Type H):</b> Recognizes a type defined in the Options screen by an operator.</li> </ul>
Description	(Optional) A free text field where information about the reader is entered.
Door Contact	<p>The controller input device wired to the door open/close control device (door contact). An alarm is sounded when a door is forced or stays open beyond a predefined delay (<b>Door Alarm Delay</b>).</p> <p>For more information, see <a href="#">"Reader Details" on page 453</a>.</p>
Feedback	When selected, verifies the physical entry or exit point of a cardholder, which has been granted access, is used (i.e. after reading a badge and granting access, the door is actually opened).

Parameter	Description
1st Relay	<p>Activated when access is granted to open doors, gates, etc. Select the relay from the drop-down list. The list is specific to the controller connected to the reader. The relay activates during the <b>Door Open Time</b>.</p> <p>For more information, see <a href="#">"Reader Details"</a> on page 453.</p>
2nd Relay	<p>Activated by the same access granted event as the first relay (<b>1st Relay</b>). The relay stays active for the length of the <b>Door Open Time</b>, unless the <b>Bypass Relay</b> checkbox is selected.</p> <p>Select a secondary relay from the drop-down list. The list is specific to the controller connected to the reader.</p>
Bypass Relay (May not be visible)	<p>When selected, an access granted event will activate the <b>2nd Relay</b> for the length of the <b>Door Alarm Delay</b> instead of the length of the <b>Door Open Time</b>.</p> <p>Typically, the <b>Bypass Relay</b> is selected when an authorized employee must enter premises to switch off an alarm via a keypad.</p>

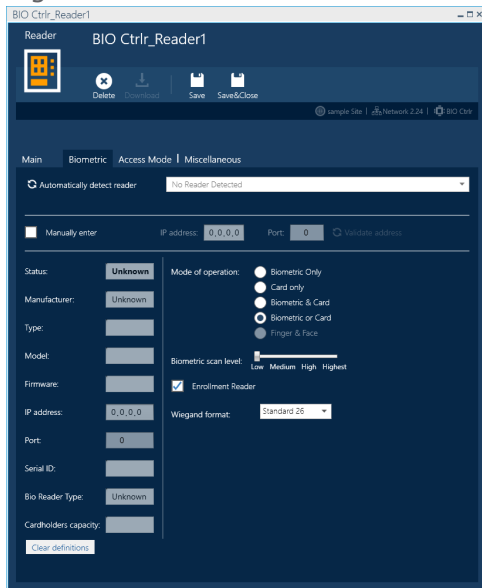
Parameter	Description
Door Type	<p>Where authorization is controlled. The control type options available from the drop-down list are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Access controller</b> (default): Access is granted if a badge is authorized or RTX is used.</li> <li>» <b>Controlled by input</b>: Disables the reader as long as the Logical state of the input selected in the <b>Controlled by</b> field is <b>ON</b>.</li> </ul> <p>An example of when you would use this <b>Door Type</b> would be for door interlocking, to control a clean room where dust or small particles may be a problem. Each door's reader is controlled by the other door's contact input. As a result, the reader of each door will be disabled when the opposite door is opened. A badge swipe event at a disabled reader is <i>not</i> recorded by the GuardPoint10 system.</p> <ul style="list-style-type: none"> <li>» <b>Mantrap Type 1</b>: A door is opened after access is granted via its reader or RTX button (the door status is given by the door contact defined for that door), a second access cannot be granted from the same reader until the opposite door is opened and then closed. This opposite door may be opened either through its reader (if it is located inside the mantrap) or with its RTX button.</li> <li>» <b>Mantrap Type 3</b>: A door is opened after access is granted via its reader or RTX button (the door status is given by the door contact defined for that door), a second access cannot be granted from the same reader until the opposite door is opened and then closed. After the initial door is closed, the opposite door is automatically opened.</li> <li>» <b>Mantrap Type 4</b>: A door is opened after access is granted via its reader or RTX button (the door status is given by the door contact defined for that door), a second access cannot be granted from the same reader until the opposite door is opened and then closed. This opposite door is opened automatically when a controller input is triggered (i.e. a laser tripwire is crossed as a cardholder approaches the opposite door. The controller input is selected from the <b>Controlled By</b> parameter below.</li> </ul> <p>For more information about mantraps and real time use of a mantraps, see <a href="#">"Managing a Mantrap" on page 69</a>.</p>
Controlled By (may not be visible)	Designates the specific input device that controls the authorization used in the <b>Door type</b> parameter for the opposite door.

Parameter	Description
T&A Reader	<p>Designates the reader's event including a timestamp (the time a badge swipe took place).</p> <p>This parameter is only relevant for the T&amp;A Roll Call screen and a Time &amp; Attendance report.</p> <p>For more information about Time &amp; Attendance, see <a href="#">"Time &amp; Attendance" on page 257</a>.</p> <p>The available values from the fields drop-down list are:</p> <ul style="list-style-type: none"> <li>» <b>Entrance Reader:</b> Designates a badge swipe as an entrance event. The event and timestamp are made available to Time &amp; Attendance.</li> <li>» <b>Exit Reader:</b> Designates a badge swipe as an exit event. The event and timestamp are made available to Time &amp; Attendance.</li> <li>» <b>Entrance Reader / Exit Reader:</b> Designates a badge swipe as a possible entrance or exit event. The event and timestamp are made available to Time &amp; Attendance. Time &amp; Attendance infers the badge swipe designation based on the previous badge swipe.</li> </ul> <p>This value may not be available in the drop-down list. For more information, see <a href="#">"Allow T&amp;A Readers to be 'Entrance &amp; Exit'" on page 578</a>.</p> <ul style="list-style-type: none"> <li>» <b>None:</b> The badge swipe event is potentially unavailable in Time &amp; Attendance.</li> </ul> <hr/> <p><b>Note:</b> If the reader's controller has a <b>Purpose</b> setting of <b>Lift</b>, the reader's <b>T&amp;A Reader</b> field is irrelevant.</p>
From Area	<p>The area where a cardholder swipes their badge to gain access to another area defined as the <b>To Area</b>.</p> <p>For information about the Area module, see <a href="#">"Area" on page 315</a>.</p>
To Area	<p>The destination area that a cardholder will access after swiping their badge in the <b>From Area</b>.</p> <p>For information about the Area module, see <a href="#">"Area" on page 315</a>.</p>
Enrollment reader	<p>When selected, the reader will have a second potential purpose besides a standard access verification point. The second purpose would be for enrolling a badge code via the <b>Get</b> button on the Badges screen and via the <b>Get</b> button in a cardholder details' General tab.</p> <p>A badge code enrolled via a cardholder details' <b>Get</b> button, discard any Multiple Access Group limitation to the enrollment reader where the badge code is swiped.</p>

## Biometric Tab

The Biometric tab is visible when the **Biometric** type is selected in the reader details' Main tab.

Figure A-9



Biometric Tab Parameters

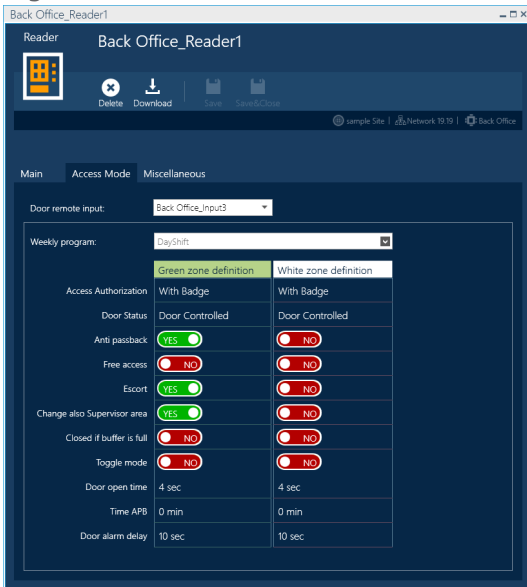
Parameter	Description
Automatically Detect Reader	When clicked, a search is performed on the LAN network for biometric readers. After the search is completed, the drop-down list to the right of the <b>Detect Reader</b> button is populated with the search results. The operator then selects the desired reader from the drop-down list.  Information about the selected reader automatically populates the fields below and to the left of drop-down list.
Manual Enter	An alternative to the Automatically Detect Reader search. It allows the user to enter the IP address and port number of a known biometric reader.
IP Address	The manually entered IP address of the selected biometric reader.
Port	The manually entered port number where the selected biometric reader is connected.
Validate Address (Button)	Relevant when a biometric reader's <b>IP Address</b> and <b>Port</b> is manually entered.  When clicked, it determines if the reader can send and receive data from the system. If successful, a green checkmark ✓ will appear. If not successful, a red "x" will appear.
Status (Read-Only)	The real-time connection status of a selected reader. The options are <b>Connected</b> and <b>Disconnected</b> .
Manufacturer (Read-Only)	The name of the manufacturer who produced the selected reader.

Parameter	Description
Type (Read-Only)	The type of reader detected.
Model (Read-Only)	The selected reader's model name or identification number determined by the reader's manufacturer.
Firmware (Read-Only)	The low-level software for the reader hardware.
IP Address (Read-Only)	The manually entered IP address of the selected biometric reader.
Port (Read-Only)	The manually entered port number where the selected biometric reader is connected.
Serial ID (Read-Only)	The unique identification number of the selected reader. The Serial ID is determined by the reader's manufacturer.
Bio Reader Type (Read-Only)	The components supported by the selected reader to identify a cardholder (i.e. Biometric scanner, badge scanner, or keypad). The <b>Mode of Operation</b> area will update to reflect supported components.
Cardholder Capacity (Read-Only)	The maximum number of cardholders that can be saved in the selected reader's local database.
Mode of Operation	Based on the components supported by the selected reader, the operator can select the component(s) that will be used by the reader to identify cardholders. For example, if the <b>Bio Reader Type</b> field shows <b>Biometric &amp; Card</b> , the operator may choose one of the following options to identify cardholders: <ul style="list-style-type: none"> <li>» Biometric only</li> <li>» Card only</li> <li>» Biometric &amp; Card</li> <li>» Biometric or Card</li> <li>» Finger &amp; Face (this option only enabled when the reader can scan fingerprints and faces)</li> </ul>
Biometric Scan Level	The degree of detail used to compare a scanned fingerprint or face to biometric samples stored in the system database.

Parameter	Description
Enrollment Reader	<p>When the checkbox is selected, the selected reader may be used to add biometric data to the system database where it can be downloaded to the local database of other biometric readers in the system.</p> <hr/> <p><b>Note:</b> The selected <b>Mode of Operation</b> is not relevant to the <b>Enrollment Reader</b> setting. For example, if the <b>Mode of Operation</b> is set to <b>Card Only</b>, the reader can still be used to enroll a cardholder's biometric data, as long as the reader's <b>Enrollment Reader</b> checkbox is selected.</p>
Wiegand Format	The structure of the data stored in an access control credential and recognized by the reader. Currently, there is support for Mifare 32 and Proximity 125kHz (Standard 26).
Clear Definitions (Button)	When clicked, all fields in the Biometric tab will empty.

## Access Mode Tab

Figure A-10





Parameter	Description
Door Remote Input	<p>Controller input device that is connected (wired) to the Request to Exit button (RTX). For example, a button at a receptionist's desk that unlocks the front door. In this example, the button on the desk is the RTX device.</p> <p>For more information about the RTX input devices, see <a href="#">"Default Connections for Inputs, Relays, and RTX" on page 712.</a></p> <hr/> <p><b>Note:</b> When an RTX input device is associated with an Event's Weekly Program (via the Event Handling Program/Alarms dialog), the RTX button is active and raises an alarm during the green periods of the Weekly Program. However, during the white periods of the Weekly Program, the RTX button doesn't open the door (and doesn't raise an alarm).</p>
Weekly Program	<hr/> <p><b>Note:</b> This parameter is not relevant for readers connected to a controller whose <b>Purpose</b> is set to <b>Lift</b>. Weekly Programs for readers connected to Lift controllers are set in the Access screen, see <a href="#">"Access Groups Screen" on page 506.</a></p> <hr/> <p>The Weekly Program (WP) assigned to a door's reader. The purpose of the reader's WP is to identify the green and white periods where the green and white columns in the tab will be applied.</p> <p>A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays and Special Days. WPs set periods of reader behavior during which different rules (green or white) are applied to the reader. These rules are based on the Green Zone Definition column and the White Zone Definition column found in the reader details' Access Mode tab.</p> <p>Select a WP for the reader via the drop-down arrow. A list of available WPs is displayed.</p> <div data-bbox="628 1348 724 1444" data-label="Image"> </div> <p>Figure A-11</p> <p>Choose a WP from the list, a graphic representation of the schedule appears to the right of the WP in focus. Click the <b>Select</b> button to associate the WP in focus with the reader.</p> <p>The default WP is <b>WP Always</b>. This allows a reader to operate in <b>Green Zone Definition</b> mode unless another WP is selected.</p> <p>For more information about WPs, see <a href="#">"Time Zones" on page 113.</a></p>

Parameter	Description
Green Zone Definition / White Zone Definition	<p>Identifies the access rules applicable to the two states of the Weekly Program.</p> <ul style="list-style-type: none"> <li>» <b>Green Zone Definition:</b> Rules to apply during the green period of the applicable Daily program.</li> <li>» <b>White Zone Definition:</b> Rules to apply during the white period of the applicable Daily program.</li> </ul> <p>The reader automatically selects its current <b>Zone Definition</b> based on the period set for that day in the Weekly Program associated with it.</p> <hr/> <p><b>Note:</b> The <b>Zone Definitions</b> that appear in the tab depends on the content of the Weekly Program selected.</p> <p>For example, if the selected Weekly Program is <b>WP Always</b>, only the <b>Green Zone Definition</b> column will appear in the tab. And, if the selected Weekly Program is <b>WP Never</b>, only <b>White Zone Definition</b> column will appear in the tab.</p> <p>If the selected Weekly Program has both green and white periods, both columns will appear in the tab.</p>
Access Authorization	<p>Method used to initiate access authorization. The option from the drop-down list are as follows:</p> <ul style="list-style-type: none"> <li>» <b>With Card</b> (Default option for badge reading only).</li> <li>» <b>With Keypad</b> (Just enter a PIN via a reader's keypad).</li> <li>» <b>With Card or Keypad</b></li> <li>» <b>With Card and Keypad</b> (The required option if duress codes will be allowed at the reader. For more about duress codes, see "<a href="#">PIN Code</a>" on <a href="#">page 610</a>).</li> </ul> <hr/> <p><b>Note:</b> This parameter must be assigned values for <b>Security Level 1</b> and <b>Security Level 2</b>.</p>

Parameter	Description
Door Status	<p>A door's status in relation to the security system. The status options available from the drop-down list are as follows:</p> <ul style="list-style-type: none"><li>» <b>Door Controlled:</b> Standard access mode, access depends on badge (and possibly PIN) authorizations.</li><li>» <b>Door Locked:</b> Access is denied while in this state, regardless of badge and possibly PIN authorizations.</li><li>» <b>Door Unlocked:</b> Access controls are not enforced (badge and/or PIN are irrelevant).</li></ul> <p><b>Note:</b> This parameter must be assigned values for <b>Security Level 1</b> and <b>Security Level 2</b>.</p>

Parameter	Description
Anti-passback	<p>(Also known as APB) Prevents the misuse of the access control system. It establishes a specific sequence in which a badge must be used for the system to grant access.</p> <p>Anti-passback is applicable on a controller that has two or four readers.</p> <p>When set to <b>Yes</b>, the cardholder cannot swipe their badge at the same reader again until they first swipe at a second reader <i>connected to the same controller</i>.</p> <div data-bbox="448 510 1471 976" style="background-color: #4a90e2; color: white; padding: 10px;"> <p><b>How anti-passback affects cardholders.</b></p> <p>An environment where a controller has two readers (Reader_1 and Reader_2) and Reader_1 has <b>Anti-passback</b> set to <b>Yes</b>, the following is required from the cardholder. A cardholder who swipes their badge at Reader_1 must swipe their badge at Reader_2 before they can swipe their badge at Reader_1 again.</p> <p>If Reader_1 has a <b>Time APB</b> value in addition to having <b>Anti-passback</b> set to <b>Yes</b>, a cardholder who swipes their badge at Reader_1 must <b>wait the specified time set in Time APB</b> before they can swipe their badge at Reader_1 again.</p> </div> <p>The system recognizes the following types of anti-passback events:</p> <ul style="list-style-type: none"> <li>» <b>Local Anti-passback:</b> The controller itself manages the event. It prevents a cardholder from accessing the premises after swiping the badge twice, in succession, at the same reader.</li> <li>» <b>Timed Anti-passback:</b> (Also called "lock out delay") Prevents a cardholder from accessing the premises after swiping their badge twice at the same reader within a predefined time frame. The time frame is defined in the "<b>Time APB</b>" on the facing page parameter. Timed Anti-passback is generally used in organizations where there is no provision for an exit reader connected to the same controller, and the security administrator wants to stop multiple badge swipes by a single badge in quick succession.</li> <li>» <b>Global Anti-passback:</b> Requires a cardholder to follow a predefined path to their target destination. (i.e. a cardholder may only pass from one predefined level to a second predefined level (Lobby to Cafeteria)).</li> </ul>
Free Access	<p>All badges in the reader's controller memory will have access, as long as access is available via one of the readers connected to the same controller, regardless of the escort setting, anti-passback setting, or the reader's WP.</p>
Escort	<p>When set to <b>Yes</b>, it places relevance to a cardholder's <b>Needs Escort</b> parameter and <b>Supervisor</b> parameter settings as they pertain to access events.</p> <p>For information about escort rules, see "<a href="#">Escort Rules for Access Events</a>" on page 697.</p>

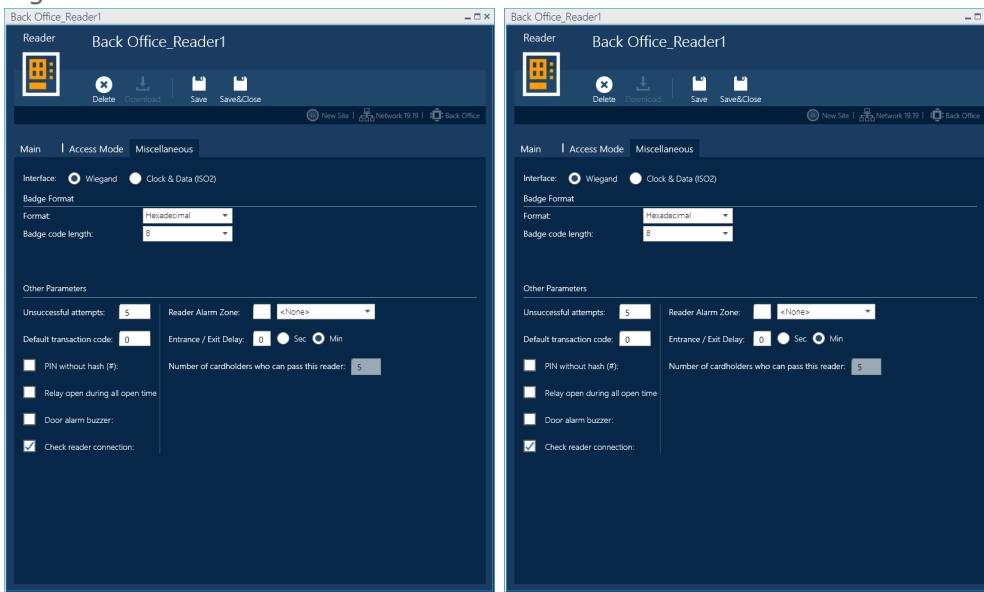
Parameter	Description
Change Also Supervisor Area	<p>When <b>Change also Supervisor area</b> is set to <b>Yes</b>:</p> <p>In case a Supervisor is acting as an escort for another cardholder at an Area door that is an entrance or exit to that Area the Supervisor as well as the cardholder will be recorded as entering or exiting the Area after both badges are swiped at the reader.</p> <p>When <b>Change also Supervisor area</b> is set to <b>No</b>, only the cardholder will be recorded as entering or exiting the Area After both badges are swiped.</p>
Closed if buffer is full	<p>When selected, and the controller's <b>Event Buffer</b><sup>1</sup> is full due to a communication failure with the PC, the reader refuses access to all cardholders. If this parameter is not selected, and the controller's event buffer is full, the event buffer operates as a <b>FIFO buffer</b><sup>2</sup>.</p> <p>After communication with the PC is re-established, the buffer can be cleared, via polling, and this parameter will no longer be relevant.</p>
Toggle Mode	<p>When selected, the reader changes the state of a relay after a valid badge swipe. The relay remains in the changed state until the next valid badge swipe.</p> <p>For example, the first cardholder at an office swipes their badge (or scan their biometric) like any other standard reader configuration to open the door. However, future cardholder access events will not require a badge swipe (or biometric scan). If they do a swipe, the relay will change the relay state again after the door closes.</p> <p>If the reader's Weekly Program period where the toggle is set to <b>Yes</b> ends and a Weekly Program period where Toggle is set to <b>No</b> begins, then the relay will reset to its normal state.</p>
Door open time	<p>The number of seconds allotted to a cardholder to pass through a doorway after receiving authorization. Corresponds to the activation delay of the relay that controls the door.</p> <p>Available values: 0-119 seconds</p>
Time APB	<p>The delay before a cardholder can receive authorization to swipe their badge at the same reader a second time in succession. For more information, see the "<a href="#">Anti-passback</a>" on the previous page.</p>
Door Alarm Delay	<p>The number of seconds that a door may remain open. If the door is still open after the <b>Door Alarm Delay</b> times out, a <b>Door Left Open</b> alarm is triggered.</p> <p>For this option to be enabled, the door's input must be in an armed Alarm Zone.</p> <p>Available values: 0-75 seconds, in 5 second intervals.</p>

<sup>1</sup>A temporary storage area in a controller. The buffer contains system events involving entities attached to the controller. An Event buffer is read and cleared by the system during polling (a query as to whether a controller has any data to transmit).

<sup>2</sup>A method of memory management for storing data that arrives at a controller (First In First Out). The oldest transactions are erased to make space for the newer transactions.

# Miscellaneous Tab

Figure A-12



## Miscellaneous Tab Parameters

Parameter	Description
<p>Interface (Group)</p>	<p><b>Note:</b> If the "License Plate Recognition: Recognizes a scanned / photographed car license plate numbers." on page 456 checkbox, found in the reader's Main tab in the Badge Types drop-down list, is selected, the Interface fields are automatically set and are read-only.</p> <p>These fields allow you to define a particular interface within the badge technology selected in the reader details' Main tab.</p> <p>The interfaces available are:</p> <ul style="list-style-type: none"> <li>» <b>Wiegand</b></li> <li>» <b>Clock &amp; Date (ISO2)</b></li> </ul> <p>The interface fields provide a way to customize the format to suit possible preexisting badges at a particular installation.</p> <p>The interface selected is applied to all readers connected to the same controller.</p>

Parameter	Description
Format (visible for Wiegand interface)	<p>Hexadecimal digits on Wiegand badges (default). If Decimal is selected, a <b>Customer Code Length</b> parameter appears.</p> <p>A best practice is to maintain a consistent reader format throughout your system.</p> <p>For more information about controller supported formats, contact GuardPoint10 technical support.</p> <hr/> <p><b>Note:</b> If you choose a different format for a reader, only badges enrolled at a reader with the same format will be recognized.</p>
Badge Code Length	<p>The number of digits in a badge code that is read by the system.</p> <p>Available values:</p> <p><b>Wiegand:</b> 8 (default), 10, 12</p> <p><b>Clock &amp; Data (ISO2):</b> 8 (default) - 12</p>
Badge Code Position (visible for Clock & Data (ISO2) interface)	<p>The system reads the first set of (8 - 12) characters recorded on the badge strip by default. However, this parameter allows you to choose a different set of characters by specifying the position of the first character in the set.</p> <p>Available values: 0 - 37, the default value 0 corresponds to the first encoded character</p>
Customer Code Position (visible for Clock & Data (ISO2) interface)	<p>The system reads the first set of (8 - 12) characters of a customer code by default. However, this parameter allows you to choose a different set of characters by specifying the position of the first character in the set.</p> <p>Available values: 0 - 37, the default value 0 corresponds to the first encoded character</p>
Customer Code Length (may not be visible)	<hr/> <p><b>Note:</b> Visible when the badge format is Wiegand-Decimal and Clock &amp; Data (ISO2).</p> <hr/> <p>Available values:</p> <ul style="list-style-type: none"> <li>» Wiegand, Decimal: 0, 3</li> <li>» Clock &amp; Data (ISO2): 0 - 8</li> </ul>
Customer Code Value (may not be visible)	<hr/> <p><b>Note:</b> Visible when the badge format is Wiegand-Decimal and Clock &amp; Data (ISO2).</p> <hr/> <p>Contains placeholders for the Custom code. The number of placeholders displayed depends on the <b>Customer Code Length</b> selected.</p> <p>If the <b>Custom Code Length</b> value is zero, there will be no placeholders.</p>

Parameter	Description
Other Parameters (Group)	The following parameters are outside the scope of the badge technology or format.
Unsuccessful Attempts	Specifies the number of successive unsuccessful attempts allowed by the system before displaying "Unsuccessful Attempts" in the Event Log screen. Available values: (00-99)
Default Transaction Code	Specifies the transaction code sent by the controller to the system when an access granted event occurs. For more information about transaction codes, see <a href="#">"Convention for Reader Transaction Codes" on page 710</a> .
PIN without hash (#)	This parameter is relevant when the reader is configured to check the PIN code. When selected, a cardholder will be granted access, if the reader is a keypad device and the cardholder enters a PIN without a hash "#" at the end.  <b>Note:</b> This option is supported on controller firmware versions 18/10/10 and later.
Relay open during all open times	In the Default setting (i.e. when this box is NOT selected), the controller deactivates the door relay as soon as the door sensor detects that the door has been opened. Selecting this option will leave the relay active during the <b>Door Open time</b> .  What does it mean in the real world when the checkbox is clear? After a cardholder swipes their badge and gains access (opens the door) to the relay is off and the door will lock after it is closed.  What does it mean in the real world when the checkbox is selected? After a cardholder swipes their badge and gains access (opens the door) the relay remains on for the duration of the <b>Door Open Time</b> value and the door will be unlocked regardless of its closed state.
Door alarm buzzer	When selected, the reader's buzzer sounds in the following scenarios:  <ul style="list-style-type: none"> <li>» When the door is opened without authorization. If the door is opened without authorization, the buzzer is activated immediately and a door alarm is raised in the system.</li> <li>» When the door remains open too long after a valid scan. If the door is opened after a valid scan and then remains open, the buzzer sounds in short intervals after 75% of the <b>Door Alarm Delay</b> time has passed, as an indicator that a door alarm is going to be raised. When the remaining 25 % of the <b>Door Alarm Delay</b> time has passed, a continuous 'beep' is sounded, indicating that a door alarm has been raised.</li> </ul> <b>Note:</b> In both scenarios, the buzzer stops when the door is closed.



Parameter	Description
Check reader connection	<p>Enables automatic report transactions if the reader is disconnected from the controller.</p> <hr/> <p><b>Note:</b> This feature is only supported on IC4000 controllers.</p>
F1 (may not be visible)	<p>Associates a transaction code with the reader's keypad F1 function key. This parameter is for readers equipped with a keypad and function keys F1/F2/F3. The <b>F1</b> field may be used to enter a transaction code, which is sent when access is granted to the cardholder and the [F1] function key is pressed.</p> <p>The <b>F1</b> fields are relevant to installations that include SENSOR customized controller firmware. Values for the <b>F1</b> fields will be provided by SENSOR to support the unique functionality requested.</p> <p>Standard controller firmware does not use the <b>F1</b> fields.</p>
Reader Alarm Zone	<p>Assigns an alarm zone to a reader. This means that the reader will be locked during times when the alarm zone is armed and will deny access to all cardholders, except for those cardholders defined as a <b>Supervisor</b>.</p> <p>For information about alarm zones, see <a href="#">"Alarm Zones (Setup)" on page 301</a> and <a href="#">"Alarm Zones (Security)" on page 365</a>.</p> <p>For information about making a cardholder a <b>Supervisor</b>, see <a href="#">"Supervisor" on page 615</a>.</p> <p>The <b>Reader Alarm Zone</b> includes a drop-down list containing all existing alarm zones that may be selected and assigned to the reader. The number to the left of the drop-down list displays a controller-specific internal number assigned to the selected alarm zone. The number is only relevant for readers that have a keypad. The number is not editable.</p> <p>If an alarm zone is disarmed, a cardholder may enter the number on the reader's keypad to change the state of the alarm zone from disarmed to armed. The change to an armed state automatically takes place only after a specified delay time has passed. This gives the cardholder time to exit the alarm zone before it is armed. The delay is defined in the <b>Entrance/Exit Delay</b> field of the reader detail's Miscellaneous tab.</p> <p>If an alarm zone is armed and a cardholder, <i>denoted as a supervisor</i>, swipes their badge at the reader, the zone is temporarily disarmed automatically for a predefined period. This provides the supervisor time to enter the zone and disarm it, via a reader with a keypad or a SENSOR controller inside the zone before it is reset to armed. This delay is defined in the <b>Entrance/Exit Delay</b> field of the reader's Miscellaneous tab.</p>

Parameter	Description
Entrance/Exit Delay	<p>Works with the <b>Reader Alarm Zone</b> setting. It specifies the time delay before a change to the arm/disarm state of a selected alarm zone will take place. <b>The Entrance/Exit Delay</b> setting applies when a cardholder with Supervisor initiates the Entrance or Exit at the reader.</p> <div data-bbox="450 376 1471 1070" style="background-color: #4F81BD; color: white; padding: 10px;"> <p><b>Scenarios where the Reader Alarm Zone fields and the Entrance/Exit Delay fields would work together</b></p> <p>Scenario 1: Change from armed to disarmed</p> <p>A cardholder (with supervisor status) is the first to arrive at the office. The office alarm is armed from the previous night. To disarm the alarm the cardholder swipes their badge at the front door and then rushes to the controller before the delay period has passed to enter the code that will disarm the alarm zone for the rest of the day (or until it is rearmed).</p> <p>Scenario 2: Change from disarmed to armed</p> <p>The last employee in the office has to lock up before they go home. After swiping their badge at the front door they enter a code on the reader's keypad. After entering the code the employee has a limited time to exit the premises before the alarm zone is armed for the night (or until a supervisor disarms it).</p> </div>
Number of cardholders... (may not be visible)	<p><b>Note:</b> An Options screen setting determines if this information is displayed.</p> <hr/> <p>Shows the number of cardholders downloaded to the reader.</p> <p>This field is primarily used for troubleshooting and is not necessary for normal infrastructure setup and maintenance.</p>

## MultiSite impact on the interface - Reader details



**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

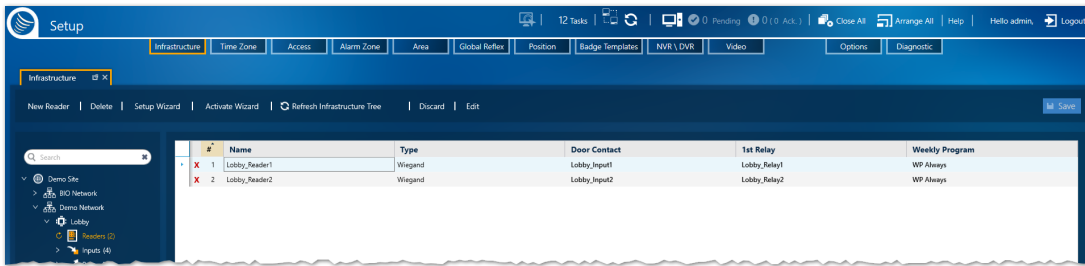
When MultiSite is set to **Yes** in the Options screen, the impact on the reader details is as follows:

- » An **Owner** field identifies the site that has ownership of the reader. The owner has complete control of the reader.
- » A **Share With** field displays a list of sites where an operator in the reader's owner site can choose to share the reader with another site.
- » An operator who does not have authorization in the owner site, but whose own site is a sharer of the reader will have read-only access to the reader's details.



# Reader Table

Figure A-13



A reader is an access control tool. It accepts credentials from cardholders, and usually sends the credential information (i.e. a number) to a controller. Credentials can come in many forms such as scanned badges, PIN codes, and scanned biometric characteristics, depending on the type of reader installed.

The table displays information for those readers connected to a common controller. The tree in the image above shows that the controller called "Lobby" has two readers. After "Readers (2)" in the infrastructure tree is put in focus, a table listing general details about each reader is displayed in the work area to the right of the tree.

Keep in mind that there are two possible configurations for a controller **Access** and **Lift**. Access refers to a controller connected to a reader that allows access via a door. Lift refers to a controller connected to a reader that allows access via a lift (elevator) to various floors in a building.

If a controller is configured for a lift, the reader connected to the controller represents the lift's passenger car and the reader's relays represent the floors that the lift may stop at to allow passengers on or off. For more information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10" on page 53.](#)

The Reader table column descriptions below are the same, regardless of the controller configuration (**Access** and **Lift**).

For information about table filters, see ["Table Filters" on page 695.](#)

Reader Table Parameters

Parameter	Description
Delete <b>X</b>	Removes the reader's link to the controller. All data related to the reader is removed from the system database and the controller's local database.
#	The connector number on the controller, where the reader is physically connected to the controller. The number of connectors varies according to controller type.
Name	The name of the reader.
Badge Types	A classification of a reader's scan options. The classification is set in the Type area of the reader's details and is determined by the technologies available to the reader (i.e. Proximity 125kHz, Magnetic, License Plate Recognition, Biometric, etc.).

Parameter	Description
Door Contact	<p>The contact that signals the opening of the door.</p> <p><b>Note:</b> If an alarm controller that works exclusively with monitors (such as IC1604 or IC2000 Alarm) is selected, GuardPoint10 displays the following message: "Alarm monitoring controller without readers !"</p>
1st Relay	<p>The name of the relay used for door activity. A reader may have more than one relay.</p> <p>Click <b>Edit</b> in the action bar for secondary relay options.</p>
Weekly Program	<p>The Weekly Program (WP) assigned to a reader. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays and Special Days. WPs set periods a behavior for the reader (green or white). For more information about WPs, see "<a href="#">Weekly Program Time Zones</a>" on page 120. For information about behavior settings for readers, see "<a href="#">Reader Details</a>" on page 453.</p>

## MultiSite impact on the interface - Reader table



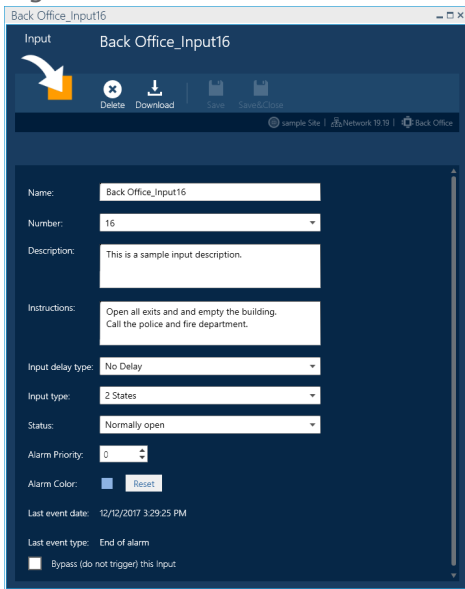
**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the Reader table is as follows:

- » An operator who does not have authorization in the owner site, but whose own site is a sharer of the reader will have read-only access to the Reader table. A user will not be able to edit or delete a reader that they do not own.
- » An operator who does have authorization to the site that shares the controller of the displayed Reader table can add (and own) a new reader as long as the number of readers already existing is not the maximum allowed by the controller or the license.

# Input Device Details

Figure A-14



An input is an electrical connection point that may be connected to external sensors or detectors to sense external events (i.e. Door contacts, Door remote control (called 'Request-to-Exit' or 'RTX'), Motion detectors, Passive infra-red, etc.). Inputs are usually used for alarm management.

The following describes the information found in an input's details.

Table A-1 Input Device Parameters

Parameter	Description
Name	<p>A free text field that identifies the input device. The default name is "&lt;Controller name&gt;_Input_&lt;#&gt;".</p> <p>A best practice is to rename the input device to something that identifies the input's location, type, or purpose.</p> <p>The new name must be unique.</p>
API Key (may not be visible)	<p>An input URI that an API can use to identify it.</p> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this field value.</p>
Number	<p>The connector number on the controller, where the input device's wires are physically connected. The number of connectors varies according to controller type. For more information about controller types and available connectors, see "<a href="#">Default Connections for Inputs, Relays, and RTX</a>" on page 712.</p>
Description	<p>(Optional) A free text field where information about the input device is entered.</p>

Parameter	Description
Instruction	<p>A free text field where information intended to deal with an alarm triggered from the input would appear on an Alarm card. An Alarm card may appear in the Display Event screen or the Security Center screen. For information about the Display Event screen, see <a href="#">"Security Center Screen" on page 680</a>. For information about the Display Event screen, see <a href="#">"Display Events Screen" on page 657</a>.</p>
Input Delay Type	<p>An alarm and input device interaction. The available options from the drop-down list are:</p> <ul style="list-style-type: none"> <li>» <b>No Delay</b>: An alarm is raised as soon as the input device is activated.</li> <li>» <b>After... (if on alarm)</b>: If the input device is still activated, an alarm will be raised after a specified number of seconds.</li> <li>» <b>After... (even if no more under alarm)</b>: Even if the input device is no longer activated, an alarm will be raised after a specified number of seconds.</li> </ul> <hr/> <p><b>Note:</b> If the input is connected to a reader / door, the <b>Input Delay Type</b> field will be disabled.</p>
Duration Period (visible when input is delayed)	<p>The number of seconds an alarm is delayed in relation to when the input device is triggered.</p> <p>Default: 2 seconds</p>
Input Type	<p>The states that may be detected by the input device. The available types from the drop-down list is as follows:</p> <ul style="list-style-type: none"> <li>» <b>2 States</b>: The two possible states of the sensor/detector connected to the input device (i.e. opened or closed).</li> <li>» <b>4 States</b> (also known as "supervised"): In addition to the 2 States mentioned above, the input device also detects the status of the line that connects the sensor/detector to the input device. The detected line statuses are: <ul style="list-style-type: none"> <li>» <b>Line_cut</b>: Tampering issue.</li> <li>» <b>Line_short</b>: Electrical issue.</li> </ul> </li> </ul> <hr/> <p><b>Note:</b> A 2 State input device cannot be defined as a 4 State input device. However, if the line does not have to be supervised, a 4 State input may be redefined as a 2 State input. Consult your controller documentation to determine which types of input states are available (see the <a href="#">"Controller Comparison Tables" on page 705</a>).</p>

Parameter	Description
Status	<p>An alarm sounds when the input device is armed and the expected status of the input is changed. The available expected status types from the drop-down list is as follows:</p> <ul style="list-style-type: none"> <li>» <b>Normally open:</b> The input device will raise an alarm, if, while armed, its status changes from <b>open</b> to <b>closed</b>.</li> <li>» <b>Normally closed:</b> The input device will raise an alarm, if, while armed, its status changes from <b>closed</b> to <b>open</b>.</li> </ul>
Alarm Priority	By assigning a priority (0 - 255) to an input's alarm, an operator can sort alarms that appear in the Security Center screen's Alarm list. For information about the Alarm list, see <a href="#">"Security Center Screen" on page 680</a> .
Alarm Color	<p>The selected text color of the alarm triggered by the input in the Event log. This color will override the default alarm color set in the Options &gt;Event Log screen (<b>Start of Alarm, Start of Alarm Delayed, End of Alarm</b>).</p> <p>The <b>Reset</b> button, alongside the color picker, will return the alarm text color to the Options &gt; Event Log default.</p>
Last Event Date	Shows the time and date of the last physical event on the input device. This refers to the <b>Physical State</b> value (i.e. open, closed). For more information, see <a href="#">"Input Device Table" on page 480</a> .
Last Event Type	Shows the last physical event type that took place on this input device. For more information, see <a href="#">"Input Device Table" on page 480</a> and refer to the <a href="#">"Input Type" on the previous page</a> column value.
Bypass	<p>When selected, transactions sent by the input device are ignored by the system. For example, if a change to the expected status of the input is detected, the input will send an alarm transaction. However, the transaction will be ignored by the system and the event won't appear in the log.</p> <p>This field also exists in the <a href="#">"Input Device Table" on page 480</a>. These fields are linked. If marked as bypassed in one table, it will automatically be marked as bypassed in the other table.</p>

## MultiSite impact on the interface - Input details



**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the input details is as follows:

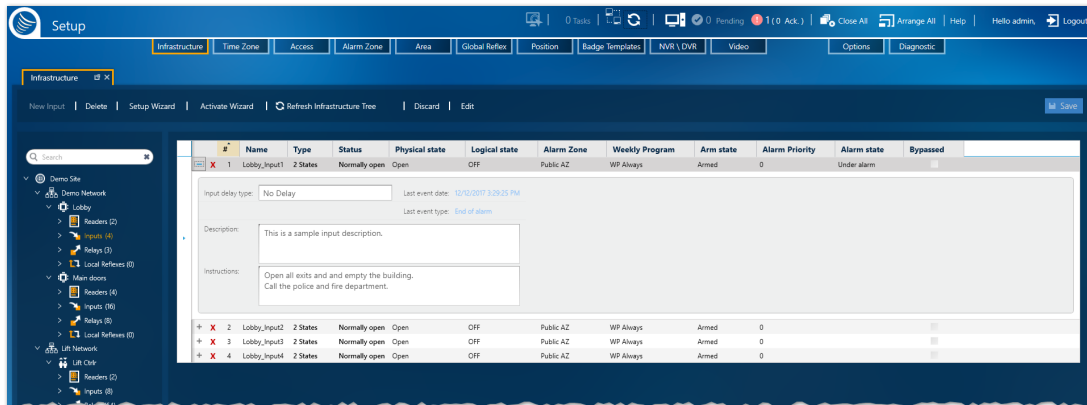
- » An **Owner** field identifies the site that has ownership of the input. The owner has complete control of the input.
- » A **Share With** field displays a list of sites where an operator in the input's owner site can choose to share the input with another site.



- » An operator who does not have authorization to the owner site, but whose own site is a sharer of the input will have read-only access to the input's details.

# Input Device Table

Figure A-15



An input is an electrical connection point that may be connected to external sensors or detectors to sense external events (i.e. Door contacts, Door remote control (called 'Request-to-Exit' or 'RTX'), Motion detectors, Passive infra-red, etc.). Inputs are usually used for alarm management.

The table only displays input device information for those devices connected to a common controller. For example, the tree in the image above shows that the controller called "Lobby" has four inputs. After "Inputs (4)" is put in focus, a table listing general details about each input device is displayed in the work area to the right of the tree. A description of each column in the table is provided below.

The second table below describes the parameters visible when an input row is expanded.

For information about table filters, see ["Table Filters" on page 695](#).

To expand an Input table row, click . To collapse a row, click . These icons appear to the left of the input device name in each row.

Table A-2 Input Device Table Column Parameters

Parameter	Description
Delete	Removes the input's link to the controller. All data related to the input is removed from the system database and the controller. This operation requires an operator to confirm the delete action.
#	The connector number on the controller, where the input device's wires are physically connected. The number of connectors varies according to controller type. For more information about controller types and available connectors, see <a href="#">"Controller Support for Readers, Inputs, and Outputs" on page 711</a> .
Name	The unique name of an input device.

Parameter	Description
Type	<p>The states that may be detected by the input device. The available types from the drop-down list are as follows:</p> <ul style="list-style-type: none"> <li>» <b>2 States</b>: The two possible states of the sensor/detector connected to the input device (i.e. opened or closed).</li> <li>» <b>4 States</b> (also known as "supervised"): In addition to the 2 States mentioned above, the input device also detects the status of the line that connects the sensor/detector to the input device. The detected line statuses are as follows: <ul style="list-style-type: none"> <li>» <b>Line_cut</b>: Tampering issue.</li> <li>» <b>Line_short</b>: Electrical issue.</li> </ul> </li> </ul> <hr/> <p><b>Note:</b> A 2 State input device cannot be defined as a 4 State input device. However, if the line does not have to be supervised, a 4 State input may be redefined as a 2 State input. Consult your controller documentation to determine which types of input states are available (see the "<a href="#">Controller Comparison Tables</a>" on page 705).</p>
Status	<p>The expected status of the input. The available status types from the drop-down list are as follows:</p> <ul style="list-style-type: none"> <li>» <b>NO (Normally Open)</b>: The input device will raise an alarm, if, while armed, its status changes from <b>open</b> to <b>closed</b>.</li> <li>» <b>NC (Normally Closed)</b>: The input device will raise an alarm, if, while armed, its status changes from <b>closed</b> to <b>open</b>.</li> </ul>
Physical State	<p>The current state of the input. The possible statuses are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Open</b></li> <li>» <b>Closed</b></li> </ul>
Logical State	<p>If there is a conflict between the <b>Status</b> status and the <b>Physical State</b>, the <b>Logical State</b> will be <b>ON</b>. Otherwise, the Logical state will be <b>OFF</b>.</p> <div style="background-color: #4F81BD; color: white; padding: 10px; border-radius: 5px;"> <p><b>What this means:</b></p> <p>If an input is configured as normally closed and for some reason its current physical state is open, the logical state will be <b>ON</b>. If the input is armed while its logical state is <b>ON</b>, an alarm will be triggered.</p> <p>If the <b>Status</b> status and the <b>Physical State</b> do not conflict, the <b>Logical State</b> will be <b>OFF</b> and an alarm will not be triggered.</p> </div>

Parameter	Description
Alarm Zone	<p>Input devices may be grouped into zones called <b>Alarm Zones</b>. An alarm zone may be armed or disarmed, either automatically, by attributing a Weekly Program, or manually (through an override action).</p> <p>When an alarm zone is armed, all the alarm input devices belonging to that alarm zone are also armed.</p> <p>When an alarm zone is disarmed the input devices belonging to that alarm zone are also disarmed.</p> <p>For more information about alarm zones, see <a href="#">"Alarm Zones (Setup)" on page 301</a>.</p>
Weekly Program	<p>The Weekly Program (WP) assigned to an input device via an alarm zone. For information about alarm zones, see <a href="#">"Alarm Zones (Setup)" on page 301</a>.</p> <p>A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for holidays. WPs set periods of acceptability, during which time, different groups of cardholders may enter. For more information about WPs, see <a href="#">"Time Zones" on page 113</a>.</p>
Arm State	<p>The input device's current state (arms or disarms). You can apply a manual override to the state via the Alarm Zone Security screen, see <a href="#">"Alarm Zone Security Screen for GuardPoint10 Alarm Zones" on page 662</a>.</p> <p>When armed, and the expected status of the input device changes (see the <b>Logical State</b> above) the input device triggers an alarm and sends an alarm transaction to the system.</p> <hr/> <p><b>Note:</b> This manual <b>Arm/Disarm</b> setting takes priority over an input device's associated Alarm Zones Weekly Program.</p>
Alarm Priority	<p>A priority (0 - 255) that allows an operator to sort alarms that appear in the Security Center screen's Alarm list. For information about the Alarm list, see <a href="#">"Security Center Screen" on page 680</a>.</p>
Alarm State	<p>If an input's alarm is triggered, it may have one of the following three states:</p> <ul style="list-style-type: none"> <li>» <b>Under alarm:</b> The alarm has not been addressed yet.</li> <li>» <b>Acknowledged:</b> The alarm has been acknowledged (see <a href="#">"Dashboard" on page 333</a> and <a href="#">"Addressing Alarms via a Security Center Icon" on page 391</a>).</li> <li>» <b>Confirmed:</b> After acknowledging the alarm, it is confirmed (see <a href="#">"Dashboard" on page 333</a> and <a href="#">"Addressing Alarms via a Security Center Icon" on page 391</a>).</li> </ul> <p>If an input is disarmed after an alarm is triggered, the <b>Alarm State</b> will still display the current state of the alarm.</p>

Parameter	Description
Bypassed	<p>When selected, transactions sent by the input device are ignored by the system. For example, if an input's logical state is <b>ON</b>, the input will send an alarm transaction. However, the transaction will be ignored by the system and the event won't appear in the Event log.</p> <p><b>Note:</b> This field also exists in the <a href="#">"Alarm Zone Setup Screen" on page 521</a>. These fields are linked. If marked as bypassed in one table, it will automatically be marked as bypassed in the other table.</p>

Table A-3 Input Device Table Expanded Row Parameters

Parameter	Description
Input delay type	<p>An alarm and input device interaction. The available option from the drop-down list are:</p> <ul style="list-style-type: none"> <li>» <b>No Delay:</b> If an input is armed while its <b>Logical State</b> is <b>ON</b>, an alarm will immediately trigger.</li> <li>» <b>After... (if on alarm):</b> If an input is armed while its <b>Logical State</b> is <b>ON</b>, an alarm will trigger after a specified number of seconds.</li> <li>» <b>After... (even if no more under alarm):</b> If an input is armed while its <b>Logical State</b> is <b>ON</b>, an alarm will trigger after a specified number of seconds, even if the <b>Alarm State</b> value is no longer <b>Under Alarm</b> (i.e. Acknowledged or Confirmed). For information about Acknowledged and Confirmed operations, see <a href="#">"Dashboard" on page 333</a> and <a href="#">"Addressing Alarms via a Security Center Icon" on page 391</a>.</li> </ul>
Duration Period (visible when input is delayed)	<p>The number of seconds an alarm is delayed in relation to the input device trigger time.</p> <p>Default: 2 seconds.</p>
Last Event Date	Shows the time and date of the last physical event on the input device. This refers to the <b>Physical State</b> value.
Last Event Type	Shows the last physical event type that took place on this input device. Refer to the <a href="#">"Type " on page 481</a> column values describes previously in this table.
Description	<p>(Optional) A free text field where information about the input device is visible.</p> <p>The description is recorded in an Input's details.</p>
Instructions	<p>A free text field that contains the protocol for a triggered alarm. When an alarm is raised, this instructional text will appear in a virtual badge on the Events screen (see <a href="#">"Display Events Screen" on page 353</a>).</p> <p>An example of an instruction would be, "Lockdown all elevators and building exits. Send a security team to the alarm zone where the event took place".</p> <p>The instruction is recorded in an Input's details.</p>

## MultiSite impact on the interface - Input table



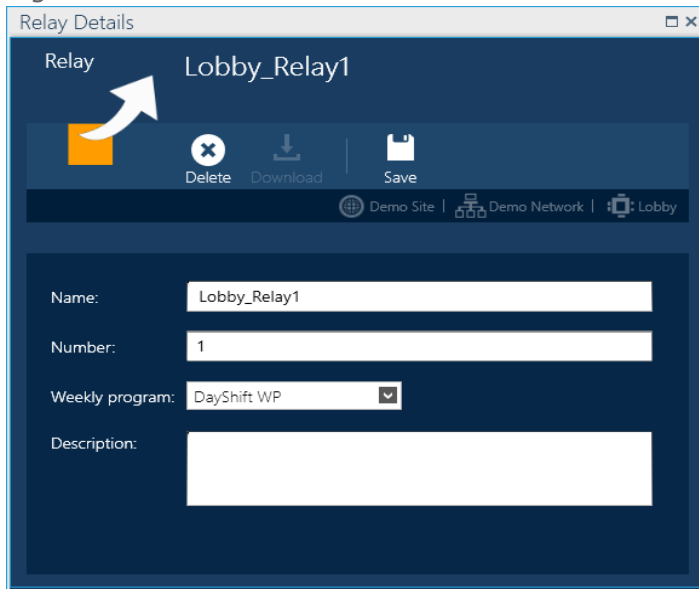
**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the Input table is as follows:

- » An operator who does not have authorization in the owner site, but whose own site is a sharer of the input will have read-only access to the Input table. A user will not be able to edit or delete an input that they do not own.
- » An operator who has authorization in a site shares the controller of the displayed Input table, can add (and own) a new input as long as the number of inputs already existing is not the maximum allowed by the controller.

# Relay Details

Figure A-16



Door Access Groups relays activate external devices. (door locks, audible signals, indicator lights, etc.).

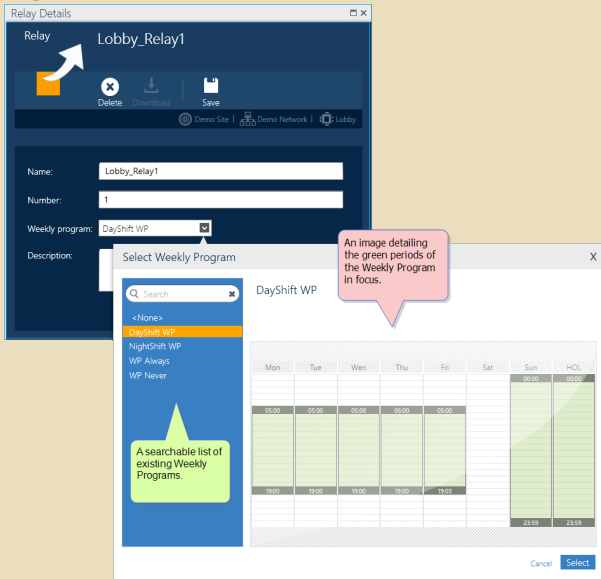
If the relay is part of a Lift Access Group, relays enable/disable floor button on a lift panel. For more information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10" on page 53](#).

For more information about the different types of access groups, see ["Access" on page 139](#) and ["Access Groups" on page 140](#).

The following describes the information found in a relay's details.

### Relay Parameters

Parameter	Description
Name	<p>A free text field that identifies the relay. The default name is "New Relay".</p> <p>A best practice is to rename the relay to something that identifies the relay's location or purpose.</p> <p>The relay name must be unique.</p>
API Key (may not be visible)	<p>A relay URI that an API can use to identify it.</p> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this field value.</p>
Number	<p>The connector number on the controller where the relay wires are physically connected. The number of connectors varies according to controller type.</p> <p>For more information about controller types and available connectors, see <a href="#">"Default Connections for Inputs, Relays, and RTX" on page 712</a>.</p>

Parameter	Description
<p>Weekly Program</p>	<p>The Weekly Program (WP) assigned to a relay that <i>is not connected to a reader</i>. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for holidays. A WP sets periods where a relay is activated/deactivated.</p> <p>You cannot add or change the WP of a relay if it's connected to a reader.</p> <p>For more information about WPs, see "<a href="#">Weekly Program Time Zones</a>" on <a href="#">page 120</a>.</p> <p>Select a WP for the relay from the drop-down arrow. A list of available WPs is displayed.</p> <p><b>Figure A-17</b></p>  <p>Choose a WP from the list, a graphic representation of the schedule appears to the right of the WP in focus. Click the <b>Select</b> button to associate the WP in focus with the relay.</p> <p>The default WP is <b>None</b></p> <div data-bbox="427 1420 1469 1816" style="background-color: #4F81BD; color: white; padding: 10px;"> <p><b>Scenario where a relay with a WP would be used</b></p> <p>People want free access to the office kitchen. The GuardPoint10 system does not have to know when cardholders enter or exit the kitchen, but the kitchen door should still be locked at night.</p> <p>GuardPoint10 installation personnel would install just a relay without a reader and give the relay a WP with a green period of 9:00 to 17:00 (assumed working hours). Before 9:00 and after 17:00 the kitchen door will be locked.</p> </div>
<p>Description</p>	<p>(Optional) A free text field where information about the relay is entered.</p>



## MultiSite impact on the interface - Relay details



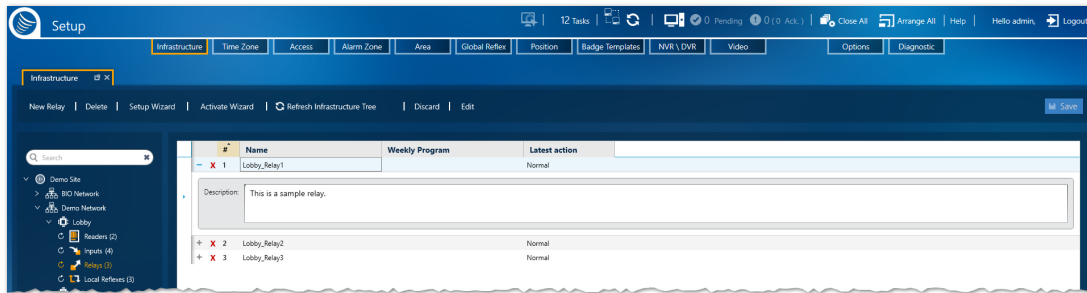
**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the relay details is as follows:

- » An **Owner** field identifies the site that has ownership of the relay. The owner has complete control of the relay.
- » A **Share With** field displays a list of sites where an operator in the relay's owner site can choose to share the relay with another site.
- » An operator who does not have authorization in the owner site, but whose own site is a sharer of the relay will have read-only access to the relay's details.

# Relays Table

Figure A-18



Relays activate external devices. (door locks, audible signals, indicator lights, etc.).

In a Lift Access Group, relays are used to enable/disable floor buttons in a lift's panel, this provides control over where the lift can stop based on the cardholder's authorization. A reader, in a lift controller environment, is used to identify the lift (elevator) car itself and not access. For more information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10" on page 53](#).

For more information about different types of access groups, see ["Access" on page 139](#) and ["Access Groups" on page 140](#).

The Relay table only displays relay information for those relays connected to a common controller. The tree in the image above shows that the controller called "Lobby" has three relays. After "Relays (3)" is put in focus, a table listing general details about each relay is displayed in the work area to the right of the tree.

For information about table filters, see ["Table Filters" on page 695](#).

A description of each column in the table is provided below.

To expand a relay table row, click . To collapse a row, click . These icons are to the left of the relay device number in each row.

Table A-4 Relay Table Column Parameters

Parameter	Description
Delete	Removes the relay's link to the controller. All data related to the relay is removed from the system database and the controller's local database. This operation requires an operator to confirm the delete action.
Open details button	Displays the relay's details. For information about a relay's details, see <a href="#">"Relay Details" on page 485</a> .
#	The connector number on the controller where the relay wires are physically connected. The number of connectors varies according to controller types.  For more information about controller types and available connectors, see <a href="#">"Default Connections for Inputs, Relays, and RTX" on page 712</a>
Name	The unique name of a relay.

Parameter	Description
Weekly Program	<p>The Weekly Program (WP) assigned to a relay. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for holidays. WPs set periods of acceptability during which different groups of workers may enter.</p> <p>For more information about WPs, see <a href="#">"Weekly Program Time Zones" on page 120</a>.</p>
Latest Action	<p>When the normal setting (Status) has been altered by an action, process, or an alarm zone's automatic operation, this column contains information about the action that was most recently performed. Otherwise, it reads <b>Normal</b>.</p>
Description	<p><b>Note:</b> Visible only after a row is expanded.</p> <p>(Optional) A free text field where information about the relay is entered.</p>

## MultiSite impact on the interface - Relay table



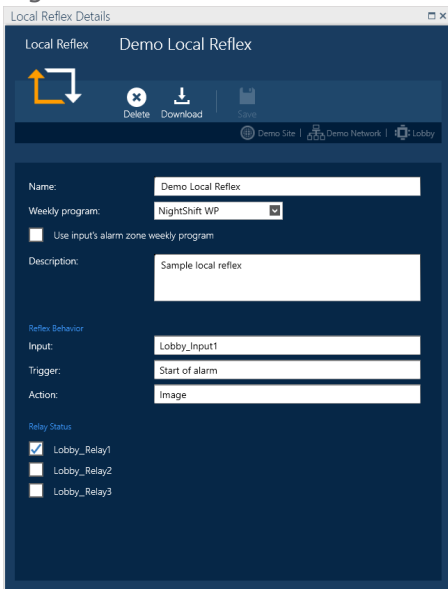
**Note:** You may not have the MultiSite module in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the module.

When MultiSite is set to **Yes** in the Options screen, the impact on the Relay table is as follows:

- » An operator who does not have authorization in the owner site, but whose own site is a sharer of the relay will have read-only access to the relay's details. A user will not be able to edit or delete a relay that they do not own.
- » An operator, who does have authorization to the site that shares the controller of the displayed Relay table, can add (and own) a new relay as long as the number of relays already existing is not the maximum allowed by the controller.

# Local Reflex Details

Figure A-19



A local reflex is the activation of one or more relays triggered by a status change of an input connected to the same controller.

The following describes the information found in a local reflex's details.

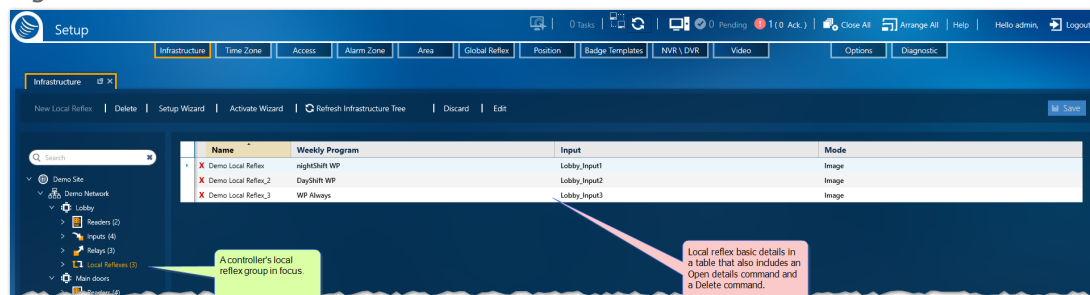
Table A-5 Local Reflex Parameters

Parameter	Description
Name	<p>A free text field that identifies the local reflex. The default name is "New Local Reflex".</p> <p>A best practice is to rename the local reflex to something that identifies the local reflex's location or purpose.</p> <p>The name must be unique.</p>
API Key (may not be visible)	<p>A local reflex URI that an API can use to identify it.</p> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this field value.</p>
Weekly Program (may not be visible)	<hr/> <p><b>Note:</b> If the <b>Use input's alarm zones weekly program</b> checkbox is selected, this parameter is not visible.</p> <hr/> <p>The Weekly Program assigned to the local reflex, unless the weekly program is inherited from the specified input's alarm zone's Weekly Program.</p>
Use input's alarm zone's weekly program	<p>When selected, the alarm zone's Weekly Program assigned to the input, which is specified in the <b>Reflex Behavior group</b>, governs the local reflex.</p>

Parameter	Description
Description	(Optional) A free text field where information about the local reflex is entered.
Reflex Behavior	The title of a group of parameters.
Input	The input where the trigger for the local reflex originates.
Trigger	<p>The event that must occur via the selected input for the reflex to start. The available triggers are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Start of alarm</b></li> <li>» <b>End of alarm</b></li> <li>» <b>Line cut</b></li> <li>» <b>Line short</b></li> <li>» <b>Input open</b></li> <li>» <b>Input close</b></li> <li>» <b>Any state</b></li> </ul>
Relay Mode	<p>The action started by the local reflex. The available actions are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Image:</b> When the input is activated, the relay(s) are activated. When the input is deactivated, the relay(s) are deactivated.</li> <li>» <b>Always Activated:</b> When the input(s) is activated, the relay(s) are activated and stay activated, even if the input(s) are deactivated. The relay(s) must be deactivated manually (see "<a href="#">Alarm Zone Security Screen for GuardPoint10 Alarm Zones</a>" on page 662).</li> <li>» <b>Activate During a Specific Time:</b> When the input is activated, the relay(s) are activated for a predefined duration.</li> <li>» <b>Toggle:</b> When the input is activated, the relay switches states (or toggles) from activated to deactivated or deactivated to activated. The toggle occurs each time the input is activated.</li> </ul> <p>If the relay's Weekly Program period where the toggle is set to <b>Yes</b> ends and a Weekly Program period where Toggle is set to <b>No</b> begins, then the relay will reset to its normal state.</p>
Duration Time (may not be visible)	<hr/> <p><b>Note:</b> Visible only if Activate During a Specific Time is selected in <b>Action</b>.</p> <hr/> <p>Applies the specified time to the action selected.</p> <p>Available values for Activate During a Specific Time: 1 – 120 sec.</p>
Relay Status	When a relay's checkbox is selected, the relay will trigger the local reflex after it is activated.

# Local Reflex Table

Figure A-20



A local reflex is the activation of one or more relays triggered by a status change of an input connected to the same controller.

The table only displays information for those local reflexes connected to a common controller. The tree in the image above shows that the controller called "Lobby" has three local reflexes. After "Local Reflex (3)" is put in focus, a table listing general details about each local reflex is displayed in the work area to the right of the tree. A description of each column in the table is provided below.

For information about table filters, see **"Table Filters" on page 695**.

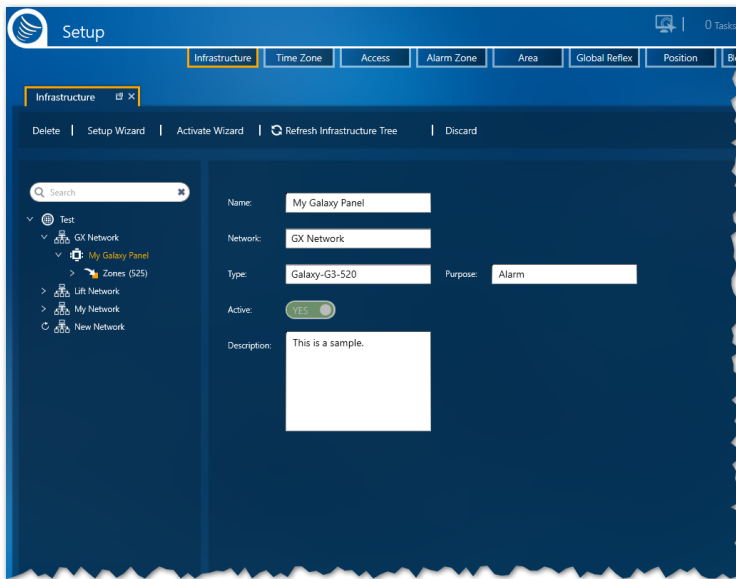
Table A-6 Local Reflex Table Column Parameters

Parameter	Description
Open details / Delete commands	The <b>Open details</b> button opens a local reflex's details. and the Delete icon (✘) removes the local reflex from the system database and the controller's local database.
Name	The unique name assigned to a local reflex.
Weekly Program	The Weekly Program assigned to a local reflex or the Weekly Program assigned to the alarm zone, where the local reflex's input is assigned.
Input	The name of the input that will trigger the local reflex.

Parameter	Description
Mode	<p>The action started after the local reflex is triggered. The actions available are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Image:</b> When the input is activated, the relay(s) are activated. When the input is deactivated, the relay(s) are deactivated at the same time.</li> <li>» <b>Always Activated:</b> When the input(s) is activated, the relay(s) are activated and stay activated, even if the input(s) are deactivated. The relay(s) must be deactivated manually (see "<a href="#">Alarm Zone Security Screen for GuardPoint10 Alarm Zones</a>" on page 662).</li> <li>» <b>Activate During a Specific Time:</b> When the input is activated, the relay(s) are activated for a predefined duration.</li> <li>» <b>Toggle:</b> When the input is activated, the relay switches states (or toggles) from activated to deactivated or deactivated to activated. The toggle occurs each time the input is activated.</li> </ul> <p>If the Weekly Program period where the toggle is set to <b>Yes</b> ends and a Weekly Program period where Toggle is set to <b>No</b> begins, then the relay will reset to its normal state.</p>

# Galaxy Panel Details

Figure A-21



A Galaxy panel is a microprocessor-based circuit board from Honeywell. The panel monitors and manages various kinds of alarms and alarm detectors (i.e. fire, intruder, etc.).

A Galaxy network can only have one Galaxy panel. Though multiple Galaxy networks may be added to the GuardPoint10 infrastructure.



**Note:** This document only covers Galaxy information as it pertains to GuardPoint10. The reader of this topic is assumed to have knowledge of the Galaxy system.

The following describes the information found in a Galaxy panel's details.

### Panel Parameters

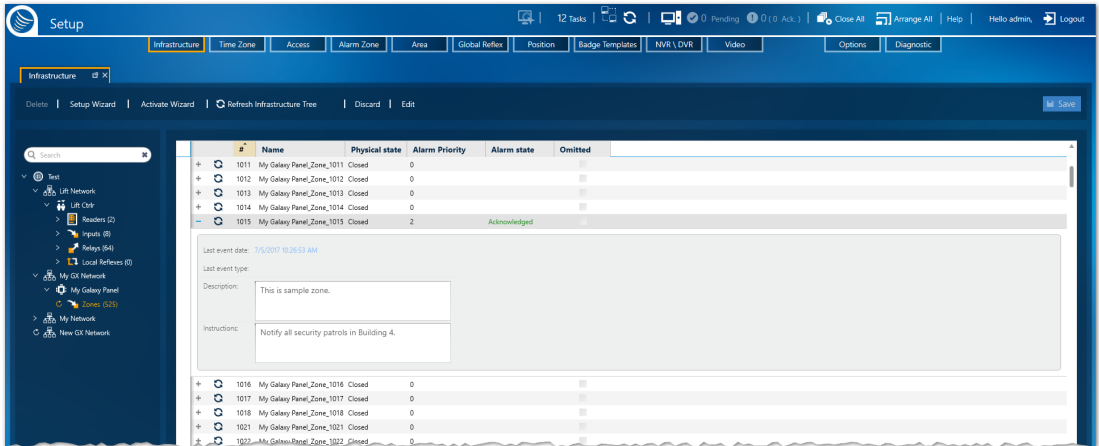
Parameter	Description
Name	<p>A free text field that identifies the Galaxy panel. The default name is "New Galaxy Panel".</p> <p>A best practice is to rename the panel to something that identifies a panel's location or purpose and allows you to recognize the panel (i.e. "Warehouse 4" or "Showrooms").</p> <p>The new name must be unique to the site. No other panel or controller can have the same name.</p>
API Key (may not be visible)	<p>A Galaxy panel URI that an API can use to identify it.</p> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this field value.</p>



Parameter	Description
Also Rename Groups and Zones (Only visible when renaming an existing panel)	<p>When selected, Galaxy groups and zones connected to the panel are renamed to their default name with the new panel name incorporated.</p> <p><b>Note:</b> If a group or zone has a custom name, the name will be overwritten with the new default name that includes the name of the panel.</p>
Network	The name of the Galaxy network where the panel will be located.
Type	<p>The type of panel that is being added to the Galaxy network. GuardPoint10 supports multiple types of Galaxy panels. To select a panel type, for a new panel integration, click on the field, and select the type from the drop-down list.</p> <p>After a new panel integration is saved, the <b>Type</b> value is fixed and cannot be changed.</p>
Purpose	The plan or environment of the panel. This will always be <b>Alarm</b> .
Active	<p>If set to <b>Yes</b>, the panel has established communication with GuardPoint10.</p> <p>If set to <b>No</b>, the panel gathers data locally, but GuardPoint10 does not poll the Galaxy system panel to provide the data to GuardPoint10.</p>
Description	(Optional) A free text field where information about the panel is entered.

# Galaxy Zone Table

Figure A-22



A Galaxy zone is the equivalent of an GuardPoint10 input. A zone is an electrical connection point that may be connected to external sensors or detectors to sense external events (i.e. Smoke detectors, Window contacts, Motion detectors, Passive infra-red, etc.). Galaxy zones are usually used for alarm management.

There are five special zones in all Galaxy system types. These zones are called *tamper zones*. A tamper zone monitors panel operations and the box containing the panel (i.e. Open panel box, Low battery, and Power failure). A tamper zone's physical state cannot be requested via GuardPoint10. A tamper zone cannot be omitted or disarmed from GuardPoint10.

The Zone table only displays zone information for those devices connected to a zone in the common Galaxy panel. The first five physical connection point (numbered 1 - 5) are connected to the tamper zone.

The first table below describes the content of each column in the Zone table.

The second table describes the parameters visible when a zone's row is expanded.

For information about table filters, see **"Table Filters" on page 695**.

To expand a zone table row, click . To collapse a row, click . These icons appear in the first column of the table.

Table A-7 Zone Table Column Parameters

Column	Description
Refresh	Refreshes the data provided by the Galaxy panel.
#	The connector number on the panel, where the zone device's wires are physically connected. The number of connectors varies according to the Galaxy panel type.

Column	Description
Name	<p>The unique name of a zone. These names are automatically generated by GuardPoint10. The names may be edited at any time.</p> <hr/> <p><b>Note:</b> The zone names displayed in the Zone table are not the same names displayed in the Galaxy panel keypad.</p>
Physical State	<p>The current state of a zone. The possible statuses are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Open</b></li> <li>» <b>Closed</b></li> </ul> <hr/> <p><b>Note:</b> A tamper zone's physical state is not visible in the Zone table.</p>
Alarm Priority	<p>A priority (0 - 255) that allows an operator to manage and display an alarm based on severity (i.e. sort alarms in the table or on the Security Center screen's Alarm list). For information about the Alarm list, see "<a href="#">Security Center Screen</a>" on page 680.</p>
Alarm State	<p>If a zone's alarm is triggered, it may have one of the following three states:</p> <ul style="list-style-type: none"> <li>» <b>Under alarm:</b> The alarm has not been addressed yet.</li> <li>» <b>Acknowledged:</b> The alarm has been acknowledged (see "<a href="#">Dashboard</a>" on page 333 and "<a href="#">Addressing Alarms via a Security Center Icon</a>" on page 391).</li> <li>» <b>Confirmed:</b> After acknowledging the alarm, it is confirmed to remove the under alarm state (see "<a href="#">Dashboard</a>" on page 333 and "<a href="#">Addressing Alarms via a Security Center Icon</a>" on page 391).</li> </ul>
Omitted	<p>When selected, transactions sent by the zone device are ignored by GuardPoint10. For example, if a zone's physical state is <b>ON</b>, the zone will send an alarm transaction to GuardPoint10. However, the transaction will be ignored by GuardPoint10 as well as the Galaxy panel, and the event will not appear on the screen.</p> <hr/> <p><b>Note:</b> <b>Omit</b> is disabled for tamper zones.</p>

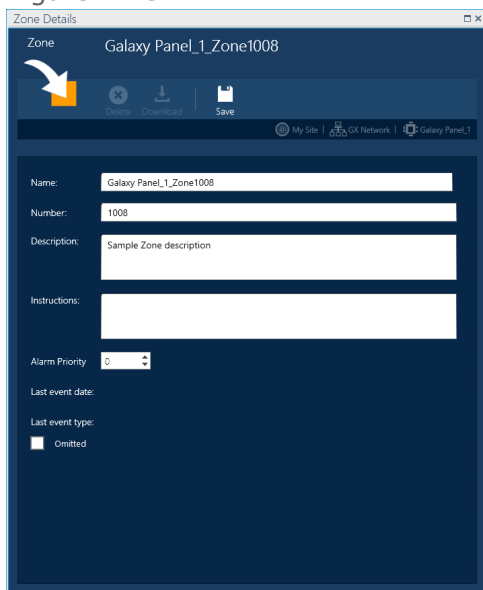
Table A-8 Zone Table Expanded Row Parameters

Parameter	Description
Last Event Date	Shows the time and date of the last physical event on the zone's device. This refers to the <b>Physical State</b> value.
Last Event Type	Shows the last physical event type that took place on this zone's device. Refer to the " <a href="#">Physical State</a> " above column values describes previously in this table.

Parameter	Description
Description	<p>(Optional) A free text field where information about the zone is visible. The description is recorded in a zone's details.</p>
Instructions	<p>A free text field that contains the protocol for the triggered alarm. When a zone is under alarm, this instructional text will appear in a card on the Display Events screen (see "<a href="#">Display Events Screen</a>" on page 353) and other places where the card may appear.</p> <p>An example of an instruction would be, "Lockdown all elevators and building exits. Send a security team to the Galaxy zone device, where the event took place".</p> <p>The instruction is recorded in a zone's details.</p>

# Zone Details

Figure A-23



**Note:** This topic assumes that a Galaxy panel has been integrated into your GuardPoint10 system.

A Galaxy zone is equivalent to an GuardPoint10 input. It is an electrical connection point in a Galaxy panel that may be connected to external sensors or detectors to sense events (i.e. motion detectors, smoke detectors, passive infra-red, etc.).

The following describes the information found in a zone's details.

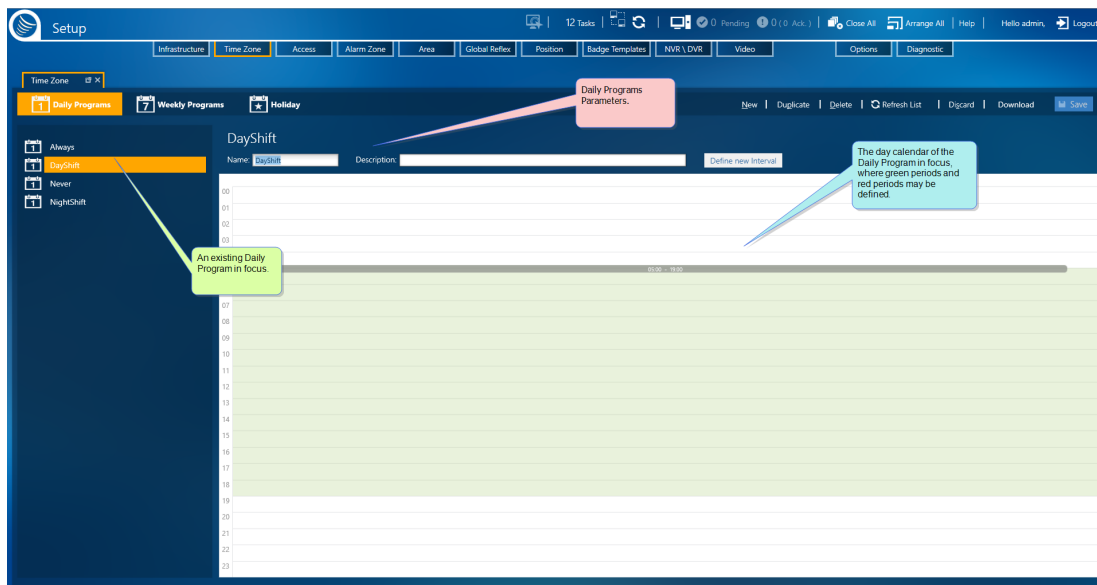
Table A-9 Zone Parameters

Parameter	Description
Name	<p>A free text field that identifies the input device. The default name is "&lt;Controller name&gt;_Input_&lt;#&gt;".</p> <p>A best practice is to rename the input device to something that identifies the input's location, type, or purpose.</p> <p>The new name must be unique.</p>
Number	<p>The connector number on the controller, where the input device's wires are physically connected. The number of connectors varies according to controller type. For more information about controller types and available connectors, see <a href="#">"Default Connections for Inputs, Relays, and RTX" on page 712</a>.</p>
Description	<p>(Optional) A free text field where information about the input device is entered.</p>

Parameter	Description
Instruction	A free text field where information intended to deal with an alarm triggered from the zone would appear on an Alarm card. An Alarm card may appear in the Display Event screen or the Security Center screen. For information about the Display Event screen, see <a href="#">"Security Center Screen" on page 680</a> . For information about the Display Event screen, see <a href="#">"Display Events Screen" on page 657</a> .
Alarm Priority	By assigning a priority (0 - 255) to a zone's alarm, an operator can sort alarms that appear in the Security Center screen's Alarm list. For information about the Alarm list, see <a href="#">"Security Center Screen" on page 680</a> .
Last Event Date	Shows the time and date of the last physical event relevant to the zone. This refers to the <b>Physical State</b> value (i.e. open, closed). For more information, see <a href="#">"Galaxy Zone Table" on page 496</a> .
Last Event Type	Shows the last physical event type that took place in this zone. For more information, see <a href="#">"Input Device Table" on page 480</a> .
Omitted (checkbox)	When selected, an alarm is broadcast from the zone but ignored by the Galaxy system and GuardPoint10. The Omit setting in Galaxy is equivalent to the Bypass setting in GuardPoint10.

# Time Zone Daily Program

Figure A-24



A Daily Program is a 24-hour segment of time during which a set of green and white periods exist. Up to four green periods can exist in one Daily Program. A Daily Program is used to build Weekly Programs (WPs). A Weekly Program uses up to 10 instances of a Daily Program (7 weekdays, Holidays, and two Special days) to set access rules for cardholders, entities, and devices.

The system supports a maximum of 255 Daily Programs.

A Daily Program can have multiple green periods and each period can be adjusted from within the graphic display. The maximum number of green periods per Daily Program is set in the Options screen's General tab.

The Daily Program screen contains three main areas:

- » On the left side of the screen is a list of operator-built and built-in Daily Programs. There are two built-in Daily Programs. The built-in Daily Programs cannot be edited or deleted.
  - » **Always:** The Daily Program's entire 24-hour period is green.
  - » **Never:** The Daily Program's entire 24-hour period is white (there are no green periods).
- » To the right of the list are the Daily Program parameters. The parameters are as follows:

Table A-10 Daily Program Parameters

Parameter	Description
Name	<p>A free text field that identifies the Daily Program. The default name is "New Daily Program".</p> <p>A best practice is to rename the Daily Program to something that identifies the target audience for the program. The name should make Daily Program selection intuitive to an operator who is building a WP.</p> <p>The name must be unique.</p>

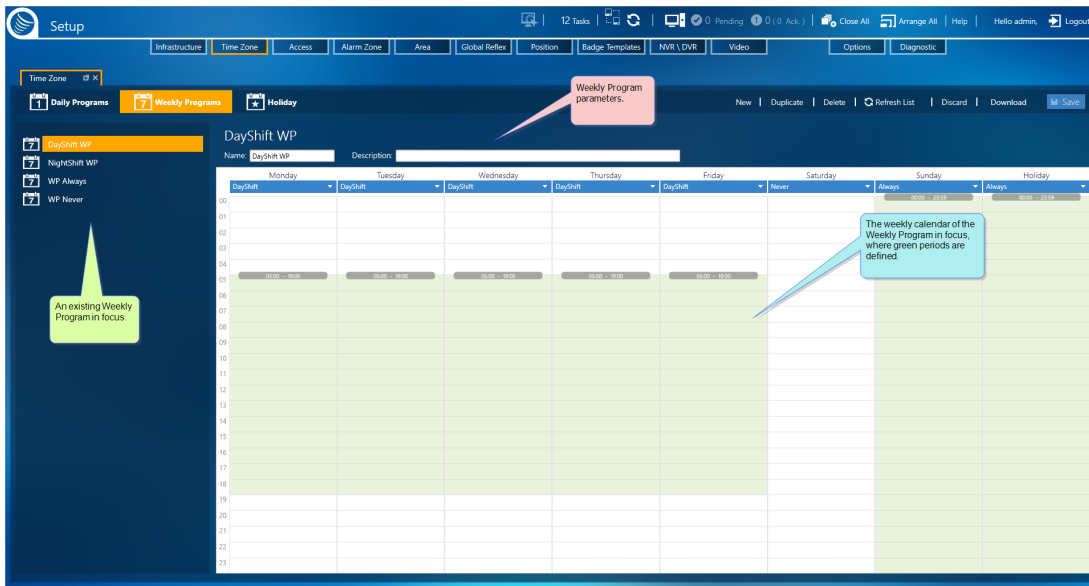
Parameter	Description
Description	(Optional) A free text field where information about the Daily Program is entered.

- » Below the Daily Program parameters is a graphic display illustrating the green and white periods assigned to a 24-hour period. A period of time that is not colored green, is, by definition, categorized as white.



# Time Zone Weekly Program

Figure A-25



A Weekly Program (WP) consists of seven days plus one Holiday and two additional Special days. The availability of Holidays and Special days is dependent on your system's settings (see "Use Special Days" on page 568).

Holidays and Special days are defined as exceptions to the green and white periods based on yearly calendar *dates* and not the *day* of the week.

The system can support a maximum of 127 WPs.

The WP screen contains three main areas:

- » On the left side of the screen is a list of operator-built and built-in WPs. The two built-in WPs cannot be edited or deleted. The two built-in WPs are as follows:
  - » WP Always: The WP's entire calendar is green.
  - » WP Never: The WP's entire calendar is white (there are no green periods).
- » To the right of the list are the parameters of the WP in focus. The parameters are as follows:

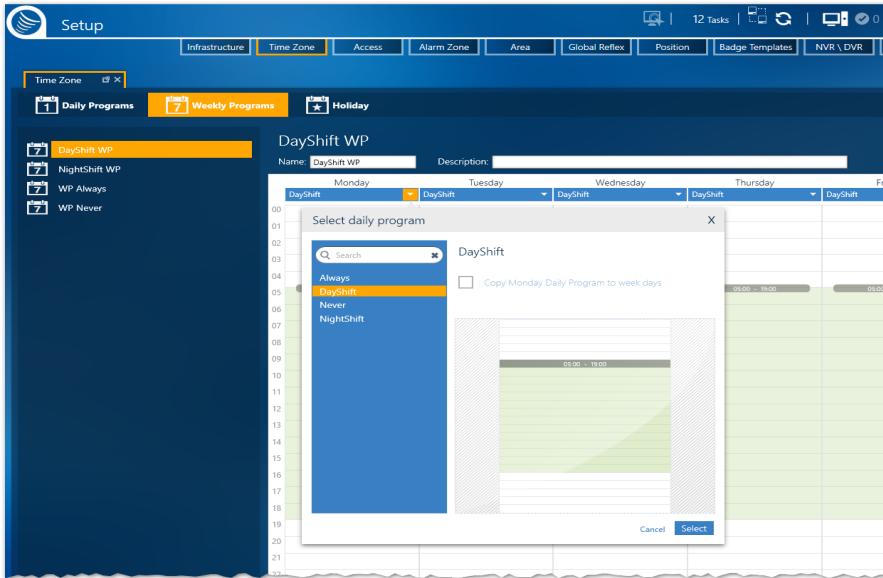
**Table A-11** Weekly Program Parameters

Parameter	Description
Name	<p>A free text field that identifies the WP. The default name is "New Weekly Program".</p> <p>A best practice is to rename the WP to something that identifies the target audience for the program.</p> <p>The name must be unique.</p>
Description	<p>(Optional) A free text field where information (i.e. who or what is the intended target of the WP) is entered.</p>

- » Below the WP parameters is an image illustrating the green and white Daily Program periods assigned to the WP calendar. A period of time that is not colored green, is, by definition, a white period.

At the top of each column in the image is the name of the day of the week. Below the name of the day is the name of the Weekly Program assigned to that day. The Weekly Program is selected via the down arrow next to the Weekly Program name.

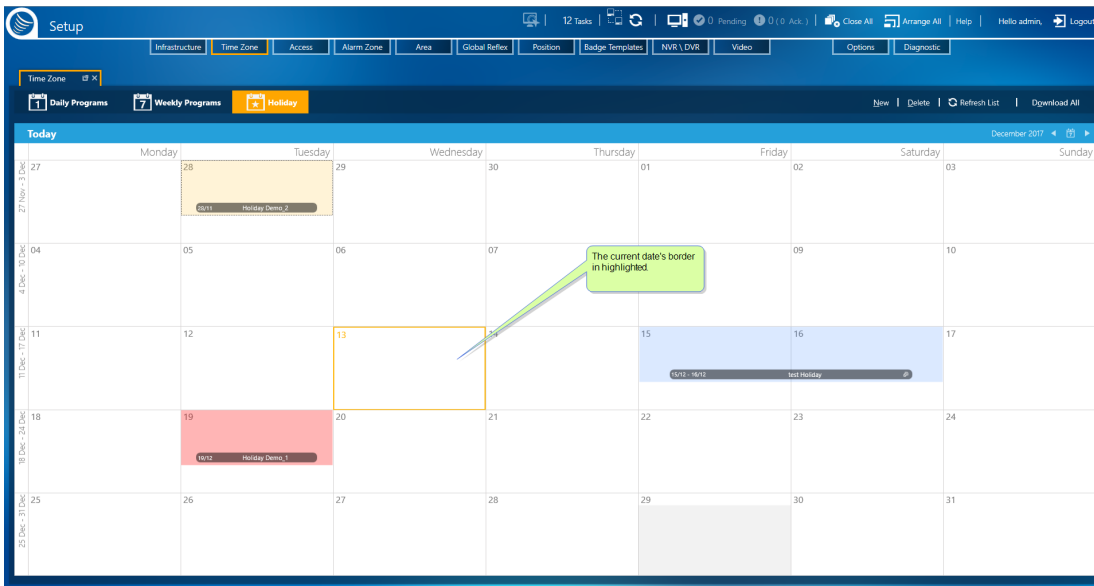
Figure A-26



**Note:** The first column in the image is the first day of the workweek selected in the Options screen.

# Time Zone Holidays & Special Days

Figure A-27



The Holidays and Special Days screen is a monthly calendar where dates can be designated as exceptions to any day in a WPs standard seven day week. A Holiday/Special Day can be applied to one day in the calendar or consecutive dates in the calendar.

The system can support a maximum of:

- » 60 Holidays
- » 60 Special Days 1s
- » 60 Special Day 2s

A total of 180 Holidays & Special Days.

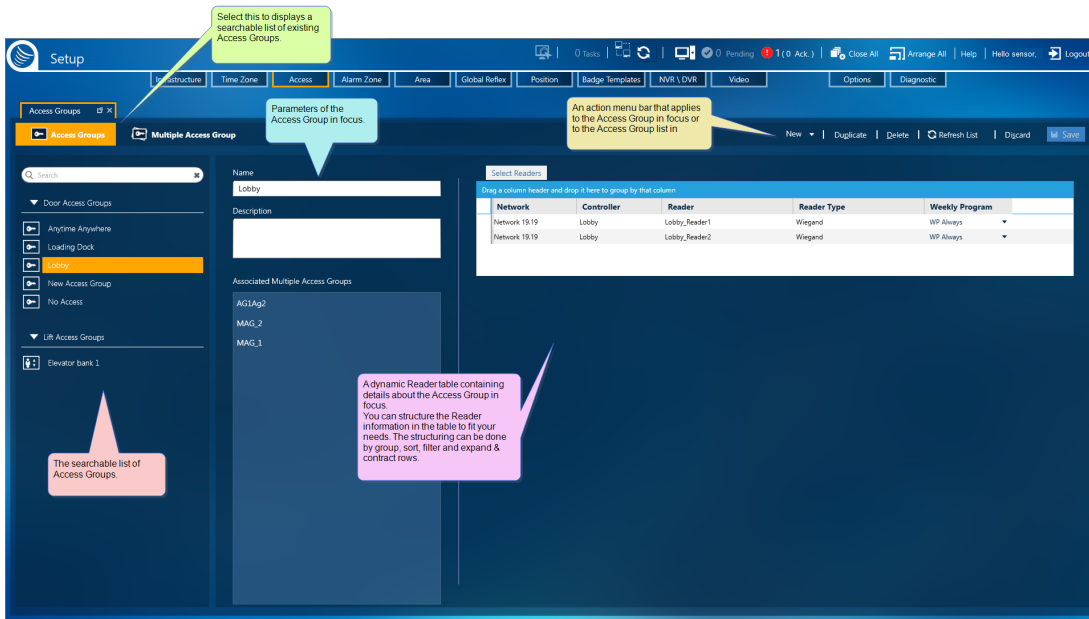
In the calendar, Holidays and Special Days are color-coded as follows:

- » Holidays are **violet**
- » Special Days 1s are **beige**
- » Special Days 2s are **pink**

Each date in the calendar can hold one Holiday or Special Day.

# Access Groups Screen

Figure A-28



There are two types of Access Groups on the Access Groups screen:

- » **Door Access Group:** This type of group includes most all doorways that allow cardholders to go from one location to another.
- » **Lift Access Group:** This type of group is designated for lift (elevator) doors. It allows cardholders to go into an elevator passenger car and choose an authorized destination floor. For more information about Lift setup, see "[Understanding the Lift Setup concept in GuardPoint10](#)" on [page 53](#).

Access Groups determine which doors or elevators are accessible, via reader device, to a cardholder during a cardholder's Weekly Program (WP) green period.

From a technical standpoint, an Access Group determines the badge codes that will be saved in a controller. For example, a cardholder assigned an Access Group, which includes Controller1\_Reader1, will have the cardholder's badge code save in Controller1's local database.

The Access Groups screen includes four distinct areas:

## A list of existing Access Groups

The area contains two show/hide lists of built-in and user-defined Access Groups. The lists are labeled **Door Access Groups** and **Lift Access Groups**. To see the content of one of these lists click the arrow preceding the list label name.

Select an Access Group from a list to see the group's parameters and other details specific to the group in focus.

If the **Lift Access Groups** is empty, the list label will not appear on the screen.

## An Access Group action bar

From the action bar, you can add/edit/delete operator-defined groups or group information. Any changes saved in the Access Groups screen are automatically attached to any previously associated cardholder via its Multiple Access Group.

## Access Group parameters

Contains basic information about the Access Group in focus.

If the **Anytime Anywhere** or the **No Access** group is in focus, the parameters displayed will be read-only. The **Anytime Anywhere** and **No Access** groups are built into the system.

- » **Anytime Anywhere:** Allows access to all spaces at all times except for lifts (elevators).
- » **No Access:** Denies access to all spaces at all times.

## MultiSite Impact

When **MultiSite** is set to **Yes**:

- » **Anytime Anywhere:** Available only to super users. It applies access authorization to all spaces at all times for all sites (except for elevators).
- » **Prefixed Anytime Anywhere:** Each site in the system has its own **Anytime Anywhere** access group and is prefixed with the name of the site. It allows access to all spaces at all times within the site.

Table A-12 Access Group Parameters

Parameter	Description
Name	<p>A free text field that identifies the Access Group. The default name is "New Access Group".</p> <p>A best practice is to rename the Access Group to something that identifies the group's purpose.</p> <p>The new name must be unique.</p>
Description	<p>(Optional) A free text field where information about the Access Group is entered.</p> <p>If an Access Group will be used in a cardholder's "<a href="#">Personal Door Access Groups</a>" on page 613 list, and there is a desire to color code the Access Group name in the list, enter the following code in the Access Group's description:</p> <pre>{"Type": "SAP2AC", "Color": "blue" }</pre> <p>You can substitute an HTML Color Codes (i.e. <b>#2424ff</b>) instead of the word <b>blue</b> in the code.</p>

Parameter	Description
Associated Multiple Access Groups	<p>Lists the Multiple Access Groups where the Access Group in focus is a member. An Access Group can be the only member of a Multiple Access Group or it can be one of many members of a Multiple Access Group.</p> <p>An Access Group can be a member of more than one Multiple Access Group or, be a member of no Multiple Access Group.</p> <p>An Access Group (Lift or Door) may be assigned to a cardholder without being the Access Group being in a Multiple Access Group</p>

## Dynamic Access Group Reader table

Contains information about readers associated with the Access Group in focus. For quicker analysis, you can restructure and filter the information in the table to narrow the range of information displayed.

For information about table filters, see **"Table Filters" on page 695**.

The **Select** button above the table allows you to add or delete a reader from the Door Access Group table and add or delete relays from the Lift Access Group table.

Drag a column heading into the **Group By** bar to Group Access Group data and help you show a subset of data you want to analyze. For example, in a Door Access Group table, you may want to group an unwieldy list of access group readers by networks and controllers.

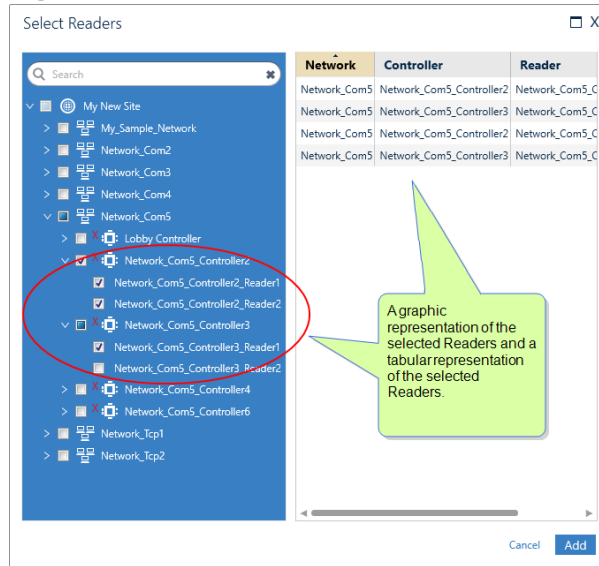
Table A-13 Access Group Readers Table

Parameter	Description
-----------	-------------

Select Readers button  
(only for a Door Access Group table)

Creates an association between a reader and the Access Group in focus.  
To associate a reader with an Access Group, click the **Select Readers** button. A Select Readers dialog is displayed, where one or more readers can be selected from the expandable site tree.

Figure A-29



After selecting a reader, the selection appears in tabular form to the right of the tree. After selecting all of the required readers, click the **Select** button. An association with the Access Group in focus is created and the readers are displayed in the Access Group Readers table.

To edit the list of selected readers, click **Select Readers**, and then click on the red "X" at the beginning of a selected reader row. Click the **Select** button. The association with the Access Group in focus is removed.

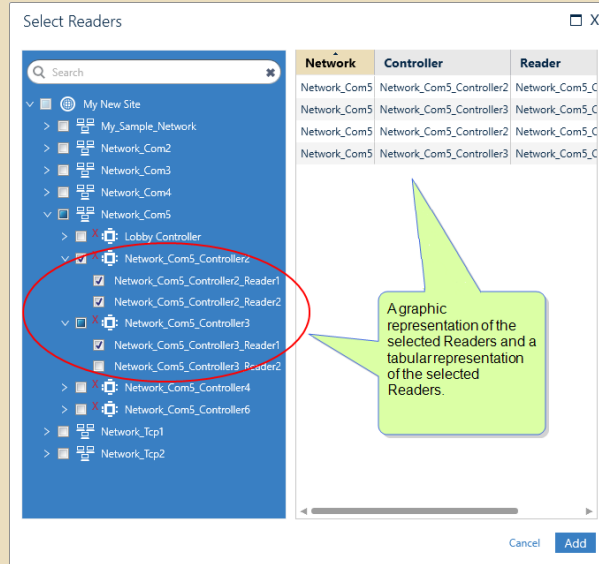
Parameter	Description
-----------	-------------

Select Relays button  
(only for a Lift  
Access Group table)

Creates an association between a relay, which represents a floor in a building, and the Lift Access Group (reader), which represents an elevator in a building, in focus.

To associate a relay with a Lift Access Group, click the **Select Relays** button. A Select Relays dialog is displayed, where one or more relays can be selected from the expandable site tree.

Figure A-30



A relay may only be associated with one Lift Access Group.

After selecting a relay, the selection appears in tabular form to the right of the tree. After selecting all of the required relays, click the **Select** button. An association with the Lift Access Group in focus is created and the relays are displayed in the Lift Access Group Readers table.

For more information about Lift setup, see ["Understanding the Lift Setup concept in GuardPoint10"](#) on page 53.

To edit the list of selected relays, click **Select Relays**, and then click on the red **X** at the beginning of a selected relay row. Click the **Select** button. The association with the Access Group in focus is removed.

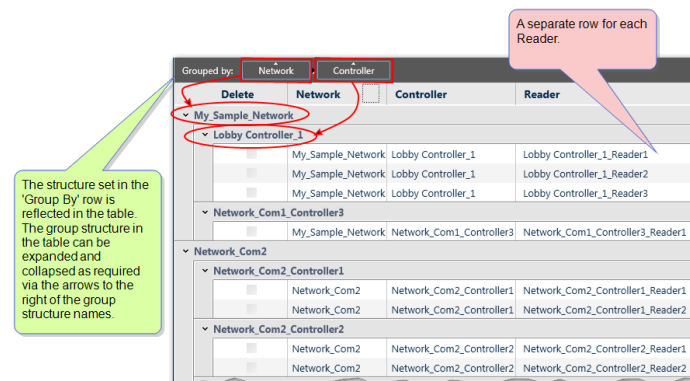


Parameter	Description
Automatically create Multiple Access Group (checkbox only visible when creating a new Access Group)	When selected, a Multiple Access Group is created with the same name as the new Access Group. The new Multiple Access Group will have one associated Access Group. The associated group will be the new Access Group that shares the same name.  <b>Note:</b> In the Multiple Access Group screen, additional Access Groups may be added to the Multiple Access Groups automatically created via the <b>Automatically create Multiple Access Group</b> checkbox. For more information about Multiple Access Groups, see " <a href="#">Access Groups</a> " on <a href="#">page 140</a> .

Group By bar	<p>Restructures the Access Group Readers or Relays table based on the criteria (column headings) dragged into the <b>Group By bar</b>.</p> <p>To change the table's structure:</p> <ul style="list-style-type: none"> <li>» Select a column heading from the row below the <b>Group By bar</b> and drag it into the <b>Group By bar</b>, the heading becomes a criteria, and the table reflects the new criteria structure.</li> <li>» Re-order criteria already in the <b>Group By bar</b> (drag and drop one criteria in front of another) changes the structure applied to the table.</li> <li>» <b>Mouseover</b><sup>1</sup> a criteria already in the <b>Group By bar</b> and click the delete <b>x</b> on the right side of a criteria frame; the criteria is removed from the row.</li> </ul>
--------------	--

The following information describes the columns in the Access Group Readers table. The information is presented in the default Grouped By structure.

Figure A-31



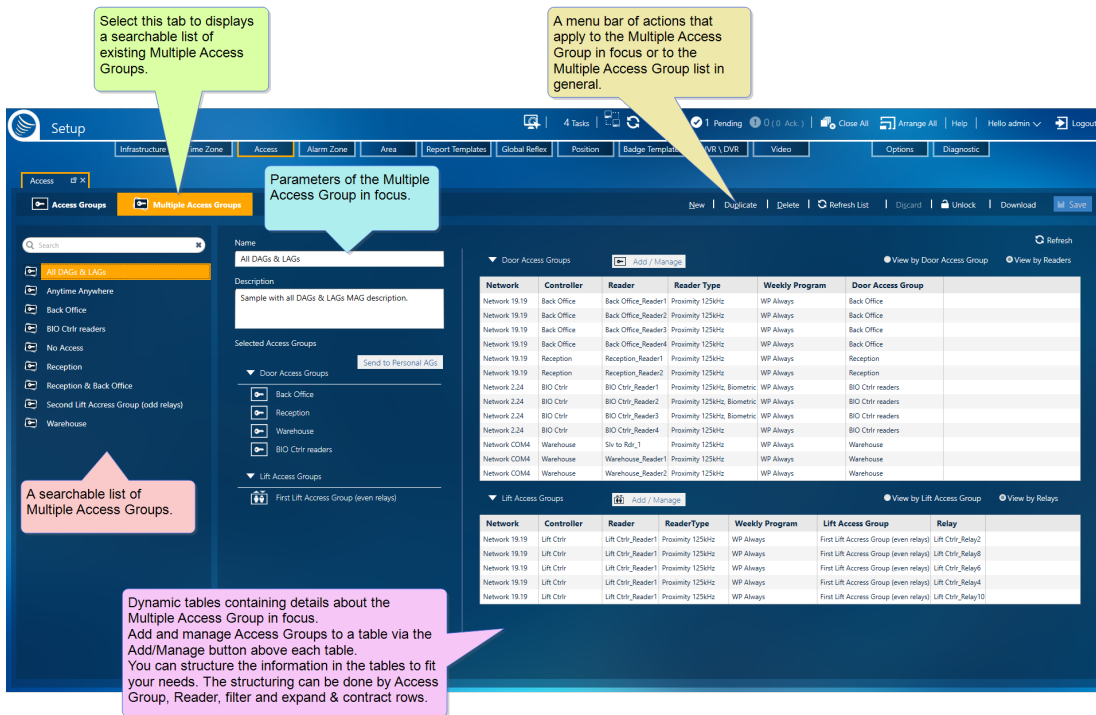
Network	The name of the network where the reader is connected.
Controller	The name of the network's controller where the reader is connected.

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

Parameter	Description
Reader	<ul style="list-style-type: none"> <li>» For Door Access Groups, the name of the reader associated with the Door Access Group in focus. Open the drop-down list to select a different reader connected to the same controller as the currently selected reader.</li> <li>» For Lift Access Groups, the name of the reader (elevator) associated to the Lift Access Group in focus. Because a Lift Access Groups can only have one elevator, the displayed table will show the same elevator name in the <b>Reader</b> column.</li> </ul>
Reader Type	Lists the recognition types or technology types of code read by the reader (i.e. Proximity 125kHz, Biometric, etc.).
Weekly Program (only for a Door Access Group table)	<p>The Weekly Program (WP) assigned to the reader in the specific Access Group in focus. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for holidays and Special Days. WPs set periods of acceptability during which different groups of workers may enter. For more information about WPs, see <a href="#">"Access Groups" on page 140</a></p> <p>The WP in an Access Group's reader row is connected to the cardholder's ability to access premises by being granted access, via a reader.</p> <p>The WP described in the reader's details refers to the expected reader's behavior during the white and or green periods. For more information, see <a href="#">"Reader Details" on page 453</a>.</p>
Relay (only for a Lift Access Group table)	<p>The name of the floor in the building where the elevator may stop. Each row in the table will show a different relay (floor) for the elevator.</p> <p>A relay (floor) may only be associated with one elevator.</p> <p>For information about Lift setup in GuardPoint10, see <a href="#">"Understanding the Lift Setup concept in GuardPoint10" on page 53</a>.</p>

# Multiple Access Group Screen

Figure A-32



A Multiple Access Group is a container that holds individual Access Groups (Door Access Groups or a Lift Access Group). An Access Group's association to a cardholder may go through a Multiple Access Group or, be associated directly without being a member of a Multiple Access Group.

For information about Lift setup in GuardPoint10, see ["Understanding the Lift Setup concept in GuardPoint10" on page 53.](#)

A Multiple Access Group may contain multiple Door Access Groups, but only one Lift Access Group.

Determining when to associate an Access Group with a cardholder directly or through a Multiple Access Group is based on the environment where access will be controlled. For example, if cardholders can be grouped by the spaces they would need to access (i.e. warehouse workers in a warehouse), use Multiple Access Group. If cardholders cannot be grouped this way (i.e. students in university do not necessarily take the same classes at the same time), associate Access Groups directly for each student.

## MultiSite Impact

When **MultiSite** is set to **Yes**:

- » **Anytime Anywhere:** Available only to super users. It includes the **Anytime Anywhere** access group, where all spaces at all times for all sites (except for elevators) are accessible.
- » **Prefixed Anytime Anywhere:** Each site in the system has its own **Anytime Anywhere** Multiple Access Group which is prefixed with the name of the site. It includes the prefixed **Anytime Anywhere** access group that allows access to all spaces at all times within the site.

The Multiple Access Group screen includes four distinct areas:

## A list of existing Multiple Access Groups

The area contains a list of built-in and operator-defined Multiple Access Groups. Select a Multiple Access Group to see the group's parameters and other details specific to the group in focus.

## A Multiple Access Group action bar

From the action bar, you can add / duplicate / delete operator-defined groups or group information. Any changes saved in the Multiple Access Group screen are automatically applied to all currently associated cardholders.

## Multiple Access Group Parameters

Contains basic information about the Multiple Access Group in focus.

If the **Anytime Anywhere** or the **No Access** built-in group is in focus, the parameters displayed will be read-only. The **Anytime Anywhere** and **No Access** groups are built into the system.

- » **Anytime Anywhere:** Allows access to all spaces at all times except for lifts (elevators).
- » **No Access:** Denies access to all spaces at all times.

Table A-14 Multiple Access Group Parameters

Parameter	Description
Name	<p>A free text field that identifies the Multiple Access Group. The default name is "New Multiple Access Group".</p> <p>A best practice is to rename the Multiple Access Group to something that identifies the group's purpose and the type of cardholder who would be associated with it.</p> <p>The Multiple Access Group name must be unique. However, it can share the same name as an individual Access Group.</p>
Description	(Optional) A free text field where information about the Multiple Access Group is entered.

Parameter	Description
Is Applied to Visitors (Checkbox may not be visible)	When selected, the Multiple Access Group will be available when creating a cardholder who is a visitor Type or updating an existing cardholder visitor Type. You will be able to assign the Multiple Access Group to the cardholder visitor Type from the Multiple Access Group drop-down list in the cardholder details' General tab.



Figure A-33

In addition, the Multiple Access Group will be added to the Visitor Control module where it can be assigned to a visitor or a meeting's participants.

**Note:** The Visitor Control module may be missing from your installation. The module is an add-on that can be purchased and installed separately. If you would like to add this module, please contact your GuardPoint10 provider.

Parameter	Description
Selected Access Groups area	<p>Lists Door Access Groups and Lift Access Group in show/hide lists. These Access Groups are members (inside) of the Multiple Access Group container. A Multiple Access Group can contain one or more Access Groups.</p> <p>To see the Access Groups that are already inside the Multiple Access Group, click the arrow preceding the list label name.</p> <p>If there are no Door Access Groups inside the Multiple Access Group in focus, the Door Access Groups show/hide list label will not appear.</p> <p>If there are no Lift Access Groups inside the Multiple Access Group in focus, the Lift Access Groups show/hide list label will not appear.</p> <p>An Access Group can be a member of more than one Multiple Access Group.</p> <p>The order in which the Access Groups appear on an Access Group list determines the priority of the Access Group rules. If a conflict in the rules exists, the Access Group with the higher priority takes precedence.</p> <div data-bbox="427 770 1471 1258" style="background-color: #4a90e2; color: white; padding: 10px;"> <p><b>For example:</b></p> <p>DoorAccessGroup_1 states that a cardholder can use the loading dock door from 20:00 until 7:00. DoorAccessGroup_2 states that a cardholder <i>cannot</i> use the loading dock door from 20:00 until 7:00.</p> <p>If DoorAccessGroup_1 appears higher in the Selected Door Access Groups list than DoorAccessGroup_2, access will be granted, following the rule in DoorAccessGroup_1.</p> <p>If DoorAccessGroup_2 appears higher in the Selected Door Access Groups list than DoorAccessGroup_1, access will be denied, following the rule in DoorAccessGroup_2.</p> </div>
Send to Personal AGs button	<p>To the right of the <b>Access Groups show / hide list label</b> is the <b>Send to Personal AGs</b> button.</p> <p>It unlinks (or disassociates) cardholders linked to the Multiple Access Group in focus. Then directly links the Multiple Access Group's contents to the cardholder's a <b>Door Access Group</b> and <b>Personal Lift Access Group</b> items.</p> <p>To see the results of this procedure, open the cardholder details of a cardholder that was associated with the Multiple Access Group. The Multiple Access Group switched to <b>No Access</b>, and the Door Access Groups field and Lift Access Group field displays the content of the Multiple Access Group.</p>

## A dynamic Multiple Access Group Tables

Contains information about readers and or relays associated with an Access Group that is a member of the Multiple Access Group in focus. Door Access Groups and Lift Access Group have their own separate tables. For quicker analysis, you can change the view of the information in the table with column filters and the **View by...** buttons above the table.

To add an Access Group to a table click the Add/Manage button above a table. The Select Access Groups dialog is displayed with the relevant group types. Add/Remove Access Groups from the list of selected Access Groups as required. Then, if necessary, reorder the list of selected Access Groups to change the Access Group rule priority.

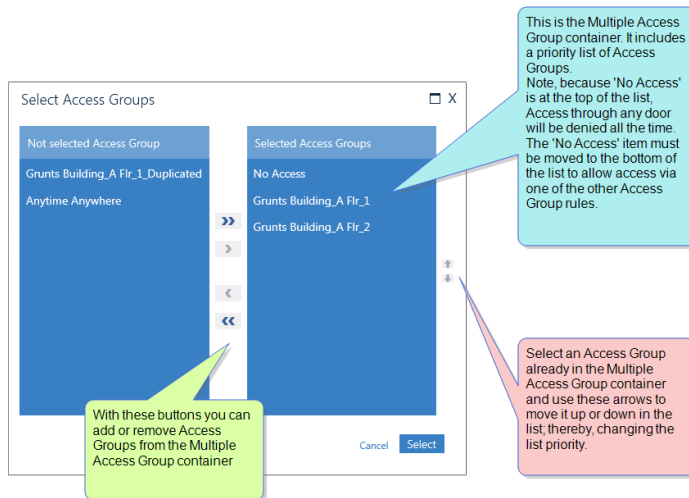


Figure A-34

**Note:** The built-in **No Access** Group is the exception to the priority rule. It can be placed at the top of the list where it would be excluded from the list of other selected Access Groups.

For information about table filters, see **"Table Filters" on page 695**.

The following information describes the columns and functionality of the Multiple Access Group table. The information is presented with the default **View By Access Group** structure.

Figure A-35

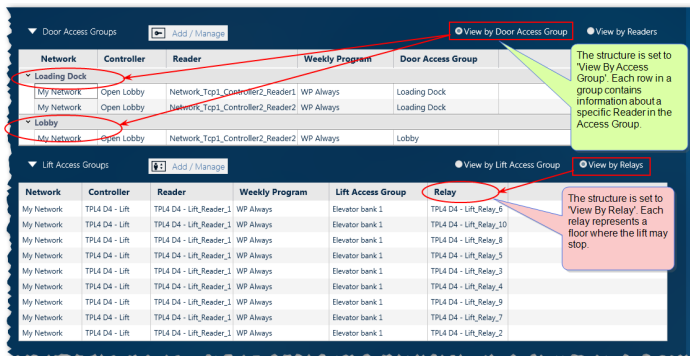


Table A-15 Multiple Access Group Table

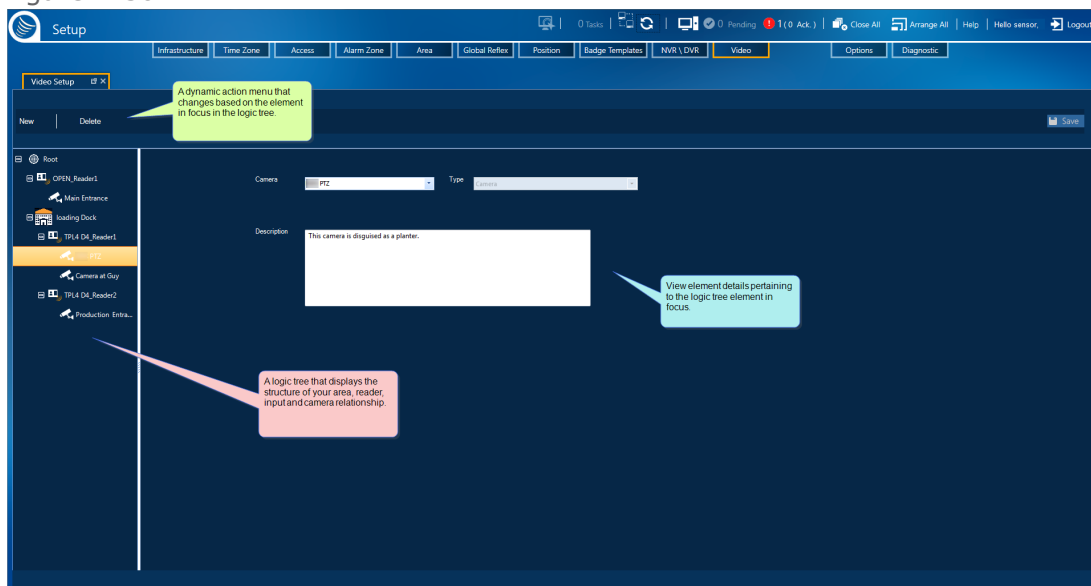
Parameter	Description
Network	The name of the network where the reader is connected.
Controller	The name of the network's controller where the reader is connected.

Parameter	Description
Reader	<p>Depending on the Access Group type, the Reader column will show:</p> <ul style="list-style-type: none"> <li>» The name of the reader associated with a Door Access Group associated with the Multiple Access Group in focus.</li> </ul> <p>Or,</p> <ul style="list-style-type: none"> <li>» The name of the reader (elevator) associated with a Lift Access Group associated with the Multiple Access Group in focus.</li> </ul>
Reader Type	Lists the recognition types or technology types of code read by the reader (i.e. Proximity 125kHz, Biometric, etc.).
Weekly Program	<p>The Weekly Program (WP) associated with a reader. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for holidays. WPs set periods of acceptability during which different groups of workers may enter. For more information about WPs, see <a href="#">"Daily Program Time Zones" on page 114</a>.</p> <p>The WP in the Access Group is connected to the cardholder's ability to access premises by being granted access via a reader. The WP, described in the reader's details, refers to the expected work hours anticipated by the reader (white and green). For more information, see <a href="#">"Reader Details" on page 453</a>.</p>
Door Access Group (only in the Door Access Group table)	The individual Door Access Group (a member of the Multiple Access Group in focus) associated with the reader.
Lift Access Group (only in the Lift Access Group table)	The individual Lift Access Group (a member of the Multiple Access Group in focus) associated with the reader (Lift).
Relay (only in the Lift Access Group table)	The floors in the building known to the reader (Lift). Each relay is connected to a button in the Lift panel. The buttons are enabled or disabled based on the cardholder's authorizations.



# Video Setup Screen

Figure A-36



Through the Video Setup screen, operators build structures and relationships between the cameras in their NVR/DVR system and readers and inputs in their GuardPoint10 system database.

The relationships are grouped together in areas. Think of an area as a physical, measurable area that all of the elements in the group share. For example, a lobby (area) can include a reader and door lock input device as well as a panic button at a secretary's desk and cameras.

The Video Setup screen includes the following three areas:

## Logic tree

A representation of the relationship between elements in your NVR/DVR system and your GuardPoint10 system database. These relationships are necessary to create a fully functional Video Setup screen.

## Tree action bar

Allows you to add or delete elements in the logic tree.

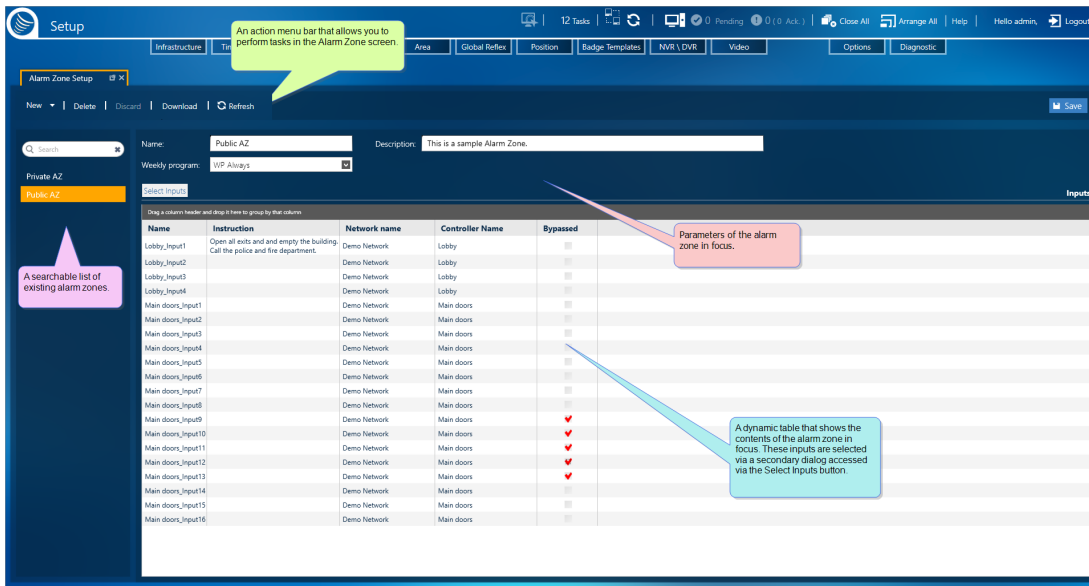
# Element parameters

Element Table Parameters

Parameter	Description
Type	<p>Identifies an element by its physical representation such as:</p> <ul style="list-style-type: none"> <li>» <b>Area</b>: A physical, measurable area that all elements in the group share. This element exists only for a Video grouping.</li> <li>» <b>Reader</b>: Acquires data from a cardholder to determine if access will be granted or denied. The reader data is gathered from the GuardPoint10 system database.</li> <li>» <b>Input</b>: Initiates an action based on reader results and other triggers. The input data is gathered from the GuardPoint10 system database.</li> <li>» <b>Camera</b>: Gathers images (video or still pictures). The camera data is gathered from the NVR or DVR system and may be triggered by GuardPoint10 events.</li> </ul>
Name	<p>Except for an <b>Area</b>, a name is determined by the system where the element was created. Select the element from the <b>Name</b> drop-down list that consists of all available elements of the selected type.</p>
Provider (visible when the Type is 'Camera')	<p>Select the NVR/DVR where the camera is connected. The drop-down list of cameras changes according to the NVR/DVR selected.</p>
Description	<p>(Optional) A free text field where information about the selected element may be entered.</p>

# Alarm Zone Setup Screen

Figure A-37



An GuardPoint10 alarm zone allows you to apply a Weekly Program and reflexes to a group of inputs.

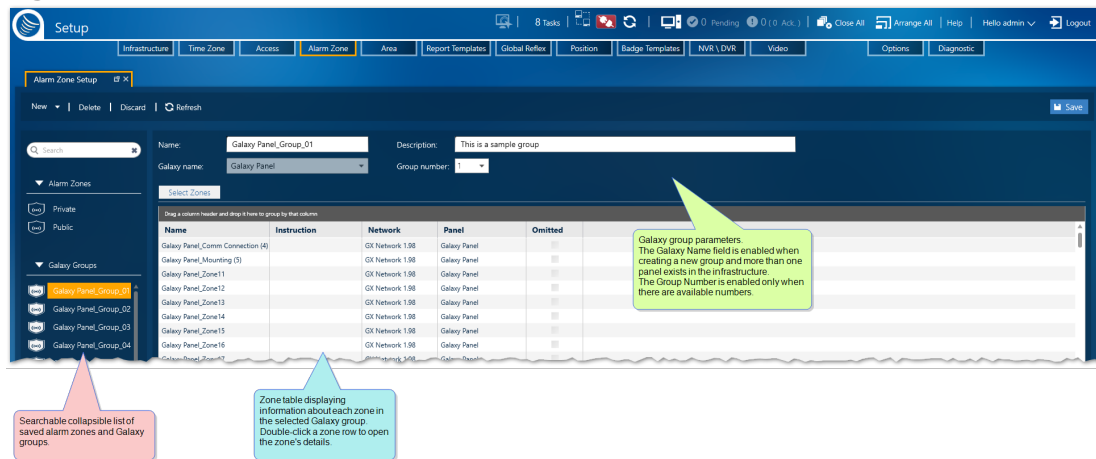
## Galaxy group specific screen

If there is a **Galaxy**<sup>1</sup> panel integrated into the GuardPoint10 infrastructure, the following actions take place or area available to the user:

- » Galaxy groups that exist in the panel will be automatically added to the GuardPoint10 database and appear in the list of saved alarm zones and Galaxy groups.
- » Initially, all zones will be in Galaxy's **Group\_1**.
- » When you select a Galaxy group from the saved list, the group's Name and Description Panel name where the group is located, and the group number will be displayed on the screen. In addition, a Zone table listing Galaxy zones found in the group is displayed.

<sup>1</sup>A Honeywell alarm monitoring system where detectors are connected to a Galaxy panel. The panel manages various kinds of alarms (i.e. fire, intruder, etc.).

Figure A-38



## GuardPoint 10 Alarm Zone specific screen

The Alarm Zone screen has five distinct areas:

### Searchable collapsible list of existing alarm zones

The list includes all alarm zones that have been saved in the system database. Place an alarm zone in focus to see information about the zone and its contents.

### Alarm zone action bar

From the action bar, you can add, delete, discard or download alarm zones. Any saved changes to an alarm zone are automatically applied to the governing rules of the inputs included in the alarm zone.

### Alarm zone parameters

Contains basic information about the alarm zone in focus.

The parameters are as follows:

Table A-16 Alarm Zone Parameters

Name	Description
Name	<p>A free text field that identifies the alarm zone by name. The default name of a new alarm zone is "New alarm zone".</p> <p>A best practice is to rename the alarm zone to something that identifies the zone's specific function.</p> <p>The name must be unique.</p> <p>In the case of a Galaxy group, the name of the group will be displayed. New groups cannot be added from GuardPoint10, however, their names can be changed. Group names must be unique. An GuardPoint10 alarm zone and a Galaxy group cannot have the same name.</p>
Description	<p>(Optional) A free text field where information about an alarm zone or Galaxy group is entered.</p>
Weekly Program	<p>The Weekly Program (WP) assigned to an alarm zone. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for holidays. WPs set the arm and disarm periods of an alarm zone. In a green period an alarm zone is armed and during white periods an alarm zone is disarmed. These arm and disarm periods may be manually overridden via the "<a href="#">Alarm Zones (Security)</a>" on page 365 screen and the "<a href="#">Security Center</a>" on page 389 screen, where an icon, shape, or textbox is linked to a relevant alarm zone.</p> <p>For more information about WPs, see "<a href="#">Weekly Program Time Zones</a>" on page 120.</p>

## Alarm Zone Inputs table

For information about table filters, see "[Table Filters](#)" on page 695.

A description of each column in the Alarm Zone Input table is provided below.

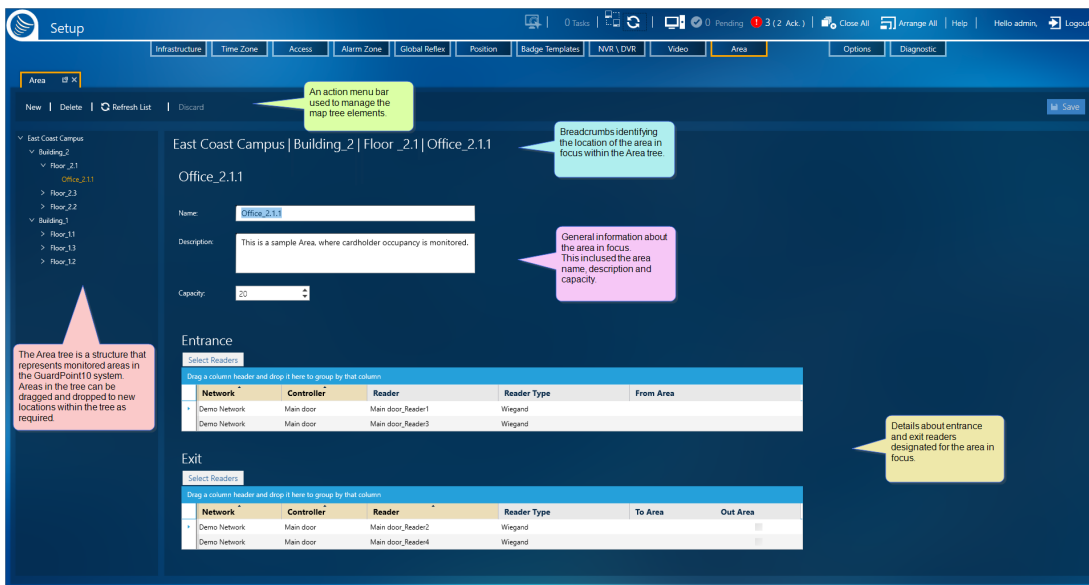
Table A-17 Alarm Zone Input Table Options and Columns

Parameter	Description
Group By bar	<p>Restructures the table based on the criteria (column heading) dragged into the <b>Group By bar</b>.</p> <p>To change the table's structure:</p> <ul style="list-style-type: none"> <li>» Select a column heading and drag it to the <b>Group By bar</b>, the heading becomes a criteria, and the table reflects the new criteria structure.</li> <li>» Re-order criteria already in the <b>Group By bar</b> (drag and drop one criteria in front of another) changes the structure applied to the table.</li> <li>» <b>Mouseover</b><sup>1</sup> a criteria already in the <b>Group By bar</b> and click the delete <b>x</b> on the right side of a criteria frame; the criteria is removed from the table.</li> </ul>
Name	The name of an input placed in the alarm zone.
Instruction	Text describing operator protocol in case an alarm is triggered by the input device (i.e. "Call supervisor and police").
Network Name	The name of the network where an input is located.
Controller Name	The name of the controller, within the network, where an input is connected.
Bypassed	<p>When selected, transactions sent by an input device are ignored by the system. For example, if a change to the expected status of the input is detected, the input will send an alarm transaction. However, the transaction will be ignored by the system and the event won't appear in the log.</p> <p>This field also exists in the <a href="#">"Input Device Table" on page 480</a>. These fields are linked. If marked as bypassed in one table, it will automatically be marked as bypassed in the other table.</p>

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

# Area Screen

Figure A-39



The Area screen provides the tools necessary to add and manage areas in your GuardPoint10 environment. Areas are used to monitor cardholder occupancy via the Security Center screen and Area Roll Call screen. In addition, an area's condition may be actionable through a global reflex specifically designed to address areas.

Besides the basic Name and Description fields, an area consists of three elements or values, capacity, entrance readers, and exit readers.

The Area screen has four distinct areas:

## Area tree

The Area tree reveals the logical structure of your saved areas and allows you to open the details of an area with a simple click. An area may have sub-areas in the tree which in the real-world indicates that one area is accessible from its parent area (a larger area where the sub-area is located).

The initial default area name derives its name from the site name found in the Infrastructure tree (see ["Site Details" on page 443](#)). This name may be changed at any time. A new area must be a sub-area of the initial default area.

An area may have multiple sub-areas and multiple levels within the tree.

The Area tree's area / sub-area relationship is not based on the physical connection between readers and areas do not share information based on the area / sub-area relationship. The tree structure logic is the choice of the user building the tree.

## Area action bar

The action bar provides the operator with the tools necessary to add an area to the system and display it in the tree or delete an area from the system and tree. An area can only be deleted if it doesn't have

any sub-areas.

## General Area fields

Figure A-40



These fields hold general information about the area selected in the Area tree.

Table A-18 General Area fields

Name	Description
Name	The display name of the area selected in the Area tree. The name is limited to 50 characters.
Description	(Optional) A free text field where information about the area is entered. The description is limited to 200 characters.
Capacity	The maximum number of cardholders recommended for an area.
Global Anti-Passback (GAPB) (may not be visible)	Displayed when the Options screen's setting <b>GAPB</b> is set to <b>Yes</b> . Turns an area into a GAPB area. Default value: <b>No</b> For information about Global Anti-Passback, see " <a href="#">Understanding Anti-passback in GuardPoint10</a> " on page 80.
Current GAPB Areas (may not be visible)	Displayed when the Options screen's setting <b>GAPB</b> is set to <b>Yes</b> . Lists current GAPB areas in the system. In a MultiSite environment, all GAPB areas are displayed in the list regardless of the owner site.
Number of remaining Areas that may have the GAPB option (may not be visible)	Displayed when the Options screen's setting <b>GAPB</b> is set to <b>Yes</b> . Displays the number of areas that may become GAPB areas. The maximum number of areas that can be GAPB areas is 31 (including the Offsite area, which is built-in to GuardPoint10).

## Entrance and Exit tables

Contains reader information about those readers identified as an entrance or exit point for the area in focus. An area may have more than one entrance or exit point.



Table A-19 Entrance Reader Table Parameters

Name	Description
Network	The name of the network where the selected reader is connected.
Controller	The name of the network's controller where the selected reader is connected.
Reader	The name of the selected reader connected to the controller and designated as an entry point to the area in focus.
Reader Type	Lists the recognition types or technology types of code read by the selected reader (i.e. Proximity 125kHz, Biometric, etc.).
APB (Green Zone) (may not be visible)	<p>Displayed when the Options screen's setting <b>GAPB</b> is set to <b>Yes</b>.</p> <p>Indicates the Anti-passback setting of the reader in its green zone. The setting is found in the reader's details, Access Mode tab.</p> <p>The Anti-passback setting must be set to <b>Yes</b> to participate in the GAPB.</p> <p>For information about Global Anti-Passback, see "<a href="#">Understanding Anti-passback in GuardPoint10</a>" on page 80.</p>
APB (White Zone) (may not be visible)	<p>Displayed when the Options screen's setting <b>GAPB</b> is set to <b>Yes</b>.</p> <p>Indicates the Anti-passback setting of the reader in its white zone. The setting is found in the reader's details, Access Mode tab.</p> <p>The Anti-passback setting must be set to <b>Yes</b> to participate in the GAPB.</p> <p>For information about Global Anti-Passback, see "<a href="#">Understanding Anti-passback in GuardPoint10</a>" on page 80.</p>
From Area	If the area in focus is accessible from a different area, via the same reader, the table cell will contain the name of the other area.
Offsite	If the reader (entrance point) leads to a space that is a non-GuardPoint10 area (i.e. the street), you can select the checkbox in this table cell. The <b>To Area</b> value will be automatically changed to <b>Offsite</b> without the need to open the reader's details.

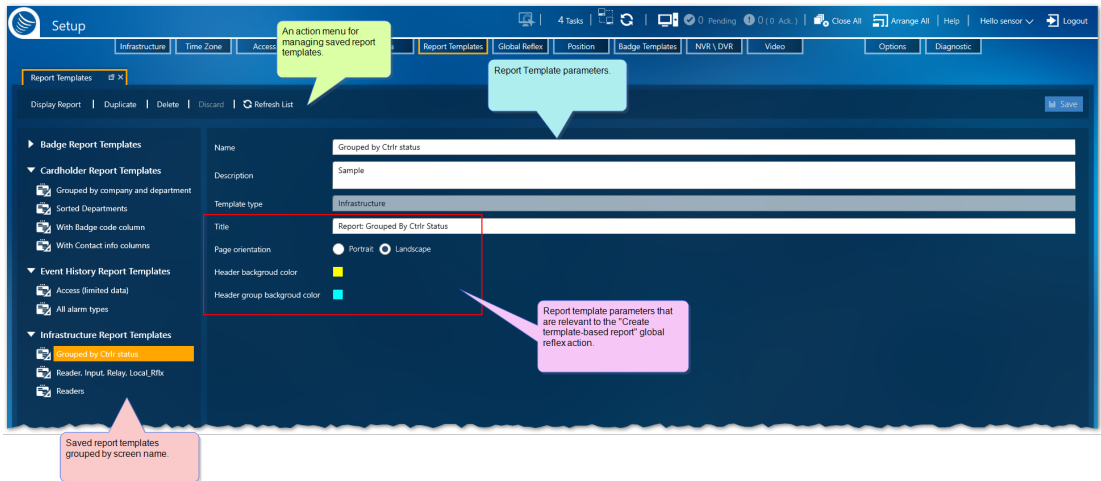
Table A-20 Exit Reader Table Parameters

Name	Description
Network	The name of the network where the selected reader is connected.
Controller	The name of the network's controller where the selected reader is connected.
Reader	The name of the selected reader connected to the controller and designated as an exit point to the area in focus.

Name	Description
Reader Type	Lists the recognition types or technology types of code read by the selected reader (i.e. Proximity 125kHz, Biometric, etc.).
APB (Green Zone) (may not be visible)	<p>Displayed when the Options screen's setting <b>GAPB</b> is set to <b>Yes</b>.</p> <p>Indicates the Anti-passback setting of the reader in its green zone. The setting is found in the reader's details, Access Mode tab.</p> <p>The Anti-passback setting must be set to <b>Yes</b> to participate in the GAPB.</p> <p>For information about Global Anti-Passback, see <a href="#">"Understanding Anti-passback in GuardPoint10" on page 80</a>.</p>
APB (White Zone) (may not be visible)	<p>Displayed when the Options screen's setting <b>GAPB</b> is set to <b>Yes</b>.</p> <p>Indicates the Anti-passback setting of the reader in its white zone. The setting is found in the reader's details, Access Mode tab.</p> <p>The Anti-passback setting must be set to <b>Yes</b> to participate in the GAPB.</p> <p>For information about Global Anti-Passback, see <a href="#">"Understanding Anti-passback in GuardPoint10" on page 80</a>.</p>
To Area	<p>If the reader (exit point) is also an entry point to another area, the name of that other area appears in this table cell.</p> <p>This value is usually selected from the reader's details.</p>
Offsite	<p>If the reader (exit point) leads to a space that is a non-GuardPoint10 area (i.e. the street), you can select the checkbox in this table cell. The <b>To Area</b> value will be automatically changed to <b>Offsite</b> without the need to open the reader's details.</p>

# Report Template Screen

Figure A-41



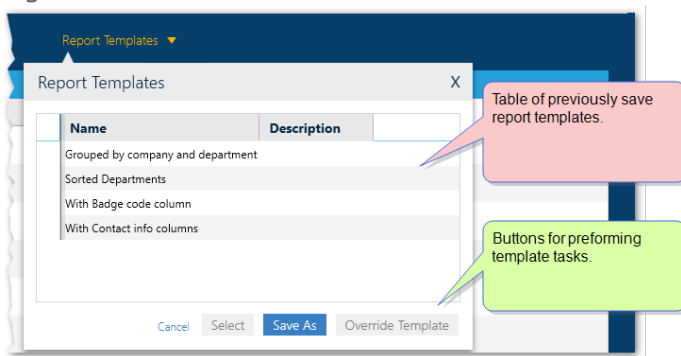
A template contains a design layout to be used for an GuardPoint10 screen display. The screens where a template is applicable are Infrastructure (Table view), Badges, Cardholders, and Event History in addition to the global reflex "Create Template-based report" on page 548 action.

Templates are created from its source screen where the template can be applied. The Report Template screen contains the tools for managing and editing template data and structure.

The Report Template screen is accessible from two places:

- » The Setup task group's primary menu bar.
- » The **Save As** button or **Override** button found in a screen's Report Template dialog.

Figure A-42



The Report Template screen has three distinct areas:

## Action menu where templates are Managed

From the Action menu you have the following options:

- » **Display Report:** Opens the relevant screen and loads the template in focus.
- » **Duplicate:** Adds a new template identical to the one in focus. The new template's name will have the text "\_Duplicate" appended to it.
- » **Delete:** Removes the template in focus from the system. A template that is used in a global reflex "[Create Template-based report](#)" on page 548 action cannot be deleted.
- » **Discard:** Returns a template's parameters to their last saved values.

## List groups contain saved report templates

A collapsible list of saved report templates is grouped by the screen where a template may be applied and allows you to open a template's parameters.

If a screen does not have any templates, the screen group will not appear in the list.

## Template parameters

A series of parameters that contain information about a selected template. These parameters can be grouped into two categories:

- » General information
- » Global reflex specific information

The following table describes the parameters:

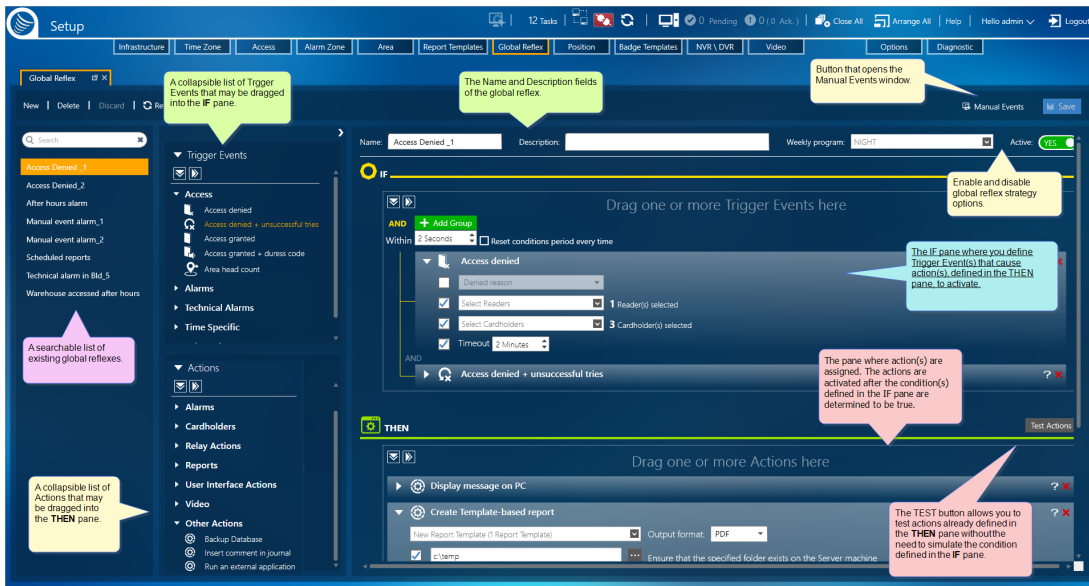
**Table A-21** Report Template Parameters

Name	Description
<b>General information</b>	
Name	A free text field that identifies a template by name. This is the name that will appear in the list of saved templates as well as in a screen's Report Template dialog, where the template may be selected and applied. A best practice is to name a template something that identifies the purpose of the template.
Description	(Optional) A free text field where information about a report template is entered.
Template Type	A read-only field that shows the screen group name where the template is saved.
<b>Global reflex specific information</b>	
Title	The text that will appear on a report that is in a global reflex " <a href="#">Create Template-based report</a> " on page 548 action.

Name	Description
Header Background Color	The color of the first row of a reports table. To change the color, click on the current color and then select a new color.
Header Group Background Color	The color of the first row of a report table's group. This parameter only applies to a template where the Group By bar is used. To change the color, click on the current color and then select a new color.

# Global Reflex Screen

Figure A-43



A Global Reflex allows you to specify a trigger event or events that will set off a specific action or actions, or add a manual event name that, when selected, will trigger an action and without conditions.

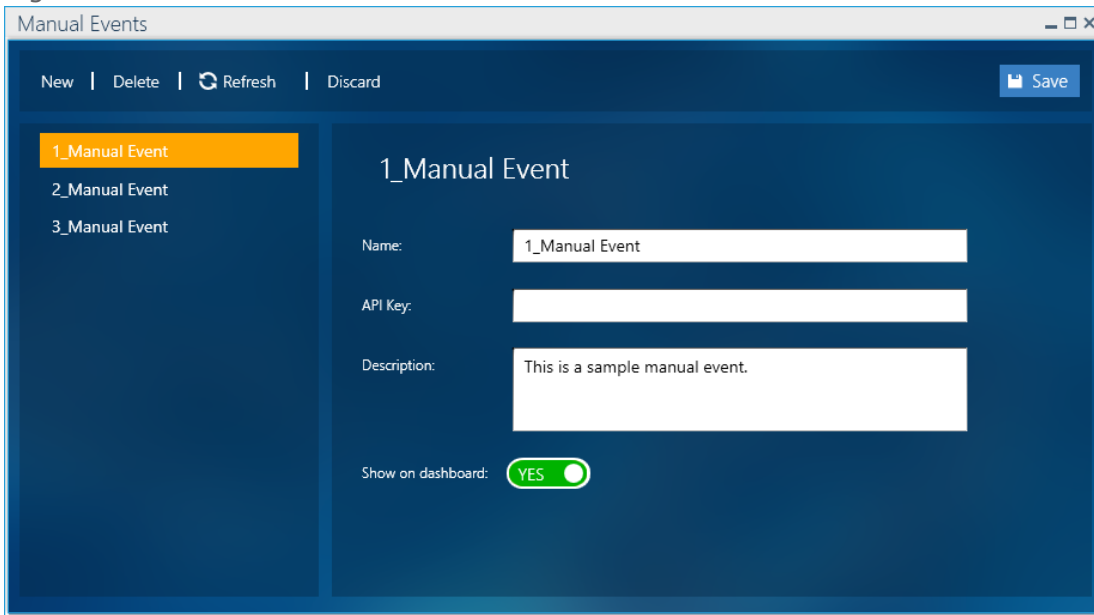
## Manual Events

The **Manage Manual Event** button, next to the **Save** button, opens a Manage Manual Event window, where manual events may be added, deleted, and edited. A manual event is a trigger without conditions attached to it. A manual event may be triggered using one of the following methods:

- » By name, via an operator action on the dashboard or via the Security Center screen.
- » By name via an API command
- » As part of a conventional global reflex condition

The Manual Event window is where a manual event is named, defined and, if necessary, provided with an **API Key** and or added to the dashboard's Manual Events drop-down list.

Figure A-44



**Note:** The manual event **API Key** field may not be visible on your screen and should only be entered or edited when instructed by your API developer.

The Manual Events feature is available where a license has Advanced Global Reflexes.

For more information about Manual Events, see ["Adding a Global Reflex Manual Event"](#) on page 328.

## Conventional Global Reflexes

### Global Reflex general parameters

The parameters are as follows:

*Table A-22 Global Reflex Parameters*

Name	Description
Name	<p>A free text field that identifies a global reflex. The default name of a new global reflex is "New Reflex".</p> <p>A best practice is to rename the global reflex to something that identifies the condition and action that it represents.</p> <p>The name must be unique.</p>
Description	<p>(Optional) A free text field where information about a global reflex is entered.</p>

Name	Description
Weekly Program	<p>The global reflex will be automatically enabled during the selected Weekly Program's green period. If no Weekly Program is selected the global reflex will be enabled or disabled based on the <b>Active</b> setting.</p> <p>The <b>Active</b> setting overrides the enabled state of the Weekly Program setting. If <b>Active</b> is set to <b>No</b>, the global reflex will be disabled regardless of the Weekly Program selected.</p>
Active	<p>A Yes/No setting that enables or disables a global reflex. This means that GuardPoint10 could ignore a global reflex's conditions and actions (when <b>Active</b> is set to <b>No</b>) without deleting the global reflex from the list of saved global reflexes. The global reflex can then be re-activated at a later time by simply changing the <b>Active</b> setting to <b>Yes</b>.</p>

## IF statement pane Trigger Events

The **IF** pane allows you to define one or more trigger events that must be true for the one or more actions, defined in the **THEN** pane, to take place.

Trigger events are grouped by subject in the Trigger Event pane. Each subject may be expanded to show the related Trigger Events, where they can be dragged & dropped into the **IF** pane.

The list of trigger event subjects can be collapsed or expanded via the large arrow buttons above the list.

A trigger event may have one or more parameters, all of an event's parameters must be satisfied for the trigger event to be true.

Trigger events may have an **OR** or **AND** logical operator to connect two or more events. The **OR** operator means that only one connected trigger event in the **IF** pane has to be true. The **AND** operator means that all connected trigger event has to be true within the specified times.

Complex trigger event conditions can be constructed by grouping trigger events and embedding one group of trigger events in another.

Relationship lines between trigger events and trigger event groups exist to better identify connective relationships between the trigger events.

The AND operator has the following two related parameters:

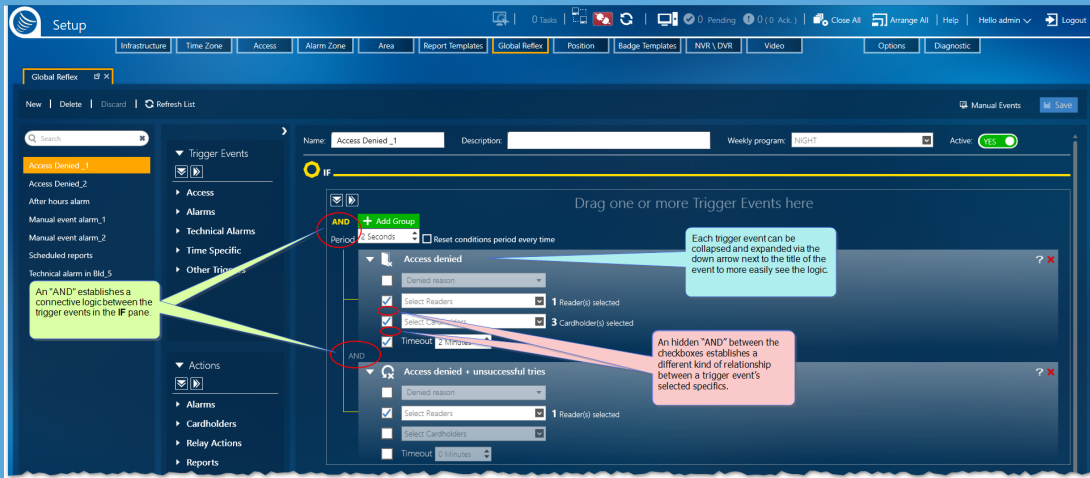
- » **Within field:** All event triggers in the event trigger group must be satisfied within the specified time to consider the event trigger group true.
- » **Reset condition period every time checkbox:** When the checkbox is selected, after the AND connected event trigger group is true (all event triggers in the group are satisfied), the group will reset and a new instance of the event triggers in the group will have to be satisfied).

The **Add Group** button next to the **OR** and **AND** button allow you to embed a new event trigger group in the group where the **Add Group** button was clicked.



## How to read a Global Reflex's IF pane

In the following image, the **OR** means that one of the Trigger Events (i.e. Access Denied or Access Denied + Unsuccessful Tries) must be true for the **THEN** actions to take place.



For the Access Denied Trigger Event to be true, imagine there is an “AND” between the selected checkboxes. This “AND” means that the access denied cause must be due to a detected stolen badge AND the stolen badge must have been swiped at the specified readers.

The same logic would also be applied to the Access Denied + Unsuccessful Tries Trigger Event to make it true.

The following table contains the Subjects and Trigger Events available for the **IF** pane. Each Trigger Event listed has its own set of parameters where the Trigger Event's specifics are defined.

A Trigger Event's specific is applicable when its checkbox is selected. After selecting a Trigger Event and dragging it to the **IF** pane, you select the specifics and, where relevant, enter values. For example, if an Access Denied Trigger Event's Reader specific checkbox is selected, select one or more readers where a Denied Access condition would have to take place for the **THEN** action to execute.

Table A-23 Trigger Events

Trigger Event	Description
<b>Subject: Access</b>	

Trigger Event	Description
Access Denied	<p>The cardholder is denied access, and all of the Trigger Event's selected specifics have been satisfied.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <a href="#">Denied Reason</a></li> <li>» <a href="#">Selected Reader</a></li> <li>» <a href="#">Selected Department</a></li> <li>» <a href="#">Selected Cardholder</a></li> <li>» "Timeout" on page 543</li> </ul>
Access Denied + unsuccessful Tries	<p>The individual is denied access, after exhausting the limited number of entry attempts allowed by the system, and all of the Trigger Event's selected specifics have been satisfied.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <a href="#">Denied Reason</a></li> <li>» <a href="#">Selected Reader</a></li> <li>» <a href="#">Selected Department</a></li> <li>» <a href="#">Selected Cardholder</a></li> <li>» "Timeout" on page 543</li> </ul>
Access Granted	<p>The cardholder is allowed access, and all of the condition's selected specifics have been satisfied.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <a href="#">Transaction Code</a></li> <li>» <a href="#">Selected Reader</a></li> <li>» <a href="#">Selected Department</a></li> <li>» <a href="#">Selected Cardholder</a></li> <li>» "Timeout" on page 543</li> </ul>

Trigger Event	Description
Access Granted + Duress Code	<p>The cardholder is allowed access, but a duress code has been entered at the reader and all of the Trigger Event's selected specifics are satisfied. Due to the assumed duress of the cardholder, additional security protocols may be initiated in addition to the <b>THEN</b> actions triggered by the specifics.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <a href="#">Transaction Code</a></li> <li>» <a href="#">Selected Reader</a> <p>A duress code may only be used at a reader where the <b>Access Authorization</b> is set to <b>With Badge and Keypad</b>. For more information about <b>Access Authorization</b>, see "<a href="#">Reader Details</a>" on page 453.</p> </li> <li>» <a href="#">Selected Department</a></li> <li>» <a href="#">Selected Cardholder</a></li> <li>» "<a href="#">Timeout</a>" on page 543</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Entering a duress code requires a reader device that includes a keypad.</p> </div>
Area Head Count	<p>A formula that includes an area's cardholder occupancy value and either a fixed number or a number derived from an area's capacity is used to determine the conditioned state (true or false).</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <b>Area Name:</b> Areas where the formula will be applied.</li> <li>» <b>Where the head count is:</b> An Arithmetic qualifier (=, &gt;, &lt;, or in combination).</li> <li>» <b>Fix value:</b> Compared to a value not connected to the capacity. This is especially valuable when an area has an unlimited capacity.</li> <li>» <b>Area Capacity:</b> Compared to an area's capacity or a value derived from the capacity.</li> <li>» <b>Percent of Capacity:</b> Compared to a percentage of an area's capacity.</li> <li>» <b>Run only once:</b> When selected, the first time the event trigger is true, the action will be invoked. All subsequent true events will be ignored until the event trigger is returned to a false state.</li> <li>» "<a href="#">Timeout</a>" on page 543</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p> </div>

**Subject: Alarms**

Trigger Event	Description
Acknowledge or Confirm	<p>An alarm has been triggered on one of the selected inputs.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <b>Acknowledge:</b> A selected input's alarm has been acknowledged.</li> <li>» <b>Confirm:</b> A selected input's alarm has been confirmed.</li> <li>» <b>Confirm All:</b> All input alarms have been confirmed.</li> <li>» <b>Acknowledge or Confirm:</b> A selected input's alarm has been "Acknowledged" or "Confirmed".</li> <li>» <b><u>Input</u></b></li> <li>» "Alarm Zone" on page 544</li> <li>» "Timeout" on page 543</li> </ul> <hr/> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p>
Line Cut or Short	<p>A line cut or line short alarm has been triggered on one of the selected inputs.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <b>Line Cut:</b> One of a selected input's wires was cut.</li> <li>» <b>Line Short:</b> One of a selected input's wires has a short.</li> <li>» <b>Line Cut or Line Short:</b> One of a selected input's wires has been "Cut" or "Has a Short".</li> <li>» <b><u>Input</u></b></li> <li>» "Alarm Zone" on page 544</li> <li>» "Timeout" on page 543</li> </ul> <hr/> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p>

Trigger Event	Description
Start or End of Alarm	<p>An alarm has been triggered and the Trigger Event's selected specifics have been satisfied.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <b>Start of Alarm:</b> A selected input's alarm has started.</li> <li>» <b>End of Alarm:</b> A selected input's alarm, previously determined to be started is now determined to be ended.</li> <li>» <b>Start or End of Alarm:</b> A selected input's alarm state changed from "Start to End" or "Start".</li> <li>» <b><u>Input</u></b></li> <li>» "Alarm Zone" on page 544</li> <li>» "Timeout" on page 543</li> </ul>
<b>Subject: Technical Alarms</b>	
Battery Power	<p>An alarm that indicates that a controller's battery health has changed.</p> <p>The specifics available is:</p> <ul style="list-style-type: none"> <li>» <b>Low:</b> A selected controller's internal battery has changed "Normal to Low".</li> <li>» <b>Normal:</b> A selected controller's internal battery has changed "Low to Normal".</li> <li>» <b>Low or Normal:</b> A selected controller's internal battery has changed from "Low to Normal" or "Normal to Low".</li> <li>» <b><u>Controller name</u></b></li> <li>» "Timeout" on page 543</li> </ul> <hr/> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p>

Trigger Event	Description
Controller Box	<p>An alarm that indicates that a controller's casing has been opened.</p> <p>The specifics available is:</p> <ul style="list-style-type: none"> <li>» <b>Box Opened:</b> A selected controller's casing, previously determined to be closed is now determined to be opened.</li> <li>» <b>Box Closed:</b> A selected controller's casing, previously determined to be opened is now determined to be closed.</li> <li>» <b>Box Opened or Closed:</b> A selected controller's casing has changed from "Open to Close" or "Close to Open".</li> <li>» <b><a href="#">Controller name</a></b></li> <li>» <b><a href="#">"Timeout" on page 543</a></b></li> </ul> <hr/> <p><b>Note:</b> This Trigger Event is only relevant for controllers that have a tamper alarm built into the controller (i.e. IC2001, IC4001 and IC550).</p> <hr/> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p>
Power Down or Up	<p>A controller internal alarm that indicates that a controller has a power down state or a power restored state.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <b>Power Down:</b> A selected controller last determined to have power is no longer powered.</li> <li>» <b>Power Up:</b> A selected controller last determined to have no power is now powered.</li> <li>» <b>Power Down or Up:</b> A selected controller has changed power state.</li> <li>» <b><a href="#">Controller name</a></b></li> <li>» <b><a href="#">"Timeout" on page 543</a></b></li> </ul> <hr/> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p>

Trigger Event	Description
Power Supply	<p>A specific alarm that indicates that a controller has a power source status change (i.e. from a wall socket (primary source) to a battery).</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <b>Interrupted:</b> A selected controller last determined to be powered from a non-battery source (primary) is no longer powered from that source.</li> <li>» <b>Restored:</b> A selected controller last determined to have an interrupted power source is now powered from the original primary source.</li> <li>» <b>Interrupted or Restored:</b> A selected controller has changed from its last power source determination (either interrupted or restored).</li> <li>» <b><a href="#">Controller name</a></b></li> <li>» <b><a href="#">"Timeout" on page 543</a></b></li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This trigger event is detected by controllers via their PSF inputs. The controllers that have PSF inputs are <b>IC2001, FLASH, and IC550</b> controller types.</p> </div>
Reader Connectivity	<p>An alarm that indicates that a reader has changed its connectivity status to its controller.</p> <p>The specifics available are:</p> <ul style="list-style-type: none"> <li>» <b><a href="#">Selected Reader</a></b></li> <li>» <b><a href="#">"Timeout" on page 543</a></b></li> <li>» <b>Interrupted:</b> A selected reader last determined to be connected to its communication cable is now not connected.</li> <li>» <b>Restored:</b> A selected reader last determined to be disconnected from its communication cable is now connected.</li> <li>» <b>Interrupted or Restored:</b> A selected reader has changed from its last connection determination (either connected or disconnected) from its communication cable.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This trigger event is not detected by IC2000, IC4000 controller types.</p> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p> </div>

**Subject: Time Specific**

Trigger Event	Description
Schedule	<p>Action(s) will take place based on a timed Trigger Event.</p> <p>The units of time when the action(s) can take place are:</p> <ul style="list-style-type: none"> <li>» <b>Periodically</b></li> <li>» <b>Daily</b></li> <li>» <b>Weekly</b></li> <li>» <b>Monthly</b></li> </ul> <p>Each time unit type has <b>Start</b> and <b>End</b> fields where the range can be specified, and a <b>Perpetual</b> checkbox that makes the trigger open-ended (no end time) with no <b>End</b> time.</p> <p>In addition to a <b>Start</b> and <b>End</b> time, there are recurrence fields specific to each time unit type. The recurring events take place between the <b>Start</b> and <b>End</b> times.</p> <p>The first triggered action takes place at the specified <b>Start</b> time.</p> <hr/> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p>
<b>Subject: Other Triggers</b>	
Manual Events	<p>Where a manual event, named via the Manual Event window, may be specified.</p> <p>A manual event may be selected for one or more actions and added to one or more global reflexes. Each action in a global reflex that includes a manual event will be executed when the condition is true or when the Manual Event is selected via operator action or API command.</p> <p><a href="#">"Timeout" on the facing page</a></p> <hr/> <p><b>Note:</b> This trigger is available where a license has Advanced Global Reflexes.</p>

The following table lists the specifics available in multiple Trigger Events. The goal of these specifics is to narrow the condition set by the Trigger Event. For example, instead of just making the condition **Access Granted**, you can refine the condition to **Access Granted to a particular cardholder at a particular reader**.

To enable a Trigger Event's specific, select the checkbox to the left of the specific.



Table A-24 Trigger Event Specifics

Specific	Description
Timeout	<p>This specific is available for all Event triggers except <b>Schedule</b>. If the condition specified in the trigger event is not received by the GuardPoint10 system before the timeout expires, the actions assigned to the global reflex will not take place.</p> <div style="background-color: #4a90e2; color: white; padding: 10px; border-radius: 5px;"> <p><b>Timeout sample use</b></p> <p><b>Create a simple global reflex with the following:</b></p> <p>Trigger Event: <b>Access denied</b> with a Denied reason: <b>Stolen card</b>. Set the Timeout to <b>5 minutes</b>.</p> <p>Action: Display message on PC with the message text, <b>"Someone is trying to use a stolen badge."</b></p> <p><b>How it works under the following three circumstances:</b></p> <ul style="list-style-type: none"> <li>- Swipe a badge, with a status of <b>Stolen</b>, at a reader. The PC message will appear.</li> <li>- Disconnect the reader's controller from the network and swipe a badge, with a status of <b>Stolen</b>, at a reader. Reconnect the controller to the network within 5 minutes of the trigger event taking place. The PC message will appear.</li> <li>- Disconnect the reader's controller from the network and swipe a badge, with a status of <b>Stolen</b>, at a reader. Reconnect the controller to the network <i>6 minutes</i> after the trigger event takes place. The PC message will <i>not</i> appear.</li> </ul> <p>Regardless of the circumstance, the Trigger Event will appear in the Event log.</p> </div>
Denied Reason	<p>This specific is only available for Denied Access Trigger Events. It allows you to specify the cause of the denied access event (i.e. Card Stolen or Cardholder Invalid). The reason that must be true to trigger the <b>THEN</b> action may be selected from the specific's drop-down list.</p>
Transaction Code	<p>This specific is only available for Access Granted Trigger Events. To make the condition true, the reader, where access is attempted, transmits a transaction code along with the cardholder's badge data to the controller. The transaction code value that must be true to trigger the <b>THEN</b> action may be selected from the specific's drop-down list.</p>

Specific	Description
Controller	This specific is available for a Box Opened Trigger Event. To make the condition true, the controller, where access is attempted, must be one of the controllers selected for this specific's Select Controllers dialog. The Select Controllers dialog is displayed after you click the down-arrow in the <b>Select Controllers</b> field.
Reader	This specific is available for Denied Access, Access Granted, and Connected Reader Trigger Events. To make the condition true, the reader, where access is attempted, must be one of the readers selected for this specific's Select Readers dialog. The Select Readers dialog is displayed after you click the down-arrow in the <b>Select Readers</b> field.
Cardholder	This specific is available for Denied Access and Access Granted Trigger Events. To make the condition true, the cardholder attempting to gain access must be one of the selected cardholders for this specific. Cardholders may be selected from the Select Cardholder dialog that is displayed after you click the down-arrow in the <b>Select Cardholders</b> field.
Department	This specific is available for Denied Access and Access Granted Trigger Events. To make the condition true, the cardholder attempting to gain access must be assigned to one of the selected departments for this specific. A department may be selected from the list that is displayed after you click the down-arrow in the <b>Select Department</b> field. Multiple departments can be selected from the list with the <b>Shift</b> or <b>Ctrl</b> keys on the keyboard.
Input	This specific is available for Alarm Trigger Events. The input specific selected, determines which input must be under alarm to make the Alarm trigger event true.
Alarm Zone	This specific is available for Alarm Trigger Events. The Alarm Zone specific selected, determines that any input in the Alarm Zone must be under alarm to make the Alarm trigger event true.
Start/End/Perpetual/Recur every	<p>These specifics are available for the Schedule Trigger Event. They are used to determine the range of the schedule and the frequency of the action(s) applied to it.</p> <div data-bbox="467 1489 1473 1908" style="background-color: #4a90e2; color: white; padding: 10px;"> <p><b>Schedule Use Example</b></p> <p>A Daily schedule trigger event with the following specifics:</p> <p>Start on April 1, 2018, at 11:30 AM and is Perpetual with a Recurrence of 2 days. This schedule trigger has an action that will show a message "Cafeteria is open".</p> <p>What this means is that every other day at 11:30 AM, a message will appear on all PCs running GuardPoint10 stating that the Cafeteria is open.</p> </div>

**Note:** If you have selected one or more controllers, readers, inputs, or cardholders the number of selections will appear to the right of the respective field. Click on the number of selections to see a list of exactly what or who was selected.

## THEN statement pane (action)

If all of the specifics of one of the **IF** panes' defined Trigger Events are true, all of the action(s) in the **THEN** pane will take place.

### How to read a Global Reflex's THEN pane

The order in which the actions appear in the **THEN** pane is not relevant. The actions will be executed when the Trigger Event is true.

The screenshot shows a software interface for configuring a 'THEN' pane. On the left is a list of action categories: Alarms, Cardholders, Relay Actions, Reports, User Interface Actions, Video, and Other Actions. The 'THEN' pane itself contains three actions: 'Display message on PC' (with a parameter 'Denied access events at Reception requires attention'), 'Send Free Command', and 'Cardholder status' (with a parameter 'Select Cardholders' and a value of '3 Cardholder(s) selected'). A 'Test Actions' button is visible in the top right. Callouts provide the following information:
 

- A list of actions that may be added to the THEN pane with a simple drag & drop.
- Expandable/Collapsible actions that have been added to the THEN pane.
- All actions in the THEN pane may be invoked, regardless of the trigger events state, via the Test Actions button.
- Each action includes parameters that determine the action's behavior. These parameters are visible when an action is expanded.

Each action type has its own fields that set the behavior of the action.

The following table contains the action options available for the **THEN** pane grouped by subject. The list of Action subjects can be collapsed or expanded via the large arrow buttons above the list.

Table A-25 **THEN** Actions

Action	Description
<b>Subject: Alarms</b>	

Action	Description
Alarm Zone Operations	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, one of the following selected actions is performed:</p> <ul style="list-style-type: none"> <li>» <b>Cancel Temporary Action:</b> When all of the specifics of a Trigger Event condition in the <b>IF</b> pane is true and a temporary action is taking place in the Alarm Zone Security screen, the temporary action will be terminated. If all of the specifics of a Trigger Event condition in the <b>IF</b> pane is true and a temporary action is not taking place, the inputs will be governed by the alarm zone's designated Weekly Program. For information about the Alarm Zone Security screen, see <a href="#">"Overriding an Alarm Zone's Status" on page 366</a>.</li> <li>» <b>Return to Weekly Program:</b> When all of the specifics of a Trigger Event condition in the <b>IF</b> pane is true, the input is governed by the alarm zone's designated Weekly Program.</li> <li>» <b>Arm &gt; Arm duration:</b> The selected alarm zone's input(s) are armed for a specified amount of time. The fields where the armed time is specified appears to the right of the <b>Arm duration</b> selection. While armed, inputs can send alarm transactions to the system.</li> <li>» <b>Arm &gt; Arm constantly:</b> The selected alarm zone's input(s) are armed indefinitely. To change the armed status of the input, go to the Security task group and open the Alarm Zone Security screen (see <a href="#">"Overriding an Alarm Zone's Status" on page 366</a>). While armed, inputs can send alarm transactions to the system.</li> <li>» <b>Arm &gt; Arm until next time zone:</b> The selected alarm zone's input(s) are armed until the time zone changes (from a green period to a white period or from a white period to a green period). For information about green and white periods, see <a href="#">"Time Zones" on page 113</a>. While armed, the inputs can send alarm transactions to the system.</li> <li>» <b>Disarm &gt; Disarm duration:</b> The selected alarm zone's input(s) are disarmed for a specified amount of time. The fields where the disarmed time is specified appears to the right of the <b>Disarm duration</b> selection. While disarmed, the inputs are unable to send alarm transactions to the system.</li> <li>» <b>Disarm &gt; Disarm constantly:</b> The selected alarm zone's input(s) are disarmed indefinitely. To change the disarmed status of the input, go to the Security task group and open the Alarm Zone Security screen (see <a href="#">"Overriding an Alarm Zone's Status" on page 366</a>). While disarmed, the inputs are unable to send alarm transactions to the system.</li> <li>» <b>Disarm &gt; Disarm until next time zone:</b> The selected alarm zone's input(s) are disarmed until the time zone changes (from a green period to a white period or from a white period to a green period). For information</li> </ul>

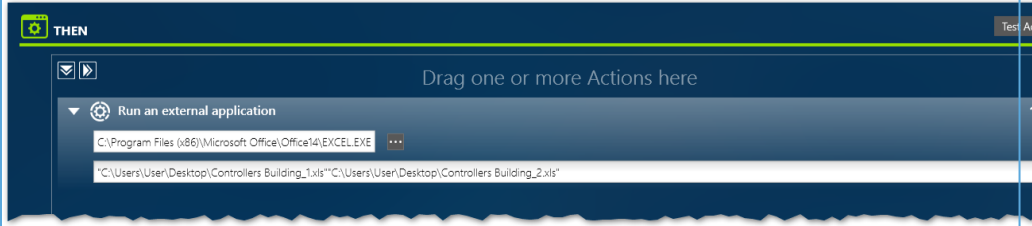
Action	Description
	<p>about green and white periods, see <a href="#">"Time Zones"</a> on page 113.</p> <p>While disarmed, the inputs are unable to send alarm transactions to the system.</p>
Galaxy Group Operations	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the selected Galaxy Group's "set" operation is performed.</p> <hr/> <p><b>Note:</b> This action is only relevant when a Galaxy system is integrated into your GuardPoint10 system.</p> <p>This action is available where a license has Advanced Global Reflexes.</p>
Simulate an Input	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, this action informs the controller of a simulated change in an input's state for a specified time. The actual state has not changed, but for the time specified, the controller behaves as if it has changed.</p>
<b>Subject: Cardholders</b>	
Cardholder Status	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the specified list of cardholders will be set to valid or invalid. The change depends on whether this action's <b>Valid</b> field is set to <b>Yes</b> or <b>No</b>.</p> <hr/> <p><b>Note:</b> This action is available where a license has Advanced Global Reflexes.</p>
<b>Subject: Relay Actions</b>	

Action	Description
Activate/Deactivate Relays	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, one of the following selected actions is performed on the specified relay(s):</p> <ul style="list-style-type: none"> <li>» <b>Activate Relays Continuously:</b> The selected relays will be unlocked until an operator changes the action via another Global Reflex or the Alarm Zone Security screen (see <a href="#">"Overriding an Alarm Zone's Status" on page 366</a>).</li> <li>» <b>Deactivate Relays Continuously:</b> The selected relays will be locked until an operator changes the action via another Global Reflex or the Alarm Zone Security screen (see <a href="#">"Overriding an Alarm Zone's Status" on page 366</a>).</li> <li>» <b>Return All Relays to Normal:</b> The selected relays will be in their defined normal state. The normal state is determined by the Weekly Program assigned to the relays.</li> <li>» <b>Activate Relay For:</b> The selected relays will be unlocked for a specified number of seconds. Specify the number of seconds in the <b>Activate the Relay For</b> action's accompanying time field.</li> </ul> <p>To specify the relay(s) where the action will be applied, select a relay(s) from the Select Relays dialog that displays after you click the down-arrow in the <b>Select Relays</b> field.</p>
Unlock All Doors	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, one of the following selected actions is performed on all relays on the site:</p> <ul style="list-style-type: none"> <li>» <b>Activate All Door Relays:</b> All relays on the site will be unlocked until an operator changes the action via another Global Reflex or the Alarm Zone Security screen (see <a href="#">"Overriding an Alarm Zone's Status" on page 366</a>), or a different Global Reflex changes the relay states.</li> <li>» <b>Return All Door Relays to Normal :</b> All relays on the site will be put in their defined normal state. The normal state is determined by the Weekly Program assigned to each relay.</li> <li>» <b>Activate All Relays For:</b> All relays on the site will be unlocked for a specified number of seconds. Specify the number of seconds in the <b>Open All Relays For</b> action's accompanying time field.</li> </ul>
<b>Subject: Reports</b>	
Create Template-based report	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the specified template may be saved as an Excel file or PDF output file. The file can also be emailed as an attachment.</p> <p>The PDF output file option is not available for right-to-left languages.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This action is available where a license has Advanced Global Reflexes.</p> </div>

Action	Description
Display Area Report on PC	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the specified Area Report is displayed on workstations, where GuardPoint10 is running.</p> <hr/> <p><b>Note:</b> This action is available where a license has Advanced Global Reflexes.</p>
Send an Area Report via Email	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, an email with an attached real-time Area Report, for the specified areas, will be sent to the email address(es) entered.</p> <p>All of the fields in the email may be edited. Each selected Report in the <b>Area(s) in Report</b> drop-down list will have its own individual email; one attached report per email.</p> <p>Sending an email to multiple email addresses requires a semi-colon separator (";") between addresses.</p> <hr/> <p><b>Note:</b> To invoke an email action, the <b>SMTP Mail Server</b> settings must be completed. These settings are found in the Options &gt; System &amp; SQL screen. For more information, see "<a href="#">SMTP Mail Server</a>" on page 581.</p> <p>This action is available where a license has Advanced Global Reflexes.</p>
<b>Subject: User Interface Actions</b>	
Display Message on PC	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the text entered in the message field displays on the screens, where GuardPoint10 is running.</p> <p>The displayed message can contain dynamic information about the trigger event (i.e. the name of the controller where the event took place). The dynamic codes available are as follows (without quotes):</p> <ul style="list-style-type: none"> <li>» Cardholder Name = "%ch%"</li> <li>» Reader Name = "%reader%"</li> <li>» Reader UID = "%readerUID%"</li> <li>» Input Name = "%input%"</li> <li>» Input UID = "%inputUID%"</li> <li>» Controller Name = "%controllerName%"</li> <li>» Controller UID = "%controllerUID%"</li> <li>» Log Date = "%logDate%"</li> </ul> <p>A sample message with dynamic content is:</p> <p><b>%ch% just entered the office from %reader%.</b></p>

Action	Description
Play a Sound	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the selected system sound will play.</p> <p>» To select a standard sound built-in to the PC, click the down-arrow in the <b>Select Sound File</b> field and choose the sound that will play.</p>
<b>Subject: Video</b>	
Send Message to NVR	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the text entered in the message field to the specified NVR.</p> <p>The message must end with "<b>&lt;EOF&gt;</b>".</p> <p>This message can contain dynamic information about the trigger event (i.e. the name of the controller where the event took place). The dynamic codes available are as follows (without quotes):</p> <ul style="list-style-type: none"> <li>» Cardholder Name = "%ch%"</li> <li>» Reader Name = "%reader%"</li> <li>» Reader UID = "%readerUID%"</li> <li>» Input Name = "%input%"</li> <li>» Input UID = "%inputUID%"</li> <li>» Controller Name = "%controllerName%"</li> <li>» Controller UID = "%controllerUID%"</li> <li>» Log Date = "%logDate%"</li> </ul> <p>A sample message with dynamic content and closing code is:</p> <p><b>Hello world from %ch%. &lt;EOF&gt;</b></p>
<b>Subject: Other Actions</b>	
Backup Database	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the Main database, the Journal or, both are backed up on the SQL Server.</p> <hr/> <p><b>Note:</b> This action is available where a license has Advanced Global Reflexes.</p> <hr/>
Insert Comment in Journal	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the text entered in the comment field is recorded in the Event Table Log.</p>



Action	Description
<p>Run an External Application</p>	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> area are true, the external application entered in the Application field will open with arguments parsed from the Parameters field.</p> <div data-bbox="406 338 1469 689" style="background-color: #4F81BD; color: white; padding: 10px;"> <p><b>Run External Application Example</b></p> <p>A controller open box event exists. The action (or one of the actions) triggered by this event will open an excel spreadsheet with detailed information about each controller in the system.</p> <p>The case above would require the following information in the <b>Run External Application</b> action fields:</p> </div>  <p>The top field specifies the path to the Excel application on the Server installation machine. The second field specifies the Controller Info file path (the path must be in quotation marks) that will be opened automatically in Excel.</p> <p><b>Note:</b> This action is only relevant in the GuardPoint10 Server installation, where the Server installation has the external application installed locally and parameters are available.</p> <p>When triggered, this action will only run on the GuardPoint10 Server installations.</p> <p>This action is available where a license has Advanced Global Reflexes.</p>
<p>Run SQL Script (may not be visible)</p>	<p>A collection of SQL commands that are stored in a text file and perform some GuardPoint10 operation or task. The script can be targeted to the Main database, the journal or, both. The script can also be specified as a stored procedure.</p> <p>This action should be added by a developer with a knowledge of SQL and intimate knowledge of GuardPoint10.</p> <p>This action is only available when the Options &gt; System &amp; SQL screen's <b>Display SQL script action in Global Reflex</b> setting is set to <b>Yes</b>.</p> <div data-bbox="406 1794 1469 1899" style="background-color: #F0E68C; padding: 10px;"> <p><b>Note:</b> This action is available where a license has Advanced Global Reflexes.</p> </div>

Action	Description
Send an Email	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the email will be sent to the specified email address(es).</p> <p>All of the fields in the email may be edited.</p> <p>Sending an email to multiple email addresses requires a semi-colon separator (";") between addresses.</p> <p>An email may contain dynamic information about the trigger event (i.e. the name of the controller where the event took place). This dynamic information may be in the subject or body of an email. The dynamic codes available are as follows (without quotes):</p> <ul style="list-style-type: none"> <li>» Cardholder Name = "%ch%"</li> <li>» Reader Name = "%reader%"</li> <li>» Reader UID = "%readerUID%"</li> <li>» Input Name = "%input%"</li> <li>» Input UID = "%inputUID%"</li> <li>» Controller Name = "%controllerName%"</li> <li>» Controller UID = "%controllerUID%"</li> <li>» Log Date = "%logDate%"</li> </ul> <p>A sample message with dynamic content is:</p> <p><b>%ch% just entered the office from %reader%.</b></p> <hr/> <p><b>Note:</b> To invoke an email action, the <b>SMTP Mail Server</b> settings must be completed. These settings are found in the Options &gt; System &amp; SQL screen. For more information, see <a href="#">"SMTP Mail Server" on page 581</a>.</p> <p>This action is available where a license has Advanced Global Reflexes.</p>
Send Free Command	<p>When all of the specifics of a Trigger Event condition in the <b>IF</b> pane are true, the command specified is sent to the specified controller.</p> <p>This action requires technical knowledge not readily available to a typical GuardPoint10 operator.</p> <p>This action is only available when the Options &gt; System &amp; SQL screen's <b>Debug by Diagnostic</b> setting is set to <b>Yes</b>.</p> <hr/> <p><b>Note:</b> This action is available where a license has Advanced Global Reflexes.</p>



**Note:** If you have selected one or more relays or one or more inputs, the number of selections will appear to the right of the respective field. Click on the selected number to see a popup list of exactly what was selected.

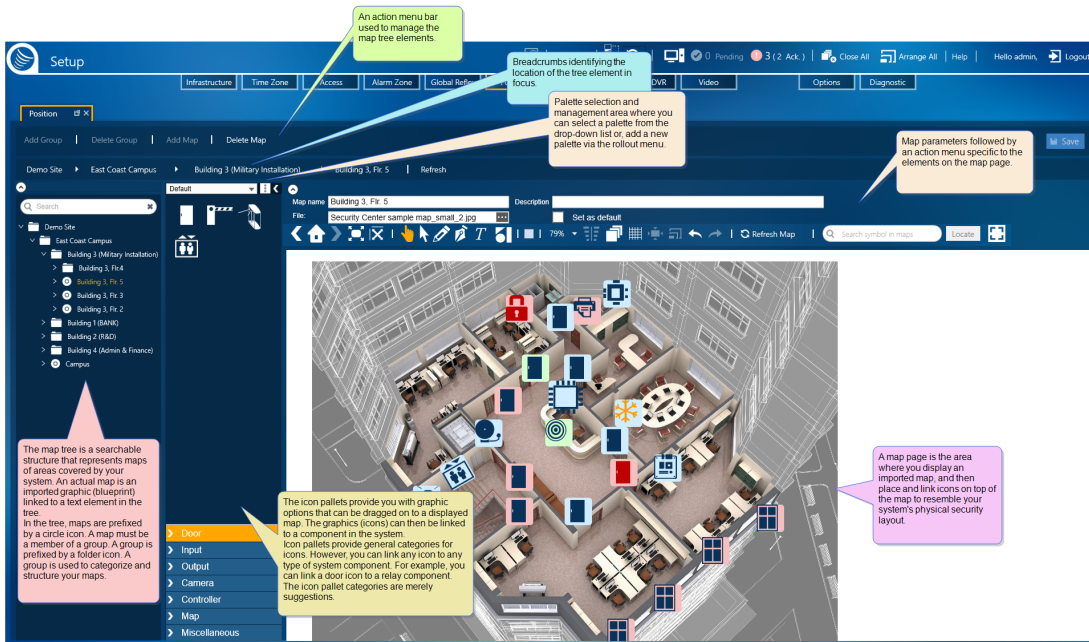
To verify the reflex action is operating correctly, at various stages, click the **TEST** button at the top right of the **THEN** pane and observe the results.

Beware, if you are testing the **Send an Email** action, the email will be sent to all listed addresses.



# Position Screen

Figure A-45



The Position screen provides the tools necessary to build your Security Center screen's map pages. Add layers of icons, shapes, and textboxes on top of a floor plan or map. Link icons to various parts of your system (controllers, readers, inputs, cameras, etc.). Link, shapes, and textboxes to maps, alarm zones, areas or, nothing at all.

The goal is to approximate the physical layout of your system and allow security personnel (operators) to easily detect changes and drill down to relevant information about the changes. By placing each icon on a map layer, where its physical counterpart is located in the real world, an operator can detect changes and patterns, and quickly take any required action based on the nature of an event and its proximity to sensitive areas.

The Position screen has five distinct areas:

## Searchable tree of maps

The map tree reveals the structure of your map groupings and allows you to open a map with a simple click. Alternatively, you can navigate to subsequent maps via the arrows in the **breadcrumbs**<sup>1</sup> found above the tree search field.

The initial default group derives its name from the site name found in the Infrastructure tree (see "Site Details" on page 443).

A map must be in a group (folder). A group may have multiple maps and multiple sub-groups. The purpose of a group is to create a logical structure for the maps.

A map can have sub-maps, but not sub-groups.

<sup>1</sup>A graphical control element used as a navigational aid in GuardPoint10' GUI. It allows operators to keep track of their current location.

## Tree & Map action bar

This action bar provides the operator with the tools necessary to add groups and maps to the map tree or delete groups and maps from the tree.

A group can only be deleted if it doesn't have any sub-groups or sub-maps.

A map can only be deleted if it doesn't have sub-maps.

The commands available in the tree map action bar can also be found in the context menu of an element in the tree. For example, right-click on a map element; a context menu appears with an Add map and a Delete map item.

## Pallet panel

Figure A-46



A pallet holds stencils for Doors, Inputs, Relays (Output), Controllers, Maps, Cameras, and Miscellaneous items. A stencil contains icons related to the stencil label. For example, the Default palette Door stencil contains icons for various types of doors (i.e. standard, revolving, gate, etc.).

**Note:** If your GuardPoint10 system includes an integrated Galaxy panel, elements from the panel can be placed on a map via a relevant stencil, like any GuardPoint10 element.

A Galaxy panel may be linked to a Controller stencil icon.

A Galaxy group may be linked to a Miscellaneous stencil icon, a shape, or a textbox.

A Galaxy zone may be linked to an Input stencil icon.

Additional (custom) palettes may be added at any time. The stencils in these custom palettes may include duplicate icons from other palettes, as well as, new icons created via a third-party product called Inkscape.

For information about creating icons via Inkscape, see "[Create XAML icons for Custom Palettes](#)" on [page 269](#).

The palette where you may drag an icon is selected from the Palette drop-down list at the top of the panel.

Palettes are managed from the rollout menu to the right of the Palette drop-down list. The palette management options are as follows:

- » Add a new palette
- » Rename an existing palette
- » Duplicate an existing palette
- » Delete a palette
- » Import a palette
- » Export a palette

From any palette other than the Default palette, icon management may be performed. This includes adding, editing, and deleting an *icon set* from a palette stencil. An icon set includes all variations of a palette icon and icon overlays specific to the icon set. Icon management takes place via the Add / Edit Symbol window.

To access the Icon Management window, display the relevant stencil and do one of the following:

» Click the Add Icon button .

» Right-click an existing icon, and then select **Edit** from the context menu.

## The Icon Management (Add / Edit Symbol) window is displayed.

Figure A-47

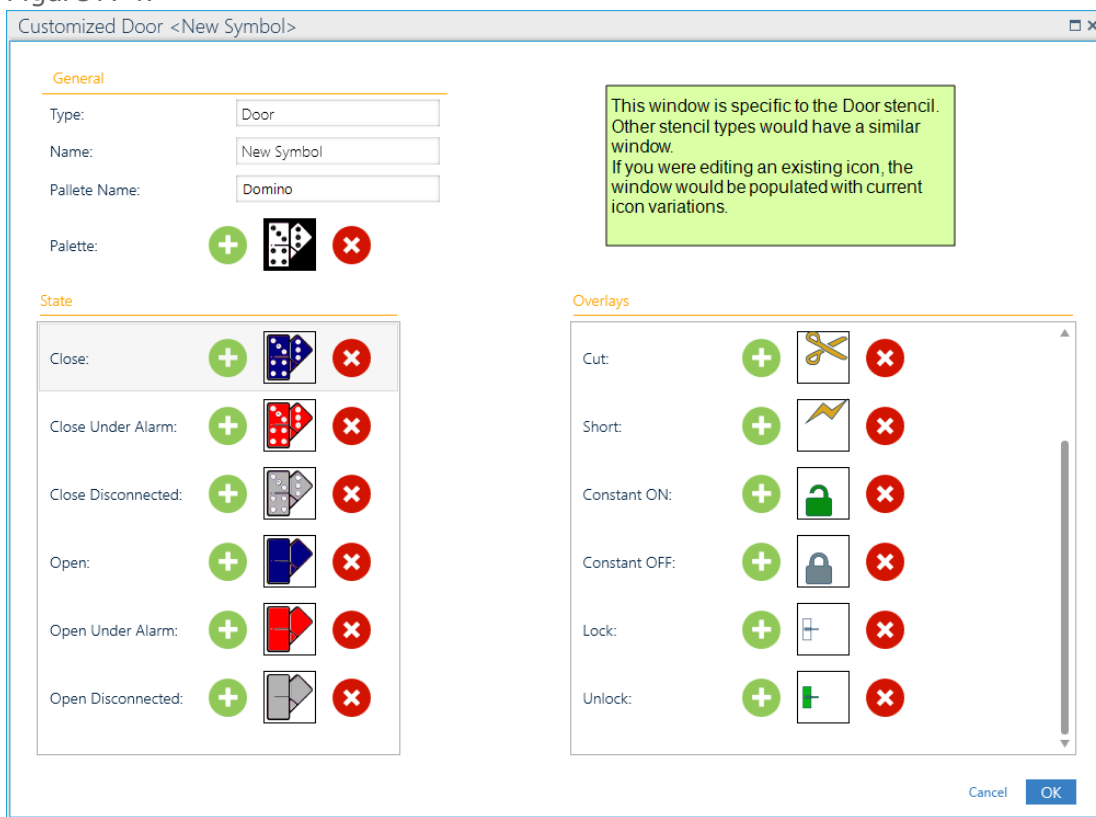


Table A-26 General Area of the Icon Management Window

Name	Description
Type	Name of the stencil where the icon set will be accessible (read-only).
Name	Name of the icon set. In the stencil, this name will be used as a tooltip for the icon.

Name	Description
Palette Name	Name of the custom palette where the stencil and icon set are located (read-only).
Palette	Displays a Thumbnail of the loaded icon that will appear in the stencil. In addition, a Load and Remove button is located on either side of the thumbnail, these buttons allow you to select a different icon.

The State area of the Icon Management window.

This area may vary depending on the stencil selected. For example, a Map stencil would only have a Normal and Under Alarm state.

**Table A-27** State Area of the Icon Management Window

Name	Description
Close	Symbol variation that appears when an element linked to the icon is closed. Applicable to Type: Door, Input, Output (Relay).
Close Under Alarm	Symbol variation that appears when an element linked to the icon is closed and under alarm. Applicable to Type: Door, Input, Output (Relay).
Close Disconnected	Symbol variation that appears when an element linked to the icon was last determined to be closed, but is no longer connected to the controller. Applicable to Type: Door, Input, Output (Relay).
Open	Symbol variation that appears when an element linked to the icon is open. Applicable to Type: Door, Input, Output (Relay).
Open Under Alarm	Symbol variation that appears when an element linked to the icon is open and under alarm. Applicable to Type: Door, Input, Output (Relay).
Open Disconnected	Symbol variation that appears when an element linked to the icon was last determined to be open, but is no longer connected to the controller. Applicable to Type: Door, Input, Output (Relay).
Symbol	An icon variation applicable to a Camera icon. Applicable to Type: Camera.
Normal	Symbol variation that appears when an element linked to the icon may only have two states (linked and not linked) The <b>Normal</b> icon variation appears when the element is linked. Applicable to Type: Controller, Map, Miscellaneous.

Name	Description
Disconnected or Deactivated	Symbol variation that appears when a Controller element linked to the icon is not connected to the system or deactivated. Applicable to Type: Controller.
Under Alarm	Symbol variation that appears when an element linked to the icon is under alarm or has member elements under alarm. For example, a map icon would appear under alarm if an icon on that map is under alarm. Applicable to Type: Map, Miscellaneous.
Galaxy Pending	Symbol variation that appears when a Miscellaneous icon, shape, or textbox is linked to a Galaxy element with a pending alarm. Applicable to Type: Miscellaneous.
Galaxy Disconnected	Symbol variation that appears when a Miscellaneous icon, shape, or textbox is no longer linked to a Galaxy group. Applicable to Type: Miscellaneous, shapes, and textboxes.

The Overlay area of the Icon Management window.

This area may vary depending on the stencil selected. For example, a Map stencil would only have an Alarm overlay while an input would have many more overlays (i.e. Alarm, Delayed Alarm, Cut, Short, Constant ON, Constant OFF, etc.).

Any changes to an overlay apply only to the icon set currently displayed.

**Table A-28** *Overlay Area of the Icon Management Window*

Name	Description
Alarm	Symbol that appears over an icon when an element linked to the icon changes due to a triggered alarm. Applicable to Type: Door, Input, Map, Miscellaneous.
Delayed Alarm	Symbol that appears over an icon when an element linked to the icon changes due to a triggered alarm, but the element's details are set up with a delay time. Applicable to Type: Door, Input.
Cut	Symbol that appears over an icon when an element linked to the icon has a wire connected to the controller cut. When triggered from an input, the Cut overlay will remain on the icon until the issue is resolved. Applicable to Type: Door, Input.



Name	Description
Short	<p>Symbol that appears over an icon when an element linked to the icon has a short in a wire connected to the controller.</p> <p>When triggered from an input, the Short overlay will remain on the icon until the issue is resolved.</p> <p>Applicable to Type: Door, Input.</p>
Constant ON	<p>Symbol that appears over an icon when the element linked to the icon has been manually set to Constant ON.</p> <p>Applicable to Type: Door, Input, Output (Relay).</p>
Constant OFF	<p>Symbol that appears over an icon when the element linked to the icon has been manually set to Constant OFF.</p> <p>Applicable to Type: Door, Input, Output (Relay).</p>
Lock	<p>Symbol that appears over an icon linked to a door that is locked.</p> <p>Applicable to Type: Door.</p>
Unlock	<p>Symbol that appears over an icon linked to a door that is unlocked.</p> <p>Applicable to Type: Door.</p>
Box Open	<p>Symbol that appears over a Controller icon when the controller casing is opened (i.e. tampered).</p> <p>Applicable to Controllers only.</p>
Low Battery	<p>Symbol that appears over a Controller icon when the controller's internal battery has changed from 'Normal' to 'Low'.</p> <p>Applicable to Controllers only.</p>
Power Supply Failure	<p>Symbol that appears over a Controller icon when a controller last determined to be powered from a non-battery source (primary) is no longer powered from that source.</p> <p>Applicable to Controllers only.</p>
Galaxy Pending	<p>Symbol that appears over an icon linked to an input that is a Galaxy zone in a pending state.</p> <p>Applicable to Type: Input.</p>



**Note:** If an icon variation thumbnail is empty (not loaded), the background color, and any required overlay, will appear in the Security Center screen without an icon.

# Map/Group parameters and action bar

## Map/Group parameters


Contains basic information about a map page or a map group.

Depending on the focus item (map page or map group), one of the following sets of parameters is displayed:

Table A-29 Map Group Parameters

Name	Description
Group Name	<p>A free text field that identifies a map group by name. The default name of a map group is "Untitled Map Group". This is the name that will appear in the map tree.</p> <p>A best practice is to rename the map group something that identifies the grouping logic.</p> <p>The name must be unique within the context of map groups. A map group and a map page may have the same name.</p>
Description	(Optional) A free text field where information about a map group is entered.

Table A-30 Map Page Parameters

Name	Description
Map Name	<p>A free text field that identifies a map page by name. The default name of a new map page is "Untitled". This is the name that will appear in the map tree.</p> <p>A best practice is to rename the map page something that identifies the map location.</p> <p>The name must be unique; a map page cannot have the same name as another map page. However, a map page can have the same name as a map group.</p>
Description	(Optional) A free text field where information about a map page is entered.
File	<p>Opens a standard Open File dialog where the map's graphic file is selected. The file formats supported are:</p> <p>BMP, DIB, RLE, JPG, JPEG, JPE, JFIF, GIF, TIF, TIFF, PNG, WMF</p>
Set as Default (Check-box)	When selected, the current map page will automatically display when the Security Center screen is opened or when the <b>Default map</b> button  is clicked.



**Note:** To simplify the Position screen, you may choose to hide or show the map page parameters described in the table above. Click the arrow button just above the Name field label to hide the










parameters. Click the button again to show the parameters.









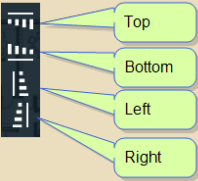

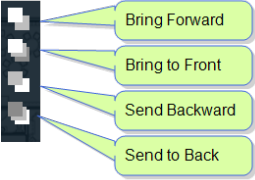

## Map page action bar






The map page action bar, found just below the map page parameters, consists of three groups of actions: Navigation, View, and Icon / Shape / Textbox.

The following table describes all of the actions available.

Table A-31 Map Page Action Bar

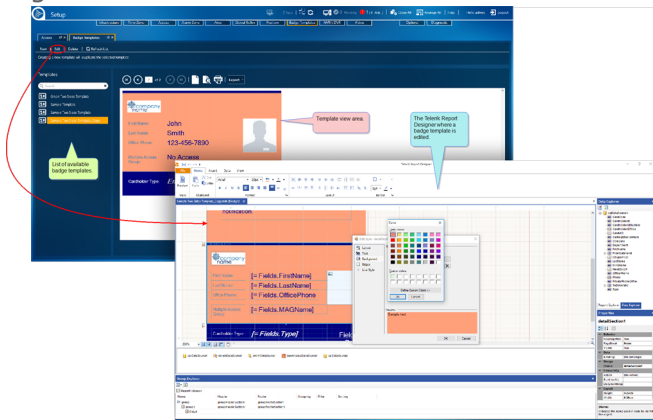
Name	Description
	Click the arrows to go to the previous or next map page in the map tree. Click the house to go to the default map page.
	The map zoom setting will automatically change to <b>Fit to Page</b> so all items on the map page are displayed.
	The map aligns to the left-top corner of the map page.
	The Pan hand moves the display in the direction of the mouse movement.
	The arrow selects icons, shapes, or textboxes.
	Lets you draw freehand shapes as if you were sketching on a map.
	Lets you draw shapes one segment at a time by placing each node with precision and controlling the shape of each line segment of the shape.
	Lets you add a textbox with a semi-transparent background color. The colors can be selected from the textbox context menu.  Click  to place the textbox on a map, and then resize the box. Click inside the textbox to change the default text. Double-click inside the box to link the box. A textbox can be linked to a map, alarm zone, or area via its symbol properties dialog (see " <a href="#">Linking an Icon, Shape, or Textbox</a> " on <a href="#">page 284</a> ).

Name	Description
	<p>Lets you add a basic shape with a background color.</p> <p>The colors can be selected from the shape's context menu.</p>  <p>Click  to select the basic shape that will be placed on a map, and then resize the shape as needed. Double-click inside the shape to link the shape. A shape can be linked to a map, alarm zone, or area via its symbol properties dialog (see <a href="#">"Linking an Icon, Shape, or Textbox" on page 284</a>).</p>
	<p>Lets you select a default semi-transparent background color for shapes. The default color will be applied to:</p>  Basic shapes  Shapes made one segment at a time  Freehand shapes
Magnification	<p>From the drop-down list, select a magnification level for the map page. The current magnification is displayed in the action bar.</p>
	<p>Enabled when two or more objects on a map page are selected.</p> <p>It aligns the selected objects according to the option selected from the Align drop-down list.</p> 
	<p>The Order drop-down list places a selected icon, shape, or textbox in front or behind other objects on the map page.</p>  <p>When you have two or more objects overlapping each other, the effect of the order option becomes apparent.</p>
	<p>Show or hide a grid over the map. When in Show mode, the grid overlays the map and makes it easier to line up selected icons, shapes or, textboxes.</p>

Name	Description
	<p>Enabled when the grid over the map is visible and at least one object on the map page is selected.</p> <p>Moves the selected object to align with the nearest grid line.</p>
<p>Group (Only available from a context menu when multiple objects are selected)</p>	<p>Groups or ungroups multiple objects. When grouped, position settings may be applied to the group as a whole. When ungrouped, position settings and properties may be applied individually.</p>
	<p>Duplicates the currently selected object(s). Visually, the objects are identical, but a duplicate does not inherit the properties of the original object. For more information, see "<a href="#">Linking an Icon, Shape, or Textbox</a>" on page 284.</p>
	<p>Repeats the last action performed before <b>Undo</b> was clicked.</p>
	<p>Reverses the previous action (undo).</p>
<p>Locate</p>	<p>The locate field is part of the find tool. Enter text in the field, and then open the field's drop-down list. Objects in the Graphic Module that contain the text will appear on the list.</p> <p>Select one of the objects listed and click the <b>Locate</b> button. The map page, where the object is located, is displayed and the object in question is placed in focus.</p>
	<p>Displays a map in full screen / Exit full screen. To accommodate the full screen view, other panes on the screen will be collapsed.</p>

# Badge Templates Screen

Figure A-48



**Note:** This topic is only relevant for GuardPoint10 installations that include the Badge Template module. For information about the Badge Template module, see ["Badge Templates" on page 293](#).

The Badge Templates screen is where badge templates are created. GuardPoint10's built-in template is not editable. To create a new template, duplicate an existing built-in or operator-built template and edit the duplicate template's content via the Telerik Report Designer.

A badge template is assigned to a cardholder Type. This means that cardholders of the same Type (i.e. Employee) will have badges of the same design. The Type assignment is made via the **New** drop-down list in the Cardholders screen. However, an exception may exist where a cardholder is manually assigned a badge template that is not linked to the cardholder's Type. These exceptions are addressed in the cardholder's details and the Badges screen.




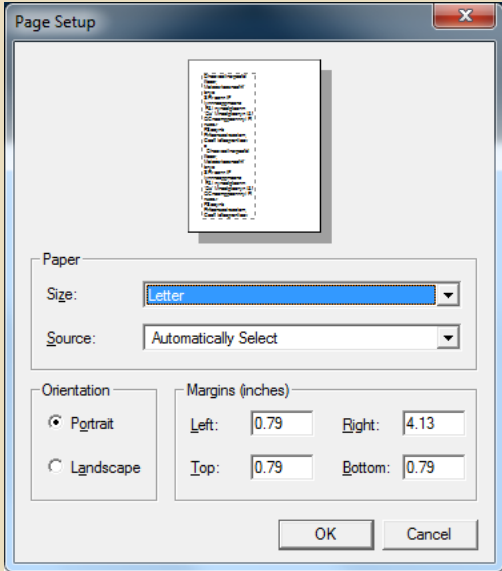

A description of the Badge Templates screen elements is provided below.


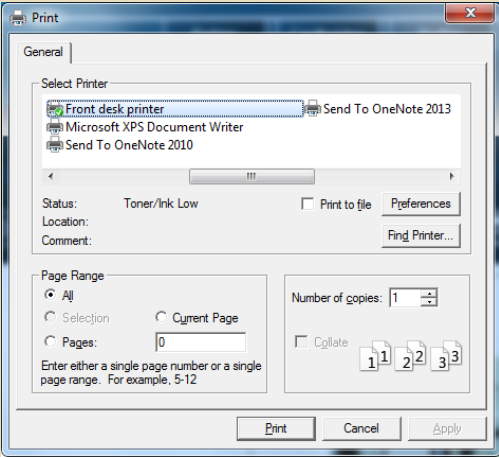
## Badge Templates Screen Elements

Parameter	Description
Template selection list	<p>A list of templates available in GuardPoint10. There are two types of templates listed, a built-in template, and operator-built templates. An operator-built template is based on a copy of the built-in template or another operator-built template customized to fit the operator's needs.</p> <ul style="list-style-type: none"> <li>» <b>Built-in template:</b> An available badge template that may be used as a starting point for operator-built templates. The built-in template is named <b>Sample Template</b>. The template cannot be deleted or edited. It is the default template for cardholder Types.</li> <li>» <b>Operator-built templates:</b> Badge templates designed by an operator via the Telerik Report Designer. The number of templates required depends on the requirements of the organization. For example, each department may have a different badge color and a visitor badge may not include a photo of the visiting cardholder. An operator-built template starts as a duplicate of an existing template and is then customized / edited by an operator.</li> </ul>

Parameter	Description
Template View	Displays the last saved version of the template in focus. In addition, there is a toolbar above the template view window that includes pagination buttons, print-related buttons, and an Export button.
Template View Magnification	Below the Template View area is a magnification scrollbar. The scrollbar allows an operator to see a more detailed view of the displayed template.

### Badge Template Screen Toolbar

Parameter	Description
 	Pagination buttons that allow you to navigate multiple page badges.
	<p>Opens a Windows Page Setup dialog where paper, orientation, and margins may be set.</p> <p>The paper size and source options available depend on the printer where the badge will be printed.</p> <p>Figure A-49</p> 
	Displays the badge in focus on the selected paper with the page values selected in the Page Setup dialog (Print Preview).

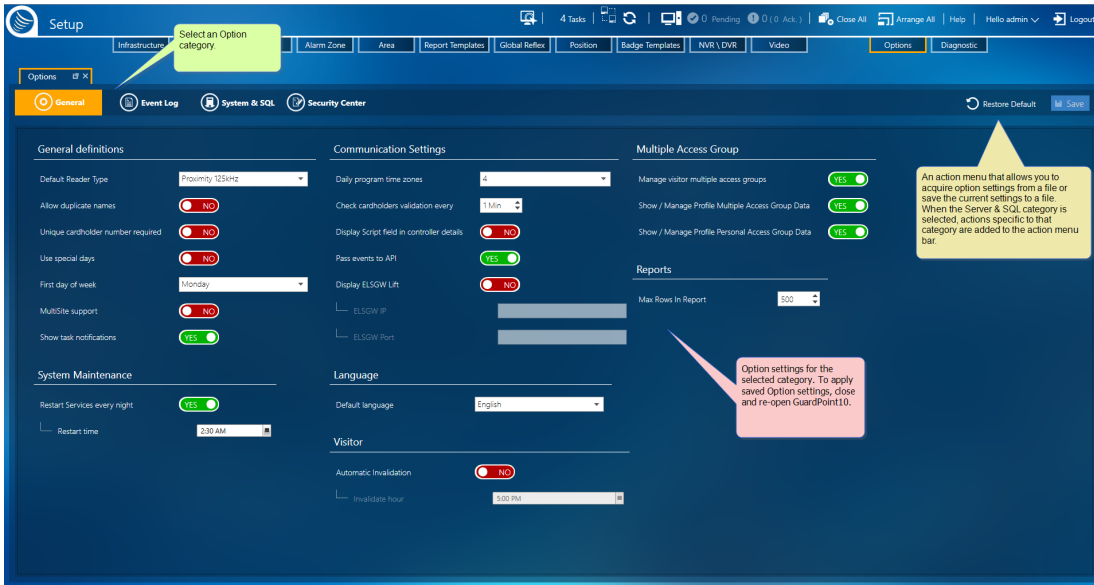
Parameter	Description
	<p>Opens a Windows Print dialog where an operator may select the printer and other print options to print the badge template currently displayed.</p> <p>Figure A-50</p> 
<div data-bbox="129 853 263 925"> <b>Export</b> </div> <ul style="list-style-type: none"> <li data-bbox="129 936 336 969">Acrobat (PDF) file</li> <li data-bbox="129 981 400 1014">CSV (comma delimited)</li> <li data-bbox="129 1025 293 1059">Excel 97-2003</li> <li data-bbox="129 1070 229 1104">TIFF file</li> <li data-bbox="129 1115 280 1149">Web Archive</li> </ul>	<p>Opens a drop-down list of formats where the data fields on the badge template displayed may be exported.</p> <p>If the template includes an image and the image is not supported in the selected export format (i.e. Excel), the image will be excluded from the export process.</p>



# Options Screen

This screen defines GuardPoint10 settings that may be altered to fit your environment and work protocol.

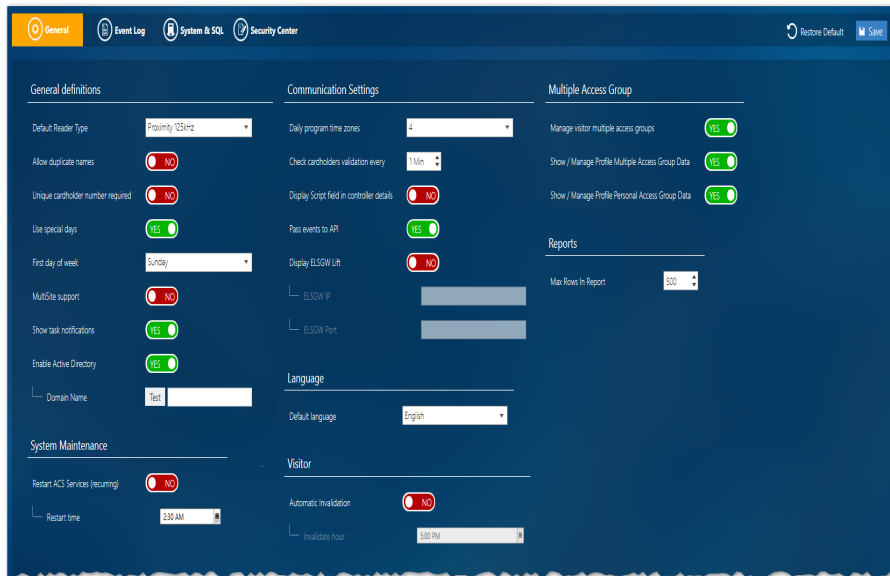
Figure A-51



The options are categorized into the following logical tabs.

## General Tab

Figure A-52



## General Tab Options

Option	Description
Default Reader Type	<p>The reader technology type set is the default for a new reader. The default technology type may be changed for an individual reader via the <a href="#">"Reader Details"</a> on <a href="#">page 453</a>.</p> <p>Default value: <b>Proximity 125kHz</b>.</p>
Allow Duplicate Names	<p>When set to Yes, cardholders with the same last and first name may coexist in the system. In this case, it is necessary to enter a unique Number per person in the cardholder details' <b>Number</b> parameter.</p> <p>Default value: <b>No</b> .</p>
Unique Cardholder Number Required	<p>Every cardholder is identified in the system by a combination of the first name, last name and number. It is recommended that this option be always set to <b>Yes</b>. However, if the <b>Allow Duplicate Names</b> option is set to Yes, then <b>Unique Cardholder Number Required</b> must be set to <b>Yes</b>.</p> <p>Default value: <b>Yes</b>.</p>
Use Special Days	<p>Adds two supplementary daily programs (S1-S2) in the Weekly Program definition.</p> <p>Default value: <b>Yes</b> .</p>
First Day of the Workweek	<p>The first day of a normal workweek.</p> <p>Default value: <b>Monday</b>.</p>
MultiSite support	<p>When set to <b>Yes</b>, enables MultiSite functionality and moves the current infrastructure to a MultiSite infrastructure.</p>
Show task notification	<p>When set to <b>Yes</b>, will show the start and end notification of a task at the bottom right of the screen.</p>
Display MultiSplit	<p>When set to <b>Yes</b>, will show MultiSplit related elements in the Infrastructure screen. This includes the <b>Split Servers</b> button in the Action bar, and the <b>Split Server</b> parameter in Network details.</p>

Option	Description
Enable Active Directory	<p>When set to <b>Yes</b>, GuardPoint10 reads <b>Active Directory</b><sup>1</sup> (Windows) user credentials (username and password) from a Windows Server where the Active Directory is located. This is the first step in allowing users to log in to GuardPoint10 with their attached Active Directory credentials instead of their GuardPoint10 user name and password.</p> <p>A Windows username is attached to an GuardPoint10 user in the Users details. The Login screen will include a <b>Login with Windows Credentials</b> button for users to log in with their Windows credentials.</p> <p>For users who do not want to log in with their Windows credentials or, are not attached to Windows credentials, the GuardPoint10 <b>User name</b> and <b>Password</b> fields are still available on the login screen along with the standard <b>LOGIN</b> button.</p>
Domain Name	Where the Active Directory is located. The organization's IT department should provide this information. Click the Test button to verify the location entered is connected.
Restart ACS Services (recurring)	(recurring)Set to <b>Yes</b> by default. This option compensates for a Windows shortcoming. It will make your system's uptime more reliable. During restart, controllers will remain operational and data will be retained.
Restart Time	Works in with <b>Restart Services Every Night</b> . Specifies the time when the restart will take place.
Daily Program Time Zones	<p>Number of green periods to allow in a Daily Program.</p> <p>The available options are 2 and 4.</p> <p>Default value: <b>2</b></p>
Check Cardholder Validation Every	<p>Number of minutes. (1 to 1440) between cardholder data validation checks. If information (i.e. time-related definitions – From/To date, Schedule Access Groups, Exceptions) needs to be added or deleted from a controller that is validating or invalidating cardholders, the corresponding cardholders' parameters are sent to the controller's local database from the system database.</p> <hr/> <p><b>Note:</b> This setting only sets the interval between checks, not the actual time at which the checks take place. Thus, when setting From/To times, to be sure that controllers are updated in time, the operator must allow for the update being sent from the server up to the specified amount of time before the value is required. (see "<a href="#">Cardholders</a>" on page 193).</p> <hr/> <p>Default frequency: <b>30 minutes</b>.</p>

<sup>1</sup>An Active Directory (AD) sits on a domain controller Server machine. Among other things, an AD authenticates and authorizes all users and computers in a Windows domain type network. When you log in to Windows with a Username and Password the Username and Password credentials are validated via the AD.

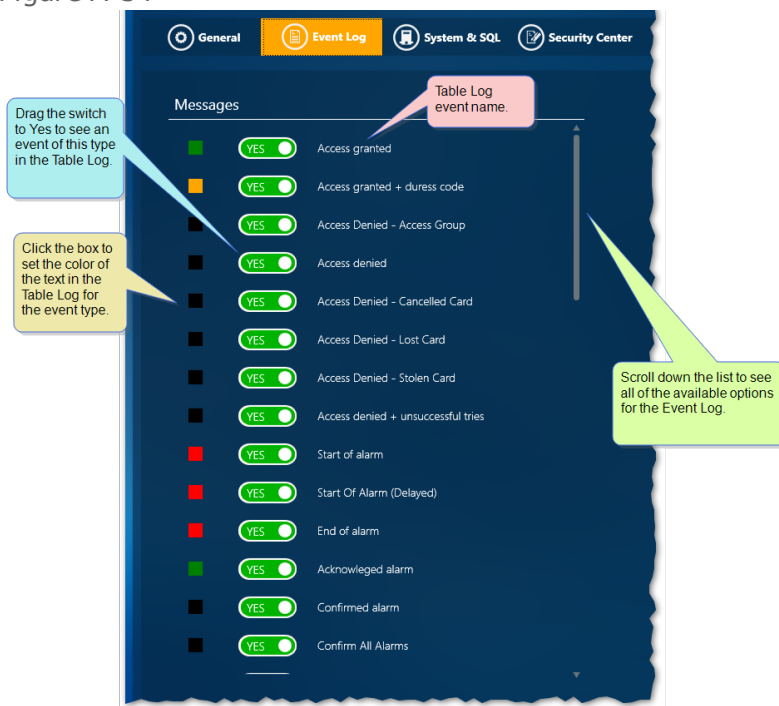
Option	Description
Skip a Repeating Alarm	<p>Reduces unnecessary alarms caused by a malfunctioning detector.</p> <p>Maximum number of seconds between repeating alarm events before an alarm is skipped is 15 seconds. If the setting is edited, the user must initialize the controller before the setting change is carried out.</p> <p>To disable this setting, set the value to zero seconds.</p> <p>Relevant for firmware newer than 18/12/2019</p>
Display Script Field in Controller Details	<p>Shows the script field in a controller's details. For more information about scripts, see <a href="#">"Controller Details" on page 450</a>.</p> <p>Default value: <b>No</b> .</p>
Pass Events to API	<p>Set this option to <b>Yes</b> when:</p> <ul style="list-style-type: none"> <li>» There is another system listening to API events.</li> <li>» Users will be working with the <b>GuardPoint10 Web module<sup>1</sup></b>.</li> </ul>
Display ELSGW Lift	<p>Allows the user to add Mitsubishi ELSGW Lift to the GuardPoint10 system via the infrastructure and Access screens.</p> <p>Default value: <b>No</b> .</p>
ELSGW IP	<p>The IP address of the Mitsubishi ELSGW Lift. Enabled when <b>Display ELSGW Lift</b> is set to <b>Yes</b>.</p>
ELSGW Port	<p>The Port of the Mitsubishi ELSGW Lift. Enabled when <b>Display ELSGW Lift</b> is set to <b>Yes</b>.</p>
Default Language	<p>The interface language of :</p> <ul style="list-style-type: none"> <li>» The currently logged-in operator and all other users except for the admin operator</li> <li>» The GuardPoint10 Login screen</li> <li>» The default language of future operators added to the system</li> </ul> <p>The default language of a specific operator may be changed at any time via the Users screen <a href="#">"Language" on page 628</a> field of the operator in focus.</p>
Automatic Invalidation	<p>When set to <b>Yes</b>, a visitor's badge will be acted upon at the time specified in the <b>Invalidate Hour</b> field.</p>
Invalidate Hour	<p>The time at which the invalidate action will take place, when <b>Automatic Invalidation</b> is set to <b>Yes</b>.</p>

<sup>1</sup>The WebApp is a limited version of the GuardPoint10 interface. It is available on any device that supports HTML5. To learn how to connect to the module, contact your provider.

Option	Description
Manage Visitor Multiple Access Groups	<p>When set to <b>Yes</b>, an <b>Is Applied to visitors</b> checkbox will be added to the Access' Multiple Access Group's screen. The checkbox will allow an operator to assign the Multiple Access Group to a cardholder visitor in the cardholders details, and adds the Multiple Access Group to the Visitor Control module.</p> <p>Figure A-53</p>  <p><b>Note:</b> The Visitor Control module may be missing from your installation. The module is an add-on that can be purchased and installed separately. If you would like to add this module, please contact your GuardPoint10 provider.</p>
Show / Manage Profile Multiple Access Group Data	<p>When set to <b>Yes</b>, a <b>Show Multiple Access Groups</b> checkbox will be added to the Profiles screen. The checkbox will allow an operator to see the Multiple Access Group associated with the operator's (user's) attached profile.</p>
Show / Manage Profile Personal Access Group Data	<p>When set to <b>Yes</b>, a <b>Show Personal Access Groups</b> checkbox will be added to the Profiles screen. The checkbox will allow an operator to see the Personal Access Groups associated with the operator's (user's) attached profile.</p>
Max. Rows in Report	<p>Any exported report (i.e. Cardholders and Badges) will be limited to the number of rows specified.</p>

# Event Log Tab

Figure A-54



The default switch value for all of the events listed below is **Yes**. This means that the events described below will be displayed in the Events screen's Table Log.

Table Event Log Options

Event	Event is stored and displayed in the Event Log screen...
Access Granted	The cardholder has presented a valid badge.
Access Granted + Duress Code	The cardholder has presented a badge and a duress code at a reader with a keypad.  <b>Note:</b> A duress code may only be used at a reader where the <b>Access Authorization</b> is set to <b>With Badge and Keypad</b> . For more information about <b>Access Authorization</b> , see " <a href="#">Reader Details</a> " on page 453.
Access Denied - Access Group	The cardholder has presented a valid badge, but the cardholder's assigned Access Group(s) does not include the reader where access is attempted or the time when access is attempted.
Access Denied	If the cardholder is denied access, due to reasons not covered by any of the other Access Denied options listed.
Access Denied - Canceled Badge	The cardholder is denied access, due to their badge having a status of <b>Canceled</b> .  The badge status can be changed via the Badges screen.

Event	Event is stored and displayed in the Event Log screen...
Access Denied - Lost Badge	The cardholder is denied access, due to their badge having a status of <b>Lost</b> . The badge status can be changed via the Badges screen.
Access Denied - Stolen Badge	The cardholder is denied access, due to their badge having a status of <b>Stolen</b> . The badge status can be changed via the Badges screen.
Access Denied + Unsuccessful tries	The cardholder is denied access after multiple attempts.
Start of Alarm	Record when an alarm is triggered in the log.
Start of Alarm: (Delayed)	When an alarm is triggered with a set delay. The delay provides a grace period that allows a cardholder to enter a code or scan their badge over a different reader/keypad device.
End of Alarm	Record when an alarm stops sounding after a defined period in the log.
Acknowledged Alarm	If an alarm has been detected by the system and acknowledged by an operator via the GuardPoint10 dashboard.
Confirmed Alarm	An alarm has been detected by the system and confirmed by an operator via the GuardPoint10 dashboard.
Confirm All Alarms	Multiple alarms have been detected by the system and a <b>Confirmed All</b> operation has been performed by an operator via the GuardPoint10 dashboard.
Line Short	The status of the line that connects a sensor/detector to a 4 State input device changes to <b>line short</b> .
Line Cut	The status of the line that connects a sensor/detector to a 4 State input device changes to <b>line cut</b> .
Table Error	A table in a controller's local database fails.
Low Battery	The backup battery in a controller is low.
Battery is OK (restored)	The battery was previously low (or not OK in some other way) and is now nominal.
Power Down	The primary power supply to a controller fails.
Power Up	The primary power supply to a controller continues to provide power after a failure ('Power Down' event).
Power Supply Failure Input Psf Closed	The Psf (the power supply component in a controller) switches off the Power supply.
Power supply OK Input Psf Opened	The Psf (power supply component in a controller) restores the Power supply to a controller, after it had switched off the Power supply (a <b>Power Supply Failure Input Psf Closed</b> event).

Event	Event is stored and displayed in the Event Log screen...
Sabotage (Box Opened)	A controller's box (casing) is opened.
Box Closed	If a controller's box (casing) is opened and afterward the status of the box changes to closed.
Communication OK	Communication check between a controller and the system is successful.
Polling Error	A controller fails to query each entity or device (i.e. reader, relay, input ), in turn, as to whether it has any data to transmit to the system database.
Satellite Alarm	<p>Relevant where a controller has relay extension cards and a relay satellite card (primarily used in Lift controllers).</p> <p>The alarm occurs when the controller fails to communicate with one of the readers connected to it.</p>
Satellite Alarm 136	<p>Relevant where a controller has relay extension cards and a relay satellite card (primarily used in Lift controllers).</p> <p>The alarm occurs when the controller fails to communicate with one of the readers connected to it for a specific reason. The number 136 is the reason ID.</p> <hr/> <p><b>Warning:</b> If this alarm occurs, contact GuardPoint10 technical support.</p>
Reader Disconnected	<p>A controller fails to communicate with a reader because the reader's wires are physically disconnected from the controller.</p> <hr/> <p><b>Note:</b> This event is not detected by IC2000, IC4000 controller types.</p>
Reader Connected	<p>A controller successfully communicates with a reader after a <b>Reader Disconnect</b> event (i.e. after the reader's wires are reconnected to its controller).</p> <hr/> <p><b>Note:</b> This event is not detected by IC2000, IC4000 controller types.</p>
User Acknowledgment	An operator acknowledges an event via the GuardPoint10 dashboard.
User Confirmation	An operator confirms an event via the GuardPoint10 dashboard.
User Comment	An operator may enter a comment on an event acknowledgment or confirmation event.
Access Denied - Unknown Badge Code	An individual attempts to access a door with a badge that is not recognized by the system.
Unknown Badge + Unsuccessful tries	An individual attempts to access a door multiple times with a badge that is not recognized by the system.

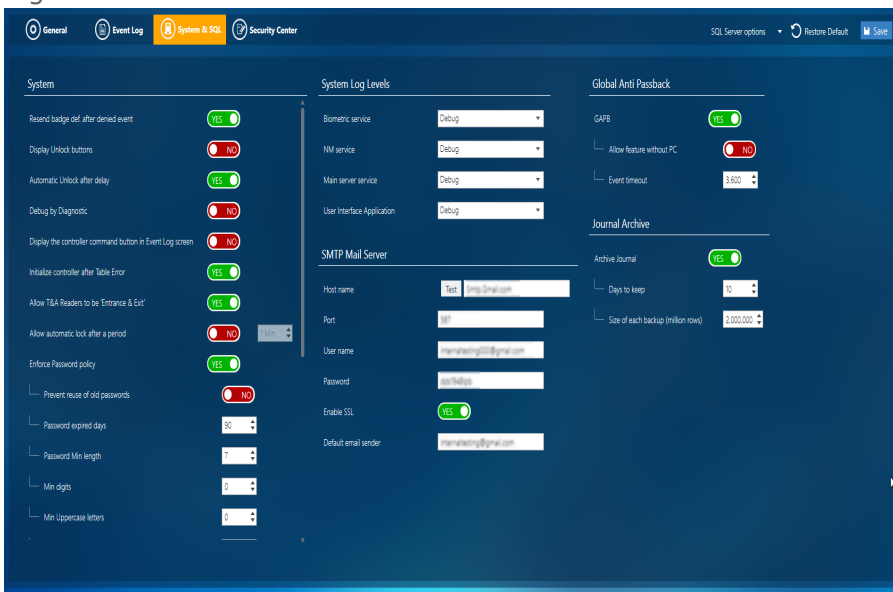


Event	Event is stored and displayed in the Event Log screen...
Non-allocated (Free) Badge	An individual attempts to access a door with a badge that is recognized by the system, but has not been assigned to a cardholder.
Application Login	An operator successfully logs in to GuardPoint10.
Application Logout	An operator successfully logs out of GuardPoint10.
Audit	An audit is initiated on a controller to determine the state of the controller's data.
Controller Command	<p>A controller is sent controller commands from the system.</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>Note:</b> If a controller doesn't acknowledge these commands (usually due to a communication problem), the commands are left as pending in the controller buffer, and are cleared as soon as the communication is restored. Pending commands can be viewed via the GuardPoint10 dashboard.</p> </div>
Controller is between 80% and 90% full	A controller's memory is at or approaching 90% Controller is more than 90% full.
Controller is more than 90% full	A controller's memory is approaching 100% capacity.
Biometric Reader Connected	A biometric reader is connected communicating and polling the GuardPoint10 system.
Biometric Reader Disconnected	A biometric reader is that was previously connected is no longer connected communicating and polling the GuardPoint10 system.
Global Reflex	A Global Reflex event occurs. A Global Reflex is an operator-specified event that triggers an operator-defined process. For example, If the last cardholder in an Access Group space leaves (the event), the lights in that space automatically turn off (the process).
Global Reflex Test	A Global Reflex Test event occurs via the <b>TEST</b> button on the Global Reflex screen. It executes one or more actions assigned to a condition though the actual condition does not exist.
Galaxy Message	A Galaxy event occurred. For more information about Galaxy systems, see <a href="#">"Integrating a Galaxy System into the Infrastructure"</a> on page 82.
Clean up Internal Logs - Succeeded	A regularly scheduled internal database maintenance operation was successfully performed.
Clean up Internal Logs - Failed	A regularly scheduled internal database maintenance operation was unsuccessful.
Clean up old completed jobs - Succeeded	A regularly scheduled internal job maintenance operation was successfully performed.

Event	Event is stored and displayed in the Event Log screen...
Clean up old completed jobs - Failed	A regularly scheduled internal job maintenance operation was unsuccessful.
Run SQL Script in Database - Succeeded	Related to the Global Reflex action Run SQL script. Log entry is performed when the script ran successfully in the database.
Run SQL Script in Database - Failed	Related to the Global Reflex action Run SQL script. Log entry is performed when the script ran unsuccessfully in the database.
Run SQL Script in Journal - Succeeded	Related to the Global Reflex action Run SQL script. Log entry is performed when the script ran successfully in the journal.
Run SQL Script in Journal - Failed	Related to the Global Reflex action Run SQL script. Log entry is performed when the script ran unsuccessfully in the journal.
API Event Logs	An API Get or Put was successfully performed.
Backup Database - Succeeded	A Backup Database action, initiated via operator action or global reflex, was successfully completed.
Backup Database - Failed	A Backup Database action, initiated via operator action or global reflex, was unsuccessful.
Backup Journal - Failed	A Backup Journal action, initiated via operator action or global reflex, was successfully completed.
Backup Journal - Succeeded	A Backup Journal action, initiated via operator action or global reflex, was unsuccessful.
Restore Database - Failed	A Restore Database action, initiated via operator action, was unsuccessful.
Restore Database - Succeeded	A Restore Database action, initiated via operator action, was successfully completed.
Restore Journal - Failed	A Restore Journal action, initiated via operator action, was unsuccessful.
Restore Journal - Succeeded	A Restore Journal action, initiated via operator action, was successfully completed.

# System & SQL Tab

Figure A-55



## System & SQL Options

Option	Description
Resend Badge Def. After Denied Event	Resend badge definitions to a controller's local database after the send event was previously denied. Default value: <b>No</b>
Display Unlock Buttons	An <b>Unlock</b> button will appear in relevant action bars. The <b>Unlock</b> button will force an unlock event. A best practice is to leave this setting off unless instructed otherwise by technical support or by technicians with intimate knowledge of the system. Default value: <b>No</b>
Automatically Unlock After Delay	After access has been granted, but the device fails to unlock, this option will force an unlock event after a predefined delay. Default value: <b>Yes</b>
Debug by Diagnostic	Shows the Misc. menu in the Diagnostic screen. This menu should only be used by technicians with intimate knowledge of GuardPoint10. Default value: <b>No</b>
Display the Controller Command Button in Event Log Screen	Show commands originating from a controller in the Log table. The Log table is accessed from the Security task group's Event Log tab.
Initialize controller after table error	If a data table in a controller becomes corrupt, GuardPoint10 will automatically initialize the controller and the table will be rebuilt.

Option	Description
Allow T&A Readers to be 'Entrance & Exit'	A reader details' <b>T&amp;A Reader</b> field will include an <b>Entrance Reader / Exit Reader</b> option in its drop-down list.
Allow Automatic Lock After a Period	If there is no operator activity for a specified period, the currently logged-in operator is logged out of the system and the interface is frozen until an operator logs back into the system.  Default value: <b>No</b>
Enforce Password Policy	Forces new password configurations which use the policies defined in the following seven parameters. By increasing the complexity and adding an expiration, password security is made stronger.  <b>The Policy will be enforced the next time a user changes their password.</b>
Password Min. Length	The minimum number of characters required for a password.
Password expired days	The number of days a password will be valid.
Enforce Password History	Prevents a user from recycling previously used passwords.
Minimum Digits	A minimum number of numbers required for a password.
Minimum Uppercase Letters	The minimum number of uppercase letters required for a password.
Minimum Lowercase Letters	A minimum number of lowercase letters required for a password.
Minimum Special Characters	A minimum number of special characters required for a password. Examples of special characters are !@#\$%^.
Display the Number of Cardholders Who Can Pass a Reader	This field can be found in a reader detail's Miscellaneous tab. It shows the number of cardholders downloaded to the reader.  This field is primarily used for troubleshooting and is not necessary for normal infrastructure setup and maintenance.
Display F1 Code in Reader Details	When set to <b>Yes</b> , a series of <b>F1</b> related fields will appear in a reader details' <b>Miscellaneous</b> tab. The <b>F1</b> fields are relevant to installations that include SENSOR customized controller firmware. Values for the <b>F1</b> fields will be provided by SENSOR to support the unique functionality requested.  Standard controller firmware does not use the <b>F1</b> fields.

Option	Description
Display API Keys	<p>When set to <b>Yes</b>, an API Key field will appear in each Infrastructure tree item's details. The key is used by an API to identify the particular elements of the infrastructure (i.e. site, network, controller, reader, input, relay, and local reflex).</p> <p>When set to <b>No</b>, any data that was previously entered in these fields are still saved in the system database, though the fields are no longer visible on the screens.</p> <p>A best practice is to set <b>Display API Key</b> to <b>Yes</b>. Enter API keys in the infrastructure fields as required, and then set the <b>Display API Key</b> to <b>No</b> so other operators will not inadvertently change a key value.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Unless instructed by your API developer, do not change this parameter setting.</p> </div>
Display Flashing Non-compliant Icon	<p>When set to Yes, the machine where the red noncompliance icon appears in the dashboard will flash. If it is set to No, the red icon will appear on the dashboard, but it will not flash.</p>
Display SQL Script Action in Global Reflex screen	<p>When set to Yes, The Run SQL script action will be available in the Global Reflexes Actions list.</p> <p>This option is only relevant where a license has Advanced Global Reflexes.</p>
Polling Error Message Delay (in sec.)	<p>The number of seconds GuardPoint10 waits before generating a Polling Error for an unresponsive controller. (Polling Errors are displayed in the Event Log screen and the Event History screen).</p> <p>Default <b>30 sec.</b></p> <p>Default: <b>30 second delay</b></p>
Network Default Command Timeout Delay (in msec.)	<p>The number of milliseconds, after a rejected command was sent, that the NM Service will wait before resending the command.</p> <p>Default frequency: <b>1000 msec</b></p>
Network Default Polling Timeout Delay (in msec.)	<p>The number of milliseconds, after an unsuccessful polling event, that the NM Service will wait before resending the poll.</p> <p>Default frequency: <b>1000 msec</b></p>
Network Default Polling Interval (in msec.)	<p>The number of milliseconds, after a successful polling event, that the NM Service will wait before sending a new poll to the same controller.</p> <p>Default frequency: <b>50 milliseconds</b></p>
GAPB	<p>Displays Global Anti-Passback settings in the Area Setup, Area Roll Call, and Reader details.</p> <p>Enables the enforcement of previously added Global Anti-Passback rules.</p> <p>Default value: <b>No</b></p>

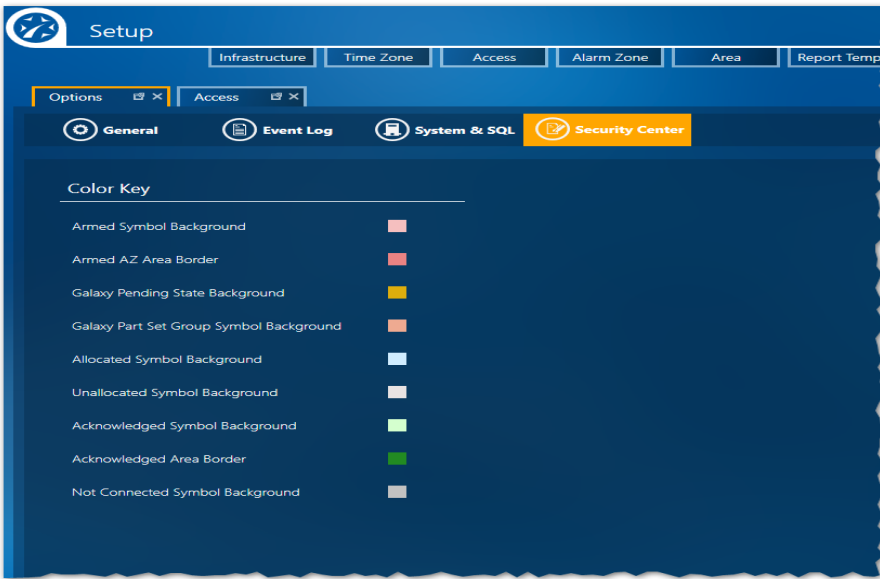
Option	Description
Allow Feature without PC (GAPB)	<p>When set to <b>Yes</b>, After each Access Granted event, the controller, connected to the reader where the event took place, will broadcast, on its bus 1, the GAPB update message 26/49. Only the controllers in the same network will be updated.</p> <p>At the controller initialization, Mess 76 must be sent with byte 1/bit 5 SET. In that case, at each access granted at a reader, the controller will broadcast on its bus 1 the GAPB update message 26/49.</p> <p>GuardPoint10 will broadcast the same message to all the other networks.</p> <p>Default value: <b>No</b></p>
Event Timeout (GAPB)	<p>The number of seconds between the time a command 26 is broadcast and the time that a disconnected controller is back online. If the time displayed has expired, the broadcast is considered too old and it is ignored by the controller.</p> <p>Default value: <b>30</b></p>
Archive Journal	<p>Moves current journal entries to an archive. The archiving process starts when the GPPServer is restarted. GuardPoint10 services are restarted automatically as part of the System Maintenance process.</p>
For Events Older Than (in Days)	<p>Qualifies the age of the journal entries that will remain in the current journal during the archive process. For example, if the <b>For Events Older Than (in Days)</b> value is <b>90</b>, the last 90 days of entries will remain in the current journal.</p> <p>Default value: <b>90</b> day</p>
Max Rows per Archive (in Millions)	<p>Limits the size of each archive created during the archive process to the specified number of entry rows. After the maximum number of rows (entries) have been placed in an archive, a new archive is added where subsequent entries will be moved.</p> <p>Default value: <b>1</b> million</p>

Option	Description
System Log Levels	<p>Settings that filter the content of specified log files. The available settings are as follows:</p> <ul style="list-style-type: none"> <li>» Debug</li> <li>» Info</li> <li>» Warning</li> <li>» Error</li> </ul> <p>These settings are set to <b>Warning</b> by default.</p> <p>The log file files are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Biometric Service</b></li> <li>» <b>NM Service</b></li> <li>» <b>Main Server Service</b></li> <li>» <b>User Interface Application</b></li> </ul> <p>All of the logs can be found in C:\ProgramData\ACS\Logs</p>
SMTP Mail Server	<p>Settings that support the global reflex actions that send emails. The settings are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Host name:</b> The host name of the outgoing SMTP (Simple Mail Transfer Protocol) server.</li> <li>» <b>Port:</b> The port number used by the outgoing mail server.</li> <li>» <b>User Name:</b> The user name for the global reflex account. Some email providers want your full email address as your user name.</li> <li>» <b>Password:</b> The email password used to sign in to the global reflex account.</li> <li>» <b>Enable SSL:</b> If the outgoing mail server supports SSL encryption, set this parameter to <b>Yes</b>.</li> <li>» <b>Default Email Sender:</b> The email address that appears as the default sender in the global reflex action. This address may be changed for each instance of a global reflex action.</li> </ul>

Option	Description
SQL Server Options	<p>Located at the top right of the System &amp; SQL tab, it provides access to the following database administrator actions, via a drop-down list:</p> <ul style="list-style-type: none"> <li>» <b>Backup Database:</b> Copies the current database and saves it with a timestamp appended to the database name. The database is saved in the SQL Server's default backup folder.</li> <li>» <b>Backup Journal:</b> Copies the current journal and saves it with a timestamp appended to the journal name. The journal is saved in the SQL Server's default backup folder.</li> <li>» <b>Restore Database:</b> Opens a file explorer at the SQL Server's default backup folder location, where a previously backed up database may be selected.</li> <li>» <b>Restore Journal:</b> Opens a file explorer at the SQL Server's default backup folder location, where a previously backed up journal may be selected.</li> </ul>

## Security Center

Figure A-56



The following options pertain to the Setup tasks' Position screen and the Security tasks' Security Center screen.

Security Center Color Key

Option	Description
Armed Symbol Background	Indicates the background color of an icon representing an armed physical component in the system.



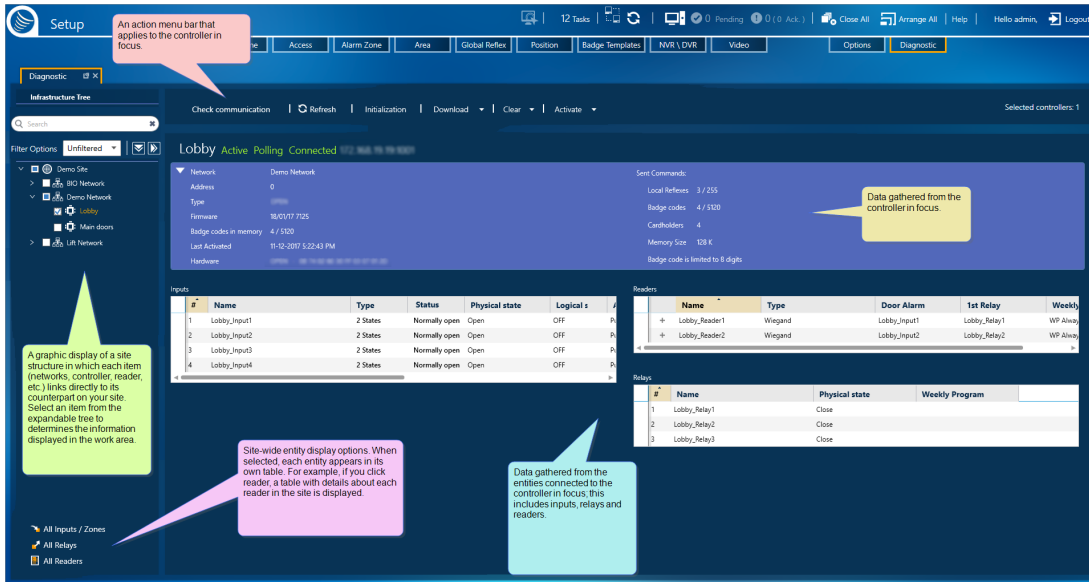
Option	Description
Armed AZ Area Border	Indicates the frame color of a shape or textbox linked to an armed Alarm Zone in the system.
Galaxy Pending State Background	<p><b>Note:</b> Relevant where Galaxy is integrated</p> <p>Indicates the background color of a Galaxy element icon that is in the process of updating information acquired from the Galaxy panel.</p>
Galaxy Part Set Group Background	<p><b>Note:</b> Relevant where Galaxy is integrated</p> <p>Indicates the background color of a Galaxy group icon or the frame color of a Galaxy group, shape, or textbox where the group is Part Set.</p>
Allocated Symbol Background	Indicates the background color of an icon representing a physical component in the system.
Unallocated Symbol Background	Indicates the background color of an icon that has not been allocated to a physical component in the system.
Acknowledged Symbol Background	Indicates the background color of an icon representing a triggered and acknowledged event for a physical component in the system.
Acknowledged Area Border	Indicates the frame color of an icon representing a triggered and acknowledged event for an alarm zone.
Not Connected Symbol Background	<p>Indicates the background color of an icon representing a physical component that has been disconnected from the system or is non-responsive.</p> <p>Alternatively, it may indicate an icon that is not been linked to a physical component.</p>

In all Options screen tabs, at the top right next to the **Save** button, there is a **Restore Default** button. The **Restore Default** button allows an operator to return all option settings to their default values, regardless of the Options tab currently open.

# Diagnostic Screen

**Warning:** Some of the tools on the Diagnostic screen are only for a technician with intimate knowledge of your system, and the controllers in the system. Some of the tools on this screen could potentially result in irreparable damage to the data stored on a controller.

Figure A-57



GuardPoint10 captures data from the system's site, networks, and controllers, and then displays the data in the appropriate area of your Diagnostic screen. The Diagnostic screen allows you to evaluate the current health of your system quickly on a network-by-network and controller-by-controller basis.

The Diagnostic screen has five distinct areas:

## Site tree

Browse your system through the site tree. The tree includes all site networks and their controllers.

Above the site tree are the following:

- » Search field: Displays tree elements based on the text in the element name.
- » Expand/Collapse buttons: Changes the tree hierarchy view.
- » Filter options: Displays controllers in the tree based on the selected controller state in the drop-down list.

The available filter options are:

- » Activated controllers
- » Deactivated controllers
- » Disconnected controllers
- » Unfiltered (default)

## Diagnostic action bar

Includes actions to resolve any issue with a controller or entity.

A checkbox by each element of the expandable site tree allows you to perform diagnostic tasks on multiple controllers at the same time. If the action selected requires information from the system database, and one of the selected controllers is not answering the database, the selected action will skip the non-answering controller.

The number of selected controller (and Galaxy panel) checkboxes appears on the right side of the action bar. If there are no selected checkboxes the field is hidden.

## Controller data

Displays information about the controller in focus and the information stored in the controller's memory.

If there is an issue with the communication between the controller in focus and the system, only the details that are stored in the system database are displayed.

If there are no communication issues between the controller in focus and the system, data is only taken from the controller's memory.

The controller data displayed is as follows:

Table A-32 Controller Data on the Diagnostic screen

Name	Description
Name	The name of the controller in focus.
Communication information	<ul style="list-style-type: none"><li>» <b>Active / Not Active:</b> Is the controller taking action based on the information sent to it by an entity. For example, If a controller is not active and a reader sends valid card information to the controller the fact that the information was received by the controller is recorded, but the relays will not be triggered and the door will not unlock.</li><li>» <b>Polling / Not Polling:</b> Is the system querying each controller in turn, as to whether it has any data to transmit.</li><li>» <b>Connected / No Answer:</b> Is the controller connected to the network and if so, depending on the type of connection (COM or TCP), via which port or IP address.</li></ul>
Network	The name of the network where the controller is located
Address	The physical address of the controller, as set in the hardware's <b>Dipswitch</b> <sup>1</sup> .
Type	The name of the controller type (i.e. IC1000, IC4000, etc.).

<sup>1</sup>A series of tiny switches built into circuit boards. The housing for the switches has the same shape as a chip and is usually red.

Name	Description
Firmware	<p>Current firmware version information. The firmware version is given in a dd/mm/yy date format, followed by ROM information that may be used by a hardware technician.</p> <p>GuardPoint10 compatible controllers must have firmware from 2016 or later.</p>
Badge Codes in Memory	The total number of cardholders for whom information is currently held in the controller followed by the controller's maximum capacity.
Last Activated	The date and time when the controller was most recently activated, see <a href="#">Active/Not Active</a> above.
Hardware	The name of the controller type followed by code that a hardware technician, intimately familiar with SENSOR controllers, uses to identify the hardware in the controller.
Sent Commands	<p>Statistics about the controller, this includes:</p> <ul style="list-style-type: none"> <li>» How many Local Reflexes are in use followed by a controller's maximum capacity.</li> <li>» How many badge codes are in q controller followed by the controller's maximum capacity.</li> <li>» How many cardholders are in the controller's memory.</li> <li>» The controller's memory size.</li> <li>» The badge code length limit.</li> </ul> <hr/> <p><b>Note:</b> Badge codes generated as a result of a cardholder's license plate number entry will only be acknowledged at a controller where a License Plate Recognition reader (LPR) is connected, regardless of the Multiple Access Group assigned. This will be reflected in the cardholder total and badge code total displayed in the Diagnostic screen.</p>

## Entity Data Tables (inputs, relays, and readers)

A group of three tables, one for each entity type connected to the controller in focus. These tables include information about the entities.

The Reader table is unique in that each row can be expanded by clicking + at the beginning of each row. However, the only time you would want to expand a reader row is if the reader is a biometric reader.

Table A-33 Diagnostics Input Device Table

Name	Description
#	The connector number on the controller, where the input device's wires are physically connected. The number of connectors varies between the controller types. For more information about controller types and available connectors, see <a href="#">"Default Connections for Inputs, Relays, and RTX" on page 712.</a>
Name	The name of the Input device.
Type	<p>The states that may be detected by the input device. The available types from the drop-down list are:</p> <ul style="list-style-type: none"> <li>» <b>2 States:</b> The two possible states of the sensor/detector connected to the input device (i.e. opened or closed).</li> <li>» <b>4 States</b> (also called 'supervised'): In addition to the 2 States mentioned above, the input device also detects the status of the line that connects the sensor/detector to the input device. The detected line statuses are: <ul style="list-style-type: none"> <li>» <b>Line_cut:</b> Tampering issue.</li> <li>» <b>Line_short:</b> electrical issue.</li> </ul> </li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> A 2 State input device may not be defined as a 4 State input device, but a 4 State input may be redefined as a 2 State input, as long as the line does not need to be supervised. Consult your controller documentation to determine which types of input states are available (see <a href="#">"Controller Comparison Tables" on page 705.</a>)</p> </div>
Status	<p>The expected status of the input. The available status types from the drop-down list are:</p> <ul style="list-style-type: none"> <li>» <b>NO (Normally Open)</b></li> <li>» <b>NC (Normally Closed)</b></li> </ul>
Physical State	<p>The current state of the input. The possible statuses are:</p> <ul style="list-style-type: none"> <li>» <b>Open</b></li> <li>» <b>Closed</b></li> </ul>

Name	Description
Logical State	<p>If there is a conflict between the Status and the Physical State, the Logical state will be <b>ON</b>. Otherwise, the Logical state will be <b>OFF</b>.</p> <div style="background-color: #4a90e2; color: white; padding: 10px; border-radius: 5px;"> <p><b>What this means:</b></p> <p>If an input is configured as normally Closed and for some reason its current physical state is Open, the logical state will be On.</p> <p>If the input is armed while its logical state is On, an alarm will trigger.</p> <p>If the Status and the Physical State do not conflict, the Logical state will be OFF and no alarm will trigger.</p> </div>
Alarm Zone	<p>Input devices may be grouped into zones called "Alarm Zones". An alarm zone may be armed or disarmed, either automatically, by attributing a Weekly Program, or manually, through an override action. An alarm zone's armed or disarmed state has the following effects on its member input devices:</p> <ul style="list-style-type: none"> <li>» Armed alarm zone: All the alarm input devices belonging to the alarm zone are armed.</li> <li>» Disarmed alarm zone: All the alarm input devices belonging to the alarm zone are disarmed.</li> </ul> <p>For more information about alarm zones, see <a href="#">"Alarm Zones (Setup)" on page 301</a>.</p>
Weekly Program	<p>The Weekly Program (WP) assigned to an input device via an alarm zone. For information about alarm zones, see <a href="#">"Alarm Zones (Setup)" on page 301</a>.</p> <p>A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays and Special days. WPs set periods of acceptability, during which time, different groups of workers may enter. For more information about WPs, see <a href="#">"Daily Program Time Zones" on page 114</a>.</p>
Arm/Disarm	<p>Manual override arm or disarm state of the input device. The manual override is performed via the Alarm Zone Security screen (see <a href="#">"Alarm Zone Security Screen for GuardPoint10 Alarm Zones" on page 662</a>).</p> <p>When armed, and the expected status of the input device changes (see the <b>Logical State</b> above) the input device raises an alarm by sending an alarm transaction to the system.</p> <div style="border: 1px solid black; padding: 5px; background-color: #f1c40f;"> <p><b>Note:</b> This manual <b>Arm/Disarm</b> setting takes priority over an input device's associated Alarm Zones Weekly Program.</p> </div>

Name	Description
Alarm State	<p>If an input's alarm is triggered, it may have one of the following three states:</p> <ul style="list-style-type: none"> <li>» <b>Under alarm:</b> The alarm has not been addressed yet.</li> <li>» <b>Acknowledged:</b> The alarm has been acknowledged (see <a href="#">"Dashboard" on page 333</a>).</li> <li>» <b>Confirmed:</b> After acknowledging the alarm, it has been confirmed (see <a href="#">"Dashboard" on page 333</a>).</li> </ul> <p>If an input is disarmed after an alarm is triggered, the Alarm State will still display the current state of the alarm.</p>
Bypass	<p>When selected, transactions sent by the input device are ignored by the system. For example, if an input's logical state is ON, the input will send an alarm transaction. However, the transaction will be ignored by the system and the event won't appear in the Event log.</p> <hr/> <p><b>Note:</b> This field also exists in the <a href="#">"Alarm Zone Setup Screen" on page 521</a>. These fields are linked. If marked as bypassed in one table, it will automatically be marked as bypassed in the other table.</p>

Table A-34 Diagnostics Relay Table

Name	Description
#	The connector number on the controller, where the relay's wires are physically connected. The number of connectors varies between controller types. For more information about controller types and available connectors, see <a href="#">"Controller Comparison Tables" on page 705</a> .
Name	The name of the relay.
Physical State	The current state of the relay: <b>Open</b> or <b>Close</b> .
Weekly Program	<p>The Weekly Program (WP) assigned to a relay. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays. WPs set periods of acceptability, during which time, different relay actions may take place. For more information about WPs, see <a href="#">"Daily Program Time Zones" on page 114</a>.</p> <hr/> <p><b>Note:</b> A relay's Weekly Program has priority over an associated alarm zone's Weekly Program.</p>

Table A-35 Diagnostics Readers Table

Name	Description
Name	The name of the reader.
Type	A classification of a reader's scan/recognition options. The classification is set in the Type area of the reader's details and is determined by the functions the reader can perform (i.e. Access, License Plate Recognition, Biometric, etc.).
Door Alarm	The alarm zone associated with the reader. When the reader's alarm zone is armed, access via the reader is denied. The only exception is for supervisors. If a supervisor attempts to enter an alarm zone via the reader, the zone is temporarily disarmed during the <b>Entrance/Exit delay</b> . This allows the supervisor to access the zone and disarm it from an alarm from inside the alarm zone (see " <a href="#">Alarm Zones (Setup)</a> " on page 301).  <b>Note:</b> A cardholder can be designated a supervisor in the cardholder's details Personal tab.
First Relay	The name of the first relay triggered by the reader. A reader may have more than one relay (i.e. a Mantrap).
Weekly Program	The Weekly Program (WP) assigned to a reader. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays. WPs set periods of acceptability, during which time, different reader actions may take place. For more information about WPs, see " <a href="#">Daily Program Time Zones</a> " on page 114.  <b>Note:</b> A reader's Weekly Program has priority over an associated alarm zone's Weekly Program.

If a reader's **Type** is Biometric, the expanded row will display information specific to the biometric reader as well as command buttons specific to the reader.

Figure A-58



The information about the biometric reader is straightforward and also appears in the Infrastructure's reader details > "[Biometric Tab](#)" on page 459. However, there are two exceptions:



- » **Cardholders in Memory:** Shows the number of cardholders in the biometric reader's memory along with the memory's capacity.
- » **Cardholders Sent Command:** Shows the number of cardholders in the memory of the controller connected to the biometric reader along with the memory's capacity.

In addition to the reader and controller information, there are the following buttons:

- » **Initialize:** Data, which was previously acquired and saved in the reader's local database, is downloaded from the system database to the respective reader, where it will overwrite preexisting local data.
- » **Clear Memory:** Erases all data from the reader's local database rendering the reader useless until the reader is initialized.
- » **Factory Reset:** Changes the values found in the reader details' Biometric tab to the factory defaults. For more information, see "[Biometric Tab](#)" on page 459.



**Note:** If the IP address of a biometric reader is changed, go to the Infrastructure screen and delete the reader. After the reader is deleted, add it back to the infrastructure with the new IP address.

## Site-wide entity data (inputs, relays, and readers)

In the "[Entity Data Tables \(inputs, relays, and readers\)](#)" on page 586, the tables covered the entities connected to the controller in focus. However, the three tables displayed from this group include the entities connected to all of the controllers on the site.

These site-wide tables include a **Group By bar** above the column headings. The **Group By bar** allows you to restructure a site-wide table based on the criteria (column heading) dragged into the **Group By bar**.

To change a table's structure:

- » Select a column heading from the row below the **Group By bar** and drag it to the **Group By bar**, the heading becomes a criteria, and the table reflects the new criteria structure.
- » Re-order criteria already in the **Group By bar** (drag and drop one criteria in front of another) changes the structure applied to the table.
- » **Mouseover**<sup>1</sup> a criteria already in the **Group By bar** and click the delete **x** on the right side of a criteria frame; the criteria is removed.

The columns in each of the site-wide tables are as follows:

**Table A-36** *Diagnostics Site-wide Input Devices Table*

Name	Description
Network Name	The name of the network where the controller is a member.
Controller Name	The name of the controller that is connected to an input device.
Name	The name of the input device.

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

Name	Description
#	<p>The connector number on the controller where the input device's wires are physically connected. The number of connectors varies between controller types. For more information about controller types and available connectors, see <a href="#">"Default Connections for Inputs, Relays, and RTX" on page 712</a>.</p>
Type	<p>The states that may be detected by the input device. The available types from the drop-down list are:</p> <ul style="list-style-type: none"> <li>» <b>2 States</b>: The two possible states of the sensor or detector connected to the input device (i.e. opened or closed).</li> <li>» <b>4 States</b> (also called 'supervised'): In addition to the 2 States mentioned above, the input device also detects the state of the line that connects the sensor or detector to the input device. The detected line states are: <ul style="list-style-type: none"> <li>» <b>Line_cut</b>: Tampering issue.</li> <li>» <b>Line_short</b>: electrical issue.</li> </ul> </li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> A 2 State input device may not be defined as a 4 State input device, but a 4 State input may be redefined as a 2 State input, as long as the line does not need to be supervised. Consult your controller documentation to determine which types of input states are available (see <a href="#">"Controller Comparison Tables" on page 705</a>).</p> </div>
Status	<p>The expected status of the input. The available status types are:</p> <ul style="list-style-type: none"> <li>» <b>NO (Normally Open)</b></li> <li>» <b>NC (Normally Closed)</b></li> </ul>
Physical State	<p>The current state of the input. The possible states are:</p> <ul style="list-style-type: none"> <li>» <b>Open</b></li> <li>» <b>Closed</b></li> </ul>
Logical State	<p>If there is a conflict between the Status State and the Physical State, the Logical State will be ON. Otherwise, the Logical State will be OFF.</p> <div style="background-color: #4a90e2; color: white; padding: 10px; margin-top: 10px;"> <p><b>What this means:</b></p> <p>If an input is configured as normally Closed and for some reason its current physical state is Open, the logical state will be <b>ON</b>.</p> <p>If the input is armed while its logical state is <b>ON</b>, an alarm will trigger.</p> <p>If the Status and the Physical State do not conflict, the Logical state will be <b>OFF</b> and no alarm will trigger.</p> </div>

Name	Description
Alarm Zone	<p>Input devices may be grouped into zones called "Alarm Zones". An alarm zone may be armed or disarmed, either automatically, by attributing a Weekly Program, or manually, through an override action. An alarm zone's armed or disarmed state has the following effects on its member input devices:</p> <ul style="list-style-type: none"> <li>» Armed alarm zone: All the alarm input devices belonging to the alarm zone are armed.</li> <li>» Disarmed alarm zone: All the alarm input devices belonging to the alarm zone are disarmed.</li> </ul> <p>For more information about alarm zones, see <a href="#">"Alarm Zones (Setup)" on page 301</a>.</p>
Weekly Program	<p>The Weekly Program (WP) assigned to an input device via an alarm zone. For information about alarm zones, see <a href="#">"Alarm Zones (Setup)" on page 301</a>.</p> <p>A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays. WPs set periods of acceptability, during which time, different groups of workers may enter. For more information about WPs, see <a href="#">"Daily Program Time Zones" on page 114</a>.</p>
Arm/Disarm	<p>Manual override arm or disarm state of the input device. The manual override is performed via the Alarm Zone Security screen (see <a href="#">"Alarm Zone Security Screen for GuardPoint10 Alarm Zones" on page 662</a>).</p> <p>When armed, and the expected status of the input device changes (see the <b>Logical State</b> above) the input device raises an alarm by sending an alarm transaction to the system.</p> <hr/> <p><b>Note:</b> This manual <b>Arm/Disarm</b> setting takes priority over an input device's associated Alarm Zones Weekly Program.</p>
Alarm State	<p>If an input's alarm is triggered, it may have one of the following three states:</p> <ul style="list-style-type: none"> <li>» <b>Under alarm:</b> The alarm has not been addressed yet.</li> <li>» <b>Acknowledged:</b> The alarm has been acknowledged (see <a href="#">"Dashboard" on page 333</a>).</li> <li>» <b>Confirmed:</b> After acknowledging the alarm, it has been confirmed (see <a href="#">"Dashboard" on page 333</a>).</li> </ul> <p>If an input is disarmed after an alarm is triggered, the Alarm State will still display the current state of the alarm.</p>

Name	Description
Bypass	<p>When selected, transactions sent by the input device are ignored by the system. For example, if an input's logical state is ON, the input will send an alarm transaction. However, the transaction will be ignored by the system and the event won't appear in the Event log.</p> <p><b>Note:</b> This field also exists in the <a href="#">"Alarm Zone Setup Screen"</a> on <a href="#">page 521</a>. These fields are linked. If marked as bypassed in one table, it will automatically be marked as bypassed in the other table.</p>

Table A-37 Diagnostics Site-wide Relays Table

Name	Description
Network Name	The name of the network where the controller is a member.
Controller Name	The name of the controller that is connected to the relay.
Name	The name of the relay.
#	The connector number on the controller, where the relay is physically connected. The number of connectors varies, according to the controller type. For more information about controller types and available connectors, see <a href="#">"Controller Comparison Tables"</a> on <a href="#">page 705</a> and <a href="#">"Default Connections for Inputs, Relays, and RTX"</a> on <a href="#">page 712</a> .
Weekly Program	<p>The Weekly Program (WP) assigned to a relay. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays. WPs set periods of acceptability, during which time, different relay actions may take place. For more information about WPs, see <a href="#">"Daily Program Time Zones"</a> on <a href="#">page 114</a>.</p> <p><b>Note:</b> A relay's Weekly Program has priority over an associated alarm zone's Weekly Program.</p>
Physical Status	The current state of the input device ( <b>Open</b> or <b>Close</b> ).

Table A-38 Diagnostics Site-wide Readers Table

Name	Description
Network Name	The name of the network where the controller is a member.
Controller Name	The name of the controller connected to the reader.
Name	The name of the reader.

Name	Description
Type	A classification of all of the reader's scan/recognition options. The classification is set in the Type area of the reader's details and is determined by the functions the reader can perform (i.e. Access, License Plate Recognition, Biometric, etc.).
#	The connector number on the controller, where the reader is physically connected. The number of connectors varies, according to the controller type. For more information about controller types and available connectors, see <a href="#">"Controller Comparison Tables" on page 705</a> .
First Relay	The name of the first relay triggered by the reader. A reader may have more than one relay (i.e. a Mantrap).
Door Alarm	<p>The alarm zone associated with the reader. When the reader's alarm zone is armed, access via the reader is denied. The only exception is for supervisors. If a supervisor attempts to enter an alarm zone, via the reader, the zone is temporarily disarmed during the <b>Entrance/Exit delay</b>. This allows the supervisor to access the zone and disarm it from inside the alarm zone (see <a href="#">"Alarm Zones (Setup)" on page 301</a>).</p> <hr/> <p><b>Note:</b> A cardholder can be designated a supervisor from the cardholder's details Personal tab.</p>
Weekly Program	<p>The Weekly Program (WP) assigned to a reader. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays. WPs set periods of acceptability, during which time, different reader action may take place. For more information about WPs, see <a href="#">"Daily Program Time Zones" on page 114</a>.</p> <hr/> <p><b>Note:</b> A reader's Weekly Program has priority over an associated alarm zone's Weekly Program.</p>

## Galaxy specific diagnostic displays

When a Galaxy network or panel is selected from the expandable site tree, the Diagnostic screen displays data specific to the Galaxy system.

The Galaxy network displays:


- » The Site where the Galaxy network integration is located
- » The Galaxy system type
- » The number of zones supported by the Galaxy panel

The Galaxy panel displays:

- » The Site where the Galaxy network integration is located
- » The Galaxy system type
- » The last time that the Galaxy panel was activated via the Infrastructure screen.

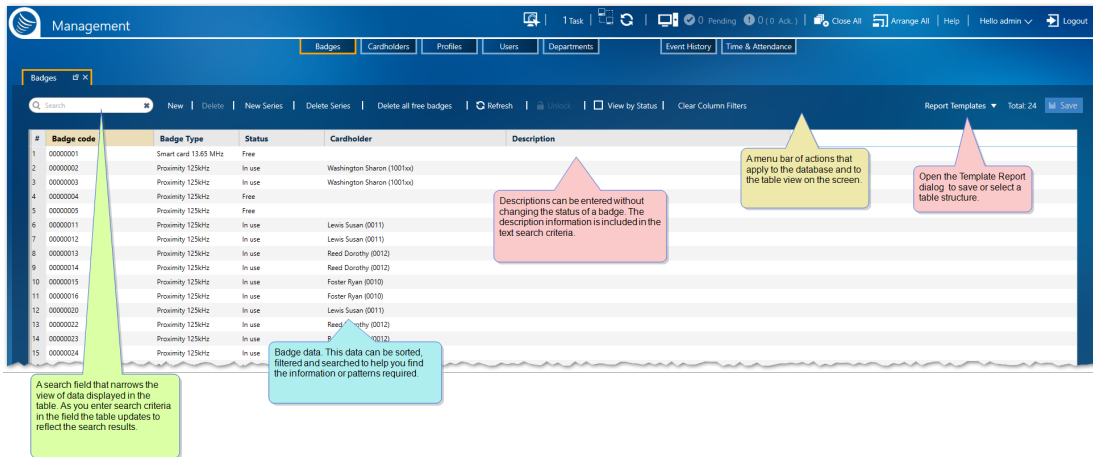
In addition to Galaxy panel information displaying after selecting a Galaxy panel, the panel's Zone table is also displayed. A Zone table displays the following information:

Table A-39 Zone Table Column Parameters

Column	Description
Refresh 	Refreshes the data provided by the Galaxy panel.
#	The connector number on the panel, where the zone device's wires are physically connected. The number of connectors varies according to the Galaxy panel type.
Name	The unique name of a zone.
Physical State	<p>The current state of the zone. The possible statuses are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Open</b></li> <li>» <b>Closed</b></li> </ul> <hr/> <p><b>Note:</b> A tamper zone's physical state is not visible in the Zone table.</p>
Alarm Priority	A priority (0 - 255) that allows an operator to manage and display an alarm based on severity (i.e. sort alarms in the table or on the Security Center screen's Alarm list). For information about the Alarm list, see " <a href="#">Security Center Screen</a> " on page 680.
Alarm State	<p>If a zone's alarm is triggered, it may have one of the following three states:</p> <ul style="list-style-type: none"> <li>» <b>Under alarm:</b> The alarm has not been addressed yet.</li> <li>» <b>Acknowledged:</b> The alarm has been acknowledged (see "<a href="#">Dashboard</a>" on page 333 and "<a href="#">Addressing Alarms via a Security Center Icon</a>" on page 391).</li> <li>» <b>Confirmed:</b> After acknowledging the alarm, it is confirmed (see "<a href="#">Dashboard</a>" on page 333 and "<a href="#">Addressing Alarms via a Security Center Icon</a>" on page 391).</li> </ul>
Omitted	<p>When selected, transactions sent by the zone device are ignored by GuardPoint10. For example, if a zone's physical state is <b>ON</b>, the zone will send an alarm transaction GuardPoint10. However, the transaction will be ignored by GuardPoint10 and the Galaxy panel, and the event will not appear on the screen.</p> <hr/> <p><b>Note:</b> This parameter is disabled for tamper zones.</p>

# Badges Screen

Figure A-59



The Badges screen displays a table of all badge codes that can be added to a Badge Template (see "Badge Templates Screen" on page 564).

The system treats the Badges screen as a report where information can be filtered, sorted, or grouped according to the needs of the operator.

A Badges report may be saved as a Report Template via the action bar's **Report Template** button. The advantages of a report template are:

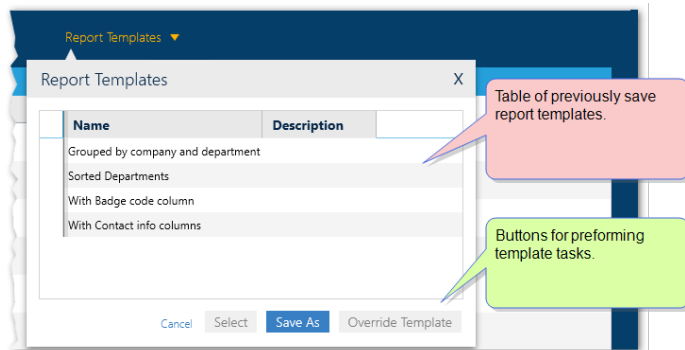
- » Load and display a complex report structure with a couple of clicks.
- » Automatically save a template report to file or email it to others via a global reflex "Create Template-based report" on page 548 action.

## Report Template dialog

The structure of the screen table can be saved in a template so it can be applied later, either to the screen display or a global reflex "Create Template-based report" on page 548 action. The data in a template is dynamic and will change to reflect the environment.

To start using templates click the **Report Templates** button.

Figure A-60



The table in the Report Template dialog contains the names and descriptions of previously save templates, which are specific to the screen displayed.

From the screen's Report Template dialog you can click:

- » **Save As:** Opens the ["Report Template Screen" on page 529](#), where the current structure of the displayed table can be saved.
- » **Override:** Opens the ["Report Template Screen" on page 529](#), where the current structure of the displayed table can override the last selected template with the current structure of the displayed table.
- » **Select:** Displays current data in the template selected from the dialog's table.

## A little about badge codes

A card or badge is a physical device that has a unique code by which the system can identify it. Each badge code must be registered in the system database. After a badge code is registered, it can be assigned to a cardholder. During this process, the system assigns a cardholder an *internal system cardholder number*. This number is a cardholder's internal GuardPoint10 system ID. Generally, the badge code and the internal system cardholder number are unknown to the assigned cardholder.

When a badge is swiped at a reader, the controller to which the reader is connected first checks if the badge is known (i.e. its badge code is in the controller's local database) and if so, to whom it is assigned. This is required to check the access authorization of the cardholder.

The reading technology is defined in the ["Reader Details" on page 453](#) and badge technology is defined in the Badges screen.

Because badge and cardholder management tasks are usually bound together, many of the Cardholder operations can also be performed via the Badges screen and many of the Badge operations can be performed via the Cardholder screen.



**Note:** A cardholder may be defined with more than one badge.

A description of each column in the Badges table is provided below.

For information about table filters, see ["Table Filters" on page 695](#).

## Report Options

The area contains export options for the displayed Badges Report table.

Table A-40 Report Options

Option	Description
Report Template	Opens a dialog where a template may be selected saved or overwritten.

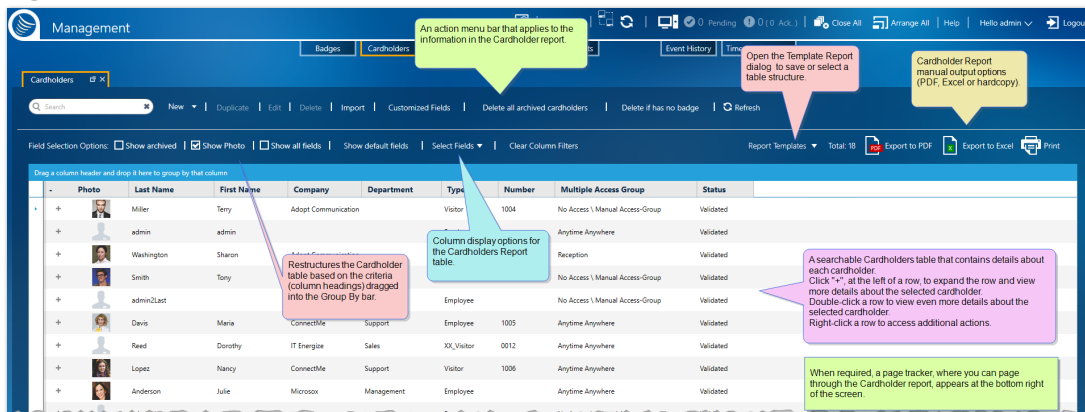


## Badges Table Options and Columns

Parameter	Description
Badge Code	Code attached to a badge. The code may be expressed in decimal or hexadecimal values. Where required, leading zeros will be entered automatically to the default length of the badge code.
Type	<p>The technology of a badge or method required for badge code recognition. The badge type default is defined in the Options screen's General tab, in the <b>Default Badge Technology</b> parameter.</p> <p>For more information about the Options screen, see <a href="#">"Options Screen" on page 567</a>.</p> <p>The badge technology may be changed via a drop-down list opened from a badge code's <b>Type</b> cell.</p>
Status	<p>A badge has one of the following statuses:</p> <ul style="list-style-type: none"> <li>» <b>Free:</b> Badge is available for cardholder assignment.</li> <li>» <b>In Use:</b> Badge is assigned to a cardholder.</li> <li>» <b>Canceled:</b> Badge is automatically invalidated, but still exists in the system. If someone attempts to use a canceled badge, the Event log will document the attempt and security personnel may take action based on a predefined protocol.</li> <li>» <b>Lost:</b> Badge is automatically invalidated, but still exists in the system. If someone attempts to use a lost badge, the Event log will document the attempt and security personnel may take action based on a predefined protocol.</li> <li>» <b>Stolen:</b> Badge is automatically invalidated, but still exists in the system. If someone attempts to use a stolen badge, the Event log will document the attempt and security personnel may take action based on a predefined protocol.</li> </ul> <p>If a badge has a status of Lost, Stolen, or Canceled, The operator can detach the cardholder from the badge via the badge's context menu.</p> <p>Select the View by Status checkbox in the toolbar, above the table, to change the table view. When selected the table will display expandable status categories that contain badge codes of the selected status.</p>
Cardholder	<p>The name of the cardholder assigned to a badge. A badge can exist in the system without an assigned cardholder.</p> <p>Double click the Cardholder field to open the assigned cardholder's details. If there is no assigned cardholder an empty cardholder's details will appear where a new cardholder may be defined.</p>
Description	A free text field used by an operator to describe specifics about the badge; this may include how it is used and the type of cardholder who would have the badge. For example, a range of badges may be designated only for visitors, another range only for freelancers, etc. This information would be added to the badge's description.

# Cardholders Screen

Figure A-61



A cardholder is an individual, registered in the system database, as a person who may be assigned the following:

- » Badge code
- » Weekly Program
- » Multiple Access Group
- » Personal Door Access Group
- » Personal Lift Access Group.
- » and more.

A cardholder's unique identification is determined by a combination of a cardholder's first name last name and an internal system identification number.

Because badge and cardholder tasks are bound together, at times, many of the cardholder operations can also be performed via the Badges screen and many of the Badge operations can be performed via the Cardholder screen.

The system treats the Cardholders table as a report where information can be filtered sorted and grouped according to the requirements of the operator.

A Cardholder report output may be in a PDF format or an Excel format. In addition, the report may also be printed.

A Cardholder report may be saved as a Report Template via the action bar **Report Template** button. The advantages of a report template are:

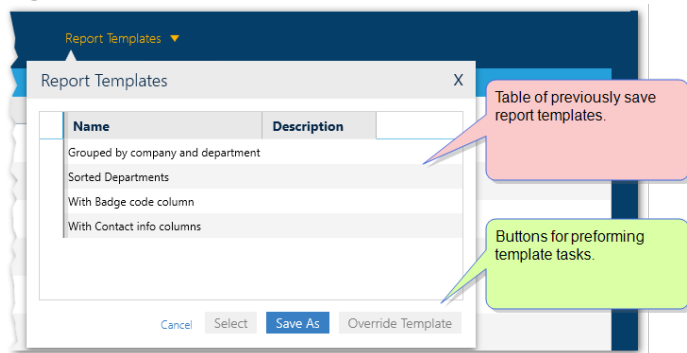
- » Load and display a complex report structure with a couple of clicks.
- » Automatically save a template report to file or email it to others via a global reflex "[Create Template-based report](#)" on page 548 action.

## Report Template dialog

The structure of the screen table can be saved in a template so it can be applied later, either to the screen display or a global reflex "[Create Template-based report](#)" on page 548 action. The data in a template is dynamic and will change to reflect the environment.

To start using templates click the **Report Templates** button.

Figure A-62



The table in the Report Template dialog contains the names and descriptions of previously save templates, which are specific to the screen displayed.

From the screen's Report Template dialog you can click:

- » **Save As:** Opens the "Report Template Screen" on page 529, where the current structure of the displayed table can be saved.
- » **Override:** Opens the "Report Template Screen" on page 529, where the current structure of the displayed table can override the last selected template with the current structure of the displayed table.
- » **Select:** Displays current data in the template selected from the dialog's table.

The Cardholders screen includes four distinct areas:

- » Column Selection Options
- » Report Export Options
- » Cardholder Report Table
- » Report Pagination Controls

## Column Selection Options

The Field Selection Options bar and the Group By bar below contain powerful column display options for the Cardholder Report table.

Table A-41 Column Selection Options

Column Option	Description
Group By bar	<p>Restructures the report table based on the criteria (column heading) dragged into the <b>Grouped By</b> bar.</p> <p>To change the report table's structure:</p> <ul style="list-style-type: none"> <li>» Select a column heading from the table and drag it to the <b>Grouped By</b> bar, the heading becomes the focus of the report table, and the table restructures accordingly.</li> <li>» Restructure heading already in the <b>Grouped By</b> bar (drag and drop one heading in front of another) changes the structure applied to the report table.</li> <li>» <b>Mouseover</b><sup>1</sup> a heading already in the <b>Grouped By</b> bar and click delete <b>x</b> on the right side of a criteria frame; the heading is removed, though the column remains.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> If there are more than 4,000 pages (100,000 cardholders), the <b>Grouped By</b> bar will be disabled.</p> </div>
Show Archived	<p>Displays a row for each cardholder that was been previously archived. An archived cardholder does not have an assigned badge code and their status is set to <b>Archived</b>.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> An archived cardholder is frozen and cannot be assigned a badge or be granted authorizations. However, an archived cardholder is still in the system database and may be restored at any time.</p> <p>When an archived cardholder is <b>Deleted</b>, it is erased from the system database and can only be recovered via a third-party back-up system.</p> </div>
Show Photos	<p>Adds a Photo column to the report table, where an image of a cardholder may be displayed. The image can be used for visual ID verification.</p> <p>If a cardholder does not have a photo in the system database, an avatar is used as a placeholder.</p>
Show All Fields	<p>All available columns will appear in the report table.</p>
Show Default Fields	<p>A standard group of columns will appear in the report table. Other columns may be added, via the <b>Select Fields</b> drop-down list, as required.</p>
Select Fields	<p>A drop-down list of available columns appears. You can select any of the columns listed to display in the report table. This allows you to customize your report to fit your specific requirements.</p>

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

# Report Export Options

Contains export options for the displayed Cardholder Report table.

Table A-42 Report Options

Option	Description
Report Template	Opens a dialog where a template may be selected saved or overwritten.
Export to PDF	Takes the column data of the currently displayed report table and generates a PDF file. The PDF file can be easily transferred to a third-party outside the system, where it can be viewed with a PDF reader (i.e. Adobe Acrobat <sup>®</sup> Reader).
Export to Excel	Takes the column data of the currently displayed report table and generates an Excel <sup>®</sup> spreadsheet (XLS file) that can easily be transferred to a third-party outside the system and viewed in any application that supports XLS or XLSX file formats.
Print	Takes the column data of the currently displayed report table and generates hardcopy (paper) output via a selected printer. The hardcopy will have the same layout as the PDF file.



**Warning:** Keep in mind, when you circulate an exported cardholder report, confidential cardholder data may be inadvertently revealed to unauthorized sources.

## Cardholder Report table

A description of each column in the Cardholder Report table is provided below.

For information about table filters, see **"Table Filters" on page 695**.

Table A-43 Cardholder Report Table Options and Columns

Parameter	Description
Expand and Contract (+, -)	<p>Expands and contracts a cardholder row. When expanded, information is displayed in a more user-friendly format, including badge codes. In addition, you double-click on an expanded or contracted row to open the selected cardholder's details (see <b>"Operator (User): MultiSite Impact Cardholder Details" on page 607</b>) where more information about the cardholder is available.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> If a cardholder row is expanded, the cardholder's photo or avatar will appear in the expanded row, regardless of the <b>Show Photo</b> setting above the table.</p> <p>In addition, the badge code(s) assigned to a cardholder will also appear in the expanded row. If a cardholder does not have a badge assignment, no badge code will be displayed.</p> </div>





Parameter	Description
Photo (may not be visible)	Where an image of a cardholder may be displayed. A member of the security staff can later use the image for visual ID verification.  If a cardholder doesn't have a photo in the system database, an avatar is used as a placeholder.
Last Name	The cardholder's last name as it would appear on the screen.
First Name	The cardholder's first name as it would appear on the screen.
Company	The name of a company (known to the system) where the cardholder has an association (i.e. employment).
Department	The name of the department within the company where the cardholder is assigned.
Type	The status of the cardholder in the selected company. The GuardPoint10 built-in types are <b>Employee</b> and <b>Visitor</b> . However, an operator may add additional types, as required, via an Add New Cardholder operation (see <a href="#">"Adding Customized Fields to Cardholder Details" on page 199</a> ).
Number	The internal system number assigned to each cardholder. A cardholder's uniqueness is determined by a combination of a cardholder's first name, last name, and internal system number. However, there is an option to allow duplicate names, in such cases, the internal system number alone represents the uniqueness of a cardholder.
Area	A defined area where the cardholder can currently be found.
Multiple Access Group	The Multiple Access Group associated with a cardholder. A Multiple Access Group is a container that holds individual Access Groups.  An Access Group contains a list of readers where a cardholder may gain access to a space.  For more information about Access Groups, see <a href="#">"Access Groups" on page 140</a> .

Parameter	Description
Status	<p>The current status of the cardholder is displayed. There are three possible status values:</p> <p><b>Valid:</b> Access is based on the cardholder's Multiple Access Group.</p> <p><b>Invalid:</b> The cardholder's Multiple Access Group is overridden and the cardholder's access rights are denied.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> To set a finite period for a cardholder's <b>Valid</b> setting, the <b>From Date</b> and <b>Expire Date</b> parameters in the cardholder's details must be set accordingly.</p> </div> <p><b>Archived:</b> The cardholder's access rights and settings are frozen. The cardholder cannot be assigned a badge or be granted authorizations. However, an archived cardholder is still in the system database and may be restored at any time.</p>
From Date	The date and time, when a cardholder's <b>Valid</b> setting begins.
Expire Date	The date and time, when a cardholder's <b>Valid</b> setting ends.
Badge Template	<div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> This column is only relevant for GuardPoint10 installations that include the Badge Template module.</p> <p>For information about the Badge Template module, see "<a href="#">Badge Templates</a>" on page 293.</p> </div> <p>The name of the badge template that will be used when the badge assigned to the cardholder is printed. The template determines the layout and cardholder details that will appear on a cardholder's printed badge.</p>
Last Pass Reader	The name of the reader where a cardholder last scanned their badge, used a PIN code or a combination of the two, depending on various parameter settings.
Last Pass Date	The date and time when a cardholder last scanned their badge, used a PIN code or a combination of the two, depending on various parameter settings.
Badge Code	The badge code or codes assigned to a cardholder. If a cardholder does not have a badge assignment, no badge code will be displayed.
Car License Plate	The license plate number of the cardholder as it was entered in the cardholder's details' Personal tab (see " <a href="#">Personal Tab</a> " on page 614).
Email	The email address of the cardholder as it was entered in the cardholder's details' Personal tab (see " <a href="#">Personal Tab</a> " on page 614).
Mobile	The mobile phone number of the cardholder as it was entered in the cardholder's details' Personal tab (see " <a href="#">Personal Tab</a> " on page 614).
ID	The identification number (ID) assigned to a cardholder. If a cardholder does not have an ID, no value will be displayed.

# Report Pagination Controls

The area below the Cardholder Report table that allows you to page through cardholder data quickly. The pagination controls are only visible when the cardholder data require it. If all of the data fit in the table on one page, the pagination controls are hidden.

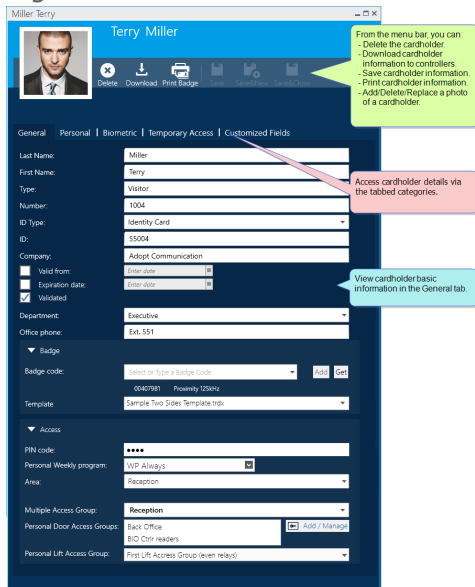
Table A-44 Report Pagination Options

Paging Option	Description
	Goes to the first page of the report table.
	Goes to the previous page of the report table.
	Goes to the next page of the report table.
	Goes to the last page of the report table.
Page <input type="text" value="4"/> of 4	Enter a page number in the field, and then press the <b>Enter</b> key. The specified page is displayed.



# Operator (User): MultiSite Impact Cardholder Details

Figure A-63



The top of the cardholder details includes the following:

» Menu bar:

- » **Delete:** Erases the cardholder from the system database. You cannot restore a delete cardholder.
- » **Download:** Send cardholder details to local controller databases. The controllers, where the details are sent, are determined by the readers, where the cardholder has access authorization.
- » **Print Badge:** Opens the Badge Template dialog where the cardholder's badge appears with the currently assigned template. The displayed badge can be printed or exported from the Badge Template dialog.

If the cardholder has more than one badge code, any of the badge codes may be selected in the Badge Template dialog.

If the cardholder does not have a badge code, the Badge Template dialog will be disabled.

- » **Save:** Saves the cardholder details in the system database and possibly follow-up with another action (Close details or Open details for a new cardholder).
- » **Photo ID:** Visual identification of a cardholder. If a cardholder does not a photo in the system, an avatar will be used as a placeholder.

Cardholder details are located in three tabs. Each tab contains detail parameters affiliated with the tab title. The tabs and their parameter descriptions are as follows:

# General Tab

Figure A-64

General Tab Parameters

Parameter	Description
Last Name	The cardholder's last name as it would appear on the screen.
First Name	The cardholder's first name as it would appear on the screen.
Type	The status of the cardholder in the selected company. The GuardPoint10 built-in types are Employee and Visitor. However, an operator may add additional types as required (see <a href="#">"Adding Customized Fields to Cardholder Details"</a> on page 199).
Number	The internal system number assigned to a cardholder. A cardholder's uniqueness is determined by a combination of a cardholder's first name, last name, and internal system number.
ID Type	The source of the ID number provided in the <b>ID</b> parameter (i.e. Driver License, State Issued ID, Student ID, etc.).
ID	A third-party identification number (i.e. a driver license number) that, if necessary, can be verified by authorities.

Parameter	Description
Company	<p>The name of the company where the cardholder has an association. If the company is already in the system, you can select it from the drop-down list. If the company is not in the system just type it in the field and it will be added to the system database.</p>
Validated From / Expiration Date / Validated	<p>If the cardholder will be valid for a finite period, set the <b>Valid From</b> date and <b>Expire Date</b> date parameters.</p> <p>If the cardholder's validity is open ended (undetermined expiration date), select <b>Validated</b>.</p>
Department	<p>The name of the department, from the selected company, where the cardholder has an association.</p> <p>If the selected department has a Multiple Access Group designation and is initially selected for a new cardholder the designated Multiple Access Group will be used as a default in the <b>Multiple Access Group</b> field.</p>
Office Phone	<p>The phone number and extension where the cardholder may be reached on the premises.</p>
Badge Code	<p>The unique code or codes that identifies a badge, license plate, or biometric markers. A cardholder may have more than one badge code assigned to them. Though, a badge code assignment is not required.</p> <p>If the badge code that will be assigned to a cardholder is already in the system (in the Badges screen) and is free, a filter will be used in this field. The filter is applied to a partially typed badge code or a partially typed badge code description text. Long badge code descriptions are truncated in the cardholder details.</p> <p>If the badge code is unknown or unspecified, use the <b>Get</b> button. The <b>Get</b> button allows you to acquire a badge code via a reader device scan.</p> <p>After acquiring a badge code, (the badge code appears in the <b>Badge code</b> field), the code can be assigned to the cardholder by clicking the blue plus sign "+" next to the field. Assigned badge codes appear below the <b>Badge code</b> field along with the badge codes <b>Type</b> designation.</p>
Template	<div style="border: 1px solid black; padding: 5px;"> <p><b>Note:</b> This parameter is only relevant for GuardPoint10 installations that include the Badge Template module.</p> <p>For information about the Badge Template module, see <a href="#">"Badge Templates" on page 293</a>.</p> </div> <p>The name of the badge template that will override the default template of the assigned cardholder's status <b>Type</b>. The template determines the layout and cardholder details that will appear on a cardholder's printed badge.</p>

Parameter	Description
PIN Code	<p>(<b>P</b>ersonal <b>I</b>dentification <b>N</b>umber) Used where a keypad is available. The PIN may be required depending on the settings.</p> <div data-bbox="448 304 1471 696" style="background-color: #4F81BD; color: white; padding: 10px;"> <p><b>Sample Scenarios:</b></p> <p>Scenario 1: If a cardholder requests access outside of their normal green period, in addition to scanning their badge, they may be required to enter a PIN on a reader device that includes a keypad.</p> <p>Scenario 2: If a cardholder requests access via a reader that is currently in its white period (determined in the reader's Weekly Program), the reader's white period rules may require the cardholder to scan their card and enter a PIN via the device's keypad.</p> </div> <div data-bbox="448 719 1471 864" style="background-color: #F0E68C; padding: 10px;"> <p><b>Note:</b> The PIN <b>9999</b> is a special code. If a cardholder is issued the PIN code 9999, any four-digit combination can be entered at a keypad (with a badge scan) and it will be acknowledged as the correct PIN code.</p> </div> <p>If a cardholder is assigned a PIN, they are automatically assigned a duress code too. A cardholder's duress code is their PIN incremented by 1. For example, a cardholder with a PIN of 1234 will have a duress code of 1235. And if a PIN code is 1239, the duress code will be 1240.</p> <p>With a duress code, a cardholder is granted access (according to normal access rules), but the entry in the Event log indicates that the entry was requested under duress and the operator should take appropriate action.</p> <div data-bbox="448 1167 1471 1312" style="background-color: #F0E68C; padding: 10px;"> <p><b>Note:</b> A duress code may only be used at a reader where the <b>Access Authorization</b> is set to <b>With Badge and Keypad</b>. For more information about <b>Access Authorization</b>, see "<a href="#">Reader Details</a>" on page 453.</p> </div>

Parameter	Description
Personal Weekly Program	<p>Applies a Weekly Program, selected for a particular cardholder, to a reader that also has WP Personal selected. The Personal Weekly Program is included in the Multiple Access Group selection, which has a <b>WP Personal</b> Weekly Program association.</p> <div data-bbox="448 376 1469 680" style="background-color: #4F81BD; color: white; padding: 10px;"> <p><b>The Personal Weekly Program is implemented in the system as follows:</b></p> <p>In an Access Group, when a reader is assigned the Weekly Program called <b>WP Personal</b>, the system determines the access green period by the Personal Weekly Program parameter value of each individual cardholder after they swipe their badge at the reader.</p> </div> <hr/> <p><b>Note:</b> If a cardholder does not have a value in their Personal Weekly Program parameter, the system will use the <b>WP Never</b> default value.</p>
Area	<p>Identifies the area where a cardholder is currently located. This value is determined by the cardholder's badge swipe. An operator may select a different area from the <b>Area</b> drop-down list, this selection will override the previously displayed value.</p> <p>For information about the Area module, see "<a href="#">Area</a>" on page 315.</p>

Parameter	Description
Global Anti-Passback (GAPB) (may not be visible)	<p>Displayed when the Options screen's setting <b>GAPB</b> is set to <b>Yes</b>.</p> <p>Displays the GAPB location (GAPB level) of the cardholder as it is saved in a controller's local database.</p> <p>The two buttons used to manage the GAPB level and resolve any conflict with the <b>Area</b> field just above it.</p> <p>For example, if a cardholder goes from Office, which is a GAPB area, to, Kitchen, which is <i>not</i> a GAPB area. The cardholder's <b>Global Anti-Passback (GAPB)</b> field is unchanged and shows <b>Office</b>, but the <b>Area</b> field will update and show <b>Kitchen</b>, which is the physical location of the cardholder.</p> <p>The buttons are:</p> <ul style="list-style-type: none"> <li>» <b>Send GAPB</b>: Broadcasts command 26 to all relevant networks in the system.</li> <li>» <b>Clear GAPB</b>: Moves the cardholder from the current GAPB level (area) to <b>Not located</b>. The cardholder that was moved to <b>Not located</b> will now also have a Free Access Granted event at any reader. This means that a cardholder can exit one GAPB area and enter another GAPB area even if it violates a GAPB rule.</li> </ul> <p>For information about Global Anti-Passback, see "<a href="#">Understanding Anti-passback in GuardPoint10</a>" on page 80.</p> <hr/> <p><b>Note:</b> The Free Access Granted event is not area or GAPB area specific. The cardholder may swipe for a Free Access Granted event at any available reader in the system.</p>

Parameter	Description
Multiple Access Group	<p>The Multiple Access Group assigned to a cardholder. A Multiple Access Group is a container that holds individual Access Groups.</p> <p>An Access Group contains reader information used to determine which controllers will download the assigned cardholder's badge code. For more information about Access Groups, see <a href="#">"Access Groups" on page 140</a>.</p> <hr/> <p><b>Note:</b> If a cardholder is of type <b>Visitor</b>, only the Multiple Access Groups permitted to be assigned to a visitor will be available in the <b>Multiple Access Group</b> drop-down list. A Multiple Access Group is made available to visitors via the Access screen's Multiple Access Group tab.</p> <hr/> <p><b>Note:</b> For cardholders with Temporary Access.</p> <p>If a cardholder has temporary access scheduled via a Multiple Access Group, the word "<b>Schedule</b>" will appear in red after the <b>Multiple Access Group</b> field. The field will not be editable until the temporary access has expired.</p> <p>For more information about temporary access, see <a href="#">"Temporary Access Tab" on page 617</a>.</p> <hr/> <p><b>Note:</b> The Multiple Access Groups available for assignment to a cardholder depends on the profile of the operator creating the assignment. For information about Profiles, see <a href="#">"Profiles" on page 91</a>.</p>
Personal Door Access Groups	<p>A list of one or more Door Access Groups assigned directly to a cardholder bypassing a Multiple Access Group. Manage the list of Door Access Groups via the <b>Edit</b> button next to the list. Selected Door Access Groups are listed in order of priority.</p> <p>Where a conflict exists with the selected Multiple Access Group and a Personal Door Access Group, the Personal Door Access Group assigned directly to a cardholder takes priority over the assigned Multiple Access Group.</p> <p>A Personal Door Access Group contains reader information used to determine which controllers will download the assigned cardholder's badge code. For more information about Access Groups, see <a href="#">"Access Groups" on page 140</a>.</p> <p>To address a conflict within the Personal Door Access Group list, the list that appear in the details are listed by priority.</p> <hr/> <p><b>Note:</b> A cardholder of type visitor may be assigned the Door Access Group <b>Anytime Anywhere</b> via the Personal Door Access Group list, even though the Multiple Access Group <b>Anytime Anywhere</b> will not be available to a cardholder of type visitor.</p>

Parameter	Description
Personal Lift Access Group	<p>A drop-down list where a single Lift Access Group may be assigned directly to a cardholder.</p> <p>A Lift Access Group contains relay information used to determine which controllers will download the cardholder's badge code and enable a set of lift panel buttons. For more information about Access Groups, see <a href="#">"Access Groups"</a> on page 140.</p> <p>Where a conflict exists with the selected Multiple Access Group and a Lift Access Group, Personal Lift Access Group assigned directly to a cardholder takes priority over the assigned Multiple Access Group.</p>

## Personal Tab

Figure A-65

Personal Tab Parameters

Parameter	Description
Car License Plate	Cardholder's vehicle license plate number.
Phone/Fax	Cardholder's landline number or fax number.
Mobile	Cardholder's cell phone number.
Email	Cardholder's email address.

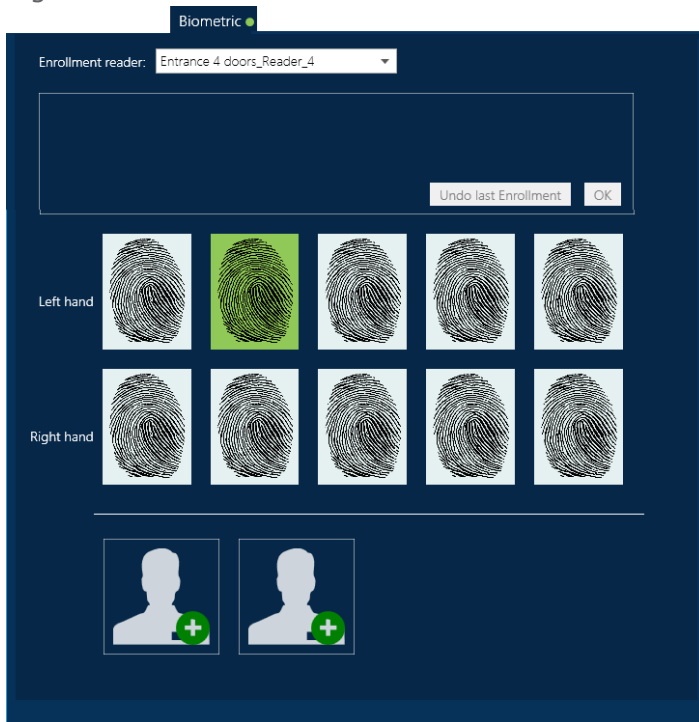


Parameter	Description
Description	<p>A free text field for information relevant to the cardholder's use of the security system. For example:</p> <ul style="list-style-type: none"> <li>» Handicapped Status.</li> <li>» Additional vehicles available to the cardholder.</li> <li>» The number of badges that the cardholder has previously reported stolen.</li> </ul>
Street, Apt.	Cardholder's home address.
City	The city or town where the cardholder lives
Post Code	A series of digits and/or letters included in a cardholder's postal address.
At motorized reader, badge is not returned	Relevant where a badge is scanned inside a reader. When selected, the device performs a standard insert & scan operation, but after the scan, the reader holds on to the badge and does not return it to the cardholder.
No APB, No Timed Anti-passback	<p>When selected, the cardholder will be excluded from any Anti-passback rules on a reader level.</p> <p>For more information about APB, see <a href="#">"Anti-passback" on page 466</a>.</p>
No Access during Holidays	When selected, access is granted only during the defined workweek's green period, not Holidays or Special days, regardless of what the Weekly Program may indicate.
Reset APB Area When Downloading	<p>When selected, the APB will be reset for the cardholder when controller data is downloaded.</p> <p>This means that if a cardholder swipes their badge at a reader where Anti-passback exists, and then their cardholder information is downloaded to the reader's controller in an unrelated action, the cardholder will be able to swipe their badge again at the same reader successfully thereby restarting the anti-passback rule.</p> <p>For more information about APB, see <a href="#">"Anti-passback" on page 466</a>.</p> <hr/> <p><b>Note:</b> This gives the cardholder one access event 'free' of APB checking. When GAPB is requested, it also allows the system to re-synchronize the APB level of the cardholder. The next access granted at any reader will update the APB level from this reader so that a new APB sequence from this level can be started.</p>
Escort Setting buttons	The following radio buttons determine the escort rule that will be applied to a cardholder or supervisor after a badge swipe.
Supervisor	The individual does not require an escort at a reader, regardless of the reader's <b>Escort</b> parameter setting.

Parameter	Description
Basic Supervisor	The individual requires an escort at a reader where the reader's <b>Escort</b> parameter is set to <b>Yes</b> . The escort may be a Cardholder or Supervisor.
Cardholder	The individual requires an escort at a reader where the reader's <b>Escort</b> parameter is set to <b>Yes</b> . The escort may be a Cardholder or Supervisor. Default setting.
Basic Cardholder	The individual requires an escort at a reader where the reader's <b>Escort</b> parameter is set to <b>Yes</b> . The escort must be a Supervisor or Basic Supervisor.

## Biometric Tab

Figure A-66



If one or more biometric samples are enrolled, a green dot will be appended to the Biometric tab text. This will allow you to identify the cardholder as having an enrolled biometric sample without opening the Biometric tab.

Biometric Tab Parameters

Parameter	Description
Enrollment Reader	A drop-down list of available biometric readers where an operator selects the reader where a biometric sample will be enrolled.
Undo Last Enrollment (Button)	When clicked, the previous biometric sample enrollment action is removed and the space in the Fingerprint or Face area is made available (changes to white).

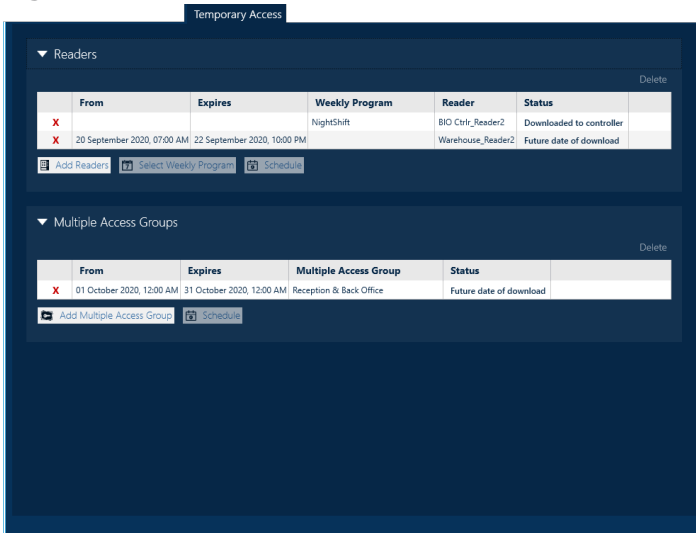
Parameter	Description
OK (Button)	When clicked, the operator confirms that a biometric sample has been successfully scanned and allows the operator to scan another biometric sample.
Fingerprint area	<p>Each fingerprint image represents an opportunity to enroll a fingerprint. The fingerprint images are color code as follows:</p> <ul style="list-style-type: none"> <li>» A fingerprint image with a white background indicates that the image is empty and a fingerprint may be enrolled at that location.</li> <li>» A fingerprint image with a blue background indicates that the fingerprint image is in Scan mode. A finger may be placed in the reader where it will be scanned and enrolled in the blue image location.</li> <li>» A fingerprint image with a green background indicates that a fingerprint has been scanned and enrolled at the green image location.</li> </ul> <p>Two consecutive scans are required for a fingerprint to be enrolled.</p>
Face area	<p>Two samples of a cardholder's picture (face) can be stored as a biometric sample. The samples are used to compare facial markers with those of an individual attempting to gain access via a facial recognition reader.</p> <p>Each sample is displayed in the Biometric tab.</p> <p>There is no relationship between the image at the top left of a cardholder's details and the Biometric sample.</p>

**Note:** When reading a face or fingerprint, some biometric readers display a badge code on the reader screen during the verification. This badge code is intentionally incorrect. For security reasons, the actual badge code assigned to the biometric sample is never displayed on the reader screen.

## Temporary Access Tab

The parameters in this tab are for cardholders who are temporarily assigned to a space. For example, an employee reassigned to an alternative office because their normal office is being painted.

Figure A-67



There are multiple approaches when assigning temporary access to a cardholder. You can:

- » Assign a specific reader with a Weekly Program.
- » Assign a specific reader with a date range.
- » Assign a Multiple Access Group with a date range.
- » Assign a Multiple Access Group or a specific reader without a Weekly Program or date range. This would make the Temporary Access item an ad hoc non-temporary reader or Multiple Access Group.

All of the approaches that include a Weekly Program or date range option allow the cardholder access authorization for a finite amount of time.

If there is a conflict between a Temporary Access item and the Multiple Access Group, Door Access Group or, Personal Lift Access Group found in the General tab, the Temporary Access item has priority.

For step-by-step instructions about providing temporary access to a cardholder, see "[Temporary Access](#)" on page 168.

Temporary Access Tab Parameters

Parameter	Description
<b>Reader area</b>	
From	The date and time when the cardholder may begin to gain access via the reader.
Expires	The date and time when the cardholder can no longer gain access via the reader.
Weekly Program	The Weekly Program assigned to the reader specifically for this cardholder's temporary access.
Reader	The name of the reader.
Status	Indicates whether the information in the reader row has been saved.

Parameter	Description
<b>Multiple Access Groups area</b>	
From	The date and time when the cardholder may begin to gain access via the reader included in the Multiple Access Group.
Expires	The date and time when the cardholder can no longer gain access via the reader included in the Multiple Access Group.
Multiple Access Group	The name of the Multiple Access Group where Access Groups, and their readers, are located.
Status	Indicates whether the information in the Multiple Access Group row has been saved.

## Customized Fields Tab

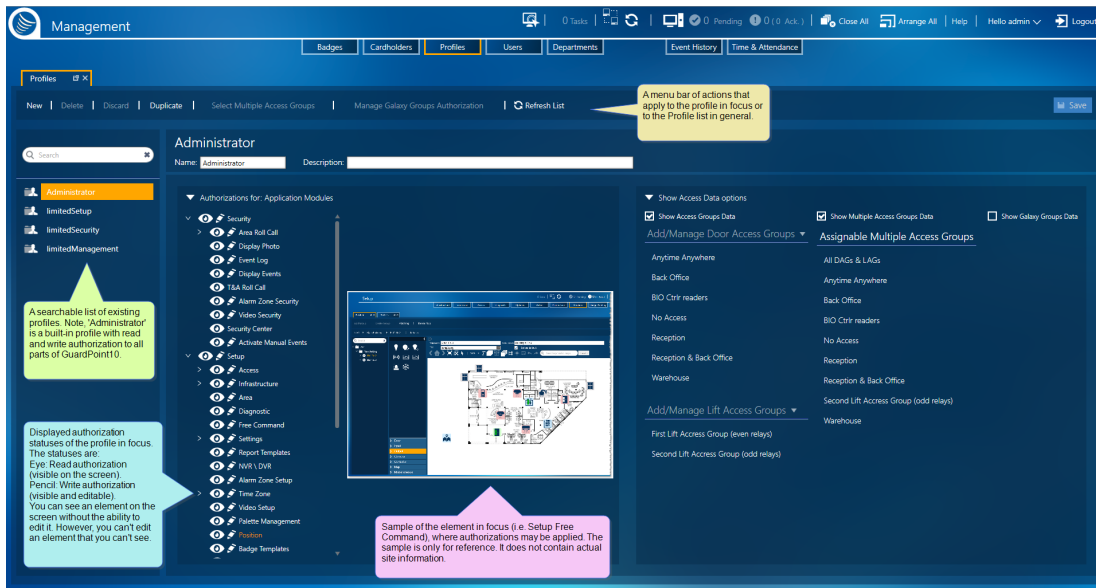
Figure A-68

The content of the Customized Fields tab is set in the Customized Fields window. The Customized Fields window is opened via the Cardholders screen. For more information, see "[Adding Customized Fields to Cardholder Details](#)" on page 199.

**Note:** If there are no customized fields defined, the Customized Fields tab will not appear in the cardholder details.






# Profiles Screen

Figure A-69



A profile determines what an operator can and cannot do within GuardPoint10. Administrators group authorizations into sets, called profiles. These profiles are assigned to operators. Every operator associated with a profile has all of the authorizations included in the profile.

There are three categories of GuardPoint10 GUI authorization:

- » **Hidden:** The task screen or element on the screen is hidden from an operator. A dulled, eye icon  with a dulled pencil icon  represents a hidden screen or element where the operator has no authorizations.
- » **Read-only:** An operator may only see the task screen or element on the screen. A white, eye icon  represents a read-only authorization.
- » **Read and Write:** An operator may see and edit the task screen or element on the screen. A white, eye icon  with a white pencil icon  represents a read and write authorization.

For GuardPoint10 systems that have a Galaxy panel integration, there are authorization settings specific to the Galaxy groups belonging to the panel.

To change an authorization setting, click on the relevant icon. The icon Change to white or becomes grayed-out.

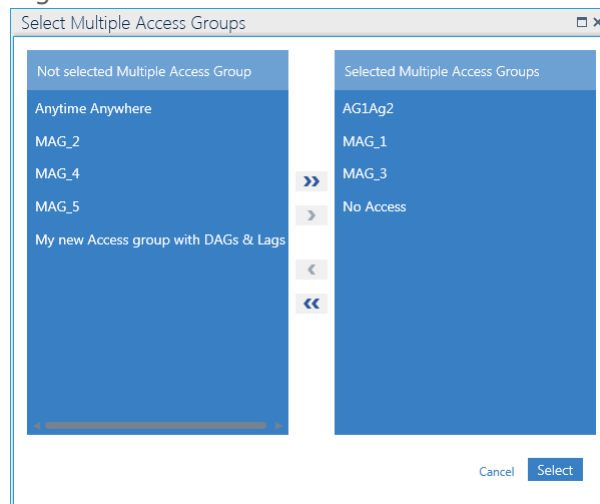
Descriptions of profile parameters and elements that can be authorized are provided below.

## Profile Parameters

Parameter	Description
Name	A descriptive name of the profile as it would appear in the searchable list of existing profiles.
Description	A description of the profile. For example the type of operators who would be attached to the profile.

Parameter	Description
Show Multiple Access Groups Data checkbox (checkbox may not be visible)	<p>Available when Options screen's <a href="#">"Show / Manage Profile Multiple Access Group Data"</a> on page 571 is set to <b>Yes</b>.</p> <p>Shows a list of Multiple Access Groups that may be assigned by an operator with the selected profile.</p> <p>The list of Multiple Access Groups is compiled via the <b>Select Multiple Access Groups</b> button in the action bar.</p> <p>The <b>Select Multiple Access Groups</b> button opens a Select Multiple Access Groups dialog, where Multiple Access Groups may be made available to an operator with the profile.</p> <p>Whenever an operator need to assign a Multiple Access Group, they will only be able to choose from the list of Multiple Access Groups select for their profile.</p> <p>To create a list of Multiple Access Groups, click <b>Add Multiple Access Group Authorization</b>, in a profile's parameter area, to open the Select Multiple Access Group dialog, and then select the Multiple Access Groups that will be available to an operator, with the profile and place them in the right column.</p>

Figure A-70



The **Door Access Groups** and **Lift Access Group** Authorization is based on the contents of the Multiple Access Groups selected.

**Note:** The **Add Multiple Access Group Authorization** is only available when the Options screen General tab's **Profile Multiple Access Group** option is set to Yes.



Parameter	Description
Show Access Group Data Options	<p>Shows a list of data options available based on the Options &gt; General tab settings. These options include:</p> <ul style="list-style-type: none"> <li>» <b>Personal Access Groups</b></li> <li>» <b>Multiple Access Groups</b></li> <li>» <b>Galaxy Groups</b></li> </ul> <p>that are assigned by an operator with the selected profile.</p> <p>Whenever an operator need to assign an Access Group, they will only be able to choose from the list of Access Groups select for their profile.</p> <p>Door and Lift Access Groups can be added or deleted via the <b>Add/Manage</b> button next to the list titles.</p> <p>Multiple Access Groups and Galaxy Group access are managed from the relevant button in the Profile screen's Action bar.</p>



#### Profile Authorization Elements



Authorization	Description
Security	Access available to all Security task screens. This group covers Display Photo through Security Center.
Display Photo	Access available to the Display Photo screen. The Display Photo screen takes access event information, including cardholder information, and displays it with an emphasis on a cardholder's photo.
Area Roll Call	Access available to the Area Roll Call screen, where a cardholder's presents is easily determined (Inside or Outside).
Event Log	Access available to the Event Log screen where access events, alarms, audits, etc. can be viewed in a table.
Display Events	Access available to the Display Events screen, where cardholder access and alarms may be monitored in real time via a table.
Alarm Zone Security	Access available to the Alarm Zone Security screen.
Video Security	Access available to the Video Security screen.
Security Center	Access available to the Security Center screen's graphic display.
Setup	Access available to all Setup task screens. This group covers <b>Access</b> through <b>Badge Templates</b> .
Access	Access available to the Access screen. This group covers <b>Access Groups</b> (door and lift) and <b>Multiple Access Group</b> .
Access Groups	Access available to the Access Groups screen.



Authorization	Description
Multiple Access Group	Access available to the Multiple Access Groups screen.
Infrastructure	Access available to the Infrastructure screens. This group covers <b>Activate Controller(s)</b> through <b>Site Properties</b> .
Activate Controller (s)	Access available to the context menu's Activate command.
Controller Properties	When a controller is in focus, this will provide access to the controller's parameters visible to the right of the infrastructure tree.
Input	When an input device is in focus, this will provide access to the input device's parameters visible to the right of the infrastructure tree.
Local Reflex	When a Local Reflex is in focus, this will provide access to the Local Reflex's parameters visible to the right of the infrastructure tree.
Network Properties	When a network is in focus, this will provide access to the network's parameters visible to the right of the infrastructure tree.
Relay	When a relay is in focus, this will provide access to the relay's parameters visible to the right of the infrastructure tree.
Reader	When a reader is in focus, this will provide access to the reader's parameters visible to the right of the infrastructure tree.
Site Properties	When a Site is in focus, this will provide access to the site's parameters visible to the right of the infrastructure tree.
Diagnostic	Access available to the Diagnostic screen and all of its actionable menu items.
Free Command	Access available to the <b>Send Free Cmd</b> item via the Diagnostic screen's <b>Misc.</b> action menu item. The <b>Misc.</b> menu item is visible after <b>Debug by Diagnostic</b> is set to <b>Yes</b> in the System & SQL tab, available in the Options screen.
Settings	Group name covering License, <b>Options</b> , and <b>Baudrate</b> .
License	Access available to the License window, where the scope of your GuardPoint10 version is documented and changes to the license agreement may be initiated.
Options	Access available to the Options screen, where default options are set for the GuardPoint10 site.
Site Baudrate	Access available to the Baudrate field in the Infrastructure's Site details.
AlarmZone Setup	Access available to the Alarm Zone screen.
Time Zone	Access available to the Time Zone screen. Includes: Daily Programs, Weekly Programs and Holiday.

Authorization	Description
Daily Programs	Access available to a Time Zone's Daily Programs screen.
Holiday	Access available to a Time Zone's Holiday screen.
Weekly Programs	Access available to a Time Zone's Weekly Programs screen.
Video Setup	Access available to the Video Setup screen.
Position	Access available to the Position screen. The Position screen allows you to place icons designating inputs, reflex, processes, actions, and icons representing other maps) on a map page. The map page is monitored by security personnel via the Security Task group's Security Center screen.
Palette Management	Enables the user to add palettes to the Position screen and to add icons to a palette, except for the Default palette.
Badge Templates	Access available to existing badge templates and the Telerik Badge Template Designer.
Activation Wizard	From the Infrastructure screen, access available to the Activation Wizard. This authorization item only has an eye icon  .
Setup Wizard	From the Infrastructure screen, access available to the Setup Wizard. This authorization item only has an eye icon  .
Management	Access available to all Management task screens. This group covers <b>Event History</b> through <b>Users Management and Profiles</b> .
Event History	Access available to the Event History screen.
Cardholder	Access available to the Cardholders screen. This group covers <b>Add Cardholder Type</b> through <b>Import Cardholders</b> .
Add Cardholder Type	Access available to the <b>Add Cardholder Type</b> option in the Cardholder screen's <b>New</b> action menu item. The built-in types are <b>Employee</b> and <b>Visitor</b> .
Biometric Data	Access available to the Biometric tab in a cardholder's details.
Customized Fields Details	Access available to the customized fields added in the Customized Fields window. The customized fields are visible in the cardholder details Customized Fields tab. If there are no customized fields, the tab will not appear in the cardholder details' tab stack.

Authorization	Description
Customized Fields	<p>Access the Customized Fields window via the <b>Customized Fields</b> button in the Cardholder screen's action menu. The following field types may be added to cardholder details via the Customized Fields window:</p> <ul style="list-style-type: none"> <li>» Free text field</li> <li>» Yes/No slider</li> <li>» Number field</li> <li>» Date field</li> </ul>
Temporary Access Details	Access available to the Temporary Access tab in a cardholder's details.
General Details	Access available to the Cardholder Details' General tab.
Personal Details	Access available to the Cardholder Details' Personal tab.
Cardholder Details	Access available to a cardholder's details including all of the details tabs. This includes General, Personal, and Visit Details.
Import Cardholders	Access availability to the Import Cardholders dialog. The maximum number of cardholders that can be imported at one time is 1,500.
Time & Attendance	Access available to the Time & Attendance screen.
Badge	Access available to the Badges screen. This group covers <b>Badge Maintenance</b> through <b>New Badge Series</b> .
Badge Maintenance	Access to the get badge codes from reader devices, via a <b>Get</b> button. The <b>Get</b> button is available in the Badges table and a cardholder's details.
Delete Badge Series	Access available to the Delete Badge Series dialog.
New Badge Series	Access available to the New Badge Series dialog.
Department	Access available to the Departments screen.
User (Operator) Management and Profile	Access available to the Users screen and the Profiles screen. This group covers <b>Profiles</b> through <b>Users</b> .
Profiles	Access available to the Profiles screen.
Users	Access available to the Users screen.
Alarm Operations	<p>Group name covering the <b>Acknowledge</b> through <b>Confirm All</b>.</p> <p>This authorization group item only has an eye icon .</p>
Acknowledge	<p>Controls access to the Acknowledge command. The command can be found in various locations as a button or context menu item.</p> <p>This authorization item only has an eye icon .</p>

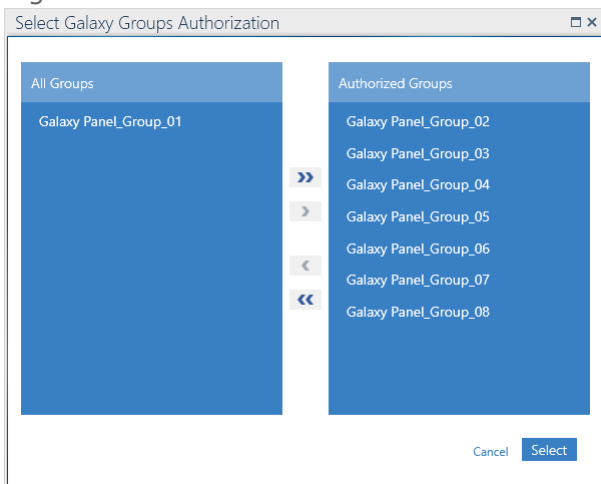
Authorization	Description
Confirm	Controls access to the Confirm command. The command can be found in various locations as a button or context menu item.  This authorization item only has an eye icon  .
Confirm All	Controls access to the Confirm All command. The command can be found in the Unconfirmed Alarms dialog, the Video Security screen, Active Alarms screen, etc.  This authorization item only has an eye icon  .

## Galaxy group-specific authorization management

This section is relevant for GuardPoint10 systems that include a Galaxy integration.

The **Select Galaxy Group Authorizations** button opens a dialog of the same name where Galaxy groups may be added or removed from an existing Authorization list; by default, all groups start in the Authorization list, as long as the Galaxy system was integrated before the profile was added.

Figure A-71

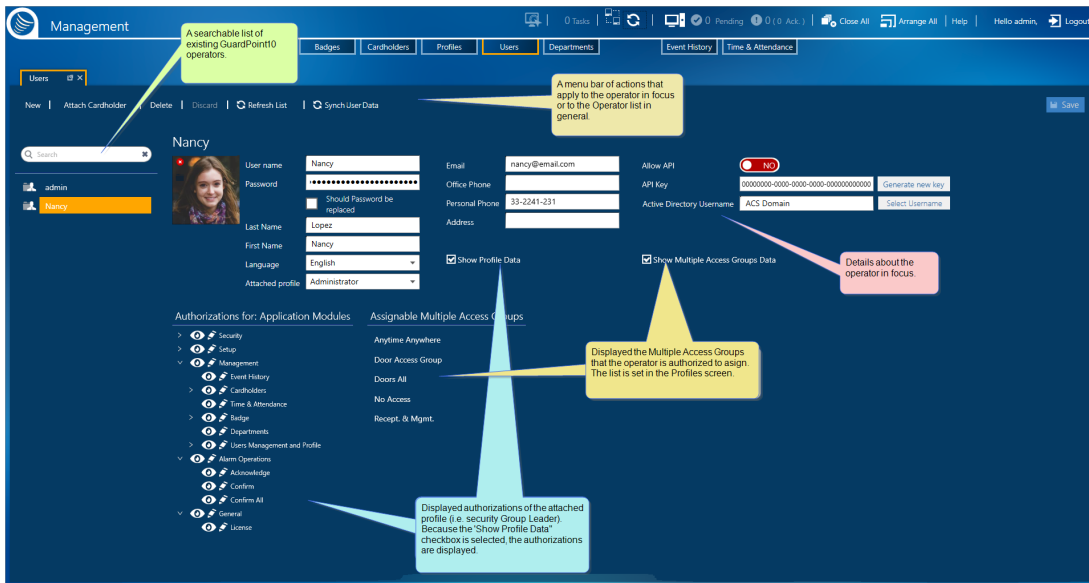


To see a list of authorized Galaxy groups alongside the GuardPoint10 Application Module tree, select the **Show Galaxy Groups Data** checkbox.

# Users Screen

For Operators

Figure A-72



An operator is a person entrusted with security system operations via the GuardPoint10 user interface (GUI). An operator is bound to a set of authorizations, which allow an operator to read or read & write to various parts of the interface. The permissions are grouped into profiles. For more information about profiles, see "[Profiles](#)" on page 91.

An operator is defined by their GuardPoint10 login credentials (operator name and password).

If the user information is automatically taken from a Windows Active Directory, the **Sync User Data** button in the Action bar will update all user data with data from the Active Directory's corresponding fields. However if, the user's Last name or First name fields are filled before clicking **Sync User Data**, the data in the field will not be updated.

A description of operator parameters is provided below.

## Operator Parameters

Parameter	Description
Operator Name	Part of the credentials used to log into GuardPoint10.
Password	Part of the credentials used to log into GuardPoint10.
Should Password be replaced	When the checkbox is selected, the user is forced to change their password the next time they log in to GuardPoint10.
First Name	The operator's first name as it will appear on the screen.
Last Name	The operator's last name as it will appear on the screen.

Parameter	Description
Language	<p>After an operator logs in, this will be the language of the user interface displayed on the screen.</p> <p>The default operator language is chosen via the <a href="#">"Options Screen" on page 567</a>.</p>
Email	The email address of the operator.
Office Phone	The primary office telephone number of the operator.
Mobile Phone	The mobile telephone number of the operator.
Address	The home address of the operator.
Attached Profile	The authorization group (profile) assigned to the operator. For information about Profiles, see <a href="#">"Profiles" on page 91</a> .
Allow API	<p>Set to <b>Yes</b> allows:</p> <ul style="list-style-type: none"> <li>» The user's API Key to be available for API user (operator) authentication. If it is set to <b>No</b>, the authentication fails regardless of the <b>API Key</b> value.</li> <li>» The user to log in to the <b>GuardPoint10 Web module</b><sup>1</sup> with their user name and password.</li> </ul> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this parameter setting.</p>
API Key	<p>A user-controlled string that authenticates the user (operator) in an API. This string exists for specific resources (i.e. controllers, relays, etc.).</p> <hr/> <p><b>Note:</b> Unless instructed by your API developer, do not change this parameter setting.</p>

<sup>1</sup>The WebApp is a limited version of the GuardPoint10 interface. It is available on any device that supports HTML5. To learn how to connect to the module, contact your provider.

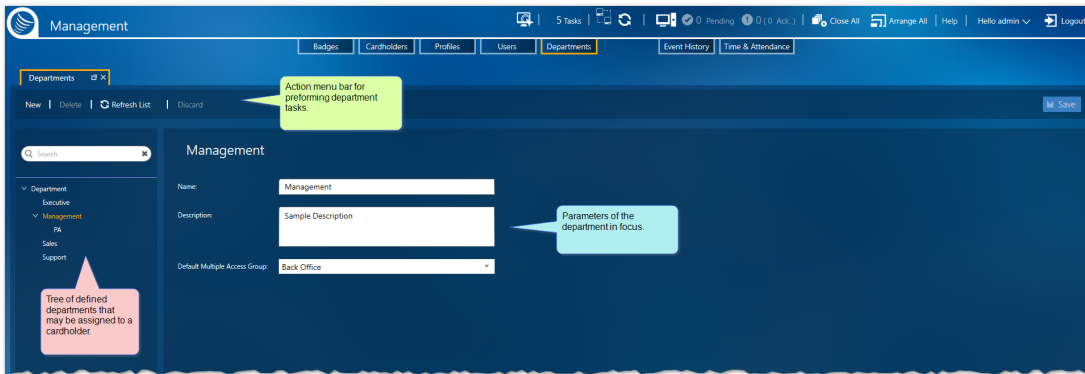
Parameter	Description
Active Directory User Name (may not be visible)	<p>Displays when the Option <b>Enable Active Directory</b> is set to <b>Yes</b>.</p> <p>The field shows the selected Active Directory (Windows) username credential . The accompanying <b>Attach</b> button opens a dialog where an existing Windows login username can be selected and attached for the selected GuardPoint10 user.</p> <p>If a Windows login username is selected, the GuardPoint10 user will be able to log in to GuardPoint10:</p> <ul style="list-style-type: none"> <li>» With a single click of the <b>Login with Windows Credentials</b> button found on the Login screen.</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>» Enter their GuardPoint10 user name and password, and then click <b>LOGIN</b> on the Login screen.</li> </ul> <p>After attaching a Windows user to an GuardPoint10 user, multiple fields in the user's details are automatically filled in with user information from the Active Directory. These fields will remain editable.</p> <p>Click the <b>Detach</b> button the separate an GuardPoint10 user from the Windows user. The fields that were automatically filled in will remain filled and editable.</p> <p>The only way an GuardPoint10 user can log in to GuardPoint10 is by entering their user name and password, and then click <b>LOGIN</b> on the Login screen.</p>
Show Profile Data	<p>When selected, a read-only expandable tree listing the parts of the GuardPoint10 GUI with the operator's profile authorization settings are displayed.</p>
Show Multiple Access Group Data	<p>When selected, a read-only list of Multiple Access Groups that the operator is authorized to assign is displayed.</p> <p>The <b>Show Multiple Access Group Data</b> checkbox only appears when the Options screen's <b>Profile Multiple Access Group</b> General option is set to Yes.</p>



**Note:** The **Show Profile Data** and the **Show Multiple Access Group Data** displayed content is dependent on the **Attached Profile** selected for the operator.

# Departments Screen

Figure A-73



A department is assigned to a cardholder and is used as a management criteria for table views and report generation.

A description of department parameters is provided below.

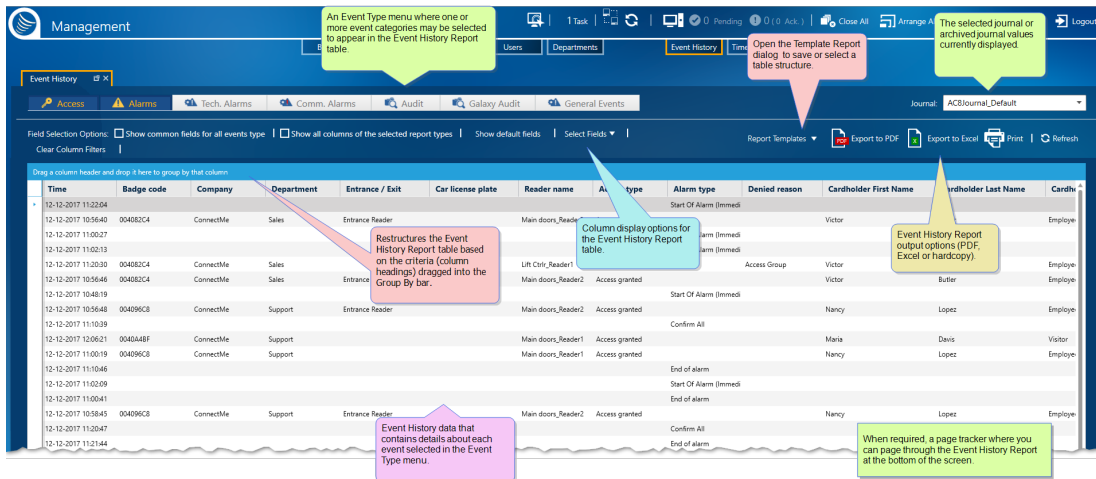
### Department Parameters

Parameter	Description
Name	A free text field that identifies the department. The department name must be unique.
Description	(Optional) A free text field where information about a department is entered.
Default Multiple Access Group	<p>The Multiple Access Group automatically assigned to a new cardholder, who has not been saved yet, after the cardholder is assigned to the department in focus. The Multiple Access Group for an individual cardholder can be changed at any time via the cardholder's details or the Cardholder screen's table.</p> <p>A department's Multiple Access Group assignment can be changed at any time and will impact new cardholders added from that point forward. Where a conflict exists between the assigned Multiple Access Group and an assigned Personal Door Access Group or Personal Lift Access Group, the Personal Door Access Group or Personal Lift Access Group will take priority over the Multiple Access Group.</p> <p>If <b>Default Multiple Access Group</b> is set to <b>Anytime Anywhere</b>, a cardholder, of type <b>Visitor</b>, will bypass the default setting and initially be set to <b>No Access</b>.</p> <p>For more information about cardholder details, see <a href="#">"Operator (User): MultiSite Impact Cardholder Details"</a> on page 607.</p>



# Event History Screen

Figure A-74



Each event that takes place in the system is recorded in the system database. The Event History screen allows you to manage these past events to create a concise, legible Event History report that can be shared with relevant personnel.

The system treats the Event History screen as a report where information can be filtered, sorted, and grouped according to the needs of the operator.

The information displayed in the report can be from the current journal or a previously archived journal. Select the journal or archive from the **Journal** drop-down list. For more information about archived journals, see "[System Database and Journal Management Options](#)" on page 239 and "[Load and View a Previously Archived Journal](#)" on page 252.

An Event History report's manual output may be in a PDF format or an Excel format. In addition, the report may also be printed.

An Event History report may be saved as a Report Template via the action bar **Report Template** button. The advantages of a report template are:

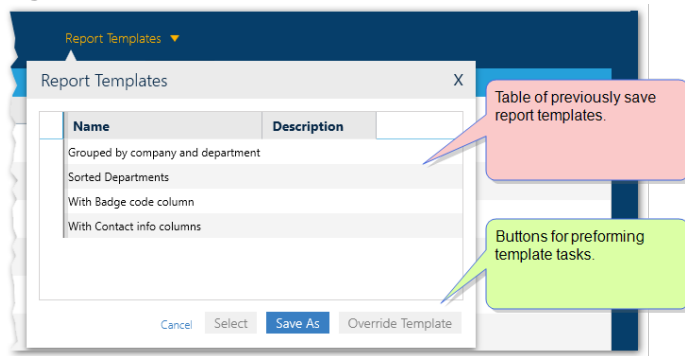
- » Load and display a complex report structure with a couple of clicks.
- » Automatically save a template report to file or email it to others via a global reflex "[Create Template-based report](#)" on page 548 action.

## Report Template dialog

The structure of the screen table can be saved in a template so it can be applied later, either to the screen display or a global reflex "[Create Template-based report](#)" on page 548 action. The data in a template is dynamic and will change to reflect the environment.

To start using templates click the **Report Templates** button.

Figure A-75



The table in the Report Template dialog contains the names and descriptions of previously save templates, which are specific to the screen displayed.

From the screen's Report Template dialog you can click:

- » **Save As:** Opens the "Report Template Screen" on page 529, where the current structure of the displayed table can be saved.
- » **Override:** Opens the "Report Template Screen" on page 529, where the current structure of the displayed table can override the last selected template with the current structure of the displayed table.
- » **Select:** Displays current data in the template selected from the dialog's table.

The Event History screen includes four distinct areas:

## Event Type Menu

The menu allows you to choose one or more types of events that will appear in the Event History Report table. A selected Event Type has a blue background and an unselected Event Type has a white background.

Table A-45 Event Type Menu Options

Event Type	Description
Access	Any event related to access.
Alarms	Any event related to an alarm triggered by a security-related rule (i.e. an invalid PIN has been entered multiple times within a 2 minute period).
Tech Alarms	Any event related to an alarm triggered by an internal system hardware or software event (i.e. controller switched to an internal power source).
Comm. Alarms	Any event related to an alarm triggered by a system communication issue.
Audit	Any audit event, excluding Galaxy-related events.
Galaxy Audit	Galaxy-related event.

Event Type	Description
General Events	Internal system events that do not fall into any of the other categories of events on the screen. For example, scheduled database log maintenance operations.

## Column Selection Options

The area contains powerful column display options for the Event History Report table.

Table A-46 Column Selection Options

Column Option	Description
Show common fields for all event types	The same five columns, regardless of the type(s) of events selected from the Event Type menu, are displayed. These columns are as follows: <b>Time:</b> A timestamp indicating the date and time when the event occurred. This column appears for all event types whether <b>Use common fields for all event types</b> is selected or not. <b>From:</b> Where the event originated. <b>Transaction:</b> The action that caused the event. <b>Data:</b> Information included in the transaction <b>Denied reason:</b> Elaboration about why the expected result was denied.
Show All Columns of the Selected Report Types	All columns, regardless of the event type(s) selected, are displayed.
Show Default Fields	Only those default columns related to the selected event type(s) are displayed.
Select Fields	Allows you to cherry-pick the columns that will display from a rollout list of available columns. The available columns are determined by the event types selected.

## Report Options

The area contains export options for the displayed Event History Report table.

Table A-47 Report Options

Option	Description
Report Template	Opens a dialog where a template may be selected saved or overwritten.

Option	Description
Export to PDF	Takes the column data of the currently displayed report table and generates a PDF file. The PDF file can be easily transferred to a third-party outside the system, where it can be viewed with a PDF reader (i.e. Adobe Acrobat <sup>®</sup> Reader).
Export to Excel	Takes the column data of the currently displayed report table and generates an Excel spreadsheet (XLS file) that can easily be transferred to a third-party outside the system and viewed in any application that supports XLS or XLSX file formats.
Print	Takes the column data of the currently displayed report table and generates hardcopy (paper) output via your selected printer.



**Warning:** When you circulate an exported Event History report, confidential data may be inadvertently revealed to unauthorized sources.

## Event History Report table

For information about table filters, see **"Table Filters" on page 695**.

The **Grouped By** bar, located just above the table column headings, restructures the report table based on the criteria (column heading) dragged into the **Grouped By** bar.

To change the report table's structure:

- » Select a column heading and drag it to the **Grouped By** bar, the heading becomes a criteria, and the report table reflects the new criteria structure.
- » Re-order criteria already in the **Grouped By** bar (drag and drop one criteria in front of another) changes the structure applied to the report table.
- » **Mouseover**<sup>1</sup> a criteria already in the **Grouped By** bar and click the delete **x** on the right side of a criteria frame; the criteria is removed.



**Note:** If there are more than 400,000 pages (10 million entries), the **Grouped By** bar will be disabled.

A description of each column in the Event History Report table, broken down by Event Type, is provided below.



**Note:** The Time column appears for all event types. It shows the date and time that an event occurred.

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

## Event Type: Access

Table A-48 Access Event Type Table Columns

Parameter	Description
Access Type	<p>The result of the access attempt (i.e. <b>Access Granted</b> or <b>Access Denied</b>).</p> <p>The <b>Access Denied</b> type appears with a simple clear explanation why access was denied (i.e. "Unknown Badge Code"). However, there is one <b>Access Denied</b> type called <b>Inhibited Cardholder</b> that may require some more information.</p> <p>The <b>Inhibited Cardholder</b> type may occur in the following two cases:</p> <p>A reader has the weekly program <b>WP Personal</b> selected in the access group of the cardholder, and the cardholder does not have a Personal Weekly Program selected in their details.</p> <p>A reader assigned <b>Badge Type</b> does not match the badge type of a cardholder's swiped badge.</p>
Badge Code	A unique code assigned to the badge used in an attempt to access the premises. The code is detected when the badge is swiped at a reader.
Cardholder First Name	The first name of the cardholder assigned to the badge that was used in the access attempt.
Cardholder Last Name	The last name of the cardholder assigned to the badge that was used in the access attempt.
Cardholder Type	The nature of the cardholder's relationship to the workplace (i.e. Employee, Visitor, etc.).
Car License Plate	<p><b>Note:</b> This column is only relevant when the reader is of <b>Badge Type License Plate Recognition</b>.</p> <p>The plate number is recorded by the camera at an entrance, and then translated into an 8-digit Proximity 125kHz code. This code is sent to the reader's controller where it is treated as a badge number.</p>
Company	The name of the company where the cardholder has an association.
Denied Reason	If access was denied, this column elaborates on the reason why it was denied.
Department	The name of the department, from the selected company, where the cardholder has an association.

Parameter	Description
Entrance / Exit (T&A Reader)	<p>A designation of a reader's access event. The event may be one of the following:</p> <p><b>Entrance:</b> A cardholder entered a space.</p> <p><b>Exit:</b> A cardholder exited a space.</p> <p><b>Entrance or Exit:</b> A cardholder entered or exited a space.</p> <p><b>None:</b> No designation is applied to a reader event.</p>
Escort Badge Code	<p>A unique code assigned to the badge used by the escort cardholder. The escort must accompany the cardholder who is attempting to access the premises. The code is detected when the badge is swiped at a relevant reader. A relevant reader is a reader that has its <b>Escort</b> parameter is set to <b>Yes</b>.</p> <p>(Optional column)</p> <p>For information about escort rules, see <a href="#">"Escort Rules for Access Events" on page 697</a>.</p>
Escort First Name	<p>The first name of the cardholder assigned to the <b>Escort Badge Code</b>.</p> <p>(Optional column)</p>
Escort Last Name	<p>The last name of the cardholder assigned to the <b>Escort Badge Code</b>.</p> <p>(Optional column)</p>
Is Escort	<p>A checkbox indicator that identifies whether the Escort rules apply to the reader.</p> <p>(Optional column)</p> <p>For information about escort rules, see <a href="#">"Escort Rules for Access Events" on page 697</a>.</p>
Is Slave	<p>A checkbox indicator that identifies whether the reader where the cardholder attempted to enter is a slave reader.</p> <p>For information about slave readers, see <a href="#">"Has a Slave Reader" on page 455</a>.</p> <p>(Optional column)</p>
Reader Name	<p>The reader where an access event took place.</p>
Time	<p>The timestamp when an access event occurred.</p>
Transaction Code	<p>When a cardholder is granted access at a specific reader, a transaction code is associated with the transaction.</p> <p>For information about transaction codes, see <a href="#">"Convention for Reader Transaction Codes" on page 710</a>.</p> <p>(Optional column)</p>

## Event Type: Alarms

Table A-49 Alarm Event Type Table Columns

Parameter	Description
Alarm Type	The rule or event state that caused the alarm.
Confirmed Comments	When confirming an individual alarm, there is an opportunity to include a description. This column displays the description.
Input Name	The name of the input device where the alarm was triggered.
Is Acknowledged	A checkbox indicator that identifies whether an alarm was acknowledged.
Is Confirmed	A checkbox indicator that identifies whether an alarm was confirmed.
User First Name	The first name of the operator who Confirmed the alarm. (Optional column)
User Last Name	The last name of the operator who Confirmed the alarm. (Optional column)

## Event Type: Tech. Alarms

Table A-50 Tech. Alarm Event Type Table Columns

Parameter	Description
Technical Controller Name	The type of controller (manufacturer's product name) where the reader and or input is connected.
Technical Type	The technical event that caused the alarm.
Technical Input Name	The type of input (manufacturer's product name) where the alarm was triggered. (Optional column)
Technical Reader Name	The type of reader (manufacturer's product name) where the alarm was triggered.
Time	The timestamp when a technical alarm occurred.

## Event Type: Comm. Alarms

Table A-51 Comm. Alarm Event Type Table Columns

Parameter	Description
Comm. Controller Name	The type of controller or controller name where the communication alarm was triggered.

Parameter	Description
Comm. Network Name	The network name where the communication alarm was triggered.
Comm. Type	The communication event type that caused the alarm.
Reader Name	The reader name where the communication alarm was triggered. (Optional column)
Time	The timestamp when a communication alarm occurred.

## Event Type: Audit

*Table A-52 Audit Event Type Table Columns*

Parameter	Description
Audit Type	The event type that caused the audit.
Audit Data	The data that initiated where the audit event took place.
Entity Name	The data table where the audit took place.
Time	The timestamp when an audit occurred.
Audit User Name	The login user name of the operator who initiated the event that caused the audit.

## Event Type: Galaxy Audit

Any Galaxy action performed via GuardPoint10 (Group set, Unset, Part set, Zone omitted, etc.) automatically creates an audit event.

*Table A-53 Galaxy Audit Event Type Table Columns*

Parameter	Description
Time	The time and date that when the Galaxy alarm event took place.
Galaxy Panel Name	The name of the Galaxy panel, integrated into GuardPoint10, where the alarm event was managed.
Zone Name	The Galaxy zone where the alarm was triggered or, the zone that was edited.
Description	A short description of an event that took place in the Galaxy panel. When displayed in uppercase characters (e.g. 'Group has been set – FULL SET REMOTE' ) it means that GuardPoint10 has received confirmation that the Galaxy panel has updated the corresponding status.



Parameter	Description
Event Code	A Galaxy-specific event code. For more information about the code, see your Galaxy documentation.
Event Description	A short description of an event that took place in the Galaxy panel.
Event Group	The Galaxy group where the triggered zone or, edited zone is located.
Is New Alarm	When the box is filled, the event was an alarm event and it was triggered recently.
Peripheral	
SIA Data Block	GuardPoint10 uses SIA protocol in its driver code to communicate with a Galaxy panel. The data block displayed identifies the code used in the event.
Site Code	
User Number	The Galaxy number assigned to the user who made the action.
Zone Number	The unique number used to identify the zone where an event took place. The event may not be specific to a zone; in this case, there will be no value displayed.

## Event Type: General Events

Any internal GuardPoint10 system operation creates an audit event.






**Table A-54** *General Events Type Table Columns*

Parameter	Description
Time	The time and date that when the actuated operation took place.
Operation name	The name of the internal operation actuated.
Activation	The nature of the event that actuated the operation.
Additional Information	More detailed information about the actuated operation.

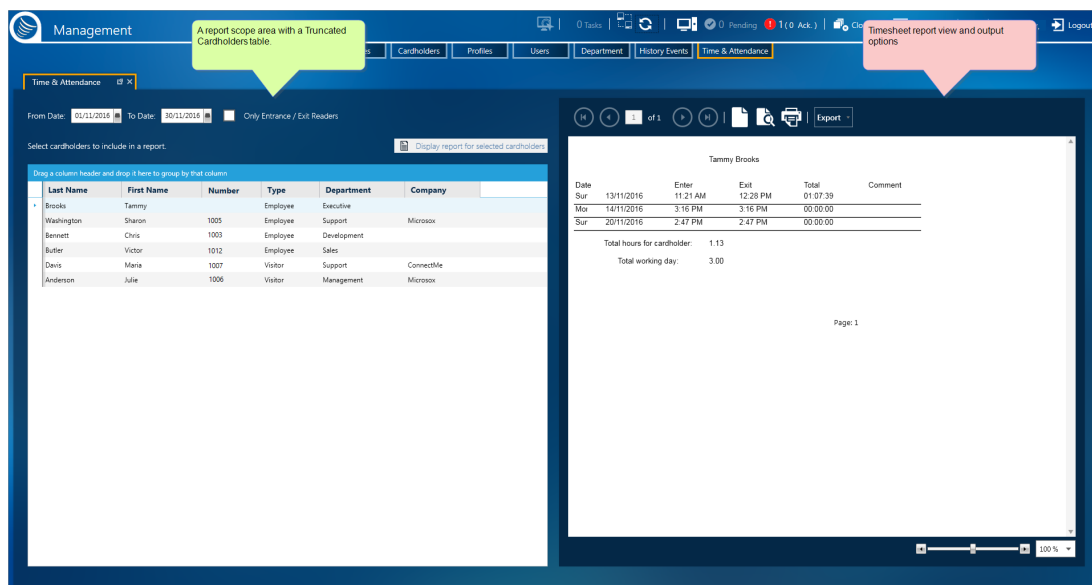
## Report Pagination Controls

The area below the Event History Report table allows you to page through event history data quickly. The pagination controls are only visible when the event history data require it. If all of the data fits in the table on one page, the pagination controls are hidden.

Table A-55 Report Pagination Options

Paging Option	Description
	Go to the first page of the report.
	Go to the previous page of the report.
	Go to the next page of the report.
	Go to the last page of the report.
	Enter a page number in the field, and then press the <b>Enter</b> key. The specified page is displayed.

# Time & Attendance Screen



A cardholder's daily arrival and departure times are taken from the system database and used to automatically generate a timesheet report for one or more selected cardholders with a single click.

An operator, via the date fields found above the truncated cardholders table, sets the scope of a report.

The truncated cardholders table is dynamic and allows operators to filter sort and group cardholders according to the requirements of the timesheet report. After a timesheet report is generated, the report may be exported to multiple formats. In addition, the report may also be printed on a networked printer.

The Time & Attendance screen includes two distinct areas:

- » A report scope area
- » Timesheet report view and output options

## A report scope area

The area is where cardholders are selected to be included in a report and a date range is specified.

**Table A-56** Report Scope Area

Column Option	Description
From Date	The period from which the system database will provide data for the report.
To Date	The end of the period from which the system database will provide data for the report.

Column Option	Description
Only Entrance/Exit Reader	<p>When selected, only the timestamp from a designated reader will be used in a Time &amp; Attendance Timesheet report.</p> <p>This means the first entrance event of the day from a reader with a <b>T&amp;A Reader</b> field set to <b>Entrance</b> and the last exit event of the day from a reader set to <b>Exit</b>.</p> <p>For more information about designating a reader for entrance or exit, see <a href="#">"T&amp;A Reader" on page 459</a>.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> If the Options screen's <b>Allow Dual Readers (Entrance and Exit)</b> is set to Yes, the same reader may be set for both entrance and exit.</p> </div>
Truncated Cardholders Table	A dynamic table that allows an operator to easily find and select cardholders to include in the report. The table includes any cardholder that fits a selected criteria, even cardholders that have been archived or deleted -as long as they have an access event within the criteria.
Display Report for Selected Cardholders button	When clicked, a report is generated and displayed to the right of the truncated cardholders table.

Table A-57 Truncated Cardholders Table Details

Parameter	Description
Group By bar	<p>Restructures the table based on the criteria (column heading) dragged into the <b>Grouped By</b> bar above the table column headings.</p> <p>To change the report table's structure:</p> <ul style="list-style-type: none"> <li>» Select a column heading from the table and drag it to the <b>Grouped By</b> bar, the heading becomes a criteria, and the report table reflects the new criteria structure.</li> <li>» Re-order criteria already in the <b>Grouped By</b> bar (drag and drop one criteria in front of another) changes the structure applied to the report table.</li> <li>» <b>Mouseover</b><sup>1</sup> a criteria already in the <b>Grouped By</b> bar and click the delete <b>x</b> on the right side of a criteria frame; the criteria is removed.</li> </ul>
Last Name	The cardholder's last name.
First Name	The cardholder's first name.
Number	The cardholder's assigned number.

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).



Parameter	Description
Type	The cardholder's general employment status in the organization.
Department	The name of the department within the company where the cardholder is assigned.
Company	The name of a company where the cardholder has an association (i.e. employment).


Each column in the table includes a filter accessed from a column's heading, for information about table filters, see **"Table Filters" on page 695**.

## Timesheet report view and output options

This area displays the generated timesheet report and includes a toolbar for easy report navigation, printing, and an export option to multiple file formats.

**Table A-58** Report View and Output Options

Export Option	Description
	<p>Navigation buttons that display Previous, Next, First, or Last report pages. Alternatively, enter a page number in the text field to display that particular page.</p>
	<p>This set of buttons shows:</p> <ul style="list-style-type: none"> <li>» Print setup options</li> <li>» Print Preview</li> <li>» Printer selection options</li> </ul>

Export Option	Description
	<p>Opens an export drop-down list where you select the file format that you would like to export the currently displayed timesheet report.</p> <p>The formats available are:</p> <ul style="list-style-type: none"> <li>» PDF</li> <li>» CSV (comma separated values)</li> <li>» Excel</li> <li>» RTF (Rich Text Format)</li> <li>» TIF</li> <li>» MHTML (Web Archive - saves as web page content and incorporates external resources)</li> </ul>
Magnification slider	Below the report view area is a slider where you may adjust the magnification level of the pages displayed on the screen.



**Warning:** Keep in mind, when you circulate an exported timesheet report, confidential cardholder data may be inadvertently revealed to unauthorized sources.

# Visitor Control Web Application

Figure A-76

**Visit & Meeting Log table displays visit and meeting event information stored on the database.**

**View details about a particular visit or meeting by clicking the row with the relevant event information.**

**Day Calendar page where meeting and visit details can be accessed and updated. All page entries appear alongside their start times.**

**Toolbar that allows you to create new visits or meetings. In addition, you can enter criteria text in the Search field to display only the Log rows that includes the specified criteria.**

**The icon at the beginning of each Meeting row contains three avatars grouped together.**

**A visit will display the photo of the visitor-cardholder (if it's in the details). Otherwise, only the visitor-cardholders name will be displayed.**

**Visit details page where information about a visit is entered/viewed/edited.**

**In addition, the progression of a visit is recorded in the details page. This includes Enrolled, Checked in, Started, etc.**

USER/MEETING	START DATE	END DATE	COMPANY	STATUS	HOST	SECRET
Salvo meeting	18/12/2017 09:05	18/12/2017 12:15	ConnectMe	Enrolled	Nancy Lopez	
Julie Anderson	13/12/2017 13:10	13/12/2017 15:11	Microsox	Enrollment	Terry Miller	Subscription Block
Julie Anderson	13/12/2017 14:41	13/12/2017 19:00	Microsox	Checked In	Nancy Lopez	
Project Kickoff meeting	13/12/2017 14:05	13/12/2017 15:15	Microsox	Started	Terry Miller	Accompany all
Pamela Ward	13/12/2017 06:00	13/12/2017 15:09	Adopt Communication	Enrolled	Terry Miller	

Figure A-77

**Meeting details page where information about a meeting is recorded and edited.**

**Name and, if available, a photograph of the meeting's host. Below the host information, optional information about the host's assistant may be recorded as well as any remarks relevant to the meeting.**

**Table of people invited to the meeting. After each participant arrives for the meeting, they are Checked In. After Check In, a participant's status in the meeting can be progressed to 'Started meeting' and then 'Ended meeting'.**

**The status of a meeting itself advances from Enrolled to Checked in, and Started only after one of the participant's status changes accordingly. A meeting's 'End meeting' status is applied only after all of the participants have progressed to an 'Ended meeting' status.**

**Project kickoff meeting**

Start date: 13/12/2017 14:05 | End date: 13/12/2017 15:15

Save | Delete

**Host details**

Terry Miller  
First Name: Terry | Last Name: Miller

Executive Ex 556  
Department: Executive | Office phone: Ex 556 | Private phone / Fax: [blank]

**Comments**

Sample meeting 1:Many

Meeting Location: [blank]

**Participants**

Participants: [checked] Accompany all | Add Participant

FIRST NAME	LAST NAME	COMPANY	PHONE	STATUS
Julie	Anderson	Microsox	345178905678	Enrollment
Pamela	Ward	Adopt Communi...	456800	Checked-in
Maria	Davis	ConnectMe		Started

The Visitor Control is a standalone HTML page that provides meeting and visitor management. This includes individuals not previously entered into the system database. Within the module, meeting participants and visitors can be tracked until the scheduled event (meeting or visit) has ended.

What's the difference between a meeting and a visit?

- » A meeting is an encounter between a cardholder (host) and multiple visitors (participants) on the premises where access and security are monitored and managed through the system database.
- » A visit is a meeting between a cardholder (host) and a single visitor (visitor-cardholder) on the premises where access and security are monitored and managed through the system database.

The Visitor Control module screen is divided into the following parts:

- » **Meeting and Visitors Log:** Lists all scheduled meetings and visits and provides access to meeting and visit details.
- » **Day calendar:** Displays scheduled meetings and visits on the day calendar page where the meeting or visit is scheduled to start. Navigate day calendar pages with the arrows at the top of the calendar page, just below the date. A displayed day calendar page shows meetings and visits in the page's timeline. The color in which a meeting or visit appears on a day calendar page depends on the stage of the meeting or visit's lifecycle. Actions can be triggered to indicate advancements in the lifecycle of a meeting or visit from the calendar items details.
- » **Meeting details** or **Visit details:** Provides tools for scheduling and editing meetings and visits. Meeting and visit details display over the day calendar.

## Meeting and Visitor log

Figure A-78

VISIT/MEETING	START DATE	END DATE	COMPANY	STATUS	HOST	ESCORT
Sales meeting	18/12/2017 09:05	18/12/2017 12:15	ConnectMe	Enrollment	Nancy Lopez	
Julie Anderson	13/12/2017 15:10	13/12/2017 15:11	Microsox	Enrollment	Terry Miller	Supervisor Escort
Julie Anderson	13/12/2017 14:41	13/12/2017 19:00	Microsox	Checked-In	Nancy Lopez	
Project kickoff meeting	13/12/2017 14:05	13/12/2017 15:15	Microsox	Started	Terry Miller	
Pamela Ward	13/12/2017 06:00	13/12/2017 15:09	Adopt Communication	Ended	Tony Lowman	

The Meeting and Visitor log is found on the left side of the screen and includes the following:

## Log columns

Meeting and Visitor Log Columns

Column	Description
Visit/Meeting	The name of the visitor invited. OR, The title of a meeting where one or more visitors are enrolled participants.
Start Date	The date and time a visit or meeting is scheduled to begin.



Column	Description
End Date	The date and time a visit or meeting is scheduled to end.
Company	<p>The organization where the host of a meeting or a visitor is affiliated.</p> <p>If there is a meeting where the participants come from multiple companies, this column will display the number of companies that have participants in the meeting.</p>
Status	<p>The current state (milestone) in a meeting or visit's lifecycle. There are four statuses:</p> <ul style="list-style-type: none"> <li>» <b>Enrolled:</b> In a visit event, the visit has been created and saved, but the visitor has not been checked in.  In a meeting event, the meeting has been created and saved, but the meeting may not have any participants added to the event; and, if there are participants, none of them have been checked in.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> If a meeting participant or visitor is enrolled and the event (meeting or visit) has been saved, the individual will be added to the system database and appear in the Cardholders screen.  These cardholders will not be archivable or deletable until the event that triggered their database entry has a status of <b>Ended</b>.</p> </div> <ul style="list-style-type: none"> <li>» <b>Checked in:</b> In a visit event, the visitor has been checked in and received access rights and, if required, a badge.  In a meeting event, at least one participant has been checked in, received access rights and, if required, a badge.</li> <li>» <b>Visit Started:</b> In a visit event, the visitor is with the visit host or escorted to the visit location.  In a meeting event, at least one of the participants is with the meeting host or has been escorted to the meeting location.</li> <li>» <b>Visit Ended:</b> In a visit event, the visitor has been returned their ID (if it was exchanged in the Check In process) and has left the premises.  In a meeting event, all participants have been returned their IDs (if it was exchanged in the Check In process) and have left the premises.  After a meeting or visit has ended, the participants or visitor's access rights are no longer valid. They are archived in the Cardholders screen and if they were assigned a badge code, the code status has been changed to <b>Free</b> in the Badges screen.</li> </ul>
Host	The name of the meeting or visit's sponsor (the cardholder who requested the meeting or visit). The host must have a Type value of Employee in the Cardholders screen.

Column	Description
Escort	<p>Indicates whether a visitor or at least one meeting participant requires an escort or someone else to accompany them while they are on the premises.</p> <p>The difference between Escort and Accompany is:</p> <ul style="list-style-type: none"> <li>» <b>Escort:</b> When selected, the visitor or participant must comply with the GuardPoint10 escort rules.</li> </ul> <p>For information about escort rules, see "<a href="#">Escort Rules for Access Events</a>" on page 697.</p> <ul style="list-style-type: none"> <li>» <b>Accompany:</b> When selected, the heading of the details page change to red and the visitor or participant only needs a cardholder of any type to physically shadow them while on the premises. No GuardPoint10 escort rules are applied.</li> </ul>

## Log Options

### Meeting and Visitors Log Options

Column	Description
Search	<p>Filters the log based on the search criteria entered in the Search field. The mechanism searches all of the log columns for the criteria. The criteria must be at least two characters.</p> <p>Meeting that include participants from multiple companies will be included in the search, even though the names of the companies will not appear in the <b>Company</b> column.</p>
Sort	<p>Sorts the log table based on the sort arrow clicked and the direction the arrow is pointing. Each column heading includes a sort arrow. Click a sort arrow to sort the log by the content of the column where the arrow was clicked. Whether a sort is ascending or descending, depends on the direction the arrow is pointing.</p>
Column Filter	<p>Filters the log view based on the filter criteria entered in a column's filter drop-down box. If a filter is in use the Filter icon will have a gray background.</p> <p>To remove a filter click <b>Clear</b> in the filter drop-down box.</p>

## Day calendar

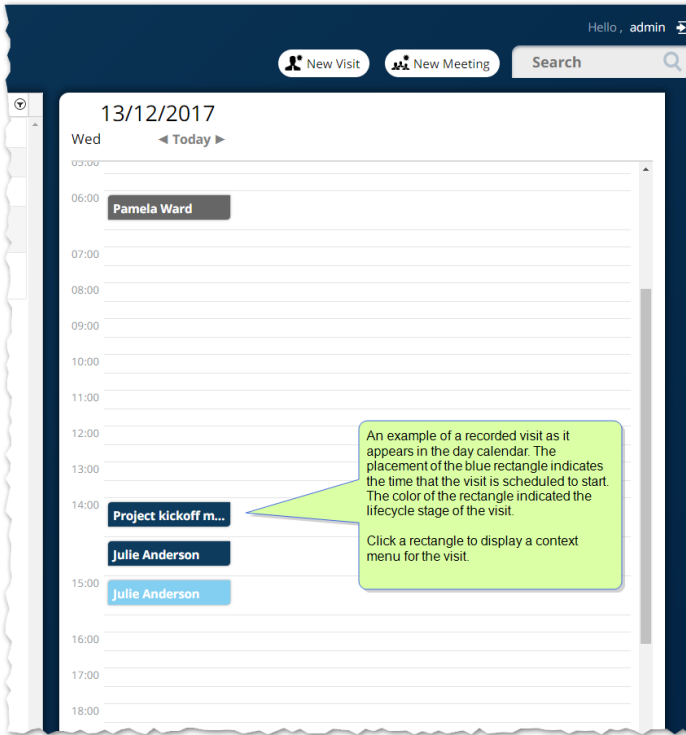
The day calendar is displayed on the right side of the Visitor Control screen, opposite the log. The day calendar shows meetings and visits scheduled to take place on the opened page of the calendar. Each meeting and visit event appears on the page next to the time when the meeting or visit is scheduled to start.

Meeting and visit events are color-coded to reflect their lifecycle status as follows:

- » **Light blue:** A meeting or visit has been recorded, but not started (Enrolled).
- » **Dark blue:** A visit has been checked in or started. In the case of a meeting, at least, one participant is checked in.
- » **Brown:** A visit has ended. In the case of a meeting, all of the participants are recorded as ending their visit.

If a meeting or visit takes place over multiple days, the event will appear on each day of the event in the day calendar.

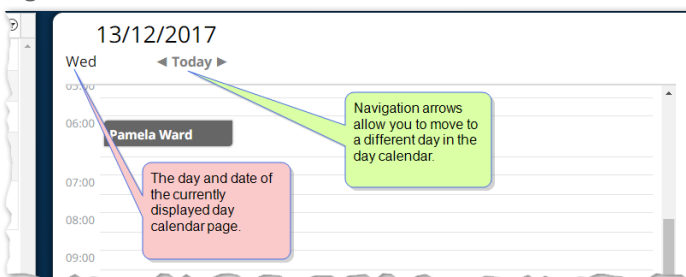
Figure A-79



Displayed meeting or visit details appear over the day calendar hiding the day calendar until the details are no longer displayed.

Navigate to a particular page in the day calendar with the arrows in the heading.

Figure A-80



On a day calendar page, click on a meeting or visit to open a drop-down list of actions for the selected event. The list includes the following:

- » **View details:** Opens a details page of the meeting or visit. The details displayed over the day calendar. From the details, you can click **Edit** or **Delete** in the details' header. The meeting or visit may also be advanced in its lifecycle (i.e. Start, Check in or End).

Alternatively, Double-clicking on an event in the calendar will automatically open the details in **Edit** mode.

- » **Edit:** Opens an editable version of a meeting or visit's details. The details displayed in Edit mode over the day calendar. From the editable view, you can add and update information as well as advance the lifecycle (i.e. Start, Check in, or End).
- » (Only for visits) **Start, Check In or End:** The visit's lifecycle is advanced and open. The lifecycle option that appears in the list depends on the visit's current lifecycle status.
- » **Duplicate:** Opens new meeting or visit details identical to the meeting or visit event where **Duplicate** was selected. The duplicate is not saved until the **Save** button is clicked. The duplicate will be un-started and without a recorded check in, regardless of the lifecycle stage of the meeting or visit from which it was copied.



**Note:** A duplicate should be considered a starting point for a new meeting or visit. Since meeting participants and visitors cannot be in two places at the same time, appropriate changes should be made to the duplicate.

- » **Delete:** Removes the meeting or visit from the day calendar page and the system. A visitor-card-holder created via the meeting or visit is archived in the Cardholders screen and any badge code assigned via the meeting or visit event, has changed its status to **Free** in the Badges screen.

## Meeting Details

Meeting Details Page

Parameter	Description
Meeting Title	A free text field that identifies the subject of a meeting.
Start Date	The date and time a meeting is scheduled to begin. This value can be set to a past, present, or future time.
End Date	The date and time a meeting is scheduled to end. The <b>End Date</b> must be later than the <b>Start Date</b> .
Host Details	<p>Displays the following information:</p> <ul style="list-style-type: none"> <li>» Name of the sponsor of the meeting.</li> <li>» A picture of the host. If a picture is not available, an avatar will appear.</li> <li>» The name of the company and department where the host is affiliated.</li> <li>» The Office phone and Private phone/Fax number of the host.</li> </ul> <p><b>Note:</b> The default Host name is the name of the logged-in operator. The name can be changed to any other cardholder who is an Employee <b>Type</b>. For more information about cardholder <b>Type</b>, see "<a href="#">Type</a>" on page 608.</p>

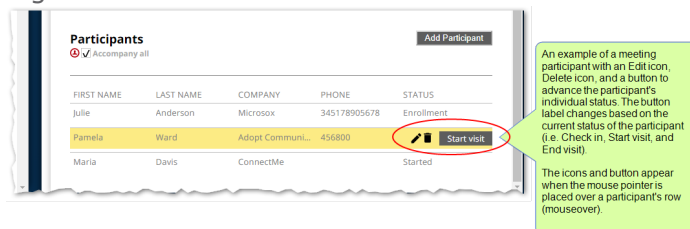
Parameter	Description
Comments	A free text field containing notes about a meeting (i.e. an agenda, preparation instructions, material to be distributed at the meeting, etc.).
Meeting Location	Where the meeting will take place (i.e. address, floor, and room number).
Participants	Lists information about the participants invited to a meeting.
Accompany All (checkbox)	When selected, the heading of the details page change to red, and all participants will be required to have someone accompany them while they are on the premises.
Add Participant (button)	Appends a new participant to a list of meeting participants. Each participant entry includes fields for details, and buttons to advance a participant's status in the meeting.
Save (button in the heading) (may not be visible)	Saves the meeting information. The saved meeting appears in the log on the left side of the screen and in the day calendar.
Save&New (button in the heading) (may not be visible)	Saves the meeting information. The saved meeting appears in the log on the left side of the screen and in the day calendar. In addition, a new meeting details page is displayed.
Delete (button in the heading)	Removes the meeting from the system, and archives the participants in the GuardPoint10 Cardholders screen. If a participant had been issued a badge code, the code status is changed to <b>Free</b> in the Badges screen.
Edit button in the heading (may not be visible)	Meeting details become editable. Click <b>Save</b> after performing your edits or the new information will be lost.

## Meeting participant details

A meeting participant's basic details are displayed in the Participants table at all times, this includes a participant's first and last name, company affiliation, phone number, and the participant's status (enrolled, checked in, started, or ended).



When you mouseover a participant's row, Edit and Delete icons appear along with a button to advance the participant's status.

Figure A-81



Click the Edit icon  to display the following additional participant details.

## Meeting Participant Details

Parameter	Description
First Name	The first name of a visitor invited to participate in the meeting.
Last Name	The last name of a visitor invited to participate in the meeting. This field is required.
Company	The organization where the participant is affiliated.
Phone	The phone number where the participant may be contacted.
Status (may not be visible)	<p>The participant's current status in relation to the meeting (i.e. Enrolled, Checked in, Started, Ended).</p> <p>When the Edit icon  is clicked and the participant's information is expanded and the status does not appear. However, the status may be determined based on the label in the advance status button. For example, if the button label reads <b>End visit</b> that means the participant's status has already been advanced to <b>Started visit</b>.</p>
Access Authorization	<p>A drop-down list of Multiple Access Groups. A Multiple Access Group contains authorizations for designated spaces where participants, assigned the Multiple Access Group will have access.</p> <p>The selected Multiple Access Group should include access to the meeting location. For more information, see <a href="#">"Multiple Access Groups" on page 156</a>.</p> <p>This field is required.</p>
Car License Plate	The license plate number of the participant's vehicle. The plate number works with GuardPoint10's LPR feature to create an alternate cardholder identification platform.
GuardPoint10 Escort	<p>When selected the participant must be accompanied by a designated escort (set in a cardholder's details) at relevant readers.</p> <p>For information about escort rules, see <a href="#">"Escort Rules for Access Events" on page 697</a>.</p>
Save&Close (button)	Saves a participant's information and hides all but the most basic participant information (the first row). The first row of a participant's information can be expanded via the Edit icon  displayed when an operator mouseovers a participant's row.
Cancel (button)	Reverts to the previously saved participant details and closes the participant's details.
Advance status (button)	<ul style="list-style-type: none"> <li>» Advances an <b>Enrolled</b> participant to <b>Check in</b>.</li> <li>» Advances a <b>Checked in</b> participant to <b>Start visit</b>.</li> <li>» Advances a <b>Started visit</b> participant to <b>End visit</b>.</li> </ul> <p>If a participant has been checked in, additional detail fields will appear. These fields pertain to the participant's badge assignment.</p>

## Participant check in details

When a participant initially presents themselves to an operator, a Check In operation may be performed. This operation may include an exchange where the participant would hand over some form of ID and in return, the participant would receive a badge to access the premises. When the participant's status is changed to **End visit**, the ID is returned.

Participant Check In Details

Parameter	Description
Badge	The badge number assigned to the participant. If a badge code has not been assigned, via the Cardholders screen, a list of <b>Free</b> badge codes is available via the Badge field. You may have to enter a character found in a known Free code to see a list of codes that include that character.
ID Type	The type of ID presented by a participant in exchange for a badge (i.e. Passport, Driver license, Identity card, etc.).
ID Number	The unique number on the ID presented by the participant.
Rack Number	The slot number where the ID will be kept until it's returned to the participant.
Security Clearance (checkbox)	When selected, the participant has received clearance to enter the premises.

## Visit Details

Visit Details

Parameter	Description
First name Last name	Free text fields that identify a visitor. The visitor's name is also used as the title of the visit. The last name field is required.
Start Date	The date and time a visit is scheduled to begin. This value can be set to a past, present, or future time.
End Date	The date and time a visit is scheduled to end.
Company	The organization where the visitor is affiliated.
Phone	The phone number where the visitor may be contacted.
Access Authorization	A drop-down list of Multiple Access Groups. A Multiple Access Group contains designated spaces where a visitor, assigned the Multiple Access Group, will have the authorization to enter. Select a Multiple Access Group that includes access to the visit <b>Location</b> . For more information about Multiple Access Groups, see " <a href="#">Multiple Access Groups</a> " on page 156.

Parameter	Description
Visit Location	Where a visit will take place (i.e. address, floor, and or room number).
Car License Plate	The license plate number of the visitor's vehicle. The plate number works with GuardPoint10's LPR feature to create an alternate cardholder identification platform.
Accompany (checkbox)	When selected, the heading of the details page change to red, and the visitor will be required to have someone accompany them while they are on the premises.
GuardPoint10 Escort (checkbox)	<p>When selected, the heading of the details page changes to red.</p> <p>The visitor must be accompanied by a designated escort (set in a cardholder's details) at relevant readers. A relevant reader is a reader that has its <b>Escort</b> parameter set to <b>Yes</b>.</p> <p>For information about escort rules, see <a href="#">"Escort Rules for Access Events" on page 697</a>.</p>
Security Clearance (checkbox)	When selected, the visitor has received clearance to enter the premises.
Picture placement	An area where a picture of the visitor may be displayed. Mouseover the picture area to open a File Selection dialog where an image file may be selected. If a picture is not available, an avatar will appear.
Host Details	<p>Displays the following information:</p> <ul style="list-style-type: none"> <li>» Name of the visit sponsor (the person who the visitor is meeting).</li> <li>» A picture of the host. If a picture is not available, an avatar will appear.</li> <li>» The name of the company and department where the host is affiliated.</li> <li>» The Office phone and Private phone/Fax numbers of the host.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> The default Host name is the name of the logged-in operator. The name can be changed to any other cardholder who is an Employee <b>Type</b>. For more information about cardholder <b>Type</b>, see <a href="#">"Type" on page 608</a>.</p> </div>
Comments	A free text field containing notes about the visit (i.e. an agenda or preparation instructions).
Save (button) (may not be visible)	<p>Saves the visit information. The saved visit appears in the log on the left side of the screen and in the day calendar.</p> <p>After a visit is enrolled (before check in) the visitor's status cannot be changed via the Cardholders screen.</p>
Save&New (button in the heading) (may not be visible)	Saves the visit information. The saved visit appears in the log on the left side of the screen and in the day calendar. In addition, a new set of visit details is displayed.



Parameter	Description
Delete (button)	Removes the visit from the system and archives the visitor-cardholder in the GuardPoint10 Cardholders screen. If the visitor-cardholder was assigned a badge code, the code's status is changed to <b>Free</b> in the Badges screen.
Edit (button) (may not be visible)	Visit details become editable. Click <b>Save</b> after performing your edits or risk losing your changes.
Check In (button)	<p>Changes the status of the visit in the log to "Checked In", opens Check In details and changes the <b>Check In</b> button to a <b>Start visit</b> button.</p> <p>Check in means that the visitor has physically presented themselves to an operator, who will enter visit information.</p> <p>The Check In process may include an exchange of a visitor's ID for a badge. The details about the exchange includes:</p> <ul style="list-style-type: none"> <li>» <b>Badge</b>: The badge number.</li> <li>» <b>ID Type</b>: The ID presented by the visitor in exchange for a badge.</li> <li>» <b>Rack Number</b>: The rack where the ID will be kept until it is returned to the visitor.</li> </ul>
Start Visit (button)	<p>Changes the status of the visit in the log from <b>Enrolled</b> to <b>Started visit</b>. After the <b>Start Visit</b> button is clicked, it changes to an <b>End Visit</b> button.</p> <p>A visit is started when the visitor is with the visit host or on their way to the visit host.</p>
End Visit (button)	<p>Changes the status of the visit in the log from <b>Started visit</b> to <b>Visit Ended</b>. Even though the visit is ended, the details may still be edited, but the life-cycle of the visit cannot be reversed (i.e. an ended visit cannot be changed to a started visit).</p> <p>After a visit has ended, in the GuardPoint10 Cardholders screen the visitor is archived and, if a badge code was assigned, the code status is changed to <b>Free</b> in the Badges screen.</p>

## Visitor options and Check In details are as follows:

### Visitor Options and Check In Details

Parameter	Description
Badge	The badge number assigned to the visitor. If a badge has not been assigned, via the Cardholders screen, the Badge area is blank.
ID Type	The type of ID presented by the visitor in exchange for a badge (i.e. Passport, Driver license, Identity card, etc.).
ID Number	The unique number on the ID presented by the visitor.

Parameter	Description
Rack Number	The slot number where the ID card, presented by a visitor, will be stored until it's returned.

## Reports page

Figure A-82

The screenshot shows the Amadeus8 Visitor Control interface. The top navigation bar includes 'Home' and 'Hello, admin'. The main content area features a 'Reports List' sidebar on the left and a central report table. The table has columns for 'visit / meeting name', 'from', 'to', 'host name', and 'visitor name'. A 'Refresh' button is located above the table. Callouts provide the following information:

- Yellow callout:** Click Home to return to the Home page. On the Home page, click Reports to open the Reports page.
- Blue callout:** Each report type has its own set of filters above the Report table. Enter or select filter criteria and click Refresh to see the filtered report.
- Purple callout:** The list includes CVS (Excel) and PDF export formats. Click a format and the currently displayed report is saved in your default download folder.
- Green callout:** A list of available report types. When a report is selected, the unfiltered results appear to the right of the list.
- Pink callout:** A report table unique to each report type displays in an easy to read layout.

visit / meeting name	from	to	host name	visitor name	Export
Project kickoff meeting	2017-12-13 12:05:00	2017-12-13 13:15:00	Terry Miller	Maria Davis, Pamela Ward, Julie Anderson	
Julie Anderson	2017-12-13 13:10:04	2017-12-13 13:11:00	Terry Miller	Julie Anderson	
Julie Anderson	2017-12-13 12:41:08	2017-12-13 17:00:00	Nancy Lopez	Julie Anderson	
Sales meeting	2017-12-18 07:05:00	2017-12-18 10:15:00	Nancy Lopez	Maria Davis, Julie Anderson	
Pamela Ward	2017-12-13 04:00:00	2017-12-13 13:09:43	Tony Lowman	Pamela Ward	

The Reports page includes multiple report options that may be filtered to fit your needs. The available reports are as follows:

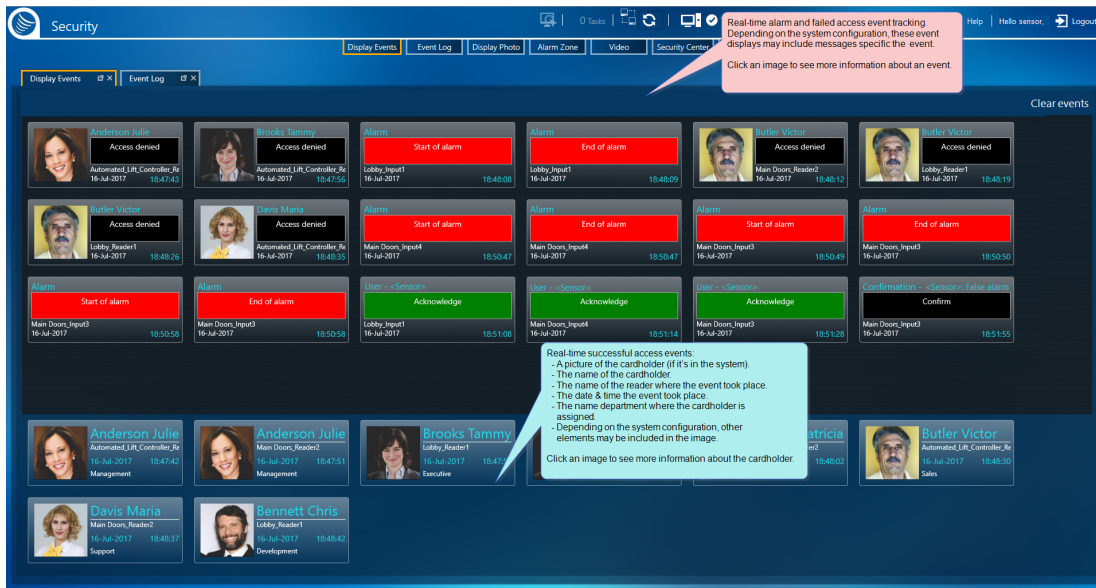
- » **General Visit / Meeting:** Basic information about visit or meeting events that have not been deleted or ended.
- » **General Visitor:** Basic information about visitors who are in the system database and have not been archived.
- » **Badge History:** Information about where and who has used or been assigned a badge.
- » **Visitor on Site:** A list of visitors who are currently on the premises.
- » **General Host:** Basic information about employees who are or will host existing visits or meetings.

Use the filter fields and Refresh button, found just above the Report table, to narrow the data displayed in the current report.

After you are happy with the displayed report, click one of the export options to save the report in your default download folder.

# Display Events Screen

Figure A-83



Displays real-time information about cardholder activities and alarms.

The Events screen includes two areas:

## Alarm and failed event tracking

Displays real-time information about the events as they occur. General information about an event appears in a card-like graphic. Click a card to flip it and see more information about a specific event.

The screen initially opens with the previous five alarms or failed events displayed.

Alarm cards contain text describing the cause of the alarm and a timestamp indicating when the alarm occurred.

Each alarm card has the following context menu options:

- » **Acknowledge:** The alarm is recognized by the operator. An acknowledgment is reflected in the alarm card and on the dashboard. An alarm must be acknowledged before it can be confirmed.
- » **Confirm:** Opens a Confirmation dialog where you may enter a description of the alarm and details that confirm your observation of the alarm. Click **Confirm** to complete the confirmation process. After an alarm is confirmed, its card is removed from the Events screen. The confirmation event can be seen in the Event log (see "Event Log Screen" on page 357).
- » **Navigate to Map:** If an alarm's input is linked to an icon that appears on a map in the Security Center, the map will be automatically displayed.

## Cardholder access event tracking

Displays real-time information about the successful comings & goings of cardholders. General information about a cardholder event appears in a card-like graphic. Click a card to flip it and see more

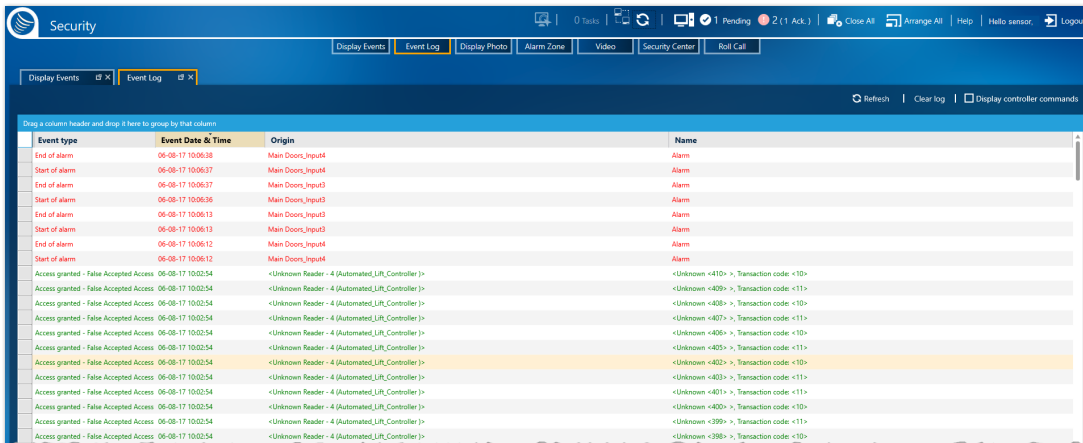
information about the cardholder. Double-click a card to open the cardholder's details.

For information about a cardholder's details, see "[Operator \(User\): MultiSite Impact Cardholder Details](#)" on page 607.

A **Clear Events** button, at the top right of the screen, empties both areas. This is a tool to clear the display only, the events are still in the log and may be active.

# Events Log Screen

Figure A-84



Displays a record of all events that take place in the system; this includes cardholder events, alarm events, and internal system events.

The events are displayed in a tabular format. The event data is color-coded according to the event type. For information about customizing the color-coding, see ["Changing Option settings" on page 237](#).

A **Clear Log** button, above the table and to the right of the screen, empties the Event Log table. This is a tool to clear the table, the events are still in the database and may be active.

A **Refresh** button, alongside the **Clear Log** button, updates the Event Log table.

The **Display Controller Commands** checkbox allows you to display internal transactions and commands from controllers. This option is only displayed when set in the Options screen.

The Event Log table may be filtered by each column for easy data management.

For information about table filters, see ["Table Filters" on page 695](#).

The options and columns in the Event Log table are as follows.

Event Log Table Options and Columns

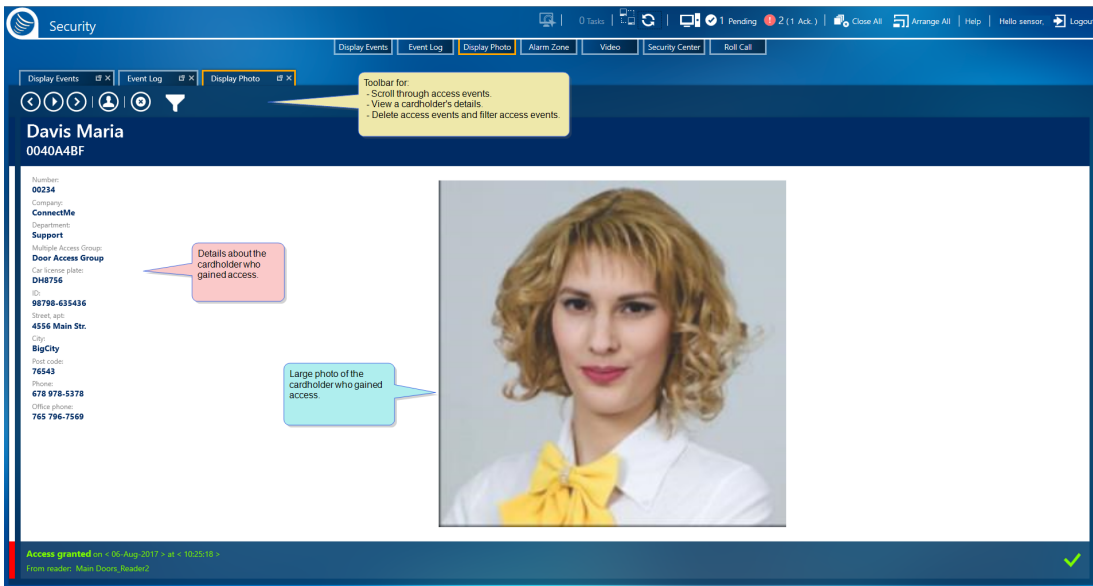
Column/Option	Description
Group By bar (Display option)	<p>Restructures the Event Log table based on the criteria (column heading) dragged into the <b>Group By bar</b>.</p> <p>To change the table's structure:</p> <ul style="list-style-type: none"> <li>» Select a column heading from the table and drag it to the <b>Group By bar</b>, the heading becomes a criteria, and the table reflects the new criteria structure.</li> <li>» Re-order criteria already in the <b>Group By bar</b> (drag and drop one criteria in front of another) changes the structure applied to the table.</li> <li>» <b>Mouseover</b><sup>1</sup> a criteria already in the <b>Group By bar</b> and click the delete <b>x</b> on the right side of a criteria frame; the criteria is removed.</li> </ul>

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

Column/Option	Description
Event Type	A label that categorizes an event. Each event is color-coded according to its category.
Event Date & Time	A timestamp that identifies when an event occurred.
Origin	The physical location where an event was triggered, or the event that triggered a subsequent event.
Cardholder Name	The name of the cardholder who triggered an event. If a cardholder did not trigger the event, the field is empty.

# Display Photo Screen

Figure A-85



The Display Photo screen initially shows a large photo of the cardholder who most recently attempted to access a space via a reader. The photo is accompanied by general information about the displayed cardholder and the access event.

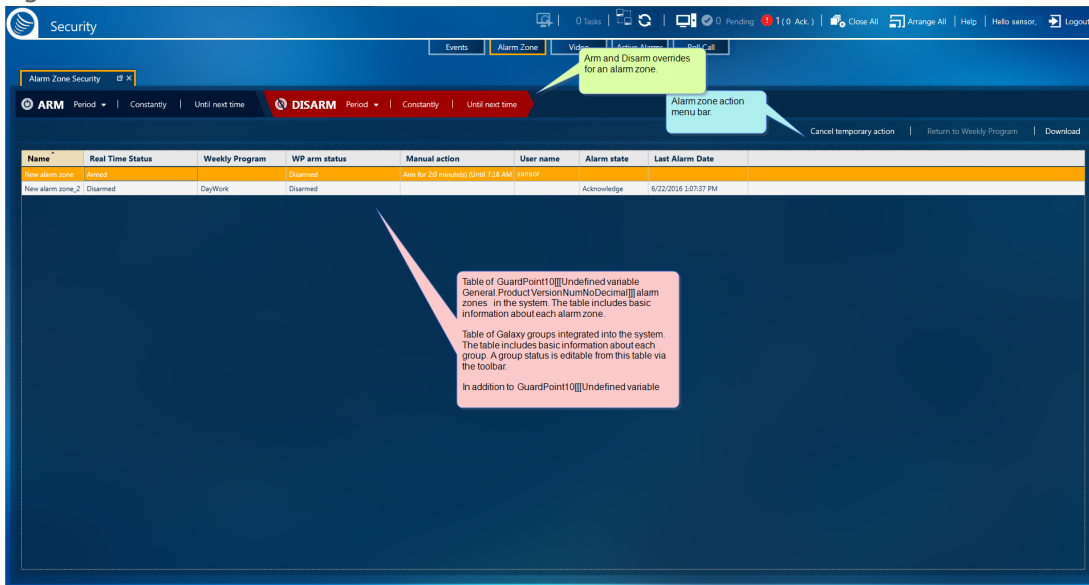
Figure A-86

The Photo Display window also included a toolbar that allows the operator to:

- » Scroll through cardholder displays in the order in which access events took place.
- » Delete a displayed cardholder event or, filter the cardholders displayed by either Multiple Access Group or reader where the event took place.
- » Display more details about the currently displayed cardholder.

# Alarm Zone Security Screen for GuardPoint10 Alarm Zones

Figure A-87



The Alarm Zone Security screen lists GuardPoint10 alarm zones and Galaxy groups in its table. The toolbar and table columns change depending on which row (alarm zone or group) is selected. This topic covers the screen information displayed when an alarm zone is selected. For information about the Alarm Zone Security screen when a Galaxy group row is selected, see ["Alarm Zone Security Screen for Galaxy Groups"](#) on page 664.

The Alarm Zone Security screen displays alarm zone information for each designated alarm zone space and includes tools to override the current state of an alarm zone's input(s).

The Alarm Zone Security screen includes three areas.

## Override menu

The override menu has two parts: ARM and DISARM. The commands allow you to manually override the current state of the alarm zone in focus, regardless of the Weekly Program assigned to the zone.

## Action menu

Removes an override command that has been applied to the alarm zone in focus. In addition, the action menu transmits any alarm zone changes made in the Alarm Zone Security screen to the relevant controllers. A relevant controller would be a controller connected to one or more of the input devices included in the alarm zone.



# Alarm Zone table

The Alarm Zone table consists of a row for each alarm zone in the system and a series of columns that contain parameter information about each zone.

For information about table filters, see **"Table Filters" on page 695**.

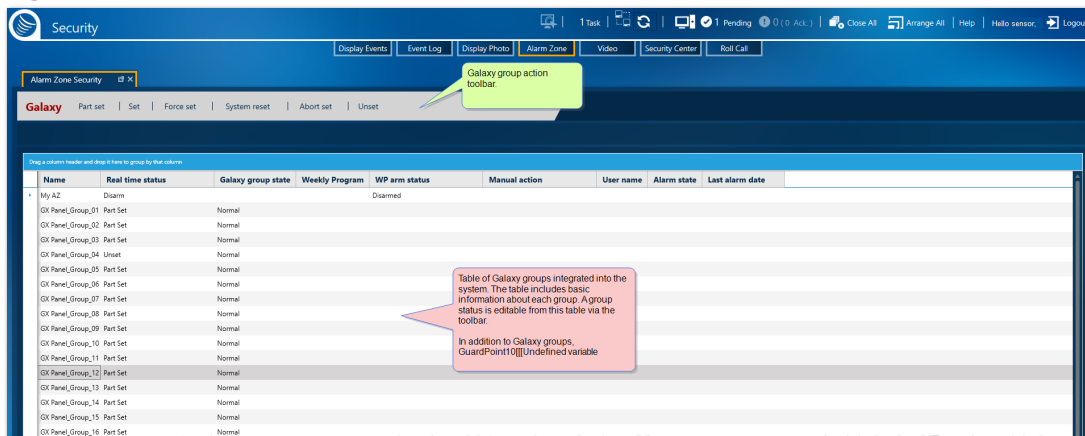
The GuardPoint10 relevant columns in the Alarm Zone/Galaxy group table are as follows.

GuardPoint10 Relevant Table Parameters

Parameter	Description
Name	The name of the alarm zone described in the table row.
Real Time Status	The current state of the alarm zone (armed or disarmed).
Weekly Program (WP)	The Weekly Program (WP) assigned to the alarm zone. A WP is a timetable made up of 8 Daily Programs, one for each day of the week and an extra program for Holidays and Special Days. WPs set periods as behavior for the input device included in the alarm zone (green or white). For more information about WPs, see <b>"Weekly Program Time Zones" on page 120</b> .
WP Arm Status	Correlates the Weekly Program (WP) assigned to the alarm zone with the current time of day to determine the WP's status (i.e. is the WP in its green period or white period).
Manual Action	Determines if the alarm zone is governed by an override command, and if so, which command.
User Name	The name of the operator who initiated the <b>Manual Action</b> . If there was no <b>Manual Action</b> , the field is empty.
Alarm States	Has the alarm been triggered and is it still active.
Last Alarm Date	The date and time that the alarm was last triggered.

# Alarm Zone Security Screen for Galaxy Groups

Figure A-88



**Note:** This topic assumes that a Galaxy panel has been integrated into your GuardPoint10 system.

The Alarm Zone Security screen lists GuardPoint10 alarm zones and Galaxy groups in its table. A Galaxy group is a collection of Galaxy zones. A Galaxy zone is equivalent to an GuardPoint10 input. The toolbar and table group columns change depending on which row (alarm zone or group) is selected. This topic covers the screen information and toolbar displayed when a Galaxy group is selected. For information about the Alarm Zone Security screen when an GuardPoint10 alarm zone row is selected, see "[Alarm Zone Security Screen for GuardPoint10 Alarm Zones](#)" on page 662.

The Alarm Zone Security screen displays Galaxy group information for each group in a Galaxy system that has been integrated into GuardPoint10 and includes actions in the toolbar to change the current state of a group and its zones.

The Alarm Zone Security screen includes two areas.

## Action toolbar

Applies a selected status update to a Galaxy group row in focus. The statuses available are as follows:

- » **Part set:** One or more zones in the Galaxy group is either armed, disarmed, or omitted.
- » **Set:** All of the zones in the Galaxy group are armed. An armed zone is a zone that broadcasts an alarm when it is triggered.
- » **Force set:** Arms all of the zones in the Galaxy group, except for a triggered armed zone that is omitted. A *triggered armed zone that is omitted* means that an alarm is broadcast from the zone but ignored by the Galaxy system and GuardPoint10.

In the case where an operator unomits all of the triggered armed and omitted zones of a Forced set group, the zones will be armed and the group state will change to Set.

- » **System reset:** Resetting a Galaxy group and will return the group in focus to its normal state.

If there is a tamper zone in the group and the tamper zone alarm is triggered, the group it belongs to cannot be reset until the cause of the tamper alarm is resolved.

- » **Abort set:** Normally opening a zone during an exit routine resets the exit timer. The **Abort set** action stops the reset routine. The exit time determines the time allowed to leave the premises via the exit route before the group is set (armed).
- » **Unset:** All of the zones in the Galaxy group are disarmed. A disarmed zone is a zone that does not broadcast an alarm when the zone is triggered.



**Note:** Initiating a System Reset from the Galaxy panel keypad will return all Galaxy groups, originating from that panel to their normal state.

**Note:** The statuses available in the action menu are also available in a rows context menu.

## Alarm Zone/Galaxy group table

The Alarm Zone/Galaxy group table consists of a row for each alarm zone and Galaxy group in the system and a series of columns that contain parameter information about each zone or group.

For information about table filters, see **"Table Filters" on page 695**.

The Galaxy relevant columns in the Alarm Zone/Galaxy group table are as follows.

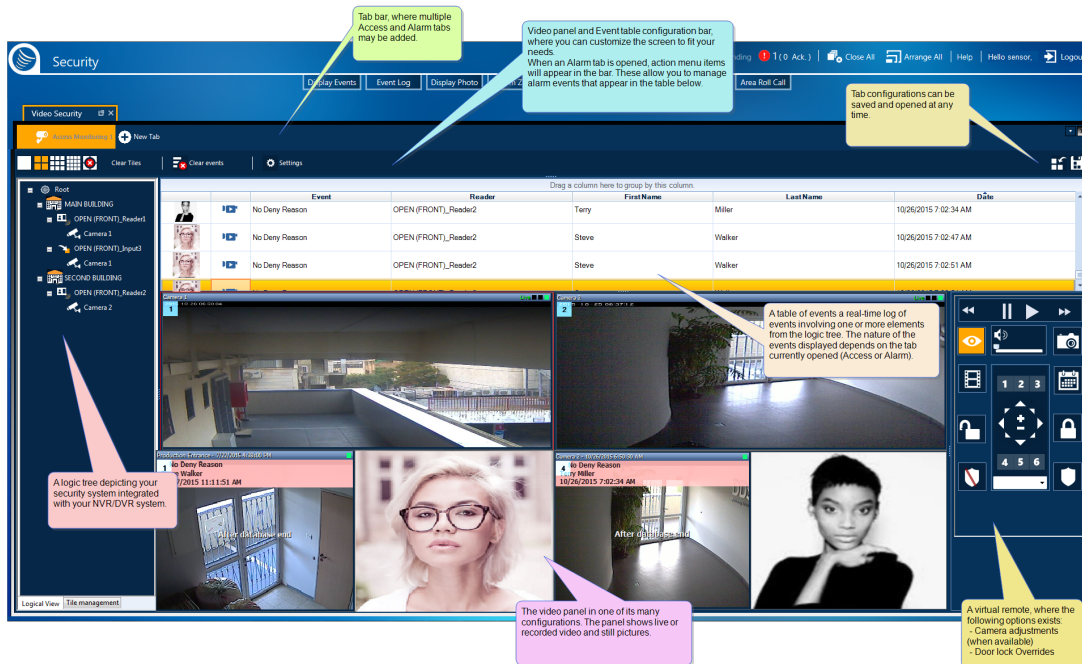
Galaxy Group Relevant Table Parameters

Parameter	Description
Name	The name of the alarm zone or Galaxy group described in the table row.
Real Time Status	The column describes the preparedness of the zone or group. This means: The current status of an alarm zone (armed or disarmed). Or, The current status of a Galaxy group (set, unset, or part set).

Parameter	Description
Galaxy Group State	<p>The current action state of the Galaxy group. The action states are as follows:</p> <ul style="list-style-type: none"> <li>» <b>Normal</b>: No further action required.</li> <li>» <b>Alarm</b>: At least one zone in the group has been triggered and a reset operation action performed not from GuardPoint10 nor from the keypad.</li> <li>» <b>Reset Required</b>: An operator committed an illegal or unsuccessful operation so the group needs a <b>System reset</b> action.</li> </ul> <p>For example, if an operator clicks <b>Part set</b> for a group that has a triggered zone (zone1) in it, and then if another zone (zone2) in the same group is activated, the Galaxy system will raise an alarm for the second zone (zone2), but a <b>System Reset</b> action is required before another zone (zone 3) alarm may be triggered.</p> <ul style="list-style-type: none"> <li>» <b>Ready to set</b>: All zones in the Galaxy group are in their normal state. When determining if a Galaxy group is ready, omitted zones are not taken into account.</li> <li>» <b>Time locked</b>: A Galaxy group is locked out and cannot be unset, unless an alarm has been triggered in the group.</li> </ul> <div style="border: 1px solid black; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Because Galaxy group actions may be performed locally from the Galaxy panel or application as well as GuardPoint10, the <b>Galaxy Group State</b> value may change without any Alarm Zone Security screen operator action.</p> </div>

# Video Security Screen

Figure A-89



Displays real time and recorded images (video and snapshots) that enable an operator to monitor video linked to access control events and alarm events. In addition, the operator may override an input status or alarm zone status based on activity observed via the Video Security screen.

The Video Security screen includes six areas:

## Tab bar

The tab bar allows you to monitor two categories of events, Access Monitoring, and Alarm Monitoring. You may create multiple tabs for each tab type (Access or Alarm). Each tab may have a customized screen display. For example, you can have an Access tab that includes a 16-camera display in the video panel. You can then add an additional Access tab that displays a 4-camera display, one for each entrance, where the cardholder's image will appear on top of the video upon an access event.

If an alarm event occurs, and an operator has not addressed it (Acknowledge or Confirm), the Alarm tab will flash red.

Each tab in the tab bar has a context menu that allows you to manage the Video Security screen.

The items in the context menu include the following:

- » **Close:** Closes the tab where the context menu was opened.
- » **Close all:** Closes all of the tabs in the tab bar.
- » **Close all but this:** Closes all of the tabs in the tab bar except for the tab where the context menu was opened.
- » **New horizontally tab group:** Splits the Video Security screen horizontally. If multiple tab types are visible in the tab bar, the split will be grouped by tab type. If all of the tabs visible in the tab

bar are of the same type, the split will move the tab where the context menu was opened on one side of the split and all other tabs on the other side of the split.

- » **New vertically tab group:** Splits the Video Security screen vertically. If multiple tab types are visible in the tab bar, the split will be grouped by tab type. If all of the tabs visible in the tab bar are of the same type, the split will move the tab where the context menu was opened on one side of the split and all other tabs on the other side of the split.
- » **Move to previous tab group / Move to next tab group:** Moves the tab, where the context menu was opened, to a different pane in a split-screen.

Visible only when multiple tab groups (horizontal or vertical) exist.

- » **Rename tab:** Opens a field where you can rename the tab, where the context menu was opened. A best practice is to rename the tab to something short and descriptive.
- » **Hide Logic tree:** Hides the Logic tree and Tile management pane in the tab where the context menu was opened. The Logic tree and Tile management pane in all other tabs, visible in the tab bar, remains unchanged. For information about the logic tree and Tile management pane, see "[Logic tree & Tile management](#)" on page 671.
- » **Hide event/alarm table:** Depending on the type of tab where the context menu was opened, this item will either hide the Access Event log table or hide the Alarm Event log table. For information about the logs, see "[Real-time Access or Alarm log](#)" on page 670.
- » **Hide virtual remote:** Hides the virtual remote in the tab where the context menu was opened. The virtual remote in all other tabs, visible in the tab bar, remains unchanged. For information about the virtual remote, see "[Virtual remote](#)" on page 672.






## Display settings and action bar

Display settings are generic and appear in Access tabs and Alarm tabs.

The action bar (**Acknowledge**, **Confirm** and **Confirm All**) is specific to Alarms and will only appear in an Alarm tab.

The tables below describe each option available in the action bar.

Generic Display Settings

Setting	Description
	The video panel will display a single tile where a video or still image may be viewed.
	The video panel will display 4 tiles where videos or still images may be viewed.
	The video panel will display 9 tiles where videos or still images may be viewed.
	The video panel will display 16 tiles where videos or still images may be viewed.
	In the video panel, all videos that were placed in tiles are removed. The tiles are cleared.

Setting	Description
Clear Events	The Access table or Alarm table, currently displayed, is cleared. The cleared data is not deleted from the system and can still be viewed in the Event History screen.
Settings	<p>Opens a dialog where two things may be specified:</p> <ul style="list-style-type: none"> <li>» How a cardholder's photo will appear in a tile (only relevant in an Access Monitoring tab): <ul style="list-style-type: none"> <li>» <b>Photo overlay</b>: The cardholder's photo will appear on top of the event image.</li> <li>» <b>Side by side video</b>: The event image will be cropped and the cardholder's photo will appear alongside the event image.</li> <li>» <b>Photo only</b>: The event image will be hidden and only the cardholder's photo will appear in the tile.</li> <li>» <b>Hide photo</b>: The event image will appear in the tile without the cardholder's photo.</li> </ul> </li> <li>» How an event's image will appear in a tile: <ul style="list-style-type: none"> <li>» <b>Display event as snapshot</b>: A still image of an event appears in a designated tile.</li> <li>» <b>Display event as video</b>: A 30 second delay is applied to the event display. When the video does appear in the tile, you can use the player controls in the virtual remote to fast forward 30 seconds and see the event take place.</li> <li>» <b>Display event as live</b>: A live video stream appears in the tile where you can see the event take place in real time.</li> </ul> </li> <li>» Filter records without video: Prevents events from appearing in the table if the reader or input, where the event took place, does not have a camera associated with it.</li> </ul>

#### Alarm Monitoring Tab's Action Bar

Setting	Description
Acknowledge	The alarm in focus is acknowledged. This acknowledgment is also reflected in the pending area of the dashboard.
Confirm	<p>Opens a dialog where you may enter a description of the alarm and details that confirm your observation of the alarm. Click <b>OK</b> to complete the confirmation process.</p> <hr/> <p><b>Note:</b> An alarm event must be acknowledged before it can be confirmed.</p> <hr/>

Setting	Description
Confirm All	Automatically confirms all alarm events listed in the alarms table without the need to acknowledge the alarms first. This operation does not include a description option.

## Real-time Access or Alarm log

The Access table -visible via an opened Access tab- consists of a row for each access event that has taken place since the beginning of the current session or since the **Clear events** button was last clicked.

The Access table contains the following information:

Access Event Table

Column	Description
Group By bar	Restructures the Access Event log table based on the criteria (column heading) dragged into the <b>Group By bar</b> . To change the table's structure: <ul style="list-style-type: none"> <li>» Select a column heading and drag it to the <b>Group By bar</b>, the heading becomes a criteria. and the table reflects the new criteria structure.</li> <li>» Re-order criteria already in the <b>Group By bar</b> (drag and drop one criteria in front of another) changes the structure applied to the table.</li> <li>» <b>Mouseover</b><sup>1</sup> a criteria already in the <b>Group By bar</b> and click the delete <b>x</b> on the right side of a criteria frame; the criteria is removed.</li> </ul>
Cardholder photo	A photo of the cardholder who initiated the access event is displayed. If there is no photo in the system database an avatar is displayed.
Link icon to an associated video or still image	If a video or still image of an event was recorded, an icon will be displayed. Drag the icon to a tile in the video panel to show the recording.
Event	Describes the nature of the access event (i.e. Access granted, invalid cardholder, etc.).
Reader	The name of the reader where the access event took place.
First Name	The first name of the cardholder who initiated the access event.
Last Name	The last name of the cardholder who initiated the access event.
Date	The date and time when the access event took place.

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).



The Alarm table -visible via an opened Alarm tab- consists of a row for each alarm event that has taken place since one of the following:

- » The beginning of the current session
- » The **Clear events** button was last clicked.
- » A Confirm operation was performed.

The Alarm table contains the following information:

Alarm Event Table

Column	Description
Group By bar	<p>Restructures the Alarm Event log table based on the criteria (column heading) dragged into the <b>Group By bar</b>.</p> <p>To change the table's structure:</p> <ul style="list-style-type: none"> <li>» Select a column heading and drag it to the <b>Group By bar</b>, the heading becomes a criteria, and the table reflects the new criteria structure.</li> <li>» Re-order criteria already in the <b>Group By bar</b> (drag and drop one criteria in front of another) changes the structure applied to the table.</li> <li>» Mouseover a criteria already in the <b>Group By bar</b> and click the delete <b>x</b> on the right side of a criteria frame; the criteria is removed.</li> </ul>
Alarm	<p>The internal system event that caused the alarm to appear in the Alarm table.</p> <hr/> <p><b>Note:</b> The table will display an alarm's start event, but not an alarm's end event. End events can be seen on the Event screen.</p>
Alarm Date	Show the date and time when the alarm event took place.
Input	The name of the input where the access event or the alarm event was triggered.
State	Shows whether an alarm event was addressed by an operator, and if so, how (i.e. acknowledged, confirmed). If an operator did not address the alarm event, the alarm's state is 'Active'.

## Logic tree & Tile management

There are two tabs at the bottom of the pane called **Logic view** and **Tile management**.

- » Logic view includes a representation of the relationship between GuardPoint10 elements and your NVR/DVR system elements. The tree may consist of Areas, Readers, Inputs, and Cameras. Cameras may be dragged and dropped into a video panel tile to view live images. The logic tree is configured in the Video Setup screen. For more information, see "[Video \(Setup\) and NVR/DVR](#)" on page 243.
- » Tile management allows an operator to link a camera to a specific tile. Once the link is established, events viewed by the camera will display in the specified tile.


## Video panel

Shows either a live video stream or playback in one or several tiles.

Tiles are numbered from 1 to 16, depending on the number of tiles you chose to display (see "[Generic Display Settings](#)" on page 668).

Access Monitoring tabs and Alarm Monitoring tabs have independent video panels. This means that there is no connection between them. They work independently and are configured independently.

If a new access or alarm transaction is received from a reader or input that has a relationship to a camera (see "[Logic tree & Tile management](#)" on the previous page), the playback of this event is automatically displayed in a video panel tile.

Double-click a tile to change the video panel configuration to a single view , where the selected tile is displayed.

If two or more cameras are linked to a reader/input, where an event took place, the operator may choose to view the event from the second camera. To change cameras, right-click on the relevant tile and select the other camera from the context menu item **Show on other cameras** and select the second camera.



**Note:** Video events may also be seen from the Security Center screen. For information, about the Security Center, see "[Security Center](#)" on page 389.



## Virtual remote




The virtual remote allows an operator to control a live video stream or a playback on the tile in focus. When changing the focus between different tiles, the color of "Live Camera" and "Playback" buttons change to reflect the mode of the selected tile (i.e. Live mode or playback mode).


In addition, the virtual remote allows operators to manually override the lock/open state of a door or the arm/disarm state of an alarm zone.


The table below describes each virtual remote control available.

Virtual Remote Controls

Setting	Description
	<b>Live Camera button:</b> Switches the tile in focus to the Live Video Stream mode. When the button has an orange background, the current view is live footage.
	<b>Playback button:</b> Switches the tile in focus to Playback mode. When the button has an orange background, the tile in focus is in Playback mode. Playback mode is used in conjunction with the <b>Calendar</b> button to choose a specific date and time of the video record that will be played back (play a previously archived video).




Setting	Description
	<p><b>Snapshot button:</b> Captures a still image from a video running in the tile in focus. The captured image is saved as a BMP file in the folder:</p> <p>C:\ProgramData\ACS\GUI\Snapshots</p> <p>The file name is in the following format: snapshot_&lt;camera name&gt;_&lt;YYYY_MM_DD&gt;_&lt;HH_mm_ss&gt;.</p>
	<p><b>Calendar button:</b> Opens a Date &amp; Time dialog where you can specify a point in a playback's track where the video will start to play. After you click <b>OK</b> in the dialog, the playback automatically starts to play the specified footage in the tile in focus.</p>
	<p><b>Open Door:</b> Opens a context menu, which provides you with multiple open door override options. These options are applied to the relays of the relevant reader associated with the selected tile's camera feed. If the selected tile is empty, there is no context menu.</p> <p>The available open door options are:</p> <ul style="list-style-type: none"> <li>» Open &lt;readername&gt; constantly</li> <li>» Open &lt;readername&gt; for 5 seconds</li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> 5 seconds is the default setting. You can change the value in the Options screen (see "<a href="#">Options Screen</a>" on page 567).</p> </div> <ul style="list-style-type: none"> <li>» Return &lt;readername&gt; relays to normal mode</li> <li>» Open 'All' associated doors at the same time</li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> The Open 'All'... option only appears when multiple readers are associated with the camera feed current displayed in the tile in focus.</p> </div>

Setting	Description
	<p><b>Lock Door:</b> Opens a context menu, which provides you with multiple lock door override options. These options are applied to the relays of the relevant reader associated with the selected tile's camera feed. If the selected tile is empty, there is no context menu.</p> <p>The available lock door options are:</p> <ul style="list-style-type: none"> <li>» Close &lt;readername&gt; constantly</li> <li>» Close &lt;readername&gt; for 5 seconds</li> </ul> <hr/> <p><b>Note:</b> 5 seconds is the default setting. You can change the value in the Options screen (see "<a href="#">Options Screen</a>" on page 567).</p> <hr/> <ul style="list-style-type: none"> <li>» Return &lt;readername&gt; relays to normal mode</li> <li>» Close 'All' associated doors at the same time</li> </ul> <hr/> <p><b>Note:</b> The Close 'All'... option only appears when multiple readers are associated with the camera feed current displayed in the tile in focus.</p>

Setting	Description
	<p><b>Arm Alarm Zone:</b> Open a context menu, which provides you with multiple arm override options for an alarm zone of an input linked to the selected camera.</p> <p>To see the context menu, the camera feed must be displayed in a tile that is in focus.</p> <p>The available alarm zone arm options are:</p> <ul style="list-style-type: none"> <li>» ARM &lt;alarm zone name&gt; for 5 seconds</li> </ul> <div style="border: 1px solid black; background-color: #f9e79f; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> 5 seconds is the default setting. You can change the value in the Options screen (see "<a href="#">Options Screen</a>" on page 567).</p> </div> <ul style="list-style-type: none"> <li>» ARM &lt;alarm zone name&gt; for 1 minute</li> </ul> <div style="border: 1px solid black; background-color: #f9e79f; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> 1 second is the default setting. You can change the value in the Options screen (see "<a href="#">Options Screen</a>" on page 567).</p> </div> <ul style="list-style-type: none"> <li>» ARM &lt;alarm zone name&gt; constantly</li> <li>» ARM &lt;alarm zone name&gt; until next time zone</li> </ul> <p>This means that the alarm zone will remain armed until the associated time zone switches from a green period to a white period or vice versa.</p> <ul style="list-style-type: none"> <li>» ARM 'All' associated alarm zones at the same time</li> </ul> <div style="border: 1px solid black; background-color: #f9e79f; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> The ARM 'All'... option only appears when multiple inputs are associated with the selected camera.</p> </div>

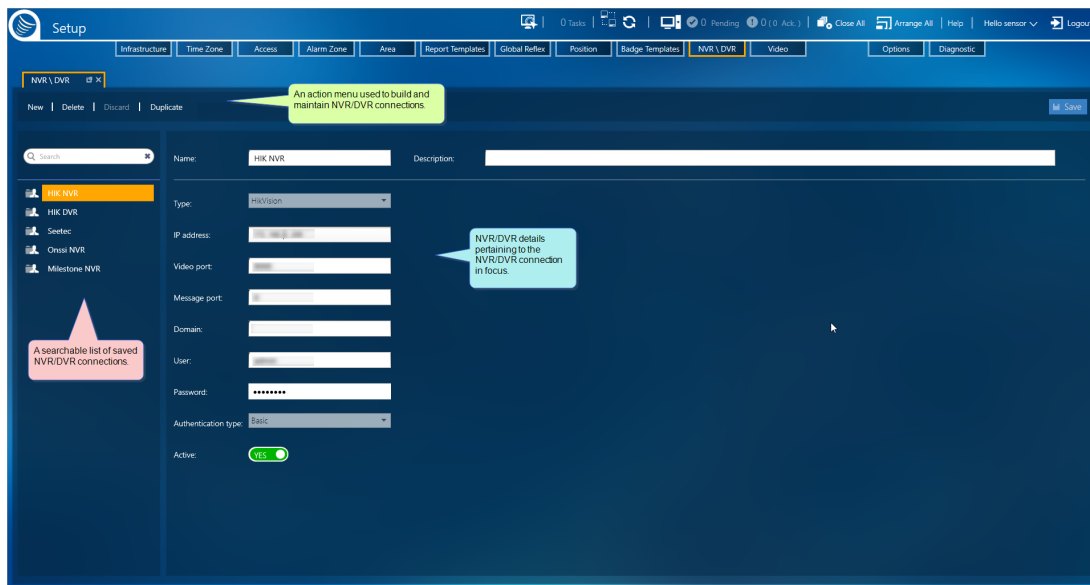
Setting	Description
	<p><b>Disarm Alarm Zone:</b> Open a context menu, which provides you with multiple disarm override options for an alarm zone of an input linked to the selected camera.</p> <p>To see the context menu, the camera feed must be displayed in a tile that is in focus.</p> <p>The available alarm zone disarm options are:</p> <ul style="list-style-type: none"> <li>» DISARM &lt;alarm zone name&gt; for 5 seconds</li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> 5 seconds is the default setting. You can change the value in the Options screen (see "<a href="#">Options Screen</a>" on page 567).</p> </div> <ul style="list-style-type: none"> <li>» DISARM &lt;alarm zone name&gt; for 1 minute</li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> 1 second is the default setting. You can change the value in the Options screen (see "<a href="#">Options Screen</a>" on page 567).</p> </div> <ul style="list-style-type: none"> <li>» DISARM &lt;alarm zone name&gt; constantly</li> <li>» DISARM &lt;alarm zone name&gt; until next time zone</li> </ul> <p>This means that the alarm zone will remain disarmed until the associated time zone switches from a green period to a white period or vice versa.</p> <ul style="list-style-type: none"> <li>» DISARM 'All' associated alarm zones at the same time</li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> The DISARM 'All'... option only appears when multiple inputs, belonging to various alarm zones, are associated with the selected camera.</p> </div>
	<p><b>PTZ controls:</b> Moves a <b>PTZ</b><sup>1</sup> camera during Live mode. Use the arrows to move to the required position. The Plus/Minus buttons are used to zoom in or zoom out.</p> <p>When displaying a previously recorded video, the PTZ controls are hidden.</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> The HIK NVR/DVR, by default, assumes all cameras are PTZ enabled.</p> </div>

<sup>1</sup>A pan-tilt-zoom camera is a camera that is capable of remote directional and zoom control.

Setting	Description
	<p><b>Note:</b> For these buttons to be enabled, presets must be predefined in your NVR/DVR system.</p> <p><b>PTZ Presets:</b> Moves a PTZ camera to a predefined position. These buttons are only available during Live mode. A preset can be selected by clicking a preset number or by selecting a preset position by name from the drop-down list found just below the 4, 5, 6 preset numbers.</p> <p>When displaying a previously recorded video, the PTZ controls are hidden.</p>
	<p><b>Volume Control:</b> Adjusts the volume of the selected camera.</p>
	<p><b>Playback Controls:</b> The controls include <b>Rewind</b>, <b>Pause</b>, <b>Play</b>, and <b>Fast Forward</b>.</p> <p>These controls allows you to pinpoint a time in a track where you want to play or pause a playback.</p>

# Video NVR/DVR Screen

Figure A-90



Through the Video NVR/DVR screen, operators build connections between GuardPoint10 and third-party NVR/DVR systems. In addition, the NVR/DVR screen is where the rules governing the behavior established by the connection to the NVR/DVR systems, and the Video Security screen are configured.

GuardPoint10 only supports 64-bit NVRs/DVRs.

The NVR/DVR screen includes the following distinct areas:

## A list of existing NVRs/DVRs

The area contains a searchable list of previously saved NVR/DVR connections.

Select an NVR/DVR connection from the list to see the connection's parameters and other details specific to the NVR/DVR connection in focus.

## An NVR/DVR connection action bar

From the action bar, you can add / delete / duplicate an NVR/DVR connection. Any unsaved changes to an NVR/DVR connection may be discarded at which point the NVR/DVR connection reverts to its previously saved values.

The action also includes a **Define General Configuration** button that opens a list of parameters that govern the behavior of the Video Security screens.

## NVR/DVR connection parameters

Contains fields about the NVR/DVR connection in focus.

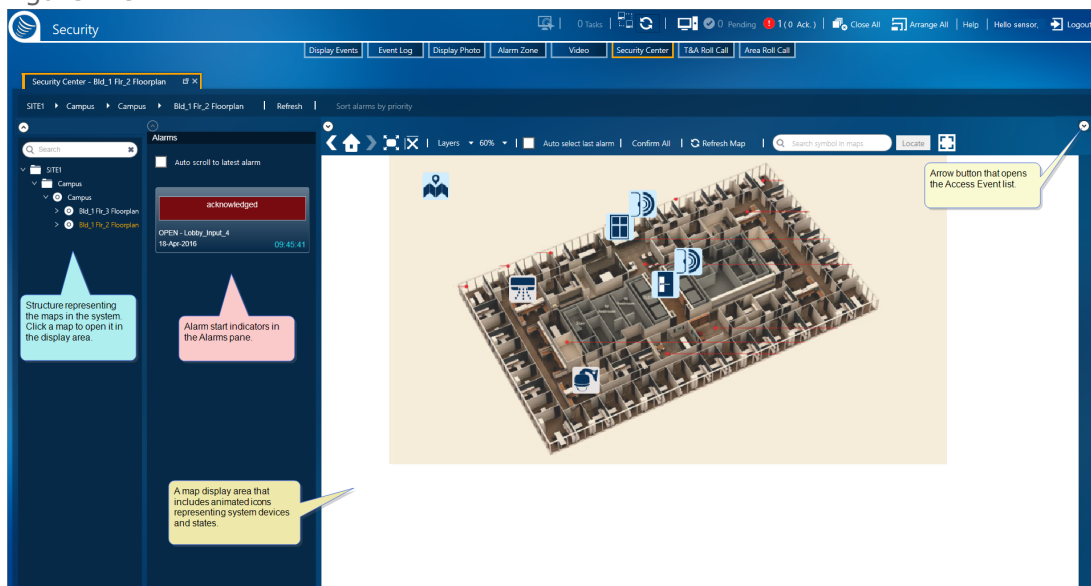


Table A-59 NVR/DVR Connection Parameters

Parameter	Description
Name	<p>A free text field that identifies the NVR/DVR connection. The default name is "New NVR".</p> <p>A best practice is to rename the NVR/DVR connection to something that identifies the NVRs/DVRs monitoring space.</p>
Description	(Optional) A free text field where information about the NVR/DVR connection is entered.
Type	The name of the NVR/DVR provider where the connection is being established.
IP Address	Identifies a TCP network destination of a provider's NVR/DVR. The site uses the IP address to route camera-captured data to theGuardPoint10 system.
Video Port	The port used by an NVR/DVR to communicate with theGuardPoint10 system. This information should be provided by hardware installation personnel.
Message Port	The port where an NVR looks for messages from GuardPoint10. An NVR message is made via a Global Reflex Action.
Domain	The name of the domain where the NVR/DVR is located.
User	The user name used to login to the NVR/DVR.
Password	The password used to login to the NVR/DVR.
Authentication Type	<p>The single sign-on credential type used by the NVR/DVR access authentication. The available options are <b>Basic</b> and <b>Windows</b>.</p> <p><b>Windows</b> authentication is sensitive to the network environment (i.e. the domain server). <b>Basic</b> authentication takes the user name and password defined in the NVR or DVR regardless of the environment.</p> <p>A best practice when experiencing streaming issues is to check the network environment or, switch from <b>Windows</b> to <b>Basic</b> authentication.</p> <hr/> <p><b>Note:</b> HikVision does not support <b>Windows</b> authentication. If <b>HikVision</b> is the selected <b>Type</b>, The <b>Authentication Type</b> field will automatically set to <b>Basic</b> and will be read-only.</p>
Active	When set to <b>YES</b> , camera-captured data from the NVR/DVR is acquired by GuardPoint10 as required.

# Security Center Screen

Figure A-91



The Security Center screen provides a central alarm monitoring and management facility, where graphic representations of controllers, doors, inputs, relays, and alarms status may be monitored on a map. Actions and processes can be triggered from an individual icon or an object's context menu.

Multiple instances of the Security Center screen may be open at the same time. Each instance works independently.

Searchable tree of maps

The Security Center screen has the following primary areas:

- » Searchable tree of maps
- » Alarms list
- » Access Event list
- » Map navigation and map page view options
- » Map page

## Searchable tree of maps

The map tree reveals the structure of the map groupings.

A map must be in a folder (group) a group may have multiple maps and multiple sub-groups. The purpose of a group is to create a logical structure for maps.

A map can have a sub-map, but not a sub-group.

## Alarms list

The list contains current alarms that require an operator's attention.

Each alarm contains text describing the cause of the alarm and a timestamp indicating when the alarm occurred.


At the top of the Alarms list, is an **Auto Scroll to Latest Alarm** checkbox. When selected, the last alarm triggered will be in view in the list.

A listed alarm has the following context menu options:

- » **Acknowledge:** The alarm is recognized by the operator. An acknowledgment is reflected in the alarm listing and in the pending area of the dashboard. An alarm must be acknowledged before it can be confirmed.
- » **Confirm:** Opens a Confirmation dialog where you may enter a description of the alarm and details that confirm your observation of the alarm. Click **Confirm** to complete the confirmation process. After an alarm is confirmed, it is removed from the alarms list. The confirmation event can be seen in the Event log (see ["Display Events Screen" on page 353](#))
- » **Navigate to map:** If the alarms input appears on a map in the Security Center, the map will be displayed and the icon is brought into view.

Above the alarms list are the following sort options:

- » **Sort alarms by priority:** Restructures the list of alarms by priority with the highest priority alarm at the top of the list. The priority number is set in an input's details (see ["Alarm Priority" on page 500](#)). If you sort the alarm list by priority, this button changes to a **Sort alarms chronologically** button.
- » **Sort alarms chronologically:** The most recent alarm appears at the top of the list and the oldest at the bottom. If you sort the alarm list chronologically, this button changes to a **Sort alarms by priority** button.



**Note:** An alarm's Acknowledge and Confirm designations can also be performed via the dashboard (see ["Dashboard Content & Actions" on page 334](#)).

## Access Events list

The list contains cards. Each card has information about an access event. The card appears in real time. The list is sorted chronologically with the most recent event at the top.

The list is opened by clicking the arrow button on the far right of the toolbar where the Map navigation and map page view options are located.





Each access event card contains information about the event and a timestamp indicating when the event took place. A photo of the cardholder who initiated the event is also displayed on the opposite side of the card (click the card to flip it). If the cardholder does not have a photo in the system, an avatar will be used as a placeholder. The cardholder's details may also be displayed from the card (double-click the card).

The Access Event pane, where the list is located, is opened by default. To hide/show the pane, click the arrow to the right of the Description field (near the screen border).

## Map navigation and map page view options

The map navigation and page view options available in the menu are described in the following table.

Table A-60 Map Navigation & Map Page View Menu

Name	Description
	Click the arrows to go to the previous or next map page in the map tree. Click the house to go to the default map page.
	The map zoom will automatically change to "Fit to Page".
	The map aligns to the left-top corner of the map page.
Layers	From the Layer's drop-down list, select the type of icons to show or hide on the map page.
Magnification	From the drop-down list, select a magnification level of the map page.
Auto select last alarm	When selected, an alarm instance will trigger the icon, representing the physical component in the system where the alarm was triggered, to be brought into view, regardless of the currently opened map.  Essentially, the checkbox automates the <b>Navigate to map</b> action (see <a href="#">Navigate to map</a> ).
Confirm All	Automatically confirms all alarm events listed. This operation does not include a description option and does not require an operator to first acknowledge the alarms.
Refresh	Eliminates any lag in the screen display.
Locate	The locate field is a Find tool. Enter text in the field, and then open the field's drop-down list. Objects that contain the text will appear on the list.  Select one of the object names and click the <b>Locate</b> button. The map page where the object is located is displayed and the object in question is in focus.
	Displays a map in full screen / Exit full screen. To accommodate the full screen view, other panes on the screen will be collapsed.

## Map page

















The map page is a primary monitoring area. The map page includes two layers:







- » The layer where a map, blueprint, or floorplan is visible.
- » The layer where icons, shapes, and textboxes, which are mapped to a corresponding physical component in the system, are visible.







Events and status changes that take place on your system are identified by a change in the appearance of the relevant icon, shape, or textbox on a map page.

The following is a key to event and status changes reflected in an icon, shape, or textbox :

Table A-61 Map Page Object Key

Object	Description & Example
Relay	ON: icon orange foreground  OFF: icon blue foreground  A door associated with a relay that is ON 
Input & Door	Armed and a physical change in status: Red foreground and blinking, red sound-emitting graphic 
Input & Door	Armed and a physical change in status, but the alarm start is configured with a delay: Red foreground with an orange clock in the foreground and blinking, red sound-emitting graphic 
Input & Door	Disarmed and a physical change in status: The door or input icon will appear open or closed, depending on the physical status (i.e.   ).
Relay & Door	Constant state ON: Green power symbol on top of the icon. If there is an association between the relay and the door, both will appear with the power symbol   Constant state OFF: Red power symbol on top of the icon. If there is an association between the relay and the door, both will appear with the power symbol  
Object backgrounds	Normal operation: Light blue  Input & Door armed: Light red  Acknowledged alarm: Light green  No communication: Dark gray background  Unlinked or deactivated input: Light gray background 

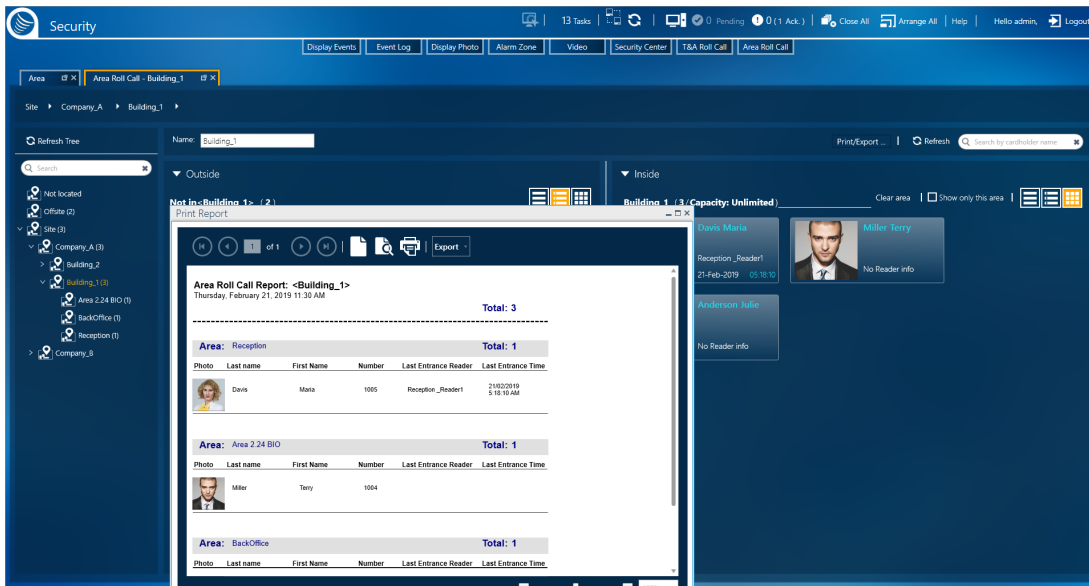
Object	Description & Example
Line Tampering	<p>Only relevant where an icon is linked to a 4 State input device that is connected to a sensor/detector.</p> <p>There are two tampering alarm icons:</p> <p>A line that connects a sensor/detector to the input device is cut: </p> <p>A line that connects a sensor/detector to the input device has caused a short circuit: </p> <p>The Line Cut and the Short overlays will remain on the icon until the line issue is resolved.</p> <div style="border: 1px solid black; padding: 5px; background-color: #fff9c4;"> <p><b>Note:</b> The line tampering overlays will also appear when the input icon is linked to a Galaxy zone (input).</p> <p>Even when the Galaxy group, where the zone is located, is not armed, tampering will be detected.</p> </div>
Shape or Textbox	<p>Linked map has an alarm on its icon layer: Red border and blinking, red sound-emitting graphic </p> <p>Linked map has an acknowledged alarm on it: Green border </p> <p>Linked area has a blue border.</p> <p>Linked area that is at or above the area's defined capacity has a red border.</p>
Miscellaneous icon linked to an area	<p>Linked area has a blue background.</p> <p>Linked area that is at or above the areas defined capacity has a red background.</p> <p>The Area's icon can be linked to an Area's Roll Call screen or Area details screen.</p>
Map icon	<p>Linked map has an alarm on its icon layer: Red border and blinking, red sound-emitting graphic </p> <p>Linked map has an acknowledged alarm on it: Green background </p>

Object	Description & Example
Controller icon	<p>Deactivated: Very dark gray foreground with a dark background. All icons representing a physical component connected to the deactivated controller appear with a dark background </p> <p>Where a sensor exists in a controller, a linked controller has a Box Open alarm on its icon layer: </p> <p>Where a sensor exists in a controller, a linked controller has a Low Battery alarm on its icon layer: </p> <p>Where a sensor exists in a controller, a linked controller has a Power Supply Failure alarm on its icon layer: </p>
Galaxy Panel linked to a Controller icon	<p>A Controller icon linked to a Galaxy panel may display and behave and display overlays like a Controller icon linked to an GuardPoint10 controller. However, there are additional alarm overlays that may only appear on the Galaxy panel icon layer.</p> <p>Communication issue with the alarm panel: </p> <p>Alarm panel mounting issue: </p>

The border and background colors described in the " [Map Page Object Key](#)" on page 683 table reflects the default colors set in the Options screens Security Center tab, see "[Security Center](#)" on page 582.

# Area Roll Call Screen

Figure A-92



The Area Roll Call screen provides a central screen where a cardholder's presence in a particular area is made known via a table or graphic display.



The Area Roll Call screen has three primary sections:

- » **Searchable tree of areas:** Reveals the Area structure built in via the Area screen. It allows an operator to display information about cardholders in the selected area and not in the area with a simple click.
- » **Outside:** Displays the cardholders who are off the premises or whose location is unknown. Initially, the Outside section is contracted with hidden details. Click the arrow at the left of the Outside text to expand the section and show the details.
- » **Inside:** Displays the cardholders who are in the selected area or one of its sub-areas.

## Searchable tree of areas

The area tree reveals the structure of the areas defined via the Area screen.

An area must be a sub-area of another area, the initial area is the site. An area may have multiple sub-area levels.

An area in the tree is preceded by an icon . When an area's occupancy is equal to or more than its capacity, the icon's background turns red .

The **Not Located** tree item and the **Offsite** tree item are special areas. The **Not Located** item includes cardholders who have never entered the site or, some other special circumstance. The **Off-site** item includes cardholders who have entered the site in the past, but are currently not on the site (i.e. went home).



## Outside and Inside partition

Both sides of the partition (Outside Inside) are similar in their appearance. The primary difference is the content. The Inside contains the cardholders who are in the area and possibly sub-areas. The Outside contains all cardholders who are not in the Inside.

For the **Not Located** tree item, the Outside table includes all cardholders who are **Offsite** or **onsite (i.e. in an area)**.

For the **Offsite** tree item, the Outside table includes all cardholders who are **in an area** and excludes those cardholders who are **Not Located**.

The areas are separated by an adjustable partition line that allows you to increase or decreases the space on either side of the screen.

The **Print/Export...**, **Refresh** and **search field** only apply to the Inside.

The **Show only this area** checkbox filters the Inside content to only show the cardholders in the area that is in focus and exclude any sub-area content. This filter also applies to a report generated from the Area Roll Call screen.

The **Clear Area** button moves all cardholders from the **Inside** table to **Not located**. If the area is also a GAPB area (GAPB level), the cardholder's GAPB level will also be moved to **Not located**. The cardholders that were moved to **Not located** will now also have a free Access Granted event at any reader. If the area is a GAPB area, this means that a cardholder can exit one GAPB area, or enter another GAPB area even if it violates a GAPB rule.




For more information about Global Anti-Passback (GAPB), see "[Understanding Anti-passback in GuardPoint10](#)" on page 80.



**Note:** The Free Access Granted event is not area or GAPB area specific. The cardholder may swipe for a Free Access Granted event at any available reader in the system.

Each area consists of the following:

Table A-62 Area Roll Call Screen Items

Name	Description
Group Title	Identifies the <b>Inside</b> and <b>Outside</b> areas of the Area Roll Call screen. Each title is followed by the number of cardholders currently in the title's group.
 View Switch button	Changes the view of a cardholder group. The button changes as required to one of the following: <ul style="list-style-type: none"> <li> Switches from Table view to Card view.</li> <li> Switches from Card view to Table view.</li> </ul>
Search Field	Narrows the displayed content of both partitioned areas to only show the cardholders included the search criteria.

Name	Description
Print/Export...	<p>Open a Print Report window where Inside Outside cardholder information is displayed in a table. From the Print Report window's toolbar, you can do the following:</p> <ul style="list-style-type: none"> <li>» Click the <b>arrow buttons</b> to page through the report.</li> <li>» Click the <b>Print icon</b> to open a standard windows Print dialog and send the report to a local printer.</li> <li>» Click <b>Export</b> to select a file format and location where you can save the Area Roll Call data.</li> </ul>

Table A-63 Area Roll Call Table Heading and Card Information

Name	Description
Photo	<p>Where an image of a cardholder may be displayed. A member of the security staff can later use the image for visual ID verification.</p> <p>If a cardholder doesn't have a photo in the system database, an avatar is used as a placeholder.</p>
Last Name	The cardholder's last name.
First Name	The cardholder's first name.
Number	The internal system number assigned to each cardholder. A cardholder's uniqueness is determined by a combination of a cardholder's first name, last name, and internal system number. However, there is an option to allow duplicate names, in such cases, the internal system number alone represents the uniqueness of a cardholder.
Last Entrance or Exit Reader	The name of the reader where a cardholder last attempted to gain access.
Last Entrance or Exit Date	The date and time when a cardholder last attempted to gain access.

If in Graphic view, click on a card to flip it and see the following additional information:

Table A-64 Area Roll Call Card Information - Backside of Card

Name	Description
Number	The internal system number assigned to each cardholder. A cardholder's uniqueness is determined by a combination of a cardholder's first name, last name, and internal system number. However, there is an option to allow duplicate names, in such cases, the internal system number alone represents the uniqueness of a cardholder.

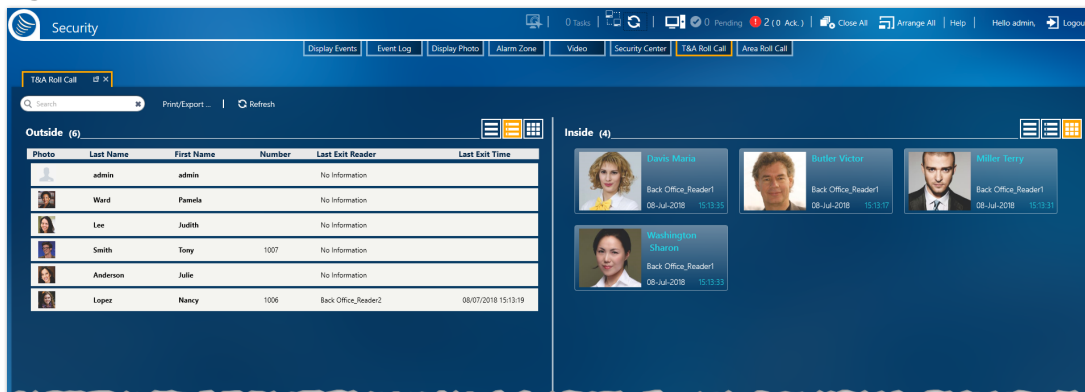
Name	Description
Company	The name of a company (known to the system) where the cardholder has an association (i.e. employment).
Department	The name of the department where the cardholder has an association.
ID	A third-party identification number (i.e. a driver license number) that, if necessary, can be verified by authorities.
Last Pass Reader	The name of the reader where a cardholder last scanned their badge, used a PIN code or a combination of the two, depending on various parameter settings.
Last Pass Date	The date and time when a cardholder last scanned their badge, used a PIN code or a combination of the two, depending on various parameter settings.

Click on a card to flip it back to the front.

Double-click a table row or a card to open a cardholder's details. For information about cardholder details, see ["Reader Details" on page 453](#).

# T&A Roll Call Screen

Figure A-93



The T&A Roll Call screen provides a central screen where a cardholder's presence is made known via a table or graphic display.

The T&A Roll Call screen has two primary areas:





- » **Outside:** Displays the cardholders who are off the premises or whose location is unknown.
- » **Inside:** Displays the cardholders who are on the premises.

The areas are identical in their functionality and appearance. The only difference is the content.

The areas are separated by an adjustable partition line that allows you to increase or decrease the space on either side of the screen.

Each area consists of the following:

Table A-65 T&A Roll Call Screen Items

Name	Description
Group Title	Identifies the <b>Inside</b> and <b>Outside</b> areas of the T&A Roll Call screen. Each title is followed by the number of cardholders currently in the title's group.
  View Switch button	Changes the view of a cardholder group. The button changes as required to one of the following: <ul style="list-style-type: none"> <li> Switches from Table view to Card view.</li> <li> Switches from Card view to Table view.</li> </ul>
Search Field	Narrows the displayed content of both partitioned areas to only show the cardholders included in the search criteria.

Name	Description
Print/Export...	<p>Open a Print Report window where Inside Outside cardholder information is displayed in a table. From the Print Report window's toolbar, you can do the following:</p> <ul style="list-style-type: none"> <li>» Click the <b>arrow buttons</b> to page through the report.</li> <li>» Click the <b>Print icon</b> to open a standard windows Print dialog and send the report to a local printer.</li> <li>» Click <b>Export</b> to select a file format and location where you can save the T&amp;A Roll Call data.</li> </ul>

Table A-66 T&A Roll Call Table Heading and Card Information

Name	Description
Photo	<p>Where an image of a cardholder may be displayed. A member of the security staff can later use the image for visual ID verification.</p> <p>If a cardholder doesn't have a photo in the system database, an avatar is used as a placeholder.</p>
Last Name	The cardholder's last name.
First Name	The cardholder's first name.
Number	The internal system number assigned to each cardholder. A cardholder's uniqueness is determined by a combination of a cardholder's first name, last name, and internal system number. However, there is an option to allow duplicate names, in such cases, the internal system number alone represents the uniqueness of a cardholder.
Last Pass Reader	The name of the reader where a cardholder last scanned their badge, used a PIN code or a combination of the two, depending on various parameter settings.
Last Pass Date	The date and time when a cardholder last scanned their badge, used a PIN code or a combination of the two, depending on various parameter settings.

If in Graphic view, click on a card to flip it and see the following additional information:

Table A-67 T&A Roll Call Card Information - Backside

Name	Description
Number	The internal system number assigned to each cardholder. A cardholder's uniqueness is determined by a combination of a cardholder's first name, last name, and internal system number. However, there is an option to allow duplicate names, in such cases, the internal system number alone represents the uniqueness of a cardholder.

Name	Description
Company	The name of a company (known to the system) where the cardholder has an association (i.e. employment).
Department	The name of the department where the cardholder has an association.
ID	A third-party identification number (i.e. a driver license number) that, if necessary, can be verified by authorities.
Last Pass Reader	The name of the reader where a cardholder last scanned their badge, used a PIN code or a combination of the two, depending on various parameter settings.
Last Pass Date	The date and time when a cardholder last scanned their badge, used a PIN code or a combination of the two, depending on various parameter settings.

Click on a card to flip it back to the front.

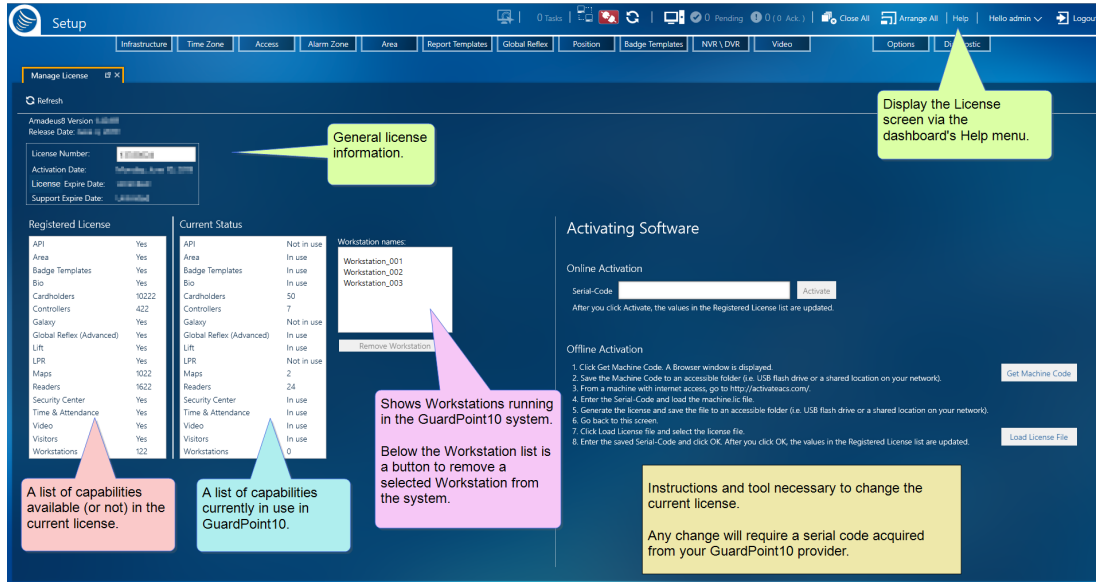
Double-click a table row or a card to open a cardholder's details. For information about cardholder details, see ["T&A Reader" on page 459](#).

# License, Help, and About

This topic includes information available via the Help item in the dashboard.

- » The License Details screen presents the scope of the GuardPoint10 license, and what is currently in use.

Figure A-94



- » The GuardPoint10 Help is displayed in a web browser that supports HTML5. It includes:
  - » General information about GuardPoint10 solution modules.
  - » A detailed description of each screen.
  - » Step-by-step instruction to perform the various tasks available and more...
- » The About box includes the version number of your GuardPoint10 installation as well as copyright information.

## To open the License screen:

- » From the Dashboard, click Help > License. The License screen is displayed.

**Note:** The number of cardholders counted as **in use** by the license is based only on the cardholders who have badge codes.

## To change the current license:

Follow the instructions on the screen for either Online or Offline license activation.

If the machine running GuardPoint10 is connected to the internet, acquire the serial code from your GuardPoint10 provider, and use Online activation.

If the machine running GuardPoint10 is *not* connected to the internet, acquire the serial code from your GuardPoint10 provider, and follow the Offline activation instruction.

## To remove a workstation from the GuardPoint10 system:

1. In the Workstation Name list, all workstations currently running in the system are listed.
2. To deny one of the listed workstations GuardPoint10 system access, select the workstation that will be removed.
3. Click the Remove Workstation button. The Workstation is removed from the list.

The next time an operator logs in the GuardPoint10 from the workstation, the workstation will reappear in the Workstation Name list.



**Warning:** After activating a license, it is permanently connected to the GuardPoint10 Full installation (server) machine. If the machine, where the GuardPoint10 Full installation exists, is at some point replaced, a new license must be acquired and activated.

## To open the Help:

- » From the Dashboard, click Help > Help. The default web browser opens with the GuardPoint10 Help home page displayed.

Or,

- » Open an GuardPoint10 screen where help is required and press F1. The Help topic related to the opened screen is displayed.

We encourage you to use the Help's powerful search tool to learn more about GuardPoint10 and all of its features.

## To open the GuardPoint10 About Box:

From the Dashboard, click Help > About. The About box is displayed with information about your GuardPoint10 software.



# APPENDIX B:

## Table Filters

If your table contains a lot of content, it can be difficult to find information quickly. Filters narrow down the data in your table, enabling you to view only the information you need in a manageable table.

Most every column in an GuardPoint10 table has a filter. There are some minor variations between filters, but fundamentally, they are all the same.

There are two categories of filter, Basic and Advance. use either filter category or a combination of the two to get the desired table view.

To open a filter and set filter criteria:


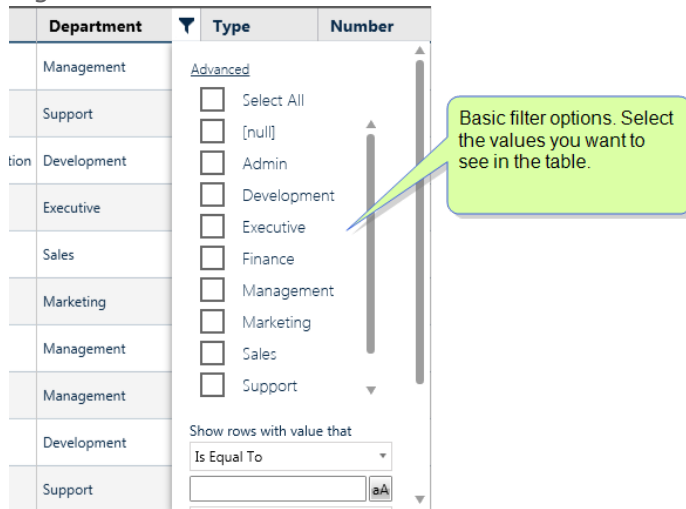
1. **Mouseover**<sup>1</sup> a column heading. A funnel icon appears .
2. Click the icon. A filter rollout is displayed.

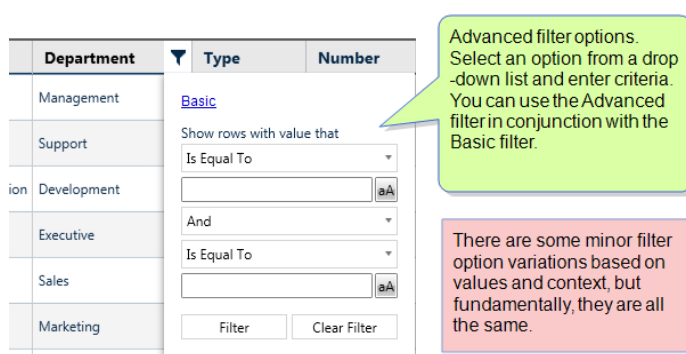
Figure B-1



Initially, only the basic options are visible in the dialog.

- » **Basic:** The basic options usually consist of checkboxes for each possible value that may appear in the column. If you only want to see rows that contain a specific value, select the checkbox for that value. You can select more than one checkbox.
- » **Advanced:** Click **Advanced** in the rollout to set a more complex filter option. This option uses logical operators to determine which rows will be visible in the table. Look at the drop-down list of operators and play with it a little to get familiar with the filter tool.

Figure B-2



After a filter has been selected, the funnel icon in the column heading, where the filter was created, changes to yellow and remains visible in the column heading.

As the size of your data increases, rely on the filters to help you find information quickly.

To remove a filter, click the **Clear Filter** found at the button at the bottom of the rollout.

<sup>1</sup>Moving a cursor over a specific point on a page (i.e. text, field, or row).

# APPENDIX C:

## Escort Rules for Access Events

The following demonstrates the logic of the escort rules in various scenarios, assuming that the reader's **Escort** parameter is set to **Yes**:

- » A cardholder's **Needs Escort** parameter checkbox is selected, the cardholder may swipe their badge, but another cardholder with the **Supervisor** parameter checkbox selected must swipe their badge afterward making the supervisor the designated escort.

In addition, a cardholder whose **Needs Escort** and **Supervisor** parameter checkboxes are *not* selected may swipe their badge, but another cardholder with the **Needs Escort** parameter checkbox selected must swipe their badge afterward making the cardholder (with **Needs Escort** selected) the designated escort.

- » A cardholder's **Needs Escort** and **Supervisor** parameter checkboxes are *not* selected, the cardholder may swipe their badge, but another valid cardholder (regardless of their **Needs Escort** or **Supervisor** setting) must swipe their badge afterward making the valid cardholder the designated escort.
- » A cardholder's **Supervisor** parameter checkbox is selected, the cardholder may swipe their badge, but another valid cardholder (who has either their **Needs Escort** or **Supervisor** checkbox selected) must swipe their badge afterward making the valid cardholder the designated escort.
- » A cardholder's **Needs Escort** and **Supervisor** parameter checkboxes are both selected, the cardholder may swipe their badge without a required second valid cardholder. In addition, the cardholder may escort (be the second swipe) for any valid cardholder who has either their **Needs Escort** or **Supervisor** checkbox selected.

Where a second badge swipe is required, the second badge must be scanned within the time frame set in the **Door Open Time** parameter (default is 4 sec). The second cardholder is recorded as having accompanied the first cardholder. In the Table Log, this is considered a single event. The following is an example of the single log entry.

Figure C-1

06-07-15 13:45:21 Access Granted 'John Smith {Robert Brown}'; From reader C3rdr1

The name of the escort is in curly brackets.

# APPENDIX D:

## Hardware Information

General information about your system's SENSOR hardware will give you a better understanding of how your system works. Take advantage of this information to better configure your system's features and troubleshoot GuardPoint10 issues.

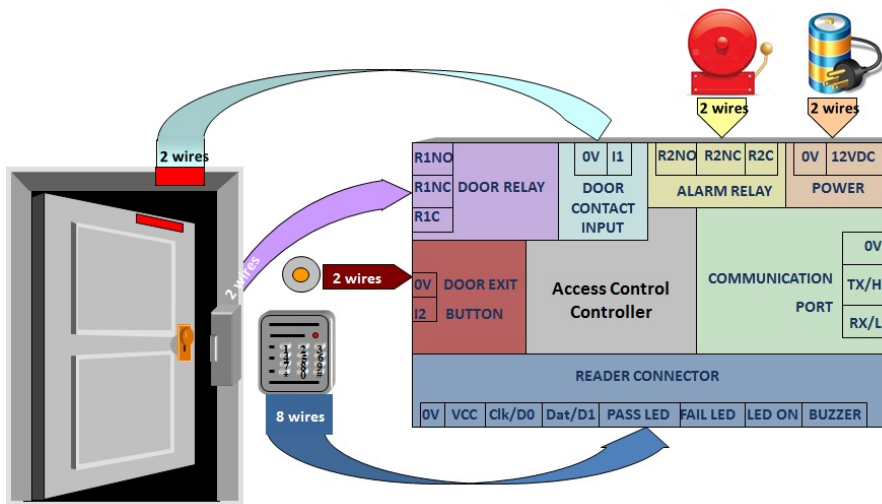
# Hardware Installation

SENSOR system controllers are microprocessor based. They are designed to operate 24 hours a day, 7 days a week.

GuardPoint10 compatible controllers must have firmware from 2016 or later.

To manage the security of a given environment requires a controller to be connected to various types of external devices such as badge readers, electrical door openers, alarm detection devices, printers, mainframes, etc.

Figure D-1



To accommodate the various types of connections, the system is subjected to some rigid constraints related to:

- » Electromagnetic Interferences (EMI) along the lines connecting a controller to any external devices. In case of lightning, an undesired voltage may reach thousands of volts.
- » The external devices themselves. In most cases, the devices are not supplied by SENSOR but are chosen in response to the constraints of a particular installation site (local distributors, national operating standards, etc.).

All SENSOR equipment is provided with internal protection against all such interference; these devices include varistors, protection diodes, etc. However, since SENSOR controller installation sites vary, we have put together some basic rules that should be observed when selecting a controller installation site. The rules are as follows:

1. The control unit (the electronic board) must never be installed inside a high voltage electrical power box and must never be placed in close proximity to large transformers or high voltage/-current source devices.
2. For maintenance, consider the accessibility of a controller.
3. The controller must be grounded separately. Therefore, one must verify in advance whether the installation site provides adequate grounding facilities.
4. The cover or case that contains a controller unit must be tightly screwed down or locked in place and accessible after mounting.

5. It is essential to plug the SENSOR controller's 230 volt sector cable into a "clean" line (i.e. a line not being used by other pieces of heavy equipment) or into an independent line, which has been specifically allocated to the controller. The line must be properly grounded.
6. Never use the same system cables guide to pass wires from another system, like sirens, electric door openers, etc.
7. Four categories of cable that go to and from a controller:
  - » A 230 volt cable
  - » Cables connecting readers, alarm entries and push-buttons
  - » A communication cable
  - » Cables connecting electric door openers or external release devices

These cables must be installed as far apart from each other as possible.

## Third-party hardware

### Biometric readers

GuardPoint10 supports Suprema biometric readers:

- » **BioEntry W2 (model name: BEW2-ODP)** with **firmware v1.1.2** or higher.
- » **BioEntry W2 (model name: BEW2-OAP)** with **firmware v1.1.2** or higher.
- » **BioEntry P2 (model name: BEP2-OD)** with **firmware v1.1.1** or higher.
- » **BioEntry P2 (model name: BEP2-OA)** with **firmware v1.1.1** or higher.
- » **BioLite BLN2-OAB** with **firmware 1.0.2 2018/07/09** or higher
- » **BioLite BLN2-PAB** with **firmware 1.0.2 2018/07/09** or higher
- » **BioLite BLN2-ODB** with **firmware 1.0.2 2018/07/09** or higher
- » **Facestation F2 (FSF2ODB)** with **firmware 1.0.5 2021/04/22** or higher
- » **Facestation F2 (FSF2-DB)**with **firmware 1.0.4 2021/03/03** or higher
- » **Facestation F2 (FSF2-AB)** with **firmware 1.0.4 2021/03/03** or higher

**Note:** Suprema2 devices only support em-marine badges.

**Note:** BioLite reader support excludes keypad functionality.

The firmware may be downloaded from the following site:

<https://www.supremainc.com/en/content/biostar-2-bioentry-w2-fw-v112>

Only em-marine badges are supported by Suprema2 devices.

### QR readers/scanners

GuardPoint10 supports most any QR code reader that has a Wiegand output. However, we have only tested the following QR reader in our lab:

- » **Carea Technology CR-3058C)**
- » **Datalogic Magellan™ 1100i)**

» **Newland FM30 Grouper II Series (FM3051 and FM3056)**

## Galaxy panels

Galaxy Dimension - Technical Specifications<sup>1</sup>

Description	GD-48	GD-96	GD-264	GD-520
Zones onboard (maximum) Inclusive wireless zones	16 - (48) 32	16 - (96) 80	16 - (264) 192	16 - (520) 192
Outputs (400rnA) on-board	8	8	8	8
RS485 Databuses	1	2	2	4
Users	100	250	1000	1000
7 Day Timer Schedules	19	35	67	67
Zone types	52	52	52	52
Keypads (Keyprox)	8 (3)	16 (7)	16 (7)	32 (24)
Bus mounted prox readers (MAX)	4	16	16	32
Event Log	1000	1500	1500	1500
RS232	Built-in	Built-in	Built-in	Built-in
Groups	8	16	32	32

Galaxy 3(G3) and Dimension (GD): RIO (Remote Input Output) & Buses

Galaxy Type	BUS RS485	Modules RIO
GD-48	1	4
GD-96	2	10
GD-264	2	31
GD-520	4	63
G3-48	1	4
G3-144	2	16
G3-S20	4	63

Every RIO has 8 zones and 4 relays

<sup>1</sup>In addition to the Number of zones indicated, each Galaxy type has 5 supplementary "tamper" zones.



Galaxy 3(G3) and Dimension (GD): Number of Groups, Inputs, and Relays

Galaxy Type	Group	No. of Inputs	No. of Relays
GD-48	8	48	24
GD-96	16	96	48
GD-264	32	264	132
GD-520	32	520	260
G3-48	4	48	24
G3-144	8	144	72
G3-S20	32	520	260

## NVR/DVR video surveillance systems

The video systems that may be connected to GuardPoint10 are as follows:

- » HikVision DVR
- » HikVision NVR
- » Milestone
- » Cayuga
- » OnSSI
- » Seetec
- » TVT
- » Dahua

Be aware, any GuardPoint10 workstation where an OnSSI video will play may require the following software installed:

- » Ocularis Viewer (64-bit)
- » Ocularis Client (64-bit)
- » LPR Camera systems

See "[Configuring a Video NVR/DVR connection](#)" on page 244 for more information about Onssi, Seetec, and Cayuga.

# Common Controller Features

SENSOR has many different types of controllers. Each controller was designed to satisfy the security needs of a specific environment. However, there are some features that have been maintained within each controller design. These features are:

## » **Real time clock (RTC)**

The controller internal memory stores all the system parameters (I/O parameters, time zones, etc.) that were previously downloaded from the PC. In addition, the controller records each event with the time and date of its occurrence.

## » **High-speed CPU**

CPU deals with all access control and alarm management tasks in high-security installations that require very large databases.

## » **On-board Lithium Battery**

For memory and real time clock (RTC) backup for 10 years.

## » **1MB Flash Memory**

It allows easy firmware upgrade (from PC). Controllers must have firmware from 2016 or later.

## » **Independent decisions at the local level**

Such as door opening, relays activating, reflexes triggering, without any computer intervention, without degradation of the security standard, even in the event of communication failure.

## » **Compatible with other SENSOR controllers**

## » **Communication baudrate<sup>1</sup> from 9,600 to 115,000 Bauds**

## » **Use of new technologies providing maximal protection against external disturbances**

## » **Programmable communication encryption**

## » **Simple installation and programming**

## » **Multi-technology readers**

Such as biometric, smart card, proximity, magnetic, etc.

## » **LED indication status**

The communication status (Rx/Tx) and the status of each input and output are indicated by a LED: Green LED for 'Rx' and red LED for 'Tx', Input LED is 'ON' when the relevant input is open or line is cut, Relay LED is 'ON' when the relevant relay is activated.

## » **Removable connectors**

---

<sup>1</sup>The rate at which information (signal or symbol changes) is transferred per second.

# Controller Comparison Tables

Table D-1 Controller Door/Reader Comparison Table

	Maximum Doors	Maximum Readers	Supported Technologies	Supports Reader Connection Status
IC550	1	2	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	Yes
IC1000	2	2	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	Yes
IC2000	2	4 (includes 2 slaves)	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	–
IC4000	4	4	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	–
IC2001	2	4 (includes 2 slaves)	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	Yes
IC4001	4	4	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	Yes
IC1604	–	–	-	–
IC500/NX <sup>1</sup>	2	2	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	Yes
IC1000/NX <sup>2</sup>	2	2	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	Yes
IC500 <sup>3</sup>	1	2	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	Yes
IC1000 <sup>4</sup>	2	2	Biometric, Smart Card, Proximity 125kHz, Mag Stripe	Yes

<sup>1</sup>GuardPoint10 Entry version only

<sup>2</sup>GuardPoint10 Entry version Only

<sup>3</sup>Not supported in GuardPoint10 Entry version

<sup>4</sup>Not supported in GuardPoint10 Entry version

Table D-2 Controller Input Comparison Table

	Input- s on board	Super- vised on- board inputs	Input dia- gnostic LED's	Additional super- vised inputs on ext. board	Additional tamper (MS) mon- itoring input	PSU Failed mon- itoring	Low bat- tery mon- itoring
IC550	4	Yes	Yes	–	Yes	Yes	Yes
IC1000 (old)	4	–	–	–	–	–	–
IC1000	4	Yes	Yes	–	Yes	Yes	–
IC2000	8	4 Only	Yes	8	–	–	–
IC4000	8	4 Only	Yes	8	–	–	–
IC2001	8	Yes	Yes	–	Yes	Yes	Yes
IC4001	8	Yes	Yes	8	Yes	Yes	Yes
IC1604	16	Yes	Yes	8	–	–	–
IC500/NX 1	4	–	–	–	–	–	–
IC1000/N- X <sup>2</sup>	4	–	–	–	–	–	–
IC500 <sup>3</sup>	4	–	–	–	–	–	–
IC1000 <sup>4</sup>	4	–	–	–	–	–	–

Table D-3 Controller Outputs (Relays) Comparison Table

	Outputs on board	Output diagnostic LED's	Additional out- puts on exten- sion board	Additional outputs on Satellites
IC550	2	Yes	–	–
IC1000 (old)	3	Yes	–	–
IC1000	3	Yes	–	–
IC2000	4	Yes	12	48

<sup>1</sup>GuardPoint10 Entry version only

<sup>2</sup>GuardPoint10 Entry version Only

<sup>3</sup>Not supported in GuardPoint10 Entry version

<sup>4</sup>Not supported in GuardPoint10 Entry version

	Outputs on board	Output diagnostic LED's	Additional outputs on extension board	Additional outputs on Satellites
IC4000	4	Yes	12	48
IC2001	4	Yes	12	–
IC4001	4	Yes	12	48
IC1604	4	Yes	12	48
IC500/NX <sup>1</sup>	2	Yes	–	–
IC1000/NX <sup>2</sup>	2	Yes	–	–
IC500 <sup>3</sup>	2	Yes	–	–
IC1000 <sup>4</sup>	2	Yes	–	–

Table D-4 Controller Communication Comparison Table

	RS232 Connectivity	RS485 Connectivity	TCP/IP on board	TCP/IP on extension board	PoE Connectivity	2nd Comm Port	3rd Comm Port
IC550	–	–	Yes	–	Yes	–	–
IC1000 (old)	Yes	Yes	Option	–	–	–	–
IC1000	–	Yes	Option	–	–	–	–
IC2000	Yes	Yes	–	Option	–	Option	–
IC4000	Yes	Yes	–	Option	–	Option	–
IC2001	Yes	Yes	Option	Option	–	Option	–
IC4001	Yes	Yes	Option	Option	–	Option	–
IC1604	–	Yes	–	Option	–	Option	–
IC500/NX <sup>5</sup>	Yes	Yes	Option	–	–	–	–
IC1000/NX <sup>6</sup>	Yes	Yes	Option	–	–	–	–

<sup>1</sup>GuardPoint10 Entry version only

<sup>2</sup>GuardPoint10 Entry version Only

<sup>3</sup>Not supported in GuardPoint10 Entry version

<sup>4</sup>Not supported in GuardPoint10 Entry version

<sup>5</sup>GuardPoint10 Entry version only

<sup>6</sup>GuardPoint10 Entry version Only

	RS232 Connectivity	RS485 Connectivity	TCP/IP on board	TCP/IP on extension board	PoE Connectivity	2nd Comm Port	3rd Comm Port
IC500 <sup>1</sup>	Yes	Yes	Option	–	–	–	–
IC1000 <sup>2</sup>	Yes	Yes	Option	–	–	–	–

---

<sup>1</sup>Not supported in GuardPoint10 Entry version

<sup>2</sup>Not supported in GuardPoint10 Entry version

# Controller ROM Versions Table for Different Door/Reader Configurations

Controller ROM Versions Table

Controller Type	Readers	Doors	ROM Version	Badge Capacity
IC2000	4	2	5041	8704
			5042	20480
			5043	4352
			5044	6400
			5045	2048
			5046	5120
			5047	10240
			5048	32512
			5049	44544
IC4000	4	4	6041	8704
			6042	20480
			6043	4352
			6044	6400
			6045	2048
			6046	5120
			6047	10240
			6048	32512
IC1000	2	2	7041	8704
			7043	4352
			7044	6400
			7045	2048
			7046	5120



**Note:** If a controller has reached its badge code capacity during a download process, the download will discontinue and no additional badge codes will be saved on the controller.

To resolve the capacity issue, delete badge codes that are not in use and currently saved on the controller to make room for additional badge codes. Alternatively, consult your provider about changing the ROM in the controller.

# Convention for Reader Transaction Codes

Table D-5 Convention for Reader Transaction Codes

Code	Description
0	<b>Entrance:</b> This is a 'Clock ON' for normal Time & Attendance. The name can be edited, but this transaction code should not be deleted.
1	<b>Exit:</b> This is a 'Clock OFF' for normal Time & Attendance. The name can be edited, but this transaction code should not be deleted.
Other	<b>(Transaction Codes 2-19, 30-97):</b> May be allocated to designate Clocking ON or Clocking OFF for any specific working-time or non-working time activity. Any 'Clock ON' transaction at a reader with a different transaction code (i.e. belonging to a new Category) will automatically end the clocking for the previous category. Therefore, while separate readers may be configured to record specific 'Clock OFF' transactions from designated work categories, in general, this is not required.
20 - 29	Reserved for Access Control use: These should NOT be selected –where these transaction codes are used, the system will automatically assign values.
98, 99	Transaction codes with special meanings, such as <b>Supervisor transaction.</b>



# Controller Support for Readers, Inputs, and Outputs

Reader Table Parameters

Controller Type	Door	Readers	Inputs on Board	Inputs on ext. Board	Relays on Board	Relays on ext. Board	Relays on Satellite
IC2000	2	4 (includes 2 slaves)	8	8	4	12	48
IC4000	4	4	8	8	4	12	48
IC1000	2	2	4	-	3	-	-
IC1604	-	-	16	8	4	12	48
IC2001	2	4 (includes 2 slaves)	8	8	4	12	48
IC4001	4	4	8	8	4	12	48
IC550	1	2	4	-	2	-	-
IC500 NX <sup>1</sup>	1	2	4	-	3	-	-
IC1000 NX <sup>2</sup>	2	2	4	-	3	-	-
IC500 <sup>3</sup>	1	2	4	-	3	-	-
IC1000 <sup>4</sup>	2	2	4	-	3	-	-

<sup>1</sup>GuardPoint10 Entry version only

<sup>2</sup>GuardPoint10 Entry version Only

<sup>3</sup>Not supported in GuardPoint10 Entry version

<sup>4</sup>Not supported in GuardPoint10 Entry version

# Default Connections for Inputs, Relays, and RTX

When a new controller is created, it automatically allocates some of its inputs and outputs to a regular door configuration:

- » A relay for the door open mechanism,
- » An input for the door contact (which detects the door's physical status, open or closed, and may raise an alarm)
- » An input for the Request to exit (RTX) switch.

The following table shows the default parameters. If required, these can be changed by an operator in the relevant setup screens.

Reader Table Parameters

	Readers 1	Readers 2	Readers 3	Readers 4
Door alarm	i1	i2	i5	i6
Door relay	r1	r2	r3	r4
RTX (Request to Exit)	i3	i4	i7	i8

# INDEX

## A

### Access

temporary access 140, 168,  
212, 216, 227, 613, 625

Access Group 55, 57, 64, 87, 141,  
145, 148, 154, 157, 160, 163,  
166, 174, 181, 197, 201, 211-  
212, 219, 227, 230, 232, 363,  
412, 444, 455, 488, 513, 586,  
600, 609, 629-630, 661

Multiple Access Group 142,  
146, 149

### Active Alarms

map page 263, 279-281, 284,  
287-288, 390-391, 395,  
399, 624, 680

map tree 263, 279-281, 284,  
288, 390-391, 395, 554,  
680

### Alarm Zone

Weekly Program 663

### Alarm Zone Security

screen 662, 664

### Anti-passback

APB 80, 466

## B

Badge 64, 182-183, 185-186, 189-  
190, 196, 202, 205, 208, 221,  
223, 293-295, 300, 355, 416,  
420, 426, 432, 456, 474, 537,  
564, 586, 600, 607, 622, 635,  
709

code 64, 198, 202, 222, 600,  
609

owner 599

status 599

### Badge code

decimal 178, 180, 191, 599

hexadecimal 64, 456

Badgecode 143, 150, 463, 475, 501, 503, 505, 588, 615, 623, 663, 719  
 hexadecimal 178, 180, 191, 599

Biometric 62, 214, 453, 459, 474, 586, 590, 616

**C**

Card 3, 63, 354, 397, 456, 687, 690, 705

Cardholder 103-104, 106, 168, 182-183, 186, 189, 191, 194, 196, 199, 201, 203, 205, 208, 211-212, 214, 216, 219, 221, 223, 227, 233, 253, 338, 345, 347, 353, 355, 358, 361, 402, 421, 461, 536, 568, 598, 607, 624, 630, 635, 657, 660, 670  
 details 199, 216, 607, 625  
 Personal Weekly Program 355, 611, 635  
 PIN code 610  
 supervisor 466, 615, 697, 710

Controller  
 details 450, 570  
 script 452

**D**

Departments 201, 229, 232, 234-235, 625, 630

**E**

Event Tracking  
 alarms & access denide events 663

Events  
 screen 353-354, 657

**G**

Galaxy 82-83, 281, 305, 307-308, 310, 370-371, 445, 494, 496, 499, 521, 547, 555, 583, 595, 620, 626, 632, 638, 663

**H**

Holidays 113-114, 120, 130-131, 134, 136,

**I**

Input  
 details 476  
 table 480, 587

**L**

Local Reflex  
 details 490  
 table 492

**M**

Multiple Access Group 55, 87, 140, 146, 154, 157, 160, 163, 166, 174, 181, 197, 201, 211-212, 219, 227, 230, 232, 363, 412, 444, 459, 507, 513, 586, 600, 609, 629-630, 661  
 Access Group 516

**N**

Network  
 details 445

**O**

Operator 104-106, 110-111, 334, 366, 564, 607, 625

Options  
 Event Log tab 572  
 General tab 568  
 screen 567

**P**

Position  
 map group 560  
 screen 554

## Profile

authorizations 11, 33, 91, 93-94, 97, 103-105, 111, 139, 166, 193-194, 465, 518, 602, 620, 627, 652

## R

### Reader

details 170, 453

table 474, 527, 711-712

### Relay

details 485

### Relays

table 488, 594

## S

Setup Wizard 33, 38, 40, 440, 624

Site Details 443

## T

### Time Zone

Daily Program 501

Holidays & Special Days 505

Weekly Program 503

## V

### VPlus Security

Alarm log 379, 388

Alarm tab 667

Logic tree 244-245, 519, 668

Tile management 377, 668

video 243, 247, 373-374, 377, 379-380, 383, 385, 387-388, 520, 667, 703, 719


video panel 374, 377, 381, 383, 385, 667

virtual remote 376, 381, 383, 385, 388, 668, 723

**This page intentionally left blank to ensure new chapters start on right  
(odd number) pages.**

# FAQ

## **An icon at the top of my screen is flashing red; what's wrong and how do I fix it?**

When there is an active alarm, an exclamation point in a red circle flashed on the dashboard . The number of alarms that require confirmation appears to the right of the icon. In parentheses following the number of alarms is the number of active alarms that have been acknowledged (a precursor to a confirm operation).

To confirm an active alarm:

1. Click the flashing icon on the dashboard. The Unconfirmed Alarms dialog is displayed.
2. Right-click on a row and select an action (Acknowledge or Confirm) from the context menu, depending on the Status of the alarm.

Usually, an alarm has to be acknowledged before it can be confirmed. However, you can click the Confirm All action text above the table to confirm

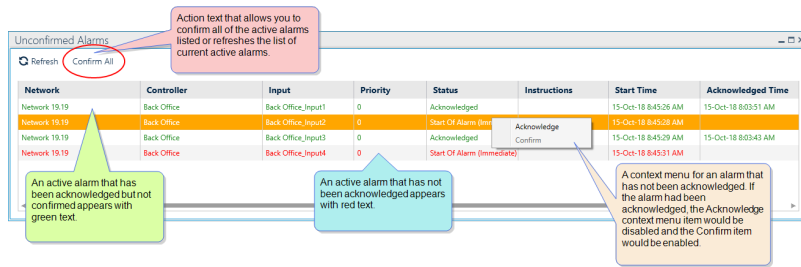


Setup

Management

Security

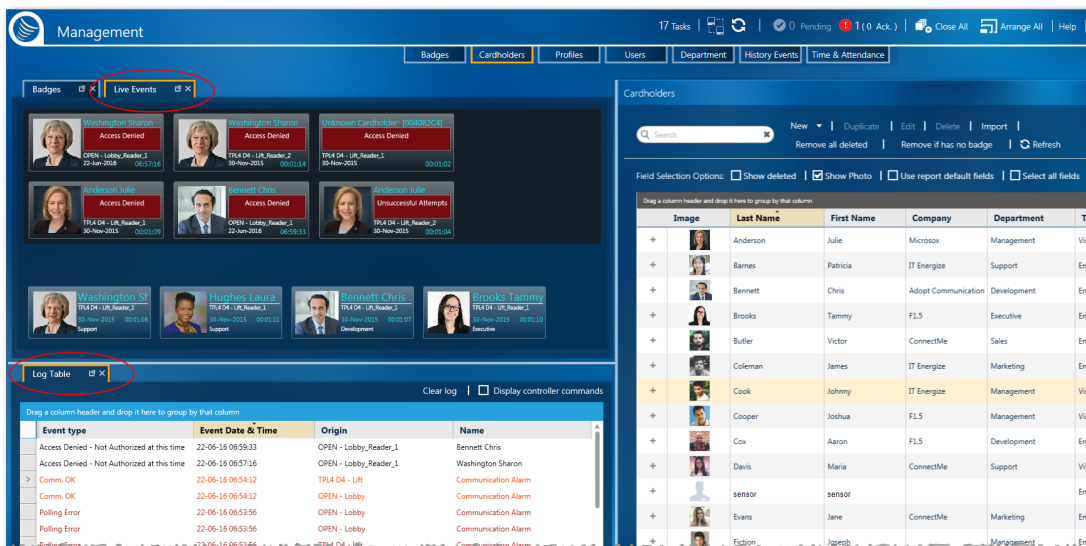
all listed active alarms, regardless of their status.



## Why does the Event Log Table appear at the bottom of console?

The Event Log Table is coupled with the Events screen. The Log table appears in a separate tile at the bottom of the console because you have opened the Events screen, which will automatically be appended to the initial tab stack.

The Log Table can be moved to another sidebar tile; popped-out, appended to an existing tab stack, or deleted at any time. For more information about changing the Log Table view, see "[Getting familiar with the GuardPoint10 console](#)" on page 28.



## There are modules discussed in the documentation, but I can't find them in my GuardPoint10 installation.

Perhaps you do not have the required modules in your license agreement. Contact your GuardPoint10 vendor for information about acquiring the modules.

### Where is the Graphics module?

The Graphic Module includes the Setup Task group's Position screen and the Security Task group's Security Center screen.

- » The Position screen allows you to compose a Security Center environment.
- » The Security Center screen allows you to monitor alarms in a floorplan or map environment, where alarm types and locations can be easily determined.

### Where is the Video module?

The Video Module includes the Setup Task group's Video Setup screen and the Security Task group's



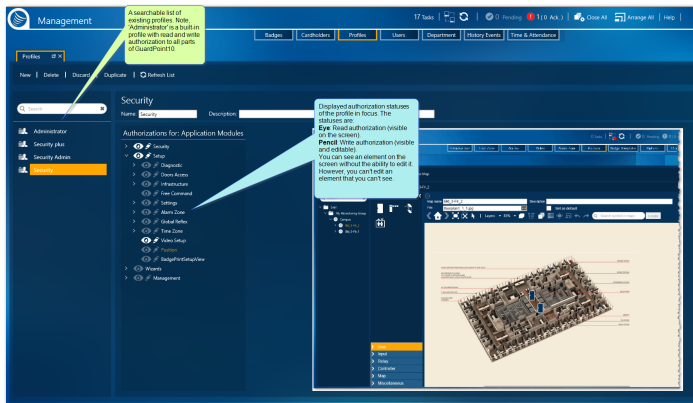
Video Security screen.

- » The Video Setup screen allows you to integrate and structure your NVR or DVR video system into your GuardPoint10 system.
- » The Video Security screen allows you to monitor events and video footage where video cameras have been integrated into your GuardPoint10 system.

### Why can't I edit data on some screens?

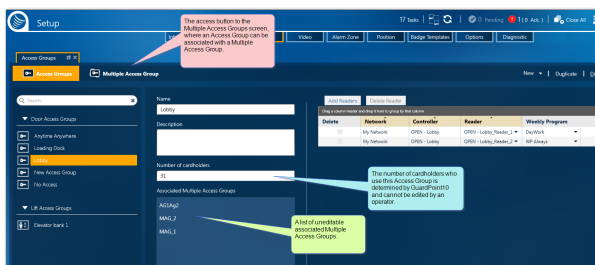
There are three possible reasons why data may be uneditable:

- » Some data requires authorization to edit it. Authorizations are determined by an operator's assigned profile. A profile is created and configured in the Profiles screen.



Preceding each module listed are two icons  . If the eye icon is dulled, the module cannot be seen. If the pencil icon is dulled, the module cannot be edited.

- » Some data is set in a different GuardPoint10 screens. For example, in the Access Groups screen, the list of associated Multiple Access Groups is not editable and can only be changed from the Multiple Access Groups screen.



- » GuardPoint10 automatically sets some data. For example, the number of cardholders who use a selected Access Group (see the image above) is determined by an internal system calculation.

### In the Time Zones screen, what's the difference between a Holiday and a Special day?

In terms of functionality, there is no difference between a Holiday and a Special day. They are date-specific exceptions to the green and white periods set for the day of the week when the Holiday/Special day falls out.

A Holiday column always appears at the end of a WP's weekly calendar.

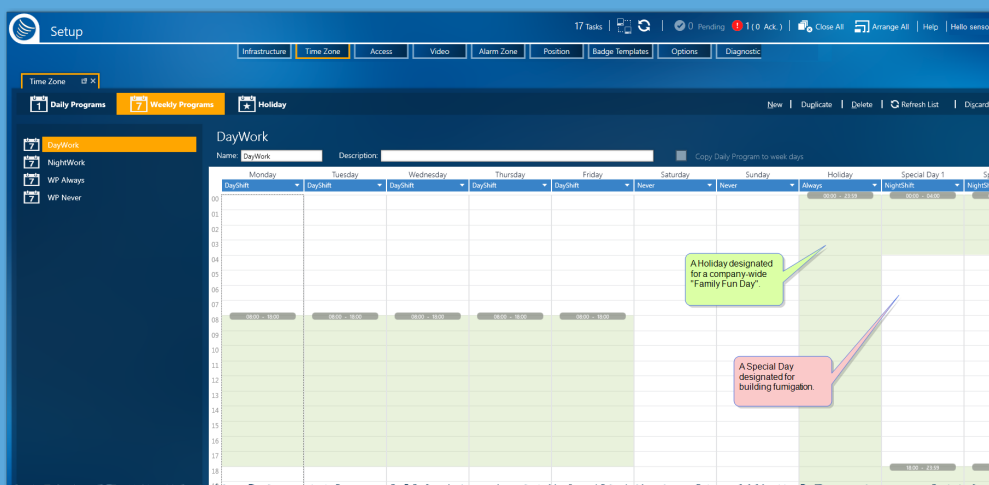
If the Options' General Definitions tab item **Use Special Days** is set to **YES**, two Special day columns appear after the Holiday column in a WP.

A Holiday and the Special days are assigned to a date in a yearly calendar and a Daily Program where green and white periods are defined (like any other day of the week in the weekly calendar displayed on the screen).

## An example where you may use a Holiday entry and a Special day entry in the same WP is as follows:

One day a year your building is closed for fumigation; no employees will be allowed to enter. To recode this entry, you would select a WP used by all employees and configure a Special day with the Never Daily Program.

In addition, your company has an annual "Family Fun Day" the first Monday in August where all employees and their families are invited out to a company-sponsored event; the building is closed from 13:00 until 24:00. To recode this entry, you would select the same WP used for the fumigation day and configure the Holiday column with a relevant half day Daily Program (a green period from 00:00 to 13:00).



## In the Time Zones screen, why can't I edit or delete some of my Weekly Programs (WP)?

The **WP Always** and **WP Never** weekly programs are built-in to GuardPoint10 and cannot be edited or deleted.

## What's the difference between deleting a badge and removing a badge?

### Deleted badges:

When you delete a badge, you are suspending it. The badge still exists in the database, but it cannot be assigned to a cardholder.

If a badge's status is anything other than **In Use**, it can be deleted.

A deleted badge can be undeleted at any time.

### Removed Badges:

When you remove a badge, you are erasing it from the database. It cannot be un-removed at a later time.

Badges are removed in batches. A batch can be qualified into two groups:

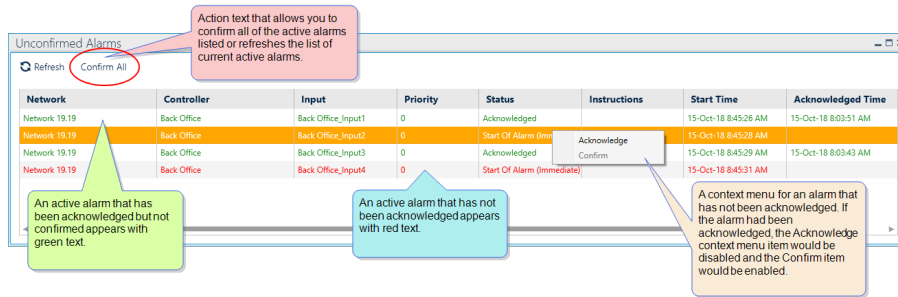
- » Remove deleted badges
- » Remove unallocated badges (not **In Use**)

To reintroduce a removed badge to the system, you would have to recreate it as a new badge.

### Why can't I confirm an active alarm?

To confirm an individual alarm, you would first have to acknowledge it. However, there is a shortcut, where you can confirm all active alarms in a single operation. The batch confirm operation bypasses the acknowledgment step.

The acknowledge operation and the confirm operation, as well as the confirm shortcut operation can be performed via the Unconfirmed Alarms dialog.



### Do I need Excel installed on my PC to generate an Excel report?

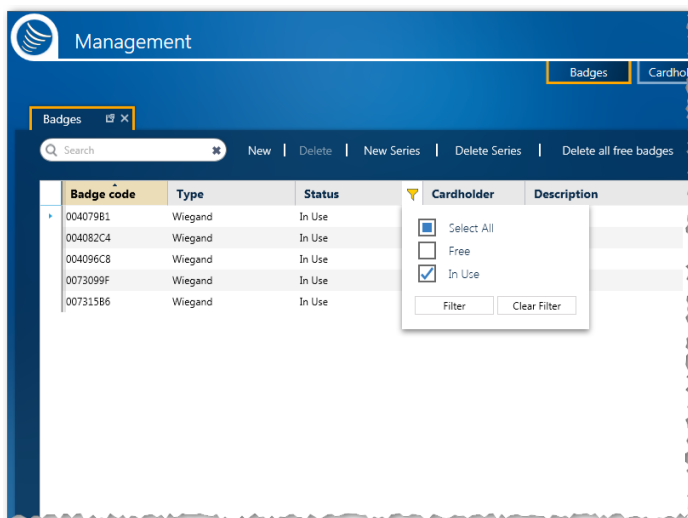
No. You do not need excel to generate an excel report. After you generate a report in an Excel format, you can open it in any application that supports an XLS or XLSX file types.

### In the Cardholders screen, why can't I see all of the cardholder images?

A cardholder's photo is not required by the GuardPoint10 system. If a cardholder does not have a photo in the system, an avatar is used as a placeholder.

### How do I clear a Column Filter in a table?

If a Column Filter is applied to a column, a yellow funnel icon appears in the column heading. Click the funnel to open a filter rollout where filter options are available. At the bottom of the rollout is a **Clear Filter** button. Click the button to remove the filter for that column.



### **Where can I get the template to import cardholder data?**

The import template is a special Excel file included in a standard GuardPoint10 installation. The template file is called hr1.xls, and in a standard installation, it can be found at:

...\GuardPoint10\FormatFiles\hr1.xls

The template can be populated manually or automatically via a mapping mechanism via a third-party application.

### **Is there a limit to the number of cardholders and badges I can add to the system?**

The number of cardholders and badges that may be added to your system database is limited by your GuardPoint10 license agreement and the capacity of a controller's ROM, where cardholder and badge information is saved in a local database.

If you want to increase the number of cardholders and badges allowed in your system, contact your GuardPoint10 vendor.

### **How do I assign an Access Group to a cardholder?**

An Access Group is used to determine which badge codes are stored in a controller. There are two variations of Access Group:

- » A Door Access Group is usually applied to access point (i.e. doors).
- » A Lift Access Group is applied to the button panel in a lift. This allows the cardholder press only those floor buttons where they have been given access authorization.

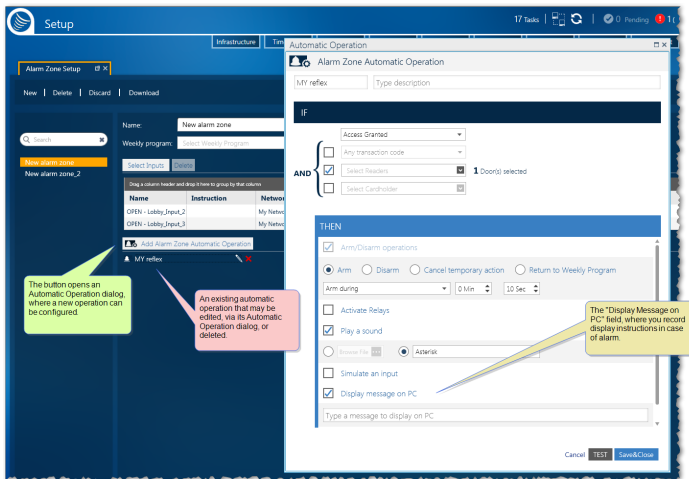
There are three methods you can use to assign an Access Groups:

- » Through a Multiple Access Group container that can hold one or more Access Groups.
- » Through a direct Access Group assignment (Personal Door Access Group and/or Personal Lift Access Group) where one or more Access Groups can be assigned to a cardholder without the need of a Multiple Access Group.
- » **Combine** the two assignment methods.

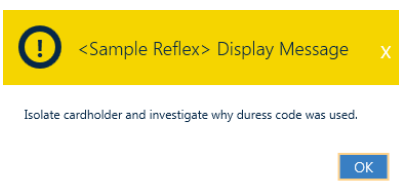
To determine the best method, evaluate the environment where the system will be used. For example, in an office where all of the cardholders in a department would generally have access authorization to the same spaces, you would assign a Multiple Access Group. In a school environment where very few students would have the same class schedule, you would assign Access Groups directly for each student.

### **Can I display instructions in case of alarm?**

Yes. Instructions for a trigger are created in the trigger's Alarm Zone, via an Alarm Zone Automatic Operation dialog.




When the alarm in the Alarm Zone is triggered, the instruction will appear in the form of a message dialog on an operator's screen.



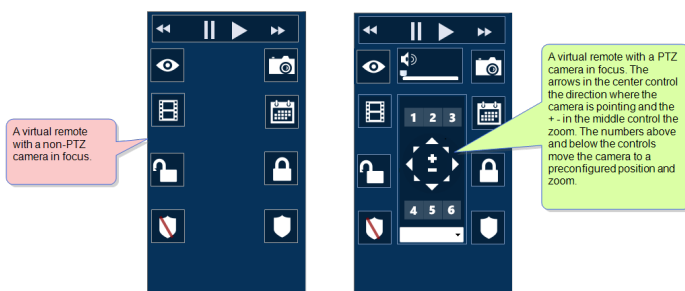
### Can I share my Video layout with other operators and across other GuardPoint10 installations?

Yes. A Video layout zone can be saved as an XML file via the  icon.

Any operator who can access and edit the Video Security screen can load a copy of the XML layout file via the  icon. After a layout file is loaded, the Video Security screen will display according to the instructions in the layout file.

### In the Video Security screen, why can I move some cameras with the virtual remote, but not others?

The ability to change a camera's Pan Tilt and Zoom (PTZ) depends on the NVR/DVR installed at your site and the camera design. If a camera is PTZ enabled and your NVR/DVR recognizes it as a PTZ camera, the virtual remote will display the tools necessary to manipulate a selected camera's view.



### Why is my GuardPoint10 installation running slow?

This can be caused by your antivirus software. To resolve this issue, add the following applications to your antivirus' exceptions list:

- » C:\Program Files (x86)\GuardPoint10\Gui\ACS.Client.GUI.Shell.exe
- » C:\Program Files (x86)\GuardPoint10\AcsServer\ACS.WService.exe

If your GuardPoint10 installation is a Client Only installation, only add the C:\Program Files (x86)\GuardPoint10\Gui\ACS.Client.GUI.Shell.exe application to your antivirus' exceptions list.