



Forcefield Operators Manual

Copyright	© 2012 UTC Fire & Security. All rights reserved.
Trademarks and patents	<p>The Forcefield name and logo are trademarks of UTC Fire & Security.</p> <p>GE and the GE monogram are trademarks of the General Electric Company and are under license to UTC Fire & Security, 9 Farm Springs Road, Farmington, CT 06034-4065, USA.</p> <p>Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.</p>
Manufacturer	Interlogix (a division of UTC Fire & Security Australia Pty Ltd) Level 1, 271–273 Wellington Road, Mulgrave, VIC, 3170, Australia
ACMA compliance	 N4131
Contact information	For contact information, see www.interlogix.com.au .

Content

Important information iv

Chapter 1 Introduction 1

Audience 2
Scope of this manual 2
Related documents 2

Chapter 2 Forcefield overview 3

Key Forcefield concepts 4
What's new in this release 14

Chapter 3 Operator interface 15

Main screen 16
Forcefield title bar 17
Screen icons 17
Forcefield Speed Bar 18
Command shortcuts 19
Main menu 21
Navigating Forcefield 22

Chapter 4 Forcefield tasks 39

Overview 40
Operator-related tasks 42
User-related tasks 44
Alarm-related tasks 58
History file-related tasks 62
Challenger-related tasks 63
Holiday-related tasks 69
Timezone-related tasks 71

Chapter 5 Forcefield commands 75

Introduction 77
Main menu 77
Triggering menu 77
Backups menu 85
Graphics menu 94
Guard Tour menu 106
Control menu 109
Control > Alarm Panel 111
Control > Intercoms 115
Control > Video 116
History menu 120
History > Show DVR Footage menu 125
Users menu 129

- Users > Access menu 140
- Users > Modify Status menu 146
- Users > Profiles menu 146
- Users > Reports menu 152
- Users > Smart Card Programmer menu 160
- Users > Transfer User Data menu 161
- Users > User Numbering menu 162
- Operators menu 163
- Databases menu 166
- Databases > Computer Equipment menu 167
- Databases > Computer Equipment > Storage menu 179
- Databases > Duress menu 182
- Databases > Intercoms menu 184
- Databases > Management Software menu 187
- Databases > Management Software > Clusters menu 187
- Databases > Management Software > Computer Categories menu 188
- Databases > Management Software > Members menu 192
- Databases > Management Software > System Events menu 194
- Databases > Third Party menu 195
- Databases > Timezones menu 199
- Databases > Video menu 200
- Databases > Video > DVR Video menu 201
- Databases > Video > Matrix Video menu 206
- Status menu 210
- Status > Alarm Panel Status menu 210
- Status > Door Status menu 211
- Status > Equipment Status menu 213
- Status > System Status menu 214
- Challenger menu 216
- Challenger > Download Challenger Data menu 221
- Admin menu 223
- Admin > Configuration menu 226
- Admin > Data Mirroring menu 246
- Admin > Tools menu 249

Appendix A Challenger programming 253

- Introduction 255
- Inputs 256
- Areas 259
- Arming Stations 260
- DGPs 263
- Alarm Groups 268
- Timers 269
- System Options 270
- Auto Reset 273

Communication Options	273
Text Words	277
Printer Options	277
Event Flags	278
Timezones	278
Doors & Lifts	279
User Category Data	287
Relays	288
Auto Access – Secure	289
Areas Assigned to Vaults	290
Floors	290
Holidays	290
Input Shunts	291
Time Zones to Follow Relays	292
Regions	293
Cameras	293
Custom RAS Display	294
Battery Test	294
Maintenance	294
Security Password	295
Macro Logic	295
Panel Condition Events	296
Floor Groups	297
Door Groups	297
Radio Options	297
Ethernet Configuration	298
Panel Link (V9 only)	299

Appendix B Using offsite redundancy 303

Overview	304
Setting up offsite redundancy	304
Recovering from failover	305

Appendix C Forcefield 6 menu reference 307

Main menu	308
-----------	-----

Glossary 317

Index 325

Important information

This is the Forcefield Security Management System Operators Manual. This document includes an overview of the product and detailed instructions explaining:

- How to program the Forcefield system
- How to use Forcefield to control a Challenger security system
- How to maintain the Forcefield system

There is also information describing how to contact technical support if you have questions or concerns.

To use this document effectively, you should have the following minimum qualifications:

- A basic knowledge of security systems
- A basic knowledge of security system management software such as Forcefield

Note: Some of the tasks and programming options described in this manual are to be used only by Forcefield technicians who have been trained and assessed in relevant integration and programming.

Read these instructions and all ancillary documentation entirely before installing or operating this product. The most current versions of this and related documentation may be found on our website at www.interlogix.com.au.

Command convention

Forcefield provides both graphical and keyboard options for operating the system:

- Graphical operation means that you use a pointing device such as a mouse or touch-screen to select and execute commands.
- Keyboard operation means that you use a keyboard to select and execute commands

Note: 100% graphical operation requires operators to log in using the Forcefield software keyboard (see Figure 9 on page 23) or by using a proximity card (Tecom 27-bit or Wiegand 26-bit).

Graphical commands include clicking on the Forcefield Speed Bar buttons, tool bar buttons, or additional buttons that may be provided on various forms. For example, see Figure 19 on page 33 for a screen that has both tool bar buttons and additional buttons. Notice that many of the buttons have labels that list the relevant keyboard shortcuts that apply when the window has focus. For example:

- The Close button is labelled 'ESC' to indicate that pressing the ESC key on the keyboard provides the same action as clicking the Close button with the mouse.

- The Text Resp (text response) button is labelled 'Text Resp' (with the T underlined) to indicate that pressing the ALT key and the T key on the keyboard simultaneously provides the same action as clicking the Text Resp button with the mouse.

In describing the command menu structure in this document, the symbol > is used to indicate sub-menus. For example, 'Select Users > Access > Generate IUM Data', means the same as 'From the main menu, click Users, click Access, and then click Generate IUM Data'.

This manual uses the classic menu locations of commands. A Forcefield 6 system can use either the Forcefield 6 menu structure or the classic menu structure. See "Configuring login options" on page 229 for details.

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Interlogix (a division of UTC Fire & Security Australia Pty Ltd) be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Interlogix shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Interlogix has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Interlogix assumes no responsibility for errors or omissions.

Chapter 1

Introduction

Summary

This is the *Forcefield Security Management System Operators Manual*. This document includes an overview of the product and detailed instructions explaining:

- How to program the Forcefield system
- How to use Forcefield to control a Challenger security system
- How to maintain the Forcefield system

Content

Audience 2

Scope of this manual 2

Related documents 2

Audience

This manual is for use by trained Forcefield installation technicians and operators. It provides the following information:

- Introduction to key Forcefield concepts, see Chapter 2 “Forcefield overview” on page 3.
- Using the Forcefield operator interface, see Chapter 3 “Operator interface” on page 15.
- Descriptions of tasks typically performed by Forcefield operators, see Chapter 4 “Forcefield tasks” on page 39.
- Forcefield command reference, see Chapter 5 “Forcefield commands” on page 75.
- Challenger programming reference, see Appendix A “Challenger programming” on page 253.

Scope of this manual

This manual is a supplement to the Forcefield online help and is intended only as an offline reference and a guide to using Forcefield.

It is not an exhaustive guide to every field on every screen that exists within Forcefield (most fields have context-sensitive online help).

Related documents

Refer to the *Forcefield Installation and Setup Manual* for setting up the Forcefield server computer and installing Forcefield client on Windows computers. It includes Installer reference sections, and is for use by trained Forcefield installation technicians.

Refer to the *Forcefield External Interfaces Manual* for reference material for setting up external interfaces such as CCTV, duress, intercom, paging, email, Smart Card Programmer, Card Layout Editor, and photo ID. It is for use by trained Forcefield integration technicians and Forcefield operators.

Refer to the *Challenger V8 & V9 Programming Manual* for details about Challenger programming.

Refer to the *TS0099 Enhanced Challenger TCP/IP Interface Installation and Programming Guide* for details about setting up IP communications with a Challenger panel.

Chapter 2

Forcefield overview

Summary

Forcefield uses a number of key concepts to manage Challenger data and to enable operators to work as efficiently as possible. This chapter describes key Forcefield concepts and features added in this release.

Content

Key Forcefield concepts 4
What's new in this release 14

Key Forcefield concepts

What is Forcefield?

Forcefield is multi-operator, multi-tasking, network-enabled software designed to control Challenger panels and other high-level interfaces such as CCTV switchers, intercom systems, and more.

The Forcefield operator interface is provided via the Forcefield Client application running on Microsoft Windows computers, connected to Forcefield nodes via LAN/WAN or dial-up. Forcefield Enterprise may also have an operator interface connected directly to a node.

Up to 1,000,000 user records (with customised database fields) can be programmed in the Forcefield system, while thousands of Forcefield operators can be supported with defined levels of menu access.

Depending on version, add-on license modules provide enhanced functionality such as:

- Multi-node capability (Forcefield standard edition requires a multi-node license)
- Offsite redundancy capability (requires both a multi-node license, if applicable, and offsite redundancy license)

This manual refers to the Forcefield server as a node, except where server functionality is being described.

Nodes and workstations

Forcefield standard edition

Standard hardware (Figure 1 on page 5) is used for the primary controlling node (and optionally the backup controlling node). The user interface is provided via the Forcefield Client application on Windows computers.

Forcefield Enterprise edition

Rack-mount workstation hardware (Figure 1 on page 5) is used for the primary controlling node (and optionally the backup controlling node). Non-controlling nodes can use either standard or Enterprise hardware. Enterprise hardware can connect with more Challenger panels than standard hardware. The user interface is provided via the Forcefield Client application on Windows computers.

Figure 1: Forcefield hardware examples (images may not match actual product)



Standard hardware



Enterprise rack-mount hardware

The Forcefield server application runs on computers (nodes) using the QNX operating system. Subject to licensing, a Forcefield primary controlling node or non-controlling node can connect with the following:

- Challenger panels via serial RS-232, local area network (LAN), wide area network (WAN), leased line, dial-up modem, etc.
- Forcefield clients via LAN/WAN or via dial-up
- CCTV switchers, Digital Video Recorders (DVR), associated CCTV video cameras, and to Teleste Video Surveillance systems
- Intercom systems
- Duress/Paging system
- Serial, parallel, or network printers
- Smart Card Programmer

The Forcefield Client application runs on Microsoft Windows personal computers. Each Forcefield client can:

- Print to Windows system printers.
- Connect with a Smart Card Programmer.
- Operate the Forcefield Client Card Layout Editor, which enables the operator to design user card layouts and to print photo ID cards on a (Windows system) card printer.

Watch house functionality

Forcefield workstations can be used as watch house workstations (or *Pods*), when Forcefield is running in watch house mode.

In watch house mode one workstation is designated as a “night switch workstation”. As operators log onto other watch house workstations, the members handled at each workstation are removed from the members of the night switch workstation. Any workstations not designated as watch house workstations operate in standard mode.

When no operator is logged into a watch house workstation, all the workstation's members are transferred to the night switch workstation. When an operator logs back into a watch house workstation, the workstation's members are transferred back to the workstation. Each watch house workstation operator is assigned all members because members are controlled at the workstation level instead of the operator level.

Refer to “Configuration” on page 226 for details about selecting watch house mode and specifying the master control (night switch) node.

Refer to “Workstations” on page 173 for details about designating specific workstations as watch house workstations.

Challenger programming

Subject to authorisation levels, Forcefield operators can remotely configure Challenger programming options, which eliminate the need to program individual Challenger panels on-site. The complete programming details of every Challenger panel are maintained and backed up on the server in the Forcefield databases.

Managing data integrity

When Forcefield is used to program a Challenger panel, or used to upload a panel's programming, the Forcefield system becomes the *primary* location for the panel's data, and the panel becomes the *secondary* location. It is vital that future programming is done only via Forcefield and not via a remote arming station (RAS), or via other management software connected to the panel.

Programming by any means other than Forcefield may result in a loss of data, errors in data, or uncertainty about the validity of data.

Members and member groups

The Forcefield concept of *member* restricts the operator from viewing records, and controlling and receiving events, that are not within their authority (member group). The Forcefield database can therefore be partitioned into virtual sub-systems. At the same time a privileged operator may be given “all members” for global system control and monitoring.

The terms members and member groups have particular meanings in Forcefield:

- ‘Member’ is the term (that you define) which is used to identify field equipment or user records.
- ‘Member group’ is a group of members, which is then assigned to Forcefield resources such as operators and workstations. One member group is assigned to each operator.

Linking members to Forcefield records

Does the operator assign a member to a user—or assign a user to a member? Which one ‘belongs’ to the other? In fact, it doesn’t matter how you look at it. To take user records as an example, a user record is linked to a member via the member field on the user maintenance screen.

See Figure 2 on page 8 for an example of a User Maintenance window where the user is linked to a member named ‘Building C’.

Using members to organise records

Forcefield records are linked to members in order to filter (restrict) the way the records are used. For example, all the records for a particular Challenger (the Forcefield records for a Challenger and its doors, floors, areas, etc.) can be linked to the member that you’ve named ‘Factory’. In this manner, it’s quick to search for the appropriate Forcefield records if you filter the search by the member name.

User records can also be linked to the ‘Factory’ member, or you can create new members specifically to keep user records together (e.g. a member named ‘Users at 100 High St.’).

Using member groups to assign records to operators

A member group is a group of members. A member group is linked to Forcefield resources such as operators, workstations, printers, etc., in order to determine which members are visible to the resource.

For example, a building located at 100 High St. uses two Challenger panels, where each has its respective Forcefield records linked to members named ‘01 Devices’ and ‘02 Devices’. In addition, all staff working at the location are linked to a member named ‘Users at 100 High St.’.

A member group named ‘100 High St.’ is made up of the members:

- ‘01 Devices’
- ‘02 Devices’
- ‘Users at 100 High St.’

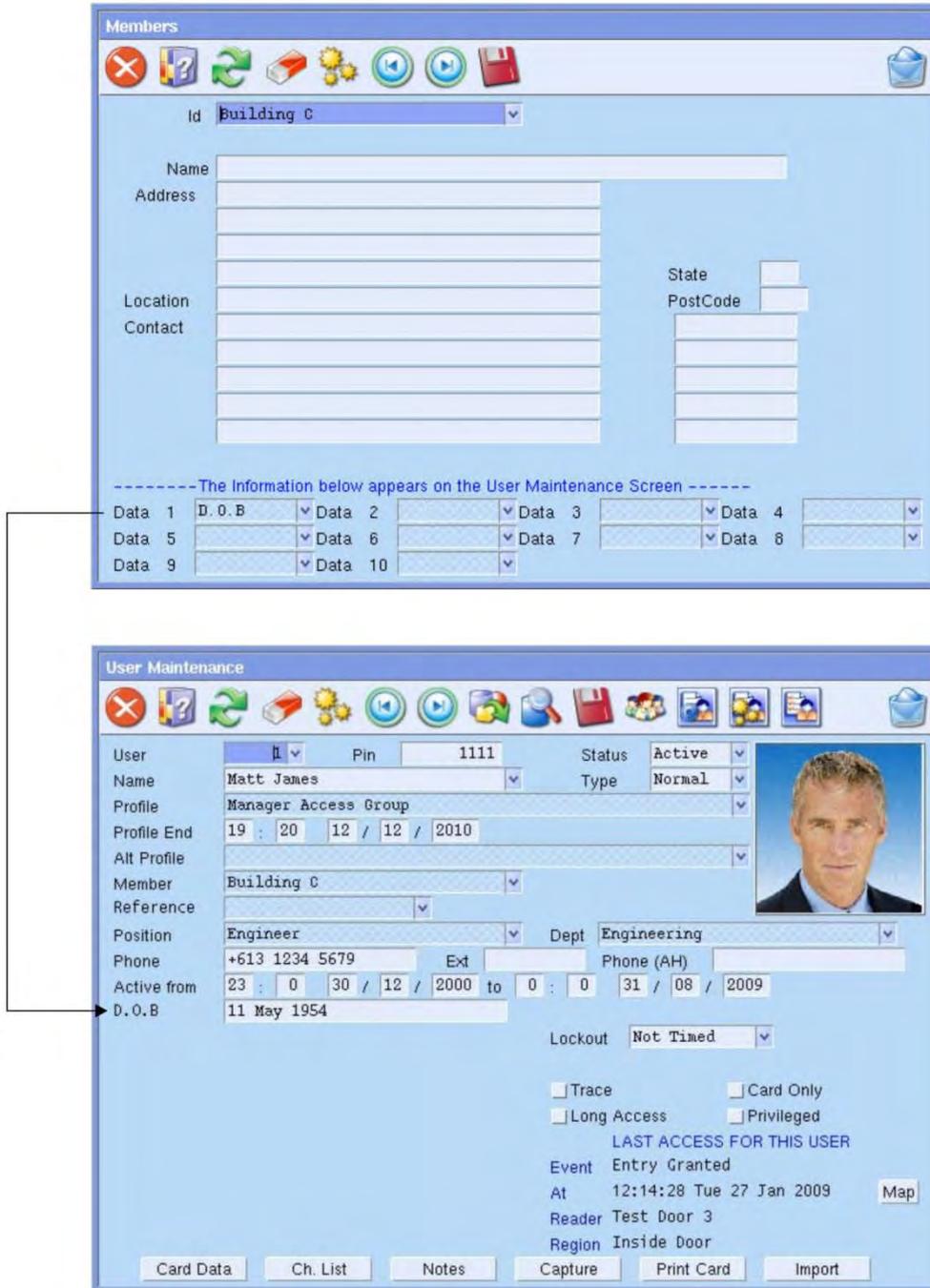
The member group ‘100 High St.’ is linked to a Forcefield operator controlling the building’s security system. This allows the operator to see all the equipment and user records pertaining to the building, without having to deal with unneeded data (Forcefield can hold up to 1,000,000 user records). By restricting the operator to the three members in the operator’s member group, we therefore prevent the operator from accessing all other records in the Forcefield system.

Using member’s extra data fields

Member records have a particular function in regards to user records and user reports. The members screen has ten optional user fields, which, if completed, appear as labels on the User Maintenance form (for users linked to that member name), and are included in User reports.

To see how this information appears in Forcefield, see Figure 2 below for an example of a Members screen where one of ten user data field labels are defined, and then displayed in the respective User Maintenance window.

Figure 2: Members programming window (note populated Data 1 field)



Clusters

Clusters are a means of grouping together field equipment records of the same type, which enables a single operation to affect all the elements in the cluster. For example, a group of doors may be clustered to 'Fire Doors'. The operator may then open all the fire doors in a single operation.

A cluster may be defined for Doors, Inputs, Areas, Relays, Floors, RASs, DGPs, Lifts, or Challenger panels. A device may be connected up to 32 clusters. For example, Door 19 could be in the 'Fire Door' cluster and the 'Front Fire Door' cluster and the 'Office Door' cluster, and so on.

See "Program Clusters" on page 187 for additional details.

User profile

A user profile is a collection of user information such as member, date range, position, department, card type, trace, long access, card only, privileged options, and Challenger access.

Profiles can be defined and used to manage user records in bulk and for a specified time. For example, a profile granting Challenger access to a group of users may be set to expire at a pre-set time and date, after which a specified alternative profile takes effect.

User records may be updated in bulk by making changes to a shared profile and then using the Sync to Profile operation to update the user records to the new user profile data.

See "Program Profile" on page 147 for additional details.

Forcefield Client

The Forcefield graphical interface may be operated from a Microsoft Windows computer via TCP/IP using the Forcefield Client application. Forcefield Client also provides Photo ID (which is not available on nodes (QNX computers)).

Monitoring background processes

Forcefield monitors its background processes. If a background process terminates abnormally, an alarm will be generated to alert the operator.

Offsite redundancy facility

A Forcefield primary controlling node (server) can be configured to use a mirror node. If the primary controlling node fails, then the mirror node becomes active and operates as node 1.

Notes

- All Challenger panels connected to the primary controlling node must be upgraded to firmware version V8-C-MFx.8106 (or later). Failure to upgrade the panel firmware may result in very slow event reporting.
- In cases where the primary and backup controlling nodes are connected to the security system or other high-level interface (HLI) via serial connections, suitable serial port monitoring and switching equipment would be required to cater for the situation where the primary controlling node fails and the backup controlling node takes control. Forcefield will use the equivalent ports on the backup controlling node as on the primary controlling node. Such switching equipment must be provided by the customer.

Incidents

An incident is a series of events that begin with an alarm event and belong to one member.

The use of incidents is optional and configured in “Configuration” on page 226. If used, Forcefield can be configured for incidents to be either automatically generated by Forcefield or manually generated by operators from the alarm screen.

An automatically generated incident is started when an event causes an alarm and there is not already an incident for that member. All events coming in (that belong to the same member as the initiating event) are included in the incident. The incident ends when the operator removes it via the alarm screen.

Forcefield desktop

Refer to “Main screen” on page 16 for images of the Forcefield desktop.

Activity Icons

Activity icons on the Forcefield desktop indicate when reports, backups, Challenger downloads and uploads are active, or automatic processes are scheduled. Refer to “Screen icons” on page 17 for details.

Colours

The colour of the desktop background and the colours of the data entry fields on the various screens are configurable on a workstation basis.

Background

A background image may be displayed on the desktop of the Forcefield server. The image file must be placed in the correct directory using operating system-level tools (there is no Forcefield configuration tool for this purpose).

Tip: Use of this feature may slow screen updates.

System time

The system time can be set by double-clicking the clock display on the alarm line.

Menu

The menu may be hidden, leaving the Forcefield desktop free for applications.

Remote computer connectivity

Forcefield can allow remote computers to access the Forcefield directories on an individual read/write basis using NFS (Network File System) facilities.

Forcefield can connect to external storage devices allowing backups to be written to remote computer systems by using either:

- NFS, or
- CIFS (Common Internet File System)

Data entry screens (forms)

Searchable fields have a down arrow next to the field, clicking this icon performs the same function as the F4 key or right-click.

'Go to' fields are indicated by a crosshatched background when the field is in focus.

Event window

The Forcefield event window is now member aware. It will only display events that are linked to the workstation and/or operator member group.

Door lock override

Door Lock Override allows the operator to specify time periods when a door should be unlocked, together with optional areas that should be disarmed.

Door monitor

A Door Monitor allows selected doors to be monitored and controlled (opened) on a workstation basis.

When a user access event occurs, the event details and user image (if any) will be displayed and user details may be retrieved from the door monitor.

History and database backups

Backups may now be performed across the network to NFS or CIFS mounted directories on remote computers.

Forcefield can be set up to automatically backup databases and history at a set time. History events are generated for backup initiation and successful completion, and Forcefield can be set up to check for these events.

History export

Forcefield history may now be exported as CSV (comma separated value) files. Forcefield can be set up to automatically export history at a set time.

Graphics

- Forcefield supports up to 65,535 maps.
- There are 10 levels of maps allowed for a Live Animation Point (LAP), and a LAP report is available.
- Printers and computers (nodes) can be placed on maps.
- Doors may be represented by the traditional line icon or by a symbol.

Reports

All reports have the Forcefield License Site ID displayed in the report title.

Guard tour

A guard tour is a defined series of checkpoints at which a security guard must check in, within specified time intervals. Failure to check in on time triggers an alarm or other event.

Users

Forcefield can have up to 1,000,000 user records (Challenger limitations still apply). The Forcefield user number is not necessarily the Challenger user number. For example, Forcefield user 3 may be:

- User 5 in Challenger 1
- User 56 in Challenger 123
- User 12345 in Challenger 45, etc.

See “Show Ch. User Number” on page 162 for details.

Photo ID

Photo ID and Card generation facilities are provided by Forcefield client. Refer to the *Forcefield External Interfaces Manual* for details.

User import and export

Manual or automatic import and export of user data is provided. Refer to “Import User Data” on page 162 and to “Export User Data” on page 161.

User profile

See “User profile” on page 9 or “Program Profile” on page 147 for additional details.

User access groups

Challenger Access Groups will only be visible to an operator if every component of that group is in the operator’s or workstation’s member group (e.g. a door group will show only if every door in the group has members accessible to the operator).

Interface to DVR

A Forcefield system may interface via Ethernet (IP) connections to Digital Video Recorders (DVR), associated CCTV video cameras, and to Teleste Video Surveillance systems.

Authorised operators can:

- Access live and recorded video footage from maps.
- Program Forcefield to activate a camera and to record footage in response to events such as an alarm or by someone using a reader.
- Find recorded footage by searching the DVR by text tags or by time (see “History > Show DVR Footage menu” on page 125).
- Display up to 16 images of DVR video on a single screen using multi-view (see “Multiview” on page 203).

Refer to the *Forcefield External Interfaces Manual* for details of integrating a DVR or Teleste system into Forcefield.

Interface to third-party systems

Forcefield can be integrated with third-party devices, so that it can send event data to, and receive messages from, external systems. Third-party integration enables Forcefield to perform actions via the event triggering system.

See “Databases > Third Party menu” on page 195 and *Forcefield External Interfaces Manual* for details.

What’s new in this release

Forcefield 6.4 provides the following new functionality (major changes only):

- Support for Windows 7 64-bit and Windows XP 64-bit.
- Up to eight conditions can be used in trigger logic for event and time triggers.
- Ability to select one or more user fields to show in the Event Monitor (such as a user’s phone number). See “Displaying user details in the Event Monitor” on page 38.
- Integration with TruVision DVRs.
- Full configuration of TruVision video devices (such as adding IP cameras, configuring frame rates, setting up motion detection grids, and so on) all from within Forcefield itself.
- Increased maximum DVR/NVR units from 99 to 999.

Chapter 3

Operator interface

Summary

This chapter describes the Forcefield workspace.

The Forcefield application runs in the QNX operating system on each node. The Forcefield Client application runs in the Windows operating system on standard personal computers and effectively provides a remote user interface to the Forcefield application.

In this manual, Forcefield Client is used for screen examples because Forcefield Client screens are typically identical to Forcefield screens.

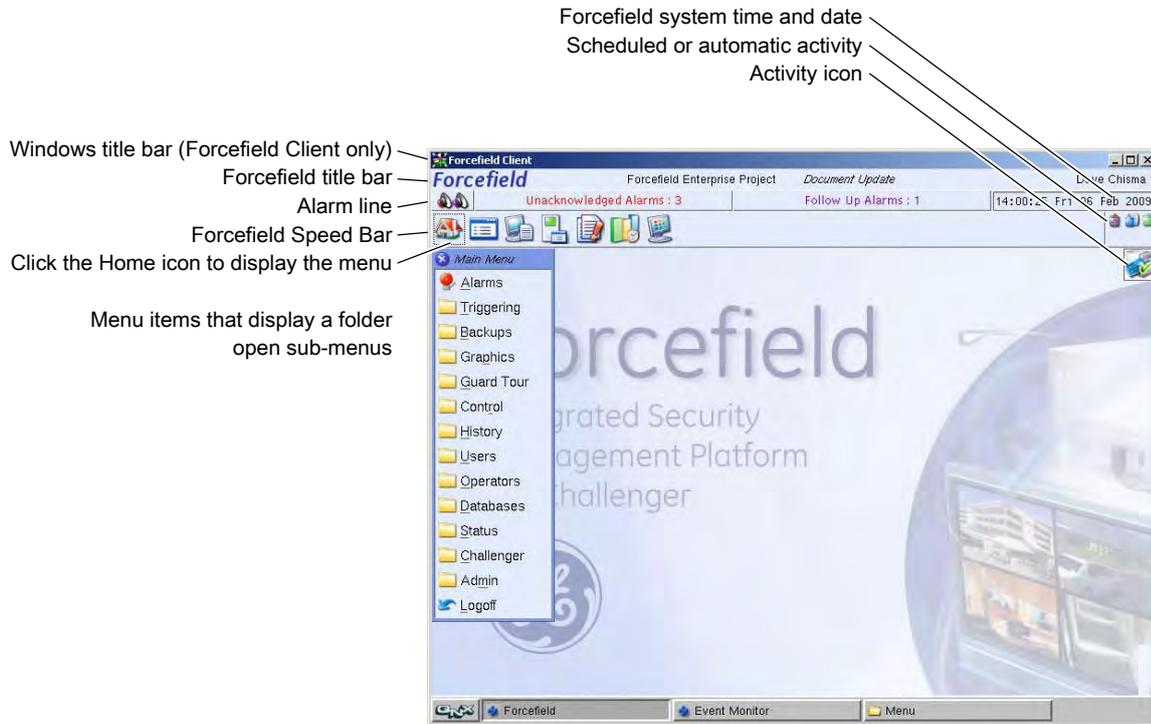
Content

Main screen	16
Forcefield title bar	17
Screen icons	17
Forcefield Speed Bar	18
Command shortcuts	19
Main menu	21
Navigating Forcefield	22

Main screen

After the operator logs in to Forcefield, the main Forcefield screen displays the Speed Bar, shortcuts to alarm screens (when alarms are present), alarm line, date and time, workstation ID, and operator name.

Figure 3: Forcefield main window with default Speed Bar buttons



The Forcefield client may be configured to display alarm priority details in place of the Unacknowledged Alarms and the Follow Up Alarms buttons. See “Using the alarm line priority details” on page 35 for details.

Hold the cursor over a button or an automatic activity indicator to display the name or function (Figure 4 below)

Figure 4: Popup help example



Forcefield title bar

Double-click “Forcefield” in the title bar to open the About box.

Figure 5: Forcefield About box



The About box displays details about the Forcefield software versions and service packs (if applicable) currently installed on the node and the client.

Screen icons

The Forcefield desktop may display animated and still icons to indicate various background processes and scheduled activities.

Activity icons

Activity icons on the Forcefield desktop indicate when reports, backups, Challenger downloads and uploads are active. These allow the operator to easily determine what background tasks are running and the ability to individually terminate those tasks.

The following animated icons display in the Forcefield main window to indicate an activity is running.

Table 1: Activity icons (still images of animated icons)

Screen icon	Background task
	Download (to panel)
	Upload (from panel)
	Backup
	Restore
	Report

Screen icon	Background task
	Process
	A Learn Reader is assigned to this workstation.

Automatic activity icons

The Forcefield main window may display icons to indicate scheduled or automatic activities as shown in Table 2 below.

Table 2: Scheduled activity icons

Screen icon	Scheduled or automatic task
	Auto database backup —pop-up message indicates the scheduled time and destination) of a currently active scheduled backup (see “Auto Database Backup” on page 86).
	Auto history backup —pop-up message indicates the scheduled time, destination, and settings) of a currently active scheduled backup (see “Auto History Backup” on page 87).
	Auto history export —pop-up message indicates the scheduled time, destination, and settings) of a currently active scheduled export (see “Auto History Export” on page 88).
	Auto user import —pop-up message indicates the user data source when Import User Data is set to automatic (see “Import User Data” on page 162).
	Auto user export —pop-up message indicates the user data destination when Export User Data is set to automatic (see “Export User Data” on page 161).

Hold the cursor over an automatic activity icon to display details in a pop-up window.

Forcefield Speed Bar

The configurable Forcefield Speed Bar on the main window can be used to quickly open and close Forcefield screens and to execute commands. The Speed Bar can be configured—images changed, buttons added, and so on.

The functions of the default Forcefield Speed Bar buttons are shown in Figure 6 below.

Figure 6: Default Forcefield Speed Bar



Figure 6 legend

Item	Description
1.	Forcefield Menu, displays the main menu.
2.	Toggle Events Window, displays or hides the Events window
3.	Computer Status, displays the Computer Status/License Information window
4.	Challenger Status Report, displays the Challenger Device Status Report window
5.	Abnormal Status Report, displays the Abnormal Challenger State Report window
6.	History Statistics, displays the History Statistics window
7.	Alarm Map, Displays the Alarm Map window for the highest-priority alarm (the cursor automatically points to the alarm). If there is more than one alarm with the same priority, the map with the oldest alarm displays.

See “Speed Bar Configuration” on page 243 for details about configuring the Forcefield Speed Bar.

Command shortcuts

Keyboard shortcuts and tool bar buttons are provided for most Forcefield commands.

Figure 7: Example of a Forcefield window toolbar

Throughout the operator interface, there are typically several methods by which the operator can execute commands—typically by using the keyboard or by using a pointing device to click a screen element such as a tool bar button.

In addition to these two main methods of operation, there are often further alternatives such as right-click or double-click commands. Table 3 below is a list of keyboard shortcuts and corresponding tool bar buttons.

Table 3: Forcefield Shortcuts (some are window-specific)

Key	Button	Name	Function
Tab	n/a	n/a	Use the Tab key to move the focus forward to different fields or buttons.
Shift+Tab	n/a	n/a	Use the Shift+Tab key combination to move the focus backwards to different fields or buttons.
Ctrl+Tab	n/a	n/a	Use the Ctrl+Tab key combination to move the focus to the first field.
ESC		Close	Close the current window or menu.

Key	Button	Name	Function
ESC		Stop	Stops the current process.
F1		Help	Displays on line help for the selected field.
Shift+F1		Print	Sends the current form to the workstation's default printer. In order to display this button, the workstation must have a default printer assigned and have printing enabled in Workstation Options.
F2		Undo	Restores values to their saved values (not applicable to deleted records).
F3		Make	Creates a new record using the data displayed in the associated field. Alternatively, double-click the field to create the new record.
F4		Search	Used for searching or listing of options. Alternatively, right-click the data field to search.
Shift+F4		Advanced Search	Used for searches on selected screens.
F5		Save	Used for storing the values that have been entered in a field or form.
F5		Select	Selects the displayed record.
F6		Run	Used to start processing the current function.
F8		Delete	Delete a selected record from a Forcefield database or deactivate a timed automatic function (for example, auto-database backup).
F9		Clear	Clears the selected field.
F10	n/a	Default	Sets a selected field to the default value (where applicable)
F11		Clear all	Clears all fields in the current form. Depending on the particular application, the F11 button may populate the fields with default data.
F12		List	Used to list the components and sub-components of a group.
Alt+B		Bulk	Initiates bulk processing of user records.
Alt+C		Cluster	Open the Cluster screen (from screens that either program or control Doors, Inputs, Areas, Relays, Floors, RASs, DGPs, Lifts, or Challenger panels).
Alt+D		Download	Transfers data from Forcefield to a Challenger panel.
Alt+M	n/a	Menu	Opens the main menu. Alternatively, press Enter to open a selected main menu item.
Page Up		Previous	Displays the previous record.

Key	Button	Name	Function
Page Down		Next	Displays the next record.
Ctrl+↑		Scroll Up	Displays the previous page in a list.
Ctrl+↓		Scroll Down	Displays the next page in a list.
n/a		View Last Report	Displays the most recently-run unprinted report by the current operator at this workstation.
n/a		Print Last Report	Prints the most recently-run unprinted report by the current operator at this workstation.
n/a		Go To	'Go to' fields are indicated by a crosshatched background when the field is in focus. Double-click the field (or press F3) to go to the associated form. Alternatively, right-click the data field to search.
n/a		Assign date & time	Automatically populates date and time fields with values from, for example, today, yesterday, etc.
n/a		Issue Card	Click Issue Card on the User Card Data window to open the Issue User Card window.
n/a		Learn Card from Reader	Click Learn Card from Reader on the User Card Data window to enable card data to be read from the system's TS0862RAW card reader or from a designated IUM Learn Reader.
n/a		Set Default	Click Set Default on the User Maintenance window to save the currently-displayed data as a template, or to load a previously-saved template.
n/a		Clear Default	Click Clear Default on the User Maintenance window (in default data mode) to remove the current template.
n/a		Config Form	Click Config Form on the User Maintenance window to open the Maintenance Config window, to specify which fields on the User Maintenance window are to be read-only (not editable). See "Show PIN Code" on page 140 for details.

Background task indicators appear from time to time in the main window. These are described in "Monitoring background processes" on page 9.

Main menu

If the main menu is not displayed, click the Forcefield Menu button to open it (alternatively, use the keyboard shortcut ALT+M).

The top level of the old Forcefield menu structure is displayed in Figure 3 on page 16 and in Figure 74 on page 230.

Applicable to Forcefield 6 and later, the main menu structure is configurable via “Configuring login options” on page 229. The organisation of this manual and all menu images are based on the classic menu structure. Command names are the same regardless of the menu structure, and are contained in the Index for quick reference, regardless of the structure used.

Menu items have underlined characters to indicate hot-key functionality (only when the menu is in focus). For example, press the ALT key and the T key simultaneously to open the triggering menu.

The Forcefield menu is configurable at the operator level, and does not typically display all the menu options.

Navigating Forcefield

This section describes common tasks that Forcefield operators need to be familiar with. The actual tasks that various types of operators and installation technicians will perform will vary depending on the job requirements.

This section describes:

- System startup
- Logging in
- Logging off
- Automatic shutdown
- Initial Forcefield screen
- Data entry and searching
- Generating reports
- Alarm handling process

System startup

When the Forcefield controlling node is started or restarted (and a user interface is connected to the controlling node), a message may appear briefly indicating that the computer’s “boot agent cannot continue”, and then Forcefield starts normally. You may ignore the message.

Logging in

An operator must log in to start a Forcefield session. Depending on the configuration of the Forcefield system, login may be done by entering your operator code or by badging a proximity card using the TS0862RAW interface connected to the Forcefield computer (Refer to the *Forcefield Installation and Setup Manual* for details).

The login access rights of each operator are defined in the Operators > Access menu.

The following procedure describes the use of the Forcefield login screen Figure 8 below.

Figure 8: Login screen



Use the following procedure to log in:

1. Type your operator code and press Enter.
2. Type your Password and press Enter. The password is case-sensitive (for example, the password 'THX1138 is not the same as 'thx1138). The password characters display as * for your security.

A Forcefield workstation may be configured for strictly graphical operation (where a physical keyboard is not provided). Such workstations use the Forcefield software keyboard for login (Figure 9 below) or by using a proximity card (proximity card login is not available for Forcefield clients).

Figure 9: Software keyboard used for login on workstations without a physical keyboard



The use of the software keyboard is defined in “Workstation options—login” on page 174.

Logging off

To log off, select Logoff from the main menu. Alternatively, select Logout from the Alarm map screen if the workstation is defined as a graphical login. Forcefield displays the Login screen for the next operator.

Automatic shutdown

In certain situations, Forcefield automatically shuts down to protect the integrity of the system. In each case, a message is displayed explaining the action that is being taken. Forcefield will automatically shutdown following detection of any of the following conditions:

- The server has less than 2 MB of free RAM.
- The server has less than 2 MB unused space remaining (on any hard disk that is being monitored for space).

Initial Forcefield screen

After logging in, the Forcefield desktop operates in one of two modes:

Menu mode: Click Forcefield MENU on the Speed Bar to display the main menu (the Speed Bar is depicted in Figure 6 on page 18).

Graphic mode: Similar to menu mode except that the Alarm Map window is constantly open (the Logout button replaces the Quit button). In graphic mode, Logoff is not a main menu option.

The login mode for the workstation is defined in “Workstation options—login” on page 174.

Data entry and searching

Data-entry fields in Forcefield enable the operator to quickly search for existing data, or to create new data, if needed. For example see Figure 10 on page 25, the User Profiles window has data entry fields including:

- Position—Linked to User Position data.
- Department—Linked to User Department data.

When either of these fields is active (has focus), the field’s background displays a cross-hatch pattern to indicate the linking to another form.

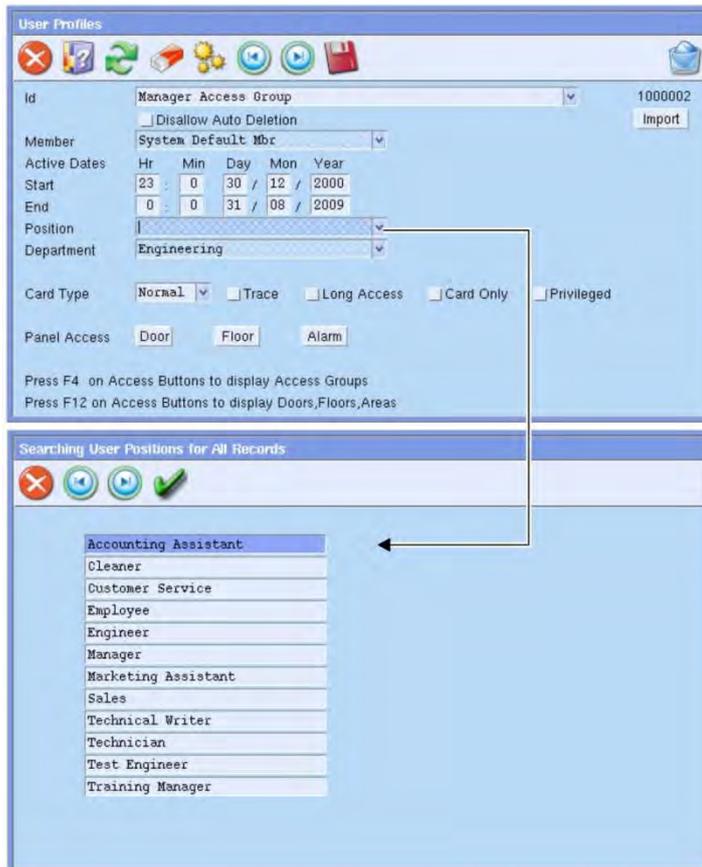
Notice how some of the fields have search arrows. Click the field’s search arrow to select from a list.

Notes

- Search arrows are used extensively in Forcefield to indicate fields that may be completed using existing data. Click the arrow to select from the list.

- When entering dates, it is not necessary to type the entire year. For example, to enter 2009 you only need to type 9 and press Enter. To enter a year before 2000 you must type the entire number.

Figure 10: Typical search operation



Click the search arrow (or press F4) to search for existing data.

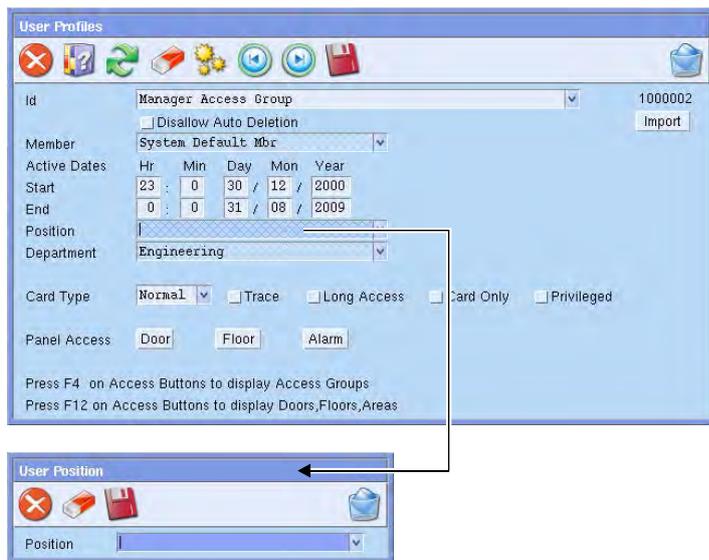
Results of search (all records displayed).

If the letters "TE" were entered before searching, only the records starting with "TE" would be displayed.

If the user position you wish to use does not exist, you have two alternatives after returning to the User Profiles window:

- Type the new user position into the Position field and save the record. The data entered and saved will not be added to the list of user positions.
- Double-click the Position field (or press F3) to go to the User Position window, and then type the new user position into the Position field and save the record. The data entered will be added to the list of user positions so that you can select it next time you need it without retyping.

Figure 11: Typical ‘Go To’ operation



Double-click the field (or press F3) to open the User Position window.

Cross-hatch field backgrounds are used in Forcefield to indicate fields that are linked to other windows. Double-click the field to open the related window.

Narrowing the search

An unfiltered list of options can be very long (Forcefield can hold up to 1,000,000 user records), so Forcefield provides several ways in which to narrow or ‘filter’ a search. These include:

- Using members and/or member groups to limit the data that the operator sees. See “Members and member groups” on page 6 for details.
- Using a text string in a data field before searching. See “Using a text string” below for details.
- Selecting a restricting value before searching. See “Selecting a restricting value” on page 27 for details.

Using a text string

For an example of using a text string, see Figure 10 on page 25 where the Position field is empty prior to searching. The search result contains every existing record. Here’s what would happen if some text were added to the Position field prior to searching:

- Type ‘Te’ or ‘te’ (search strings are not case-sensitive) and then search—the search results would contain only ‘Technical Writer’, ‘Technician’, and ‘Test Engineer’.
- Type ‘tec’ and then search—the search results would contain only ‘Technical Writer’ and ‘Technician’.
- Type ‘m’ and then search—the search results would contain only ‘Manager’ and ‘Marketing Assistant’.

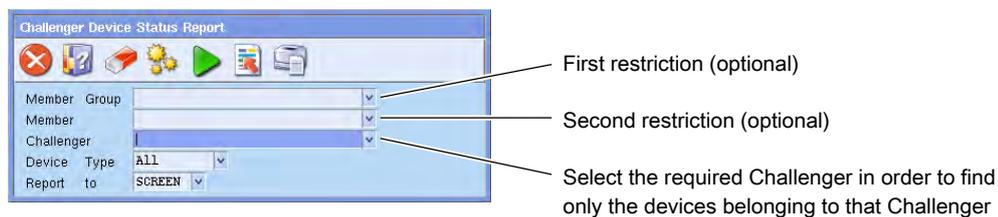
- Type 'b' and then search—Forcefield displays a message indicating that no matching data was found.
- If there is an exact match for the text string, you will see the matching record listed, and you can use the Page Up and Page Down buttons to find other records.
- You can use a pair of % characters to do a wildcard search for any string of text in users' names. For example, type "%JO%" and then press F4, and Forcefield will find all user names where either the first or last names contain JO, such as Jodie Smith or Marie Johnston.

Selecting a restricting value

'Restricting value' means to make a selection that restricts the next selection to a smaller amount of data. For example, if the operator selects a member group, the list of members available for searching will be restricted to the members that are part of the member group.

The use of restricting values to limit the size of the search results list is optional—it is provided to speed the operator's work flow when large numbers of records make it slow to find the correct entry. In the examples shown here, it would be quicker to search for the correct Challenger without using the member group and member fields.

Figure 12: Search screen with no restricting values selected



With no restricting values, a search on the Challenger field displays all Challenger panels for all members and member groups.

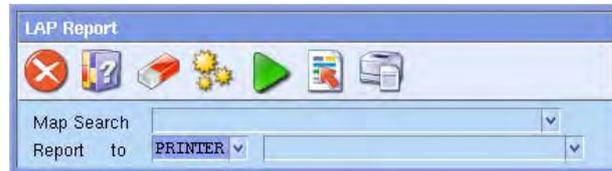
The operator can specify a member group to limit the display of members (and Challenger panels) to only those associated with the member group. Alternatively, the operator can specify a member group and/or a member to limit the display of Challenger panels to only those associated with the member.

Note: You can select a member group in order to restrict the list of available members, but not the other way around (you can't select a member in order to restrict the list of available member groups).

Generating reports

Many of the reports in Forcefield are generated using a window similar to Figure 12 on page 27. Some reports use a simpler window, such as the LAP Report window pictured below.

Figure 13: Typical report window



Map Search. Click the arrow to search for and select one or more maps. Alternatively, leave the field blank to report on all maps.

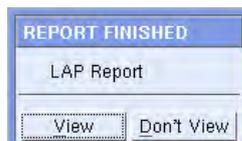
Report To. Click the arrow to select the destination for the report:

- Screen—displays the report to the screen you are operating from.
- Printer—prints the report to a specified printer.
- Disk—writes the report to a specified storage device.
- Email—sends the report via email. An email server must be configured in “Configuration” on page 226.

If you select printer and a default printer has been assigned to the workstation, this printer will be automatically selected (however, you can select another printer if required). If you select disk, you’ll need to further select the device where the report is to be written.

Some reporting options invoke a Report Finished dialog.

Figure 14: Report Finished dialog enables you to preview the results before printing



Select View to display the report on screen, alternatively select Don’t View to exit.

The report is kept on the system and is available for later viewing or printing until it is replaced by the same operator at the same workstation generating the report again, or the report has been deleted because it has been on the system longer than the time specified in Forcefield Configuration (default is 7 days). See “Configuring report options” on page 230.

Report templates

Some reports have a Template button. Click to either create a template of the current data on the screen or to retrieve data from a previously saved report template.

Figure 15: Report template dialog



Id. Select a template ID and then:

- Press Save to save a copy of the current data on the report form to the selected template ID.
- Press Run to retrieve the information from the selected template and populate the report form.

Alarm handling process

The process of responding to alarms varies depending on whether the operator uses the Unacknowledged Alarm window or the Alarm Map window as the point of entry. In addition, a workstation may be configured to display one alarm per member (see “Unacknowledged alarms” on page 31 for details).

In graphic mode (see “Initial Forcefield screen” on page 24), the operator may choose to quickly respond to an alarm indicated by a flashing red background on the Alarm Map window. Whichever the mode (graphic or menu), operators can choose the alarm handling process that best suits their needs.

Alarm handling in menu mode

To handle alarms via the Unacknowledged Alarm window:

1. Select Alarms from the main menu, or click the Alarm Screen button at the top of the main window (see “Unacknowledged alarms” on page 31).

The Unacknowledged Alarms window displays a list of alarms in priority order. Highest priority alarms are at the top of the list and new alarms are marked with an asterisk “*” (see Figure 16 on page 31).

2. Click the required alarm to open the Alarm Detail window for the alarm.
3. Respond to the alarm by selecting from pre-defined responses or by typing a text response.
4. Click the Ack Alarm button to acknowledge the alarm.

If the alarm point has reset or the alarm condition restored, the alarm is removed from the system. If the alarm has not been reset or restored, it is moved to the Follow Up Alarms window. **Note:** The device in alarm may be assigned a computer category programmed to require an acknowledgement after a restoral in order to remove the alarm.

5. If required, open the Follow Up Alarms window by clicking the Follow Up Alarms button at the top of the main screen (see Figure 3 on page 16).
6. Click the required alarm to open the Alarm Detail window for the alarm. The Alarm Detail window contains information about the state of the alarm to assist in follow-up.

Alarm handling in graphic mode

To handle alarms via the Alarm Map window:

1. In the Alarm Map window, click the device in alarm condition (indicated by a flashing red background) to open its pop-up menu. See Figure 16 on page 31 for an example of a pop-up menu (the flashing red background is hidden by the pop-up menu).

The workstation may be configured via the Bypass Menu if LAP in Alarm setting to immediately open the Alarm Detail window for the alarm when the operator clicks the LAP. If the alarm does not appear on the map, you can use the Unacknowledged Alarm window for alarm handling (see “Alarm handling in menu mode” on page 29).

2. Select Alarm from the pop-up menu to open the Alarm Detail window for the alarm.
3. Respond to the alarm by selecting from pre-defined responses or by typing a text response.
4. Click the Ack Alarm button to acknowledge the alarm.

If the alarm point has reset or the alarm condition restored, the alarm is removed from the system and the device is indicated without a coloured background. If the alarm has not been reset or restored, it is indicated by a purple background.

Note: The device in alarm may be assigned a computer category programmed to require an acknowledgement after a restoral in order to remove the alarm.

5. If required, click the device in follow-up alarm condition (indicated by a purple background) to open its pop-up menu. See Figure 16 on page 31.
6. Select Alarm from the pop-up menu to open the Alarm Detail window for the follow-up alarm. The Alarm Detail window contains information about the state of the alarm to assist in follow-up.

Figure 16: Alarm Map window pop-up menu for a selected device in alarm

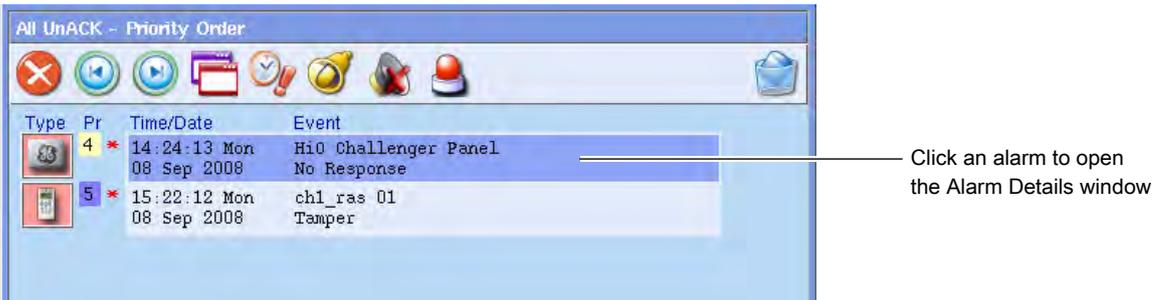


Using the alarm windows

Unacknowledged alarms

The Unacknowledged Alarms window lists all the unacknowledged alarms that are linked to members contained in the operator’s and workstation’s member groups.

Figure 17: Unacknowledged Alarms window



Alternatively, if the workstation is configured to display one alarm per member, a 1 Unacknowledged Alarm per Member window opens. Each alarm on this window represents a member: click an alarm to view all the alarms for the member, and then click an alarm to open the Alarm Details window.

To configure the workstation to display 1 alarm per member, see “Workstation options—alarms” on page 176.

The Unacknowledged Alarms window contains the following columns:

- Type—see Figure 18 on page 33 for details of alarm type icons.
- Pr (Priority)—when initially opened, the *Unacknowledged Alarms* window displays in priority order. Priority numbers 0 through 5 are colour-coded: 0 red, 1 orange, 2 pink, 3 yellow, 4 light yellow, 5 light blue. An asterisk (*) indicates new unacknowledged alarms.
- Time/Date—the time and date on which the event was received or generated by the Forcefield system.
- Event—displays the alarm ID on the first line followed by the reason.

The Alarm screen tool bar has several buttons not used on other screens. These are described in Table 4 below.

Table 4: Alarm windows tool bar buttons

Button	Name	Function
	Toggle Alarm Type	Toggles (switches) the display between the Unacknowledged alarm window and the Followup alarm window.
	Toggle Alarm Order	Toggles the alarm display order between time order and priority order. In priority order, the highest priority alarms (lowest number) appear at the top of the list. In time order, the oldest alarms appear at the top of the list. Whichever order is selected (time or priority) is maintained when switching between the Unacknowledged Alarms window and the Follow-up Alarms window.
	Silence Beeper	Turns off the beeper until a new alarm arrives or five minutes elapses.
	Silence Beeper (Permanent)	Turns off the beeper.
	Begin Incident	Manually begin an incident for the member linked to the currently-selected alarm. An Incident Report button is added to the window for an alarm that has an active incident.
	End Incident	Manually end the incident for the member linked to the currently-selected alarm.

The Unacknowledged Alarms and Follow-up Alarms buttons at the top of the main window (see Figure 3 on page 16) allow the operator to quickly switch between the Unacknowledged and Follow Up windows. Alternatively, use the Toggle Alarm Type button to switch between the Unacknowledged and Follow Up windows.

The icon at the left of the Alarm screen indicates the type of alarm: these are listed in Figure 18 on page 33.

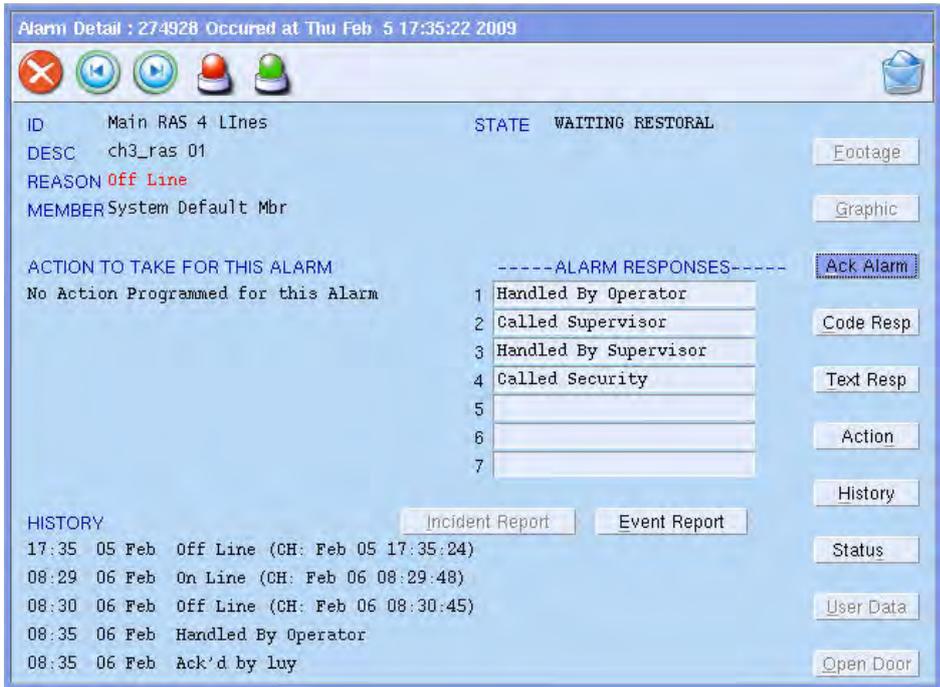
Figure 18: Alarm type icons



Alarm Details

To act on an alarm, the operator opens the Alarm Detail window by clicking the alarm (see Figure 19 below). The operator then enters a response by typing the response, or by assigning a pre-programmed response to the alarm.

Figure 19: Sample Alarm Detail window



The Alarm Detail window provides information about the alarm, and multiple ways for the operator to respond.

For many operators, the quickest way to respond to an alarm is to click the required response in the ALARM RESPONSES list. The response is added to the History section.

In addition to the ALARM RESPONSES list, the Alarm Detail window displays buttons (with associated keyboard shortcuts) that are relevant to the alarm:

- **Footage** button. The operator may click the Footage button (or use the keyboard shortcut Alt+F) to display live CCTV footage from a camera associated with the alarm. When the alarm is a sector (perimeter) alarm, the live CCTV footage displays automatically, so the Footage button isn't used.
- **Graphic** button (displayed only if the alarm point is defined to a graphic map). The operator may click the Graphic button (or use the keyboard shortcut Alt+G) to jump to the dynamic graphics (map) screen to handle the alarm. Depending on the setting in Databases > Computer Equipment > Workstations > Workstation Options, the Graphic button or shortcut opens either the first or last defined map.
- **Ack Alarm** button. After responding to the alarm, the operator clicks the Ack Alarm (acknowledge) button. The acknowledgement is added to the History section. If the alarm point has reset or the alarm condition restored, the alarm is removed from the system. If the alarm has not been reset or restored, it is moved to the Follow Up window.
- **Code Resp** button. Click to open the Alarm Response (Code) window from which the operator can select a response. The response is added to the History section. Coded responses are set up in Databases > Alarm Responses.
- **Text Resp** button. Click to open the Alarm Response (entered by operator) window from which the operator can enter a text response. The response is added to the History section.
- **Action** button. Click to display suggested actions for the operator to follow (if actions have been programmed for the alarm). The same actions are displayed in the Action To Take For This Alarm section of the window. See "Programming alarm action text" on page 58 for details.
- **History** button. Click to view the entire history of the alarm.
- **Status** button. Click to receive information about the state of the item in alarm.
- **User Data** button (user alarms only). Click to view user details including image (if available) for the user associated with the alarm.
- **Open Door** button. Opens the door.
- **Event Report** button. Click to generate a report of the alarm details.
- **Incident Report** button (displayed only when an incident is active)—use to create a report about the events that comprise the incident to which this alarm belongs.

Follow-up alarms

From the Follow Up window the operator is able to monitor the alarm condition, view details of the alarm and response messages, and enter additional responses as required. When the alarm point resets or the condition restores, the alarm is automatically removed from the Follow Up window.

Note: The device in alarm may be assigned a computer category programmed to require an acknowledgement after a restoral in order to remove the alarm.

Figure 20: Follow Up window displaying alarms in priority (Pr) order



If there is no keyboard or mouse activity for a specified time, Forcefield automatically reverts to the Unacknowledged Alarms window.

Using the alarm map window

Refer to Figure 16 on page 31 for an example of an Alarm Map window.

In graphic mode (see “Initial Forcefield screen” on page 24), a specified Alarm Map window opens by default.

Use the Forcefield Speed Bar button to display the Alarm Map window for the highest-priority alarm (the cursor automatically points to the alarm). Depending on the setting in Workstation Options, the Speed Bar button opens either the first or last defined map (see “Workstation options—graphics” on page 175).

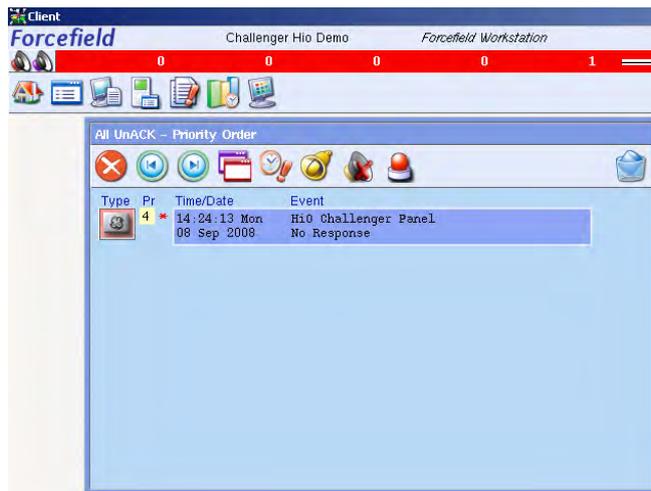
If there is more than one alarm with the same priority, the map with the oldest alarm displays.

Using the alarm line priority details

The Workstation may be configured to display a coloured bar with alarm priority details on the Alarm Line:

- A red Alarm Line indicates that there is one or more unacknowledged alarms.
- A purple Alarm Line indicates that there is one or more follow-up alarms (but only when there are no unacknowledged alarms).
- The numbers displayed in the Alarm Line indicate the total number of alarms (both unacknowledged and follow-up alarms).

Figure 21: Workstation configured for displaying alarm line priority details



Alarm Line displaying alarm counters. Position from left indicates alarm priority from 0 through 9.

This example indicates one instance of a priority 4 alarm. Up to 999 instances of the same priority may be displayed. Higher counts are indicated by *

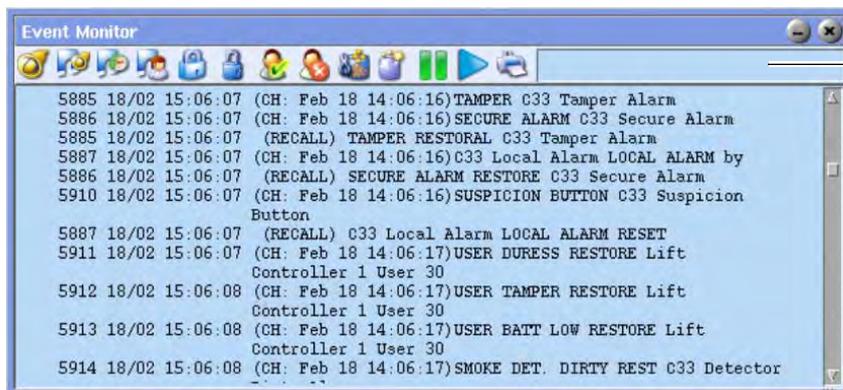
The use of priority details on the Alarm Line is defined in the Workstation Options menu (see Display Alarm Line Priority Details on page 177).

Using the Event Monitor window

Every time an event occurs, it is logged, and becomes part of the system history (for example, an operator enters new information, switches cameras, changes a database entry, responds to an alarm, or an input or output is registered by Forcefield). Whenever the Event Monitor window is open, these actions are listed. Each event is allocated a number which appears at the beginning of each event line in the list.

Note: Only events belonging to members within the member group of the operator and the workstation are displayed.

Figure 22: Event Monitor window tool bar buttons



Status message area

Use the tool bar buttons to apply filters to the events that are displayed, and to pause the flow of events on the window, as described in Table 5 on page 37.

The first eight tool bar buttons (from left) are shortcuts to populating the Event Monitor Filter Setup window with single event types. Refer to “Using multiple event filters” on page 37 for details about using additional filtering options.

Table 5: Event Monitor (or Trace Monitor) tool bar functions

Button	Name	Function
	Alarms button	Click to display (or trace) only Alarm events.
	Door Alarms button	Click to display (or trace) only Door Alarm events.
	Door Activity button	Click to display (or trace) only Door Activity events.
	Door User Activity button	Click to display (or trace) only Door User Activity events.
	Door Locks button	Click to display (or trace) only Door Locked events.
	Door Unlocks button	Click to display (or trace) only Door Unlocked events.
	Access Granted button	Click to display (or trace) only User Access Granted events.
	Invalid Badge button	Click to display (or trace) only User Invalid Badge events.
	Set Filters button	Click to open the Event (or Trace) Monitor Filter Setup window.
	Clear Filters button	Click to remove all current filters.
	Pause button	Click to freeze the display of events for the number of seconds programmed in “Workstation options—other” on page 177.
	Resume button	Click to immediately resume the display of events.
	Print button	Click to send the currently-displayed list to the printer.
Status message area		Displays the name of the current filter, displays “Filtered” for multiple filters, and displays “Paused” when the display is temporarily paused.

Using multiple event filters

Click the Set Filters button (Figure 22 on page 36) to add to a filter currently in place, or to define an event filter from scratch. The Event Monitor Filter Setup window opens.

Figure 23: Event Monitor Filter Setup window

Common window elements are described in Chapter 3. Elements specific to this window are described below. Leaving fields blank indicates no restriction on that field when matching for events: the Event Monitor displays all events; the Trace Monitor displays no events.

Different field types 'AND' together; similar fields 'OR' together. For example, you may select a specific input, AND if it generated an alarm. Alternatively, if you selected multiple inputs (points), the search would 'OR' the inputs before ANDing the other fields.

- **Operator.** Select operators to search on to create the match criteria.
- **User.** Select users to search on to create the match criteria.
- **Event Types.** Select an event type or even group for matching. Double-click the field (or press F3) to create a new event group.
- **Points.** Select the relevant points (devices) to include in the match criteria.

Displaying user details in the Event Monitor

The Event Monitor can display additional details about users when a user-related event occurs. These details include things like job titles, department name, phone numbers, and so on, as recorded in the User Maintenance window.

To configure this functionality, use the Event Monitor Information button to configure what data fields to use and optionally to provide a text prefix to help explain the purpose (for example, a prefix of “PH” to display in front of the telephone number). See “Configuring user options” on page 232 for details.

Note: Additional user details are displayed only in the Event Monitor. They are not recorded in event history.

Chapter 4

Forcefield tasks

Summary

This chapter describes the tasks that are routinely performed by all Forcefield operators, senior operators, and trained Forcefield installation technicians.

Content

Overview	40
Operator-related tasks	42
User-related tasks	44
Alarm-related tasks	58
History file-related tasks	62
Challenger-related tasks	63
Holiday-related tasks	69
Timezone-related tasks	71

Overview

This section describes the tasks that are typically performed by:

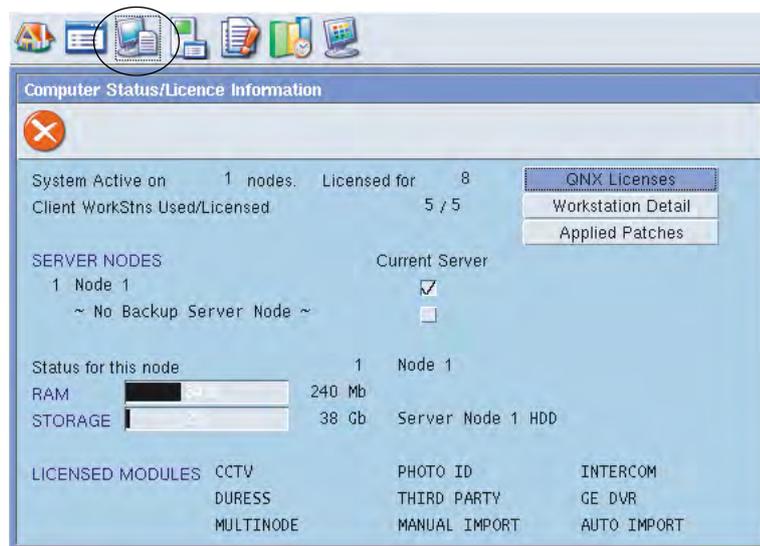
- Operators
- Senior Operators
- Trained Forcefield installation technicians

Tasks relating to installing a Forcefield system and related hardware is described in the *Forcefield Installation and Setup Manual*.

Note: Some tasks depend on Forcefield features that are subject to licensing and must be licensed before their associated menus become visible.

Click the Computer Status button (circled below) on the Forcefield Speed Bar to check the status of your Forcefield system license. Licensed Forcefield modules are listed on the bottom.

Figure 24: Computer Status window



Modules are listed after they have been purchased and installed.

Summary of operator tasks:

- Login to Forcefield, see “Logging in” on page 22
- Logout of Forcefield, see “Logging off” on page 24.
- Navigate Forcefield windows and menus, see “Navigating Forcefield” on page 22.
- Respond to and manage alarms, see “Alarm handling process” on page 29.
- Record an operator-added event, see “Add Event” on page 120.
- Control the security system remotely, see “Controlling the security system remotely” on page 42.
- Create user records, see “Maintenance” on page 131.

- Manage user records, see “User-related tasks” on page 44.
- Print card user reports, see “Card (User) Report” on page 153.
- Print Forcefield history reports, see “History Report” on page 123.
- Print Forcefield system status reports, see “Print Forcefield system status reports” on page 43.
- Monitor Forcefield event trigger operations, see “Report and review Forcefield trigger operations” on page 43.

Summary of senior operator tasks:

- Manage operator logins, see “Operator Setup” on page 164.
- Manage operators’ Forcefield menu accesses, see “Operator Menu Permissions” on page 164.
- Manually delete excess history files, see “Clear history (manually)” on page 63.
- Automate the archiving and purging of history data from Forcefield, see “Clear history (automatically)” on page 63.
- Program User Profiles, see “Program Profile” on page 147.
- Set system date and time, see “Set System Date/Time” on page 226.
- Reset a locked-out operator, see “Reset Operator Lockout” on page 226.
- Send an operator message, see “Send Operator Message” on page 226.
- Program the number of login attempts, see “Login Attempts” on page 224.
- Program the automatic logoff time, see “Workstation options—other” on page 177.
- Enable or disable a Forcefield node or workstation, see “Disable/Enable Workstation” on page 223.

Summary of installation technician tasks:

- Program Forcefield system equipment databases, see “Databases > Computer Equipment menu” on page 167.
- Program Forcefield operator accesses, see “Operator Permissions” on page 163.
- Program Forcefield workstation accesses, see “Workstation Permissions” on page 172.
- Program Forcefield alarm computer categories, see “Computer Categories” on page 188.
- Program alarm action text, see “Programming alarm action text” on page 58.
- Program Challenger databases, see Appendix A “Challenger programming” on page 253 (see also “Challenger-related tasks” on page 63).
- Program holidays, see “Holiday-related tasks” on page 69.

- Program timezones, see “Timezone-related tasks” on page 71.
- Program node-wide Forcefield settings, see “Configuration” on page 226.
- Program Forcefield clusters, see “Program Clusters” on page 187.
- Program triggering, see “Triggering menu” on page 77.
- Create and modify Forcefield maps, see “Graphics menu” on page 94.
- Optimise Forcefield operation and provide maintenance, see “Admin menu” on page 223.
- Print Forcefield system status reports, see “Print Forcefield system status reports” on page 43.
- Configure the Forcefield Speed Bar, see “Speed Bar Configuration” on page 243.

Alternatively, some installer tasks may be performed by authorised operators, as determined by the customer.

Operator-related tasks

Controlling the security system remotely

The control menu allows authorised operators to perform actions on the Challenger field equipment remotely. You may wish to open doors, isolate inputs, access areas, set relays (outputs), etc.

When a system contains a large number of items, use one or more of members, member groups, and/or clusters to restrict your selection.

- Select member groups and members to restrict the item selection list as described in “Selecting a restricting value” on page 27.
- Click the Cluster button to select a cluster (a defined list of elements). The cluster restricts the item selection list to the items contained in the cluster. See “Program Clusters” on page 187 for details.

If you do not restrict your selection (and therefore the control of items) and no item is selected, an action will be performed on every item that the operator has access to. To avoid the possibility of controlling unwanted items, take care when selecting items to control.

Note: In large systems, omitting all fields or using just member group or member fields without the ID field, is not recommended unless the operator is fully familiar with the items contained in each group.

Figure 25: Remote Control window (note cluster name “Fire Doors”)



When a cluster is used to select items (in this case the doors contained in the cluster named 'Fire Doors'), the cluster name displays in the title bar.

Control menu options typically include an Operator Notes field to provide the operator with an opportunity to enter a short description of why the action was taken. This is entered into the system log (history) for reference. It also may be compulsory depending on how Forcefield is configured.

Print Forcefield system status reports

Authorised operators may need to select Forcefield system data criteria and print reports based upon on the Forcefield and Challenger system. These reports are available from:

- Status > System Status menu. See “System Status” on page 215.
- Status > Abnormal Status Report menu or from the Forcefield Speed Bar. See “Check Log Report” on page 216.
- Status > Challenger Item Status menu or from the Forcefield Speed Bar. See “Challenger Item Status” on page 211.

Report and review Forcefield trigger operations

Authorised operators may need to monitor the event and time triggers programmed by the Forcefield installation technician to ensure the triggers are operational.

The operator will not have an understanding of every event/timer/pager type triggers that the installer has programmed unless informed. The following reports will provide the operator with the programmed settings of each event trigger. It is important the operator checks regularly that the event triggers are working as intended.

Event triggers operation can be monitored by:

- Printing or viewing reports on the configuration of each trigger, via the Triggering > Event Trigger Report. See “Event Trigger Report” on page 85.

- Automating the printed report by programming a history report template, and then setting the report to print (time trigger) periodically.
- Reviewing the history and determining that the trigger is operating correctly.

User-related tasks

Learning IUM card data

Use a card reader to learn IUM card data in order to add an unknown card to the Forcefield database.

The process is in three parts, described in the following section. The following steps assume that a suitable reader is currently available and connected to the Challenger LAN.

Part A—procedure to designate an IUM Learn Reader:

1. Open the Challenger Programming window for the required Challenger panel.
2. Click the Programming button (see Figure 72 on page 217).
3. Click Doors & Lifts to open the Door/Lift programming window (see Figure 86 on page 279).
4. Select the required door. The Programming button becomes active.
5. Click the Programming button to display the Door/Lift Menu window (see Figure 87 on page 280).
6. Click Door Access to display the Door Access programming window.
7. Right-click to check the IUM Learn Reader check box.
8. Press F5 to save.

Part B—procedure to assign a designated IUM Learn Reader to a workstation:

1. Select Users > Select Learn Reader to open the Learn Reader Select window.
2. Click the IUM Learn Reader arrow, and then select the IUM learn reader.
A workstation can use only one IUM learn reader at a time.
3. Click Run. Forcefield displays a learn reader activity icon on the desktop.



4. To end the IUM learn session, do one of the following:
 - Log out of Forcefield.
 - Clear the selection in the Learn Reader Select window, and then click Run.

- Double-click the learn reader activity icon, select the reader, and then click Stop.

Part C—procedure to learn unknown card data:

1. When the learn reader activity icon is displayed on the desktop, open the User Maintenance window for the applicable user (see Figure 54 on page 131).
2. Click the Card Data button to display the User Card Data window.
3. Badge the card at the designated IUM learn reader. Badging the card has no effect if the card data is already assigned to a user.
4. When Forcefield receives a 'User not in IUM' event from the Challenger panel, the card data is displayed in the Learn IUM User window.



5. Press F5 to save the card data to the current user record. Alternatively, click the Select a User for this card arrow, and then select a different user before saving.

Generating IUM data

Use the Generate IUM Data option to change a Challenger panel's user data from non-IUM format into IUM format. Generate IUM Data creates raw card data for each user record in the database.

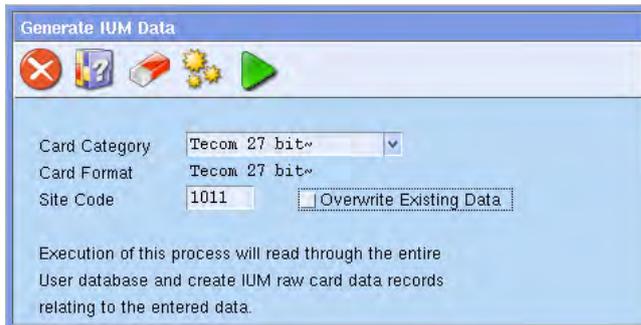
The Challenger panels to which this card data will be downloaded is determined by:

- the card category
- the user's access groups
- the user's status (data is not downloaded for expired, lost, or void cards).

This operation does not need to be repeated each time IUM is added to a non-IUM Challenger panel. However, it would need to be repeated to create IUM data for a different card category.

To generate IUM data:

1. Select Users > Access > Generate IUM Data.



2. Click the Card Category arrow, and then select a Card Category to identify the Challenger panels with IUM.
3. Select the Card Format.
4. Type the card site code number in the Site Code field.
5. Check the Overwrite Existing Data selection box to create raw card data for all cards, replacing any exiting raw card data.

If the selection box is cleared, raw card data will be created only for cards that do not already have raw card data.

6. Press F6 to execute.

Creating users in bulk

Authorised Forcefield operators may use the Bulk Add option to add a number of user records based on an existing user record. The record displayed is used as a template to quickly add a number of users with the same properties as the original user (in particular the user's member).

Example: You require 15 extra cleaning staff for the week over Christmas, and they all need the same properties. Add these new users quickly with the Bulk User option.

Note: If you create new records and there are already user records in the range you're creating, the old records are left untouched. The event history will list which new user numbers have been created.

To add new user records in bulk:

1. From the main menu select Users > Maintenance. The User Maintenance window opens (see Figure 54 on page 131).
2. Select a user record to use as a template.
3. On the User Maintenance window, click the Bulk button to display the Type of Bulk Processing window.

- Click Create. The Bulk User Create window opens.



- Type the start and end numbers for the new range of users in the in range and to fields. If a user record already exists within the selected range, then that user record is not changed. An entry is placed into history indicating a user record could not be created for that user number.
- Type a new user name (for example, new cleaners) in the with Name field, and this will appear on every new record. This name is prefixed to the user number (for example, if the user is 1234 and the name is “cleaner”, the new record name is “cleaner 1234”).
- Click Save (or press F5) to save the new records. To stop the process after it starts, click ESC. When you stop the process, no more new records are created.

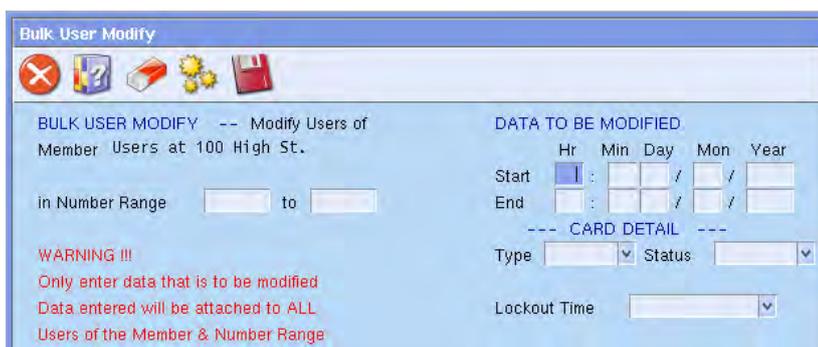
Modifying users in bulk

Authorised Forcefield operators may use the Bulk Modify option to change details such as start and end dates, user type, user status, and lockout time for a range of users.

Note: When modifying large numbers of records, updating the database may take some time.

To modify user records in bulk:

- From the main menu select Users > Maintenance. The User Maintenance window opens (see Figure 54 on page 131).
- Select a user record to use as a template.
- On the User Maintenance window, click the Bulk button to display the Type of Bulk Processing window.
- Click Modify. The Bulk User Modify window opens.



5. Type the range of the records you wish to modify in the in Number Range and to fields.
6. Type the data to be modified, as applicable, in the remaining fields.
7. Click Save (or press F5) to save the new records. To stop the process after it starts, click ESC. When you stop the process, no more records are modified. Any records already modified stay modified.

Deleting users in bulk

Authorised Forcefield operators may use the Bulk Delete option to delete a range of user records belonging to a member.

To delete user records in bulk:

1. From the main menu select Users > Maintenance. The User Maintenance window opens (see Figure 54 on page 131).
2. Select a user record to use as a template.
3. On the User Maintenance window, click the Bulk button to display the Type of Bulk Processing window.
4. Click Delete. The Bulk User Delete window opens.



5. Type the range of the users you wish to delete.
6. Press F8 to delete the records. Confirm that you wish to delete the records. To stop the process after it starts, click ESC. When you stop the process, no more records are deleted. Any records already deleted stay deleted.

Auto-allocating user numbers

Authorised Forcefield operators may use this option to automatically assign the lowest available user number in the user database.

To program Forcefield to allocate user numbers:

1. From the main menu select: Admin > Configuration > Configuration.
2. Click User. The User Config window opens.
3. Right-click to check the Allow Auto User Number Allocation check box.
4. Press F5 to save.

The next time you create a new user record (in Users > Maintenance), there's no need to search for an unused user number—Forcefield automatically finds and allocates the new user record to the lowest available user number.

Allocating PIN codes for users 1001 to 65,535

Authorised Forcefield operators may use this option to nominate a user's personal identification number (PIN) code to a number in the range from 1001 to 65,535 for non-IUM Challenger systems.

Note: The user number in non-IUM Challenger panels must be less than 1001, and so an 'offset' is used to reconcile the difference. Refer to the *Challenger V8 & V9 Programming Manual* for information on how to set a user offset.

To program Forcefield for manual PIN codes:

1. From the main menu select Admin > Configuration > Configuration. The Forcefield Configuration window opens.
2. In the Global section, double-click User. The User Config window opens.
3. Right-click to check the Manual PIN Code for Users above 1000 check box.
4. Press F5 to save the change.

Timed user access

Timed user access enables Forcefield to start a timer when a user enters or exits a site.

The types of timed user access are:

- From on site: The time interval begins when a card is badged to enter the site. The card may be used to exit the site, but it cannot be used for re-entry until the time interval expires.
- From off site: The time interval begins when a card is badged to exit the site. The card cannot be used for re-entry until the time interval expires.

Example: A wholesale market wants to ensure only genuine wholesale buyers (authorised users) are in the market during certain hours, and prevent unauthorised users from using cards assigned to authorised users (for example, if an authorised user leaves the site and gives the card to someone else). By adding an offsite lockout time limit to a user's card, the card cannot be reused to enter the site until the time limit elapses (for example, 60 minutes).

Notes

- Timed regions are associated by user, not by region.
- The use of this option alters the start date of the user record when the system applies the time restriction. This will affect some Forcefield reports.
- See also the Lockout field description in "Maintenance" on page 131.

To program timed user access:

1. From the main menu, select Users > Maintenance, the User Maintenance window opens.
2. Find the required user.

3. Click the Lockout arrow, and then select one of the lockout time options:
 - Not timed — default setting
 - From on site — the time interval begins when a card is badged to enter the site. The card may be used to exit the site, but it cannot be used for re-entry until the time interval expires.
 - From off site — the time interval begins when a card is badged to exit the site. The card cannot be used for re-entry until the time interval expires.
4. If applicable, type the number of minutes required for the lockout time in the range of 1 minute to 65,000 minutes (45 days).
5. Press F5 to save the change.

Time allowed in region

Authorised operators may use this option to create an alarm for a user when the user has been in a region too long.

Example: Workers in a freezer room (set up as a region) risk their health if they stay inside too long. Setting the time limit for each region creates an alarm event if a user stays in the region too long.

To program time allowed in region:

1. From the main menu select Challenger > Challenger Programming.
2. Type the number of the Challenger controlling the region, and press Enter to display the Challenger record.
3. Click the Programming button to display the Challenger Programming selection window.
4. Select Regions from the list, and the Region window opens.
5. Type the region number and press Enter. The name of the region appears. If the name of the region doesn't appear you'll be prompted to type a name of an existing Challenger region. Alternatively, press F4 for a list of regions.
6. Type the number of minutes to set the maximum Time Allowed in Region. The minimum is 15 minutes and the maximum is 65,535 minutes.

Set users offsite

Authorised Forcefield operators may use this option to change the status of a user or users belonging to a member or a member group to offsite. This is typically used to permit re-entry when antipassback is active and users leave the site without badging their cards. Under antipassback access, re-entry is not permitted because the users still have the status of onsite.

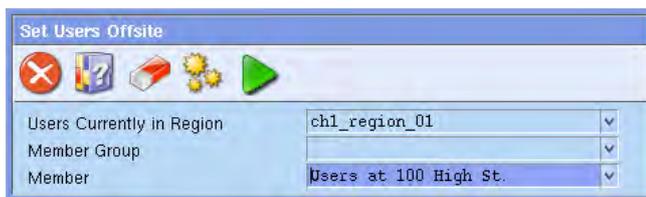
You can change the status for a single user to offsite. See "Change Status of User" on page 146 for details.

Example 1: An emergency evacuation requires all users to exit the site through emergency exits without badging out. The Set Users Offsite command is used to change each user's status to offsite, so that the users can badge in later.

Example 2: At a wholesale market the main door is intentionally left open in the late morning after main trading has completed. Users who earlier badged their cards to get in, can now leave without badging. Next morning they find they can't re-enter unless the operator manually changes the on-site status to off-site.

To change the status of a member or member group to off-site:

1. From the main menu select Users > Modify Status > Set Users Offsite. The Set Users Offsite window opens.

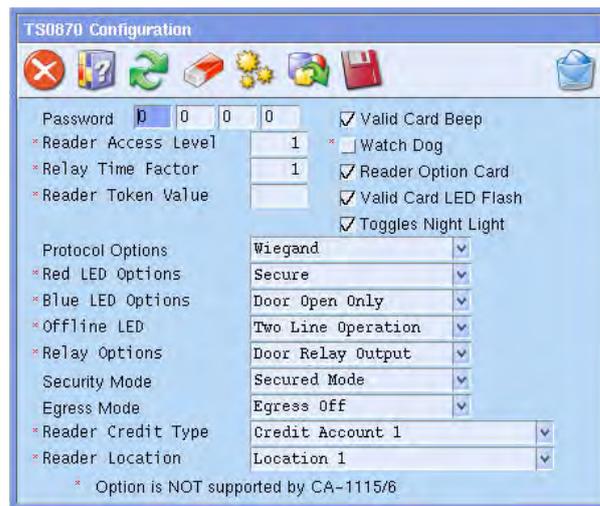


2. Optional—Right-click the Users Currently in Region field and select the region to which the on-site status currently applies. If no region is specified then all users who are currently onsite will set to offsite.
3. Optional—Right-click the member group or the member fields to select the required member group or member.
4. Press F6 to change the status to offsite for the selected users.
5. Press F5 to save the change. This sets the status of all users who were listed as being in the region and belonging to the member or member group from 'onsite' to 'offsite'.

Note: Only users belonging to members contained in the operator's member group will be set offsite.

Programming smart card options

If the RAS is a smart card reader, click Smart Card Options on the Challenger's RAS programming window to program the reader. The TS0870 Configuration window opens.

Figure 26: TS0870 Smart Card Reader Configuration window

Common window elements are described in Chapter 3. Elements specific to this window are described below. Also see the note in “Challenger programming” on page 217.

Password. If the reader (and associated cards) are to be used in secured mode, enter the 4-byte password (values from 0 through 127).

Note: Do not use the password fields if you’ve purchased the special high-security TS0870PSC Configuration Card. In this instance you must initially program the smart card reader by using the TS0870PSC Configuration Card.

Valid Card Beep (optional). When checked the reader will beep once when valid Smart Card is badged at the reader (in addition to any other beeps).

Watch Dog (optional). When checked the reader automatically sends a signal periodically to indicate that it’s connected and working. Can be used only if the reader is configured as a Wiegand device.

Reader Option Card (optional). When checked the reader accepts a configuration card more than once. If not selected, the reader can only be configured with a reader configuration card one time only to prevent unauthorised reprogramming of the reader. Any future changes must be made via the RAS keypad or by first un-flagging this option via the RAS keypad.

Valid Card LED Flash (optional). When checked the reader’s LED gives a short flash when a valid card is badged.

Toggles Night Light (optional). When checked the blue LED remains lit, with low intensity, at all times regardless of whether the red LED is on or off.

Reader Access Level (used for credit functionality). Enter a number in the range of 1 through 16 to identify the reader’s access level.

Example: A Smart Card reader at a photocopier has an access level of 4 (which permits operation by users with access levels of 4 through 16). If a user has a card with access level 5, then they can use the photocopier. Another user with a card with credit access level of 2 cannot use the photocopier.

Relay Time Factor. Enter a number in the range of 1 through 256 to specify the relay time factor. The relay time factor modifies the pulse width output of the Credit Pulsed option or the energised time for the Credit Timed option (whichever is defined in Relay Options).

The pulse width for the Credit Pulsed option is the relay time factor multiplied by .01 seconds (10 milliseconds). This gives a pulse width from 0.01 through 2.56 seconds.

The activation time for the Credit Timed option is the relay time factor multiplied by the token value of the reader. This gives a range of between 1 second and around 193 days.

Reader Token Value (used for credit functionality). Type a number in the range of 1 to 65534 to specify the reader's token value.

The reader token value determines how many credits are deducted for each token when a card is badged.

Example: On a photocopier, one token equals two credits (one credit equals 10 cents). Each time an A4 copy is made with the card, one token is deducted (two credits or 20 cents).

Protocol Options. Select the required protocol (Refer to the *TS0870x-series Installation & Programming Guide R4.0* or later for details):

- Wiegand
- Magnetic Stripe

Note: Do not select Tecom Smart Card protocol because it is not implemented in the Challenger.

Red LED Options. Select one of the following online red LED options (the reader is said to be 'online' when it is configured as a LAN device either on the Challenger LAN or the Intelligent Door/Lift Controller sub-LAN):

- Secure—the red LED is on when the area associated with the door is secure.
- Secure & Door open—the red LED is on when the area associated with the door is secure, and the red LED flashes whilst the door lock relay is active.

Blue LED Options. Select one of the following online blue LED options (the reader is said to be 'online' when it is configured as a LAN device either on the Challenger LAN or the Intelligent Door/Lift Controller sub-LAN):

- Door Open Only—the blue LED will normally be off, and will flash whilst the door lock relay is active.
- Access & door open—the blue LED is on when the alarm area associated with the door is in access, and will flash whilst the door lock relay is active.

Offline LED. Select one of the following Offline LED options (LEDs are classed as offline when the reader is attached to a Wiegand or magnetic stripe interface):

- One Line Operation—both the blue and red LEDs are controlled by the brown wire.
- Two Line Operation—the red LED is controlled by the brown wire and the blue LED is controlled by the yellow wire.

Relay Options. Select one of the following relay options:

- Door relay output—the relay output (violet wire) will operate as a door relay control output (active low) when 'online' only.
- Tamper output—the relay output activates when RAS tamper occurs (active low) in both the 'online' and 'offline' modes.
- Card present output—indicates to a third-party magnetic stripe reader interface that the card is being swiped. The relay output activates when the card data is sent to the host device (active low) but only when the card reader is in the 'offline' mode. When the transaction is complete, the relay output returns to high.
- Credit pulsed—the relay output will operate as a pulsed output (active low) when the reader is configured to operate as a credit activated device, and a credit transaction is completed. The pulse width is configurable from 10 milliseconds to 2.55 seconds.
- Credit timed—the relay output operates as a timed output (active low) when the reader is configured to operate as a credit activated device, and a credit transaction is completed. The time is configurable from 1 to 65535 seconds, multiplied by the relay time factor.
- Credit latched—the relay output operates as a latched output if the reader is configured to operate as a credit activated device. When a Smart Card with valid credit data is badged and the transaction is successfully completed, the relay output is turned on. The relay output is turned off when a valid Smart Card is badged next, with or without credits.

Security Mode. Select one of the following security mode options:

- Secured Mode—the reader sees programmed Smart Cards and user-defined cards (the 4-byte security password is used).
- Unsecured Mode—the reader only sees blank (un-programmed) cards with a unique serial number and user-defined cards (the 4-byte security password is not used).

Egress Mode. Select one of the following egress (request to exit, or RTE) mode options:

- Egress off—Egress functionality is not used.

- Standard Egress—Egress functionality is used. This option requires a simple normally open push button to be connected. The smart card reader's open collector output controls a door relay. A press of the button will release the door lock relay.
- Egress and Arm/disarm—Egress functionality is used, along with alarm control. This option requires a TS0064 Expanded Button Interface to be connected. The smart card reader's open collector output controls a door relay. A press of the TS0064's In button will release the door lock relay and disarm the area. A press of the TS0064's Out button will release the door lock relay and arm the area.

Reader Credit Type (used for credit functionality). Select one of four credit accounts to apply to the reader. Cards may be used that have the same credit account.

Reader Location (used for credit functionality). Select one of four location names to apply to the reader. Cards may be used that have the same location name.

Converting to prohibit shared profiles mode

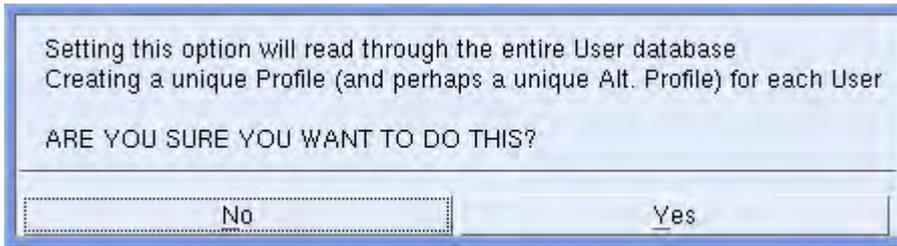
Prohibit shared profiles mode causes user profiles (and alternative user profiles) to be locked to user records. For example, user 1 can have only "User 1 Profile|" and optionally "User 1 Alt Profile|".

When prohibit shared profiles mode is selected Forcefield converts the entire user database and creates a profile (and an alternate profile, if required) for each user. This conversion may take considerable time, depending on the number of users.

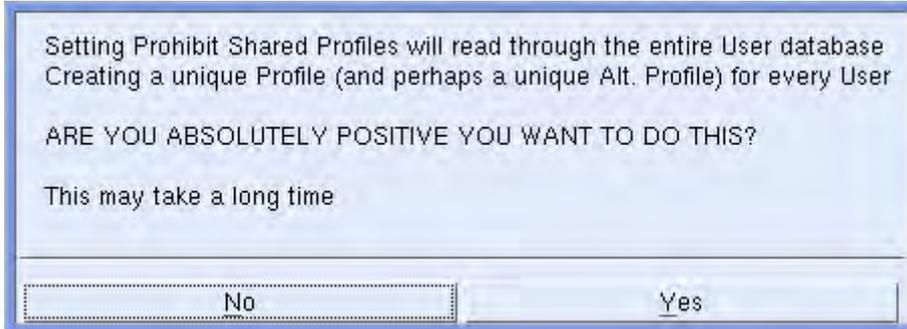
Note: No user maintenance operations may be carried out while the conversion process is active.

To enable prohibit shared profiles mode, and to convert the user database:

1. Backup the database.
2. If enabled, disable Auto Logoff on the workstation where the conversion will take place (see "Workstation options—other" on page 177).
3. Logout on that workstation.
4. Log back in with a login that has all privileges.
5. Select Admin > Configuration > Configuration, and then click User (see "Configuring user options" on page 232).
6. Select Prohibit Shared Profiles. A selection dialogue box opens.



7. Select Yes and then click Save. A second selection dialogue box opens.



8. Select Yes. A Creating User Profiles message displays. The conversion could take several hours depending on how many user records are in the database.
9. When finished a completion dialogue box opens.



10. Click Continue, and then close the Configuration windows.
11. Re-enable Auto Logoff (if previously enabled), see step 2.
12. Backup the database (do not overwrite the previous backup from step 1).
13. Shutdown the entire system.
14. Restart the system.

Importing user profile data

The User Profiles programming window (Figure 60 on page 148) displays an Import button for a saved profile, which allows a profile's contents to be copied from another profile. Import allows "template" profiles to be created, from which panel access may be assigned to other profiles when Forcefield is operating in prohibit shared profiles mode.

To import profile data into a new profile from a different profile:

1. Select Users > Profiles > Program Profile.
2. Create a new profile (or select a saved profile). A profile can be saved with just an ID, and it will be given the system default member, date starting from creation time, and a normal card type.

3. Click Import to open the User Profile Import window.



4. Click the Select Source Profile arrow and find the profile that you want to copy (in the example above, the profile “User 15 Profile |” is selected).
5. Click Execute. A selection dialogue box displays.



6. Select either Panel Access data or All data.

Configuring the user maintenance window

Forcefield operators can specify which fields on the User Maintenance window are to be read-only (not editable). This allows operators to bypass fields that they do not commonly use in order to save time when adding users.

Refer to “Maintenance Config” on page 139.

Using templates to populate new user data

The User Maintenance window (Figure 54 on page 131) has a template function that lets you:

- Define default user data that will be common across multiple users.
- Save the data as a template.
- Run the template to add new users in default data mode. The default data automatically populates the new user record, but can still be edited if desired.

To create a template for new user records:

1. Open the User Maintenance window.
2. Edit the details that you want to be common for new users (alternatively, open a user record that contains the details that you want to be common for new users).
3. Click the Set Default button. The Record Default window opens.

Figure 27: Record Default programming window

4. Type a name (without spaces) in the ID field.
5. Optionally, select a member if you want to restrict access to this record.
6. Save the record.

To use a template to populate new user records:

1. Open the User Maintenance window.
2. Click the Set Default button. The Record Default window opens (Figure 27 above).
3. Click the ID arrow, and then select the required template.
4. Click the Run button. The User Maintenance window opens with the template name displayed in the title bar (Figure 28 below).

Figure 28: User Maintenance window's title bar in default data mode

Each time you create a new user record the common fields will be populated from the template.

To remove the current template (exit from default data mode):

1. Open the User Maintenance window.
2. Click the Clear Default button.

Alarm-related tasks

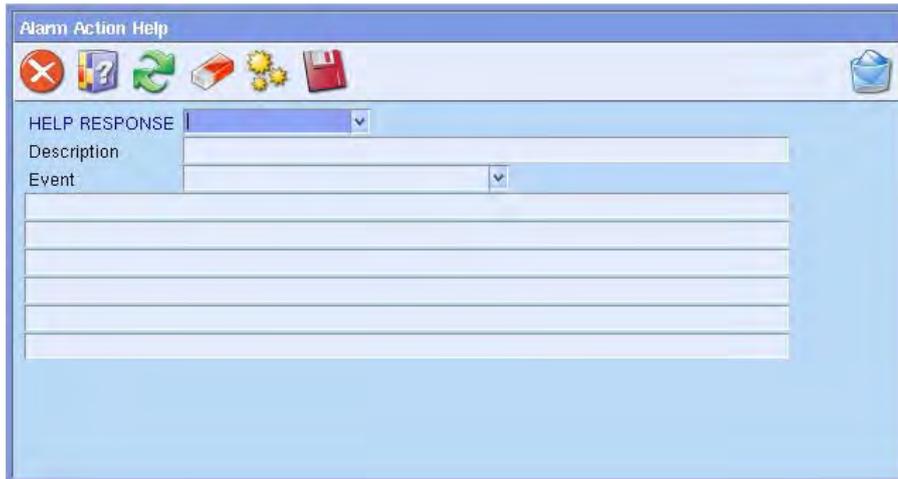
Programming alarm action text

This section describes the process of programming text for the Action To Take For This Alarm section and the Action button on an Alarm Detail window (Figure 19 on page 33).

To create alarm action text (input example):

1. Open the Challenger programming window for the required Challenger input device. See “Inputs” on page 256 for details.

2. Double-click the Help field. The Alarm Action Help window opens.

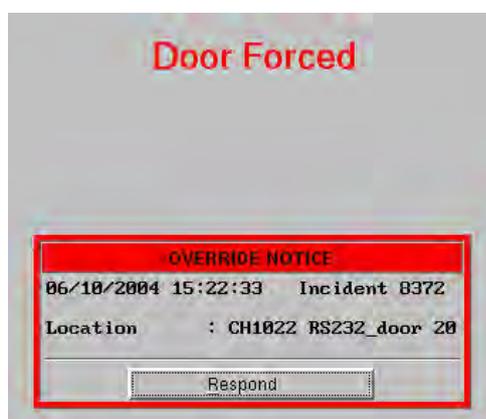


3. Click the Help Response arrow to select an existing help response file, or type a name for new action help.
4. Type a description for the action help in the Description field.
5. Click the Event arrow, and then select the event state (for example, Alarm, Tamper, etc.) for which the text applies. (The event named ~COMMON HELP~ is used to give help text that will be displayed regardless of the event that caused the alarm.)
6. Type the text to be displayed for the alarm in the remaining fields.
7. Save the alarm action help file.

Activating screen overrides with alarm events

Trained Forcefield installation technicians may alter alarm event behaviour such that predetermined events 'override' (display in front of) all other Forcefield screens (windows). Once activated, the alarm displayed on the override screen must be handled by the operator before any other Forcefield function can be used.

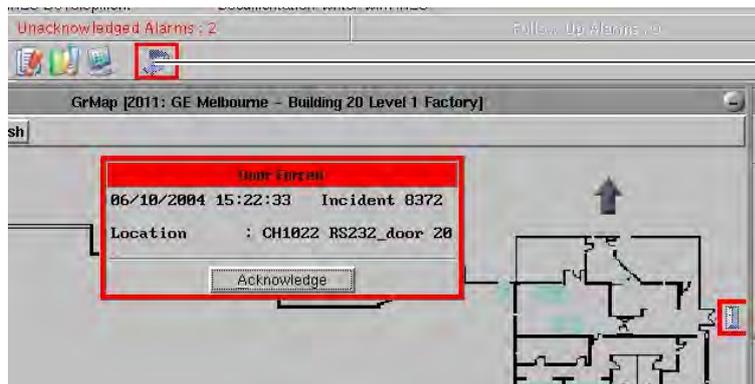
Figure 29: Example of an override screen



All other Forcefield screens are hidden by the override screen.

Click the Respond button to close the override screen.

Figure 30: Example of a Go to Override Map Speed Bar button (icons may differ)

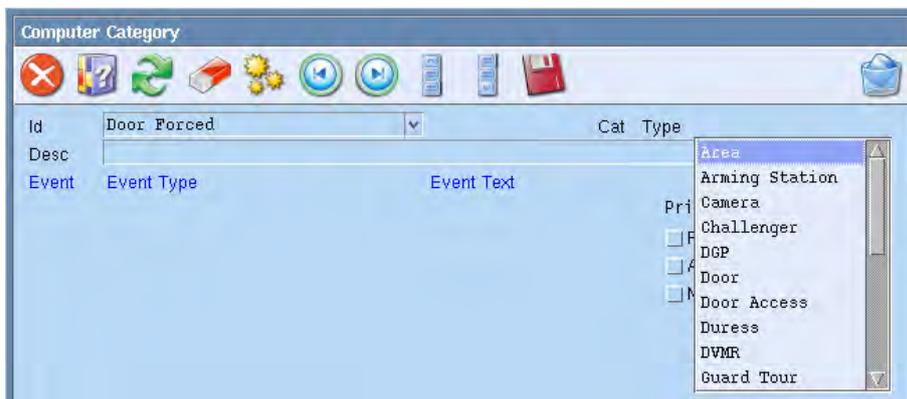


Go To Override Map button (one of many possible icons).

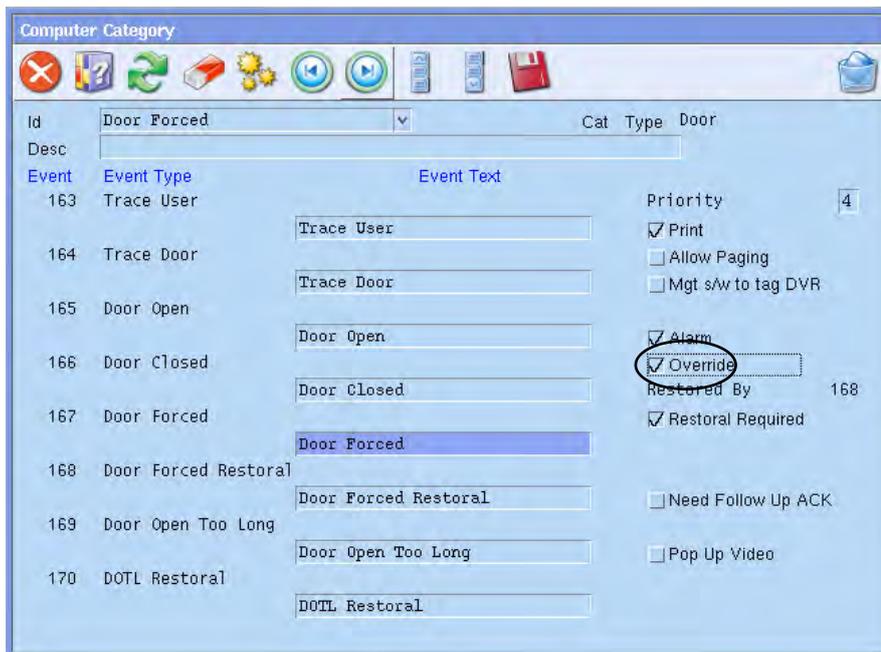
Click the Go To Override Map button to open the map containing the device for which the override event has been received.

To set up a screen override for an event:

1. From the main menu select Databases > Management Software > Computer Categories > Computer Categories. The Computer Category window opens.
2. Click the Id field, type a new name for the Computer Category, and then and press Enter. Forcefield displays a Category type selection list.



3. Select the required Category Type from the list.
4. Type a description for the new category in the description field.
5. In the Event Text list, select an event type (for example, Door Forced) for which you want to program a screen override.



6. Right-click the Override button to activate (check) it.
7. Repeat the previous two steps for additional event types, if required.
8. Press F5 to save the change.
9. Open the Challenger programming record for the device that you want to assign the screen override alarm event setting (Challenger > Challenger Programming).
10. Click the Computer Cat field and select the new screen override computer category.
11. Press F5 to save the change.
12. Add the 'Go To Override Map' button to the Forcefield Speed Bar. This button flashes when the operator responds to the Override screen. When selected, the Go To Override Map button opens the map where the alarm is indicated.

Configuring the Forcefield Speed Bar is described in "Speed Bar Configuration" on page 243.

Display highest priority alarm text

Alarm text for the highest priority alarm (lowest number) is displayed for a device that has multiple simultaneous alarm conditions of different priorities.

If more than one system alarm condition exists (for example, a low battery alarm and a tamper alarm) for a device, the highest priority alarm condition is displayed in the Unacknowledged Alarm window. Click the alarm to display the alarm details: the multiple conditions are displayed in the History section.

If a new, higher priority, alarm condition occurs, the new alarm condition automatically replaces any lower priority alarm condition. For example Figure 31 below displays a priority 1 alarm. If an alarm occurs that has greater priority (priority 0 alarm), it will be displayed in place of a priority 1 (or lower priority) alarm.

Figure 31: Alarm list displaying a priority 1 alarm

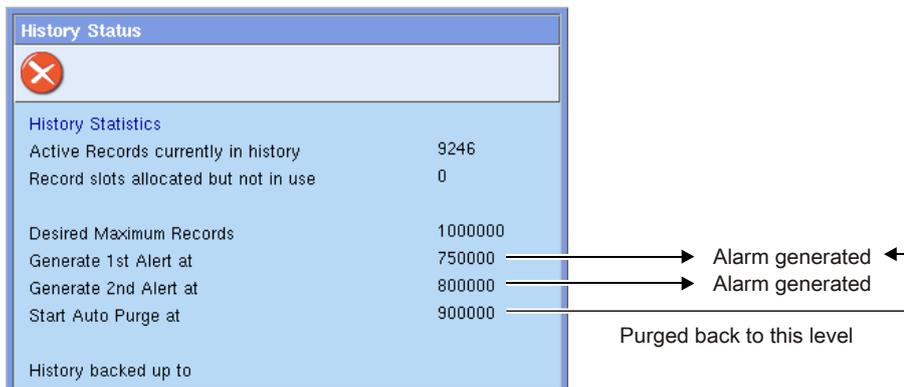


History file-related tasks

Unless regularly cleaned up, Forcefield stores events until the 'Auto Purge At' limit is reached (the default limit is 950,000 records). When the Auto Purge At limit is reached, Forcefield begins to automatically purge history records, and Forcefield performance decreases during the purge.

Click the History Statistics button (see "Forcefield Speed Bar" on page 18) or use the History > Statistics option to view the current history status and date of the most recent backup

Figure 32: History Status window



You may delete history records before the Auto Purge At limit is reached in order to prevent this automatic purging and related decrease in performance. There are two ways to delete history records:

- Use the Clear History option to delete all records. See "Clear history (manually)" on page 63.
- Use the Clear option in "Auto History Backup" on page 87 or "Auto History Export" on page 88 to automatically delete records according to the Purge Type selection on these windows.

To change the Auto Purge At limit, see “History Config” on page 121.

Clear history (manually)

Authorised Forcefield operators may use the Clear History option to delete history records.

Note: Backup your history files if they might be needed later.

To manually delete all history records:

1. From the main menu, select History > Clear History. The Clear History window opens.
2. Type your password, and confirm you wish to clear the history. All history files are deleted. There is no undo available.

Clear history (automatically)

Use Backups > Auto History Backup to automate the archiving and purging of history data from Forcefield. This command is described in “Auto History Backup” on page 87.

Challenger-related tasks

Copy Challenger

Use the Copy Challenger function to create a new Challenger record in Forcefield based on an existing Challenger record in Forcefield.

If you want to transfer a database from a Challenger to Forcefield, see “Upload Challenger” on page 66.

To create a new Challenger based on an existing Challenger:

1. From the main menu select Challenger > Copy Challenger.



2. In the ‘From Ch’ field select the Challenger to copy. Select by Challenger number or ID (Challenger name).

3. Type a number in 'to Ch' field and complete the ID field to create a new Challenger number and ID. You must create details for a new Challenger panel, that is, one that doesn't already exist. You can't copy over an existing Challenger panel.
4. Use the member field to define the member ID for the new Challenger devices (Inputs, Areas, etc.). If left blank, the member IDs of the original Challenger devices will be copied.
5. Type a description (for example, "Level 1, South West Corner") in the Description field.
6. Optionally, specify an Id_Prefix to use for devices on the new Challenger panel. See "Using ID prefix" on page 65 for details.
7. Optionally, select to Use Existing Record ID as ID postfix. See "Using existing record ID as ID postfix" on page 65 for details.
8. In the 'Custom_RAS' field, type a custom message to display on each Remote Arming Station (RAS). If left blank, it will copy the Custom RAS display information from the existing Challenger (optional).
9. In the 'Port' field, select the Challenger communications port if different to the existing Challenger panel, for example, serial port 1 on the controlling node (optional).
10. In 'Backup Dialler' field type the command (modem string) for Forcefield to dial Challenger (optional).
11. Ignore the following three fields that cannot be changed here:
 - Comms_Type displays the communication type, such as Serial, TS0898 or Dialler.
 - Comms_Mode displays the communication mode, such as polled or event driven.
 - Forcefield_Computer displays the node number that the Challenger is connected to.
12. Press F5 to save changes.

Default record IDs

When you create a new Challenger based on an existing Challenger panel, Forcefield by default, creates record IDs in the format chxx_device yy, where:

- chxx is called a prefix, and it identifies the number of the new Challenger panel.
- device yy is called a postfix, and it identifies the device type and number.
- An underscore character '_' separates the prefix from the postfix.
- The maximum number of characters (including spaces) is 30.

For example, Forcefield creates the record ID 'ch35_input 1' to represent Challenger 35, input 1—regardless of what record ID was used in the existing Challenger panel.

In order to make the new record IDs more meaningful, the Copy Challenger window has an ID Prefix field and a Use Existing Record ID as ID postfix selection. The following sections describe how to use these controls.

Using ID prefix

Type a string of text in the ID Prefix field to enable Forcefield to replace the record ID default characters chxx (see “Default record IDs” on page 64) with the specified text string. For example, in the case of Challenger 35, instead of using the default prefix 'ch35', you could have a prefix 'Factory 9'.

Using existing record ID as ID postfix

Select Use Existing Record ID as ID Postfix to reuse part of the existing Challenger record ID. For example, instead of using the default postfix such as 'input 1', you could have a postfix 'East Ceiling PIR'.

As described in “Default record IDs” on page 64, Forcefield uses an underscore character when creating record IDs. This is significant when the existing Challenger record ID also uses underscore characters, because specific rules apply to how Forcefield creates the new ID.

- If the existing Challenger record ID did not use any underscore characters, then Forcefield uses the entire record ID as the new ID postfix.
- If the existing Challenger record ID uses one or more underscore characters, then Forcefield looks for the last underscore in the ID and copies all of the text after the last underscore (the underscore is not included). Forcefield then uses this text as the new ID postfix.

The following three examples are provided to help you predict the results of using the ID Prefix field and the Use Existing Record ID as ID postfix selection, for various types of existing Challenger record IDs. They are not meant as recommendations.

Example 1—Challenger 35, input 1, where the existing record ID is 'Factory 5 East Ceiling PIR". See Table 6 below.

Table 6: No underscore used in existing record ID

ID Prefix text	ID Postfix selection	Result (30 character limit)
blank	cleared	ch35_input 1
blank	selected	ch35_Factory 5 East Ceiling PI
Factory 9	cleared	Factory 9_input 1
Factory 9	selected	Factory 9_Factory 5 East Ceili

Example 2—Challenger 35, input 1, where the existing record ID is 'Factory 5_East Ceiling PIR". See Table 7 on page 66.

Table 7: One underscore used in existing record ID

ID Prefix text	ID Postfix selection	Result (30 character limit)
blank	cleared	ch35_input 1
blank	selected	ch35_East Ceiling PIR
Factory 9	cleared	Factory 9_input 1
Factory 9	selected	Factory 9_East Ceiling PIR

Example 3—Challenger 35, input 1, where the existing record ID is 'Factory_5_East_Ceiling_PIR'. See Table 8 below.

Table 8: Multiple underscores used in existing record ID

ID Prefix text	ID Postfix selection	Result (30 character limit)
blank	cleared	ch35_input 1
blank	selected	ch35_PIR
Factory 9	cleared	Factory 9_input 1
Factory 9	selected	Factory 9_PIR

Upload Challenger

Use the Upload Challenger function to transfer database records from an online Challenger panel to an existing Challenger record in Forcefield.

Notes

- The Challenger record must already exist in the Forcefield database. At the end of the upload process Forcefield reports detected errors (if any) and displays a window allowing the operator to view the exception report.
- This function does not delete database records. Database records that are created in the panel via a RAS will be added to the Forcefield database; however, database records that are deleted in the panel via a RAS will not be deleted from the Forcefield database.
- This function does not upload the user database, so you will need to manually enter all user data into Forcefield, or use the Import User Data function (see "Import User Data" on page 162).

Check the Challenger's database record in Forcefield after an upload to ensure that the details are correct. Examples include (but are not limited to) the following:

- During the upload, a panel reports a DGP as being a four-door Controller but the corresponding Forcefield record is for a standard DGP or a 4-Lift Controller. In this case, the upload will generate an exception report listing the error. You would need to remove the incorrect Forcefield record and then reprogram it in Forcefield.

- After an upload there are input records in Forcefield that do not exist in the panel. You would need to remove the incorrect Forcefield records from the database.

If you made any changes to the Challenger's database record in Forcefield after an upload, you may perform a download to ensure that the data in both Forcefield and the panel are the same (see "Download All" on page 221).

See also "Managing data integrity" on page 6.

To upload data from a Challenger:

1. From the main menu select Challenger > Upload All Challenger Data.



2. In the 'Ch' field select the Challenger which you want to upload the database from. If you wish to use the default device ID naming, go to step 6. Steps 3, 4, and 5 are options for device ID naming.
3. Optionally, select an ID Source. The ID Source is the location for device ID names. See "Using ID source files" on page 68 for details.
4. Optionally, type an ID Prefix. See "Using ID prefix" on page 65 for details.
5. Optionally, select ID Postfix. See "Using existing record ID as ID postfix" on page 65 for details.
6. Press F6 to upload the database from an active (online) Challenger into Forcefield.

Device ID names

When Forcefield uploads a database from a Challenger panel, a conversion process takes place because a Challenger database and a Forcefield database use different formats. Part of the conversion process involves the naming of devices uploaded from the Challenger panel.

The Upload Challenger function provides several options for naming device IDs in Forcefield (steps 3, 4, and 5 above). If no options are selected, Forcefield automatically assigns default device ID names, based on the format `chx_device y`, where:

- **ch** represents Challenger
- **x** represents the Challenger number, for example, 7
- **device** represents the device type, for example, input
- **y** represents the device number, for example, 1

Example: `ch7_input 1`

Steps 4 and 5 above refer to the optional use of ID prefix and ID postfix values to add meaning to the device ID names when uploading a database. This process is similar to the one described in “Default record IDs” on page 64.

The specified ID prefix and ID postfix values are used only if the resulting device ID names are unique (they don’t already exist in the Forcefield database). If a device ID is already used, the Upload Challenger function uses the default naming convention.

Using ID source files

Step 3 on page 67 refers to the optional use of device ID name files located in the ‘ID Source’.

The external files (one for each device type) are lists of device names and numbers (up to 30 characters) in .csv (comma separated value) format that Forcefield applies to device ID names when uploading a database from a Challenger panel.

The external files must be named exactly as listed in Table 9 below, and are case-sensitive.

Table 9: Device ID external file names

File name	Device
alrmgrp.csv	Alarm Group
area.csv	Area
contrlrm.csv	Door/Lift Controller macro logic
door.csv	Door
doorgrp.csv	Door Group
evntdsc.csv	Event Flag
floor.csv	Floor
floorgrp.csv	Floor Group
holiday.csv	Holiday
inptshnt.csv	Input Shunt
inputs.csv	Input
lifts.csv	Lift
mcrlogic.csv	Challenger Macro logic
ras.csv	RAS
region.csv	Region
relaymap.csv	Relay
timezone.csv	Timezone
usrcat.csv	User Category

The following sections “CSV file format (except macro logic)” below and “CSV file format for macro logic” below describe the two file formats for the device ID name files. These files are used independently, that is, you can use any combination of files—you don’t need to create .csv files for the entire set of devices.

The device ID files are used in the Upload Challenger function (see step 3 on page 67).

Note: A utility file ForcefieldTitanDesExtract.exe is provided on the Forcefield Installation CD or USB device (in the Install folder), which can be used to create ID source files to help move databases (but not the user database) from TITAN to Forcefield.

CSV file format (except macro logic)

The file format for all types of device (except Door/Lift Controller Macro Logic) is:

“Num”, “Device Id”

For example, a device ID file for door groups 112 and 117 would be named **doorgrp.csv** and would contain the following lines:

“112”, “Factory Rear Doors”

“117”, “Warehouse Entry Doors”

Note: It is not necessary to specify intermediate names (for example, for door groups 113 through 116 in the above example). Forcefield applies default names as described in “Device ID names” on page 67 when valid data cannot be found.

CSV file format for macro logic

The file format for Door/Lift Controller Macro Logic is:

“((DGPNum –1) * 48) + Macro Num” , “Macro Logic Id”

For example, a device ID file for door controller 1 macro 1 and door controller 2 macro 5 records would be named **contrlrm.csv** and would contain the following lines:

“1”, “Dgp 1 Macro 1”

“53”, “Dgp 2 Macro 5”

Holiday-related tasks

Holidays are valid for one calendar year and new entries are required each calendar year. Holiday is only used for Challenger timezones. Forcefield does not use the holiday indication.

Assigning an existing holiday to a Challenger

To assign an existing holiday to a Challenger panel:

1. Open the holiday programming window for the Challenger (see “Holidays” on page 290).
2. Select the first available holiday, and then click the arrow to display the holiday search window.
3. Select the required holiday, and then click Select to assign it to the Challenger panel.
4. When finished, click Save on the holiday programming window.

Assigning a new holiday to a Challenger

To create a new holiday and assign it to a Challenger:

1. Open the holiday programming window for the Challenger (see “Holidays” on page 290).
2. Double-click the first available holiday field to open the Program Holiday window.
3. Type the name of the holiday and specify the date.
4. Click Save.
5. Close the Program Holiday window. Forcefield displays the new holiday in the holiday programming window.
6. When finished, click Save on the holiday programming window for the Challenger panel.

Removing a holiday from a Challenger

To remove a time zone from a Challenger panel:

1. Open the holiday programming window for the Challenger (see “Holidays” on page 290).
2. Select the holiday to be removed, and then click Clear.
3. Click Save.

Note: This does not remove the holiday record from the holiday database, it only removes it from the current Challenger panel.

Deleting a holiday

To delete a holiday from the holiday database.

1. Open the holiday programming window for the Challenger (see “Holidays” on page 290).
2. Double-click the holiday to be deleted, to open the Program Holiday window.
3. Press F8.

Note: It is not possible to delete a holiday record from the holiday database if it is in use.

Timezone-related tasks

Assigning an existing timezone to a Challenger

To assign an existing timezone to a Challenger panel:

1. Open the timezone programming window for the Challenger (see “Timezones” on page 278).
2. Select the first available timezone, and then click the timezone arrow to display the timezone search window.



3. Select the required timezone, and then click Select to assign it to the Challenger panel.
4. When finished, click Save on the timezone programming window for the Challenger panel.

Assigning a new timezone to a Challenger

To create a new timezone and assign it to a Challenger panel:

1. Open the timezone programming window for the Challenger (see “Timezones” on page 278).
2. Double-click the first available timezone field to open the Program Timezone window.
3. Program the new timezone as described in “Timezones” on page 278.
4. Close the Program Timezone window. Forcefield displays the new timezone in the timezone programming window.
5. When finished, click Save on the timezone programming window for the Challenger panel.

Removing a timezone from a Challenger

To remove a time zone from a Challenger panel:

1. Open the timezone programming window for the Challenger (see “Timezones” on page 278).
2. Select the timezone to be removed, and then click Clear.
3. Click Save.

Note: This does not remove the timezone record from the timezone database, it merely removes it from the current Challenger panel. Timezones 0 (24 Hour) and 25 (Service In) cannot be removed from the current Challenger panel.

Deleting a timezone

To delete a time zone from the timezone database:

1. Open the timezone programming window for the Challenger (see “Timezones” on page 278).
2. Double-click the timezone to be deleted, to open the Program Timezone window.
3. Press F8.

Note: It is not possible to delete a timezone record from the timezone database if it is in use. Print a Time Zone report to see where a timezone is in use (see “Time Zone Report” on page 199).

Assigning a soft timezone to a Challenger

Soft timezones are also known as ‘Timezones to follow relays’. These are timezones that are active only when a relay is active (timezones based on events instead of on time).

To assign an existing soft timezone to a Challenger panel:

1. Select the Challenger programming option Timezones To Follow Relays to open the soft timezone programming window (see “Time Zones to Follow Relays” on page 292).
2. Select the first available soft timezone, and then click the arrow to display the relay search window.
3. Select the required relay, and then click Select to assign it to the Challenger panel.
4. When finished, click Save on the soft timezone programming window for the Challenger panel.

Removing a soft timezone from a Challenger**To remove a soft timezone to a Challenger:**

1. Select the Challenger programming option Timezones To Follow Relays to open the soft timezone programming window (see “Time Zones to Follow Relays” on page 292).
2. Select the soft timezone to be removed, and then click Clear.
3. When finished, click Save on the soft timezone programming window for the Challenger panel.

Chapter 5

Forcefield commands

Summary

This chapter describes all Forcefield command that can be accessed via the menu system (with no menu restrictions in place). Forcefield has two menu types: classic and Forcefield 6. The menu type is selected in “Configuring login options” on page 229.

Content

Introduction	77
Main menu	77
Triggering menu	77
Backups menu	85
Graphics menu	94
Guard Tour menu	106
Control menu	109
Control > Alarm Panel	111
Control > Intercoms	115
Control > Video	116
History menu	120
History > Show DVR Footage menu	125
Users menu	129
Users > Access menu	140
Users > Modify Status menu	146
Users > Profiles menu	146
Users > Reports menu	152
Users > Smart Card Programmer menu	160
Users > Transfer User Data menu	161
Users > User Numbering menu	162
Operators menu	163
Databases menu	166
Databases > Computer Equipment menu	167
Databases > Computer Equipment > Storage menu	179
Databases > Duress menu	182
Databases > Intercoms menu	184
Databases > Management Software menu	187

- Databases > Management Software > Clusters menu 187
- Databases > Management Software > Computer Categories menu 188
- Databases > Management Software > Members menu 192
- Databases > Management Software > System Events menu 194
- Databases > Third Party menu 195
- Databases > Timezones menu 199
- Databases > Video menu 200
- Databases > Video > DVR Video menu 201
- Databases > Video > Matrix Video menu 206
- Status menu 210
- Status > Alarm Panel Status menu 210
- Status > Door Status menu 211
- Status > Equipment Status menu 213
- Status > System Status menu 214
- Challenger menu 216
- Challenger > Download Challenger Data menu 221
- Admin menu 223
- Admin > Configuration menu 226
- Admin > Data Mirroring menu 246
- Admin > Tools menu 249

Introduction

The Forcefield commands listed in this chapter are listed in the order they appear in the classic Forcefield menu. See also Appendix C “Forcefield 6 menu reference” on page 307 for a list of commands in the order they appear in the Forcefield 6 menu.

Menu items displayed for an individual operator are determined by the access rights assigned to the operator (or to the workstation), and so Forcefield will typically display only a portion of the commands described in this reference.

The following sections may include the “>” character to indicate sub-menus. For example, the heading ‘Users > Access menu’ indicates that Users is the top-level menu and Access is a sub-menu.

Note: Forcefield may be configured to display the Forcefield 6 menu structure. If your Forcefield commands do not display in the same order as shown in this chapter, use the index to find specific menu options. Menu options are listed in the index in the same case as on the user interface, followed by the word “option”, for example “Logoff option”, followed by the page number.

Main menu

The following sections describe the two main menu commands (Alarm and Logoff) that do not open sub-menus.

Alarms

The Alarms option opens the Unacknowledged Alarms window. See “Unacknowledged alarms” on page 31 for details.

Logoff

The Logoff option logs off the current operator and displays the Forcefield Login window.

Triggering menu

Event Check

Use the Event Check option to program Forcefield to check whether an event has occurred at a specific time, and to do some action if the event has or hasn’t occurred. This is done by scanning the history backwards from the time of the check for the selected period.

Figure 33: Event Check programming window

The screenshot shows a software window titled "Check For Event At Time". The window has a standard Windows-style title bar with icons for close, help, refresh, save, and print. Below the title bar, there are several fields for configuring an event check:

- Id:** Check Melb Door Access Denied
- Node:** Node 1
- Type:** Once Only, Keep
- Time of next:** Hr: 9, Min: 0, Day: 7, Mon: 2, Year: 2009
- Check back for:** 8 Hours
- Initiate Actions if Event:** Occurred
- Desc:** Find user refused access - void card
- Event:** Door Access, VOID CARD BADGED
- From Challenger:** (empty dropdown)
- From DOOR/LIFT:** (empty dropdown)

An "Actions" button is located at the bottom right of the window.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Type a unique ID (name) to identify this record. The ID will be written to history when the action is triggered.

Node. Select the Forcefield node (the name may differ from that shown).

Type. Select the required frequency for the event.

- Once Only, Delete: Triggers will be removed from the database once they have been executed.
- Once Only, Keep: Triggers will become inactive, but will be kept in the database so that they can be reactivated at a later time.
- Every Day
- Day of Week
- Day of Month
- Week Days
- Weekend Days

Time of Next. Specify the hour, minute, date, month, and year at which the check is to be performed. The time specified will be the time at the selected node (Forcefield computer).

Check back for. Type a value to suit the selected minutes, hours, or days. Select the minutes, hours, or days, as needed. For example, if the check has been programmed to occur at 4:00 p.m. and the Check back for field is set to 10 minutes, then Forcefield will check if the event has occurred anywhere between 3:50 p.m. and 4:00 p.m.

Initiate Actions if Event. Select either Occurred or Did Not Occur, as needed.

Desc. Type a description (optional).

Event. Select the required event. Once an event is selected, other fields will appear depending on the event selected. Enter or select data accordingly.

Note that entering data for a device, for example, will mean that only events generated by that device will initiate triggering in Forcefield.

Actions. Click the Actions button to program the actions that will be performed. The fields available on the Action window depend on the type selected.

Event check actions

Click the Action button on the Event Check window to open a Check for Event Action window. Use the Check for Event Action window to program an action that will take place when triggered. Multiple actions can be programmed for the one event.

The fields displayed on the Check for Event Action window vary to suit the selected action type. Refer to the following sections for details of each type of action:

- “Challenger control” below
- “Video control” below
- “Auto report” on page 80
- “Generate alarm” on page 80
- “Output data to port” on page 80
- “Execute process” on page 80

Challenger control

Id. Type a unique ID (name) to identify this record. As you are able to have more than one action for each trigger, each action ID must be different. The ID will be written to history when the action is triggered.

Type. When the selected action type is Challenger control, you must also select a Challenger device.

Video control

Id. Type a unique ID (name) to identify this record. As you are able to have more than one action for each trigger, each action ID must be different. The ID will be written to history when the action is triggered.

Type. When the selected action type is Video control, you must also select a Video control action:

- Camera To Monitor
- Camera To Preset
- Trigger Video Alarm
- Reset Video Alarm
- Trigger Video Macro
- Reset Video Macro
- Set Multi View

- Recording - Start
- Recording - Stop

Note: If the Video control action is “Trigger Video Alarm”, additional fields display for entering alarm codes and data, as applicable.

Auto report

Id. Type a unique ID (name) to identify this record. As you are able to have more than one action for each trigger, each action ID must be different. The ID will be written to history when the action is triggered.

Type. When the selected action type is Auto report, you must also select an output target and a report type.

Generate alarm

Id. Type a unique ID (name) to identify this record. As you are able to have more than one action for each trigger, each action ID must be different. The ID will be written to history when the action is triggered.

Type. When the selected action type is Generate alarm, you must also enter the appropriate alarm text.

Output data to port

Id. Type a unique ID (name) to identify this record. As you are able to have more than one action for each trigger, each action ID must be different. The ID will be written to history when the action is triggered.

Type. When the selected action type is Output data to port, you must also select the required format:

- ASCII—any ASCII text characters
- HEX—data must be in hexadecimal format, for example, 01345a7f (spaces are not allowed, and the data must contain an even number of characters).

Execute process

Id. Type a unique ID (name) to identify this record. As you are able to have more than one action for each trigger, each action ID must be different. The ID will be written to history when the action is triggered.

Type. When the selected action type is Execute process, you must also select the node and specify a script.

Notes

- The process may be any binary or executable script, which will be run in the environment of the Forcefield background trigger action process.
- The process may not contain redirection, piping or other shell constructs. If these are required, create a script and run that instead.

- No error checking is performed to determine if the process was successfully executed.

Event Paging

Use the Event Paging option to program paging or e-mail actions to be activated by the notification of a Forcefield event.

Email support is built in. The email server to which aresmail will send the mail for processing must be set up by your system administrator in Forcefield Configuration. The message itself is automatically composed by Forcefield according to the event type and the Computer Category for the triggering point.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Type a unique ID (name) to identify this record. Alternatively, search for existing records to view or edit.

Description. Type a short description for this paging trigger.

Page on Event. Select an event that this trigger will use to activate actions. Once an event is selected, certain other fields will appear depending on the event selected. Enter data accordingly. Note that entering data for a device, for example, will mean that only events generated by that device will initiate triggering in Forcefield.

Note: This event must also be flagged as Allow Paging in the relevant computer category record. See Figure 65 on page 190.

Click the Destinations button to open the Paging Destination window where you can program one of the paging actions (either ASCOM Duress or E-mail) that will take place when the trigger fires. Multiple actions can be programmed for the one event.

Event Trigger

Use the Event Trigger option to program actions to be activated by the notification of a Forcefield event. After the Event Trigger has been defined and saved, the Actions button displays.

Figure 34: Triggering By Event programming window

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Type a unique ID (name) to identify this record. Alternatively, search for existing records to view or edit.

Enabled. Select the Enabled check box to enable this trigger.

Description. Type a short description for this paging trigger.

Trigger on. Select an event that this trigger will use to activate actions. Leave blank to generate the trigger for all alarms that the operator responds to or acknowledges.

For Event Task Alarm Response and Event Task Alarm Acknowledged events you may select the device that caused the alarm.

Sector (if displayed). A sector number enables Forcefield to link the event to external events such as a Teleste alarm code.

Device (if displayed). Select an item or device. The type of item or device available will depend on the event chosen. Leaving blank will match the event from all devices. Note that entering data for a device, for example, will mean that only events generated by that device will initiate triggering in Forcefield.

Actions button. Click Actions to program the actions that will be performed. The fields available on the Action window depend on the type selected.

Logic button. Click Logic to program up to eight conditions that must be satisfied in order for this trigger to function.

The Trigger Actions windows and commands are similar to the Check Actions windows described in “Event check actions” on page 79.

Time Trigger

Use the Time Trigger option to program actions to be activated at a particular time.

Figure 35: Triggering By Time programming window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Type a unique ID (name) to identify this record. The ID will be written to history when the action is triggered.

Node. The node at which the event is to be initiated. Note that the time at which the event is triggered will be from the selected node (Forcefield computer). This is important as each node may be in a different time zone.

Enabled. Select the Enabled check box to enable this trigger.

Description. Type a short description of this trigger.

Type. Select the required frequency for the event:

- Once Only, Delete (triggers will be removed from the database once they have been executed)
- Once Only, Keep (triggers will become inactive, but will be kept in the database so that they can be reactivated at a later time)
- Every Day
- Day of Week
- Day of Month
- Week Days
- Weekend Days

Time of Next. Specify the hour, minute, date, month, and year at which the check is to be performed. The time specified will be the time at the selected node (Forcefield computer).

After the time trigger has been defined and saved, the Actions button appears.

Actions button. Click Actions to program the actions that will be performed. The fields available on the Action window depend on the type selected.

The Trigger Actions windows are similar to those described in “Event check actions” on page 79. Triggering by time does not include a Generate Alarm action, but there are two additional actions that can be triggered by time:

- “User data export” on page 84
- “User photo export” on page 84

Logic button. Click Logic to program up to eight conditions that must be satisfied in order for this trigger to function.

User data export

The “user data export” timed trigger action provides the following functionality:

When the action type is once only, then Forcefield exports the full user data in CSV format, starting at the designated time, similar to manually exporting user data (see “Export User Data” on page 161).

When the action type is recurring or periodic (such as every day), then Forcefield exports only the data that has been added or changed in the past week (for example).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Type a unique ID (name) to identify this record. As you are able to have more than one action for each trigger, each action ID must be different. The ID will be written to history when the action is triggered.

Type. When the selected action type is User Data Export, you must also specify an export destination (report storage device), typically a Samba (CIFS) location.

User photo export

When the action type is once only, then Forcefield exports all user photos, starting at the designated time.

When the action type is recurring or periodic (such as every day), then Forcefield exports only the data that has been added or changed in the past week (for example).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Type a unique ID (name) to identify this record. As you are able to have more than one action for each trigger, each action ID must be different. The ID will be written to history when the action is triggered.

Type. When the selected action type is User Photo Export, you must also specify an export destination (report storage device), typically a Samba (CIFS) location.

Event Check Report

Use the Event Check Report option to generate reports listing programmed event checks and associated actions.

Refer to “Generating reports” on page 28, and the following details about this report.

Trigger Id. Leave this field blank to generate a report for all records or select one or more triggers.

Event Paging Report

Use the Event Paging Report option to generate reports listing programmed paging events and associated actions.

Refer to “Generating reports” on page 28, and the following details about this report.

Trigger Id. Leave this field blank to generate a report for all records or select one or more triggers.

Event Trigger Report

Use the Event Trigger Report option to generate reports listing programmed event triggers and associated actions.

Refer to “Generating reports” on page 28, and the following details about this report.

Trigger Id. Leave this field blank to generate a report for all records or select one or more triggers.

Time Trigger Report

Use the Time Trigger Report option to generate reports listing programmed time triggers and associated actions.

Refer to “Generating reports” on page 28, and the following details about this report.

Trigger Id. Leave this field blank to generate a report for all records or select one or more triggers.

Backups menu

The Backups options are described on the following pages:

- Use “Auto Database Backup” on page 86 to automate the archiving of Forcefield databases.
- Use “Auto History Backup” on page 87 to automate the archiving and purging of history data from Forcefield.
- Use “Auto History Export” on page 88 to protect Forcefield databases and/or configuration data.
- Use “System Backup” on page 89 to automate the archiving and purging of history data from Forcefield in CSV format.

- Use “Backup History” on page 90 to protect Forcefield history.
- Use “Convert 4.5.x Database” on page 91 to convert an ARES 4.5.x backup database into a Forcefield database.
- Use “Delete Database Archive” on page 91 to remove a database archive that has previously been created when a database backup has been performed.
- Use “Delete History Archive” on page 92 to remove a history archive that has previously been created when a history backup has been performed.
- Use “Export History” on page 92 to export history data from Forcefield in CSV format.
- Use “Export History Archive” on page 92 to create a CSV file from a history archive that has previously been created when a history backup has been performed.
- Use “Format Disk” on page 93 to prepare a storage device such as an IBM-formatted disk for use in QNX. This option is available only on Forcefield Enterprise nodes.
- Use “Purge History” on page 93 to delete selected history from the hard disk.
- Use “System Restore” on page 93 to restore the system’s database to the last backup date.

Auto Database Backup

Use the Auto Database Backup option to automate the archiving of Forcefield databases.

Figure 36: Auto Database Backup programming window



Click Run to make the scheduled backup 'currently active'.

Press F8 to remove the automatic backup from the schedule.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Backup Type. Select the desired frequency of archiving:

- Daily
- Weekly
- Monthly

- Periodic (and then specify the number of days)

Backup To. Select the required storage device for the backup (backing up to remote storage is recommended). The archives are available for reporting and backing up to offline media, and each archive is created in a separate directory. Selecting the Forcefield server hard disk allows for archiving of previous history backups.

Note: The 'Backup to' storage device must be available at the specified backup time and the entire backup must fit onto one device because there is no provision for operator intervention for auto backups.

Use Data Compression. If selected, Forcefield will compress the backup data. This will take longer to achieve than a uncompressed back up. It will also temporarily use hard disk space while compressing data for storage.

Note: In the event of a defect in the storage medium, uncompressed data is typically easier to recover than compressed data.

Archive Previous Backup. This field is visible only when the Forcefield server hard disk is selected in the Backup To field. Right-click to copy the existing archive, if any, to a dated archive. The archive is available for later restoral if required.

When a scheduled backup is 'currently active', an icon displays on the main window (see "Automatic activity icons" on page 18).

Auto History Backup

Use the Auto History Backup & Purge option to automate the archiving and purging of history data from Forcefield.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Backup Interval. Select the desired interval of archiving history data:

- Daily
- Weekly
- Monthly
- Periodic (and then specify the number of days)

Only the selected interval will be backed up. For example, if the interval is weekly, then history records for the past week will be backed up.

Backup From. Optionally specify a number of days or weeks before the start of the interval to allow for overlapping backup data by adjusting the start date of the export data by the time specified. For example, if the interval is daily and you specify 1 month, then the backup will contain data from the month before the specified interval, plus the day's data.

Backup To. Select the required storage device for the backup (backing up to remote storage is recommended). The archives are available for reporting and backing up to offline media, and each archive is created in a separate directory. Selecting the Forcefield server hard disk or a Samba (CIFS) location allows for archiving of previous history backups.

Note: The 'Backup to' storage device must be available at the specified backup time and the entire backup must fit onto one device because there is no provision for operator intervention for auto-backups.

Backup Type. Select the required storage device for the backup.

- Append—adds history to a previous backup.
- Overwrite—any current backup is deleted. Selecting Archive Previous Backup automatically selects Overwrite.

Archive Previous Backup. This field is visible only when backing up to the Forcefield server hard disk or a Samba (CIFS) location). Right-click to copy the existing archive, if any, to a dated archive. The archive is available for later restoral if required. Selecting this option makes the Backup Type Overwrite.

Purge Type. Select Older Than or All.

- Select Older Than and then specify a number of days to remove only records older than the record age. For example, if number of days is 90, then the purging process will delete all records older than 90 days (from the date that the purging operation is performed).
- Select All to purge (delete) all history records.

If you wish to purge all history records without backing up history data, select a Purge Type of All and leave the Backup To field blank. Otherwise, the specified history data will be backed up prior to being purged.

When a scheduled backup is 'currently active', an icon displays on the main window (see "Automatic activity icons" on page 18).

Auto History Export

Use the Auto History Export option to automate the archiving and purging of history data from Forcefield in CSV format.

Common window elements are described in Section 3. Elements specific to this window are described below.

Export Interval. Select the desired interval of archiving history data:

- Daily
- Weekly
- Monthly
- Periodic (and then specify the number of days)

Only the selected interval will be exported. For example, if the interval is weekly, then history records for the past week will be exported.

Export From. Optionally specify a number of days or weeks before the start of the interval to allow for overlapping export data by adjusting the start date of the export data by the time specified. For example, if the interval is monthly and you specify 1 day, then the export will contain data from the day before the specified date, plus the month's data.

Export to. Select the required storage device onto which the history records will be exported. Leave the Export To field blank if you want to purge history records without backing up history data.

Note: The 'Export to' storage device must be available at the specified export time and the entire export must fit onto one device because there is no provision for operator intervention for auto export.

In format. Select, as required:

- CSV – Raw: all data in the specified records 'as is', with date and time data not in human-readable format.
- CSV – Formatted: Type a selection of data, with date and time data converted to human-readable format.

Purge Type. Select Older Than or All.

- Select Older Than and then specify a number of days to remove only records older than the record age. For example, if number of days is 90, then the purging process will delete all records older than 90 days (from the date that the purging operation is performed).
- Select All to purge (delete) all history records.

When a scheduled export is 'currently active', an icon displays on the main window (see "Automatic activity icons" on page 18).

System Backup

Use the System Backup option to protect Forcefield databases and/or configuration data.

Common window elements are described in Section 3. Elements specific to this window are described below.

BACKUP. Select the type of backup you wish to perform:

- Databases—typically includes Forcefield databases, graphics and user files.
- Hardware Config—typically includes Forcefield hardware related files, such as netmap files, TCP/IP config files.

The selection of backup files is configurable by the Forcefield system administrator.

Use Data Compression. If selected, Forcefield will compress the backup data.

This will take longer to achieve than a un-compressed back up. It will also temporarily use hard disk space while compressing data for storage.

Note: In the event of a defect in the storage medium, uncompressed data is typically easier to recover than compressed data.

Backup To. Select the required storage device for the backup (backing up to remote storage is recommended). Selecting the Forcefield server hard disk allows for archiving of previous history backups.

Note: Backup Data will automatically delete any previous backups (file names BU_DB*) in the selected storage device. Move or rename previous backup files if you want to keep them.

Archive Previous Backup. This field is visible only when the Forcefield server hard disk is selected in the Backup To field. Right-click to copy the existing archive, if any, to a dated archive. The archive is available for later restoral if required.

Backup History

Every action that Forcefield encounters is stored as history. The history created between two dates can be backed up for future reference. Backing up requires that the information in history be copied to a storage device.

Use the Backup History option to protect Forcefield history.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

From. Specify the day, month, and year that defines the beginning of the interval that you want to back up. The interval begins on the specified date at the time 00:00:00.

To. Specify the day, month, and year that defines the end of the interval that you want to back up. The interval ends on the specified date at the time 23:59:59.

Backup To. Select the required storage device for the backup (backing up to remote storage is recommended). The archives are available for reporting and backing up to offline media, and each archive is created in a separate directory. Selecting the Forcefield server hard disk or a Samba (CIFS) location allows for archiving of previous history backups.

Archive Previous Backup. This field is visible only when backing up to the Forcefield server hard disk or a Samba (CIFS) location). Right-click to copy the existing archive, if any, to a dated archive for later restoral, for use in Offline History reports, or for backing up to offline storage media by using the Backup History Archive function.

Convert 4.5.x Database

Use the Convert 4.5.x Database option to convert an Ares 4.5.x database backup into a Forcefield database (overwriting the existing Forcefield database).

Transfer the 4.5.x database backup to the Forcefield client computer by one of the following methods:

- Use a sufficiently-large ZIP drive so that the database fits on a single media.
- Use FTP to transfer the backup database from Ares 4.5.x to the Forcefield client computer.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

From Storage. Select the storage device where the backup is stored.

Profile Option. Select the appropriate profile option for the conversion:

- **Common group access.** The conversion program tries to match all the users that have the same access and create a single profile for these users. The profile ID is automatically generated by the conversion program, such as “User Profile 1”, “User Profile 2”, and so on.
- **One profile per user:** The conversion program assigns each user an individual profile. The profile ID is automatically generated by the conversion program, such as “User Profile 1” for user 1, “User Profile 2” for user 2, and so on.
- **Don’t create profile:** The conversion program assigns each user with the default profile, “No Access Profile~”.

Ignore User Department. If selected, the department field will be blank for all the users after the conversion.

Delete Database Archive

Use the Delete Database Archive option to remove a database archive that has previously been created when a database backup has been performed.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Type. Select the type of backup you wish to perform (Forcefield databases or Hardware Config):

- Forcefield databases typically includes Forcefield databases, graphics and user files
- Hardware Config typically includes Forcefield hardware related files, such as netmap files and TCP/IP config files.

From. Select the device where the archive is stored. The archives contained on the device will be listed along with the date the archive was made. Select the one you wish to delete.

Delete History Archive

Use the Delete History Archive option to remove a history archive that has previously been created when a history backup has been performed.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

From. Select the device where the archive is stored. The archives contained on the device will be listed along with the date the archive was made. Select the one you wish to delete.

Export History

Use the Export History option to export history data from Forcefield in CSV format.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Note: This command performs the same function as running a History report, but provides no filtering: all records in the selected range will be exported.

From. Specify the day, month, and year that defines the beginning of the interval that you want to back up. The interval begins on the specified date at the time 00:00:00.

To. Specify the day, month, and year that defines the end of the interval that you want to back up. The interval ends on the specified date at the time 23:59:59.

Export to. Select the required storage device onto which the history records will be exported.

In Format. Select, as required:

- **CSV – Raw:** All data in the specified records ‘as is’, with date and time data not in human-readable format.
- **CSV – Formatted:** A selection of data, with date and time data converted to human-readable format.

Export History Archive

Use the Export History Archive option to create a CSV file from a history archive that has previously been created when a history backup has been performed.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

From. Select the device where the archive is stored. The archives contained on the device will be listed. Forcefield will display the date the archive was made. Select the one you wish to delete.

To. Select the required storage device onto which the history records will be exported.

In format. Select, as required:

- CSV – Raw: All data in the specified records ‘as is’, with date and time data not in human-readable format.
- CSV – Formatted: A selection of data, with date and time data converted to human-readable format.

Delete Archive on Completion. Select this check box to remove the selected history archive after the export has been performed.

Format Disk

Use the Format Disk option to prepare a selected device (e.g. an IBM-formatted disk) for use in QNX for backup, storage, etc. This command is available only on a Forcefield Enterprise node’s user interface.

The command removes all data on the specified device.

Purge History

Use the Purge History option to delete selected history from the hard disk.

Purge History deletes all of the history from the system hard disk between the requested dates.

Note: Before performing a purge, ensure that you have backed up the selected range of history you wish to purge.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

From. Specify the day, month, and year that defines the beginning of the interval that you want to back up. The interval begins on the specified date at the time 00:00:00.

To. Specify the day, month, and year that defines the end of the interval that you want to back up. The interval ends on the specified date at the time 23:59:59.

If history in this date range has not been previously backed up, you will be prompted to confirm that the purge should continue.

System Restore

Use the System Restore option to restore the system’s database to the last backup date. This is where the storage devices selected during Backup Database are used, so it is important to properly number and date backed-up information. Restoring the database should only be used after consulting your Installation Company.

Running this process will restore previously backed up data. After copying the data to the system disk, the restore will shutdown and restart Forcefield.

Note: Restore Data should only be used as a recovery if the Forcefield computer has crashed or there has been a system failure. You will need the Forcefield License CD or USB device in order to complete this process.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Restore. Select the type of backup you wish to restore:

- Databases—typically includes Forcefield databases, graphics files, user photos, user notes, user card design layouts, alarm help files, report templates, and backup configurations.
- Hardware Config—typically includes the QNX system configuration files, such as netmap files, TCP/IP config files. The files restored include all the files in the following directories:

/etc

/etc/ppp

/etc/config

/etc/config/trap

Only to Node. Select the required node.

From. Select the device where the archive is stored. The archives contained on the device will be listed. Forcefield will display the date the archive was made. Select the archive from which you want to restore.

Graphics menu

Overview

Use the Graphics menu options to create Forcefield maps: interactive graphical interfaces by which an operator can monitor alarms and control the security system.

Note: Door inputs do not have to be placed on graphic maps. Forcefield internally redirects input events to door events for any input associated with a door. Placing these inputs onto the map clutters the map and unnecessarily takes one of the allowed LAP slots allowed per map.

A Forcefield map consists of a background drawing (either created or imported) plus one or more of the following elements:

- **Single LAP (Live Animation Point).** Indicates position and status of a single device under control of Forcefield.
- **Multiple LAPs.** Indicates alarm status of one or many devices under control of Forcefield. Multiple LAPs display only when in an alarm state.
- **Jump Zones.** A shortcut to another map.

- **Alarm Zones.** An alarm zone is typically used on a top-level map (e.g. a city map). The alarm zone is not visible until one of the points associated with the alarm zone is in alarm. Then, clicking on the (now visible) alarm zone opens the particular map (e.g. a building) that displays the alarm. If more than one of the points associated with the alarm zone is in alarm, clicking on the alarm zone opens the map with the highest priority alarm.
- **Event Macro.** Clicking on an Event Macro icon causes an event, which Forcefield can use to perform event triggering. There are a possible 256 event macros.
- **Event Macro with Confirmation.** Similar to Event Macro except that confirmation is required before issuing the trigger.

Note: A maximum of 100 LAPs can exist on a map. Any item can only be placed on up to 10 maps.

Different icons on the maps are used to indicate the position of doors, PIR detectors, arming stations, readers, etc. The various states of alarms, isolates, tampers or seals are displayed on the maps by changing the colour of the icon to indicate the condition of the point:

- **Flashing Red** indicates that an alarm has occurred, but has not been acknowledged or restored.
- **Steady Red** indicates that an area is armed.
- **Flashing Green** indicates that an alarm has been reset, but has not been handled by the operator.
- **Steady Green** indicates that an area is disarmed or a door is unlocked.
- **Dark Orange** indicates that a door is disabled.
- **Purple** indicates that an alarm has been acknowledged and is waiting to be restored.
- **Yellow** indicates that a point has been isolated.
- **Blue** indicates that a relay is active, or intercom audio is being monitored.
- **Flashing Pink** indicates that an intercom call is waiting to be answered.
- **Steady Pink** indicates that an intercom call is connected (audio channel opened).

The overall process of creating Forcefield maps is:

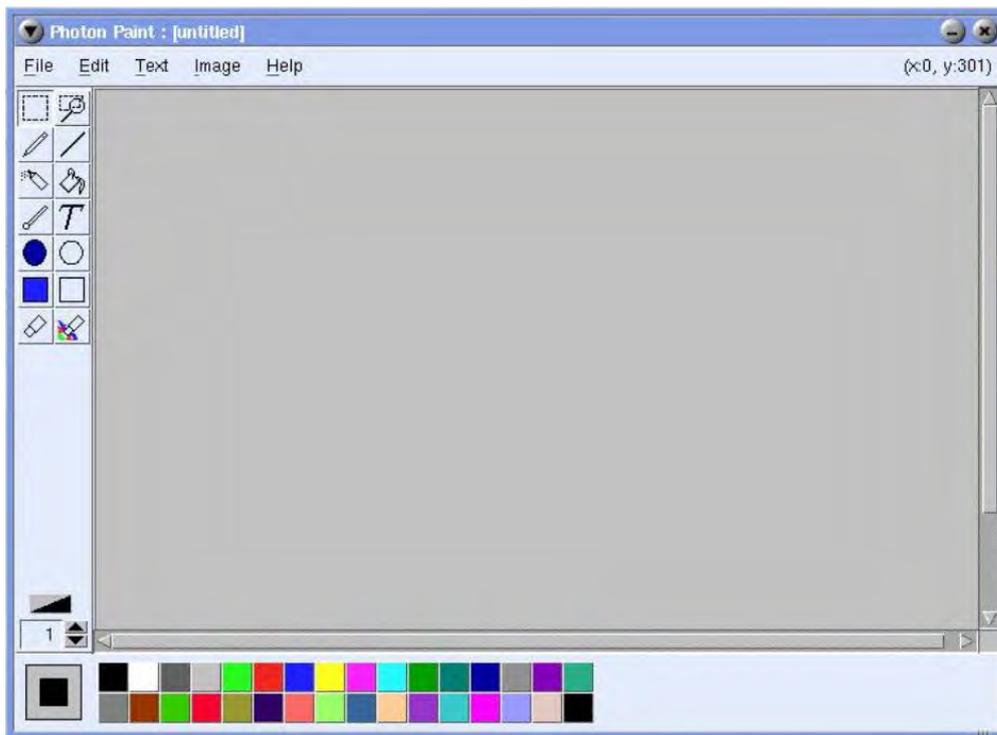
1. Draw or import a map background. The background for a Forcefield map must be a Windows picture file (.bmp), and may be created using the following methods:
 - Use Background Editor to draw a picture.
 - Use Convert DXF to Map to create a background from a .dxf format file created in a drawing application such as AutoCAD (version 12 or below).

2. Use Map Database to add the map background to the Forcefield map database.
3. Use LAP Editor to add LAPs to the map.

Background Editor

Use the Background Editor option to draw a map's background (available on the Forcefield server only).

Figure 37: Background Editor window



Save the map as a .bmp file in the folder /usr/ares/graphics/ using a unique number from 1 to 65535. The .bmp file name will correspond to the map number in the database, e.g. the background file '45.bmp' corresponds to map 45.

Note: In Forcefield, maps numbers 1, 01, 001, and so on are considered the same map number. In previous Forcefield versions, maps 1 and 01 could both exist as separate maps.

The file must be added to the map database before it can be used in Forcefield. See "Map Database" on page 105.

Convert DXF to Map

Use the Convert DXF to Map option to create a background from a .dxf format file created in a drawing application such as AutoCAD (version 12 or lower).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

To enter the map into the Forcefield database:

1. In the Id field select the device where Forcefield will search for the .dxf files to convert.
2. Click Run, and then select the required .dxf file. Forcefield converts the .dxf file to a .bmp file. Forcefield displays a dialog box.
3. Enter the required map number. The .bmp file name will correspond to the map number in the database, e.g. the background file '45.bmp' corresponds to map 45. Forcefield stores the .bmp file and displays the Map Database programming screen.
4. Enter a map description and then click Run.

Display Map

Use the Display Map option to display the map designated as the default map for the workstation (see “Workstation options—graphics” on page 175).

Figure 38: Display map window (example map only)



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Maps have buttons at the top of the window:

- Click Quit to close the map window.

- Click Map to select a different map
- Click Refresh to reload the map.

Security devices are represented by LAPs or graphic images on the map. Click a LAP to view the available menu for the LAP. See Figure 16 on page 31 for an example of a LAP menu.

Listed alphabetically, LAP menu options may include:

Alarm. Opens the Alarm Details window for the device in alarm.

Door Lock Override. Allows the operator to specify time periods when the door should be unlocked, together with optional areas that should be disarmed. This allows Forcefield to override the normal override timezone programming that controls when the door is normally locked or unlocked. Multiple overrides may be specified for a door. See “Door Lock Override” on page 111 for details.

Floor Status. Provides details of the current status of a floor.

Last User. Provides the identity of the last user to access the door, along with the time and date of access.

Next. Allows the operator to zoom in to the next map level of the selected point. If another level of map has been programmed to this point, the screen will zoom to the next map.

Remote. Allows the operator to quickly perform system functions on the selected point. The actual functions that are displayed will vary depending on the type of point selected (e.g. Input, Door, Area, RAS, DGP, etc.) and upon the operator’s permissions.

Previous. Allows the operator to zoom out to the next map level of the selected point. If another level of map has been programmed to this point, the screen will zoom to the previous map.

Status. Provides details of the current status registered on the Forcefield system of a selected point on the graphics map. A display will appear that shows the current status of the point. Click OK to clear the status window.

Unlock Times. Provides details of the current lock, unlock, or unlock times of a door.

Update Status. Allows the operator to send a status request to the appropriate Challenger, in order to receive an update on the status of a selected point. A request is sent to the selected point to return its current status to Forcefield. It does not result in any information being returned to the operator. (Not applicable to dialler connected Challenger panels.)

User Activity. Provides details of the user access (or attempted access) for the door in the current day, past 24 hours, or past week.

Video. Depending on the type of equipment represented by the LAP:

- A device camera—switches the video camera assigned to the equipment represented by the LAP, to the workstation’s first Spot Monitor (which is associated to the same video switcher as the camera).

- Intercom—switches the video camera assigned to the intercom to the workstation's intercom monitor.
- Video Camera—clicking on it will display a selection list of the workstation's monitors (the list is not used if there is only one monitor). Selecting the monitor will then switch the video from the camera to the selected monitor.
- DVR Camera—click to select live footage or recorded footage for today, the past 24 hours, or the past 7 days.

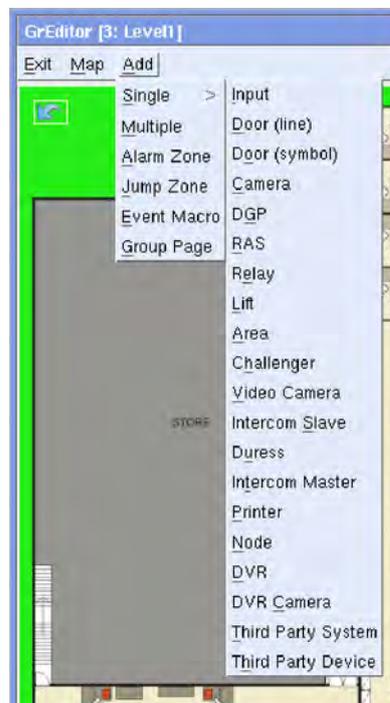
Edit Map

Use the Edit Map option to create Forcefield maps by adding points.

The Edit Map window has the following buttons at the top:

- Click Exit to close the map window.
- Click Map to:
 - Open a map.
 - Save an edited map.
 - Refresh (reload) the map.
- Click Add to place a LAP image on the map and assign functions to it (see the Add menu in Figure 39 below).

Figure 39: Map edit window (adding a 'single' type of LAP)



Right-click a LAP to view the LAP menu. LAP menu options are:

- Properties. Opens the Properties window for the LAP so that you can edit the properties, or add and remove points from multiple icons.

- Copy. Quickly place another point of the same type on the map.
- Erase. Remove the LAP from the map.
- To Back. Change the order in which LAPs appear on the map.

Adding a single point

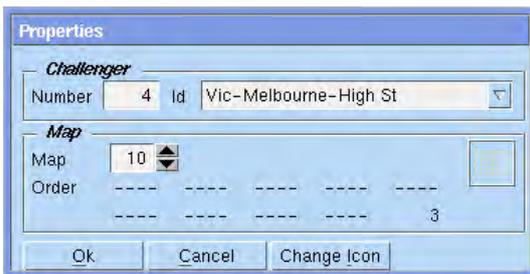
Use the Add > Single option to add new icons to a graphics map.

To add an individual point:

1. Click Add, click Single, and then select the required point type (see Figure 39 on page 99).
2. If the Symbols window shown below displays a suitable image, select the LAP image required and click OK. If you don't see the image you need, use LAP Editor to create a new image.



3. Click the map to insert the LAP (you can move it later). If the point is an area, click the map with the mouse to define up to nine corners of the area (ending up at the first corner). The Properties window displays.



4. In the Properties window, select the required Challenger panel.

The selection list for the device will display only the devices available for selection (devices already assigned to this map are not shown). Each point can be included in up to 10 maps. Any other maps that this point already appears on will be indicated by map number(s) in the map allocation list. The position of the map number indicates the map order (or zoom level) specified for each map. To allocate the point to the current map displayed, type in the map order number for the point on this particular map and click OK.

5. Click Map > Save to save the edited map.

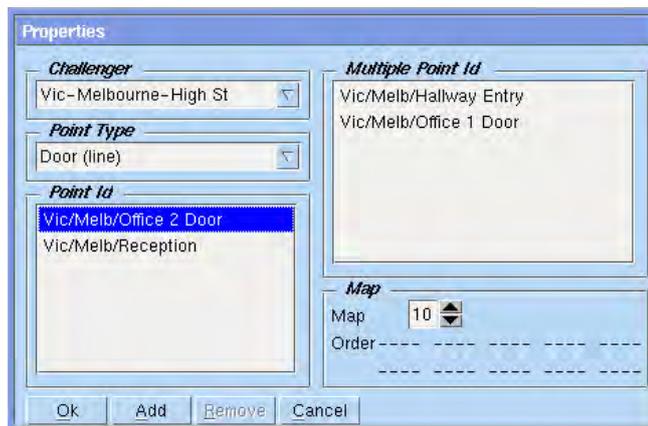
Adding a multiple point

Use the Add > Multiple option to create an icon on the graphics map that represents multiple points, e.g. where a map of a large area (state, city, large site, etc.) is used as the highest map level.

Multiple icons can represent all the points in a particular site or building. Represented on the map by a coloured circle or square, the multiple icon displays only when one or more of the points defined to the multiple icon is in alarm.

To add a multiple point:

1. Click Add, click Multiple, and then click the map to insert the multiple icon (you can move it later). The Properties window displays.



2. In the Properties window, select the required Challenger panel.

The selection list for the device will display only the devices available for selection (devices already assigned to this map are not shown). Each point can be included in up to four maps. Any other maps that this point already appears on will be indicated by map number(s) in the map allocation list. The position of the map number indicates the map order (or zoom level) specified for each map. To allocate the point to the current map displayed, type in the map order number for the point on this particular map,

3. Select a Point ID and click Add. Forcefield moves the Point ID to the Multiple Point ID list.
4. Repeat the selection of Challenger, Point Type, and Point ID, to add points to the Multiple Point ID list.
5. When finished click OK.
6. Click Map > Save to save the edited map.

Import Bitmap File

Use the Import Bitmap File option to create a background from a .bmp format file.

Common window elements are described in Section 3. Elements specific to this window are described below.

To import a bitmap file:

1. In the Id field select the device where Forcefield will search for .bmp files.
To create a storage location on the client computer, refer to the “Setting up an export/import folder on a Windows computer” section in the *Forcefield External Interfaces Manual*.
2. After selecting the device, click Run. Forcefield displays a File Selector window.
3. On the File Selector, select the required .bmp file, and then click Import. Forcefield displays the Map Database window.
4. Enter the required map number and ID. The .bmp file name will correspond to the map number in the database, e.g. the background file ‘45.bmp’ corresponds to map 45. Forcefield stores the .bmp file and displays the File Selector window to import additional .bmp files, if required.
5. When finished importing .bmp files, click Cancel on the File Selector window to close the window.

Import LAP Icon

Use the Import LAP Icon option to import symbols for use on Forcefield maps. Refer to “Edit Map” on page 99 for details about how to add a LAP icon to a map. In order to be available for graphics display, imported LAP icons must be stored in the default directory `/usr/ares/graphics/symbols/`.

Common window elements are described in Section 3. Elements specific to this window are described below.

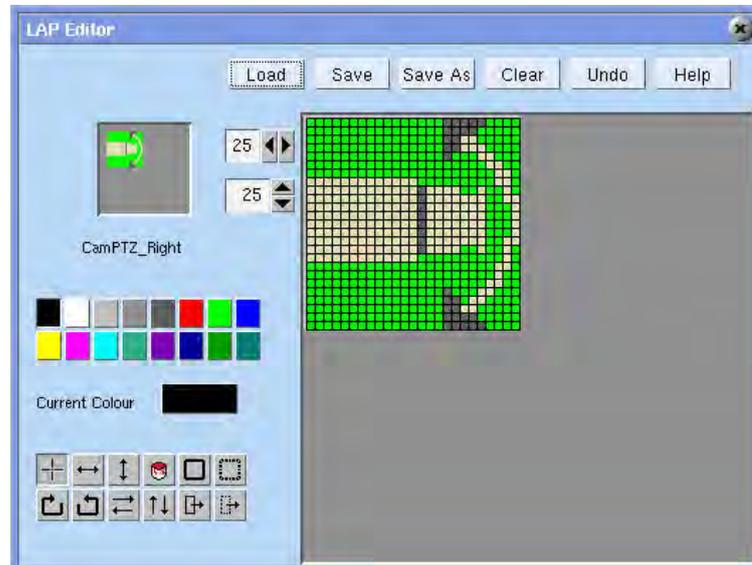
To import a LAP icon:

1. In the Id field select the device where Forcefield will search for .bmp files (52 x 52 pixels or smaller).
To create a storage location on the client computer, refer to the “Setting up an export/import folder on a Windows computer” section in *Forcefield External Interfaces Manual*.
2. After selecting the device, click Run. Forcefield displays a File Selector window.
3. On the File Selector, select the required .bmp file, and then click Import.
4. Forcefield stores the .bmp file and displays the File Selector window to import additional .bmp files, if required.
5. When finished importing .bmp files, click Cancel on the File Selector window to close the window.

LAP Editor

Use the LAP Editor option to modify or create symbols for use on Forcefield maps.

Figure 40: LAP Editor window



Symbols created with this editor can be any size from 2 x 2 to 52 x 52 pixels. They are actually created 2 pixels larger than selected, with a 1 pixel transparent border to allow for the various status colours to be displayed on the LAPs.

The default directory for these symbols is `/usr/ares/graphics/symbols/`. This location may be altered in the Save and Save As options but they will not be available for graphics display if they are not in the default directory.

The screen shows six function buttons, a work area, a display area, two size selection widgets, colour and tool selection buttons. The function buttons are:

- **Load.** Opens the file selection screen and loads the symbol from the selected file. No checking is done for unsaved data. This operation will overwrite any current data in the work area.
- **Save.** Saves the current symbol from the work area using the current filename. If there is no current filename the operation does nothing.
- **Save As.** Saves the current symbol from the work area using the filename selected from the file selection screen or a new filename entered.
- **Clear.** Clears the work and display areas.
- **Undo.** Goes back one drawing operation.
- **Help.** Displays the LAP Editor help.

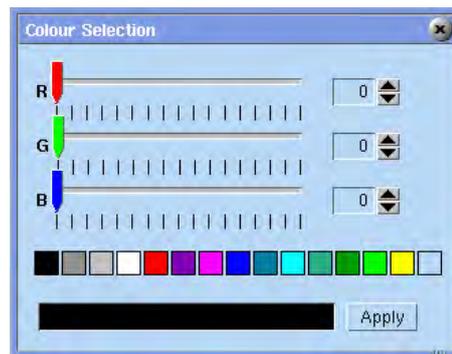
Size selection

Select the required row and column sizes by entering the value or by clicking the up/down buttons. Remember that the final symbol size will be 2 pixels larger in each direction for the transparent border.

Colour selection

The default colour palette is two rows of buttons representing the default colours. To select a non-default colour, Click the Current Colour button to bring up the colour selection widget.

Figure 41: LAP Editor window (colour selection)



To make a pixel transparent use the right mouse button in pencil mode.

Drawing Tools

Hold the cursor above a button to display the name of the button. Twelve buttons select the drawing options:

Pencil: Replaces the colour of the pixel under the cursor with the current colour for left click, transparent for right click.

Horizontal Line: Replaces the colour of the entire row under the cursor with the current colour.

Vertical Line: Replaces the colour of the entire column under the cursor with the current colour.

Paint: Replaces the colour of all pixels having the colour of the pixel under the cursor with the current colour.

Add Rectangle: Drag a rectangle, upon release the rectangle is drawn in the current colour.

Cut Rectangle: Drag a rectangle, upon release the rectangle is set to transparent the other drawing tools select operations on the current symbol.

Rotate Clockwise: The symbol is rotated 90 degrees clockwise around its centre.

Rotate Anti-clockwise: The symbol is rotated 90 degrees anti-clockwise around its centre.

Flip Horizontal: The symbol is mirror image reversed around the vertical axis.

Flip Vertical: The symbol is mirror image reversed around the horizontal axis.

Copy and Move: First an area is selected with a drag operation, then the upper left hand corner of the destination is chosen. The original area is copied to the destination.

Cut and Move: First an area is selected with a drag operation, then the upper left hand corner of the destination is chosen. The original area is made transparent and the original area is drawn to the destination.

Map Database

Use the Map Database option to add a map to the map database. All maps used by Forcefield must be entered in the map database.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

No.. Enter the map number for the .bmp file. The .bmp file name will correspond to the map number in the database, e.g. the background file '45.bmp' corresponds to map 45.

Id. Enter a name for the map. The name does not have to be unique as the map is identified by its number.

To delete a map, select the map and press F8 (Delete). Forcefield deletes the map and all its LAPs.

LAP Report

Use the LAP Report option to view an analysis of selected maps.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

For each map, the information reported includes:

- Point IDs
- Point type
- Order assigned
- Symbol assigned
- Jump Zones (links) to other maps

Guard Tour menu

Overview

A guard tour is a defined series of checkpoints at which a security guard must check in, within specified time intervals. Failure to check in on time triggers an alarm or other event.

Forcefield allows the programming of 1000 guard tours. Each guard tour contains a list of up to 1000 checkpoints (events) that a user must generate within time restrictions. Alarms will be generated (depending on the computer category) when a checkpoint event arrives late or early. The behaviour of the tour depends on its type.

A guard tour may be started by:

- A Forcefield operator who assigns a specific user to the tour.
- An event trigger, such as a guard badging a specified reader. See “Event Trigger” on page 81 for details.

Guard Tour Control

Use the Guard Tour Control option to control guard tours for a specified user.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Click List to view the status of all running guard tours.

Id. Select the required guard tour. A tour that is already running may not be selected again.

User. Select the user who will be performing this guard tour. A user already conducting a tour may not be selected for another tour.

Check Points button. Click to list the checkpoints for this guard tour.

Refresh button. Click to update the status field.

Start button. Click to start the tour.

Stop button. Click to stop the tour.

Pause button. Click to pause the tour. The tour will pause, waiting for an operator to either resume or restart it.

Resume button. Click to resume the tour from where it was paused.

Restart button. Click to restart the tour from the beginning.

Guard Tour Program

Use the Guard Tour Program option to program guard tours.

Figure 42: Guard Tour programming window (sequence order tour)



Figure 43: Guard Tour programming window (random order tour)



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Tour Id. Choose an appropriate name for the guard tour. This name will be reported in history and in any alarms generated by the tour.

Check Points button. Once a guard tour record is selected, pressing this button takes you to the Check Points programming window (see Figure 44 on page 108 and Figure 45 on page 108).

Description. Type a short description of the tour. This description will appear on any alarm detail generated by the tour.

Member. Select a member for this guard tour. An operator without access to this member will not be able to initiate, control or view this tour.

Computer Cat. Select the category suitable for the tour.

Help. Specify instructions for any alarm generated by the tour.

Type. There are two types of guard tours:

- **Sequence order** (Figure 42 above). The checkpoints must occur in the order specified. An early event will generate an alarm and the tour will continue. A late event will generate an alarm and the tour will pause, waiting for the late event. It will then continue.

- Random order (Figure 43 on page 107). The checkpoint events can take place in any order. All checkpoint events must be completed within the times specified. A late or early event will cause the tour to generate an alarm and abort. For Random type Guard tours, additional fields display for programming the minimum and maximum completion times.

Programming check points

On the Guard Tour programming windows (see Figure 42 on page 107 and Figure 43 on page 107) click the Check Points button to program the guard tour check points.

Figure 44: Check Points programming window for sequence order guard tour



Figure 45: Check Points programming window for random guard tour



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Sequence. Each checkpoint must be assigned a number. For sequential tours the events must be in this order, for random tours the number is still required, but the events may occur in any order.

Id. This is the ID that will be displayed in history and guard tour alarms.

Type. Select the type of event required for this check point.

Challenger. Select the Challenger to filter the selection of devices.

Device Id. Select the device for the check point, this cannot be blank.

Event. Select the event for the checkpoint. This will depend on the type of device selected.

Note: When selecting events for guard tour checkpoints, be aware that not all Challenger events identify the user (e.g. input unsealed event). In order to check the identity of the person passing a checkpoint ensure that only user-specific events are selected (e.g. door access granted). Events that require that a card or PIN to be used are typically user-specific events.

Minimum Interval Time field (for sequence order guard tours). This is the minimum allowed time for this checkpoint. The time starts from the arrival of the previous event or the start of the tour.

Maximum Interval Time field (for sequence order guard tours). This is the maximum allowed time for this checkpoint. The time starts from the arrival of the previous event or the start of the tour.

Guard Tour Report

Use the Guard Tour Report option to create reports about programmed guard tours.

Refer to “Generating reports” on page 28 for details.

Control menu

The control menu allows authorised operators to perform actions on the Challenger field equipment remotely. See “Controlling the security system remotely” on page 42 for additional details.

New Alarm or Call

The New Alarm or Call command is typically added to the Speed Bar as a button.

The New Alarm or Call Speed Bar button flashes when either an alarm occurs or when an intercom call arrives. Click the button to open the alarm screen or intercom window, for whichever item has the highest priority. For items of equal priority, the oldest is opened first.

Area

Areas can be remotely controlled according to timezones, user access and so on, but often it is necessary for alterations due to unusual work procedures. Use the Area option to perform remote control actions.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Actions performed on one or more areas include:

- Secure—To arm the intrusion detection devices in the selected areas.
- Access—To disarm the intrusion detection devices in the selected areas and allow users to gain access without activating alarms.
- Update Status—a request is sent to the selected item to return its current status to Forcefield. If the Update Status command fails, Forcefield displays an error message.

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

Door

This command allows the operator to remotely lock or unlock doors (or perform other actions described below). Use the Door option to perform remote control actions.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Actions performed on doors include:

- Open Door. Open doors for the unlock period set in Challenger menu options.
- Open Door for a Time. Open doors for a time period set by the operator.
- Unlock Door. Unlock doors until a lock command occurs.
- Lock Door. Lock doors until an unlock command occurs.
- Disable Door. Holds doors disabled, or unmanageable through Forcefield or a Challenger, until the Enable Door command is used.
- Enable Door. Re-enable doors and allow them to be controlled through Forcefield or a Challenger.
- Default Lock State. Sets doors to the defined default state (locked or unlocked).
- Update Door Status. Sends a request to the selected item to return its current status to Forcefield. If the Update Status command fails, Forcefield displays an error message.

Time Period. Specify the amount of time in minutes or seconds you want the selected action to run (must be from 1 to 255). Select the time mode in minutes or seconds.

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

Door Lock Override

The Door Lock Override option allows the operator to specify time periods when a door should be unlocked, together with optional areas that should be disarmed. This allows Forcefield to override the normal override timezone programming (as determined by the door controller Override Timezone settings) that controls when the door is normally locked and unlocked. Multiple overrides may be specified for a door.

For example, a door may normally lock at 6:30 pm. Door Lock Override is used to unlock the door between 7:00 pm and 10:30 pm and disarm the appropriate area. Forcefield creates the time triggers necessary to accomplish this unlocking. Multiple overrides may be entered for a particular door.

An event trigger is also created that will cause any lock events to immediately cause an unlock of the door if any lock events are reported for the door during the override time.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Unlock and Lock time fields. If the Challenger is in a different time zone to the node to which it is connected, the time difference will be have to taken into account when entering the time data. The time entered will be the time at which the node will fire the triggers. For example, add two hours if the node is in Melbourne and the Challenger is in Perth.

Areas to Arm/Disarm fields. Select any areas that need to be disarmed. At the lock time the same areas will be re-armed.

Click List (or press F12) to display:

- All the current door overrides (if no door is selected)
- All the overrides for a door (if a door is selected)

Control > Alarm Panel

Challenger

A Challenger may need to be isolated (separated from the system) without causing alarms when repairs are performed, and then later de-isolated so that system alarms can again be generated. Use the Challenger option to perform remote control actions.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Actions performed on Challenger panels include:

- **Isolate.** Isolates Challenger panels to prevent any system alarms from being generated on fault and tamper conditions.

- De-Isolate. De-isolates Challenger panels so that system alarms will be generated on the fault and tamper conditions.
- Battery Test. Isolates Challenger panels from mains power for a pre-set interval in order to test the battery.
- Cancel Battery Test. Cancels the battery test being performed on Challenger panels.
- Untimed Battery Test. Isolates Challenger panels from mains power for an unlimited period to test the batteries, until Cancel Battery Test is selected.
- Update Status. Sends a request to the selected item to return its current status to Forcefield. If the Update Status command fails, Forcefield displays an error message.

Time Period. Specify the amount of time in minutes or seconds you want the selected action to run (must be from 1 to 255).

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

DGP

Repairs can require that a DGP be isolated (separated from the system) without causing alarms. Use the DGP option to perform remote control actions.

Common window elements are described in Section 3. Elements specific to this window are described below.

Action. Actions performed on DGPs include:

- Isolate. Isolates DGPs to prevent any system alarms from being generated on fault and tamper conditions. This feature might be used to remove a DGP Siren Fail or DGP Offline message from the system when a unit has been tampered with or has stopped communicating. After the fault is reported, the DGP may be isolated while awaiting service.
- De-Isolate. Deisolates DGPs so that system alarms will be generated on the fault and tamper conditions.
- Battery Test. Isolates DGPs from mains power for a pre-set interval in order to test the batteries.
- Cancel Battery Test. Cancels the battery test being performed on DGPs.
- Untimed Battery Test. Isolates DGPs from mains power for an unlimited period to test the battery, until the Cancel Battery Test function is selected.
- Update Status. Sends a request to the selected item to return its current status to Forcefield. If the Update Status command fails, Forcefield displays an error message.

Time Period. Specify the amount of time in minutes or seconds you want the selected action to run (must be from 1 to 255).

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

Floor

The Floor option allows the operator to remotely enable or disable floors and to give free access (no card required) or secure access (card required) to a floor in specific lifts.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Actions performed on floors include:

- Secure Floor sets floors in the specified lift to require a valid card/PIN code to gain access.
- Access Floor allows floors in the specified lift to have free access (no card/code required) to gain access.
- Disable Floor sets floors into non-operation mode. It is unable to accept user cards, PIN codes, etc., even though their access level allows them to.
- Enable Floor allows floors to function normally. That is, allows users to present their cards, PIN codes etc., and gain access, providing that their access level allows them.

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

Floors. Select the required floors. Use the action Update Lift Floors Status for the lift if you want to update floor status. See “Lift” on page 114.

Note: The floors displayed for the selected lift are calculated using the Starting Floor to Activate a Relay and the Last Floor to Activate a Relay settings in lift options. See “Lift Options” on page 285 for details.

Input

Use the Input option to perform remote control actions on an input.

Control of an input allows an operator to perform a number of functions on a piece of security equipment. Repairs, for example, will often require a device to be out of action for a time. Being able to control that input means that repairs can be done without generating alarms. Once the repair is done the input can be de-isolated.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Actions performed on inputs include:

- Isolate. Disables inputs from functioning (to ignore).
- De-Isolate. Re-enables inputs to function normally.

- **Reset.** Resets inputs if the inputs in alarm have been returned to sealed condition.
- **Reset/Ack.** Resets inputs immediately if the inputs in alarm have been returned to sealed condition. If not sealed, the inputs will reset when returned to sealed condition.
- **Update Status.** Sends a request to the selected item to return its current status to Forcefield. If the Update Status command fails, Forcefield displays an error message.

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

Lift

Use the Lift option to remotely enable and disable lifts.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Actions performed on lifts include:

- **Disable.** Sets lifts into non-operation mode. Lifts are unable to accept user cards, PIN codes, etc., even though their access level allows them to.
- **Enable.** Allows lifts to function normally. That is, allows users to present their cards, PIN codes etc., and gain access to specific floors, providing their access level allows them.
- **Update Lift Floors Status.** Sends a request to the selected item to return its current status to Forcefield. If the Update Status command fails, Forcefield displays an error message.

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

RAS

Use the RAS option to remotely perform remote arming station (RAS) actions.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Actions performed on RASs include:

- **Isolate.** Isolates RASs to prevent any system alarms from being generated on RAS fault and tamper conditions. This feature might be used to remove a RAS Offline message from the system when a unit has stopped communicating. After the fault is reported, the RAS may be isolated while awaiting service.
- **De-Isolate.** De-isolates RASs so that system alarms will be generated on RAS fault and tamper conditions.

- **Open Door.** Opens the door for the unlock period set in Challenger menu options.
- **Update Status.** Sends a request to the selected item to return its current status to Forcefield. If the Update Status command fails, Forcefield displays an error message.

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

Relay

Use the Relay option to remotely perform relay actions.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Actions performed on relays include:

- **Set.** Activates relays.
- **Reset.** Deactivates relays.
- **Default.** Sets relays to the defined default state.
- **Update Status.** Sends a request to the selected item to return its current status to Forcefield. If the Update Status command fails, Forcefield displays an error message.

Operator Notes. Type a short description of why the action was taken. This is entered into the system log (history) for reference.

Control > Intercoms

Intercom Calls

Use the Intercom Calls option to display a list of waiting and connected calls (IP intercom systems only). Use the toolbar buttons to toggle the display between waiting and connected calls, and to order the calls list by time or priority.

Intercom

Use the Intercom option to control the intercom's local master music channels, and to control the volume of music and calls (if applicable). You can also select a specific intercom, and then perform control tasks via the following buttons:

Open Call. Click to send an intercom call request.

Answer Call. Click to respond to an intercom call request.

Close Call. Click to close an intercom call.

Graphic. Click to display the map associated with the intercom.

Monitoring On. Click to open a listen-only channel (may require additional hardware).

Monitoring Off. Click to close the listen-only channel.

Isolate. Click to isolate the intercom. The specified intercom cannot send or respond to calls when isolated.

Enable. Click to deisolate.

Open Door. Click to open the intercom's associated door and close the intercom call (you will need to select Yes from a confirmation window, if configured).

Show Video. Click to open the intercom's associated video view, even if the call is not answered.

Control > Video

Camera Control

This command applies to video cameras connected to Forcefield via a video switcher (referred to as CCTV cameras). This command does not apply to video cameras connected to Forcefield via a DVR. For DVR cameras, see "Show DVR Video" on page 119.

Use the Video (CCTV) option to control CCTV cameras and monitors.

Figure 46: Camera Control window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Camera. To control a PTZ (pan tilt zoom) camera, select the camera and then click Control Camera to open the PTZ controls (if a monitor is also selected, the camera is also switched to the monitor). If you select a camera, the selection will filter the list of monitors.

Monitor. To switch a camera to a monitor, you must select both the camera and the monitor, and then click Camera to Monitor. If you select a monitor, the selection will filter the list of cameras.

Control Camera button. Use a pointing device, such as a mouse, to operate the camera control functions. Click and hold to repeat the action, release to stop (except when a preset is used).

Figure 47: CCTV Camera Control window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Preset and ID fields. Select a preset. Alternatively, double-click the Preset or ID fields to create a new preset.

Action Speed. Enter a speed from 0 to 10 (where 1 is lowest speed and 10 is highest speed and 0 is stop). This field is only applied if the cameras connected to the CCTV switcher have variable PTZ speed.

If the camera is a pan-tilt-zoom (PTZ) camera, you can use the controls in CCTV Camera Control as described in Table 10 *below*. Click and hold buttons for continuous change.

Table 10: CCTV Camera Control buttons (for PTZ cameras)

Button	Function
	Pan left
	Pan right
	Tilt up
	Tilt down
	Clean lens (if supported by the camera)

Button	Function
	Zoom in
	Zoom out
	Reduce iris (reduce the amount of light passing through the lens)
	Increase iris (increase the amount of light passing through the lens)
	Focus to a closer distance
	Focus to a farther distance
	Click to move the camera to the view defined in the preset record displayed in the Preset and ID fields
	Click to program the preset view record to match the camera's current view. The preset record displayed in the Preset and ID fields will be changed. This programming button does not display on the CCTV Camera Control window when the window is opened from a map.

Display MultiView

Use the Display MultiView option to select a multiview display or to change the current multiview display. Multiview records are programmed in “Multiview” on page 203.

Note: Only cameras within the operator's and workstation's member group will be displayed. Displaying multiple images of DVR video on a single screen requires a large amount of processing power, memory, and specific video card(s) to be used in the Forcefield Client computer. Do not select a multiview display that cannot be used with your hardware. Refer to the *Forcefield External Interfaces Manual* for details.

Common window elements are described in Chapter 3.

MultiView. Click the arrow, and then select the required multiview record. Click Run to open the multiview window.

The multiview window may hide part or all of the Forcefield window. Use Alt + Tab to move between open windows. We recommend that you add a Speed Bar button for the function 'Close Multiview'.

Show DVR Video

This command applies to video cameras connected to Forcefield via a DVR. This command does not apply to video cameras connected via a video switcher (referred to as CCTV cameras). For CCTV cameras, see “Camera Control” on page 116.

Use the Show DVR Video option to select a DVR camera from which to view the current video on a Forcefield client workstation, where the Allow Video Popup selection is set for the workstation (“Workstation options—other” on page 177).

Video cameras connected to a DVR may also be used:

- via LAPs on graphics maps
- from the menu item History > Show DVR Footage

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Member. Click the Member arrow, and then select a member to filter the camera search by member. Leave this field blank to search for all DVR cameras in the operator’s member group.

Camera. Click the Camera arrow, and then select a camera.

Click Run to view the live video feed from the selected camera.

Video Playback Control

When a video player is active, you can use the buttons on the Video Playback Control window to navigate the recorded video (Table 11 below).

Table 11: Video Playback Control buttons

Button	Function
	Rewind to the beginning of the footage
	Skip back
	Play forward
	Skip forward
	Pause
	Stop playback and close the Video Playback Control window

Note: Playback control is specific to the footage being displayed when the Video Playback Control window is opened. If you need to control playback for footage from a different event, then you must close and then reopen the Video Playback Control window.

History menu

Add Event

Use the Add Event option to add text notes describing events into Forcefield history. The entry replaces the running log sheet or incident log sheet. At least one of the fields must contain text.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Type. Text entered in this field is used as the history type. This could be a heading for the type of entry, for example, "Security Alert".

Location. Text entered in this field is used as the history point. Enter any desired text, for example, "Car Park".

Notes. Text entered in this field is used as the history text. Enter any desired text, for example, "Found suspicious parcel".

Tip: To find an existing Operator Added Event, run a history report with the event type set to "Oper-Initiated, Operator Incident". Optionally, filter by operator and/or dates.

Backup History

See "Backup History" on page 90.

Clear History

See "Clear history (manually)" on page 63.

Export History

See "Export History" on page 92.

Purge History

See "Purge History" on page 93.

Statistics

The History Statistics report dynamically displays the total number of history records the system can hold, the number currently being stored, and the number of deleted history records (these remain on file but are deleted by replacing the record with a new one). An alarm can be generated at a certain level or number of history records in the system. Purge can also be set to occur when the number of history records reaches a certain level.

See “History file-related tasks” on page 62 for details.

History Config

Use the History Config option to program how Forcefield dynamically manages history records.

Figure 48: Configure History window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Desired Maximum Records. This is the maximum number of records that will be stored in the online history database. Note that each record consumes approximately 800 bytes of disk space. Note also that when records are deleted from the database that the disk space used by those records is NOT returned, but is marked as deleted and used to store new records.

The only ways to recover disk space used by history is by the following processes:

- Delete history records, see “Clear history (manually)” on page 63.
- Use the purge all option from the commands “Auto History Backup” on page 87 or “Auto History Export” on page 88.

Generate 1st Alert at. When the history becomes this full, Forcefield alerts the operator. This is also the level to which the history will be deleted if a purge is initiated because the record count reaches the Purge Level.

Generate 2nd Alert at. When the history becomes this full, Forcefield alerts the operator a second time.

Start Auto Purge at. When the history becomes this full, the History Manager will start purging records, oldest to newest, until the history database record count is down to the 1st Alert Level.

Door/Lift Activity

Use the Door/Lift Activity option to create reports about door/lift activity.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Door/Lift Id. Select the desired doors or lifts or leave blank to report on all doors and lifts.

Format. Select the report format required:

- TEXT–Event Screen Format provides a layout similar to the Forcefield Event Windows (this is the preferred format for printed reports).
- TEXT–Single Line Format provides a report with 1 text line per event usually used to export the report text to another system for processing.
- CSV–Raw provides all data in the specified records ‘as is’, with date and time data not in human-readable format.
- CSV–Formatted provides a selection of data, with date and time data converted to human-readable format.

Door/Lift User Activity

Use the Door/Lift User Activity option to create reports about door/lift user activity, in particular access granted and access denied user events.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Challenger Time selection. Leave clear to use Forcefield time. Select to use Challenger time (the time that the event happened in the Challenger). The times may be different, for example, a dialler-Challenger may not report events to Forcefield until a much later time.

Door/Lift Id. Select the desired doors or lifts or leave blank to report on all doors and lifts.

Format. Select the report format required:

- TEXT–Event Screen Format provides a layout similar to the Forcefield Event Windows (this is the preferred format for printed reports).
- TEXT–Single Line Format provides a report with 1 text line per event usually used to export the report text to another system for processing.
- CSV–Raw provides all data in the specified records ‘as is’, with date and time data not in human-readable format.

- CSV–Formatted provides a selection of data, with date and time data converted to human-readable format.

Event Report

Use the Event Report option to show all the activity relating to one event number.

Forcefield uses event numbers to group a sequence of events by number. For example, if an input goes into alarm, an event number is generated by Forcefield and it is stored to event history. Subsequent operator responses, multibreaking by the input, and the restoral event will all have the same event number. Once the alarm is cleared, the event is closed.

Refer to “Generating reports” on page 28, and the following details about this report.

Tip: To find existing events, run a history report, using date or device, etc. to find an event number. Then use the event number to run the event report, which will list all the events with the event number.

History Report

The History Report option allows reports to be generated on any item in the Forcefield system. The operator can use as many of the event parameter fields as they wish in order to define exactly what information the report will provide. If no restrictions are specified and the report is executed, all system and user history will be printed (subject to the operator’s access permissions, see “Operator Permissions” on page 163).

The report uses only current events in the history. For archived events, refer to “Offline History” on page 124.

Note: History reports for large Forcefield systems may take considerable time to run. Off-line history reports typically run much more quickly.

Common window elements are described in Section 3. Elements specific to this window are described below.

Leaving fields blank indicates no restriction on that field when searching for events.

Different field types 'AND' together; similar fields 'OR' together. For example, you may select a specific input, AND an event. Alternatively, if you selected multiple inputs, the search would 'OR' the inputs before ANDing the other fields.

Challenger Time selection box. Right-click the Challenger Time selection box to place a check mark in the box. When checked, the time and date selections pertain to the Challenger panel time and events and not to the Forcefield system time and events. Only Challenger panel events are reported, and not Forcefield events.

Event Type fields. Select an event type for the search string. You can enter two different events or event groups at the same time. To create a new event

group, enter the new ID and press F3 to go to the Event Type window (see “Events” on page 194).

Points. Select the relevant points (devices) to include for the search string.

Sort Order. Select the required report sort order:

- Date/Time
- Incident Number
- Point ID
- Operator/User
- Event Type

Format. Select the required report format:

- TEXT–Event Screen Format provides a layout similar to the Forcefield Event Windows (this is the preferred format for printed reports).
- TEXT–Single Line Format provides a report with 1 text line per event usually used to export the report text to another system for processing.
- CSV–Raw provides all data in the specified records ‘as is’, with date and time data not in human-readable format.
- CSV–Formatted provides a selection of data, with date and time data converted to human-readable format.

Incident Report

Use the Incident Report option to generate history reports for particular incident (a series of events belonging to one member). See “Incidents” on page 10.

Refer to “Generating reports” on page 28, and the following details about this report.

Report for Incident. The incident number is taken from the initiating event. Any event (for the same member) that occurs after an incident is created belongs to the same incident until the incident is closed from the Alarm Details window.

Tip: To find existing incidents, run a history report with the event type set to “Computer Event, Incident Begin” or “Computer Event, Incident End”. Use the found event number as the incident number. The report will list all events considered part of the incident.

Offline History

Use the Offline History option to perform the same functionality as the History Report (see “History Report” on page 123). However, the data comes from a storage device onto which history has previously been archived. Once the device has been selected, the date range of the history archived on the device will be displayed.

Common window elements are described in Section 3. Elements specific to this window are described below.

History Type. Click the History Type arrow, and then select from the list:

- Select Single Backup and then select a backup archive to run the report from. Once the backup archive has been selected, the date range of the history in the archive will be displayed.
- Select Date Range and Forcefield will determine which backup archives to run the report from, based on the date ranges entered. **Note:** This option may attempt to generate excessively large reports.

History From. Click the History From arrow, and then select the storage device onto which history has previously been archived.

History > Show DVR Footage menu

A Forcefield system may interface via Ethernet (IP) connection to a Digital Video Recorder (DVR) and associated CCTV video cameras.

Refer to the *Forcefield External Interfaces Manual* for details about integrating a DVR and viewing CCTV footage from a DVR.

Show DVR Tagged Footage

Use the Show DVR Tagged Footage option to search for event text tags (or text tags from other devices) recorded with the digital video.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

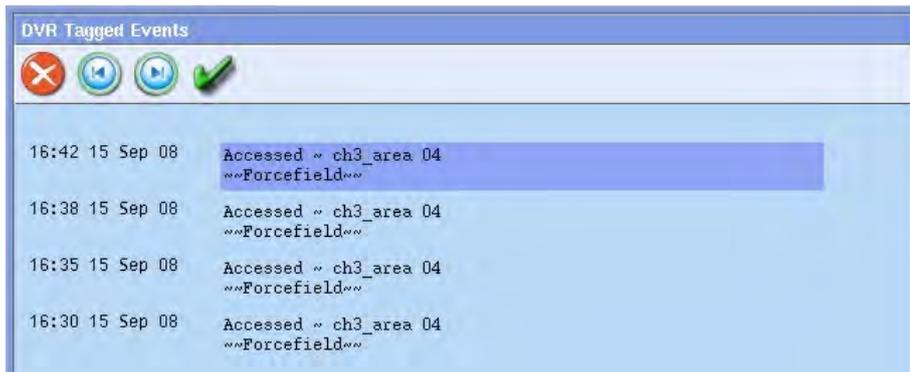
Specify the start and end times and dates, or click the Assign Date and Time button (see Table 4 on page 32) to automatically populate the date and time fields with values from, for example, today, yesterday, etc.

Specify any filtering options needed to help define the search.

Show in Point Order selection. Leave clear to display the list of event text tags in chronological order. Select to display the list of event text tags ordered by the point (door, PIR, etc.).

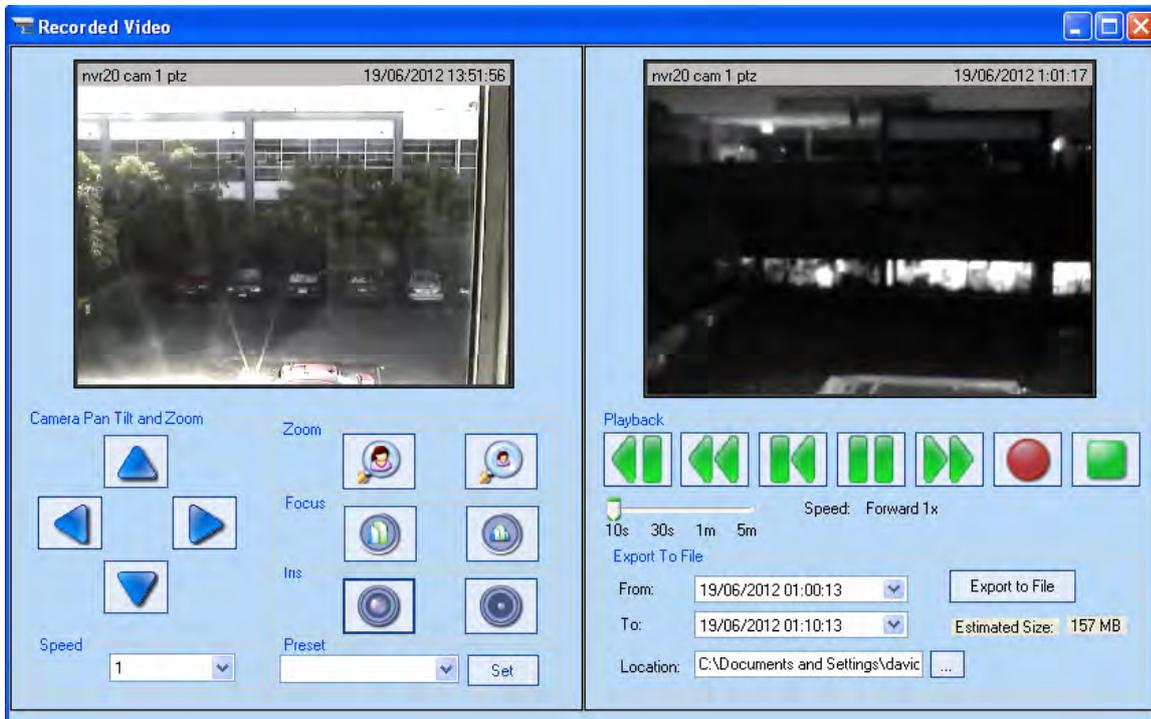
Click Run to display the DVR Tagged Events list.

Figure 49: DVR Tagged Events list



Click event text to display the Recorded Video window.

Figure 50: Recorded Video window



The Recorded Video window displays the recorded footage associated with the selected event on the right-hand side (above the VCR-style buttons). The live image from the same camera is displayed on the left.

Use the VCR buttons to rewind, play backward, play forward, and pause (stop) as described in Table 12 below.

Table 12: Recorded Video window VCR buttons

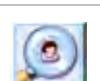
Button	Function
	Jump back by 10 s, 30 s, 1 m, or 5 m, as set by the jump interval slider.

Button	Function
	Rewind (applicable to SymDVRs only)
	Rewind to the beginning of the event.
	Pause (when paused, the Play forward button displays).
	Play forward (when playing, the Pause button displays).
	Play fast forward by the multiplier displayed below the button (for example 2x).
	Mark the start of footage segment to export (the operator must have edit permissions on the Show DVR Footage functions)
	Mark the stop of recorded footage to export, and then to select a storage location for the file.

The Export to File button or the Stop button allows you to select a storage location and to save an exported file. You can use the media player to view the exported footage. See “Viewing exported video footage” on page 128 for details.

If the camera is a pan-tilt-zoom (PTZ) camera, you can use the controls described in Table 13 below to control the view in the left-hand side of the Recorded Video window.

Table 13: DVR Camera Control buttons (for PTZ cameras)

Button	Function
	Pan left
	Pan right
	Tilt up
	Tilt down
	Zoom in
	Zoom out
	Focus in

Button	Function
	Focus out
	Reduce iris (reduce the amount of light passing through the lens)
	Increase iris (increase the amount of light passing through the lens)
	Click the arrow to select a preset view from the list

Show DVR Time Footage

Use the Show DVR Time Footage option to search for recorded video from a specific camera starting at a specific time and date.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

DVR. Select the DVR to which the camera is connected.

Camera. Select the camera.

Starting at fields. Specify the start time and date from which you want to begin viewing footage or searching for tag text.

Alternatively, click the Assign Date and Time button (see Table 4 on page 32) to automatically populate the date and time fields with values from today, yesterday, past 24 hours, or past 7 days. Once populated, you can change the values.

Click the Time Window arrow, and then select a value to limit the search (10 minutes to 1 day).

Optionally, type some text in the Tag Text field to search the DVR for instances of the tag text within the defined time interval (not supported by TruVision DVRs).

Click Run to display a window similar to Figure 50 on page 126.

Viewing exported video footage

The supplied media player is a standalone player that can be used to replay any video clip that has been exported using Forcefield. This player should be copied to media along with the video clips for authorities. It has a zero footprint – meaning it does not require installation to a machine.

Users menu

Design Card Layout

Use the Design Card Layout option on a Forcefield client to create or modify the design of user cards.

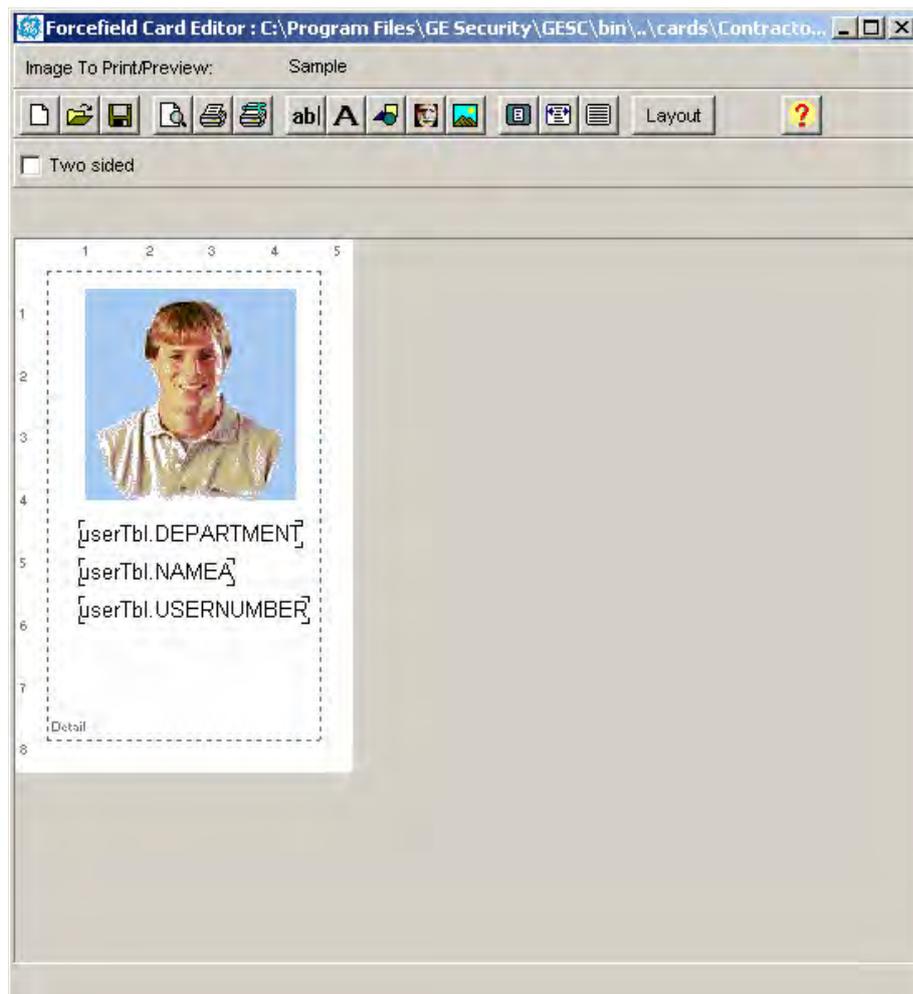
Common window elements are described in Chapter 3. Elements specific to this window are described below.

For Department. Click the arrow to select the required department (card layouts are created on a per-department basis).

Note: If you need to create a department, open the User Profiles window or the User Maintenance window, and then double-click the Department field.

Design button. Click to open the Forcefield Client Card Editor (see Figure 51 below).

Figure 51: Forcefield Client Card Layout Editor window



Refer to the *Forcefield External Interfaces Manual* for details.

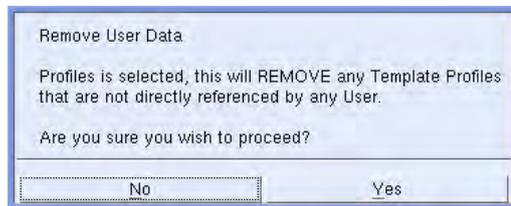
Delete Unused Data

Use the Delete Unused Data option to remove data that is not used in any user records.

Select one or more of the following data types, and then click Run:

- Select Departments to remove any unused department records.
- Select Positions to remove any unused position records.
- Select *aaaa* to remove any unused user defined data records, where *aaaa* is the configurable title of the user defined data field programmed in “Configuring user options” on page 232. The default value is ‘Reference’.
- Select Profiles to remove any unused profile records. In the case of Profiles, the message in Figure 52 below displays.

Figure 52: Delete Unused Profiles dialogue box



Note: Select No if you have any profiles that you want to use as templates and are not assigned to any users. See “Importing user profile data” on page 56 for details.

Download User

Use the Download User option to send a single user record to a single Challenger.

Select the user and Challenger, then click Run to initiate the download. If the user does not have any access groups for the selected Challenger, an error message is displayed and the download does not happen.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

User Num. Click the arrow to select a user from the list. The name displays automatically.

Challenger. Select a Challenger either by its number or by its ID.

Select Learn Reader

Use the Learn Reader option to designate an IUM learn reader near the workstation to be used to add an unknown card to a user’s record.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

IUM Learn Reader. Click the arrow to select a reader from the list. Only one reader may be selected at a time for the exclusive use by the workstation.

Click Run. Forcefield displays a learn reader activity icon on the desktop.

Figure 53: Learn Reader activity icon



There are two ways to stop the IUM learn process:

- Clear the selection and then click Run.
- Double-click the learn reader activity icon on the desktop, and then click Stop.

Refer to “Learning IUM card data” on page 44 for additional details.

Maintenance

Use the Maintenance option to add, edit, or delete user information.

Forcefield operators can specify which fields on the User Maintenance window are to be read-only (not editable). This allows operators to bypass fields that they do not commonly use in order to save time when adding users. Refer to “Maintenance Config” on page 139 for details.

Figure 54: User Maintenance window

The screenshot shows the 'User Maintenance' window with the following fields and values:

User	1	Pin	1111	Status	Active
Name	Matt James		Type	Normal	
Profile	Manager Access Group				
Profile End	19	:	20	12	/ 12 / 2010
Alt Profile					
Member	Building C				
Reference					
Position	Engineer	Dept	Engineering		
Phone	+613 1234 5679		Ext	Phone (AH)	
Active from	23	:	0	30	/ 12 / 2000
D.O.B	11 May 1954				
			Lockout	Not Timed	
	<input type="checkbox"/>	Trace	<input type="checkbox"/>	Card Only	
	<input type="checkbox"/>	Long Access	<input type="checkbox"/>	Privileged	
	LAST ACCESS FOR THIS USER				
Event	Entry Granted				
At	12:14:28 Tue 27 Jan 2009				Map
Reader	Test Door 3				
Region	Inside Door				
Card Data		Ch. List		Notes	
Capture		Print Card		Import	

By default, the previous and next buttons scroll through user records by user number.

To scroll by user name, click the Name field before using the previous and next buttons.

Common window elements are described in Chapter 3. Elements specific to this window are described below. See also “Creating new users in Unique Profile Per User mode” on page 138.

User. Forcefield stores all users in the system by a unique number.

- For non-IUM Challenger panels, the user number is also the card number.
- For IUM Challenger panels, the user number Forcefield assigns to a user is not necessarily the user number in the Challenger(s). To find the Challenger user numbers for a user press the Ch. List button.

PIN. A 4- to 10-digit number given to, or selected by a user. It is necessary to enter a PIN on the Challenger keypad as a pre-requisite to perform most Challenger functions.

Status. The status field is used to indicate to the card's current status:

- Active—Access allowed.
- Inactive—Access is denied; INACTIVE CARD BADGED alarm is generated.
- Void—Access is denied; VOID CARD BADGED alarm is generated.
- Lost—Access is denied; LOST CARD BADGED alarm is generated.
- Expired—Access is denied; EXPIRED CARD BADGED alarm is generated.

When the user record is saved the system checks the start date and time to determine whether the record should be active, inactive or expired.

- The user is active if the start date and time is the present.
- The user is inactive if the start date and time is set for the future.
- The user is expired if the end date and time is set in the past.

Forcefield automatically changes the status from inactive to active when the Begin date becomes the present, and from active to expired when the End date becomes the present.

When a card is reported lost by a user the card status should be changed from active to lost. Should the card be used an alarm will be activated. Operators with restricted access may use the change status of user command (see "Change Status of User" on page 146).

Name. Enter the user's full name.

Surname or first name should be entered consistently to ensure proper searching and card printing. Pressing F4 on the Name field will find all users with that name or sub-name. For example, type "Adam" and then press F4, and Forcefield will find all user names starting with Adam, such as Adam Smith, Adamson Brian, Adamstone Kerry, etc. You can use a pair of % characters to do a wildcard search for any string of text in users' names. For example, type "%JO%" and then press F4, and Forcefield will find all user names where either the first or last names contain JO, such as Jodie Smith or Marie Johnston.

Note: First name - last name order (for importing or exporting user data) is determined by the Surname Order value. See “Configuring user options” on page 232.

Type. Select the card type (the use of Visitor, Guard, and Dual types pertain to systems with Intelligent Access Controller doors numbered in the range 17 to 64).

- Normal—Standard card and PIN operation.
- Visitor—A visitor can only unlock the door if escorted by a guard, e.g. both the visitor and the guard must badge their card or enter their PIN to unlock the door.
- Guard—Is used with a Visitor type user to allow escorting through the premises.
- Dual—Two cards must be badged or two PIN(s) must be entered to unlock the door.

Profile. The profile determines the user’s Challenger access and other common data, such as member, dates, position, department, card type, card options. The profile may be given an expiry date. In this case, when the date is reached, the user is switched automatically to the alternative profile (for Challenger access only).

Notes

- An expired profile is indicated by two red asterisks ** next to the profile field.
- The user’s member might be different to the profile’s member. If the operator’s member group contains the user’s member, then the operator will be able to see the user record. But if the operator’s member group does not also contain the profile’s member, then the operator is not permitted to copy that user record to create another user record (either singularly or in bulk).

Profile Ends. The time at which a user is switched to an alternate profile. Leaving the expiry date/time blank will mean the profile never expires.

Alt Profile. The profile determines the user’s Challenger access and other common data, such as member, dates, position, department, card type, card options. This profile is only applied if the user record has a profile with an expiry date.

Member. The user must be allocated to a member to determine where events associated with this user are to be directed. The member also controls which user defined fields are displayed. The title of these fields vary depending on the user’s member. This allows different sets of data to be allocated to each user depending on the member they belong to.

Reference. By default, the name of this field is “Reference”. However, it can be changed by the setting of the User Defined Field Title value. See “Configuring user options” on page 232. This data is searchable and may be entered into the database by double-clicking the field.

Position. allows the entry of the user’s position, for example, Manager. This data is searchable and may be entered into the database by double-clicking the field.

Dept. Allows the entry of the user’s department, for example, Sales. This data is searchable and may be entered into the database by double-clicking the field.

Note: Do not use a space or any of the following characters in the department name \ / : * ? " < > |.

Active From and To. Each user must be within a valid date range to have access to the Challenger(s). A user that is programmed with the present date and time is downloaded to the Challenger(s) when the user record is saved (except for dialler Challenger panels). When a user is programmed with a future date and time the user record is not downloaded immediately. Forcefield automatically downloads the user on the date it becomes active. The end date and time is used to automatically remove the user’s record from the Challenger(s). The user record is not deleted from Forcefield, just made expired.

Note: Automatically generated card data for a user programmed with a future start date will be downloaded only to Challenger panels where system default IUM card categories are assigned to the panel, and the panel has a programmed Site Code A.

Lockout. Inactivates the user in one of the following conditions:

- From on site—the time interval begins when a card is badged to enter the site. The card may be used to exit the site, but it cannot be used for re-entry until the time interval expires.
- From off site—the time interval begins when a card is badged to exit the site. The card cannot be used for re-entry until the time interval expires.

The timing for on site or off site user access is determined by the number of lockout minutes specified on the user record. Forcefield resets the user’s Active From time so that the user status becomes inactive until the time is reached. As a result of this, the operator can open the user’s record and see when the lockout time is set to expire (the Active From time will appear to be in the future). If needed (for example, to allow re-entry sooner than the expiry of the lockout time), the operator may alter the user’s Active From time to the current time and then save the record. Forcefield reactivates the user record and permits access (allow up to five minutes for processing to occur).

Note: The user is deactivated in all Challenger panels associated with their access groups. Also note that the use of this option alters the start date in the user database (this will affect some reporting functions). This feature will only operate if Challenger/Door Controller is programmed to report regions.

Trace. When checked, all alarm and access functions performed by the user at doors 17 to 64 (Intelligent Access Controller doors) will cause a trace message to be sent to Forcefield.

Card Only. When checked, the user will not be able to use a PIN code. This allows the PIN code field to be used to program cards on formats not normally compatible with the Challenger system when a special reader is used.

Long Access. When checked, the user will be allowed extended door access times at doors 17 to 64 (Intelligent Access Controller doors).

Privileged. When checked, the user's code or card will override any antipassback restrictions or reader disabled functions in place on doors 17 to 64 (privileged does not override a door disabled function).

Last Access for this user. Displays the event type (such as door access granted), time and date that a card assigned to the user was last badged at a reader, the reader ID, and the region (if applicable). Click the Map button to view the reader's location on a map (if the reader is assigned to a map).

Card Data button. Click to program IUM card data for this user. See "User card data" below for details.

Note: For IUM Challenger panels, this associates an access card with the user. Card data must be entered for all the card types for all Challenger panels for that user. Failure to enter the card data will result in the user not being downloaded to Challenger panels using that card type. For non-IUM Challenger panels, the card number is the user number and this data is not required.

Capture button (available only on Forcefield clients). Click to run the User Image Capture process on the Forcefield client. Refer to the "Using Capture" section in the *Forcefield External Interfaces Manual* for details.

Ch. List (Challenger Number List) button. Click to display what user number this user is in the Challenger panels to which they have been downloaded. The Forcefield user number is not necessarily the user number in the Challenger., e.g. user 5 in Forcefield may be user 1 in Challenger 5 and user 5437 in Challenger 17.

Print Card button (available only on Forcefield clients). Click to print the user card on the default printer.

Notes button. Allows for entry of free format text notes relating to the user. A separate text file is kept for every user.

Import button (available only on Forcefield clients). Click to run the User Image Import process on the Forcefield client. Refer to the "Using Import" section in the *Forcefield External Interfaces Manual* for details.

User card data

Click the Card Data button to program unique IUM card data for this user.

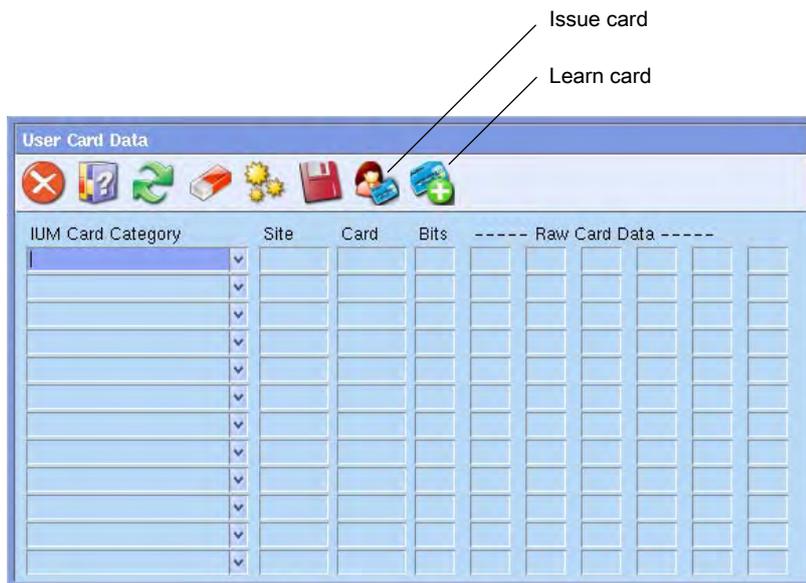
Users can have up to 12 sets of card data (IUM card categories), which link the user to IUM Challenger panels having the same card categories. This link tells Forcefield what card data to download to each Challenger.

Card data may be programmed using the following methods:

- Data for all available card formats may be entered by typing the data into the *User Card Data* window (see “Learning IUM card data” on page 44).
- Data for all available card formats may be entered by badging the unknown card at a designated IUM Learn Reader. See “Learning IUM card data” on page 44 for details.
- Data for standard-format (Tecom 27-bit or Wiegand 26-bit) cards may be entered by badging the unknown card at the system’s TS0862RAW card reader.

Note: A connected and enabled Smart Card Programmer is required for the Issue Card button to display and a specified card learn port (connected to a TS0862RAW card reader) is required for the Learn Card From Reader button to display. The card reader port is programmed in “Serial & Parallel Ports” on page 169. The card learn port is programmed in “Workstations” on page 173.

Figure 55: User Card Data window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

IUM Card Category. Click the IUM Card Category arrow, and then select the required card category. Card categories are programmed from Challenger > IUM Card Categories (see “IUM Card Categories” on page 220). Selecting a default category (e.g. Tecom 27 bit or Wiegand 26 bit) will cause the raw card data fields to become inaccessible. For these types of card, enter the site code and card number, and Forcefield will calculate the raw card data. Selecting a non-default card category will allow only raw card data to be

entered (either by typing or using an IUM Learn Reader (see “Learning IUM card data” on page 44).

Site. Contains the card’s site code.

Card. Contains the card’s number (card number is not necessarily the user number).

Bits. Contains the number of bits of card data used by this card type.

Raw Card Data. Contains the raw card data for access cards. The card data is up to 48 bits and is associated by Forcefield to the card type. This is used to identify the user in the Challenger panels that have been programmed with that card type. Each user may have a different card for different Challenger panels.

Issue Card button. Click to open the Issue User Card window. This button displays only after the Smart Card Programmer is connected and enabled.

Figure 56: Issue User Card window



Learn Card from Reader button. Click the Learn Card from Reader button, and then present the card to the system’s TS0862RAW card reader within five seconds to have Forcefield read the card data from the card. Alternatively, see “Learning IUM card data” on page 44 for details about using other card readers to learn IUM card data.

Complex user search

On the User Maintenance window click the Advanced Search button to open the User Search Selection window.

Complex user search is performed by selecting values on only the fields that are to be matched. For example, to find all users named ‘Matt’, ‘Matthew’, etc. with active cards and who work in Engineering:

1. Type ‘Matt’ into the Name field.
2. Select Status of ‘Active’.
3. Type ‘Engineering’ into the Department field.
4. Leave all other fields blank.
5. Click Run.

If any matching users are found, this process switches to Search Mode (the title bar displays “User Maintenance - SEARCH MODE”) and you can use the Next

and Previous buttons to see all the found users. To return to normal mode click Search. Whilst in search mode, any operations will present only users matching the search criteria.

Note: Performing a search in this manner may require Forcefield to search the entire user database. This may take some time, especially if the operator has a restricted member group.

Search for. Enable searching for corresponding values that are either on or off.

To use trace for example:

- Search for = ON, Trace = ON, Forcefield will search for users with trace enabled.
- Search for = ON, Trace = OFF, Forcefield will search for users with trace disabled.
- Search for = OFF, Forcefield will not search for any trace values.

User Defined fields—Five user defined fields are provided by which you may search for users having the corresponding data.

Note: If you use multiple user defined fields, the fields are ANDed, which means only records containing all the data entered will be found. User defined fields may be created from “Members” on page 192.

Tip: The search process may be accelerated when the option “Alpha-Num by Member” is selected in “Configuring user options” on page 232.

Bulk user operations

Click the Bulk button on the User Maintenance window (see Figure 54 on page 131) to perform the following bulk operations:

- Bulk Create is used to create multiple user records based on an existing user or based on a member and profile as a template. This function is described in “Creating users in bulk” on page 46.
- Bulk Modify is used to modify various data for multiple user records. The data that can be modified is date range, card state, card type, and lockout data. Note: Any data entered on this screen will be placed into all user records in the requested member and user number range. This function is described in “Modifying users in bulk” on page 47.
- Bulk Delete is used to delete multiple user records. This function is described in “Deleting users in bulk” on page 48.

Creating new users in Unique Profile Per User mode

Unique Profile Per User mode (see “Configuring user options” on page 232) causes user profiles (and alternative user profiles) to be locked to user records. As a result, when Forcefield is in unique profile per user mode, the new user window does not display search fields for either Profile or Alt Profile.

When a user record is saved for a new user, a new profile is automatically created and named according to the user number. For example, user 1 can have

only “User 1 Profile|” and optionally “User 1 Alt Profile|”. The created profile will be given the member of the user record.

Note: The only data required to create a new user record is the user name and the member (if Allow Auto User Number Allocation is enabled in “Configuring user options” on page 232).

This new profile record will have no access. To assign access data, press F3 from the profile field to go into the profile record. The new profile may be populated with data from another profile by importing some or all of the profile data. See “Importing user profile data” on page 56 for details.

Using templates to create new users with default data

Refer to “Using templates to populate new user data” on page 57 for details.

Maintenance Config

Use the Maintenance Config option to create records that specify which fields on the User Maintenance window are to be read-only (not editable). This allows operators to bypass fields that they do not commonly use in order to save time when adding users. An operator can create multiple User Maintenance Field Control records (different sites may have different needs). Only one record can be active at a time.

User Maintenance Field Control records are operator-specific, so if more than one operator needs to add users, then each operator would need to create their own records.

Once an operator creates a User Maintenance Field Control record and makes it active, the record is in effect each time that operator logs in.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

ID. Type a name to identify the User Maintenance Field Control record. An operator can create multiple records to suit multiple sites with different needs for recording user details.

Field selections. Check the required field check boxes to make the corresponding fields on the User Maintenance window read only. When creating a new user record, the read-only fields are skipped over when using the Tab key to move between fields.

Activate Field Control. Click to apply this record to the current session and for future sessions by the operator. When activated, the This record is currently active check box is populated.

Deactivate Active Record. Click to deactivate this record. When deactivated, the This record is currently active check box is cleared.

Show PIN Code

Use the Show PIN Code option to display the PIN codes for a user. Two sets of PIN codes are displayed: for IUM and non-IUM Challenger panels.

If a user has a user number over 1000 in a non-IUM Challenger, the applicable PIN code is generated by the door controller and is displayed here. For user numbers under 1000, the PIN code is the one programmed to the user in Forcefield.

User Num. Type the user number and press Enter. The IUM PIN displays.

Non IUM Pins button. Click to see the list of Challenger panels for this user and the applicable PIN code for each Challenger.

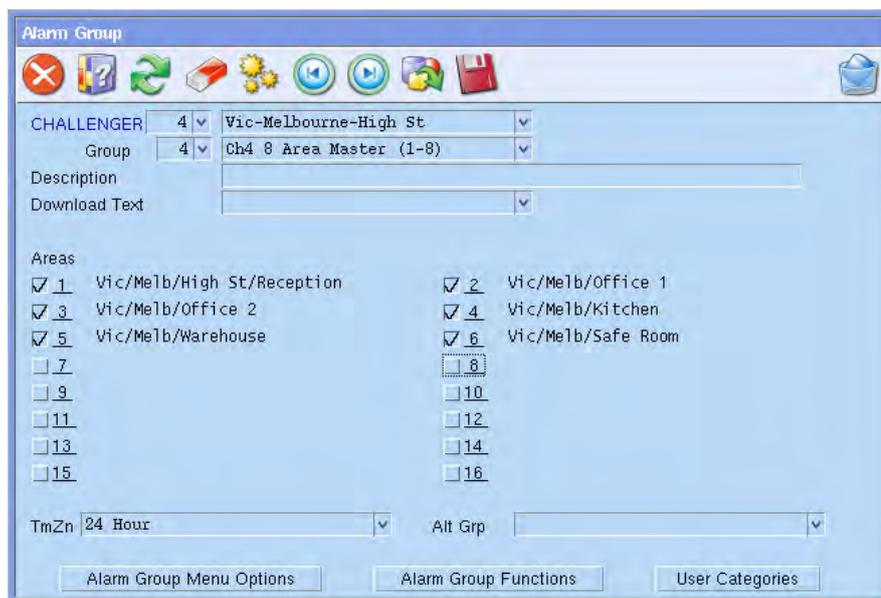
Users > Access menu

Alarm Groups

Use the Alarm Groups option to define alarm functions to users and Challenger hardware. By selecting specific areas, alarm control options, RAS keypad menu options, and a timezone to an alarm group, you are controlling the level of authority for the user in that specific Challenger.

Note: You must be extremely careful when changing alarm groups. Both the functions performed by users with that alarm group, and the functions available at remote arming stations (and door readers) with that alarm group, will be affected.

Figure 57: Challenger programming window for alarm groups



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Group. The number and ID fields identify different alarm groups within a Challenger. To create a new alarm group, you must select a Challenger panel, and then enter a new alarm group number. Alternatively, you can enter the alarm group by an ID only. Forcefield will automatically allocate the next available number. Challenger V9 panels (all versions) and Challenger V8 panels with firmware version 8.128 or later support 245 programmable alarm groups. Other versions support 128 programmable alarm groups.

Download Text. This name is downloaded into the Challenger. It comes from the Text Word library within the Challenger. It should reflect the function of the alarm group. To create a new word, enter the word and press F3.

Areas. Select the area(s) you want this alarm group to control. Areas can only be selected if they are listed. It is not possible to check an area box if the Area ID is empty.

TmZn. Determines the timezone applicable to this alarm group. Functions restricted/available via this alarm group will be applicable only for the periods allowed by the timezone.

Alt Grp. Each alarm group may have an alternative alarm group. A user is assigned an alarm group and, depending on the timezone restrictions, can have two alternative alarm groups, each with different functionality. The original and alternative alarm groups (which are programmed from the same menu) assigned to the user apply as follows:

- If the original alarm group is valid, it is used. If the original alarm group is not valid, then the first alternative alarm group is checked.
- If the first alternative alarm group is valid, it is used. If the first alternative alarm group is not valid, then the second alternative alarm group is checked.
- If the second alternative alarm group is valid, it is used.

Refer to the *Challenger V8 & V9 Programming Manual* for a more detailed explanation.

Alarm Group Menu Options button. Click to select the RAS keypad menus that you want the alarm group to have.

Alarm Group Functions button. Click to select which functions the user or RAS will have for this alarm group. Each function must be selected for it to be available to the alarm group. **Note:** If you do not select User Alarm Group, then you will not be able to attach the alarm group to any user.

User Categories button. Click to select the user category to be used in this alarm group. If more than one is selected, only the lowest will be used. User categories provide special restrictions to the alarm group.

- User Category 7 can be used to report Dead Man Alarm (if available in the applicable reporting format).

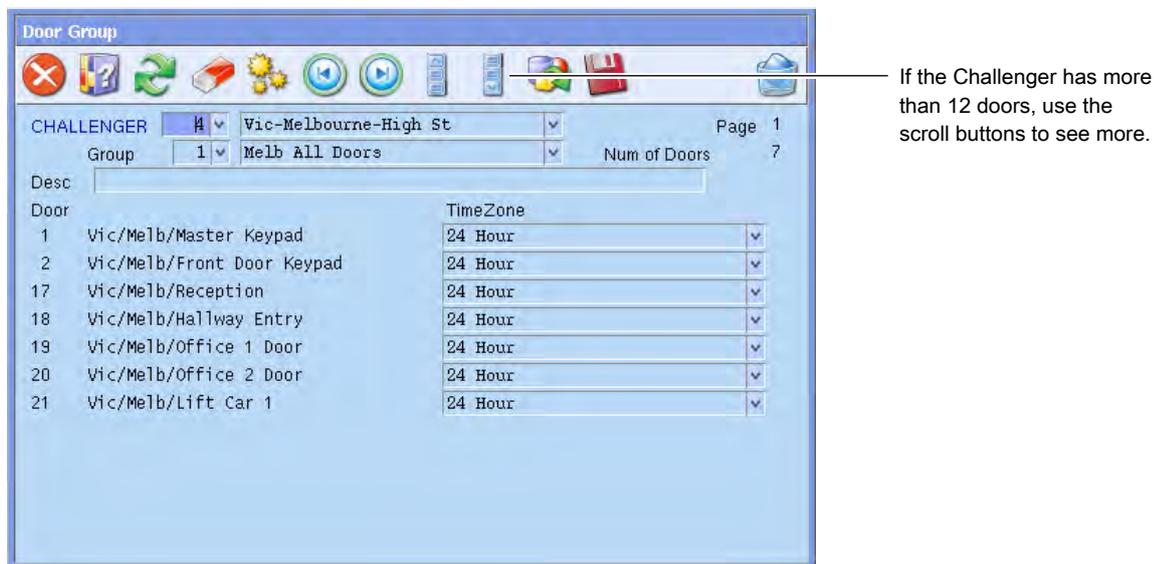
- User Category 8 can be used as the special function User Count For Each Area.

Refer to the *Challenger V8 & V9 Programming Manual* for a more detailed explanation. See also “User Category Data” on page 287.

Door Groups

Use the Door Groups option to allocate access levels to users. Door groups define which doors users are able to get access to and at what times they are able to use each door.

Figure 58: Challenger programming window for door groups



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Group. Use the group number and name as follows:

- The number field represents the door group number in the Challenger. To create a new door group enter the new number of the door group. Select the timezones required for each door in the list shown on the form. Challenger V9 panels (all versions) and Challenger V8 panels with firmware version 8.128 or later support 255 door groups. Other versions support 128 door groups.
- The ID field represents the Door Group ID in Forcefield. To create a new door group enter the new ID of the door group (Forcefield will automatically add the Door Group number when saving). Select the timezones required for each door in the list shown on the form.

Note: A door group cannot be programmed unless a Challenger ID and a door group ID are entered.

Desc. describe the function of the door group.

Door fields. Once a Challenger has been selected, the doors programmed to that Challenger will be displayed in the door fields.

Note: Even though the door is listed, it is not part of the group until it has a timezone attached to it.

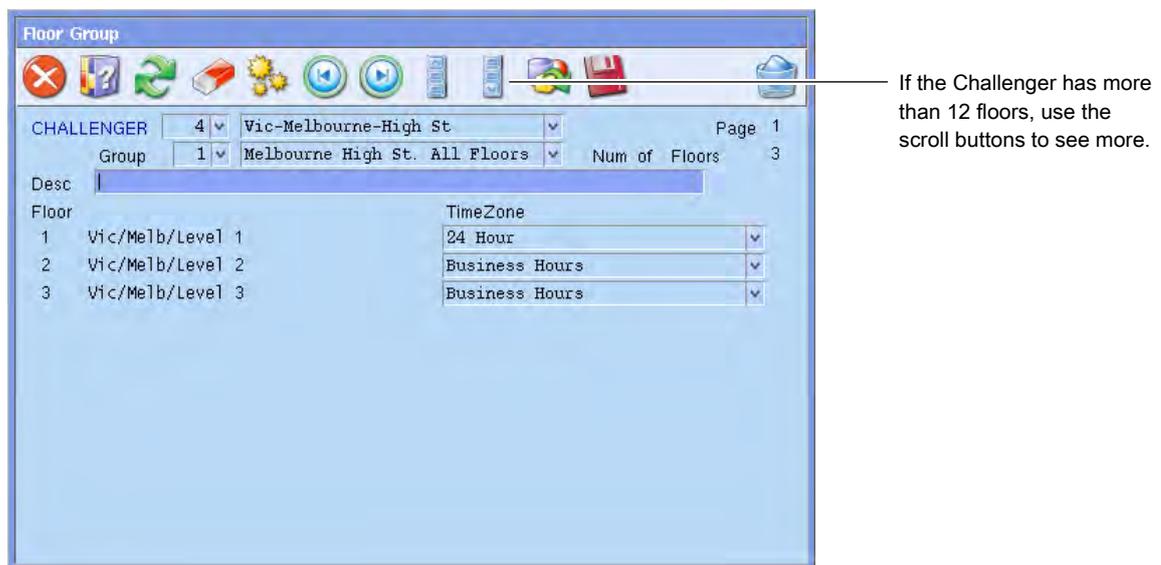
TimeZone fields. Select the timezone for the corresponding door. To create a new timezone, double-click the TimeZone field (or press F3), program the required timezone, and save. The timezone will be added to the list of timezones for this Challenger. (You must first enter a door group number and ID.)

Floor Groups

Use the Floor Groups option to allocate access levels to users. Floor groups define which floors users are able to get access to and at what times they are able to use each floor.

Note: For a user to be given access to a floor, they must be given a floor group and a door group. This is because the floor group determines what floors they can access and the door group determines what lifts they can use.

Figure 59: Challenger programming window for floor groups



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Group. Use the group number and name as follows:

- The number field represents the floor group number in the Challenger. To create a new floor group, enter the new number of the floor group. Select the timezones required for each floor in the list shown on the form. Challenger V8 panels with firmware version 8.128 or later support 128 floor groups. Other versions support 64 floor groups.

- The ID field represents the Floor Group ID in Forcefield. To create a new floor group enter the new ID of the floor group (Forcefield will automatically add the floor group number when saving). Select the timezones required for each floor in the list shown on the form.

Note: A floor group cannot be programmed unless a Challenger ID and a floor group ID are entered.

Desc. Describe the function of the floor group.

Floor fields: Once a Challenger has been selected, the floors programmed to that Challenger will be displayed in the floor fields.

Note: Even though the floor is listed, it is not part of the group until it has a timezone attached to it.

TimeZone fields: Select the timezone for the corresponding floor. To create a new timezone, double-click the TimeZone field (or press F3), program the required timezone, and save. The timezone will be added to the list of timezones for this Challenger. (You must first enter a Floor Group number and ID.)

Generate IUM Data

See “Generating IUM data” on page 45.

Modify Profile Access

Use the Modify Profile Access option to add or delete up to three access groups (one each of alarm group, door group, and floor group) for selected user profiles. User profiles may be selected individually or by member.

Access groups can be from the same or from different Challenger panels. For example, the door group may be selected from one Challenger and the alarm group from a different Challenger.

A report is generated listing the affected users.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Action. Select to add or delete the specified access groups.

Selected Profiles. Select one or more profiles to which the modifications are to be made. Selecting a member without selecting individual user profiles will result in the changes being made to every user profile in the selected member.

Challenger and Access Group. In the rows for Alarm, Door, and Floor, select a Challenger or leave blank to list the group records for all Challenger panels. Next, select the alarm group, door group, and floor group to be added or deleted from the selected user profiles. Leave a field blank to skip it.

Refer to “Generating reports” on page 28.

Alarm Group Report

Use the Alarm Group Report option to print out the contents (such as areas, control options, menu options) of alarm group(s). You must select a Challenger for the report to run.

Refer to “Generating reports” on page 28.

Door Group Report

Use the Door Group Report option to printout the contents (doors and the timezone for each door) of door group(s). You must select a Challenger for the report to run.

Refer to “Generating reports” on page 28.

Floor Group Report

Use the Floor Group Report option to printout the contents (floors and the timezone for each floor) of floor group(s). You must select a Challenger for the report to run.

Refer to “Generating reports” on page 28.

Users By Alarm Group

Use the Users By Alarm Group option to list the alarm groups in ID order and lists the users who are allocated it. This can be done on one alarm group or all alarm groups in one Challenger. You must select a Challenger for the report to run.

Refer to “Generating reports” on page 28.

Users By Door Group

Use the Users By Door Group option to list the door groups in ID order and the users who are allocated it. This can be done on one Door Group or all Door Groups in one Challenger.

Refer to “Generating reports” on page 28.

Users By Floor Group

Use the Users By Floor Group option to list the floor groups in ID order and the users who are allocated it. This can be done on one Floor Group or all Floor Groups in one Challenger. You must select a Challenger for the report to run.

Refer to “Generating reports” on page 28.

Users > Modify Status menu

Change Status of User

Use the Change Status of User option to enable the operator to change a user's card status. Although this can be achieved through User > Maintenance, the Change Status of User command allows the operator to only change the status, and so is suited to operators who do not have permission to modify user databases.

Note: Changing a user's status can deny them access to alarm control and doors, so ensure that you have selected the correct user.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Change to. Select the new status type for the user:

- **Lost**—no longer able to access any part of the system. Will generate a 'Lost Card' alarm if the card is badged on the system.
- **Void**—no longer able to access any part of the system. Will generate a 'Void Card' alarm if the card is badged on the system.
- **Lost & Log Offsite**—as above, however now adds an event into history to log the user off site for various reports.
- **Void & Log Offsite**—as above, however now adds an event into history to log the user off site for various reports.
- **Log Offsite**—adds an event into history to log the user off site for various reports. This is used when the user is no longer on site, yet the system is indicating that the user still is. Normally due to the user not badging their card when leaving the premises.

Set users offsite

See "Set users offsite" on page 50 for details.

Users > Profiles menu

Assign Profile to Users

This option does not apply to Unique Profile Per User mode. See "Configuring user options" on page 232.

Use the Assign Profile to Users option to assign a previously-created profile to one or more users. The users to which the profile is to be assigned may be selected by user number or range of numbers, and filtered by member group and/or member.

Note: This command applies the profile to the selected users and changes the Challenger access for those users. Use the sync profile data command (see “Sync Profile Data” on page 151) to apply profile changes other than Challenger access.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

User Range from and to fields: If a user number range is selected, the profile will be assigned only to the users within the number range, regardless what other selection criteria have been used.

Profile. Select the profile be assigned to the selected user(s).

Profile Ends fields: If the profile is time-limited, enter the time and date that the profile expires. If blank, the profile will not expire. After the profile has expired, the Profile field on the User Maintenance window is marked by red double-asterisks ‘**’. See “Maintenance” on page 131 for details.

Alt Profile. The profile to be applied when the primary profile expires. For example, a profile can be assigned to cleaners for special hours during a holiday, which expires at the end of the holiday. When the Alt profile expires, the cleaners’ usual profile takes over.

Program Profile

Use the Program Profile option to create or modify user profiles.

A profile is a collection of user information such as member, date range, position, department, card type, trace, long access, card only, privileged options, and Challenger access.

Changes to a profile’s Challenger access data is automatically applied to previously-created user records attached to the profile; altering other profile data is not automatically applied. For example, if you change the dates in a profile, this change will not automatically be applied to previously-created user records attached to the profile (only users created after the profile change will get the new dates).

In order to update previously-attached user records with revised profile data use the sync profile data command (see “Sync Profile Data” on page 151).

Note: Altering or deleting a profile may affect many user records as all their access rights must be checked (and altered if necessary) and downloaded to Challenger panels.

Figure 60: User Profiles programming window

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Disallow Auto Deletion. Select to prevent this record from being deleted when using the Delete Unused Data command if this record is not referenced by any user records. Select this option when creating template user profiles.

Import button (active only for a saved profile). Allows a profile's contents to be copied from another profile. A profile can be saved with just an Id, and it will be given the system default member, date starting from creation time, and a normal card type. See "Importing user profile data" on page 56 for details about using the Import button.

Member. The profile must be allocated a member ID to determine where events associated with users are to be directed. The member in the profile will also be the member of any users assigned to this profile (unless individually changed at the user record level).

Start fields. Each user must have a start/end date-time to have access to the Challenger panels. A user that is programmed with the present date and time is downloaded to the Challenger(s) when the user record is saved (not dialler-connected Challenger panels). When a user is programmed with a future date-time the user record is not downloaded immediately. Forcefield automatically downloads the user on the date it becomes active.

End fields. The end date and time is used to automatically remove the user's record from the Challenger(s). The user record is not deleted from Forcefield, just made expired.

Position. This field is described in "Maintenance" on page 131.

Department. This field is described in "Maintenance" on page 131.

Card Type field and user flag selections. These fields are described in "Maintenance" on page 131.

Door button. See “Programming Door Groups For a Profile” below.

Floor button. See “Programming Floor Groups For a Profile” below.

Alarm button. See “Programming Alarm Groups For a Profile” on page 150.

Programming Door Groups For a Profile

Click the Door button on the User Profiles window to program, allocate and view the Challenger door groups for this profile.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Timed button. Click to program times and dates for a user with this profile to have this access group only during the time specified in the subsequent window. See “Programming timed access” on page 150 for details.

List button. Displays the profile’s group IDs.

Expand button. Displays the profile’s group IDs and their timezones.

Restore button. Restores the list of Challenger panels after the Find Ch button reduced the list.

Find Ch button. Opens a Challenger search window to enable rapid selection of a Challenger from the list.

Note: If you press F8 whilst using this screen, you will delete all of the Challenger Door Group access records that have been assigned to this profile.

Programming Floor Groups For a Profile

Click the Floor button on the User Profiles window to program, allocate and view the Challenger floor groups for this profile.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Timed button. Click to program times and dates for the access group to be active at a particular Challenger panel. See “Programming timed access” on page 150 for details.

List button. Displays the profile’s group IDs.

Expand button. Displays the profile’s group IDs and their timezones.

Restore button. Restores the list of Challenger panels after the Find Ch button reduced the list.

Find Ch button. Opens a Challenger search window to enable rapid selection of a Challenger from the list.

Note: If you press F8 whilst using this screen, you will delete all of the Challenger Floor Group access records that have been assigned to this profile.

Programming Alarm Groups For a Profile

Click the Alarm button on the User Profiles window to program, allocate and view the Challenger alarm groups for this profile.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Timed button. Click to program times and dates for the access group to be active at a particular Challenger panel. See “Programming timed access” below for details.

List button. Displays the profile’s group IDs.

Expand button. Displays the profile’s group IDs and their timezones.

Restore button. Restores the list of Challenger panels after the Find Ch button reduced the list.

Find Ch button. Opens a Challenger search window to enable rapid selection of a Challenger from the list.

Note: If you press F8 whilst using this screen, you will delete all of the Challenger Alarm Group access records that have been assigned to this profile.

Programming timed access

Access groups may have timed access programmed, which Forcefield uses to determine when the access applies to users of the profile. Timed access works as follows:

- If programmed, then the access is given to the user only during the time specified here, with the proviso that the time assigned to the user record is not extended by any times assigned to the access group at the profile level. Time access can only limit, not extend, the user’s access.
- If not programmed, then the access is given to the user at all times the user is active.

Example 1: We have some users who we normally want to have access to particular doors. If we want these users to have alarm group access only during a particular time period, we would create a profile that has a door group with no timed access programmed, and an alarm group with timed access programmed for the particular time period.

Example 2: We have some users who need continuous access to Challenger A’s doors and timed access to Challenger B’s doors. The profile would therefore have two door groups: one door group assigned to Challenger A (without timed access), and the other door group assigned to Challenger B (with timed access).

For the particular door group, floor group, and/or alarm group, click the Timed button to program times and dates for the access group to be active for a particular Challenger panel. The timed access programming window displays.

Figure 61: Timed Access Window

Type the time and dates required for the profile to be active at the Challenger panel, and then click Close.

Sync Profile Data

Use the Sync Profile Data option to synchronise selected users or all users to the profile data after modifying a profile to ensure that users of the profile now have the same data as the profile. The users to which the profile is to be assigned may be selected by one or more user numbers, or by range of user numbers, and filtered by member group and/or member.

Note: This command is not required if only the Challenger access data has been changed. Challenger access data, if changed in the profile, is automatically applied to all users of the profile.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

User Range from and to fields. If a user number range is selected, the profile will be assigned only to the users within the number range, regardless what other selection criteria have been used.

Matching Profile

Use the Matching Profile option to list user profiles that match selected criteria. If multiple criteria are selected, the report shows the profiles that have all the criteria.

Refer to “Generating reports” on page 28, and the following details about this report.

Options selections. Enables matching criteria for on or off settings of Trace, Card Only, Long Access, and Privileged access.

Profile Access Report

Use the Profile Access Report option to show door, alarm, and floor access groups associated with user profiles.

Refer to “Generating reports” on page 28, and the following details about this report.

Click the Detail arrow, and then select one of:

- Groups—to list Challenger access groups.
- Detail—to list Challenger access groups and profile details.
- C.S.V.—to list Challenger access groups in CSV format (profile ID, access group type, Challenger number, access group number, access group ID).

Profile Report

Use the Profile Report option to show information associated with user profiles as selected by the report type.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the required report type:

- Summary—lists Challenger access groups
- Detailed—lists Challenger access groups and their details
- Users—lists users belonging to the profile
- Mismatch—lists users belonging to the profile, but who do not have the Challenger access that the profile requires.

Users > Reports menu

Activation Report

Use the Activation Report option to list all users who will become active on a given date or date range.

Refer to “Generating reports” on page 28, and the following details about this report.

Format. Select the required format:

- Summary lists the user number and name.
- Detail lists user number and name, active date range, PIN indication, profile, department, and position.

Report formats are further divided into:

- Multi-line is the preferred format for sending the report to a printer. It formats the reports to fit the printer page and will generate a title header for each page of output.
- Single-line places all data for one user into a single line of text. There is only one title header. This format would be used for data input into an external package.

- CSV has no title header. It contains a user 0 (zero) that does not actually exist, but is generated to indicate the date-time range chosen for the report. Data in this format is typically used in a spreadsheet or database application.

Sort Order. Select the required report sort order:

- Num. Sort by user number.
- Num by time. Sort by user number each time users became active.
- Name. Sort by user name.
- Name by time. Sort by user name each time users became active.

Area Control Report

Use the Area Control Report option to list the areas selected and displays the users with control to the areas.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the required type:

- Summary lists the user number and user name for each user having control on that area(s).
- Detailed lists all the user details as per the user maintenance screen having control on that area(s).

Card (User) Report

Use the Card (User) Report option to list various details of one or more users.

Entering data in more than one field will restrict the report to users having the specified data from all the completed fields. For example, entering ‘Smith’ for a name and ‘Engineering’ for a department will report on names beginning with ‘Smith’ (including ‘Smithson’, ‘Smithers’, etc.) in Engineering.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the required type:

- Ch. Num. Lists user number and names card status, begin and end dates, profile, position, and department, with the addition of the user’s number in each Challenger to which they have been downloaded.
- List - Multi Line. Lists user number and names card status, begin and end dates, profile, position, and department. This format is suitable for reports: each user’s data is formatted over possibly several text lines.
- List - Single Line. Lists user number and names card status, begin and end dates, profile, position, and department. Format suitable for

importation into external packages: each users data is contained on one text line.

- List - CSV. Lists user number and names card status, begin and end dates, profile, position, and department. Data in this format is typically used in a spreadsheet or database application.
- Summary. Lists the details from the User Maintenance window, including user notes, but not including the PIN (if used).
- Summary - CSV. Lists the details from the User Maintenance window, including a 'PIN' or 'No PIN' indication, but not including user notes. The format is suitable for exporting to external packages (such as Microsoft Excel) capable of reading CSV data.
- Detailed. Lists the details from the User Maintenance window, plus users' access groups.
- Expanded. Lists the details from the User Maintenance window, plus details of the contents of the access groups.
- Expired Profile - List. Lists only users whose primary profile has expired. This format is suitable for reports: each user's data is formatted over possibly several text lines.
- Expired Profile - CSV. Lists only users whose primary profile has expired. The format is suitable for exporting to external packages (such as Microsoft Excel) capable of reading CSV data. PIN codes are not shown, only an indication of whether the user has a PIN code.
- Expired Profile - Summary. Lists only users whose primary profile has expired. Lists the details from the User Maintenance window, including user notes, but not including the PIN (if used).

Sort by. Select the required report sort order:

- Num—sort by user number.
- Name—sort by user name.

PIN. Enter a user's PIN to generate a report on a single user.

User Defined fields. Select a pre-defined title (defined in the associated Member form) and optional values upon which the report will be generated. Each additional user defined field further restricts the results.

Door Access Report

Use the Door Access Report option to list the doors selected and displays the users with access to those doors.

Refer to "Generating reports" on page 28, and the following details about this report.

Report Type. Select the required type:

- Summary lists the user number and user name for each user having access to the door(s)
- Detailed lists all the user details as per the user maintenance screen having access to the door(s).

Expired Profile

Use the Expired Profile option to list all users whose profile will expire on a given date or date range.

Refer to “Generating reports” on page 28, and the following details about this report.

Format. Select either summary or detail:

- Summary lists the user number and name.
- Detail lists user number and name, active date range, PIN indication, profile, department, and position.

Report formats are further divided into:

- Multi-line: The preferred format for sending the report to a printer. It formats the reports to fit the printer page and will generate a title header for each page of output.
- Single-line: Places all data for one user into a single line of text. There is only one title header. This format would be used for data input into an external package.
- CSV: This format has no title header. It contains a user 0 (zero) that does not actually exist, but is generated to indicate the date-time range chosen for the report. Data in this format is typically used in a spreadsheet or database application.

Sort Order. Select the required report sort order:

- Num—sort by user number.
- Num by time—sort by user number each time users became active.
- Name—sort by user name.
- Name by time—sort by user name each time users became active.

Expiry Report

Use the Expiry Report option to list all users who will expire on a given date or date range.

Refer to “Generating reports” on page 28, and the following details about this report.

Format. Select either summary or detail:

- Summary lists the user number and name.
- Detail lists user number and name, active date range, PIN indication, profile, department, and position.

Report formats are further divided into:

- Multi-line: The preferred format for sending the report to a printer. It formats the reports to fit the printer page and will generate a title header for each page of output.
- Single-line: Places all data for one user into a single line of text. There is only one title header. This format would be used for data input into an external package.
- CSV: This format has no title header. It contains a user 0 (zero) that does not actually exist, but is generated to indicate the date-time range chosen for the report. Data in this format is typically used in a spreadsheet or database application.

Sort Order. Select the required report sort order:

- Num—sort by user number.
- Num by time—sort by user number each time users became active.
- Name—sort by user name.
- Name by time—sort by user name each time users became active.

Floor Access Report

Use the Floor Access Report option to list the users with access to selected floors.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the required type:

- Summary lists the user number and user name for each user having access to the floor(s)
- Detailed lists all the user details as per the user maintenance screen having access to the floor(s).

Idle User Report

Use the Idle User Report option to list all users who have not badged during the selected date range.

Refer to “Generating reports” on page 28, and the following details about this report.

Show Access Outside Date Range. Check the box to report a user's last access details if they have not used the system during the specified date range, but have accessed at another time.

Format. Select either summary or detail:

- Summary lists the user number and name.
- Detail lists user number and name, active date range, PIN indication, profile, department, and position.

Report formats are further divided into:

- Multi-line. The preferred format for sending the report to a printer. It formats the reports to fit the printer page and will generate a title header for each page of output.
- Single-line. Places all data for one user into a single line of text. There is only one title header. This format would be used for data input into an external package.
- CSV. This format has no title header. It contains a user 0 (zero) that does not actually exist, but is generated to indicate the date-time range chosen for the report. Data in this format is typically used in a spreadsheet or database application.

Sort Order. Select the required report sort order:

- Num—sort by user number.
- Name—sort by user name.

Last Access By A User

Use the Last Access By A User option to list the last reader accessed by user(s). The following data is reported user number, user name, reader, time, and region.

Refer to “Generating reports” on page 28, and the following details about this report.

Sort Type. Select the required report sort order:

- Num—sort by user number.
- Name—sort by user name.

Formats. Select the required format:

- Multi-line. The preferred format for sending the report to a printer. It formats the reports to fit the printer page and will generate a title header for each page of output.
- Single-line. Places all data for one user into a single line of text. There is only one title header. This format would be used for data input into an external package.

- CSV. This format has no title header. It contains a user 0 (zero) that does not actually exist, but is generated to indicate the date-time range chosen for the report. Data in this format is typically used in a spreadsheet or database application.

Muster Report

Typically used for evacuation reports, use the Muster Report option to list on-site users who either:

- Are mustered.
- Are not mustered.

To be mustered, a user needs to have recently badged at a muster reader (recent in terms of when the report is run). How recent depends on the muster time defined in Forcefield configuration (default is 15 minutes). See “Configuring user options” on page 232 for details.

For a RAS or door to be a muster reader, the Muster Reader check box must be selected (see “Arming Stations” on page 260 or “Door Access” on page 282).

Refer to “Generating reports” on page 28, and the following details about this report.

Type. Select the required report type:

- Not Mustered—users who have not mustered within the muster time.
- Mustered—users who have mustered within the muster time.

Users who are off site will not appear in the report (region 0 is always considered as off site).

Sort by. Select the required report sort order:

- Num—sort by user number.
- Name—sort by user name.

The optional member group and member fields serve to restrict users who should be included in the report.

Unused Data Report

Use the Unused Data Report option to list user-related data that is no longer referenced in any records.

Refer to “Generating reports” on page 28, and the following details about this report.

Unused data types to report check boxes: Select one or more types of data for departments, positions, user defined data, or user profiles.

Format. Select either printer or CSV. Data in CSV format is typically used in a spreadsheet or database applications.

User Access Report

Use the User Access Report option to list access information for selected users, showing their current status, card start date, card end date and optionally their access groups depending on whether the group options are checked.

Refer to “Generating reports” on page 28, and the following details about this report.

Sort Order. Select the required report sort order:

- User number
- User name
- User number by department
- User name by department

Detail. Select the required level of detail:

- Groups lists the access groups.
- Detail lists the access groups as well as areas, doors, and floors.
- Groups-C.S.V. lists the access groups in a CSV format (refer to online help for details).

Door Group selection. Check this box if you want the report to include the user’s door groups.

Alarm Group selection. Check this box if you want the report to include the user’s alarm groups.

Floor Group selection. Check this box if you want the report to include the user’s floor groups.

User On-Site Report

Use the User On-Site Report option to report on the movements of users around the site. On site is considered to be a Challenger region other than region zero. If a user is considered to be still on site, the on site value will have an appended plus (+) sign.

Note: The date and time specified relates to the times logged into history from the door/reader at which the cards were badged. This has no bearing on your local computer time and time zone location. For example, if you are in Perth and you select the times for the search to be 09:00 to 17:00 on the same day, then the report will look for times 09:00 to 17:00 as reported by the Challenger panels irrespective of what time zone you are in.

Refer to “Generating reports” on page 28, and the following details about this report.

Start fields: If no begin date is entered, the report will start from the first record found in the history.

End fields: If no end date is entered, the report will finish at the current date of your local computer.

Type. Select the required report type:

- **Summary:** Lists totals for each region visited by the user. A visit is considered to be active until the user enters region zero. Therefore, from the time the user is on site until the time the user is off site is considered a visit.
- **Detailed:** Lists all regions and durations each time the user enters and leaves that region, and then a total time for being on site during the date & time range.
- **Totals:** Lists only the total time on site without the region times.
- **CSV Formatted Data:** Data in this format is typically used in a spreadsheet or database application that requires dates to be in human-readable format.
- **CSV Raw Data:** Data in this format is typically used in a spreadsheet or database application that can interpret raw data. Dates are not in human-readable format.

Users By Region Report

Use the Users By Region Report option to list on-site users who are in or out of a specified region.

Only users who have accessed the system and are on site are reported. Thus users may be in the user database but not appear in this report. For this report to function, Challenger panels must be setup to report user access by region.

Refer to “Generating reports” on page 28, and the following details about this report.

Out of Region selection. Check this box if the report is to list users who are out of the selected region.

Sort by. Select the required report sort order:

- **Num:** Sort by user number.
- **Name:** Sort by user name.

Users > Smart Card Programmer menu

Display User Card

This command requires the use of a working Smart Card Programmer. Use the Display User Card option to display the data read from a user card.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

User Num. This field displays a list of users that the card data belongs to.

Read button. Place a card on the Smart Card Programmer and then click Read to read user card data. If card data read is successful, the card data is displayed on screen.

Cancel button. Click to cancel the read command.

Issue User Card

The Issue User Card option requires the use of a working Smart Card Programmer to program user cards. Refer to the *Forcefield External Interfaces Manual* for details.

Reader Config Card

The Reader Config Card option requires the use of a working Smart Card Programmer to program user cards. Refer to the *Forcefield External Interfaces Manual* for details.

Setup Programmer

The Setup Programmer option requires the use of a working Smart Card Programmer. Refer to the *Forcefield External Interfaces Manual* for details.

Users > Transfer User Data menu

Export User Data

Use the Export User Data option to export user data to a remote computer system, in either comma separated value (CSV) or tab separated value (TSV) format.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

User Num. Enter a user number to export only that user.

PIN. Enter a user's PIN to export only that user.

Name. Entering a name will export all USERS having matching names. Example; if 'smith' is entered, users such as 'smith', 'smithers', 'smithson', etc. will be exported.

Export to. Select the required storage device.

in Format. Select the required format:

- CSV—File created is userexp.csv. In this format there is 1 text line per user with data in double quotes separated by commas (e.g. "datafield1","datafield2", "...", "datafield n").
- TSV—File created is userexp.tsv. In this format there is 1 text line per user with data separated by tabs (e.g. datafield1<Tab>datafield2<Tab>..
..<Tab>datafield).

Refer to the *Forcefield External Interfaces Manual* for details on export file formats.

Note: Event triggering by time can be used to export all user data or photos, or to export only the records that have been changed since the last export. See “User data export” on page 84 and User photo export” on page 84.

Import User Data

Used the Import User Data option to initiate a manual importation of user data from an external source. A result report will be generated and sent to the selected report destination. Forcefield will attempt to read the file “user.imp” on the storage selected by the operator.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Import data from. Select the destination directory or device.

Refer to the *Forcefield External Interfaces Manual* for details on import file formats, and to related settings for Import User Data field on page 233.

Users > User Numbering menu

Show System User Number

Use the Show System User Number option to show what Forcefield system user number has been allocated to a Challenger user.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Enter the Challenger and the user number in that Challenger. Click Run (or press F6) to display the Forcefield user number assigned.

Show Ch. User Number

Use the Show Ch. User Number option to show the translation between the Forcefield user number and the corresponding user number downloaded to the Challenger panels.

For example, Forcefield user 3 may be:

- User 5 in Challenger 1
- User 56 in Challenger 123
- User 12345 in Challenger 45, etc.

Select a user by Forcefield number or name, and then click List (or press F12) to display the translation list.

Operators menu

Operator Permissions

Use the Operator Permissions option to control the level of authority an operator has to the Forcefield functions.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

See also “Workstation Permissions” on page 172.

Use the List button to look up records (such as operator or workstation records) that use the selected Computer Access record.

Id. A unique name for the Forcefield computer access record.

Functions. This is the ID of a record containing a list of Forcefield functions.

These records determine the menu access granted to an operator. For a list of existing function records press F4. If the function required is not available, enter the new required ID and press F3. To edit an existing function record, enter the function ID and press F3. Deleting a function record is not allowed from this screen. It is performed from Operators > Functions.

Member Group. restrict which members the operator has access to. Therefore only certain alarms and control can be given to each operator.

Time Zone: Select a suitable time zone. If no time zone is suitable, enter a new time zone ID, press F3 and create a new one. This time frame validates when the operator can access the Forcefield system. Note: Forcefield does not use the holiday indication on time zones for determining operator access. If the operator attempts to log in and the time zone is not valid, and an alternative computer access level is given, the alternative access will be used if its time zone is valid. See Alternate field, below.

Alternate. Alternative access is used to give an operator a different set of menus and member access depending on the time of day and day of week. An operator can have three different sets of access levels which are assigned in the following order until a valid time zone is found:

1. The original access level.
2. The alternative access level.

3. The alternative access level of the previous alternative access level.

Operator Menu Permissions

Use the Operator Menu Permissions option to create, modify, or remove a computer functions record.

This can also be performed from “Operator Permissions” on page 163, however, doing it here allows function records to be created without having to first create Operator Permissions records.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Use the List button to look up records (such as operator or workstation records) that use the selected computer functions record. See also “Workstation Permissions” on page 172.

Id. This is the ID of a record containing a list of Forcefield functions (menus that an operator can use). For a list of existing function records press F4. If the function required is not available, enter the new required ID (for example, Alarm Monitoring) and press F3. To edit an existing function record, enter the function ID and press F3. To delete an existing function record, first press F12 to find any Computer Access records that use the selected function record (you cannot delete a functions record that is currently used).

Select a Computer Functions record, and then press F3 to display the programming window. This window is used in the same manner as described in “Workstation Permissions” on page 172.

Operator Setup

Use the Operator Setup option to add, modify, and delete operators. To add, modify or delete any operators you must have the same or higher computer access level than the operator record that you are attempting to add, modify or delete. You cannot create an operator with access to more functions than you have.

To find operators having a particular computer access level, use the Shift+F4 search function. Once in search mode, press the icon or press Shift+F4 to return to normal mode.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Login Code. A login code is required for the operator to log into Forcefield.

Password. A password is (by default) required for the operator to log into Forcefield. A minimum of 4 characters must be used. However, this may be altered by your System Administrator. The password is case sensitive (abcd is not the same as aBcd).

Forcefield Access. Click the arrow to select the Computer Access record for the operator. Alternatively, double-click the field to create a new Computer Access record. This access record is used to set the Forcefield functions an operator will be allowed to access. The workstation must have the function allowed as well, unless the operator access member group contains the “Override Member”, in which case a function allowed for the operator will be allowed regardless of the workstation settings.

Name. A name is required. This name is displayed at the top right hand corner of the screen when the operator is logged in.

Phone. Optional data for administration purposes only.

Other Data fields: Optional data for administration purposes only.

Do Not Alert When Changing Database Records. Selecting this option suppresses the warning that is given to the operator when they have altered some data on the data entry screen of a database record and they have pressed escape without first saving the record.

Card Num. Used for operators logging on to the system via an access card. Enter the access card number.

Card Site Code. Used for operators logging on to the system via an access card. Enter the access card site code.

Operator Password

Use the Operator Password option to alter an operator’s password. As a security precaution there is no search facility: you must know the login code.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Login Code. Enter your login code, press Enter. The password field will become active. Enter the old password. Upon successful entry of the old password, Forcefield will prompt for the new password. Forcefield will then prompt for confirmation of the new password. Forcefield will automatically save the new password upon its second entry.

The minimum number of password characters is configurable from “Configuring login options” on page 229.

Operator Report

Use the Operator Report option to generate reports listing details of one or more operators.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the required report type:

- Summary—displays the operators' details as they appear in the operator database (passwords are not shown).
- Detailed—displays the operators' details as they appear in the operator database (passwords are not shown), plus the Forcefield Access level.
- Expanded—displays the operators' details as they appear in the operator database (passwords are not shown), the Forcefield Access level, plus members and member groups, menu functions, timezone allocation, and the alternate access level.

Databases menu

Email Addresses

Use the Email Addresses option to store the email addresses of recipients you wish to contact via Forcefield Email Paging.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Enter an ID for the recipient.

Address. Enter the full email address of the recipient, e.g.
fredblogs@myplace.com.au.

Note: An email server address must be set up by an administrator. See "Configuration" on page 226.

Holidays

Use the Holidays option to program Challenger holiday records.

If the holiday is attached to a Challenger, any changes made to the holiday record are automatically downloaded to the appropriate Challenger panels. Holiday is only used for Challenger timezones. Forcefield does not use the holiday indication.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. The name must be unique to each holiday.

Device Locale

Use the Device Locale option to set up centralised time zone control for the Forcefield system, and thereby control the time used in Challenger panels and Forcefield clients, even if located in different time zones from the Forcefield server.

For example, the Forcefield server may be in Melbourne with Challenger panels connected to it that are located in Sydney and Perth. If a location has daylight saving time, then the start and end dates for daylight saving time must be entered. The time of switching between standard and daylight saving time is at 2 a.m. on the scheduled day.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Enter an ID for the location timezone, e.g. Melbourne, Coober Pedy or even Fred's Location.

TimeZone. This is the time zone location, e.g. Australia–Central, Australia–East Coast, United Kingdom.

Has Daylight Saving. Check the box if the time zone has daylight saving time. Setting this flag will bring up the data entry fields for daylight savings data.

Daylight Savings Starts and Ends fields: Select the start and end times for daylight saving time (e.g. Last Sunday March).

Note: Daylight saving time is assumed to switch in and out at 2 a.m.. If going into daylight saving time, the time becomes 3 a.m.; going out of daylight saving time, the time becomes 1 a.m..

Databases > Computer Equipment menu

Use the Computer Equipment menu to program the items relating to computer hardware.

Node

Use the Node option to change the name of the Forcefield primary controlling node (server computer) and to create additional nodes (the use of additional nodes is subject to licensing).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Node. Select the required node.

Id. Enter the unique computer ID.

Printer Permission

Use the Printer Permission option to create printer access records to control which events can be directed to a printer. An event can be directed to a printer only if the member of the event is in the member group of the printer's assigned access.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. The identifier given to this Printer Permission record.

Member Group. Select a member group that determines from which devices events will be printed. Only events from devices having a member in this group will be printed.

TimeZone. Select a time zone to determine when this record is valid. If this record is not valid because it is out of the time zone, any alternate record will be used if its time zone is valid. Thus a printer may be set to print all events from all devices during office hours but only events from a limited range of devices at other times.

Alternate Access. allows the printer's access levels to change according to time of day. A printer can have three different sets of access levels which are assigned in the following order until a valid time zone is found:

- The original access level.
- The alternative access level.
- The alternative access level of the previous alternative access level.

Printers

If your Forcefield system requires a printer to view reports and/or print events, use the Printers option to create printer records.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Enter a unique name for the printer.

Location. Type a short description of the location of the printer.

Desc. Type a short description of the function of the printer.

Printer Access. Printer Access is used for programming which members have access to the printer. For an event printer, only events from devices having a member in the Printer's Access will be printed. To create a new Printer Access, clear any text in this field, and then double-click the field.

Print Reports. Check this selection if the printer is to print reports.

Add Form Feed after Report. Check this selection to add a form feed at the end of a report (some printers require a form feed in order to print out the last page of a report).

Print Events. Check this selection if the printer is to print live events. An event can be directed to a printer only if the member of the event is in the member group of the printer's assigned access.

Note: When a report is to be printed and both Print Reports and Print Events are selected, Forcefield sets the printer to a new page, prints the report, sets the printer to a new page, and then resumes printing events from where it left off.

In Format. Select the format required for event reporting.

Paper Width. Sets the number of columns of text the printer will print. If this is blank Forcefield will default to 80 characters.

Paper Height. Sets the number of lines of text the printer will print. If this is blank Forcefield will default to 60 lines.

Type. Select the type of the printer. Options include:

- Serial (a field displays for specifying the port)
- Parallel (a field displays for specifying the port)
- Network (fields display for specifying the host, remote name, and print cap)
- Client (a field displays for specifying the workstation)

Port field (for serial or parallel printers) : Select the port used to connect the printer to Forcefield. Double-click the field to define a new port.

Host (for network printers). Select a TCP/IP host used to connect the printer to Forcefield. Double-click the field to define a new TCP/IP host.

Remote Name (for network printers). This is the ID of the printer as known by the remote print server.

Print Cap Entry (for network printers). This is the ID of the print cap entry for this printer.

Workstation (for Forcefield Client printers). Select a workstation.

Computer Cat. Select the computer category. The computer category determines how Forcefield will handle an event from this printer.

Maps. Indicates any maps to which the printer has been added.

Help. User-programmable help screen. The help programmed here will be the help displayed as “action” on the alarm screen if this printer generates an alarm.

Serial & Parallel Ports

Use the Serial & Parallel Ports option to define serial or parallel port records. These are used for connecting external equipment to Forcefield. TCP/IP ports and addresses are handled separately.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Enter a unique name for the port.

Type. Select the option applicable to the equipment to be connected. Challenger dialler and Technical Support type ports have associated processes that are automatically started when the port record is created. For example, adding a Challenger dialler type port causes a Challenger CommsDial process to be started.

Node. Select the required node.

Device. Used to connect the Forcefield software to the server hardware. This list is generated by the operating system and needs the node number field to be entered so Forcefield can interrogate the server hardware.

HandShake. Select the type of handshaking the device uses.

- NONE—No handshaking.
- H/W—Hardware handshaking.
- S/W—Software handshaking.

Baud Rate. Select the communication speed of the device.

Parity. Select the type of parity the device is using.

Data Bits. Select 7 or 8 data bits. The default data length is 8 bits.

TCP/IP Hosts

Use the TCP/IP Hosts option to define TCP/IP addresses (Forcefield assumes all hosts have static addresses). A TCP/IP host is typically used for:

- an NFS export destination (see “NFS Exports” on page 180)
- a DVR connection (see “DVRs” on page 201)
- network printers (see “Printers” on page 168)
- for IP-connected Challenger panels.

See also “Network Configuration” on page 239.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Host Id. Enter a unique name for the TCP/IP Host.

Address. Enter the IP address., e.g. 128.37.28.1.

Node. Select the required node.

Connect Timeout in seconds. Specify the number of seconds that Forcefield will try to connect to the given IP address before it gives up.

TCP/IP Ports

Use the TCP/IP Ports option to define TCP/IP ports (used primarily for IP-connected Challenger panels). See also “Network Configuration” on page 239.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

IP Port. Enter a unique name for Forcefield to identify the TCP/IP port.

Number. Enter a valid port number, in the range 1024 to 65535.

Controlled by System Node. Select the required node.

UPS

This command applies to Forcefield Enterprise hardware only. Use the UPS option to configure the uninterruptible power supply (UPS). The use of a UPS is strongly recommended.

The UPS window allows the operating condition of a UPS connected to the system to be monitored. In the event of mains and/or battery failure the system will be automatically shut down to protect its databases and files from corruption.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

UPS Monitoring for Node. Select the node the UPS is connected to.

Active. Check the box to enable the selected node to monitor its UPS.

UPS Detection Method. Select one of the following options:

- Watchdog card—requires the installation of a watchdog card into the Forcefield server computer. A watchdog card provides instant response.
- Serial port—Forcefield will periodically poll the selected serial port for UPS status. Mains level indication connects to the CTS pin of the port. Battery level indication connects to the CD pin of the port. Failure level is always low.

Serial Port. Select the serial port used to monitor the UPS Status. The port must be programmed as type “Serial (Other)”.

Monitor Mains Fail. Check the box to enable mains fail monitoring.

On Watchdog Input. Select the input number for the monitoring device.

Fail Level. Select the fail level (i.e. high or low). Low is typical.

Monitor Low Battery. Check the box to enable low battery monitoring.

Warning Repeat Interval. Enter the number of seconds delay before the next warning will be generated. The warnings will continue to be issued at this rate until either shutdown or the UPS is fully active again.

Workstation Permissions

Use the Workstation Permissions option to program which functions are allowed for the chosen workstation type. Functions that are not programmed to the workstation type will not be permitted regardless of operator or workstation access programming.

Note: Do not remove access to the workstation access function or you will never be able to change it again.

Type. Select the type of workstation.

After selecting the required workstation type, double-click the field to open the Menu Access Programming window, which is used to program the functions that may be used by the workstation type (see Figure 62 below). Double-click a field to open the next level.

Figure 62: Menu Access Programming window—top level



The Menu Access Programming window enables you to define which Forcefield menu items are permitted and what permissions are allowed for those items. An asterisk (*) next to an item indicates that sub-menus follow, press F3 or double-click to open a new window for the sub-menu.

To deny access to this function, delete the character in the item's field (make it blank). To change the permissions for an item, enter one of the following characters in the item's field:

- V—allows access but no modify rights (view).
- E—allows access and modify rights (edit).

Note: Each window (sub-menu) must be saved in order for changes to take place.

Workstations

Workstations are where an operator accesses the Forcefield system (see Figure 63 below). Use the Workstations option to control the behaviour of Forcefield at a workstation level.

Note: If you change a workstation option, logout and then login to see the effect of the change.

Global options are changed from Admin > Configuration > Configuration (see “Configuration” on page 226).

Figure 63: Forcefield Workstation programming window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Work Station. Enter a name to identify the workstation.

Type. Displays the type of workstation (Client or Server).

Watch House Workstation. Set if the selected workstation is a watch house pod or a night switch pod.

Location. Enter a short description of the location, e.g. “In Front Guard House”.

Location TZ. Select the location timezone for this workstation. If this field is left blank, the timezone used will be the one of the controlling node for this workstation.

Desc. Enter a short description, e.g. “Visitor Registration Workstation”.

Computer Access. Select a Forcefield Access Record. This determines what functions are available. This record is ignored if the logged on operator has “Override Access”, in which case the operator’s access determines the available functions. No matter what, any function not present in the list of functions for this type of workstation will not be allowed. See “Workstation Permissions” on page 172.

Controller Node. Displays the computer ID of the Forcefield node.

Station Key. Contains a Forcefield client's security key that identifies that workstation. It must match the value set in Forcefield Client.

Card Login Port. Select the port to which will be connected a Smart Card Reader used for operator login by prox card.

Card Learn Port. Select a serial port to which will be connected an IUM Card Learn Reader. This is used in programming user records. The port type must be "Serial (Other)".

Default Printer. Select the printer to be the default printer for this workstation.

Colours button. Click to access the colour selection programming. See "Workstation options—colours" below for details.

Login button. Click to access the workstation login programming. See "Workstation options—login" below for details.

Graphics button. Click to access the workstation graphics programming. See "Workstation options—graphics" on page 175 for details.

Video button. Click to access the workstation video programming. See "Workstation options—video" on page 175 for details.

Alarms button. Click to access the workstation alarms programming. See "Workstation options—alarms" on page 176 for details.

Other button. Click to access other workstation programming. See "Workstation options—other" on page 177 for details.

Workstation options—colours

Use the Colour Configuration window to customise the colours that Forcefield will use for this workstation.

Double-click a colour field (coloured rectangle) to open the Colour Selection window.

Drag the RGB selectors with the mouse to change the colour mix, alternatively click one of the 15 colours in the palette. The new colour is previewed at the bottom. Click Apply to select the new colour.

Workstation options—login

Use the Login window to control the behaviour of Forcefield on a selected workstation.

To. Select the process to be entered when the operator logs on. This can be the Forcefield menu or Forcefield graphics.

By Keyboard. When checked the operator must key in a code to login.

By Prox. Card. When checked the operator must badge an access card to login.

Password Required. When checked a password is required to log in.

Badge. Select the required order of operation (applicable only if both login by keyboard and login by prox card are set).

Time between Card & Kbd. Enter a time in which both operations must be performed before a login attempt is aborted (applicable only if both login by keyboard and login by prox card are set).

Software Keyboard. When checked Forcefield displays a graphical keyboard on the screen at login time (used in systems where there is no hardware keyboard).

Workstation options—graphics

Use the Graphics window to control the behaviour of Forcefield on a selected workstation.

Login Home Map. Enter the number of the map that will be displayed upon initial login (if login is set to graphics) or the first map displayed from Graphics > Display map.

Status retrieval timeout. Enter a value in seconds that the graphics will wait before aborting a status retrieval request.

Show Alarm On. Select either the first defined map or last defined map for the device in alarm. This applies to the map that the Alarm Screen or the Go To Alarm Map Speed Bar button will pick.

Don't Show Map Selection List. When checked Forcefield does not display a map selection list (you may want to force the operator to stay on particular maps).

Monitor is a Touch Screen. When checked the workstation uses a touch screen. This affects the graphics and Alarm Screen interfaces, usually by adjusting the size of buttons.

Bypass Menu if LAP in Alarm. When checked Forcefield immediately displays the Alarm Screen if a LAP of a unit in alarm is clicked, thus bypassing the usual menu selection dialog.

Auto Popup Control for PTZ. When checked Forcefield immediately displays the Live Camera View window for a PTZ camera if a LAP of a unit in alarm is clicked, thus bypassing the usual LAP video menu selection dialog.

Workstation options—video

Use the Video Configuration window to control the behaviour of Forcefield on a selected workstation.

DVMR Multiview at Login. Select the multiview layout to be displayed when an operator logs in to the workstation.

Mon Group (1, 2, and 3) fields. Enter a title to be displayed on graphics maps for this monitor group, and then select the monitor group to be used. If the title is left blank, then the monitor group ID will be used. Footage for sector alarms is played back in the first three monitors of Monitor Group 1.

Intercom (1 and 2) fields. Enter a title to be displayed on graphics maps for this monitor, and then select the monitor to be used.

Alarm Spot fields. Enter a title to be displayed on graphics maps for this monitor, and then select the monitor to be used.

Show Monitor On Graphics Monitor List check boxes. For the intercom and alarm spot monitors, check the adjacent box to have the monitor appear on the video popup lists so that the operator can select them.

Video Command Priority. If required, enter a priority number for this workstation to enable commands from a higher priority workstation to override commands from a lower priority workstation.

Video Command Operator. If required, enter an identifier to allow access or control of the video system (for example, to enable a Forcefield operator to control a PTZ camera).

Forbid PTZ Control. Check this box to prevent PTZ controls from displaying in Forcefield (for example, if PTZ is controlled by another system).

Forbid CCTV Recording. Check this box to prevent the record option from displaying in Forcefield LAP menus.

Auto Popup Video Player Controls. Check this box to have Forcefield automatically open a control window for any video player started from, for example, the alarm screen. Alternatively, create a Speed Bar button to enable the operator to manually open a video player control window.

Workstation options—alarms

Use the Alarm Screen window to control the behaviour of Forcefield on a selected workstation.

Follow-up Timeout. Enter or accept the time that the Alarm screen will stay on the follow up screen, without operator activity, before reverting back to the unacknowledged screen.

Browse Timeout. Enter or accept the time that the Alarm screen will not display new alarms after operator activity. This allows the operator to browse around the Alarm screen without incoming alarms causing redisplay of the alarms.

Report Viewing of Alarm Detail. When checked Forcefield generates an event when an operator views the details of an alarm. This can be used for event triggering.

Close Detail when Alarm Removed. When checked the Alarm screen closes the detail screen if the alarm is removed. If this option is not selected, the Alarm Detail screen is blanked but remains open.

Select Response by Number. When checked the operator can select an alarm response code by entering a number as well as by selecting with the mouse.

Switch Cam. to Mon. on Detail. When checked Forcefield switches the camera to Spot Monitor 1 upon entering the Alarm Detail screen if the alarming point is associated to a CCTV camera.

Main Screen. 1 Alarm per Member. When checked Forcefield displays only one alarm per member on the Summary Alarm screen. Normally all alarms are displayed. If this option is set, selecting an alarm will bring up another summary screen showing all alarms for that member.

Show Last Tagged Alarm Footage. When checked Forcefield displays the most recent captured and tagged DVR video footage for a multi-event alarm, when the operator selects Video on the Alarm Detail window. If not set, Forcefield displays the earliest captured and tagged DVR video footage.

Display Alarm Line Priority Details. When checked Forcefield displays a count for each alarm priority level. Not set causes Forcefield to display two buttons on the alarm line with the total count displayed in each button. One is for unacknowledged alarms, the other for follow-up alarms. Click a button to open the alarm screen, initially displaying the type of alarms corresponding to the button.

Alarms Silent when Logged Out. When checked the workstation will not beep if there are alarms and no one is logged on.

Report Alarm State. When checked this workstation is to report when changes occur in the alarm line.

Disable Override Notice. When checked this workstation is not to receive override notices.

Workstation options—other

Use the Miscellaneous window to control the behaviour of Forcefield on a selected workstation.

Notes Must be Entered. When checked the operator must enter a note whenever a remote control function is initiated.

Disable CCTV Control. When checked the workstation is not allowed to control CCTV equipment such as cameras and monitors.

User Card Capture. When checked the workstation is allowed to do image capture.

User Card Import. When checked the workstation is allowed to do image importing.

User Card Print. When checked the workstation is allowed to print photo ID cards.

Allow Shutdown. When checked the workstation is allowed to shut down the Forcefield server (Forcefield will be shutdown across all workstations).

Allow Video Popup. When checked alarms programmed with video popup flag cause a video stream to be displayed on this client workstation. The member of the point in alarm must be in the operator's and workstation's member group.

Allow Screen Print. When checked, and a default printer is selected, all forms will have a button and a key shortcut of Shift+F1 which will print the contents of the form to the default printer.

Alarm/Call Event to Graphics. When checked, clicking the “New Alarm or Call” Speed Bar icon for an alarm displays the graphic of the alarming device instead of displaying the alarm screen. Similarly, clicking the “New Alarm or Call” Speed Bar icon for an intercom call displays the graphic of the calling intercom instead of displaying the intercom call screen.

Site Code. The site code selected here will be the default used when issuing smart cards from the Issue User Card screen. This value will override any value set in the global Forcefield configuration.

Card Format. The card format selected here will be the default used when issuing smart cards from the Issue User Card screen. This value will override any value set in the global Forcefield configuration.

Auto Logoff Time. Sets the amount of time an operator workstation may be inactive before the operator is automatically logged off (mouse clicks and keystrokes reset the log out timer, moving the mouse does not restart the timer). Enter 0 (zero) to disable auto logoff.

Event Monitor Browse Time. Enter the number of seconds that the pause command will apply to the Event Monitor window. The pause command may be invoked by using the pause button (Figure 22 on page 36) or by scrolling back to browse events in the list.

Trace Monitor Browse Time. Enter the number of seconds that the pause command will apply to the Trace Monitor window. The pause command may be invoked by using the pause button (Figure 22 on page 36) or by scrolling back to browse events in the list.

Equipment Report

Use the Equipment Report option to list the system’s ports, workstations, printers, nodes, or storage.

Refer to “Generating reports” on page 28, and the following details about this report.

Equip Type. Select the type of equipment to report on (ports, workstations, printers, nodes, or storage).

Id. Select one or more items for the selected type.

Records per Page. Select to either fill the page or print one record per page.

Databases > Computer Equipment > Storage menu

All Storages

Use the All Storages option to quickly find various types of storage records created in:

- “Disk Storage” below
- “NFS Storage” on page 181
- “Samba (CIFS)” on page 181

Optionally use the Node and Type selections to limit the search to the selected options.

When you find the required storage record, click Detail to open the related programming window.

Disk Storage

Use the Disk Storage option to create the database entry for storage devices installed on the Forcefield system.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. The storage device must have a unique name.

Node. Select the required node.

Type. Select the storage type:

- QNX
- FAT16
- FAT32
- CD-ROM (read-only)

Any removable storage device can be programmed for QNX as well as MS-DOS. If you want both, then two records must be created.

For example, for QNX: Node = 1, Id = ‘QNX formatted floppy’,

Type = QNX, Hardware = fd0

For MS-DOS: Node = 1, Id = ‘DOS formatted floppy’,

Type = FAT16 or FAT32, Hardware Id = fd0

Hardware. Select a hardware ID. All the devices listed here must already reside in the QNX device directory (/dev).

Monitor Space. When checked Forcefield will monitor the space of this device. Alarms are generated if the device becomes over 80% full. It is not

recommended to monitor removable storage devices. You can view the state of monitored disks using the Computer Status command (see page 214).

List NFS Storage

Use the List NFS Storage option to display a list of currently active NFS storage directories on the Forcefield node.

NFS Exports

Use the NFS Exports option to determine which Forcefield directories can be accessed by an external NFS mount. The directories are exported as read-only or read-write, as selected.

Tip: Use the Prev and Next buttons to view the entire list of Forcefield directories.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Node Num. Select the required node.

Export selections (not labelled). Check to allow this directory to be exported to external host(s).

r/w selections. Check to enable the directory for read-only or read/write by the external host(s).

Export to Host fields: Leave blank to allow exporting to all remote hosts.

Alternatively, select up to 10 specific hosts per directory to limit the export to the selected hosts.

See also “List NFS Exports” on page 214.

Note: The host records must have already been set up (see “TCP/IP Hosts” on page 170).

NFS options

The following options are not usually required for NFS Exports, but if they are required, they must be set up by a Forcefield administrator. The Forcefield administrator must modify the Forcefield NFS Exports config file (`/usr/ares/config/nfsexports.cfg`).

If set, these options will apply to all directories selected in the NFS Exports window. The export options are listed in Table 14 below.

Table 14: Application of NFS exports options

-mask=netmask - match=network	Restrict access to hosts belonging to subnet defined by <i>netmask</i> and <i>network</i> . By default, there's no restriction. Access is determined by: $client_ip \& netmask = network$
--	---

-norsvd	Don't check incoming requests, they're from a reserved port. By default, NFS requests from ports greater than IPPROTO_RESERVED are replied to with EACCESS.
-ro	Export the filesystem as read-only. By default, the filesystem is exported as read/write.
-root=<i>uid</i>	Map root's uid (real user ID). By default, root is mapped to -2.

The NFS Exports config file `nfsexports.cfg` typically contains a single line. An example is:

```
-root=0
```

NFS Storage

Use the NFS Storage option to program the database entries for remotely mounted storage (storage on another computer accessed via an NFS link).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Forcefield NFS Id. A unique name that identifies this record to Forcefield.

Node. Select the required node.

Remote Host. The IP address of the remote computer where the storage device actually exists.

Timeout. The amount of time, in seconds, that Forcefield will wait before aborting connection to the remote computer.

Mount Command. This is the command which NFS uses to mount the remote storage (for example, to mount a Microsoft Windows C:\maps directory (folder), enter "/c/maps" into this field).

Samba (CIFS)

Samba is open source software providing file and print services across various operating systems.

Use the Samba (CIFS) option to program storage records for Forcefield to use on remote computers using the Common Internet File System (CIFS), such as Windows clients. You can also use this facility to provide storage on computers using other operating systems, as long as the computers are Samba servers.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

CIFS ID. Enter the ID that Forcefield will use for the storage device.

Node. Select the required node.

Timeout. The amount of time, in seconds, that Forcefield will wait before aborting connection to the remote computer.

Machine. The network name of the remote computer, e.g. JWQWERTY or JWQWERTY:192.168.10.11. (Forcefield assumes static addressing.)

Share. The name of the share that we want to connect to on the remote computer, e.g. "public". This share must have read and write access for the user nominated in the user field.

User. The user ID that is allowed to access the share on the remote computer.

Passwd. The password for the user ID that is allowed to access the share on the remote computer.

Databases > Duress menu

The following sections describe the Duress menu (for authorised operators) and subject to licensing before they can be used (see Figure 24 on page 40 for details about how to check the status of Forcefield licensing).

Integrating a duress system is described in *Forcefield External Interfaces Manual*.

Duress Locators

Use the Duress Locators option to program the ASCOM Duress System locators.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

System. Select the Duress System to which this locator belongs.

Address. Enter the hexadecimal address of the locator.

Id. Enter an identifier for Forcefield.

Desc. Enter a description.

Maps. Displays the map numbers of any maps that contain the locator.

Duress Stations

Use the Duress Stations option to program the ASCOM duress stations. A duress station is part of an ASCOM Nira Duress System, and communicates with Forcefield via an Ascom Serial Alarm Interface P940AI.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter a number from 1 to 99 to identify this duress system.

Id. Enter an identifier for this duress system.

Enabled. Check to allow Forcefield to communicate with the station. This allows the programming of the duress system to be performed before Forcefield is connected to it.

Desc. Enter a description.

Protocol. Select the correct protocol for this duress system.

System ID. Enter the duress system ID provided by the supplier of the duress system.

Port. Select a communications port (the type must be “Duress”).

Member. Select a member.

Computer Cat. Select a computer category (the type must be “General”).

Duress Transmitters

Use the Duress Transmitters option to program the ASCOM Duress transmitters or transceivers. There are currently two types handled in Forcefield. The U970 which is purely a transmitter and the U922 which is a transceiver (it has two-way communication).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

System. Select the duress system to which this transmitter or transceiver belongs.

Xmtr Identity. Enter identity of the transmitter. This value should be provided on the Ascom Nira worksheets.

Id. Enter a name to identify the transmitter or transceiver to Forcefield.

Type. Select the type of transmitter. If you select U922 (which has two-way communication), then call number fields are provided.

Call Numbers fields (type U922 only). Enter the transceiver’s call number (page number) for type

Member. Select a member.

Computer Cat. Select a computer category (the type must be “Duress”). Note: Do not use the standard computer category named “Duress”, create a new Duress type of computer category that does not require a restoral for an alarm event.

Help. Double-click or press F3 to program alarm help information.

Locator Report

Use the Locator Report option to list the duress locators used in an ASCOM Duress System.

Refer to “Generating reports” on page 28.

Station Report

Use the Station Report option to list the ASCOM Duress transmitters or transceivers.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the report type required:

- Summary—Basic details of the duress system.
- Detailed—As above, plus listing of locators and transmitters.
- Expanded—As above, plus details of each transmitter and locator.

Transmitter Report

Use the Transmitter Report option to list the duress transmitters used in an ASCOM Duress System.

Refer to “Generating reports” on page 28.

Databases > Intercoms menu

The following sections describe the Intercoms menu (for authorised operators) and subject to licensing before they can be used (see Figure 24 on page 40 for details about how to check the status of Forcefield licensing).

Integrating an intercom system is described in *Forcefield External Interfaces Manual*.

Intercom Master

Use the Intercom Master option to program the intercom system masters.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter a number for the intercom.

Id. Enter an identifier for the intercom.

Desc. Enter a description for the intercom.

Protocol. Select the required protocol.

Tag (for Jacques protocol). Enter the tag of the intercom hardware.

Jacques Port Num (for Jacques protocol). Enter the number of the master link interface port to which the Intercom is connected.

Call No. (for Commend ICX protocol). Enter the call number of the subscriber.

- Master Level.** Select the master level. A master level 2 is connected to Forcefield. A master level 1 is connected to a master level 2.
- IP Port (for master level 2).** Enter the IP port number used to connect the Commend intercom master level 2 to Forcefield.
- Enable.** When checked Forcefield can communicate with this intercom master. This is useful to allow the intercom system to be programmed before connection to Forcefield.
- Minimum Call Digits (for Commend ICX protocol).** Enter the number of digits (numerals) that the underlying protocol uses as a minimum.
- The Forcefield-Commend protocol uses eight-digit station numbers, and automatically adds the letter “F” as a prefix to any call numbers that have fewer than eight digits. As a result, a call number “123” would be sent to Commend as “FFFFF123”.
- The minimum call digits value provides the ability to insert leading zeros in place of the letter F, where needed. For example, if the minimum call digits value is 5, a call number “123” would be sent to Commend as “FFF00123”.
- Comms Port/Host (for master level 2).** Select the intercom port or TCP/IP host that connects Forcefield to the intercom system.
- Higher Master (for master level 1).** Select the intercom master level 2 that connects this intercom master to Forcefield.
- Audio Workstn.** Select the Forcefield workstation that is to handle audio from this master.
- Background Music.** When checked the master is to have background music.
- Computer Cat.** Intercom is selected by default.
- Help.** Select or create Alarm Action Help. See “Programming alarm action text” on page 58 for details.
- Maps.** Displays the map numbers of any maps containing the Intercom system master.

Intercom Slave

- Use the Intercom Slave option to program the intercom system slaves.
- Common window elements are described in Chapter 3. Elements specific to this window are described below.
- Master.** Select the intercom master to which this intercom slave is connected.
- Slave Number.** Enter a number to identify the slave to Forcefield.
- Slave Id.** Enter an identifier to identify the slave to Forcefield.
- Tag.** Enter the tag of the intercom hardware.
- Desc.** Enter a description for the intercom.

Door. If this is a slave intercom associated with a door, enter the door ID.

Camera 1. Select the primary camera that will be used to view the intercom position.

Camera 1 View. Select the primary camera view (video preset) that will be used to view the intercom position. Camera views are programmed in “Presets” on page 207).

Camera 2. Select the second camera that will be used to view the intercom position (for example, to view the reverse of the door when camera 1 views the front of the door).

Confirm Door Open. When checked confirmation is required before Forcefield will open the door.

Background Music. When checked the intercom is to have music.

Call Button Control. When checked the operator can remove or add call button control for this intercom.

Mobile Phone Detect. Check this option if the intercom has the ability to detect the presence of a mobile phone.

PA Only. When checked this slave is to be used only for public address (it cannot open a call).

Computer Cat. Intercom is selected by default.

Help. Select or create Alarm Action Help. See “Programming alarm action text” on page 58 for details.

Maps. Displays the map numbers of any maps containing the Intercom slave.

Master Report

Use the Master Report option to list details of the intercom system.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the report type required:

- **Summary**—This will report on the details of the Master Intercom.
- **Detailed**—As above, plus listing of the slave intercoms attached to the master.
- **Expanded**—As above, plus details of each slave intercom attached to the master.

Slave Report

Use the Slave Report option to list details of the slave intercoms attached to the master.

Refer to “Generating reports” on page 28.

Databases > Management Software menu

Alarm Responses

Use the Alarm Responses option to add response codes to the system. These codes can be used by operators when attending to alarms. It is designed to speed up the process of an operator entering text by having predefined responses.

The response codes are member related. When a member record is created, Forcefield will create default response codes for that member. The default records created are defined in the file `/usr/ares/tools/config/AlarmRespDef.dat`.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Member. Select the member for the response code you are programming.

Code. All code responses are unique by their number. Each member can have 9999 responses.

Text. Enter the text for the response.

Databases > Management Software > Clusters menu

Program Clusters

Clusters are a means of grouping together field equipment of the same type, which enables a single remote control operation to affect all the elements in the cluster. For example, a group of doors may be clustered to 'Fire Doors'. The operator may then open all the fire doors in a single operation.

Use the Program Clusters option to define clusters for doors, inputs, areas, relays, floors, RASs, DGPs, lifts, or Challenger panels. A device may be connected up to 32 clusters. For example, Door 19 could be in the 'Fire Door' cluster and the 'Front Fire Door' cluster and the 'Office Door' cluster, and so on.

See "Controlling the security system remotely" on page 42 for additional details.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Elements. Click the arrow to select elements for the cluster, or click List to view the elements already selected.

Cluster Report

Use the Cluster Report option to generate a report about Forcefield cluster records.

Refer to “Generating reports” on page 28, and the following details about this report.

Cluster Type. Select the required cluster type or select All to report on all cluster types.

Cluster Id. Select the required cluster or leave blank to report on all clusters.

Cluster Usage Report

Use the Cluster Usage Report option to generate a report about records where the selected clusters are referenced.

Refer to “Generating reports” on page 28, and the following details about this report.

Cluster Type. Select the required cluster type or select All to report on all cluster types.

Cluster Id. Select the required cluster or leave blank to report on all clusters.

Databases > Management Software > Computer Categories menu

Computer Categories

Use the Computer Categories option to tell Forcefield how to handle events.

The computer category window initially opens with no events listed (see Figure 64 on page 189). Click the Id arrow, and then select a computer category to populate the window.

Figure 64: Blank Computer Category record

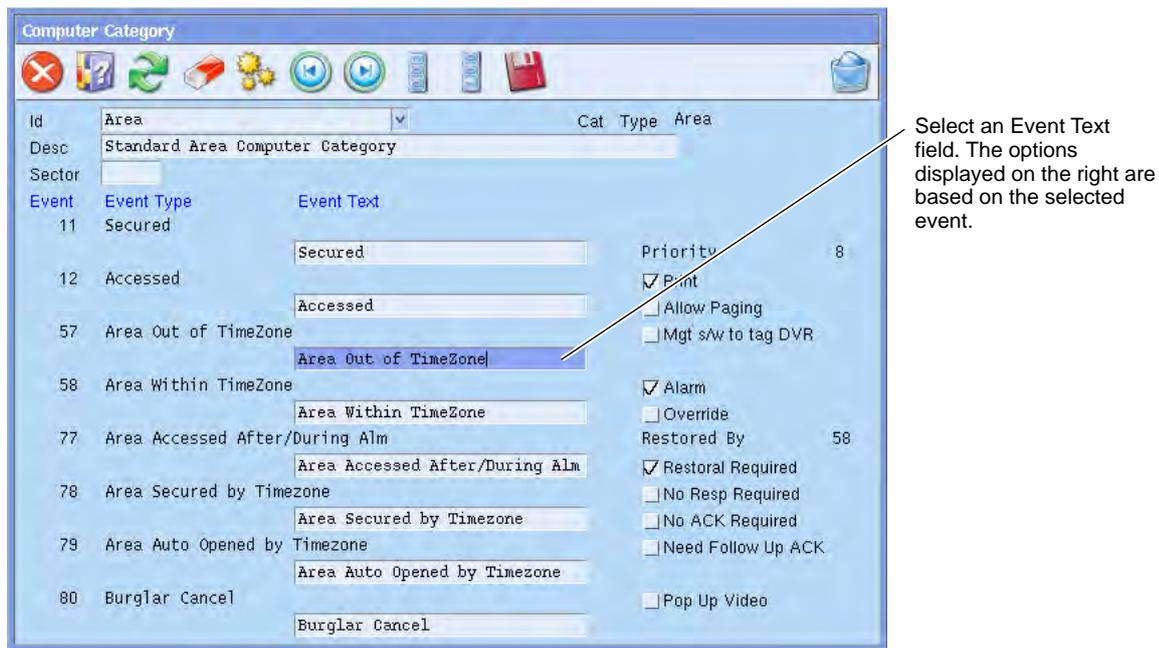
The screenshot shows a software window titled "Computer Category". At the top is a toolbar with icons for delete, help, refresh, save, and other functions. Below the toolbar is a form with the following fields and controls:

- Id**: A dropdown menu.
- Desc**: A text input field.
- Event**: A text input field.
- Event Type**: A text input field.
- Event Text**: A text input field.
- Cat**: A text input field.
- Type**: A text input field.
- Priority**: A section containing three checkboxes:
 - Print
 - Allow Paging
 - Mgt s/w to tag DVR

There are a number of standard read-only computer category records provided for use as 'templates'. These standard records cannot be modified or deleted, and it is recommended that these standard records are not used (except as templates).

Define a computer category in order to program a set of behaviours and assign them to a type of device. By doing so, you can automatically update all the devices that use the computer category by updating only the computer category.

Note: Isolation events will not generate alarms even though you may alter a computer category to do so, because there is an overriding system functionality to ignore alarm generation. This applies to Input Isolate, DGP Isolate, RAS Isolate, DOTL Isolate, Egress Isolate, and Forced Isolate.

Figure 65: Selecting options for an event within a computer category

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. This is the name of the computer category which will be used by Forcefield components, e.g. an input may have a computer category of “Front Door PIRs”.

To create a computer category, type a new ID and then press Enter. Forcefield displays a category type selection list. Select the required category type, and then Forcefield displays the events and options for the type. The options for each event may be modified and the computer category saved.

Desc. Type a description for a new computer category. A computer category with a description beginning with the word ‘Standard’ is typically one of the default, read-only computer categories supplied with Forcefield.

Sector. A sector number enables Forcefield to use the computer category to group alarm inputs together, or to link the computer category to external events such as a Teleste alarm code. If using Teleste, you need to know the specific Teleste alarm code to be used (e.g. 3301). When a sector number is used, Forcefield generates events in the following manner:

- “Alarm” becomes “Sector Alarm” or “Sector Alarm Increase”
- “Alarm ACK” become “Sector Alarm ACK”
- “Alarm Restoral” becomes “Sector Alarm Reset” or “Sector Alarm Decrease”

Event Text. The text that will be displayed and stored in history by Forcefield if this event occurs. To change the event text, edit the Event Text field. When the cursor is in the Event Text field, the list to the right are the event options (programming options for that event).

Note: If the computer category has more than eight events, use the Ctrl+up button and Ctrl+down button to select other events for that category.

The event options cannot be changed for standard computer categories, you need to create a new computer category before you can change the options.

Typical functions (some events do not have every function) of the event options are:

- **Priority.** Set the priority to be assigned to the event (1 is the highest 9 the lowest).
- **Print.** Select if the event is to be allowed to print to an event printer.
- **Allow Paging.** Select if the event is to be allowed to initiate paging. This has to also be programmed at Triggering > Event Paging.
- **Mgt s/w to tag DVR.** Select if Forcefield is to send text to a DVR to be recorded as a tag for the event.
- **Alarm.** Select if the event is to generate an alarm.
- **Override.** Select if the event is to generate an override notice.
- **Restored By.** Select if the event is to be restored by the numbered event.
- **No Response Required.** Select if this event does not require the operator to enter a response. **Note:** If the event causes an alarm but has no restoral event, both this flag and the “No ACK” flag cannot be set simultaneously (there must be some way of telling Forcefield when to delete the alarm).
- **No ACK Required.** Select if this event does not require the operator to enter a ACK. **Note:** If the event causes an alarm but has no restoral event, both this flag and the “No Response” flag cannot be set simultaneously (there must be some way of telling Forcefield when to delete the alarm).
- **Need Follow Up ACK.** Select if this event requires an acknowledgement after a restoral to remove the alarm.
- **Reset Input on ACK.** Select if input should be sent a Reset command when the operator acknowledges the alarm.
- **Pop Up Video.** Select if you want the event to cause a video stream to be displayed on a client workstation. The workstation record must also have Allow Video Popup enabled (see “Workstation options—other” on page 177).

Computer Category Report

Use the Computer Category Report option to list all the event options for one or more computer categories.

Refer to “Generating reports” on page 28.

Computer Category Usage

Use the Computer Category Usage Report option to list all records where the selected computer categories are referenced.

Refer to “Generating reports” on page 28, and the following details about this report.

Type. Select a type to limit the report to a single computer category, or use the default setting of All.

Databases > Management Software > Members menu

Members

Use the Members option to program member records. The Forcefield concept of member restricts the operator from viewing records, and controlling and receiving events, that are not within their authority (member group). The Forcefield database can therefore be partitioned into virtual sub-systems. At the same time a privileged operator may be given “all members” for global system control and monitoring.

Member records also provide Forcefield with the means of defining 10 user-defined data fields, which appear as field titles on the User Maintenance window for users assigned to the member. See Figure 2 on page 8 for an example.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Each member ID must be unique and cannot be the same as a member group ID.

Name (optional). The name of the person responsible for the member.

Address (optional). The address of the person responsible for the member.

State (optional). The state of the person responsible for the member.

PostCode (optional). The post code of the person responsible for the member.

Location (optional). The location of the person responsible for the member, e.g. General Administration Office.

Contact (optional). Additional information of further persons responsible for the member.

Nightswitch Workstation Keep Member (applies to watch house mode). Tick this option to keep this member active on the night switch workstation even if a logged-in pod workstation has this member in its member group. For example, master intercoms use this setting so that master-to-master calls can be made from the night switch workstation to pod workstations.

Data 1 to Data 10 (optional). These fields are used for displaying information on the User Maintenance window for users assigned to the member.

Member Groups

Use the Member Groups option to program member group records. A member group is a group of members, which is then assigned to Forcefield resources such as operators, workstations, and printers.

The member group restricts the records and events that are visible to operators, workstations, and printers. Conversely, the member group also determines the destination of events to particular operators, workstations, and printers.

Id. The name must be unique to each member group and cannot be the same as any member. To create a new member group record, first enter the ID, and then double-click the field (or click Make). The member selection screen opens.

In the member selection screen place a check in the box next to the members required for this member group. Press Select to save the record.

Member Report

Use the Member Report option to list the details of one or more members.

Refer to “Generating reports” on page 28, and the following details about this report.

Member Id. Select a member for a report on an individual member. Leaving the field blank will report all members in the current operator’s member group.

Member Group Report

Use the Member Group Report option to list the members allocated to one or more member groups.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the report type required:

- **Summary**—lists all the members allocated to the member group.
- **Detailed**—lists all the members allocated to the member group and the details of each of those members.

Member Group Id. Enter the ID here to generate a report on a selected member group. Leaving the ID blank generates a report for all member groups accessible by the current operator.

Member Usage

Use the Member Usage Report option to list all records where the selected members are referenced, and is useful to check before attempting to delete a member record.

Refer to “Generating reports” on page 28, and the following details about this report.

Member Id. Select a member to generate a report on the member. Leaving the field blank generates a report for all members accessible by the current operator.

Member Group Usage

Use the Member Group Usage Report option to list all records where the selected member groups are referenced.

Refer to “Generating reports” on page 28, and the following details about this report.

Member Group Id. Select a member group to generate a report on the member group. Leaving the field blank generates a report for all member groups accessible by the current operator.

Databases > Management Software > System Events menu

Events

Use the Events option to program groups of event records. Event groups are used in history reporting for event matching.

Figure 66: Forcefield Event Group programming window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Event. Enter or search for an ID that will represent a group of events. For example, to search on any one of five different events, create a new event type here and allocate the specific five events to it. Then, generate a History report for this new event type.

To create a new event type, enter the name of the event then press Save.

To enter which events make up the group, select the Events field and press F4. You can filter which events are presented by keying in a text prefix before pressing F4 (for example, to only see RAS events, enter 'arm' (for Arming Station) before pressing F4).

Events. If the event selected (or created) in the event field is a group, then the Events field displays. Right-click a check box to select (or deselect) events for this group.

Event Group Report

Use the Event Group Report option to see what event groups have been defined and what they contain.

Refer to “Generating reports” on page 28.

Databases > Third Party menu

Forcefield version 5.1.0 and later can be integrated with third-party devices, so that it can send event data to, and receive messages from, external systems. Third-party integration enables Forcefield to perform actions via the event triggering system (see “Event Trigger” on page 81).

Refer to the *Forcefield External Interfaces Manual* for details of integrating third-party devices into the Forcefield system.

Third-party integration is subject to licensing and must be licensed before the associated menus become visible.

Devices

Use the Devices option to define third-party devices to be used by Forcefield. Before you can program a device, you must first program the:

- Third-party system type (see “System Types” on page 198)
- Third-party system (see “System” on page 197)
- Device type (see “Device Types” on page 196).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

System. Select the third-party system to which this device is connected.

Number. Specify a number for this device. The maximum number is determined by the type of device.

Id. Specify a unique device ID to be used by Forcefield to identify the device.

Device Type. Select the type of device. Device types are programmed in “Device Types” below.

Desc. Type an optional short description (e.g. Front Lawn Sprinkler).

Location. Type an optional location description (e.g. At front of building).

Video Cam. Select the video camera associated with this input.

View. Selects the preset view for the video camera. If this field left blank, the video camera, if a PTZ camera, will switch to preset 1.

Member. The member controls event reporting and operator control in Forcefield.

Computer Cat. Click the arrow to select a computer category. Forcefield displays a type selection dialogue Figure 67 below). Select, as required:

- **Notify**—The computer category ‘Notify’ contains 64 notify events that may be set as alarm events (there will be no restoral events).
- **Alarm Response**—The computer category ‘Alarm and Restoral’ contains 32 groups of alarm and restore events.
- **Both (notify and alarm response)**—The computer category ‘Notify, Alarm and Restoral’ contains 16 groups of alarm, restore, and notify events

Figure 67: Computer Category Type selection dialogue



Each device can have a different computer category. The category determines how Forcefield will handle an event from this device. The default computer category names can be used, but they are standard (read-only) Forcefield computer category and cannot be modified. See “Computer Categories” on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item.

The help programmed here will be displayed as an action on the alarm screen when alarm are generated.

Maps. Displays the map numbers of any maps containing the device ID.

Device Types

Use the Device Types option to define third-party device types to be used by Forcefield. Before you can program a device type, you must first program the system type (see “System Types” on page 198).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

System Type. Select the third-party system type to which this device will be connected. System types are programmed in “System Types” on page 198.

Device Type. Specify a number for this device type. There may be up to 99 device types per system type.

Id. Type a unique name to identify the device type.

System

Use the System option to program a third-party system into Forcefield. Before you can program a system, you must first program the system type (see “System Types” on page 198).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Specify a number for this system. There may be up to nine third-party systems in Forcefield.

Id. Type a unique name to identify the third-party system.

Type. Select the system type. System types are programmed in “System Types” on page 198.

Sub Type. Select the sub type of system if required. System sub types are programmed in “System Sub Types” on page 198.

Time Sync. Select whether Forcefield or the third-party system is allowed to set the time of the other, or no time synchronisation is to occur.

Locality. Select the time zone location of the third-party system (e.g. Adelaide).

Description. Type a short description to describe the purpose of the system.

Location. Type a short description to describe the physical location of the system.

Channel Type. Select RS-232 or TCP/UDP communications, as required

Port. Select a comms port. Only one system is allowed per comms channel.

ACK Timeout. Enter a value, in seconds, that Forcefield should wait for an acknowledgement from the system before attempting to resend the event data.

Retry Attempts. Enter a value for how many times Forcefield should attempt to send event data before discarding the event.

Heartbeat. Enter a value, in minutes, for the time between heartbeat pulses from Forcefield to the system. Heartbeats are only sent when there has been no other comms activity for the specified time. This is used by Forcefield to ensure the third-party system is still online.

Sends Events check box: When checked Challenger sends events to Forcefield. The event sent will be an index into the computer category selected for one of the third-party system devices (see “Devices” on page 195).

Receives Events check box: When checked Challenger receives events from Forcefield.

in Format. Select the type of event format that the system will receive (short form binary, history CSV, or history raw).

For Access. Select the access. This controls which events the system will receive. It is based on the member or member group of the event. The access records are the same records used by printers (see “Printer Permission” on page 167).

Member. Select a member.

Computer Cat. Select a computer category (the type must be “General”).

Help. Double-click or press F3 to program alarm help information for this item. The help programmed here will be displayed as an action on the alarm screen when alarm are generated.

Maps. Displays the map numbers of any maps containing the system.

System Sub Types

Use the System Sub Types option to assign an optional sub type to a third-party system. Before you can program a sub type, you must first program the system type (see “System Types” below).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

System Type. Select the third-party system type for this sub type. System types are programmed in “System Types” below.

Sub Type. Specify a number for this sub type. There may be up to 99 sub types per system type.

Id. Type a unique name to identify the sub type.

System Types

Use the System Types option to assign a system type to each third-party system.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Specify a number for this system type. There may be up to 99 types of third-party systems.

Id. Type a unique name to identify the system type.

Databases > Timezones menu

Time Zones

Use the Time Zones option to define time zones for both Challenger and Forcefield functions. Each time zone may consist of four segments. If the first segment is not active, the next is checked, and so on.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

See “Timezone-related tasks” on page 71 for additional details.

Timezone. Type a unique timezone name.

Desc. Type a name that indicates the timezone’s purpose.

Start Time. For each segment (1 through 4), enter the time in hours and minutes hour that the timezone is to become active. 0:0 is a valid minimum start time.

End Time. For each segment (1 through 4), enter the time in hours and minutes hour that the timezone is to become inactive. 24:0 is a valid maximum end time.

Sun, Mon, ... Sat. For each segment (1 through 4), set if the timezone is to active on this day.

HOL. For each segment (1 through 4), set if the timezone is to be active on a holiday. Note: Holiday is only used for Challenger timezones. Forcefield does not use the holiday indication.

Time Zone Report

Use the Time Zone Report option to list the details of one or more time zones.

Refer to “Generating reports” on page 28, and the following details about this report.

Timezone. This function is used generate a report on the contents of the timezones. If left blank, all timezones will be included.

Timezone Usage

Use the Timezone Usage Report option to list where time zone records are referenced. This will be Challenger panels, Computer Access and Printer Access records. Within the Challenger records, the individual items (e.g. Areas, etc.) are not listed.

Refer to “Generating reports” on page 28, and the following details about this report.

TimeZone Id. Click the arrow (or press F4) to open the Search & Select window to select timezones for the report. Select the timezone or timezones you want to generate a report for. Leaving this field blank will result in a report for all timezones.

You may type text into the TimeZone Id field in order to restrict the search, however you must use the Search & Select screen to select timezones for the report.

Databases > Video menu

The following sections describe the Video menu (for authorised operators) and subject to licensing before they can be used (see Figure 24 on page 40 for details about how to check the status of Forcefield licensing).

Databases > Video > Video Service

Use the Video Service option to program a video service that Forcefield will use to communicate with TruVision DVRs (and others).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Address. Double-click the Address field, and then select or create a TCP/IP host port for the video service connection.

Port. Type the port number (default is 9300) that the Video Status Manager service will use to send data to Forcefield. Do not use the same port number as used for the Video Presentation Client (VPC). See “Configuring CCTV/intercom options” on page 229.

Password. Type the session password that was defined when Video Status Manager was installed on the video server.

Connection Retry Interval. Type the number of seconds in the range 10 to 60 that Forcefield will attempt to connect to enabled DVRs that use this record.

Heartbeat Interval. Type the number of seconds that Forcefield will send heartbeat messages to the video service. If no heartbeat response is received within 30 seconds Forcefield will close the connection.

Databases > Video > DVR Video menu

DVRs

Use the DVRs option to program the DVR that Forcefield will use.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter number for the DVR that is not already used in this system.

Id. Enter a unique name to identify the DVR. Note that cameras, presets, and DVR are kept in the same database, so the name must be unique across all of these devices.

Enabled. Check the box to have Forcefield start a driver for this DVR. Leave unchecked to program the DVR, cameras, and presets before actually physically connecting the equipment to the Forcefield system.

Location. Type a short description of the physical location of the DVR.

Desc. Type a short description of what it does.

Type. Click the arrow, and then select the type of DVR used. Select Video Service for TruVision DVRs.

Password. Type the password that Forcefield will use to connect with a SymDVR.

Configuration button. Click to launch the Edit DVR window, which is used to configure devices connected via the video service. Refer to the *Forcefield External Interfaces Manual* for details.

IP Address (displays when the type is "SymDec/SymSafe"). Click the arrow, and then select the TCP/IP Host to be used for the DVR. See "TCP/IP Hosts" on page 170.

Server (displays when the type is "Video Service"). Click the arrow, and then select the Video Service to be used for the DVR. See "Databases > Video > Video Service" on page 200.

Note: At least one (video service) DVR must be enabled before the video service can connect to the video server.

Update Camera Title button. Click to update the SymDVR with the text from the CamTitle fields for all cameras that are associated with the DVR. See "DVR Cameras" on page 202. This option is not supported by TruVision DVRs.

Locality. Click the arrow, and then select the Locality (time zone) to be used for the DVR.

Member. Determines which operators are allowed to control the device and receive events.

Maps. Displays the map numbers of maps containing the device.

DVR Cameras

Use the DVR Cameras option to program the video cameras that Forcefield will use.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

DVR. Select the DVR to which this camera is connected (see “DVRs” on page 201).

Cam. Num. Select the number that the selected DVR uses to communicate with the camera (e.g. if this is camera 6 on the DVR, enter 6 here).

Cam. Num. Select the number that the selected DVR uses to communicate with the camera (e.g. if this is camera 6 on the DVR, enter 6 here).

Note: DVRs that support both analogue and IP cameras may use an offset. For example, a TVR60 that supports 16 analogue cameras and 8 IP cameras numbers the analogue cameras 1 to 16 and numbers the IP cameras 17 to 24.

Has PTZ Control. Check the box for cameras with pan/tilt/zoom control.

Id. Enter a unique name to identify the camera. Note that cameras, monitors, presets and DVRs are kept in the same database, so the name must be unique across all of these devices.

CamTitle. Type the text overlay that will be displayed onscreen for the camera’s video. In the associated DVR programming window, click the Update Camera Title button to send the text to the DVR. See “DVRs” on page 201.

Desc. Type a short description of what it does.

Member. Determines which operators are allowed to control the device and receive events.

Configuration button. Click to open the Camera Configuration window, which is used to configure devices connected via the video service. Refer to the *Forcefield External Interfaces Manual* for details.

Maps. Displays the map numbers of maps containing the device.

Note: If you delete a DVR’s camera record for an analogue camera in Forcefield, you also need to clear the Camera Enabled check box the camera in the DVR’s Device Configuration window, Cameras tab. Refer to the *Forcefield External Interfaces Manual* for details.

DVR Presets

Use the DVR Presets option to program the video presets (predefined views for PTZ cameras) that Forcefield will use.

Note: A DVR camera must be programmed before you use this command.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Preset for Camera. Select a PTZ camera.

Num. Enter a preset number for a new view.

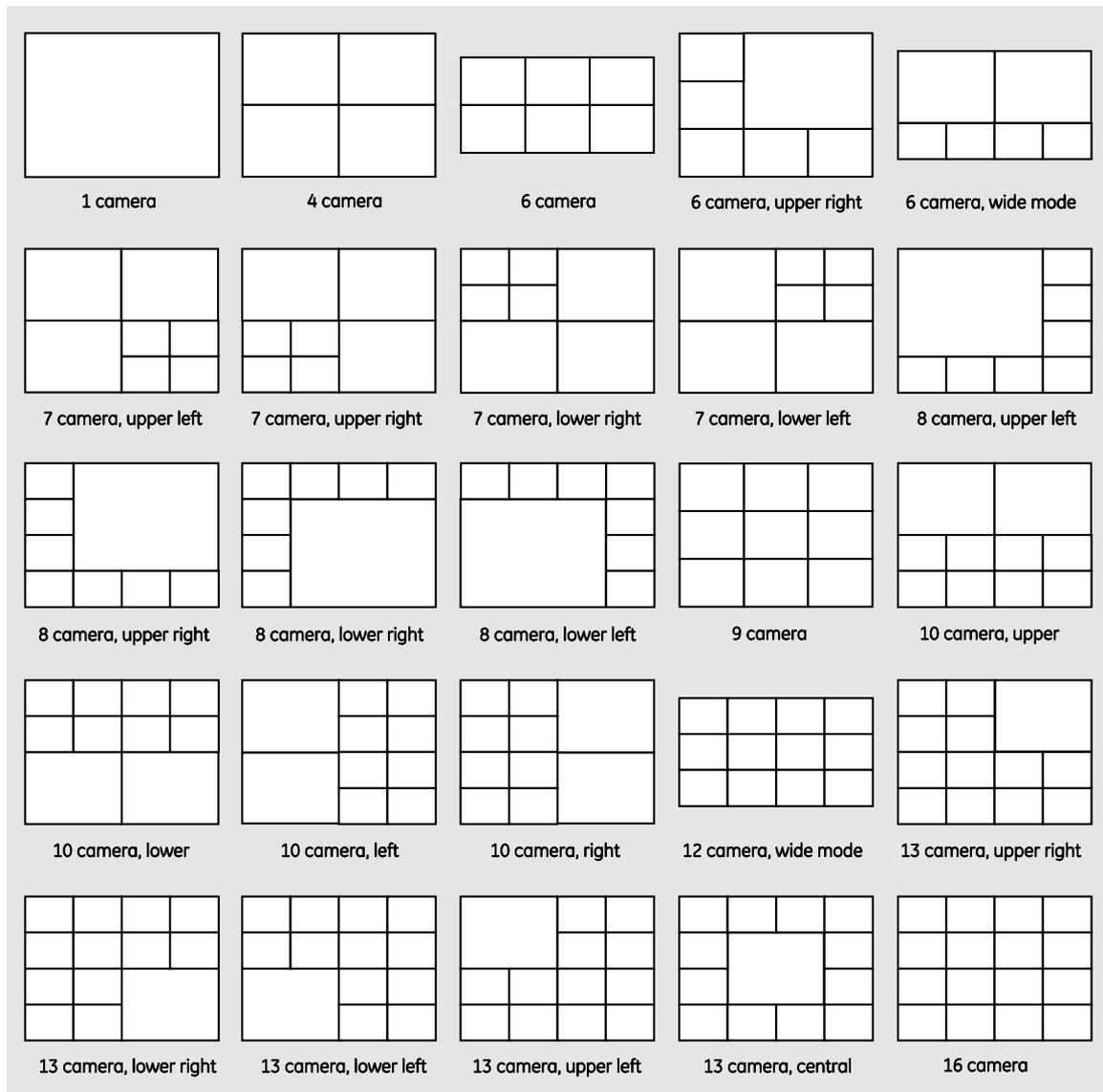
Id. Enter a unique name to identify the preset (e.g. West Wing Front Door View).
Note that cameras, monitors, presets and DVRs are kept in the same database, so the name must be unique across all of these devices. TIP: The name that you assign to a preset is added to the camera's pop-up menu on maps displaying the camera.

Desc. Enter a more detailed description of the preset's purpose, etc.

Multiview

Use the MultiView option to define a group of cameras (and optional preset views for PTZ cameras) for displaying up to 16 images of DVR video on a single screen. Figure 68 on page 204 depicts the range of options available for displaying camera views.

Figure 68: Multi-view screen layout options



These records may be associated with a workstation, in which case the multi-view will be initiated when the operator logs in (see “Workstations” on page 173). After logging in, the operator can select a different multi-view (see “Display MultiView” on page 118).

Note: Displaying multiple images of DVR video on a single screen requires a large amount of processing power, memory, and specific video card(s) to be used in the Forcefield Client computer. Multiview records programmed here might not be usable by Forcefield Client computers that do not have the required hardware. Refer to the *Forcefield External Interfaces Manual* for details.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Multi-View. Select or specify a name to identify the multi-view record.

Desc. Select type a description for the multi-view. This description will be displayed on the multi-view selection screen.

Member. Select a member. Only multiviews within an operator and workstation member group may be selected. The individual camera members are also checked when initiating multi-view action. Cameras not within the current member group will not be displayed.

Monitor number. Select from the list of monitors (applicable only to computers with multi-monitor video adaptors).

View Layout. Select from the list of view layouts. Figure 68 on page 204 depicts the range of options available for displaying camera views.

All views for a multi-view must be of the same layout. The selected layout is depicted to the right of the selection field. Once a multi-view record has been created, its layout may not be altered.

Video Quality. Select either high or low quality, as appropriate to the abilities of your network. High quality video requires more bandwidth. Select high to use the main stream video options configured for this camera within the DVR. Select low to use the sub-stream video options configured for this camera within the DVR.

Dwell. Specify the amount of time that view will be displayed before the next view is displayed. It is not possible to create a camera list without first entering a dwell time.

Detail. After specifying a dwell time, save the record, and then click the corresponding View button to select cameras for the selected view layout. The Multi View Camera Detail programming window displays the required number of camera selection fields (Figure 69 below).

Figure 69: Multi View Camera Detail programming window



Camera fields (quantity varies to suit selected layout). Click a camera arrow to select a camera. The camera's position in the selected layout is depicted to the right of the selection field.

View. Click the View arrow, and then select a preset view for a PTZ camera. See "DVR Presets" on page 202 for details.

Camera Report

Use the Camera Report option to generate a report about DVR camera records. Details include the information programmed on the DVR Camera window.

Refer to "Generating reports" on page 28.

DVR Report

Use the DVR Report option to generate a report about DVR records. Details include the information programmed on the DVR window.

Refer to “Generating reports” on page 28.

Preset Report

Use the Preset Report option to generate a report about DVR camera preset records. Details include the information programmed on the DVR Presets window.

Refer to “Generating reports” on page 28.

Databases > Video > Matrix Video menu

Cameras

Use the Video Cameras option to program the video cameras that Forcefield will use.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Switcher. Select the video switcher to which this camera is connected (see “Switchers” on page 208).

Cam. Num. Select the number that the selected switcher uses to communicate with the camera (e.g. if this is camera 6 on the switcher, enter 6 here).

Has PTZ Control. Check the box for cameras with pan/tilt/zoom control.

Id. Enter a unique name to identify the camera. Note that cameras, monitors, presets and switchers are kept in the same database, so the name must be unique across all of these devices.

Teleste Camera Id (for Teleste switchers). Enter the ID that the video system uses to identify the camera.

Desc. Type a short description of what it does.

Member. This field determines which operators are allowed to control the device and receive events.

Maps. Displays the map numbers of maps containing the device.

Monitors

Use the Monitors option to program the video monitors that Forcefield will use.

Note: Depending on the video system, “monitor” can mean a physical monitor or a picture tile on a display.

A video switcher must be programmed before you use this command.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Switcher. Select the video switcher to which this monitor is connected (see “Switchers” on page 208).

Monitor Num. Enter the number that the switcher uses to communicate with the monitor (e.g. if this is monitor 4 on the switcher, enter 4 here).

Id. Enter a unique name to identify the monitor. Note that cameras, monitors, presets and switchers are kept in the same database, so the name must be unique across all of these devices.

Teleste Monitor Id (for Teleste switchers only). Enter the ID that the video system uses to identify the monitor.

Recorder Monitor. Check this box to indicate to the video system that the video feed to this monitor can be recorded. This enables recording actions to be performed via Forcefield map icons.

Desc. Type a short description of what it does.

Member. This field determines which operators are allowed to control the device and receive events.

Monitor Groups

Monitor Groups are used by Forcefield to assign video monitors to workstations. This is to enable tidier handling of video monitors on the maps.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Physical Layout. When creating a new group select the physical layout of the monitors within the group.

Monitor Assignment. Click to open the screen to assign video monitors to the group.

Presets

Use the Video Presets option to program the video presets (predefined views for PTZ cameras) that Forcefield will use.

A video camera must be programmed before you use this command.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Preset for Camera. Select a PTZ camera.

Num. Enter a preset number for a new view.

Id. Enter a unique name to identify the preset (e.g. West Wing Front Door View). Note that cameras, monitors, presets and switchers are kept in the same database, so the name must be unique across all of these devices. TIP: The name that you assign to a preset is added to the camera's pop-up menu on maps displaying the camera.

Desc. Type a detailed description of the preset's purpose, etc.

Teleste Name (for Teleste systems only). Enter the video system's Position name correctly (case-sensitive).

Switchers

Use the Switchers option to program the video camera (CCTV) switchers that Forcefield will use.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter a unique number for a new switcher.

Id. Enter a unique name to identify the switcher. Note that cameras, monitors, presets and switchers are kept in the same database, so the name must be unique across all of these devices.

Enabled. Check the box to have Forcefield start a driver for this switcher. Leave unchecked to program the switcher, cameras, monitors and presets before actually physically connecting the equipment to the Forcefield system.

Location. Type a short description of the physical location of the switcher.

Desc. Type a short description of what it does.

Protocol. Select the switcher protocol. Additional fields may display, depending on the selected protocol.

IP Address. Enter the name of the TCP ID Host record that Forcefield will use to connect with the switcher.

IP Port. Enter the number of the TCP/IP port that Forcefield will use to connect with the switcher.

Port. Enter the ID of the port that the switcher uses to communicate with Forcefield.

Locality (DVRs only). Select the time zone locality of the DVR to enable the most efficient searching.

Default Command Operator. If required, enter a name to identify commands sent to the switcher.

User Code. Enter the login name required to communicate with the switcher.

Pwd. If prompted, enter the password for the user code.

License Key. Enter the license details (from Teleste) required to communicate with the switcher.

Hash Key. Enter the details (from Teleste) required to communicate with the switcher.

Member. This field determines which operators are allowed to control the device and receive events.

PIN. Depending on the selected protocol, a PIN field may display. Enter the PIN code that Forcefield is to emulate in order to communicate with the switcher:

- Pacom 2030 protocol—PIN is typically 9999
- Panasonic550 protocol—PIN is typically 12345

Keyboard (for Maxpro protocol). Type the keyboard number (typically 32) that Forcefield is to emulate in order to communicate with the switcher.

Camera Report

Use the Camera Report option to generate a report about Forcefield video camera records. Details include the information programmed on the Video Camera window.

Refer to “Generating reports” on page 28.

Monitor Report

Use the Monitor Report option to generate a report about Forcefield video monitor records. Details include the information programmed on the Video Monitors window.

Refer to “Generating reports” on page 28.

Preset Report

Use the Preset Report option to generate a report about Forcefield PTZ camera preset records. Details include the information programmed on the Video Presets window.

Refer to “Generating reports” on page 28.

Switcher Report

Use the Switcher Report option to generate a report about Forcefield video camera switcher records.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the required report type:

- Summary—displays the details of the switcher.
- Detailed—displays the details of the switcher, and lists the monitor and cameras attached to the switcher.
- Expanded—displays the details of the switcher, and lists the details of the monitor and cameras attached to the switcher.

Status menu

Trace Monitor

Use the Trace Monitor option to set up tracing and then to display the results of trace monitoring. The Trace monitor will beep whenever one of the traced events is detected.

The Trace Monitor is similar to the Events Monitor. Click a tool bar button to set up tracing for one or more events (tool bar buttons are described in “Using the Event Monitor window” on page 36).

Refer to “Using multiple event filters” on page 37 for details about using multiple filters.

Leaving fields blank indicates no restriction on that field when matching for events: The Event Monitor displays all events; the Trace Monitor displays no events.

Status > Alarm Panel Status menu

Abnormal Status Report

Use the Abnormal Status Report option to list alarms and/or abnormal states in the Challenger system.

Refer to “Generating reports” on page 28, and the following details about this report.

Report Type. Select the report type required:

- Alarms Only—the report contains items that are currently in alarm.
- Alarms and Abnormal Conditions—the report contains items that are in alarm and items that are not in their normal state.

The normal states of various items are:

- Input—sealed
- Area—secured
- Door—closed and locked

- Relay—reset (not active)
- Floor—secured
- DGP—online and polled
- RAS—online and polled

Challenger Item Status

Use the Challenger Item Status option to list the current state of a selected Challenger item or a group of items.

Refer to “Generating reports” on page 28, and the following details about this report.

Device Type. Select the required device type or select All to report on all device types.

Individual Item Status

Use the Individual Item Status option to list the current state of a selected item or a group of items.

Refer to “Generating reports” on page 28.

Items in State Report

Use the Items in State Report option to list all items of a particular type that are in a specified state in the Forcefield status file (for example, to list all isolated inputs for a given member group). Items that have been offline may not be current.

Refer to “Generating reports” on page 28.

Status > Door Status menu

Door Monitor

Use the Door Monitor option to display the user image, if any, and the transaction details of the last door access event for selected doors. Only the last received event is displayed.

The door access events that will be monitored are set up as a Forcefield Event Group record, specifically the Door Monitor record. If there is no such record, all the events in the Door Access computer category will be monitored. These events are global to the entire Forcefield network. See “Events” on page 194 for details of setting up Forcefield event groups.

Figure 70: Door Monitor window (user detail example)

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Setup button. Click to enter the screen to setup which doors are to be monitored.

Open Door button. Click to open the door shown in the transaction detail.

User Detail button. Click to display details of the user shown in the transaction detail.

Door Open Close Times

Doors controlled via a four-door controller (door numbers 17 through 64) can be programmed with automatic lock and unlock times. This is effectively the override timezone in the doors' access options.

Use the Door Open Close Times option to show the automatic lock and unlock times for such doors, listed by Challenger. It provides a quick way to view the times that a door becomes unlocked.

Refer to "Generating reports" on page 28, and the following details about this report.

Sort Type. Select the required sort order:

- Door ID
- Door number (Challenger door number)
- Door number by member
- Door ID by member
- Door ID by Challenger number
- Door ID by Challenger ID

Door Override Report

Use the Door Override Report option to create reports about programmed door lock overrides.

Refer to “Generating reports” on page 28, and the following details about this report.

Sort Type. Select the required sort order:

- Door ID
- Door number (Challenger door number)
- Door number by member
- Door ID by member
- Door ID by Challenger number
- Door ID by Challenger ID

Status > Equipment Status menu

Printer Status

Use the Printer Status option to display the state of all printers.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Printer. Double-click a Printer field to display a detail and control screen for the printer. This screen shows the number of events and reports waiting to be printed. It also allows the operator to stop/start the printing, or remove events queued for printing and cancel a report waiting to be printed.

Cancel Report button. Click the report to be removed, then click the Cancel Report button to stop a report from being printed.

Resume button. Click to resume printing at this printer.

Stop button. Click to stop printing at this printer.

Delete Events button. Click to remove all events currently queued for printing. This does not change the Events to be Printed number displayed on the screen (Forcefield slowly removes the events from the printer queue). To see the effect, you must go back to the summary window and re-enter the detail window.

Report. Select a single report to cancel.

Serial Port Status

Use the Serial Port Status option to display the state of a selected port for a selected node.

The Serial Port Monitor displays the process name and the PID (process identifier) for the process using the port. Also displayed are various parameters, plus the state (green for high, grey for low) for:

- DTR (Data Terminal Ready)
- RTS (Request to Send)
- BRK (Break)
- CTS (Clear to Send)
- DSR (Data Set Ready)
- RI (Ring Indicator)
- CD (Carrier Detect)
- TX (Transmit)
- RX (Receive)

List NFS Exports

Use the List NFS Exports option to display a list of directories on the Forcefield node, as defined using the command “NFS Exports” on page 180.

Up to ten specific hosts (IP addresses) per directory may be specified, in which case the IP addresses for each directory are displayed.

List NFS Storage

See “List NFS Storage” on page 180.

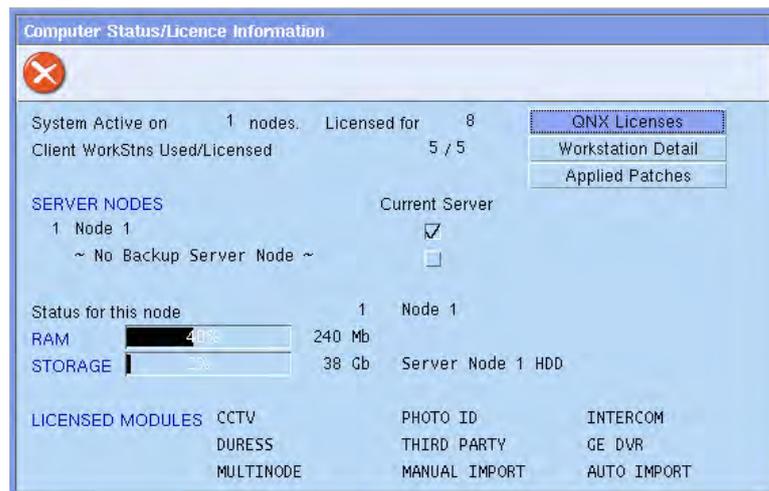
Status > System Status menu

Computer Status

Use the Computer Status option to list the system's:

- Number of nodes and remote workstations used and licensing detail.
- Whether the primary or backup server node is currently the controlling node (if applicable)
- RAM usage and capacity (for the controlling node).
- Hard disk usage and capacity (for the controlling node).
- Licensed modules, such as CCTV or Intercom.

Figure 71: Computer Status and License Information window



QNX Licenses button. Click to view details of QNX licenses for:

- Photon runtime (phrt)
- QNX (qnx)
- QNX TCP/IP runtime (tcpirt)

Each line displays in the format used/total licenses and, where applicable, the node numbers on which the item is being used.

Workstation Detail button. Click to view details of the system, including the status of each workstation and the version number of the Forcefield software currently installed (for the controlling node and active clients only).

Applied Patches button. Click to view the numbers of any service packs that have been installed (see “Service System” on page 242).

System Status

Use the System Status option to list the status of the Forcefield system at the operating system level. It runs various utilities three times at five-second intervals to evaluate how the system status changes over time.

Refer to “Generating reports” on page 28, and the following details about this report.

Node. Select the required Forcefield nodes.

Click the Report to arrow, and then select a destination. In addition to the standard reporting destinations, the System Status report may be e-mailed to a recipient from the address book (see “Email Addresses” on page 166).

Check Log Report

Use the Check Log Report option to list the contents of the Forcefield progress log. It may be requested by support staff.

Refer to “Generating reports” on page 28, and the following details about this report.

Node. Select the required Forcefield node.

Click the Report to arrow, and then select a destination. In addition to the standard reporting destinations, the Forcefield Check Log report may be e-mailed to a recipient from the address book (see “Email Addresses” on page 166).

Debug File Report

Use the Debug File Report option to list the contents of the Forcefield debug file. It may be requested by support staff. The Forcefield debug file is a log kept by Forcefield containing debugging information.

Refer to “Generating reports” on page 28, and the following details about this report.

Node. Select the required Forcefield node. Leave blank to generate for all nodes.

Click the Report to arrow, and then select a destination. In addition to the standard reporting destinations, the Forcefield Check Log report may be e-mailed to a recipient from the address book (see “Email Addresses” on page 166).

Challenger menu

Challenger ID Alteration

Use the Challenger ID Alteration option to bulk rename Challenger record identifiers. Only records within the operator’s member group will be renamed.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Ch field and Id. Select which Challenger will have its points renamed.

Record Type. Select the type of record to rename.

Alter to Member. Select a member if you want the record member altered. Leave blank to skip.

Id Source. Select a source file (see “Using ID source files” on page 68). Only records identified by number in the source file will be renamed, according to the ID in the source file. If no source file is selected, then records will be renamed by applying the prefix and postfix rules described in “Default record IDs” on page 64.

Id Prefix. Optionally specify an ID prefix. For example, in the case of Challenger 35, instead of using the default prefix 'ch35', you could have a prefix 'Factory 9'. See "Using ID prefix" on page 65 for details. Use this option only if there is no ID source file or if using an ID source file results in an error.

Id Postfix. Optionally check the check box and then select a Challenger in order to reuse part of the existing Challenger record ID. For example, instead of using the default postfix such as 'input 1', you could have a postfix 'East Ceiling PIR'. The new ID will be truncated to 30 characters. See "Using existing record ID as ID postfix" on page 65 for details. Use this option only if there is no ID source file or if using an ID source file results in an error.

Challenger programming

A Challenger panel must initially be programmed via a RAS keypad to enable communications with Forcefield.

Note: It is a requirement that Forcefield operators or Technicians using this section are familiar with the details of Challenger programming as described in the *Challenger V8 & V9 Programming Manual* and the field-level Forcefield online help.

Use the Challenger Programming option to remotely program the Challenger options that would otherwise need to be programmed locally via a RAS keypad.

Figure 72: Challenger window

The screenshot shows a 'Control Panel' window with the following configuration details:

- PANEL:** ID: Vic-Melbourne-High St, Locality: Melbourne, Member: System Default Mbr, Description: High St. Office Challenger panel.
- PANEL COMMUNICATION:** Enabled (checked), to Forcefield Node: 1, IUM (checked), Software IUM (unchecked), Panel Type: V8 Extended, Comms Type: TS0898, IUM CARD Category: Tecom 27 bit, Comms Mode: Event Driven, IP Port: Port 3001.
- COMPUTER CATEGORIES:** Chall: Challenger, Special: Special, Line: Line Activity, Comms: Ch Comms Errors.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Challenger. This number uniquely identifies the Challenger to Forcefield. It must also match the computer address in the Challenger communication options (Challenger installer menu 19, option 9).

Id. Enter a unique name for the Challenger.

Locality. This field determines in which time zone in which the Challenger is located. The Challenger's clock is referenced to this location and controlled by Forcefield.

Member. The member determines which operator can control (and/or see events from) this Challenger.

Description. Optional field to describe the panel, such as "In Cabinet behind Guard room door".

Enabled. When checked the Challenger panel can communicate with Forcefield. If a Challenger is not active, then the Challenger and all its field equipment will be greyed out on any graphics maps on which they appear.

Forcefield Node. Enter the Forcefield node number to which this Challenger panel is connected.

Panel Type. Select one of the following:

- TS Challenger for a V8 Challenger panel.
- V8 Extended for a V8 Challenger panel with support for extra door groups, floor groups, alarm groups and time zones (requires panel firmware version 8.128 or later).
- TS Panel Link for a V9 Challenger panel. When TS Panel Link is selected for a Challenger V9 panel, additional fields display.

Comms Type. Select the connection type used for the particular Challenger.

Note: If the dialler option is selected, Challenger connects via modem and only communicates with Forcefield when initiated by the operator (e.g. a remote control command), by Forcefield or by the Challenger. The communication link disconnects when there is no data to send or receive.

Mode. Select the required communication mode (polled or event-driven).

Port/IP Port/Command. For a dialler connection the entry contains the string sent to the modem. For other connection types the field contains the ID of the comms channel (depending on the comms type).

Backup Dialler. This entry is the string sent to a dialler modem if the primary Challenger communications link goes down. This will only work if dialler modem ports are set up for the node at which the Challenger is connected (see "Serial & Parallel Ports" on page 169).

Note: When a Challenger is using a backup dialler, only alarm events will be sent.

IUM. When checked the Challenger panel uses one of the following types of IUM:

- 4 MB IUM (TS0883) module
- 8 MB IUM (TS0884) module
- Software IUM

If this flag is set and the Challenger does not have the module fitted, or vice-versa, the comms process will adjust the Forcefield database record for the Challenger and will remove all entries for that Challenger from the download buffers.

Software IUM. Applies only to Challenger V8 panels that are not fitted with an IUM module, and when IUM is selected. When checked the Challenger panel is converted to software IUM mode (requires panel firmware version 8.128 or later).

Note: All users will be deleted and user 50 will be replaced with the default master user.

IUM Card Category. Select a card category type if the Challenger is fitted with an IUM module or uses software IUM. This enables Forcefield to determine which user records belong to this Challenger.

Panel Link System. Displays when TS Panel Link is selected in Panel Type. Enter a unique number greater than zero to identify the particular panel-link system to Forcefield.

Panel Link Address. Displays when TS Panel Link is selected in Panel Type. This field identifies the address of the current Challenger in the panel-link system. Valid addresses are from 0 to 15; this must match the address on the panel-link system Challenger's integration board (TS0890).

Encryption. Displays when TS Panel Link is selected in Panel Type. This field indicates that the Challenger will encrypt comms data (applicable only to panel-link system Challenger panels).

Computer Categories and Help fields—each Challenger has four computer category types, which determine how Forcefield will handle events from this Challenger:

- Challenger
- Special
- Line Activity
- Challenger Comms Errors

The computer category names listed above are the standard (read-only) Forcefield computer categories. If you use any of these names, bear in mind that you cannot change any details (such as behaviours). In actual use, you should create new (and therefore editable) computer categories with different names. See “Computer Categories” on page 188 for details.

In each of the four Computer Categories fields, click the arrow to select from the list (the list is restricted to show only the correct types of computer category).

The four computer categories (see Figure 72 on page 217) have associated Help fields to the right. In each of the four associated Help fields, double-click or press F3 to program alarm help information for the category.

Maps. Displays the map numbers of any maps containing the Challenger.

Click the Programming button to open the Challenger programming window. For details of Challenger programming, refer to the *Challenger V8 & V9 Programming Manual*, or see *Appendix A*, Challenger programming.

Copy Challenger

Use the Copy Challenger option to create a new Challenger record by duplicating the programming from another Challenger record.

User records and V9 panel-link records are not copied. Any errors will be reported to a file which can be viewed the end of the copy.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

The use of this command is described in “Copy Challenger” on page 63.

IUM Card Categories

Use the IUM Card Categories option to create records that link users to IUM-enabled Challenger panels.

User records will be downloaded only to IUM Challenger panels that have a matching card category, regardless of the access group programming. This is because the download process has to know what raw card data to send to the Challenger for the user.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Type up to 20 characters of text (e.g. “Factory 4, 26-bit”) and click Save to create a new card category. This card category may be applied to a user on the User Card Data window (see Figure 55 on page 136).

Upload All Challenger Data

Use the Upload All Challenger Data option to upload all relevant data from the selected Challenger.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

The use of this command is described in “Upload Challenger” on page 66.

Challenger Detail Report

Use the Challenger Detail Report option to list the details of a Challenger panel.

Refer to “Generating reports” on page 28.

Challenger Enabled Report

Use the Challenger Enabled Report option to list all Challenger panels that have been set as “Enabled”.

Refer to “Generating reports” on page 28.

Challenger Summary Report

Use the Challenger Summary Report option to generate a report showing a summary of a Challenger.

Refer to “Generating reports” on page 28.

Use the Format selection to generate the report in either text or CSV formats.

Challenger User Report

Use the Challenger User Report option to list the users of a Challenger.

Refer to “Generating reports” on page 28.

Challenger > Download Challenger Data menu

Delete Download Buffer

This command is typically used for dialler panels or offline panels. Use the Delete Download Buffer option to remove from the download buffers all data for a selected Challenger or all Challenger panels. Connected direct-connect Challenger panels are sent data when a record is saved, so there will usually be no data in their download buffers.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Challenger. Select a Challenger panel by its number or ID, or leave blank for all Challenger panels.

Download All

Use the Download All option to download all data for the selected Challenger. You may optionally choose to not download user data.

Any existing data in the download buffer for the selected Challenger will be removed before the addition of the new data.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Challenger. Select a Challenger panel by its number or ID.

Download Users. When checked, Forcefield downloads only user records to the Challenger. Clearing this flag will download all data to the Challenger except for user records.

Download Challenger Users

Use the Download Challenger Users option to download user data to a selected Challenger.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Challenger. Select a Challenger panel by its number or ID.

Download Changes

Use the Download Changes option to download data that is currently in the download buffer to the selected Challenger. Usually there will only be data for dialler Challenger panels because directly-connected and IP-connected Challenger panels are sent data when a record is saved.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Challenger. Select a Challenger panel by its number or ID.

Download User

Use the Download User option to send a single user record to a single Challenger.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

User Num. Select the user.

Challenger. Select a Challenger panel by its number or ID.

Select the user and Challenger, then click Run (or press F6) to initiate the download.

If the user does not have any access groups for the selected Challenger, an error message is displayed and the download does not happen.

Admin menu

Activate Shutdown

Use the Activate Shutdown option to shut down Forcefield (subject to the workstation's Allow Shutdown setting, see "Workstation options—other" on page 177).

Depending on setting of the Shutdown by Logged In Op Only field (see page 228), the initial Forcefield Shutdown window prompts for either:

- Operator code and password, or
- Password only.

Add Event

See "Add Event" on page 120.

Change Root Password

Use the Change Root Password option to change the QNX root password on the Forcefield server.

Forcefield is initially set up using a default QNX root password. This password must be changed to prevent unauthorised access to the QNX shell or to access the Forcefield server using the Forcefield Remote Configuration application (see the *Forcefield External Interfaces Manual* for details).

Type the new password and press Enter. Record the root password and keep it in a secure location.

Press Ctrl+C to close the Change Root Password window.

Disable/Enable Workstation

Use the Disable/Enable Workstation option to enable or disable a workstation login.

The Forcefield server cannot be disabled even though it appears in the list of available workstations.

To enable or disable a workstation login:

1. From the main menu select Admin > Disable/Enable Workstation.
2. Optional: Click the Node arrow, and then select the Forcefield server.
3. Optional: Click the Workstation arrow, and then select a Forcefield workstation to be disabled or enabled.

If no workstations are selected, then the command will apply to all Forcefield workstations. If no node is selected and no workstation is selected, then the command will apply to all Forcefield workstations except the current one.

4. Click the Disable/Enable arrow, and then select the required action to be performed.
5. Optional: Type a message in the Message field (e.g. to indicate who disabled or enabled the node and when).

If you leave this field blank, a default message such as “Forcefield Workstation Disabled” displays.

6. Click Run to execute.

Login Attempts

Use the Login Attempts option to keep track of the number of times in sequence that an operator (or another person using the operator’s login code) enters incorrect passwords, and to lock out the operator for a specified time.

The lock out period ends when administrator resets that login code, or when the optional Lock Out Time expires.

Track Login Attempts. When checked login attempts are tracked.

Login Attempts Allowed. Enter the number of unsuccessful attempts allowed before the operator is locked out.

Lock Out Time. Enter the number of minutes for the lock-out time. Range is from 10 to 999. Note: If 999 is entered, the operator will be locked out of the system, until an administrator resets the login code (see “Reset Operator Lockout” on page 226).

Login Message

Use the Login Message option to create a message that will be displayed to operators when they next log in to Forcefield. The message will be added to any existing message. The operator has the option to delete or keep the message.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

For Operators having Access. Create a message for all operators having this computer access.

Or Operators in Member Grp. Create a message for all operators in this member group.

Or Operator. Create a message for this operator only.

Message. Enter the text of the message.

Mount Storage

Use the Mount Storage option to temporarily mount (make a connection with) a storage device, for example, if requested by Technical Support staff in order to check the connection to the storage device. The device will remain mounted as long as this window is active, and will be unmounted when the window is closed or you click Unmount.

This option replicates the test functionality when a storage record is saved. It provides a means of testing a storage device without opening the storage device's programming window.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Id. Click the arrow to list all storage records. Click the storage device you want to test.

Mount button. Click to check the connection with a selected storage device.

Unmount button. Click to end the connection with a selected storage device (alternatively, close the window).

Page Message

Use the Page Message option to send a message to either an ASCOM Nira Duress system or to an email address.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Message Type. Select the destination type (ASCOM Duress or email).

Beeps (ASCOM Duress only). Select the type of notification that the receiver should get.

Destination. Select the destination (e.g. an e-mail recipient).

Message. Enter the message to be sent.

QNX Shell

Use the QNX Shell option to open the QNX command line.

This function is for advanced system administration and should be used by qualified personnel only as it gives access to the QNX command line.

Type EXIT and press Enter to close the QNX Shell window.

Note: The QNX Shell command opens a QNX shell with normal user privileges. At this level some system directories and commands are not accessible. Access at the superuser (root) level is password-protected and will require the operator to use the switch user command (su) and know the system root password. This information can be supplied by your Forcefield system administrator or technician.

See also “Change Root Password” on page 223.

Reset Operator Lockout

Use the Reset Operator Lockout option to reset an operator’s code after it has been locked out (see “Login Attempts” on page 224).

Common window elements are described in Chapter 3.

Send Operator Message

Use the Send Operator Message option to send messages to other workstations that have an operator logged on.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Send to Node. Select the required Forcefield node.

Work Station. Select a workstation to indicate where the message is to be delivered or leave blank for all workstations.

Message fields. Enter the message here. Click Run (or press F6) to send.

Set System Date/Time

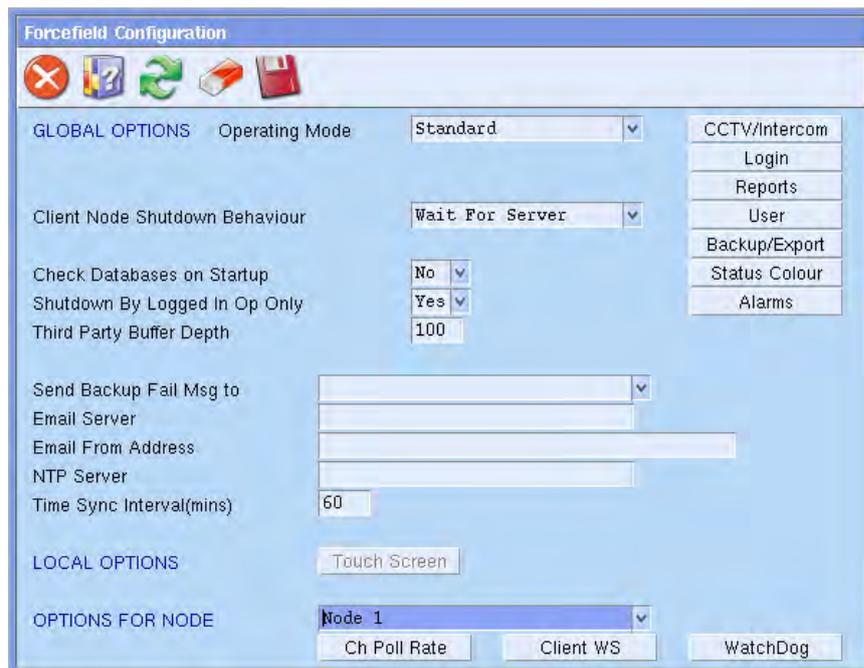
Use the Set System Date/Time option to set the time for the Forcefield server.

Admin > Configuration menu

Configuration

Use the Configuration option to control various settings for the Forcefield application.

Figure 73: Forcefield Configuration window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Operating Mode. Type a Forcefield computer can operate in two modes:

- Standard—Normal mode of operation.
- Watch House—A special mode of operation designed for watch houses.

Master Workstation field (displayed for watch house mode only). Select the workstation that is to be the master control (night switch) workstation. This is the workstation which will lose or gain members as other workstations are logged onto or off from. It is also the node to which intercom call control signals will be directed if Forcefield is controlling an intercom system.

Note: This option is displayed only when Forcefield is running in watch house mode. See “Watch house functionality” on page 5 for details.

Client Node Shutdown Behaviour. Select the Forcefield shutdown action required.

- Wait For Server—Client nodes will wait for an active server.
- Reboot—Node will reboot.
- Shutdown—Node will shutdown and not reboot.

Check Databases on Startup. Select Yes to have Forcefield check the databases at startup time. Note that the action chosen here can be overridden by the operator at startup time. Also note that a large database can take a long time to check.

Shutdown by Logged In Op Only. Select Yes to allow only the logged in operator to shut down Forcefield. The operator has to enter their password. Select No to allow any operator to shutdown Forcefield. This requires the operator to enter both their login code and password.

Third Party Buffer Depth. Amount of events that will be held in the third-party event buffer. This value is global to all third-party systems used by Forcefield. Refer to the *Forcefield External Interfaces Manual* for details of integrating third-party devices into the Forcefield system.

Send Backup Fail Msg to. Select a workstation to receive messages from the Auto Backup processes if the backup fails. A desktop message will be sent to this workstation indicating the failure and the appropriate action to take. Leaving this field blank will result in no operator notification except via alarms.

Email Server. Enter the address of the email host that Forcefield will use to send emails. See “Event Paging” on page 81 and “System Status” on page 215 for uses of email. **Note:** This email host must accept unauthenticated mail.

Email From Address. Enter the domain part of the email address that Forcefield will use for the ‘from’ address for Forcefield-generated emails. For example, enter “Fred.com” to generate emails that display a from address such as “Forcefield E-mail.Pager@Fred.com”.

NTP Server. Specify the time server IP address here to allow Forcefield to synchronize its time to NTP (Network Time Protocol) server time.

Time Sync Interval. Enter a value in minutes to control how frequently Forcefield updates its local time to other nodes in the system.

Local Options. Select the node you wish to configure.

Options For Node. Select the node you wish to configure.

CCTV/Intercom button. Click to configure CCTV/Intercom parameters (see “Configuring CCTV/intercom options” on page 229).

Login button. Click to configure Forcefield login options (see “Configuring login options” on page 229).

Reports button. Click to configure Forcefield report options (see “Configuring report options” on page 230).

User button. Click to configure Forcefield user options (see “Configuring user options” on page 232).

Backup/Export button. Click to configure folder names for a USB, NFS or CIFS storage location (see “Configuring backup and export locations” on page 230).

Status Colour button. Click to configure the colour and behaviour of Forcefield’s maps, Speed Bar, and desktop titles (see “Configuring status colours” on page 231).

Alarms button. Click to configure how Forcefield handles alarms (see “Configuring global alarm options” on page 231).

Ch Poll Rate button. Click to configure Challenger communication poll rate (see “Configuring Challenger poll rate options” on page 235).

Client WS button. Click to configure the TCP/IP port numbers required for Forcefield client communication (see “Configuring client workstation options” on page 235).

WatchDog button. (see “Configuring watchdog options” on page 236).

Configuring CCTV/intercom options

On the Forcefield Configuration window (see Figure 73 on page 227), click the CCTV/Intercom button to configure CCTV and Intercom options.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Door Open Blank Camera Delay. When the operator opens the door associated with an Intercom from the graphics, the video from the associated video camera is left connected to the intercom monitor for the time set here before the video is blanked.

Camera Number for Blank Video. This is the video camera number that will be used to select blank video. This may need to be specially set in the video switcher programming.

DVR: Tagging By Mgt. S/W Delay. This value is used when management software is tagging the DVR. The difference in time between the time the event was generated and the time the management software received the event must be less than the value specified here. If it is greater, no tagging will occur.

Multiview Minimum Dwell. Enter a value in seconds. This value will be the shortest time that can be programmed for a multiview dwell time when creating new camera multiview records, or updating existing records.

Isolated Intercom Alarm Period. This value is the amount of time that Forcefield uses to check to any isolated intercoms in the system. An alarm will be raised for each isolated intercom found.

Video Service VPC Port. Type the port number (for example, 9200) that the Video Presentation Client will use to listen for data. Do not use the same port number as used for the Video Status Manager (VSM). See “Databases > Video > Video Service” on page 200.

Intercom Alarms Only to Intercom Workstations. Select this option to restrict intercom alarms to workstations that are audio workstations for master intercoms.

Configuring login options

On the Forcefield Configuration window (see Figure 73 on page 227), click the Login button to configure Forcefield login options.

Forcefield 6 (and later) features a revised menu structure designed for rapid access to commands. However, operators familiar with navigating Ares or Forcefield (prior to version 6) may prefer to use the Classic menu structure. Both menu structures contain the same commands, so operators can choose the one that works best for them.

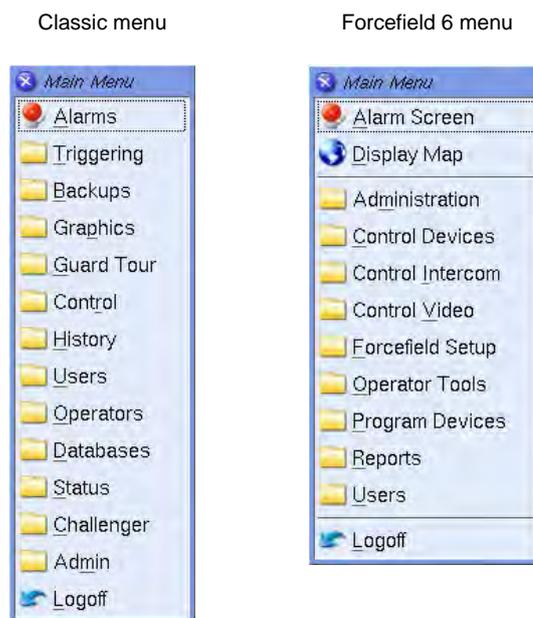
Minimum Password Length, Type a number from 4 through 12 to specify the password length.

Login Menu Structure. Select the required menu structure:

- Classic menu structure, as used in Ares or Forcefield (prior to version 6). This manual is based on the classic menu structure.
- Forcefield 6 menu structure, available only for Forcefield 6 and later. Refer to Appendix C “Forcefield 6 menu reference” on page 307 for details.

Click Save to apply the new menu structure at next login. The two menus (top level only) are shown in Figure 74 below.

Figure 74: Comparison of classic main menu to Forcefield 6 main menu



Configuring report options

On the Forcefield Configuration window (see Figure 73 on page 227), click the Report button to configure Forcefield report options.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Keep report files for. Enter the amount of time in days that Forcefield will allow report files to remain in the system before automatic deletion.

Configuring backup and export locations

This option applies to backing up or exporting files to a USB, NFS or CIFS storage location.

On the Forcefield Configuration window (see Figure 73 on page 227), click the Backup/Export button to define the folder names where Forcefield will send the backup or export files. By default, history files are sent to a subfolder named “history” and database files are sent to a subfolder named “database”.

History. The default location on the storage is “history”. For example, if using a Windows share (CIFS) whose path is C:\Forcefield, then Forcefield places history backups into C:\Forcefield\history\histdb and history exports into C:\Forcefield\history\histexp. You can change the default folder name as required.

Database. The default location on the storage is “database”. For example, if using a Windows share (CIFS) whose path is C:\Forcefield, then Forcefield places database backups into C:\Forcefield\database\db and configuration backups into C:\Forcefield\database\config. You can change the default folder name as required.

Configuring status colours

On the Forcefield Configuration window (see Figure 73 on page 227), click the Status Colour button to configure the colour and behaviour of Forcefield’s maps, Speed Bar, and desktop titles.

Populate the Blink check box to make the colour blink.

Click Set to Default to restore all colours and blinking behaviour to the initial (default) state. Note: All programmed settings for this option will be reset.

Configuring global alarm options

On the Forcefield Configuration window (see Figure 73 on page 227), click the Alarms button to configure how Forcefield handles alarms.

Incident Generation. Forcefield can group a member’s events into incidents. An incident is a series of events (starting with an alarm event) belonging to a member.

- None—incident records are not used.
- Auto—Forcefield automatically initiates incident records starting with an alarm event.
- Manual—operators must manually initiate incident records from the Alarm screen by clicking the Begin Incident button on the Alarm window (see Table 4 on page 32).

Deny ACK For Unrestored Sector Alarms. If set to Yes, alarms originating from a device with a sector number in its computer category cannot be acknowledged until restored.

Alarm Screen Sector Alarm Msg Name. If Deny ACK For Unrestored Sector Alarms is set to Yes, and the operator tries to acknowledge an unrestored alarm, Forcefield displays an error message such as “Can’t ACK. Sector Alarm Not Restored”. You can change the name “Sector” in the error message as required.

Delay Override Alarm Response. This setting controls how alarm responses are handled for devices that do not require a restoral (as set by the device's computer category). When set to Yes, the alarm response is delayed until the operator clicks Respond on the override notice, *and* acknowledges the alarm. When set to No, the alarm response is generated when the operator clicks Respond on the override notice.

Override Alarm Delivery Order. This setting controls the order in which override alarms are presented to operators. Select Time to present override alarms in chronological order. Select Priority to present alarms in order of their assigned priority number. For example, a higher priority 2 alarm will displace a lower priority 5 alarm.

Configuring user options

On the Forcefield Configuration window (see Figure 73 on page 227), click the User button to configure Forcefield user options.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Allow Auto User Number Allocation. When checked Forcefield automatically allocates a user number when an attempt is made to create a user record without a user number. Forcefield searches from user 1 to find the lowest available user number.

Manual PIN Code for Users above 1000. When checked Forcefield assigns PIN codes to users above 1000. Normally, if a user number is above 1000, Forcefield matches the PIN code automatically assigned by the door/lift controller. The user number downloaded to the Challenger must still be below 1000. Refer to "User Offset" in the Challenger programming (see "System Options" on page 270).

Prohibit Shared Profiles. When checked Forcefield uses prohibit shared profiles mode. Prohibit shared profiles mode causes user profiles (and alternative user profiles) to be locked to user records. For example, user 1 can have only "User 1 Profile" and optionally "User 1 Alt Profile".

Refer to "Converting to prohibit shared profiles mode" on page 55 before selecting this option.

Remove Unreferenced Profile on User Deletion. When checked Forcefield prompts the operator to allow deletion of a profile when a user record has been removed and no other users refer to that profile. We recommend that this option is used when Forcefield is in prohibit shared profiles mode to help ensure that unused profiles are not left in the database and accidentally reused.

User Search Order. Select one of the following options:

- **Alpha-Numeric By Member.** This option typically provides rapid searching of user records sorted within the current operator's members. This option has no effect for master operators because they have every member.

- **Strict Alpha-Numeric.** This option may be slow and the GUI may appear to be unresponsive if there are large numbers of user records and most of them don't have members within the operator's member group.

Surname Order. Select the name order. The User Maintenance window uses one field for a user's name, and this option tells Forcefield whether the first word is the user's surname or first name (see Figure 54 on page 131).

Muster Time. Specifies the time interval prior to generating a muster report that a user is considered mustered (see "Muster Report" on page 158). For example (where muster time is 15), all on-site users who badged at a muster reader within the past 15 minutes (of when the report is generated) are considered to be mustered. On-site users who have not badged at a muster reader within the past 15 minutes are considered to be not mustered.

User Defined Field Title. The value programmed here is used as the title of the user defined data field on the User Maintenance window (see Figure 54 on page 131, the default title is 'Reference'). If the user defined data field is not needed, any data that has been previously saved can be removed with "Delete Unused Data" on page 130.

Smart Card Issue Site Code. Enter the default site code to be used when issuing smart cards.

Note: The default site code can be overwritten on an individual workstation basis.

Smart Card Issue Type. Select the default card type to be used when issuing smart cards.

Note: The default card type can be overwritten on an individual workstation basis.

Import User Data. This section relates to "Import User Data" on page 162. Select an option for Forcefield to import user data:

- **No**—Forcefield will not import user data.
- **Manual**—Forcefield will import user data when initiated by the operator.
- **Auto**—Forcefield will import user data automatically. When this option is selected, additional fields display to let you specify the scan time from 15 to 999 seconds. This is the amount of time Forcefield waits before scanning the import directory for an import file.

From. Select the source directory for automatically importing user data. This should be an NFS or CIFS connected device.

Report To. Select a printer where the import report will be printed.

Export User Data. Select an option:

- **No**—Forcefield will not export user data.
- **Manual**—Forcefield will export, must be Forcefield operator initiated.

- Auto—Forcefield will export without operator intervention. When this option is selected, additional fields display to let you specify the file format and destination.

In Format. Select an option:

- CSV—refer to the *Forcefield External Interfaces Manual* for details.
- TSV—refer to the *Forcefield External Interfaces Manual* for details.

To. Select an option:

- Local—this will be the local user export directory which will have to be NFS exported so the remote computer can access the data.
- Remote—a remote NFS directory for which Forcefield has write permission or a CIFS connection (e.g. a Windows share). If you selected Remote, also select the destination directory for automatic exporting of user data. This should be an NFS/CIFS connected device.

Event Monitor Information button. Click to open the User Event Monitor Data window that you can use to select one or more types of user data to be displayed in the Event Monitor when a user-related event occurs.

For each type of user data selected, you can also add a prefix to be displayed. For example, if you select the Phone check box, then you could also add a prefix like “PH” to be displayed in front of the number.

Note: Additional user details are displayed only in the Event Monitor. They are not recorded in event history.

Configuring backup and export storage options

On the Forcefield Configuration window (see Figure 73 on page 227), click the Backup/Export button to configure the backup and export storage sub-folder names for USB, NFS, and CIFS storage locations. Backups and exports to floppy disk or cartridges use the entire device without sub-folders.

The default sub-folder names are “history”, “database” and “config”. Forcefield places history backups into the further sub-folder “backups” and history exports into the further sub-folder “exports”.

For example, if using a Windows share folder (CIFS) with a name `c:\Forcefield`, the paths specified here are the various folder names that Forcefield will create under that path (`c:\Forcefield\history\`, `c:\Forcefield\database\`, and so on).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

History. Type the name for the history sub-folder in the designated USB, NFS, or CIFS storage location. For example, if using a Windows share folder with a name `c:\Forcefield`, and “my_history” is entered, then:

- History backups will go into `c:\Forcefield\my_history\backups\`
- History exports will go into `c:\Forcefield\my_history\exports\`

Database. Type the name for the database sub-folder in the designated USB, NFS, or CIFS storage location. For example, if using a Windows share folder with a name c:\Forcefield, and “my_db” is entered, then database backups will go into c:\Forcefield\my_db\backups\.

Hardware. Type the name for the hardware sub-folder in the designated USB, NFS, or CIFS storage location. For example, if using a Windows share folder with a name c:\Forcefield, and “my_hw” is entered, then database backups will go into c:\Forcefield\my_hw\backups\.

Configuring Challenger poll rate options

On the Forcefield Configuration window (see Figure 73 on page 227), click the Ch Poll Rate button to configure Challenger poll rate.

The poll rate is used for poll/response Challenger panels. As the Challenger is a poll/response device, specifying a longer value here means that Forcefield will take longer to find out what is happening in the field equipment. Specifying a shorter time will increase the bandwidth required. This may be important if you are using a shared network (TCP/IP).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Direct Connect, poll every. The time in milliseconds of the delay between successive polls of a direct connect Challenger.

TCP/IP, poll every. The time in milliseconds of the delay between successive polls of a TCP/IP-connected Challenger (e.g. a serial Challenger connected via a terminal server such as an MSS-1).

Dialler, poll every. The time in milliseconds of the delay between successive polls of a dialler connected Challenger.

Recall, poll every. The time in milliseconds of the delay between successive recalls of Challenger status.

Event Driven, heartbeat every. **Note:** Heartbeat timeout for event-driven Challenger panels is no longer programmed via this option. Forcefield 6.1 and later uses the heartbeat timeout value programmed in the “Heartbeat Timeout” option on page 298.

Configuring client workstation options

On the Forcefield Configuration window (see Figure 73 on page 227), click the Client WS button to configure the Forcefield Client options.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Control Port. Enter the TCP/IP port number used for remote workstation identifier message transfer.

Transfer Port. Enter the TCP/IP port number used for remote workstation file transfer.

Note: Port 4868 is always required and is not configurable here. Port 4868 must always be available for Forcefield.

Configuring watchdog options

Forcefield Enterprise hardware can integrate with watchdog cards to detect mains failure, low battery, and system lockups.

On the Forcefield Configuration window (see Figure 73 on page 227), click the Watchdog button to configure the watchdog options. The Watchdog button is enabled only when the Forcefield hardware supports it.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

WatchDog Active. Check to indicate there is a watchdog card installed on this node.

Type. Select the type of watchdog card installed (WD501-P type is selected by default).

Reset Period. Enter the time in seconds that the watchdog card will wait for a pulse from Forcefield before it resets the system (if the watchdog reset line is wired to the computer's reset line). If the watchdog card does not get a pulse from Forcefield every x seconds, it will reset the system. The minimum value is 9 seconds and the default value is 60 seconds.

IRQ. Enter the IRQ (interrupt request) value the card is set for.

- If the card is an ISA bus card the address is set by jumpers on the card.
- If the card is a PCI bus card use the `show_pci -v` command to determine the I/O address and interrupt that the computer BIOS has assigned to the card.

I/O Address. Enter the I/O address of the card.

- If the card is an ISA bus card the address is set by jumpers on the card.
- If the card is a PCI bus card use the `show_pci -v` command to determine the I/O address and interrupt that the computer BIOS has assigned to the card.

Change Site ID

Use the Change Site ID option to change the name displayed at the top of the Forcefield desktop.

The Forcefield license disk contains the site ID, which is displayed at the top of the Forcefield desktop. In order to change the name displayed at the top of the Forcefield desktop both the old and new license disks are required.

The Change Site ID command uses the current license disk to confirm the site identification, and then it uses the new license disk to install the new site ID.

Change Dialup Password

Use the Change Dialup Password option to enable the Forcefield Client Point-to-Point Protocol (PPP) dialup password to be changed.

Enter the new Forcefield Client PPP dialup password, enter it a second time to confirm, and then click Save.

Commission Node

Use the Commission Node option to set up internode encryption files, which enables Forcefield to communicate between nodes.

Common window elements are described in Section 3. Elements specific to this window are described below.

Node. Select the node to be commissioned and then click Run. The new node will automatically restart and run Forcefield.

Copy System to Node

Use the Copy System to Node option to copy Forcefield files from the primary controlling node onto another node and to commission that node for use by Forcefield.

To Node. Select the destination node, and then click Run.

Icon Editor

Use the Icon Editor option to modify or create icons for use on Forcefield Speed Bar and Alarm Screens.

Figure 75: Forcefield Icon Editor window



Icons are fixed size symbols (31 x 25 pixels), and the icon files are required to be located in `/usr/ares/config/symbols/`.

The symbol editor has six function buttons, a work area, a display area, two size selection widgets, colour and tool selection buttons.

This location may be altered in the Save and Save As options but they will not be available for graphics display if they are not in the default directory.

Function buttons

The symbol editor's function buttons are:

- **Load.** Opens the file selection screen and loads the symbol from the selected file. No checking is done for unsaved data. This operation will overwrite any current data in the work area.
- **Save.** Saves the current symbol from the work area using the current filename. If there is no current filename the operation does nothing.
- **Clear.** Clears the work and display areas.
- **Save As.** Save the current symbol from the work area using the filename selected from the file selection screen or a new filename entered.
- **Undo.** Goes back ONE drawing operation.
- **Help.** Displays the Icon Editor help.

Colour selection

The default colour palette is two rows of buttons representing the default colours. To select a non-default colour, click the Current Colour button to bring up the colour selection widget.

To make a pixel transparent use the right mouse button in pencil mode.

Drawing tools

Ten buttons select the drawing options:

- **Pencil.** Tool replaces the colour of the pixel under the cursor with the current colour for left click, transparent for right click.
- **Horizontal Line.** Tool replaces the colour of the entire row under the cursor with the current colour.
- **Vertical Line.** Tool replaces the colour of the entire column under the cursor with the current colour.
- **Paint.** Tool replaces the colour of all pixels having the colour of the pixel under the cursor with the current colour.
- **Add Rectangle.** Drag a rectangle, upon release the rectangle is drawn in the current colour.
- **Cut Rectangle.** Drag a rectangle, upon release the rectangle is set to transparent the other drawing tools select operations on the current symbol.
- **Flip Horizontal.** The symbol is mirror image reversed around the vertical axis.

- **Flip Vertical.** The symbol is mirror image reversed around the horizontal axis.
- **Copy and Move.** First an area is selected with a drag operation, then the upper left hand corner of the destination is chosen. The original area is copied to the destination
- **Cut and Move.** First an area is selected with a drag operation, then the upper left hand corner of the destination is chosen. The original area is made transparent and the original area is drawn to the destination.

Tip: Hold the cursor above a button to display the name of the button.

Modify License

Use the Modify License option to add licensed modules, or install additional node licenses. The Forcefield license disk contains the details of the licensed modules (such as CCTV). In order to add licensed modules, or install additional node licenses, a new license disk is required.

Insert the new Forcefield license disk, and then click Continue to update the license.

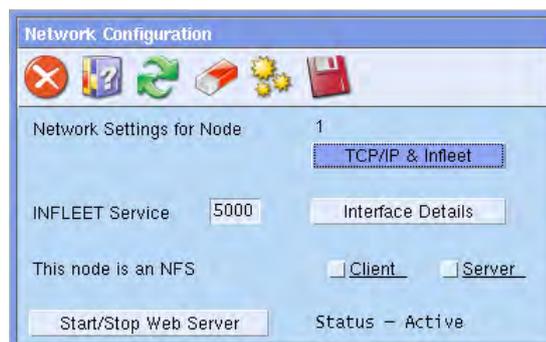
Note: Restart the Forcefield server after installing the new or modified license.

Network Configuration

Use the Network Configuration option to configure the Forcefield system network.

Note: After any details are altered, the Forcefield system will have to be shut down and rebooted for the new settings to take effect.

Figure 76: Network Configuration window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

TCP/IP & Infleet button. Click to configure IP addresses and infleet nodes. See “Configuring TCP/IP addresses and infleet nodes” on page 240 for details.

Infleet is required where nodes are to communicate using infleet (TCP/IP) instead of FLEET (QNX MAC)—this requires TCP/IP be set for the selected

nodes. Infleet configuration is required only if TCP/IP (not QNX FLEET) internode communication is required.

TCP/IP configuration is required only if:

- Forcefield clients are being used from the node.
- IP-connected Challenger panels are connected to the node.
- Infleet internode communication is required.
- Forcefield triggering is set to send packets to UDP/IP devices.
- Any third party equipment requiring TCP/IP is connected.
- NFS or CIFS facilities are required.

Note: Communication between nodes over a WAN is not recommended due to network performance considerations. All nodes including the primary and backup servers should be on the same network segment and will usually be connected to switches, so there will be no effect on other general network performance.

Interface Details button. Click to configure the network details for the this node.

See “Configuring TCP/IP addresses and infleet nodes” below for details.

Each interface corresponds to a logical LAN running on a particular Network Interface Card (NIC). The particular NIC is referenced by the -I argument to the Net.driver, e.g. Net.ether1000 -I3 would refer to LAN 3 and would be interface 3 in this utility. Normally only 1 interface is required and is capable of carrying both QNX MAC and TCP/IP traffic.

Infleet Service. The starting number for the infleet service in /etc/services. This is usually 5000, it must be identical on all nodes. Forcefield will use up to 20 consecutive values depending on the version of Forcefield and how many infleet nodes are required.

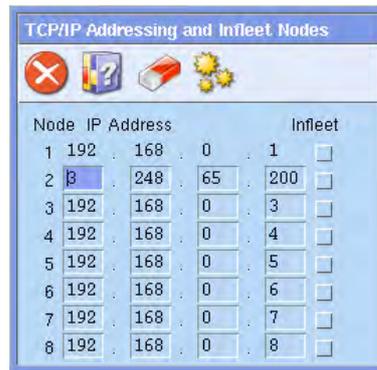
Client. When checked the Forcefield client can be an NFS client and can use NFS mounted storage on other IP hosts as though it is local storage. See “NFS Storage” on page 181 for details.

Server. When checked the Forcefield server can be an NFS server and can export Forcefield directories to allowed ‘other’ IP hosts. See “NFS Exports” on page 180 for details.

Start/Stop Web Server button. Click to toggle the state of the Forcefield server’s onboard Web server. The Web server allows Forcefield Client software to be installed via an IP connection instead of from CD or USB device. The Web server should be stopped (inactive) if it is not in use, and is inactive by default each time the Forcefield server is restarted.

Configuring TCP/IP addresses and infleet nodes

The TCP/IP Addressing and Infleet Nodes window displays node numbers followed by IP Address fields and an Infleet check box. Figure 77 on page 241 indicates a non-Enterprise Forcefield system with up to 8 nodes.

Figure 77: Network Configuration window (TCP/IP & Infleet)

Set the check box for the required node to enable TCP/IP addressing, and then program the TCP/IP address used by the default interface for that node. It is not possible to set the check box for the local node.

Note: When offsite redundancy is used, enter the IP address for the mirror site (which will operate as node 1 when active) in the IP address fields for the highest node number.

QNX normally operates on a LAN that has no routers (QNX packets are not routable).

QNX 4 uses the following Ethernet protocol:

- Ethernet 2.0 based on the DIX (Digital, Intel, Xerox) 2.0 specification
- QNX 4 has an assigned ethertype of 0x8203

To use FLEET (which is the recommended method), the network should be straight cable or routers or switches capable of passing the 0x8203 packets. If this is not possible, the FLEET packets must be encapsulated into TCP/IP.

Configuring network details

This is where the network configuration details for this node are programmed.

Figure 78: Interface Details window (example IP address used)

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Address fields. Enter the IP address of the Forcefield server (refer to your system administrator).

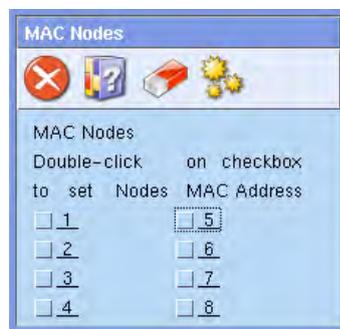
Gateway fields. Enter the gateway address of the Forcefield server (refer to your system administrator). Any gateway address set for the default interface will be the default gateway for the Forcefield server's IP traffic (i.e. any traffic to an unknown host will be routed to this gateway).

Netmask fields. Enter the netmask required for the Forcefield server (refer to your system administrator).

Broadcast fields. Enter the broadcast address (refer to your system administrator). A broadcast address is not normally required.

QNX Details. Click the MAC Nodes button to open the MAC Nodes window (Figure 79 below).

Figure 79: MAC nodes window (standard Forcefield example)



MAC nodes can communicate over QNX's normal networking protocol (FLEET). The addressing used on these nodes is the Media Access Control (MAC) address. QNX 4 uses the following Ethernet protocol:

- Ethernet 2.0 based on the DIX (Digital, Intel, Xerox) 2.0 specification
- QNX 4 has an assigned ethertype of 0x8203

To use FLEET (which is the recommended method), the network should be straight cable or routers or switches capable of passing the 0x8203 packets. If this is not possible, the FLEET packets should be encapsulated into TCP/IP. To do this from Forcefield, select those nodes as Infleet nodes.

To program an Infleet node:

1. Right-click to select the remote node's check box (the number to the right of the check box is the node number). The local node cannot be checked.
2. Double-click the populated check box to open the MAC Node Address window.
3. Click Read Current Address to enter the MAC address of the relevant node.

Service System

From time to time, we may issue service pack files for Forcefield (e.g. for a product enhancement). Use the Service System option to select and run a service file.

To run a service file:

1. From the main menu select Admin > Configuration > Service System.
2. Click the Service System from arrow, and then select the storage location containing the service file.
3. Select the storage location containing the service file.
4. Click Run to execute. Forcefield displays a File Selector window
5. Select the service file and then click Update. A QNX window opens containing instructions.
6. Follow the instructions in the QNX window to complete the procedure. The Service Forcefield window displays a progress bar during the update process.

Set Server Locale

Use the Set Server Locale option to define the time zone that the Forcefield node resides in.

If the Forcefield node is in a location that uses daylight saving time, the start and end dates must be entered. The time of switching in or out of daylight saving time is 2 a.m.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Timezone & Daylight Saving Data for Node. Select the required node.

Location. Select the timezone location required for the Forcefield node, e.g. Australia - Central, New Zealand, etc.

Has Daylight Saving. Check the box to indicate that the location uses daylight savings. Setting this option will bring up the day of week, week of month, month of year entry fields.

Speed Bar Configuration

Use the Speed Bar Configuration option to edit the Forcefield Speed Bar for a particular workstation (see Figure 6 on page 18).

After editing or adding a button, logout and then login again to see the new button. Some operators may not see new buttons because of the operator's access levels.

There are two types of Speed Bar buttons that may be added:

- Event Macro. Activates a Forcefield 'Event Macro' which can trigger numerous devices (see "Event Trigger" on page 81).
- A Forcefield menu item. Opens menu option, rather than having to navigate through the menus.

To see (and select) a current Speed Bar button, click List (or press F12).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Macro. Check the box to indicate that a macro function is required. When checked the Function list displays macros.

Icon. Select an icon to use on the Speed Bar button. To create a new icon, see “Icon Editor” on page 237.

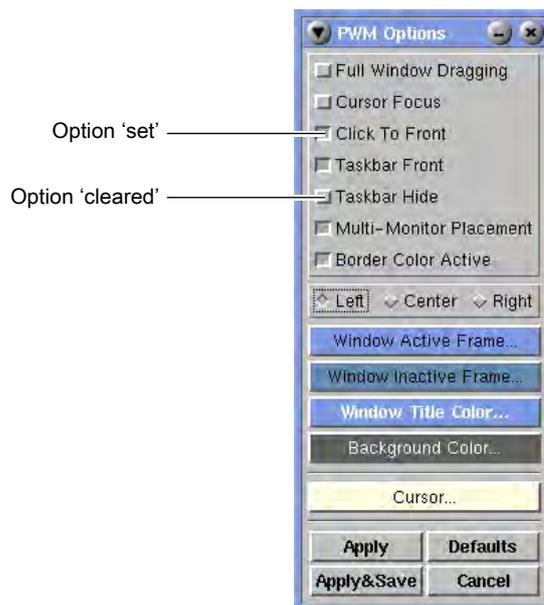
Function. Select the required function or macro.

Help String. Enter the text to be displayed when your mouse moves over the Speed Bar button.

Windows Manager Options

Use Windows Manager Options to control the appearance and behaviour of Forcefield windows, including move, resize, minimize, maximize, raise, lower, and close. It provides common window frame borders that can be customized based on the requirements of the specific application. It also creates and manages the Taskbar.

Figure 80: Windows Manager Options window



The Windows Manager Options settings for the Forcefield user workspace are as follows:

- **Full Window Dragging** selection. If set, windows are continuously redrawn as they are dragged/moved around the screen. If cleared, only an outline of the window frame is dragged and the window is redrawn at its final position. This is useful for Forcefield Client.
- **Cursor Focus** selection. If set, focus is given to the window under the cursor. If cleared, focus remains with the current focus window regardless of cursor location. The focus window is the one that receives all keystrokes.

- **Click to Front** selection. If set, a click in any part of the window will bring it to the front. If cleared, only clicking in the title bar will bring a window to the front.
- **Taskbar Front** selection. If set, the taskbar is the topmost window. If cleared, the focus window appears on top of all other windows on your workspace.
- **Taskbar Hide** selection. If set, the taskbar is hidden. If cleared, the taskbar always appears at the bottom of your workspace.
- **Multi-Monitor Placement** selection. In a multi-monitor environment, several monitors make up a single workspace, so you may want the new windows to open relative to the entire group of monitors, rather than just the current monitor. If set, new windows open relative to the entire group of monitors, rather than just the current monitor. If cleared, new windows appear on your current monitor.
- **Border Colour Active** selection. If set, applies the window active frame colour to the border.
- **Left, Centre, Right** selections. Sets the alignment of the window title.
- **Window Active Frame...** button. Enables a different colour to be selected for this item.
- **Window Inactive Frame...** button. Enables a different colour to be selected for this item.
- **Window Title Colour...** button. Enables a different colour to be selected for this item.
- **Background Colour...** button. Enables a different colour to be selected for this item (not applicable for Forcefield Client).
- **Cursor...** button. Enables a different style and colour to be selected for this item (not applicable for Forcefield Client).
- **Apply/Revert** button. Click to apply changes and save them to the configuration file. The text on the button changes to Revert. Click the Revert button to apply changes without saving them to the configuration file. Click the Revert button again (without making any more changes), to revert to the original settings. This is useful to test the behaviour of a user interface against a variety of operating paradigms without the need for saving and relaunching the configuration window.
- **Apply and Save** button. Click to save any modified options. This will write the options to the user configuration file as well as instruct Windows Manager to reconfigure itself to the new options.
- **Defaults** button. Click to restore options to their defaults. The default options are Full Window Dragging, Click To Front, and Centre title alignment. The colour defaults for the window are window green when active and medium grey when inactive.

- **Cancel** button. Click to quit the options configuration program without saving any changes. You can also cancel by closing the window from the menu or pressing the Esc key.

Admin > Data Mirroring menu

Checkpoint History

This option is displayed only for the mirror site.

Checkpoint History Mirror. This option is used to archive the history received from the primary node at the mirror node. The archive file, identified with the date and the suffix “-Mir”, can be used to generate reports via the Offline History option.

Mirror Setup

Use the Mirror Setup option to configure Forcefield’s data mirroring system for offsite redundancy.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

The Mirror Setup window differs depending on the setting of the Primary or Mirror Site field. See “Mirror Setup window for the primary site” below and Mirror Setup window for the mirror site” on page 247.

Mirror Setup window for the primary site

Primary or Mirror Site. Select Primary.

Mirror Address. Enter the IP address of the mirror site.

Comms Port. Enter the number of the mirror computer’s TCP/IP port. Note that three consecutive ports are used starting with the number entered here.

Monitor Secondary Server. When set to Yes on the primary site, Forcefield monitors the mirror site and can generate a Failure of Mirror Site alarm. This setting will not cause data and history transfer between the two sites (data and history transfer are set separately).

Heartbeat. Enter the maximum number of seconds allowed between monitoring heartbeat messages between live and mirror sites. Note: The heartbeat time on the mirror site should be higher than the value selected for the primary site. Failure to ensure this will result in the mirror site generating heartbeat timeout events.

Max Miss. Enter the number of consecutive missed monitoring heartbeats before the primary site assumes the mirror site is not available. Forcefield will start without mirror monitoring if this number of missing heartbeats is exceeded.

Start Forcefield After. When Monitor Secondary Server is set to Yes, enter the number of failed connection attempts before the primary site assumes the mirror site is not available. Forcefield will start without mirror monitoring if this number of failed connection attempts is exceeded.

Transfer Data. Select Yes if data is to be dynamically transferred from the primary to mirror site. This setting will cause buffering and transmission to the mirror site of any data changes.

Transfer Data Heartbeat. When Transfer Data is set to Yes, enter the maximum number of seconds allowed between data transfer heartbeat messages between live and mirror sites. Note: The heartbeat time on the mirror site should be higher than the value selected for the primary site. Failure to ensure this will result in the mirror site generating heartbeat timeout events.

Transfer Data Max Miss. Enter the number of consecutive missed data transfer heartbeats before an alarm is generated.

Transfer Data Max Buffered Transactions. Enter the maximum allowed number of transactions allowed in the primary site data buffers.

Transfer History. Select Yes if history is to be dynamically transferred from the primary to mirror site. This setting will cause buffering and transmission to the mirror site of any history changes.

Transfer History Heartbeat. When Transfer History is set to Yes, enter the maximum number of seconds allowed between history transfer heartbeat messages between live and mirror sites. Note: The heartbeat time on the mirror site should be higher than the value selected for the primary site. Failure to ensure this will result in the mirror site generating heartbeat timeout events.

Transfer History Max Miss. Enter the number of consecutive missed history transfer heartbeats before an alarm is generated.

Transfer History Max Buffered Transactions. Enter the maximum allowed number of transactions allowed in the primary site history buffers.

Mirror Setup window for the mirror site

Primary or Mirror Site. Select Mirror.

Primary Address. Enter the IP address of the primary site.

Comms Port. Enter the number of the primary computer's TCP/IP port. Note that three consecutive ports are used starting with the number entered here.

Monitor Primary Server. When set to Yes on the mirror site, Forcefield monitors the primary site and can take over if the primary site fails. This setting will not cause data and history transfer between the two sites (data and history transfer are set separately).

Heartbeat. Enter the maximum number of seconds allowed between monitoring heartbeat messages between live and mirror sites. Note: The heartbeat time on the mirror site should be higher than the value selected for the primary

site. Failure to ensure this will result in the mirror site generating heartbeat timeout events.

Max Miss. If the startup action is set to “Become Server”, enter the number of consecutive missed monitoring heartbeats before Forcefield starts as an active mirror site.

Takeover As Primary After. When Monitor Primary Server is set to Yes, enter the number of failed connection attempts that will trigger the mirror site to take over.

Transfer Data. Select Yes if data is to be dynamically transferred from the primary to mirror site. This setting will cause buffering and transmission to the mirror site of any data changes.

Transfer Data Heartbeat. When Transfer Data is set to Yes, enter the maximum number of seconds allowed between data transfer heartbeat messages between live and mirror sites. Note: The heartbeat time on the mirror site should be higher than the value selected for the primary site. Failure to ensure this will result in the mirror site generating heartbeat timeout events.

Transfer Data Max Miss. Enter the number of consecutive missed data transfer heartbeats before an alarm is generated.

Transfer History. Select Yes if history is to be dynamically transferred from the primary to mirror site. This setting will cause buffering and transmission to the mirror site of any history changes.

Transfer History Heartbeat. When Transfer History is set to Yes, enter the maximum number of seconds allowed between history transfer heartbeat messages between live and mirror sites. Note: The heartbeat time on the mirror site should be higher than the value selected for the primary site. Failure to ensure this will result in the mirror site generating heartbeat timeout events.

Transfer History Max Miss. Enter the number of consecutive missed history transfer heartbeats before an alarm is generated.

Startup History Archive Action. Select what to do with the primary site's history when the mirror site starts. Select New to create a new primary site history archive. Alternatively, select Append to add to the current primary site history archive. In either case, a new working archive is created when the current working archive becomes full. NOTE: No reporting is possible from the working archive. In order to report on the latest primary site history it is necessary to create a dated archive (see “Checkpoint History” on page 246).

Local Operations. Select the manner in which the mirror node operates. Select Mirror Only to restrict the Forcefield menu to setting up mirror operation only. Alternatively, select Read Only Forcefield to enable an operator to perform most functionality, except for data saving operations.

Takeover Mode. Specify how the mirror site takes over Forcefield. Select Instantly to reconfigure and reboot as the active server site as soon as failure of the primary site is detected. Select Time Delay to reconfigure and reboot

as the active server site after a configurable delay. This allows the operator at the mirror site to abort the takeover by shutting down. Select Manual to stop monitoring of the primary site, with no further action by Forcefield. A manual reconfigure and shutdown/reboot will be required to takeover as the active server site.

If the takeover mode is Time Delay, specify the number of minutes or seconds of delay time, and then select either minutes or seconds.

Startup Action. Specify the behaviour required on the mirror at startup. Select Wait for Primary if you want the mirror to wait without limit for the primary site (the operator can abort waiting). Select Become Server if you want the mirror to take over as the server node.

Statistics

Use the Statistics option to view details of mirroring.

Click the Database or History buttons to see summaries of:

- Whether mirroring is selected
- Heartbeats
- Transactions

Admin > Tools menu

Event Simulator

Use the Event Simulator option to simulate most events that can occur in a Forcefield system. For example, event simulator can be used to test event triggering.

Event simulator is used to create the same outcomes as you would expect to see generated by actual equipment. You need to know what outcome to expect in order to use this tool.

Common window elements are described in Chapter 3. Elements specific to this window are described below (the titles of the data entry fields depend upon the selected event).

Event. Select the event to be simulated (you can type some characters to filter the selection).

From Challenger. Select an existing Challenger, or type a Challenger number for an existing or non-existing Challenger.

From XX field (where XX depends on the selected event). Select an existing device or type a number for an existing or non-existing device.

User field (for user events). Select an existing user or type a number for an existing or non-existing user.

Click Run to simulate the event.

aca Events

Use the aca Events option to run the Forcefield communication analyser.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Click the Start aca by arrow, and then select one of the following options:

- **Challenger.** Show event activities for a specific Challenger panel.
- **Serial Port.** Show event activities for Challenger panels connected by direct serial or dialler connections.
- **TCP/IP Port.** Show event activities for all event-driven IP Challenger panels that are using the IP port.
- **TCP/IP Host.** Show event activities for polled IP Challenger panels that are using the IP host (the IP address). This includes any Challenger panels connected via terminal server.

QNX Shell

See “QNX Shell” on page 225.

Status File Utility

Use the Status File Utility option to read the existing status of a point, and optionally to update the status of a point.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Type. Select the type of point required (area, computer, DGP, etc.).

Point. Select the point required (only points for the selected type are displayed). The status is automatically read and displayed in the Status File Utility window.

- Click Run to re-read the status of the same point.
- Click Save to change the contents of the status file to the values set on the screen.

Alarm Status. Read-only, it is not updated on a save.

System Information

Technical support staff may use the System Information option to diagnose faults and to ensure correct system operation.

Appendix A

Challenger programming

Summary

This appendix describes how to use the Forcefield user interface to program Challenger panels connected to the system.

Content

Introduction	255
Inputs	256
Areas	259
Arming Stations	260
DGPs	263
Alarm Groups	268
Timers	269
System Options	270
Auto Reset	273
Communication Options	273
Text Words	277
Printer Options	277
Event Flags	278
Timezones	278
Doors & Lifts	279
User Category Data	287
Relays	288
Auto Access – Secure	289
Areas Assigned to Vaults	290
Floors	290
Holidays	290
Input Shunts	291
Time Zones to Follow Relays	292
Regions	293
Cameras	293
Custom RAS Display	294
Battery Test	294
Maintenance	294
Security Password	295

Macro Logic	295
Panel Condition Events	296
Floor Groups	297
Door Groups	297
Radio Options	297
Ethernet Configuration	298
Panel Link (V9 only)	299

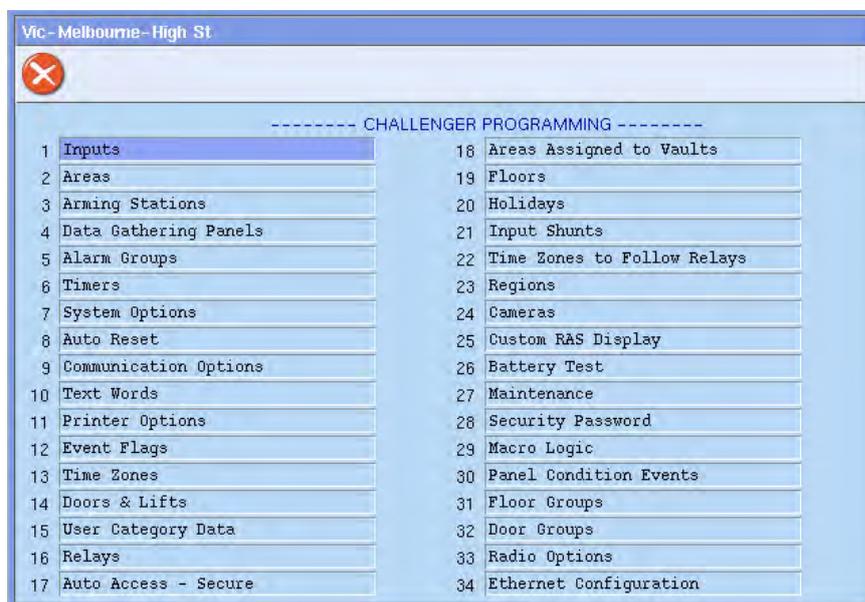
Introduction

A Challenger panel must initially be programmed via a RAS keypad to enable communications with Forcefield.

It is a requirement that Forcefield operators or Technicians using this section are familiar with the details of Challenger programming as described in the *Challenger V8 & V9 Programming Manual* and the field-level Forcefield online help.

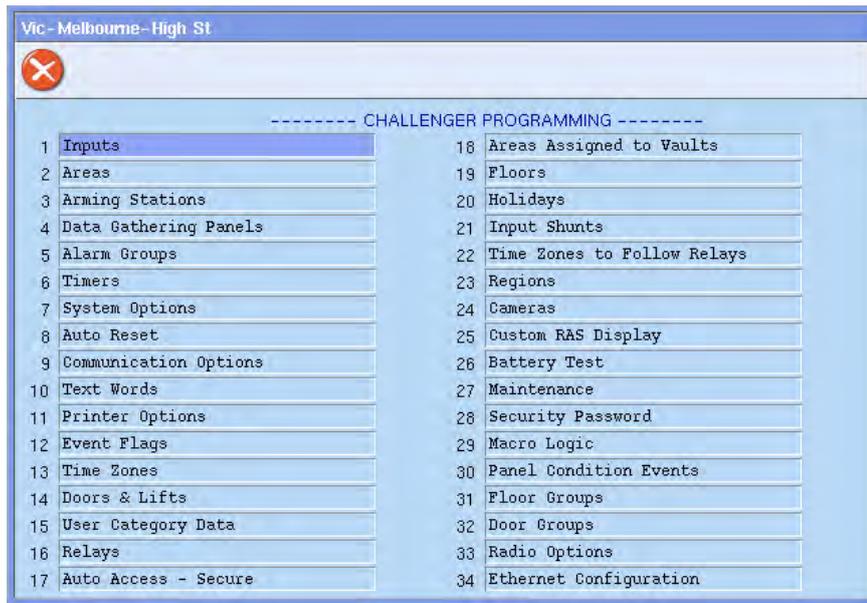
Use the Challenger Programming options to remotely program the Challenger options that would otherwise need to be programmed locally via a RAS keypad.

Figure 81: Typical Challenger Control Panel window



Refer to “Challenger programming” on page 217 for details of using the Control Panel window.

Click the Programming button to open the Challenger programming window (Figure 82 on page 256), and then click a programming item. Challenger programming items are described in the following sections (options displayed depend on panel type and communication type).

Figure 82: Typical Challenger programming options window

Inputs

This function is used to program an individual input for a Challenger panel.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter the same number as programmed in the Challenger for the input.

Inputs are numbered from 1 to 256.

Id. The Input ID (name) is used by Forcefield to identify the input. The name must be unique (it is not possible to have “Input 1” in Challenger x and “Input 1” in Challenger y).

Description. Type a short description of the input.

Name button. Click to open the Text Phrase window, used to program the input name. The input name will appear on the Challenger display during many Challenger user functions. Double-click or press F3 to program the name.

Use the Text Phrase window to:

- Select pre-defined text words from the Challenger word library (word numbers from 1 to 899) or the user-defined word library (word numbers from 900 to 999).
- Add new text words to the user-defined word library (word numbers from 900 to 999).
- Create phrases by combining text words with text variables.

All text words in the Challenger word library are identified by a reference number in the range 001 to 899. You can program up to 100 additional words numbered in the range 900 to 999.

The input name should enable easy recognition of that input. The name consists of a combination of:

- Up to four words (called text words).
- A text word may be accompanied by a numeral in the range 1 to 255 (called a text variable). Text variables enable you to use the same text words to describe more than one input.

For example, a text word 'Building' may be followed by a text variable '1' to enable the input to be displayed as "Building 1" where another input can be displayed as "Building 2" by using the text variable '2' for that input. Some other examples are:

- Office 4 Door 1 Contact
- Workshop PIR 6
- Building 6 Area 4 Room 1 Door 6

An input name can be up to 36 characters, consisting of four text words, each of which may be followed by a text variable.

Type. The input type determines exactly how the input will function in given circumstances. Each input type has been given a name and reference number. The input type selected here will also determine whether the input will function using areas or an alarm group. The appropriate option is displayed when programming the remainder of the input record.

Note: The input type is significant and influences much of the remaining programming and functions of the system. Careful attention should be given to the explanation of input types in *Challenger V8 & V9 Programming Manual*.

Areas Assigned selections. When checked associates one or more areas with the input. It will not be accessible if the input type is 6, 31, 34 or 35 (see Alarm Group field, below).

The areas that should be assigned to an input are those where:

- The condition of the input (sealed/unsealed) directly affects the area alarm status, for example, unsealed input during the active period = area in alarm.
- The status of the area (access/secure) affects the function of an input, for example, unsealed input generates alarm only if the areas assigned to it are in the active period.

The interaction between the input and the areas assigned to it will depend on the input type programmed for the input.

Note: Inputs must have at least one area assigned. It is impossible to reset an alarm on an input that has no area assigned.

Alarm Group. Click the Alarm Group arrow, and then select an alarm group to assign to an input. It will be displayed instead of area if the input type is 6, 31, 34 or 35. The function of the alarm group will depend on the input type programmed for the input. These input types would be used for key switches,

etc., to arm/disarm areas (it causes the input to act like a user entering an alarm control code).

Contact Id. Program a Contact ID code (or click the arrow, and then select a Contact ID classification) if the panel reports to a remote monitoring station using Contact ID or Tecom direct line formats.

Print When Unsealed. When checked the panel prints an event indicating the input is unsealed any time the input changes from sealed to unsealed. The event is sent to the Challenger's printer (if a printer is connected).

Event. Select a custom event flag, or a pre-defined event flag, to be activated any time an alarm is generated by the input. The selected event flag is used in addition to any pre-defined event flags programmed for this input.

Event Active On Unsealed (displays only when the Event field is populated). When checked the event specified in the Event field is triggered when the input changes from sealed to unsealed, regardless of the status of the area assigned to the input.

Test Type. This function determines the testing procedure for the input. It relates to the access and secure tests and does not affect manual tests on individual inputs. This record will not be valid unless the test mode is programmed appropriately (see "System Options" on page 270).

Video Cam. Selects the video camera associated with this input. This option is used when operator selects the video option on the graphics window. When programming this option, the video camera is identified as being controlled by a DVR or by a switcher.

- Select DVR if the camera is controlled by a DVR. Refer to the *Forcefield External Interfaces Manual* for details.
- Select Switcher if the camera is controlled by a video switcher. In this instance, selecting the video option on the graphics window will switch this camera to the selected view. The view for this camera can be selected in the View field.

Note: Sector alarm inputs have their CCTV functionality controlled by a computer category, which is assigned a sector number. As a result, the Video Cam field is not used.

View. Selects the preset view for the video camera. If this field left blank, the video camera, if a PTZ camera, will switch to preset 1.

Note: Sector alarm inputs have their CCTV functionality controlled by a computer category, which is assigned a sector number. As a result, the View field is not used.

Member. The member controls event reporting and operator control in Forcefield.

Computer Cat. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each input can have a different computer category. The category determines how Forcefield will handle an event from this input. The computer category “Input” can be used, but is a standard (read-only) Forcefield computer category and cannot be modified. See “Computer Categories” on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item. The help programmed here will be displayed as an action on the alarm window when alarm are generated.

Maps. Displays the map numbers of any maps containing the input ID.

Areas

This function is used to program an individual area for a Challenger panel.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter the same number as programmed in Challenger for the area. Areas are numbered from 1 to 16.

Id. The Area ID (name) is used by Forcefield to identify the area. The name must be unique (it is not possible to have “Kitchen” in Challenger x and “Kitchen” in Challenger y).

Text. Click the arrow to select a pre-defined text words from the Challenger word library (word numbers from 1 to 899) or the user-defined word library (word numbers from 900 to 999). Double-click the field to create a new user-defined word.

Entry and Exit time fields: Determine the amount of time allowed between entry to an area and disarming of that area and, between exit from an area and arming of that area. If the programmed time is exceeded, an alarm will be activated.

Area Disarm. The user category timer will use the time programmed here as the disarm time instead of the user category time.

Event Flag fields: Select the event flags to be assigned to the area.

Area Linked To fields (links an area to other areas to enable common control). Select the required areas to be linked.

Video Cam. Select the video camera associated with this input. This option is used when operator selects the video option on the graphics window. When programming this option, the video camera is identified as being controlled by a DVR or by a switcher.

- Select DVR if the camera is controlled by a DVR. Refer to the *Forcefield External Interfaces Manual* for details.
- Select Switcher if the camera is controlled by a video switcher. In this instance, selecting the video option on the graphics window will switch this

camera to the selected view. The view for this camera can be selected in the View field.

View. Selects the preset view for the video camera. If this field left blank, the video camera (if a PTZ camera) will switch to preset 1.

Member. The member controls event reporting and operator control in Forcefield.

Computer Cat. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each area can have a different computer category. The category determines how Forcefield will handle an event from this area. The computer category name "Area" can be used, but is a standard (read-only) Forcefield computer category and cannot be modified. See "Computer Categories" on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item. The help programmed here will be displayed as an action on the alarm window when alarm are generated.

Maps. Displays the map numbers of any maps containing the area.

Challenger V9 option

Global Area For Panel Link. Check this box to enable the global setting for this area. When the global area is armed, all the other corresponding areas on each respective V9 (Panel Link) Challenger panel will also arm. For example, if this Challenger is panel 2 and global is enabled for area 4, then when area 204 (panel 2, area 4) is armed, area 4 will arm in all linked panels.

Arming Stations

This function is used to program an individual remote arming station (RAS) for a Challenger panel.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter the same number as programmed in Challenger for the RAS. RASs are numbered from 1 to 16.

Id. The RAS ID (name) is used by Forcefield to identify the RAS. The name must be unique (it is not possible to have "Front Door" in Challenger x and "Front Door" in Challenger y).

Polled. When checked the Challenger panel polls this RAS.

Desc. Type a short description.

Smart Card Reader. When checked the RAS is designated as a smart card reader. The Smart Card Options button is active for designated smart card readers, refer to "Programming smart card options" on page 51 for details.

Area Alarm Group. Select an alarm group to determine the areas that can be controlled via this RAS, the functions which can be performed, and so on.

Note: Both the alarm group of the RAS and the alarm group of the user performing the functions must permit the action.

Relay Group. Enter the number of the relay control group. This relay control group can then be used to drive relays on the RAS. (Refer to the appropriate Arming Station Installation Guide.)

Menu Alarm Group. This alarm group is valid only when a user is performing user menu functions which require information to be displayed for areas other than those controlled by this RAS. The menu alarm group allows these areas to be displayed in status reports but they cannot be controlled via the RAS. If the menu alarm group is programmed for “No Access”, then the RAS will use the same alarm group for menu access as programmed in area alarm group.

Door Event. The event flag entered here is used to program this RAS to open a door. The event flag will be activated when a valid code is entered at this RAS. The event flag is active for the time programmed in Timer (option 6) “Door Open”.

Door Event for All Codes. When checked the door event flag will operate (unlock the door) for either a valid alarm code or a valid door code. When not selected, the door event flag will operate (unlock the door) only for a valid door code.

Note: Door codes must be at least four digits and are determined by the value of the Alarm Prefix Digits (see “System Options” on page 270).

Reset from RAS without code (use for LCD keypad RASs only). When checked a user can reset alarms by pressing [Enter] [Enter] (show alarms) followed by 0 [Enter]. The areas in alarm must be assigned to the RAS’s alarm group. When not checked, the user’s alarm code is required to reset alarms.

LCD Arming Station. When checked identifies this reader as an LCD arming station.

Cards Auto Disarm (used for card reader RASs). When checked cards can disarm areas without using the [OFF] key. When not checked, only the door is unlocked, except if Card Always Arms/Disarms is set to YES or the [ON]/[OFF] key is used.

One Key Arm/Disarm (used for keypad RASs). When checked a user can enter their user code, and then arm or disarm areas by entering the number of the area without pressing [Enter].

Note: This option is only available for areas 1 through 9. If an LCD arming station is used as master; and “Arm Using One Key” is set to YES, the system must be programmed so that areas 10 to 16 can never be armed.

Card Always Arms/Disarms (used for card reader RASs). When checked allows cards to arm/disarm alarm groups without using the [ON]/[OFF] keys. Toggle Keyboard Control must also be set to YES.

Note: The card user's alarm group and the arming station's (reader's) alarm group must both allow arm and/or disarm functions before a card can be used to arm/disarm.

Toggle Keyboard Control (used for keypad RASs). When checked the [ON] and [OFF] keys lose their function. For arm control the user must enter the user code followed by [ON], [OFF], or [Enter]. If a list of areas appears, pressing the area number and [Enter] toggles the status of the area. If no list appears, the status of the areas is toggled immediately.

Enter Key Opens Door Only (used for keypad RASs). When checked the [Enter] key unlocks the door but the [ON] and [OFF] keys are used for alarm control. When not selected, the [Enter] key unlocks the door, provides alarm control, and resets alarms. Select this option for the best user interface on LCD arming stations.

Note: This option cannot be used in conjunction with keypad duress functionality.

Display Shunting on LCD (used for LCD RASs). When checked and an input is shunted, the text 'Input Shunted' is displayed on the LCD.

Restricted User Category to Disarm. When checked users with a user category can only disarm or delay automatic arming (cannot be used for user categories with arm and reset).

3 Badge Arm. When checked the assigned areas will arm with three badges of a valid card within ten seconds (if Cards Auto Disarm is selected).

Note: Applies to RAS models with card reader. This option requires panel firmware version 8.79 or later.

Muster Reader. When checked the reader is a muster reader. For more information, see "Muster Report" on page 158. Note: Muster Reader is a Forcefield function and has nothing to do with RAS programming.

Card And PIN Always. When checked both a card and PIN must be used within the card and PIN time (see "Timers" on page 269) to access RAS menus. If not checked, then only a PIN is required.

Video Cam. Selects the video camera associated with this RAS or door. This option is used when operator selects the video option on the graphics window. When programming this option, the video camera is identified as being controlled by a DVR or by a switcher.

- Select DVR if the camera is controlled by a DVR. Refer to the *Forcefield External Interfaces Manual* for details.
- Select Switcher if the camera is controlled by a video switcher. In this instance, selecting the video option on the graphics window will switch this camera to the selected view. The view for this camera can be selected in the View field.

View. Selects the preset view for the video camera. If this field left blank, the video camera, if a PTZ camera, will switch to preset 1.

Member. The member controls event reporting and operator control in Forcefield.

Computer Cat-RAS. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each RAS can have a different computer category. The category determines how Forcefield will handle an event, such as off line or tamper, from this RAS. The computer category name “RAS” can be used, but is a standard (read only) Forcefield computer category and cannot be modified. See “Computer Categories” on page 188 for details.

Computer Cat-Access. If the RAS is used as an access control device, such as a door reader, click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each RAS can have a different access computer category. The category determines how Forcefield will handle an access event, such as invalid PIN or entry granted, from this RAS. The computer category name “Door Access” can be used, but is a standard (read only) Forcefield computer category and cannot be modified. See “Computer Categories” on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item.

The help programmed here will be displayed as an action on the alarm window when alarm are generated. The RAS-specific help text enables Forcefield to display text on the alarm window (for alarms from the RAS) in a customised manner (that is, different from another RAS).

Maps. Displays the map numbers of any maps containing the RAS.

Challenger V9 options

LED Mapping button (only for systems using panel link (V9) Challenger panels).

Click the LED Mapping button to open the Panel Link LEDs Mapping window.

For each LED on the RAS, select the linked panels and areas to indicate via the LED. This option enables the status of an area on one panel to be displayed on a RAS connected to another panel. An 8 or 16 area RAS can be programmed using this option to display any area across the V9 system. For example, RAS number 1 has LED number 16 mapped to area 201. Therefore when area 201 is armed LED 16 on RAS 1 will turn on (and not when area 16 is secured on panel 0).

DGPs

This function is used to program an individual Data Gathering Panel for a Challenger.

Figure 83: DGP programming window



Common window elements are described in Section 3. Elements specific to this window are described below.

Num. Enter the same number as programmed in Challenger for the DGP. DGPs are numbered from 1 to 15. Door and lift controllers are numbered from 1 to 12.

Id. The DGP ID (name) is used by Forcefield to identify the DGP. The name must be unique (it is not possible to have “Level 1” in Challenger x and “Level 1” in Challenger y).

Type. Click the arrow to select:

- Standard DGP
- Door Controller (refer to “Programming a door controller or a lift controller” on page 265)
- Lift Controller (refer to “Programming a door controller or a lift controller” on page 265)
- Inovonics DGP (refer to “Programming an Inovonics DGP” on page 267)

Polled. When checked the Challenger panel polls this DGP.

Location. Enter the DGP’s location details.

Member. The member controls event reporting and operator control in Forcefield.

Computer Cat. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each DGP can have a different computer category. The category determines how Forcefield will handle an event from this DGP. The computer category name “DGP” can be used, but is a standard (read-only) Forcefield computer category and cannot be modified. See “Computer Categories” on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item.

The help programmed here will be displayed as an action on the alarm screen when alarm are generated.

Maps. Displays the map numbers of any maps containing the DGP.

Programming a door controller or a lift controller

In the Challenger programming window for a door controller or a lift controller (see Figure 83 on page 264), click the Programming button to open the Door/Lift Controller programming window.

Figure 84: Door/Lift Controller programming window

The screenshot shows the 'Door/Lift Controller : 1 : Intelligent controller' window. It features a toolbar with icons for back, help, refresh, save, and print. The main configuration area includes:

- Num of Relay Controllers:** 0
- Region Limit:** (empty)
- Tamper Monitor:**
- Alarm Prefix Digits:** 0
- Siren Monitor:**
- TIMES:**
 - Card to PIN: 8 Sec
 - Mode: 5 Sec
 - Lock Release: 3 Sec
 - Dual Custody: 8 Sec
- RELAYS:**
 - Tamper:
 - Mains Fail:
 - Low Battery:
- SITE CODE:**
 - 1: (empty)
 - 2: (empty)
- SITE OFFSET:**
 - 1: 0
 - 2: 0
- Buttons:** Macro, Poll DGPs, Vers7
- Forced Door Debounce:** 0 x100mS

Below the configuration fields is a table for 'Rdr Detail' with columns for DOOR, SC, POLL, LCD, EGR, TGL, SC, POLL, LCD, EGR, TGL, and Door Id. The table is divided into two sections: RAS 1 and RAS 2.

----- RAS 1 -----											----- RAS 2 -----										
DOOR	SC	POLL	LCD	EGR	TGL	SC	POLL	LCD	EGR	TGL	Door Id										
1	In	1				5					Vic/Me1b/Reception										
	Out	9				13															
2	In	2				6					Vic/Me1b/Hallway Entry										
	Out	10				14															
3	In	3				7					Vic/Me1b/Office 1 Door										
	Out	11				15															
4	In	4				8					Vic/Me1b/Office 2 Door										
	Out	12				16															

SC=Smart Card Reader (double-click to set reader configuration)

Common window elements are described in Section 3. Elements specific to this window are described below.

Num of Relay Controllers. Records the number of relay controllers fitted to the Intelligent controller. Maximum is 32 (255 relays).

Region Limit. Specify the maximum number of personnel permitted to occupy the controller's "in" region.

Tamper Monitor. When checked the Intelligent Controller inputs are monitored for tamper alarm. If set, the inputs are monitored for four states (alarm, seal, open, and short). If not set, The inputs are monitored for two states (alarm, and seal). Should be set to the same function as set in "System Options" on page 270.

Alarm Prefix Digits. Records the difference between the number of digits in an alarm control code and the number of digits in a door control code. The complete user code is the alarm control code, and the prefix is omitted to make the door control code.

Times. Select the correct time intervals and scales for each option.

Relays. For each relay, enter a number in the range 1 to 16. These are the physical relays on the door/lift controller.

Site Code fields (also called facility code). Records the first site identification number used in cards. Each system has a unique site ID. Two site code numbers and associated card offsets can be programmed in order for the

system to be used with two sets of cards with different site codes. For example, when a system has been commissioned, one set of cards (on loan) can be used while awaiting delivery of a second set of customised cards.

Site Offset. Specifies a number that is added to, or subtracted from the actual card ID number, for cards on Site Code A. The resulting card ID after processing is the number which is used when programming users; and which is reported to the printer and computer.

Rdr Detail sections: Select the required functionality for each RAS connected to the Intelligent Controller. The 16 RASs that can be polled relate to specific doors on the controller; and the reader direction, where readers are mounted on both sides of the same door.

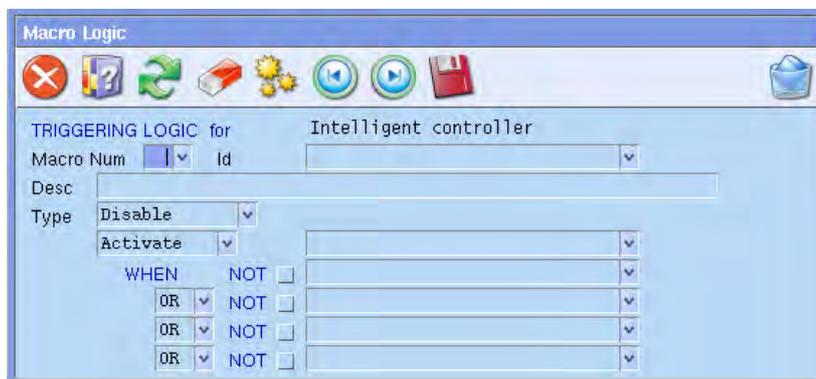
- **SC.** Check this selection to designate the reader as a Smart Card reader. Double-click a checked selection box to open the TS0870 Configuration window (see “Programming smart card options” on page 51 for details).
- **Poll.** The arming stations listed here will be polled by the controller. PIN code readers, mag card readers, and single Wiegand interface units are polled as arming stations. Polling allows the arming station to transfer data to the Intelligent Controller.
- **LCD.** RASs that have an LCD (Liquid Crystal Display) fitted.
- **EGR.** records the address of any RASs being polled that require the egress button to be wired to the IN or EGRESS terminal on the RAS. **Note:** Since this connection point does not provide fault monitoring, it is preferable to wire any egress buttons to inputs on the four-door Controller.
- **TGL.** This option is used if any RASs on the controller LAN are enabled to function in a 'Toggle Mode'.

Macro button. Click to program macros (see Figure 85 below).

Poll DGPs button. Click to select DGPs to be polled.

Vers7 button. Click to program Challenger version 7 options.

Figure 85: DGP Macro Logic Programming window



The DGP Macro Logic programming window is used to program Intelligent Controller events to be generated under specific logic conditions. Only events

relating to the controller that you are programming can be used. About half the events available can be input or output events in the macro logic, while the rest can only be input events.

Macro Num. Records the number of the macro logic program (48 programs are available).

Id. Macro identification information for Forcefield.

Desc. Macro description and associated information.

Type. Selects the function of the event flag or input when activated.

- Disabled—Macro logic program disabled.
- Non Timed—Follows the result of the logic equation only.
- On Pulse—Activates for the programmed time or the active period of the logic result, whichever is the shortest.
- On Timed—Activates for the programmed time regardless of the logic result.
- On Delay—Activates after the programmed time period unless logic result is no longer active.
- Off Delay—Follows the result of the logic equation, but remains active for the time programmed after the logic result is no longer active.
- Latched—Activates on any of the first three inputs in the logic equation and is reset by the fourth input (AND / OR function not used).

Time. Records a time period which is used when any of the timed functions are selected. A value of 2 or greater should be used. When programming 1 to 4 minute periods, program in seconds (i.e. 60, 120, 180 or 240 seconds).

Activate or Deactivate. Select whether to activate or deactivate the selected output event.

Output field (not labelled). Select the event flag to be activated.

Logic Equation fields: The logic connecting the four inputs can be programmed for AND or OR functions. A NAND or NOR function can be achieved by inverting the logic of the particular input. Set the NOT box to invert the logic of the input.

When all conditions of the logic equation are met, the result is active and the output event programmed in the previous step will be activated (depending on any timing function programmed).

Note: Any unused inputs must be left as OR functions.

Programming an Inovonics DGP

The TS0825 wireless DGP is integrated with an Inovonics receiver. TS0825 can receive signals from Inovonics transmitters, providing up to 32 virtual inputs and 2048 duress inputs.

In the Challenger programming window for an Inovonics DGP (see Figure 83 on page 264), click the Programming button to open the TS0825 programming window.

Common window elements are described in Section 3. Elements specific to this window are described below.

Site Code A. Enter the site A number in the range 1 through 511. A value of 0 disables reception.

User Offset A. Enter a positive user offset number for site A. When a duress message is sent to the Challenger, the Inovonics transmitter's duress number is added to the user offset (a sum greater than 65,535 is rolled over past zero).

Site Code B. Enter the site B number in the range 1 through 511. A value of 0 disables reception.

User Offset B. Enter a positive user offset number for site B. When a duress message is sent to the Challenger, the Inovonics transmitter's duress number is added to the user offset (a sum greater than 65,535 is rolled over past zero).

Supervision Time. Click the Time arrow, and then select a value in the range from 10 minutes through 150 hours.

Inovonics transmitters can be programmed to check-in to the DGP every 60 seconds or 5 minutes, therefore the DGP requires a wide tolerance on the time it checks for the existence of each transmitter device that is programmed to check in.

As a general rule, a small number of devices will function normally with a 60-second check-in time and a 10-minute supervision time (per formed by the DGP). However, as the number of devices increase, temporary supervision failures may be experienced. In this event, the DGP supervision time may be increased , or the transmitter devices may be reprogrammed to a 5-minute check-in time.

Points fields: Click the arrow for the required inputs 1 through 32 and select:

- Enabled, where the input is always enabled.
- Disabled, where the input is always disabled.
- Relay, where the input is controlled by the first relay assigned to the DGP.

Note: The TS0825E Inovonics EcoStream Wireless DGP is not supported in Forcefield and must be programmed via a RAS. Refer to the *TS0825E Wireless Data Gathering Panel Installation & Programming Guide* for details.

Alarm Groups

See "Alarm Groups" on page 140.

Timers

This function is used to program time values applicable to timed system functions for a Challenger.

Common window elements are described in Section 3. Elements specific to this window are described below.

Notes

- Timers will time for +/- 1 of the value entered, so avoid using values of 1 second or 1 minute. If any timer is set to 0, the timer will never time out when activated.
- If set to "0", the areas will not rearm automatically. The user category time will be overridden by the area disarmed time (if programmed) in the area database.

User category 1 to 7 fields: Program times (0 to 255 minutes) for user categories 1 through 7 for the time they are disarmed. The user categories have to be programmed for timed disarm and must be assigned to an alarm group before the time is programmed.

User category 8. The system ignores any value entered for user category 8.

Individual test. Enter the maximum time (0 to 255 minutes) to perform a test on an individual input, using User menu 12, Test Input.

Suspicion. Enter the time (0 to 255 seconds) that a camera continues to operate after a suspicion input type has switched to sealed state. **Note:** Suspicion time is available for input types 7, 40, and 47.

Access test. Enter the time to perform the access test (0 to 255 minutes).

Secure test. Enter the time to perform the secure test (0 to 255 minutes).

Warning. When user categories are used and areas are programmed for timed disarm, a warning will sound (if a warning time is programmed) indicating the areas are about to alarm. Enter the time this warning will sound (0 to 255 minutes). **Note:** The warning time must always be set for a shorter time than any user category disarmed time. The warning time must always be shorter than the shortest user category time and should be at least 2 minutes.

Delayed holdup. Enter the delay time (0 to 255 seconds) before an alarm from a delayed disarmed alarm is reported to the remote monitoring company (the delay time is ignored if another delayed input type has already been activated).

Local alarm reminder. Enter the time (0 to 255 minutes) that can elapse between acknowledging a local alarm and a re-alarm occurring, including the audible alert.

Service. User menu 17 can be used to give access to service technicians. The alarm group for the technician needs time zone 25 to be assigned. When a user enables the service technician, time zone 25 will be valid during the service time. Enter the service time (0 to 255 minutes).

Tester event. Enter the time (0 to 255 seconds) that the tester event flag is triggered to activate devices in order to perform an secure test. **Note:** The event flag will only be triggered for half the programmed time; the remaining time is used to allow the device to switch back to sealed state. The event flag used is preset to 16.

Door Open. Enter the time (0 to 255 seconds) that doors will unlock (using the door event flag) to allow doors to be opened. **Note:** This time value is common for all door event flags from RASs connected to the control panel (doors 1 to 16). Doors 17 to 64 are connected to DGPs and are individually programmed via the DGP.

Mains fail. Enter the delay time (0 to 255 minutes) before a mains is reported to the remote monitoring company. Enter a value of "0" for no delay.

Siren. Enter the time (0 to 255 minutes) that the onboard internal siren drivers activate.

RAS Card & PIN Time. If Card And PIN Always is selected in "Arming Stations" on page 260, enter the time (0 to 255 seconds) in which the entire badging and PIN entry must be completed.

System Options

This function is used to program the options that are common to the whole system for a Challenger.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Event Text. Click the arrow to select a pre-defined text words from the Challenger word library (word numbers from 1 to 899) or the user-defined word library (word numbers from 900 to 999). Double-click the field to create a new user-defined word.

Test Mode. Click the Test Mode arrow, and then select a test mode option (enable auto test, manual access/auto secure, or auto access only). The test mode determines if, or when, arm or disarm tests will be performed. The test mode option selected does not affect manual testing of any individual input.

Relay Controllers. Enter a number from 1 to 32 for the number of output controllers that are fitted to the main control panel (do not enter values for output controllers fitted to DGPs). Enter 0 if there is no output controller fitted, or if there is one 4-way relay fitted.

Alarm Prefix Digits. Enter 1 to use alarm code prefix (see note below). The alarm code prefix value enables users to enter a door code (a shorter PIN code) for access control. For example, if a user's full PIN code is five digits (e.g. 12345), and the alarm code prefix digits value is 1, then the first digit is removed for access control and the user can operate doors by entering only the last four digits of the PIN code (e.g. 2345).

Note: Control panels connected to Forcefield should use either 0 or 1 in the Alarm Prefix Digits field. A control panel that is not connected to Forcefield can use up to four alarm code prefix digits. However, Forcefield may be connected to several control panels, with varying numbers of alarm code prefix digits in each panel (one panel might use one digit and another panel might use two digits). Forcefield does not support multiple prefix digits in a system of control panels.

Film Low Level. Enter the frame count number used to indicate low film.

Film Out Level. Enter the frame count number used to indicate no film.

User Offset. This offset is used for management software packages. The number entered here will be added to the user number in the Challenger and sent to the management software. This can be used in conjunction with card offsets.

For example, the user has a proximity card with site code of 000688 and a card number of 250. The offset values are as follows:

- The site code offset is -150.
- The user offset is 75.

The Challenger will see user 100 (card number 250 adjusted by the site code offset of -150). The management software will see user 175 (user 100 in the Challenger, adjusted by the user offset of 75).

Site Code A. Records the site identification number (up to six digits) used in cards. Each system has a unique site ID. Two site code numbers and associated card offsets can be programmed in order for the system to be used with two sets of cards with different site codes. For example, when a system has been commissioned, one set of cards (on loan) can be used while awaiting delivery of a second set of customised cards.

Card Offset Site A. Specifies a number that is added to, or subtracted from the actual card ID number, for cards on site code A. The resultant card ID after processing is the number which is used when programming users; and which is reported to the printer and computer.

Site Code B. Specifies a number that is added to, or subtracted from the actual card ID number for cards on site code B.

Card Offset Site B. Specifies a number (up to six digits) that is added to, or subtracted from the actual card ID number for cards on site code B.

Display Rotate Delay. Specifies the period before LCD text begins to rotate to be altered.

Display Rotate Speed. Specifies the rotation speed of LCD text to be altered.

Areas To Total Disarm selections. When checked this option allows for input types such as 24-Hour, Access Alarm or Access Local/Secure Alarm types to be totally disarmed by assigning an extra area to the input, which is selected in this option as an area to totally disarm.

Latch System Alarms. When checked makes system alarms latching.

Auto De-Isolate. When checked inputs that are sealed and isolated are automatically deisolated when any of the areas assigned to the inputs are disarmed.

Delay Holdup Lockup (only applicable to latching delayed hold-up buttons). When checked and a delayed hold-up button is pressed, it must be reset first before it can trigger again. Therefore, a latching delay hold-up button is locked out until the physical button is taken out of its latched state (reset).

Disable Flashing LEDs. When checked disables area LEDs from flashing when an alarm occurs.

Display User Flags. When checked enables the special user flags to be displayed when programming users via a RAS.

Name File. When checked, and users are programmed via an LCD RAS, the display prompts for programming a user name when programming users.

Siren Testing. When checked the panel's sirens are tested for three seconds when the secure test is started (test mode 1 or 2).

Disable PIN Display. When checked disables PIN code from being displayed when programming users.

Dual Custody. When checked specifies use of two valid codes to access "Program Users".

Financial Institution. When checked enables three system options generally applicable to financial institutions. These are:

- Film counters are enabled during the access test mode.
- User categories 2 or 6 disable delayed holdup input types.
- Minimum PIN code length is set to five digits.

Tamper Monitoring. When checked all inputs function in four-state mode (sealed, unsealed, short, and tamper). If not selected, all inputs function in two-state mode (sealed and unsealed).

Disable Area LEDs. When checked disables LEDs for areas not reported on.

Sirens Only After Report Fail. When checked alarms will only activate sirens if Challenger fails to report to monitoring company.

Display Alarms Instantly. When checked enables alarm details to be displayed instantly on the LCD RAS.

Stop Auto Category Insert. When checked disables the ability to treat areas as vaults.

Siren & Strobe on Tamper. When checked panel or DGP tamper inputs activate siren and strobe.

Show Inputs 1 at a Time. When checked one input at a time is displayed on the LCD RAS even though there may be more than one in the list of inputs to be displayed (the user must scroll through the inputs).

Auto Reset

This function is used to program the Challenger to automatically reset alarms.

The alarms are for selected areas (determined by an alarm group) and are reset after a programmed pre-determined time.

Note: It may be necessary to program a special alarm group for this function.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Time Before Reset. Enter the time in minutes between the alarm occurring and the automatic reset.

Alarm Group. Enter the alarm group number.

Id. Enter the alarm group ID. To program a new alarm group enter an ID and press F3.

Communication Options

This function is used to record details of the communications link between the Challenger and the remote monitoring company.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

PABX. Enter the number used by the company where the installation is located to obtain an outside line via their switchboard. This field is optional and may be omitted if the system is not connected via the switchboard. In the case of STD telephone numbers, the area code may be entered in this option, or in some remote areas, the satellite access code etc. It is recommended to include one or two pauses after the PABX access code. A pause in the dialling sequence is indicated by P and can be inserted anywhere, e.g. after the PABX access code.

Phone 1. Enter the telephone number that the system will use to communicate. Up to 10 digits can be entered for each record. The area code may be included in the telephone number entry if the total length is still 10 digits or less.

Phone 2. Enter the secondary telephone number that the system will use to communicate (if applicable). If the initial dial attempt fails, the system will dial the first number again twice and if connection is not made on either occasion, the second number will be dialled three times. If connection is still not made, the attempt ceases. Time between dial attempts: 30 seconds, 60 seconds, 5 minutes, 5 minutes, 5 minutes.

Service Ph. Enter the telephone number that will be dialled by the system if the Dial For Service option is selected. Used to connect to a remote computer for programming. Used in conjunction with User menu option 7 - Service Menu.

Note: If the Challenger is reporting in a direct line format, the reporting format must be disabled and the line lead temporarily connected to a dialler line for the service connection to be made.

CallBack. Enter the telephone number that will be dialled by the system when it detects a call-back trigger. Used to connect to a remote computer for programming. If a callback number is programmed, “No of Calls” and “No of Rings” must also be programmed. A callback number must not be programmed if you wish to dial into the panel for direct connection.

Computer. The telephone number of the Forcefield computer’s modem that will be dialled by the Challenger’s modem if the option “Computer is Via Dialler” is set to yes. For example, in the event of a Challenger Ethernet failure, the Challenger may dial into the Forcefield computer’s modem (the modem must be on the same node as used for the Ethernet connection).

Cct fields: These account numbers are only valid for dialler formats (the Securitel Hard ID is not programmed here). The number of digits required for the account number will vary depending on the communication format selected.

Rpt (Areas To Report Open/Close) selections. The function of this record will vary (as follows) depending on the setting of the Common Open Close option:

1. A report will be sent to the remote monitoring company whenever an area which is set here is armed or disarmed (provided 2 below is not functional). **Note:** If you do not want to report open/close, no areas should be programmed.
2. If Common Open Close is set, then a disarm report will be sent when the first disarm area occurs for any one of the areas set. No report will be sent when the remaining areas are disarmed. An arm report will be sent when all the areas set have been armed.

System. This is a unique number which identifies your system to the monitoring company when reporting in dialler formats and will be provided by that monitoring company.

Network. Type a network address is the Challenger identification number and identifies the client to the remote monitoring company. You must record a network address if the system is communicating to the monitoring station via a direct line. The Network address is the last digit or last 2 digits of the client number supplied by the remote monitoring company. Format 9-Tecom Direct Line requires only the last digit. **Note:** Set the Network address to zero if a direct line is not being used.

Computer. Type a computer address is the Challenger identification number and identifies the client to the access control/monitoring computer.

STU. Records a number between 0001 and 9999 which identifies the Securitel Interface Units.

Type. Select the required reporting format.

Test Call. This record determines whether The Challenger activates test calls to the monitoring company and if so, how often. The test call ensures that communications are operating correctly and can be programmed to only be made if there have been no events to initiate a call since the last test call. For “once a week” options, the test call will go through on the same day as the day on which the option was selected.

To specify a particular day for the “once a week” options, set the system clock to the day of the week on which you want the test call to occur, before selecting the option required (2 or 4). The system clock must then be reset to the correct time and date.

Hour. Enter the hour (24 hour format) that the test call will be made.

Minute. Enter the minute that the test call will be made.

Encryption. records a number between 0 and 255 which is used to encode data being sent to the remote monitoring company in the Direct Line format. The encryption key number will be provided by the monitoring company. (The same number must be entered for this unit at the monitoring station Direct Line receiver). Unless otherwise instructed by the monitoring company it is recommended to leave the encryption key at 0 until communication has been established.

Num Rings. Enter the number of rings that are required before a call is detected.

Note: For Challenger panels used in New Zealand and configured to answer incoming calls, the minimum amount of rings before answering an incoming call shall be set to 4.

Num Calls. Enter the number of calls that are required before the system answers or initiates a call back.

Buff Size. Enter the number of events (0 to 255) that the Challenger panel will hold in its communications buffer.

Multibreak Alarms. When checked and an individual input alarms more than once before being reset by a user, each alarm is reported to the remote monitoring company. This record controls the way in which multiple alarms from one input are reported to the remote monitoring company. **Note:** This record is not applicable if the reporting format type is High Speed Extended or High Speed Extended Checksummed.

Multibreak Restorals. When checked, and Multibreak Alarms is checked, and multiple alarms are reported to the monitoring station, this record causes a restoral message to be sent to the monitoring company each time the input is re-sealed.

600 Ohm Load. When checked enables 600 Ohm load termination.

Network Command. When checked and system communicates to the remote monitoring company via a direct line, this record enables that company to control certain functions in the system, such as arm/disarm the system, reset alarms, isolate inputs.

DTMF. When checked DTMF Tone dialling is enabled in all dialler formats. If not checked decadic dialling is enabled in all dialler formats.

Dial Computer Alarms (applicable to a system reporting alarm events to a management computer via dialler). When checked the system will dial an alarm event to the computer instantly when the alarm occurs, otherwise the system will wait until the communications buffer is full before dialling through the events to the computer.

Dial Events Via Port. When checked the system will communicate to an access control/monitoring computer via a dial-up modem connected to the Computer Interface module fitted to the Challenger.

CID via Satellite Phone. When checked enables delivery of CID alarm events to compatible receivers connected via a satellite communication path by extending the time that the panel waits for acknowledgement from the CID monitoring station. This option requires Challenger panel firmware 8.105 or above.

Disconnect Mgt SW on CID Event. When checked the system will disconnect from the management software computer when it needs to send an event to the CID monitoring station.

Common Open Close. When checked the panel reports open (disarmed) on the area circuit number of the first area disarmed from the Rpt selection and reports closed (armed) on the area circuit number that is armed last (all others armed) from the Rpt selection. If not set, reports open/close (disarmed/armed) on each area circuit number as specified in the Rpt selection.

Isolates Don't Trigger Dialler. When checked isolating inputs will not trigger the dialler to report. Isolates will be reported when the next alarm function triggers the dialler.

Enable Line Fault Monitor. When checked the Challenger panel will monitor the integrity of the dialler telephone line. If the line is cut it will be indicated immediately on the LCD RAS, and the Report Fail event flag will be activated to provide local indication and/or to enable a backup cellular phone interface. A Line Fail report will be generated for use with a backup cellular phone interface if used. If not set, Report Fail will only be generated after four failed dial attempts and no line fail message is generated for the backup cellular dialler. **Note:** Must always be set to NO in Version 7 Challenger panels.

Defeat Answering Machine. When checked enables Forcefield to dial into a Challenger that shares a line with an answering machine. If set, after the required "Number of Calls" and "Number of Rings" has been met, the Challenger will answer instantly on the next call.

Computer Via Dialler. When checked the Challenger panel can connect to the monitoring computer via a modem connection.

Dial Computer Accesses. When checked, and the Challenger panel is connected to the monitoring computer via modem, the system will dial an access event

to the computer instantly when the event occurs. If not checked the system will wait until the communications buffer is full before dialling through the events to the computer.

Dial Events Via Onboard Modem. When checked the Challenger panel communicates to an access control/monitoring computer running Forcefield or TITAN management software via the Challenger's on-board modem (the panel's normal dialler line connection). The line lead supplied with the panel is connected to a telephone socket as it would for a normal dialler reporting format.

Text Words

All standard text words in the Challenger standard text word library are identified by a reference number in the range 001 to 899. You can program up to 100 additional words numbered in the range 900 to 999.

Click the Number arrow to search for text words by number. Alternatively, click the Text arrow to search for text words by text.

Printer Options

This option records details of the printer output options. To obtain a printer output from the Challenger, a Serial Printer Interface or Serial Computer & Printer Interface must be fitted.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Real-Time Printing. When checked enables the printer port on the Challenger to print each event as it happens ("Print History" may still be used if required). Typically not set when a printer is not connected or you do not require the printer to run in real time.

Print Alarm Events. When checked enables all alarm events to be printed.

Print Access Control Events. When checked enables all access control events to be printed.

Dump Events Occurring Outside Timezone. When checked, and a timezone is specified, the printer will only be active outside of that timezone (when the timezone is not valid). If not checked, the printer will only be active during the specified timezone.

Printer Port Connected to DVMR. When checked the panel's printer port is connected to a DVMR and will send tag events to the DVMR.

TimeZone. The printer will only be active during the timezone specified unless Dump Events Occurring Outside Timezone is set. The default timezone is Tz 0 (always valid).

Type. Select the type of printer.

Event Flags

Event flags are signals activated within the Challenger to indicate that particular conditions exist in the system. The event number is the event flag which will activate a relay.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

WARNING: Removing an event flag that is in use may cause system malfunction.

Before attempting to remove any event flag record, you must make sure it is not used in any of the following databases:

- Area
- Input
- Input Shunts
- Panel Condition Events
- Panel Link
- RAS
- Relay
- Trigger Logic
- Event Number

Timezones

The number of hard time zones that can be programmed for a Challenger panel depends on the version of the Challenger panel. Challenger V8 panel firmware version 8.128 and later supports 46 time zones in the range 1 to 24 and 42 to 63. All other versions support only 24 time zones in the range 1 to 24. All versions also have two default timezones (0 and 25).

When the Challenger panel type is set to V8 Extended, the Extended Timezones button on Timezone programming window becomes active. Click the Extended Timezones button to program timezones in the range 42 to 63.

Doors & Lifts

This function is used to program information relating to an individual door or lift for a Challenger.

Figure 86: Door or lift programming window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter the door or lift number. Doors 17 to 64 are used for door or lift numbers, these are connected to an Intelligent Controller (four-door or 4-lift controller).

Id. Enter a name to identify the door to Forcefield. The name must be unique (it is not possible to have “Door 1” in Challenger x and “Door 1” in Challenger y).

Lift. Check the box to indicate a lift.

Description. Type a description of the door or lift.

Location. The location should contain details as to the type and location of the door or lift.

Video Cam. Selects the video camera associated with this input. This option is used when operator selects the video option on the graphics screen. When programming this option, the video camera is identified as being controlled by a DVR or by a switcher.

- Select DVR if the camera is controlled by a DVR. Refer to the *Forcefield External Interfaces Manual* for details.
- Select Switcher if the camera is controlled by a video switcher. In this instance, selecting the video option on the graphics screen will switch this camera to the selected view. The view for this camera can be selected in the View field.

View. Selects the preset view for the video camera. If this field left blank, the video camera, if a PTZ Camera, will switch to preset 1.

Member. The member controls event reporting and operator control in Forcefield.

Computer Cat. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each door or lift can have a different computer category. The category determines how Forcefield will handle an event from this door or lift. The computer category name “Door” can be used, but is a standard (read-only) Forcefield computer category and cannot be modified. See “Computer Categories” on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item.

The help programmed here will be displayed as an action on the alarm screen when alarm are generated.

Maps. Displays the map numbers of any maps containing the door or lift.

Programming. Click to open the Door/Lift menu, which provides access to the door/lift programming screens, sorted by functionality.

- If Lift selection was not set, then the Door/Lift Menu for a door displays (see Figure 87 below).
- If Lift selection was set, then the Door/Lift Menu for a lift displays (see Figure 88 below).

Figure 87: Door/Lift Menu for a door



Figure 88: Door/lift menu for a lift (note the Lift Details option)



Click an option in the Door/Lift menu to program the details described in the following sections:

- “Door/Lift Options” on page 281
- “Door/Lift Alarm Control” on page 282
- “Door Access” on page 282
- “Door/Lift Hardware” on page 284
- “Door/Lift Egress” on page 285
- “Door/Lift Controller” on page 285
- “Lift Options” on page 285

Door/Lift Options

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Card Format. Specifies the data format of the reader and card, key or token being used. Click the arrow, and then select the required card format.

LED. Specifies the status that the reader LEDs will indicate.

Override Timezone. This timezone controls the times when a door can be opened without the need to use a valid card or PIN. Free access is allowed when the timezone is valid.

Authorise RAS. Allows the selection of a RAS on the Challenger LAN. When a valid card is presented and access is granted to this door, then the LCD RAS selected here will have had the code entered automatically, allowing functions to be given to that user. Effectively, this will simulate a user entering their code on the nominated RAS.

Random Event Percentage. Enter a percentage value between 0 and 100%. For example, if the value is 20%, the door random bit event would be generated an average of once every five times a valid card/code is used at the reader (this function is not currently enabled in Challenger).

Time & Attendance Reader. This function is not currently enabled in Challenger.

Door Input Holds Door Unlocked. When checked the door lock will not operate to re-lock until the door is closed. This is used where the lock mechanism, when locked, will stop the door closing.

Inhibit Override Until User Enters. When checked prevents the door from unlocking when the override timezone becomes active until a valid card/code is presented at the reader.

Report Door Open & Close. When checked the system reports to printer and/or computer whenever the door is unsealed and re-sealed.

Report Forced Door. When checked the system reports to printer and/or computer whenever the door is forced.

Report DOTL. When checked the system reports to printer and/or computer whenever the door is in Door Open Too Long (DOTL) state.

Pulse Lock Unlock Relays. When checked the system pulses the lock unlock relay.

Disable Duress. When checked the system disables the duress PIN code from reporting a duress condition.

Hold Door Unlocked Until Door Open. When checked the door will not lock until the door is opened.

Report (Un)Secured. When checked the door will report secure and unsecure events.

Map (Un)Secured to (Un)Locked. When checked secure and unsecure events will report as locked and unlocked events.

2 Badge Unlock – 1 Badge Relock. As an alternative to dual custody, two badge unlock avoids unintended unlocking of a door if a user accidentally presents their card to a reader, for example, by brushing past the reader with the card in a pocket. When two badge unlock is enabled and two different cards are presented within the dual custody time (regardless whether dual custody is used), then the door is not unlocked and a door access denied message is generated.

Version 7 Options. Click to program Challenger Version 7 options.

Door/Lift Alarm Control

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Arm/Disarm Alarm Group. Assign an alarm group that specifies the alarm system control facilities relevant to the door.

Alarm Options. Choose from the method of alarm control required from the options.

Inhibit If Areas Secured (In). When checked access at the IN reader is to be denied when the area(s) assigned to the door in “Door/Lift Hardware” on page 284 are secure.

Inhibit If Areas Secured (Out). When checked access at the OUT reader is to be denied when the area(s) assigned to the door in “Door/Lift Hardware” on page 284 are secure.

Door Access

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Access. The amount of time that the door will unlock when a user enters a valid card or PIN on the door reader.

IUM Learn Reader. When checked identifies this reader as an IUM card data learn reader. This is a Forcefield-only option, it does not form part of the door access record. See “Learning IUM card data” on page 44.

Muster Reader. When checked identifies this reader to be a muster reader. This is a Forcefield-only option, it does not form part of the door access record. For more information, see “Muster Report” on page 158.

Extended Access. The amount of time that the door will unlock when a user with “LONG ACCESS” enters a valid card or PIN on the door reader.

Shunt Option. Determines the shunt options. Shunting is a procedure which stops an open door causing an alarm for a set period of time.

- Shunt Time.** The amount of time that the door can be opened before causing an alarm.
- Shunt Until Door Closed.** When checked keeps shunting the door until it closes.
- Extended Shunt.** The amount of time that the door can be opened before causing an alarm when a user with “LONG ACCESS” enters a valid card or PIN at the door reader.
- Cancel Shunt After Door Secures.** When checked cancels shunting after the door secures.
- Shunt Warning.** Determines the amount of time that a relay may be activated to sound a warning device before the “Shunt Time” or “Extended Shunt Time” expires.
- Low Sec TZ.** The low security timezone controls the times when just a valid card or PIN may be used to open the door. When the timezone is not valid and the “Card & PIN Code Reader” is Set, a valid card AND PIN must be entered to open the door.
- Card & Pin** (determines for IN and OUT readers what method will be used to open the door). When checked enables the door to be opened by presenting a valid card to the reader AND entering a PIN on the reader keypad. If not checked, enables the door to be opened by presenting a valid card to the reader OR entering a PIN on the reader keypad.
- Dual Custody** (determines for IN and OUT readers whether two user cards or PINs are required to open the door). When checked it is necessary to record two separate codes in succession in order to open the door (either two cards, two PINs, or a card and a PIN from two different users). If not checked, it is necessary to record only one card or PIN to open the door. Separate records are programmed for the IN and OUT readers of each door. If set,
- Disable PIN Only** (for IN and OUT readers). Determines what method will be used to open the door during the low security timezone. If set, enables the door to be opened during the low security timezone only by presenting a valid card to the reader. If not set, enables the door to be opened during the low security timezone by presenting a valid card to the reader or a valid code on the reader keypad. Timezone is programmed separately for the IN reader and OUT reader.
- Inhibit Offsite Users** (for IN and OUT readers). Deny access to any users designated as being in region 0.
- In check boxes:** When checked defines the reader as an in reader for a region. When a valid card or PIN is entered at the door in reader, the region that the user is entering is recorded against the user code. The system is then able to report an antipassback violation if the user attempts to use any reader that will allow them to enter the same region.
- Out check boxes:** When checked defines the reader as an out reader for a region. When a valid card or PIN is entered at the door out reader, user code is cleared from the region that the user is exiting.

Anti-PassBack Type. Controls the operation of the reader if a card or PIN is used to enter the same region that the user is currently in.

Anti-PassBack Time. The amount of time that must elapse before a card or PIN may be used at the same door twice in succession without causing a Timed Anti-Passback violation.

Computer Cat. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each door can have a different computer category. The category determines how Forcefield will handle an event from this area. The computer category name "Door Access" can be used, but is a standard (read-only) Forcefield computer category and cannot be modified. See "Computer Categories" on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item. The help programmed here will be displayed as an action on the alarm screen when alarm are generated.

Version 7 Options. Click to program Challenger Version 7 options.

Door/Lift Hardware

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Lock Relay. This record specifies the relay to be activated when the door is accessed. Enter a number in the range 1 to 16. These are the physical relays on the door/lift controller.

Forced Relay. This record specifies the relay to be activated to indicate Forced Door. Enter a number in the range 1 to 16. These are the physical relays on the door/lift controller.

DOTL Relay. This record specifies the relay to be activated to indicate DOTL. Enter a number in the range 1 to 16. These are the physical relays on the door/lift controller.

Fault Relay. This record specifies the relay to be activated to indicate a lock or reader fault. Enter a number in the range 1 to 16. These are the physical relays on the door/lift controller.

Warning Relay. This record specifies the relay to be activated to indicate Shunt Time ending. Enter a number in the range 1 to 16. These are the physical relays on the door/lift controller.

DOTL Input. The input used to report DOTL to the Challenger.

Door Input. The door contact input.

Egress Input. The input that will activate the egress function for the door.

Monitor 2nd Door Input. When checked enables the use of two inputs to monitor the door.

Assigned Areas selections. Specifies the areas assigned to this door that will control:

- the reader LEDs if “LED On when Area Armed” is selected.
- the “Access Denied if Area Armed” and “Egress Denied if Area Armed” functions.

It is recommended that only one area number be assigned to a door.

Note: This record does not specify areas for alarm control. Areas on which the reader can perform alarm control functions are specified in the alarm group assigned to the door.

Inputs Shunted By Door button. Click to program shunts.

Door Interlock Inputs button. Click to program interlocks.

Door/Lift Egress

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Egress TimeZone: This timezone control the times when an egress button (exit button) will unlock a door to allow exit. When the timezone is valid, a user can press the egress button and the door will unlock.

Egress Option: Select the correct option.

Egress Reporting. When checked a door egress report is sent to the printer and computer when the egress input is used.

Inhibited If Areas Secure (In). When checked the egress button will not unlock the door if any of the areas assigned to the door are armed.

Inhibited If Areas Secure (Out). When checked the egress button will not unlock the door if any of the areas assigned to the door are armed.

Door/Lift Controller

See Figure 84 on page 265, and the details that follow, about programming a Door or Lift Controller.

Lift Options

If Lift selection was set on the Door/Lift window (see Figure 86 on page 279), then the Door/Lift Menu for a lift displays an additional Lift Details option.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Override Group. Records a floor group number. Each floor group is programmed with floor/s and a timezone. The lift override group determines the floor/s

which can be freely accessed in the lift controls, and the times which they can be accessed, without using a valid card or PIN at the lift reader.

Security Group. Records a floor group number. Each floor group is programmed with floor/s and a timezone. The lift override group determines the floor/s which can be freely accessed in the lift controls, and the times which they can be accessed, provided that the security input (key switch) is turned on.

Security Input. Specifies the input on the Intelligent Controller that will control the security group (described above). Note: "Inputs Report as Floors" (below) must not be set if the Security Input is used.

Starting Floor to Activate a Relay. Records the first floor to be accessed by this lift. Forcefield uses this value to determine which floors can be remote controlled for this lift.

Last Floor to Activate a Relay. Records the last (top) floor to be accessed by this lift. Forcefield uses this value to determine which floors can be remote controlled for this lift.

First Relay to Use. Records the physical relay which will control access to the starting floor. Consecutive relays will match with consecutive floor, up to the last floor number. Only used on 4-lift versions.

First Input for Button Monitoring. The first physical input which will monitor floor selection. Used when "Inputs Report as Floors" (below) is selected. Only used on 4-lift versions.

Bank Number. used when the lift controller is connected to a high-level lift protocol controller.

Car Number. used when the lift controller is connected to a high-level lift protocol controller.

Total Floors. used when the lift controller is connected to a high-level lift protocol controller.

Inputs Report as Floors. When checked enables controller inputs to monitor the floors selected, up to a maximum of 16 floors. If set, the controller inputs can be used to monitor the floor selected, which will generate a report to the printer and computer. The Security Input field (above) cannot be used. If not set, inputs are used as normal system alarm inputs and the Security Input field (above) is enabled.

Monitor High Level Floor Landings. When checked indicates that the lift controller is connected to a high-level lift protocol controller.

Wait For Floor Selection. When checked enables one floor only operation. The floor is enabled after badge and floor selection. Normal operation is to enable all floors in users floor group.

Lift Computer Category. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each lift can have a different computer category. The category determines how Forcefield will handle an event from this lift. The computer category name “Lift” can be used, but is a standard (read-only) Forcefield computer category and cannot be modified. See “Computer Categories” on page 188 for details.

Lift Help Response. Double-click or press F3 to program alarm help information for this item. The help programmed here will be displayed as an action on the alarm screen when alarm are generated.

Landing Floors button. Used when the lift controller is connected to a high-level lift protocol controller. There are 64 possible floors, displayed 32 floors at a time. Use the PREV and NEXT buttons to display the first and second set of 32 floors.

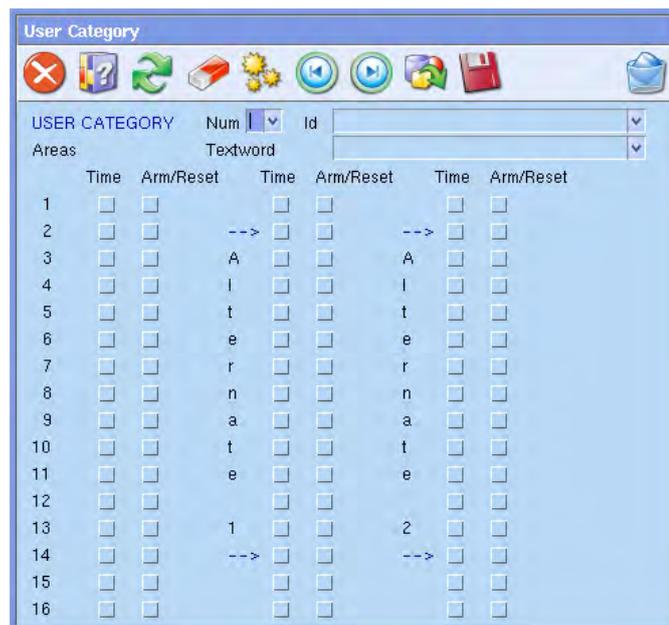
User Category Data

A user category may be used when a user needs to control some or all of the areas in their alarm group (and for alternative alarm groups, if applicable) in a manner different to that specified in the alarm group. For example, to:

- Use the timed access function on certain areas.
- Restrict alarm control to Arm/Reset only on certain areas.
- Use the User Count for each area or Dead Man Alarm functions.

The areas listed in this option must also be listed in the alarm group that the user category is assigned to in order for the function to be enabled on those areas.

Figure 89: User category programming window



Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. user categories may be numbered 1 to 8.

Id. Enter a name to identify the user category record to Forcefield.

Textword. Click the arrow to select a pre-defined text words from the Challenger word library (word numbers from 1 to 899) or the user-defined word library (word numbers from 900 to 999). Double-click the field to create a new user-defined word.

Time and Arm/Reset selections for each area: Timed disarm and/or arm/reset programming for areas 1 through 16 is accomplished via the Time selection and the Arm/Reset selection to the right of each area number. The areas used in this option must also be listed in the alarm group that the user category is assigned to in order for the function to be enabled on those areas.

Additional selection boxes are provided to program timed disarm and/or arm/reset functionality for two alternative alarm groups (if used). Alternative alarm groups are described in “Alarm Groups” on page 140.

Figure 90 below indicates the Time and Arm/Reset check boxes (circled) for area 1. The check boxes to the right are the Time and Arm/Reset check boxes for alternate 1, and the check boxes to the right of those are for alternate alarm group 2.

Figure 90: Area number with Time and Arm/Reset settings



Time selection. Programs the area for time disarm. When a user enters a code, it disarms the area and starts a timer. When the time elapses, the area re-arms.

Arm/Reset selection. Programs the area for arm/reset. When a user enters a code, it will arm the area or reset alarms.

Relays

This function is used to program an individual output for a Challenger.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Relay Num. Relays are numbered between 1 and 256.

Id. The relay ID (name) is used by Forcefield to identify the relay. The name must be unique (it is not possible to have “Lights” in Challenger x and “Lights” in Challenger y).

Event Flag fields: Select the event flag which will activate this relay. An event flag is a signal activated by an relay condition, area condition, system status or fault condition, door command (on doors 1 to 16) or shunt timer condition. The relay will follow the logic of the event flags unless the timezone (if programmed) is valid.

TimeZone. The timezone number recorded will control the times that a relay is active/inactive. If a timezone is programmed, it will set the relay when the time is valid. The status of the event flag is irrelevant when the timezone is valid. When the timezone is not valid, the relay follows the logic of the event flag. If no timezone is programmed the relay follows the logic of the event flag.

Inactive During TimeZone. When checked the relay will not activate when the timezone is valid regardless of the status of the event flag and provided the relay is not inverted. If the timezone is not valid, the relay follows the logic of the event flag.

Inverted. When checked the logic controlling the relay is reversed. If the previous logic determines that the relay is to be ON, this would change it to OFF.

Member. This field determines which operators are allowed to control the device and receive events.

Computer Cat. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each relay can have a different computer category. The category determines how Forcefield will handle an event from this relay. The computer category name "Relay" can be used, but is a standard (read-only) Forcefield computer category and cannot be modified. See "Computer Categories" on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item. The help programmed here will be displayed as an action on the alarm screen when alarm are generated.

Maps. Displays the map numbers of any maps containing the relay.

Auto Access – Secure

This function is used to program an individual arm/disarm timer for a Challenger.

An arm/disarm timer is used when you wish to ensure that areas are armed and/or disarmed at a particular time without the need to enter a user code. This function is used to relate a timezone and alarm groups to the arm/disarm functions. When this is done, the areas assigned to the alarm group will arm/disarm in accordance with the timezone designations:

- When the specific timezone expires the areas will arm.
- When the specific timezone becomes valid the areas will disarm.

Common window elements are described in Section 3. Elements specific to this window are described below.

Time Zone. Enter or select the timezone to be used for this arm/disarm program.

Alarm Group. Enter or select the alarm group to be used for this arm/disarm program.

Areas Assigned to Vaults

This function is used to define areas as part of a *vault*.

When a non-vault area is linked to a vault area, the non-vault area can be automatically armed following the arming the vault. When all of the vault's areas are armed, a timer starts. When the time expires, the linked non-vault area also arms.

Common window elements are described in Section 3. Elements specific to this window are described below.

Areas Assign To Vaults selections. Select the areas that are to be treated as vaults, and then click Save.

Floors

This function is used to record information relating to an individual floor. These are the floors that can be used in Floor Groups.

Common window elements are described in Section 3. Elements specific to this window are described below.

Num. Floors are numbered between 1 and 64.

Id. The Input ID (name) is used by Forcefield to identify the floor. The name must be unique (it is not possible to have "Floor 1" in Challenger x and "Floor 1" in Challenger y).

Description. Type a short description of the floor.

Member. The member controls event reporting and operator control in Forcefield.

Holidays

This function is used to program an individual user programmed holidays for a Challenger. Each Challenger may have up to 24 holidays.

Holidays programmed here will be available globally from the holiday database (see "Holidays" on page 166). See "Holiday-related tasks" on page 69 for additional details.

Input Shunts

This function is used to program details of a shunt timer which controls a shunt procedure. A shunt procedure inhibits an input from being activated when in an unsealed condition and for a set time period, e.g., a shunt stops a door generating an alarm when it is opened. Each shunt procedure is controlled by a shunt timer and each shunt timer must be individually programmed.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

- Num.** Records the number of the shunt timer. There are 16 shunt timers available. **Note:** Where a keypad is used to start the timer, the shunt timer number must be the same as the arming station number (1 to 16).
- Id.** The name used by Forcefield to identify the shunt. The name must be unique (it is not possible to have "Shunt 1" in Challenger x and "Shunt 1" in Challenger y).
- Desc.** Input shunt description.
- Shunted Input.** Records the number of the input which is to be shunted. An input cannot be assigned to more than one shunt timer.
- Shunt Time.** Records the amount of time that the input will be shunted.
- If the time expires and the input remains unsealed, an "input active" condition will be processed (for example, an alarm condition will occur, but the actual result depends on the input type). If the value entered is less than 128, the time is in seconds (1 to 127 seconds). To set the time in minutes, enter 128 plus the time required in minutes. For example, to program 30 minutes enter 158 (128 + 30 = 158). A value of 128 is invalid and cannot be used. For accurate timing of 1 or 2 minute periods, set the time in seconds (60 or 120 seconds).
- Relay.** The number of the relay which is connected to the shunt timer. The relay condition controls whether the input remains shunted or not. If the relay is active, the input is always shunted. When the relay de-activates, the shunt timer continues to run for the programmed "shunt time".
- Relay Id.** The name of the relay which is connected to the shunt timer. Allows the option of recording the number of the relay which is connected to the shunt timer.
- Shunt Event.** The number of the event flag which will be activated when the shunt timer is running.
- Shunt Event Id.** The name of the event flag which will be activated when the shunt timer is running.
- Warning Event.** Records the number of the event flag which will be activated when the shunt warning time is active.
- Warning Event Id.** Records the ID of the event flag which will be activated when the shunt warning time is active.

Warning Time. Records the amount of time before the shunt expires that the shunt warning event will be active. If the shunt time is in seconds, then the warning time is also in seconds. If the shunt time is in minutes, then the warning time is also in minutes.

Door Command Starts Shunt. When checked a keypad or shunt relay is required to start the shunt timer. If a keypad is used, the user must have a valid door group assigned. If not set, The condition of the input (sealed to unsealed) triggers the timer.

Cancel Door Event. When checked as soon as the input allocated to the shunt timer is active (unsealed) and then sealed, it cancels the door unlock event and cancels the shunt timer.

Entry/Exit Shunting. When checked a code is required to be entered to start the shunting or if it is not then it must be entered before the shunting expires or an alarm will be activated. **Note:** If this option is set, the Door Open Command must not be set.

Shunt In Access. When checked the door shunt procedure operates when one or more of the areas assigned to the shunted input, is in access.

Hold Door Event (used for doors with magnetic locks and drop bolts). When checked allows time for a door to be properly closed, there is a 2 second delay after the input seals and before it cancels the door event and shunt timer.

Report Open/Close. When checked will cause the input to report to the printer each time it changes from sealed to unsealed and visa versa. **Note:** If “Print Input When Unsealed” is set in the Input Database, for the input assigned to the Shunt timer, a Door Open message will be sent twice.

Shunt In Secure. When checked the door shunt procedure operates when all the areas assigned to the shunted input are secure.

Time Zones to Follow Relays

Timezones to follow relays are also known as soft timezones, and are numbered 26 through 41. These timezones are active only when a relay is active (timezones based on events instead of on time).

See “Assigning a soft timezone to a Challenger” on page 72 for details about soft timezones.

Note: ~DISABLED RELAY xxxx indicates that a relay previously entered here has since been deleted from the relay database.

Regions

Regions are used in antipassback programming and in muster reports.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Enter the region number. Each Challenger may have up to 255 regions.

Region 0 is considered to be “off site”.

Id. The region ID (name) is used by Forcefield to identify the region. The name must be unique (it is not possible to have “Reception” in Challenger x and “Reception” in Challenger y).

Description. Type a short description of the region.

User Allowed in Region for. Valid range is 15 to 65535 minutes (0 means there is no limit to how long a user may stay in the region). Forcefield uses this to track how long a user has been in a region. If a user stays in the region over this time an alarm is generated. Moving to a new region restarts the timer.

Cameras

Cameras recorded here are the frame cameras connected to the Challenger.

To program video cameras (CCTV) for a licensed Forcefield system, see “Cameras” on page 206 (Databases > CCTV > Video Cameras).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Cameras are numbered between 1 and 8.

Id. The camera ID (name) is used by Forcefield to identify the camera and must be unique (it is not possible to have “Camera 1” in Challenger x and “Camera 1” in Challenger y).

Location. Type a short description of the camera’s location.

Member. The member controls event reporting and operator control in Forcefield.

Computer Cat. Click the arrow to select from the list of computer categories (the list is restricted to show only the correct type of computer category).

Each camera can have a different computer category. The category determines how Forcefield will handle an event from this relay. The computer category name “Camera” can be used, but is a standard (read-only) Forcefield computer category and cannot be modified. See “Computer Categories” on page 188 for details.

Help. Double-click or press F3 to program alarm help information for this item.

The help programmed here will be displayed as an action on the alarm screen when alarm are generated.

Maps. Displays the map numbers of any maps containing the camera.

Custom RAS Display

Custom LCD display allows you to modify the text displayed on the LCD RASs connected to the panel. You will only see this text displayed on the RASs if there are no alarms, system or fault messages.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Display Text. You may enter up to 32 characters for this text.

Battery Test

Battery test records the details of the automatic battery test procedure and enables a manual battery test to be started. For the period of the battery test, the panel and/or DGPs and all auxiliary driven devices will be powered from the battery.

The start of the battery test for each of the devices to be tested is staggered, so that all devices don't switch to battery test at once.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Frequency. Records how often the automatic battery test will occur.

Start Time. Records the hour and minute that the battery test will start.

Run Time. Records the period, in minutes, that the automatic battery test will run for. If a battery test on any device fails, that device will immediately restore AC power.

Maintenance

Sets the date and RAS message to be displayed when the next service is due.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Date. Records the day, month, and year on which the next routine service call is due.

Text. Records a 32-character word of customised text which will be displayed on the LCD arming stations on the date specified as the maintenance date.

Security Password

Records the 10-digit security password required to access the Challenger via the upload/download software.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Password. The default password is 0000000000; it allows all computer connections.

Attempts. Enter the number of failed connection attempts allowed until the connection is locked out.

Macro Logic

This function is used to activate an event flag or an input under specific logic conditions. Up to four relays or event flags can be included in the logic equation. Each relay or event flag in the logic equation can be programmed as an AND or OR function and can also be programmed to invert the logic. Programming options are provided so that the event flag or input will pulse, time, on delay, off delay or latch when activated.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Num. Records the number of the macro logic program (there are 24 programs available).

Id. macro identification information for Forcefield.

Desc. macro description and associated information.

Type. Selects the function of the event flag or input when activated.

- Disabled—macro logic program disabled.
- Non Timed—follows the result of the logic equation only.
- On Pulse—activates for the programmed time or the active period of the logic result, whichever is the shortest.
- On Timed—activates for the programmed time regardless of the logic result.
- On Delay—activates after the programmed time period unless logic result is no longer active.
- Off Delay—follows the result of the logic equation, but remains active for the time programmed after the logic result is no longer active.
- Latched—activates on any of the first three inputs in the logic equation and is reset by the fourth input (AND / OR function not used).

Time. Records a time period which is used when any of the timed functions are selected. A value of 2 or greater should be used. When programming 1 to 4 minute periods, program in seconds (i.e. 60, 120, 180 or 240 seconds).

Activate or Deactivate. Select whether to activate or deactivate the selected event or input.

Event or Input field (not labelled). Select whether an event flag or an input is to be activated.

Output field (not labelled). Select the ID of the event flag or Input to be activated. The programmed event flag or Input will be activated when the result of the logic equation is active and any timing conditions are met.

Logic Equation fields: Program up to four logic inputs, which can be event flags or relays. The logic connecting the four inputs can be programmed for AND or OR functions. A NAND or NOR function can be achieved by inverting the logic of the particular input. Select "Inactive" to invert the logic of the input

When all conditions of the logic equation are met, the result is active and the output Event programmed in the previous step will be activated (depending on any timing function programmed).

Any unused inputs must be left as an OR function.

Panel Condition Events

These summary event flags can be assigned to system functions and system alarm/fault conditions. These event flags are activated when any of the conditions specified exist in the system. Default setting is "No event".

The system alarm/fault event flags will be latching if "Latch System Alarms" is set in system options (see "System Options" on page 270).

Note: Do not to assign event flag numbers which are pre-defined (event flags 1 to 16) or event flag numbers which have been assigned by the Installer in the input database, area database, RAS database, or shunt timers.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Mains Failure. This event flag is activated when a mains fail condition is detected on the Challenger or a DGP.

Low Battery. This event flag is activated when a low battery condition is detected on the Challenger or a DGP.

Fuse Failure. This event flag is activated when a fuse fail condition is detected on the Challenger or a DGP.

Tamper. This event flag is activated when a panel tamper condition is detected on the Challenger or a DGP.

Siren Failure. This event flag is activated when a siren fail condition is detected on the Challenger or a DGP.

DGP Isolated. This event flag is activated when a DGP has been isolated.

DGP Failure. This event flag is activated when a DGP which is programmed to be polled, is not replying to polling.

RAS Off-line. This event flag is activated when a RAS which is programmed to be polled, is not replying to polling.

Duress. This event flag is activated when a keyboard duress alarm occurs.

Film Out. This event flag is activated when the film count for a camera exceeds the programmed "Film Out" level.

Report Failure. This event flag is activated when the Challenger fails to report to the remote monitoring company.

Test Mode. This event flag is activated when the Challenger is in test mode.

All Secured. This event flag is activated when no areas are in access, there are no alarm conditions, and no entry/exit timers are running. See also Rpt "Areas to report Open/Close" on page 274.

Panel Link Failure. When a Challenger V9 panel is offline it activates the Panel Link (V9) Fail event flag.

Console Triggered. When the event flag specified here is activated, the console warning beepers are activated. The event flag also has to be assigned to the events that you want the console warning to sound on.

Floor Groups

See "Floor Groups" on page 143.

Door Groups

See "Door Groups" on page 142.

Radio Options

The radio service used in this option is no longer supported. Do not use.

Ethernet Configuration

This record programs an IP-connected Challenger panel's Ethernet communications. The appearance of the window depends on whether the communication mode is event-driven or polled.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Challenger IP. Enter the IP address of the Challenger panel's IP interface.

N/W IP. If applicable, enter the IP address that the external world sees as the Challenger's IP address, for example, in the case of the Challenger being behind a network address translation (NAT) firewall. This field is typically left blank, in which case the Challenger IP field is used.

Port. Displays the IP port programmed for the Challenger (see "Challenger programming" on page 217). This value must be entered into the Challenger via a RAS keypad to enable communications.

Host Bits. Enter a number from 2 to 24 to set the number of host bits (assigned by a Network Administrator).

Gateway IP. Enter the IP Address of the Gateway that the Challenger panel's IP interface communicates through.

Heartbeat Timeout fields. Enter the time and units that will be used for heartbeats. If no data packet is seen within the timeout period, the Challenger will go into dialler backup mode.

Note: For Forcefield 6.1 (or later), communicating with event-driven Challenger panels, enter a value of 10 or greater. The heartbeat interval is calculated in seconds (the units specified is ignored) minus 5 seconds, with a minimum result of 5 seconds. For example, enter a value of 30 to program a heartbeat timeout value of 25 seconds. At the calculated value, Forcefield will send a heartbeat probe to the Challenger to check whether it is still online.

Event ACK Timeout. Enter the time the Challenger should wait for an acknowledgement to be received. Do not use the value 0 as it will cause the Challenger to timeout on every command sent to it.

Station 1. Enter the IP address of the first contact ID station (SecureStream 1).

Station 2. Enter the IP address of the second contact ID station (SecureStream 2).

Station 3. Enter the IP address of the third contact ID station (SecureStream 3).

Encryption Key fields: The 16 encryption key fields are used to encrypt communications between the Challenger and Forcefield (or SecureStream).

Primary. Enter the IP address of the first management software site (Forcefield node).

Secondary. Enter the IP address of the second management software site (Forcefield node).

Suppress Failure Report. When checked stops “report fail” from appearing on the RAS after communication from CID site 1 is lost.

Enable TS0898 Telnet. When checked select to enable the Telnet protocol for TS0898 Challenger panels (requires Challenger firmware version 8.112 or later). This option does not apply to TS0099 Enhanced Challenger TCP/IP Interface.

Link Failure. Select the event flag that will be set if the Ethernet Link has failed and will be reset if the link is active.

Heartbeat Failure. Select the event flag that will be set if the Heartbeat has failed and will be reset if the Heartbeat is restored.

Contact ID Site Fail. Select the event flag that will be set if the CID station fails and will be reset if the CID station is restored.

Hardware Failure. Select the event flag that will be set if the Ethernet hardware has failed and will be reset if restored.

Panel Link (V9 only)

Panel Link programming arranges and connects a series of Challenger V9 panels (fitted with TS0890 Challenger Integration Units) into a complete system. The most obvious difference is the numbering system and the increase in the number of inputs and outputs.

Up to 16 panels (numbered 0 to 15) can be connected using Panel Link, with computer or printer interface connected to one or all of the panels.

Note: Do not confuse the panel link numbering system (0 to 15) with the Challenger number (1 to 1024).

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Common Area. One area per panel may be selected to arm when all the areas in the Linked Areas option are armed. Conversely, when any one of the areas in the Linked Areas option is accessed, then this area will access.

Poll selections. Select each applicable panel to make up the panel link system.

Pr fields: Enter a number from 00 to 15 to indicated the communications priority. Should a panel fail to communicate with the monitoring station, this option defines the order in which other reporting paths are tried. Priority 00 is the highest priority, priority 15 is the lowest priority.

Areas buttons: For each panel in the system, click the Areas button to open the Linked Areas window. Use the Linked Areas window to link the panel’s areas to the common area. When all these areas are armed, the common area will arm automatically, irrespective of any unsealed inputs in the common area.

Redirect Ptr. When checked sends all printer events to the master printer connected to the Challenger panel addressed as 0 (master panel). The printer

must be enabled for panel 0 and for any panels printing to panel 0. When not selected, the panel's local printer is used.

Via Port B. When checked indicates that a computer with management software is connected to the TS0892 fitted onto the TS0890 Integration Unit (this Challenger panel is connected directly to the computer). This Challenger panel cannot have a local printer.

Enable PL Sys. When checked activates the panel link settings programmed for the system.

Event Mapping button. Click to open the Panel Link Event Mapping window. See "Panel Link Event Mapping" below for details.

Relay Mapping button. Click to open the Panel Link Relay Mapping window. See "Panel Link Relay Mapping" below for details.

Panel Link Event Mapping

Event mapper enables this Challenger panel to use event flags from a linked Challenger panel.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

Panel Link Event Map. Enter an event mapper number in the range 1 to 16 for the event.

Remote Panel. Select the Challenger number associated with the required area.

State Type. Select the state the area must be in to trigger the local event flag (accessed, secured, in alarm, or panel link relay).

Remote Area. Select the area number in the range 1 to 16.

Local Event. Enter the local event flag that will be activated when the area is in the selected state.

Panel Link Relay Mapping

Panel link relays are used in panel link event mapping to activate events on other panels.

For example, you may need to activate event flag 101 on panel 1 (linked panel, which in this case is Challenger 2) when event flag 100 on panel 0 (master panel, which in this case is Challenger 1) is active. The following programming would be required:

- For Challenger 1 (panel 0), map a panel link relay number to event flag 100.
- In Challenger 2 (panel 1), program Challenger 1's panel link relay number to activate event flag 101, where the selected type is 4 (panel link relay).

Panel link relays are independent of physical Challenger relays. They are only used to pass events between Challenger panels, and cannot be used as physical relays in the way standard Challenger relays are.

Common window elements are described in Chapter 3. Elements specific to this window are described below.

For this Challenger panel, select a panel link relay number and associate it with an event flag. You can create up to 16 panel link relay maps.

Appendix B

Using offsite redundancy

Summary

Offsite redundancy (data mirroring) over TCP/IP replaces DiskShadow redundancy used in Forcefield 6.1. If upgrading from Forcefield 6.1 to 6.2 be aware that new licensing is required for this functionality.

Content

Overview 304
Setting up offsite redundancy 304
Recovering from failover 305

Overview

When using data mirroring, both the primary and mirror nodes (identical Forcefield hardware) are considered to be node 1. Unless running as the active mirror (having taken over from the primary node) the mirror node cannot be used as a normal Forcefield workstation; it can be used only to configure mirror functionality (Mirror Only mode) or for limited read-only functionality (Read Only Forcefield mode).

The primary and mirror nodes synchronise databases at start and monitor each other thereafter. If monitoring fails (and the mirror is configured to do so) the mirror will reconfigure itself as the active mirror, and then restart.

After takeover, all (IP-connected) peripheral devices that were managed by the primary node are managed by the active mirror. Recovery from takeover is achieved by manually creating a backup of the active mirror database and then restoring it to the primary.

Setting up offsite redundancy

Use the following steps to add a mirror node:

1. Set up a Forcefield server computer and licence it as the primary node (normal server setup process).
2. Set up a second Forcefield server computer and licence it for offsite redundancy (mirror node).
3. Record the IP address of the mirror node.
4. On the Forcefield primary controlling node or a client workstation, open the Network Configuration window, and then click the TCP/IP & Infleet button.
5. Enter the IP address of the mirror node in the last record (listed as node 8 for standard and node 20 for Enterprise).
6. Restart Forcefield on the primary controlling node.
7. On the primary controlling node, configure the primary site options. See “Mirror Setup window for the primary site” on page 246.
8. On the mirror node, configure the mirror site options. See “Mirror Setup window for the mirror site” on page 247. Set the startup action to “Wait For Primary”
9. Restart the mirror node, and then restart the primary node.

After the primary node starts, it will connect to the mirror node and synchronise the database.

Recovering from failover

To recover from a failover you need to:

- Correct the fault that caused the failover to occur.
- Backup the database from the active mirror to a computer on the network.
- Restore the database to the primary node.
- Reconfigure the mirror node from being the active mirror to being the backup mirror.
- Restart the primary and mirror nodes to activate synchronisation.

Use the following steps to recover from a failover:

1. Set up the recovered or replaced Forcefield server computer and licence it as the primary node. **Note:** Do not connect the Forcefield server computer to the network at this stage.
2. If the primary node's hardware was changed, use the Network Configuration option to change the primary Forcefield server's TCP/IP address from the default IP address to the actual IP address.
3. On the active mirror node, use the System Backup option to backup the databases to a previously-configured Samba (CIFS) location.
4. Check the Event Monitor to verify that the backup has completed.
5. If the primary node's hardware was changed, then the new license must also be installed on the active mirror node before it is reconfigured to be the backup mirror. On the active mirror node, use the Modify License option to relicense the mirror node.
6. On the active mirror node, use the Mirror Setup option to reconfigure the mirror node from being the active mirror to being the backup mirror.
Set Primary or Mirror Site to "Mirror"; set Monitor Primary Server to "Yes"; set Transfer Data to "Yes", set Transfer History to "Yes", set Startup Action to "Wait for Primary", and then save the record.
7. On the active mirror node, use the Activate Shutdown option to restart. The mirror node will restart and then wait indefinitely for the primary node to initiate synchronisation.
8. On the primary node, reconnect the Forcefield server computer to the network.
9. If necessary, on the primary node, create a Samba (CIFS) location to the computer where the database backup file resides.
10. On the primary node, use the System Restore option to restore the databases to node 1. Select the previously-configured Samba (CIFS) location. The node restarts when the database is restored.
11. After the restart you will be prompted for the license disk. Insert the CD or USB device, and then select Continue.

12. On the primary node, use the Mirror Setup option to configure the mirroring options as required (prior to failover).

13. On the primary node, use the Activate Shutdown option to restart the node.

Upon restart, the primary node should connect and synchronise with the mirror node, and both nodes should load Forcefield. All peripherals are now managed by the primary again.

Appendix C

Forcefield 6 menu reference

Summary

The Forcefield menu structure may be configured to display in the classic format or the Forcefield 6 format. See “Configuring login options” on page 229 for details.

This appendix lists the Forcefield menu options in the order of the Forcefield 6 menu structure. Headings represent menu folders, and each menu option is represented by a cross-references link to the topic in this manual.

Main menu

- See “Alarms” on page 77
- See “Display Map” on page 97
- See “Logoff” on page 77

Administration

Administrator Tools

- See “Activate Shutdown” on page 223
- See “Change Root Password” on page 223
- See “Configuration” on page 226
- See “Disable/Enable Workstation” on page 223
- See “Login Attempts” on page 224
- See “Network Configuration” on page 239
- See “QNX Shell” on page 250
- See “Mount Storage” on page 225
- See “Reset Operator Lockout” on page 226
- See “Set System Date/Time” on page 226

Database Tools

- See “Auto Database Backup” on page 86
- See “Convert 4.5.x Database” on page 91
- See “Delete Database Archive” on page 91
- See “System Backup” on page 89
- See “System Restore” on page 93

Data Mirroring

- See “Mirror Setup” on page 246
- See “Statistics” on page 249

Diagnostics

- See “aca Events” on page 250
- See “Event Simulator” on page 249
- See “QNX Shell” on page 250
- See “List NFS Exports” on page 214
- See “List NFS Storage” on page 180
- See “Printer Status” on page 213
- See “Serial Port Status” on page 214
- See “Status File Utility” on page 250
- See “System Information” on page 251

History

- See “Auto History Backup” on page 87
- See “Auto History Export” on page 88
- See “Backup History” on page 90
- Clear History, see “Clear history (manually)” on page 63
- See “Delete Database Archive” on page 91
- See “Export History” on page 92
- See “History Config” on page 121
- See “Purge History” on page 120
- See “Statistics” on page 121

Operators & Permissions

- See “Operator Menu Permissions” on page 164
- See “Operator Password” on page 165
- See “Operator Permissions” on page 163
- See “Operator Setup” on page 164
- See “Printer Permission” on page 167
- See “Workstation Permissions” on page 172

Time zones

- See “Device Locale” on page 166
- See “Holidays” on page 166
- See “Set Server Locale” on page 243
- See “Time Zones” on page 199

Control Devices

- See “Area” on page 109
- See “Challenger” on page 111
- See “DGP” on page 112
- See “Door” on page 110
- See “Door Lock Override” on page 111
- See “Floor” on page 113
- See “Input” on page 113
- See “Lift” on page 114
- See “RAS” on page 114
- See “Relay” on page 115

Control Intercom

- See “Intercom Calls” on page 115
- See “Intercom” on page 115

Control Video

- See “Display MultiView” on page 118

- See “Show DVR Tagged Footage” on page 125
- See “Show DVR Time Footage” on page 128
- See “Show DVR Video” on page 119
- Control Matrix Camera, see “Camera Control” on page 116
- See “Video Playback Control” on page 119

Forcefield Setup

- See “Alarm Responses” on page 187
- See “Computer Categories” on page 188
- See “Members” on page 192
- See “Member Groups” on page 193
- See “Workstations” on page 173

Communications

- See “Email Addresses” on page 166
- See “Serial & Parallel Ports” on page 169
- See “TCP/IP Hosts” on page 170
- See “TCP/IP Ports” on page 170

Graphics

- See “Convert DXF to Map” on page 96
- See “Edit Map” on page 99
- See “Import Bitmap File” on page 101
- See “Import LAP Icon” on page 102
- See “LAP Editor” on page 103
- See “Map Database” on page 105

Installer Tools

- See Change Dialup Password
- See “Change Site ID” on page 236
- See “Commission Node” on page 237
- See “Copy System to Node” on page 237
- See “Icon Editor” on page 237
- See “Modify License” on page 239
- See “Network Configuration” on page 239
- See “QNX Shell” on page 250
- See “Service System” on page 242

Management

- See “Program Clusters” on page 187
- See “Events” on page 194
- See “Guard Tour Program” on page 107
- Trigger Event Check, see “Event Check” on page 77
- Trigger Event Paging, see “Event Paging” on page 81
- Trigger Event Trigger, see “Event Trigger” on page 81

- Trigger Time Trigger, see “Time Trigger” on page 82

Preferences

- See “Login Message” on page 224
- See “Speed Bar Configuration” on page 243
- See “Windows Manager Options” on page 244

Storage & Devices

- See “All Storages” on page 179
- See “Disk Storage” on page 179
- See “List NFS Storage” on page 180
- See “NFS Exports” on page 180
- See “NFS Storage” on page 181
- See “Samba (CIFS)” on page 181
- See “Node” on page 167
- See “Printers” on page 168
- See “UPS” on page 171

Operator Tools

- See “Add Event” on page 120
- See “Door Monitor” on page 211
- See “Guard Tour Control” on page 106
- See “Page Message” on page 225
- See “Send Operator Message” on page 226
- See “Trace Monitor” on page 210

Program Devices

Challenger

- See “Challenger ID Alteration” on page 216
- See “Challenger programming” on page 217
- See “Copy Challenger” on page 220
- See “IUM Card Categories” on page 220
- See “Upload All Challenger Data” on page 220

Challenger > Download

- See “Delete Download Buffer” on page 221
- See “Download All” on page 221
- See “Download Challenger Users” on page 222
- See “Download Changes” on page 222
- See “Download User” on page 222

Duress

- See “Duress Locators” on page 182

- See “Duress Stations” on page 182
- See “Duress Transmitters” on page 183

Intercom

- See “Intercom Master” on page 184
- See “Intercom Slave” on page 185

Third Party

- See “Devices” on page 195
- See “Device Types” on page 196
- See “System” on page 197
- See “System Sub Types” on page 198
- See “System Types” on page 198

Video

- See “DVRs” on page 201
- See “DVR Cameras” on page 202
- See “DVR Presets” on page 202
- See “Multiview” on page 203

Video > Matrix Switch Video

- See “Cameras” on page 206
- See “Monitors” on page 206
- See “Monitor Groups” on page 207
- See “Presets” on page 207
- See “Switchers” on page 208

Reports

Access Control Reports

- See “Alarm Group Report” on page 145
- See “Door Group Report” on page 145
- See “Floor Group Report” on page 145
- See “Users By Alarm Group” on page 145
- See “Users By Door Group” on page 145
- See “Users By Floor Group” on page 145
- See “Door Open Close Times” on page 212
- See “Door Override Report” on page 213

CCTV Reports

- DVR Camera Report, see “Camera Report” on page 205
- See “DVR Report” on page 206
- DVR Preset Report, see “Preset Report” on page 206
- CCTV Camera Report, see “Camera Report” on page 209

- CCTV Monitor Report, see “Monitor Report” on page 209
- CCTV Preset Report, see “Preset Report” on page 209
- CCTV Switcher Report, see “Switcher Report” on page 209

Challenger Reports

- Challenger Report, Detail, see “Challenger Detail Report” on page 220
- Challenger Report, Enabled, see “Challenger Enabled Report” on page 221
- Challenger Report, Summary, see “Challenger Summary Report” on page 221
- Challenger Report, User, see “Challenger User Report” on page 221

Challenger Status Reports

- See “Abnormal Status Report” on page 210
- See “Challenger Item Status” on page 211
- See “Individual Item Status” on page 211
- See “Items in State Report” on page 211

Duress System Reports

- See “Locator Report” on page 183
- See “Station Report” on page 184
- See “Transmitter Report” on page 184

History Reports

- See “Door/Lift Activity” on page 122
- See “Door/Lift User Activity” on page 122
- See “Event Report” on page 123
- See “History Report” on page 123
- See “Incident Report” on page 124
- See “Offline History” on page 124

Intercom System Reports

- See “Master Report” on page 186
- See “Slave Report” on page 186

Management Software Reports

- See “Cluster Report” on page 188
- See “Cluster Usage Report” on page 188
- See “Computer Category Report” on page 191
- See “Computer Category Usage” on page 192
- See “Member Report” on page 193
- See “Member Group Report” on page 193
- See “Member Usage” on page 194
- See “Member Group Usage” on page 194
- See “Time Zone Report” on page 199
- See “Timezone Usage” on page 199
- See “Check Log Report” on page 216

- See “Debug File Report” on page 216
- See “Event Group Report” on page 195

Other Reports

- See “Equipment Report” on page 178
- See “Guard Tour Report” on page 109
- See “LAP Report” on page 105
- See “Operator Report” on page 165

Trigger Reports

- See “Event Check Report” on page 84
- See “Event Paging Report” on page 85
- See “Event Trigger Report” on page 85
- See “Time Trigger Report” on page 85

User Profile Reports

- See “Matching Profile” on page 151
- See “Profile Access Report” on page 151
- See “Profile Report” on page 152

User Reports

- See “Activation Report” on page 152
- See “Area Control Report” on page 153
- See “Card (User) Report” on page 153
- See “Door Access Report” on page 154
- See “Expired Profile” on page 155
- See “Expiry Report” on page 155
- See “Floor Access Report” on page 156
- See “Idle User Report” on page 156
- See “Last Access By A User” on page 157
- See “Muster Report” on page 158
- See “Unused Data Report” on page 158
- See “User Access Report” on page 159
- See “User On-Site Report” on page 159
- See “Users By Region Report” on page 160

Users

- See “Download User” on page 130
- See “Program Profile” on page 147
- User Maintenance, see “Maintenance” on page 131

Access Groups

- See “Alarm Groups” on page 140
- See “Door Groups” on page 142
- See “Floor Groups” on page 143

Card Administration

- See “Design Card Layout” on page 129
- See “Select Learn Reader” on page 130

Card Administration > Smart Card Programmer

- See “Display User Card” on page 160
- See “Issue User Card” on page 161
- See “Reader Config Card” on page 161
- See “Setup Programmer” on page 161

Profile Administration

- See “Assign Profile to Users” on page 146
- See “Modify Profile Access” on page 144
- See “Sync Profile Data” on page 151

User Administration

- See “Delete Unused Data” on page 130
- See “Generate IUM Data” on page 144
- See “Maintenance Config” on page 139
- See “Show System User Number” on page 162
- See “Show PIN Code” on page 140
- See “Show Ch. User Number” on page 162
- See “Export User Data” on page 161
- See “Import User Data” on page 162

User Status

- See “Change Status of User” on page 146
- See “Set users offsite” on page 146

Glossary

abnormal status	A security device or point that is not in its normal operating state, for example, area access, input isolated.
Access	The condition of an area or building when it is occupied and when the security system has been set so that normal activity does not trigger an alarm.
Acknowledged Alarm	See Alarm Types
Active status	The status of a card which is currently in use by a user within the security system.
Alarm	The state when an armed input device is activated, for example, an input is unsealed.
Alarm bar	The top line of the main menu window which flashes when an alarm is reported, displays the alarm icon, and alarm priorities.
Alarm Group	A Challenger feature which defines a group of Areas, functions and menu options. An Alarm Group can be assigned to certain users and input types for area control.
Alarm Response Codes	Pre-programmed common responses to alarms. When responding to alarms these codes can be quickly entered using their ID number.
Alarm window	A Forcefield window which displays Alarms reported by the security system. From this window an Alarm is dealt with until the situation causing the alarm is removed.
Alarm types	There are two types of Alarms; unacknowledged or acknowledged. In the alarm window an alarm which has had no action taken is an unacknowledged alarm. Once a acknowledgement has been made it becomes an acknowledged alarm and is moved to the follow-up alarm window.
Area	A physical space being controlled and monitored by Challenger. An Area includes everything which is physically located within its boundaries, including users, security devices, doors, floors etc. Forcefield can handle up to 5120 Challenger panels, each controlling 16 Areas.
Armed	The state of a device/area when a change in its condition (from sealed to unsealed) will cause an alarm.
Arming Station	Also called "RAS". Any device connected to the Challenger LAN that is capable of controlling the security system functions such as arm/disarm, open doors, etc.
Backup	The copying of system databases to removable storage devices for safekeeping.

Badge (a card)	The act of presenting a card to a specifically designed reader to gain access to an Area.
Card	A token carried by the user. Usually in the form of a plastic card, but it can also be a key, a proximity card, a magnetic swipe card or key tag. Used to grant access where applicable. A card uniquely identifies a user.
Card Number	Identification number of a card.
Card Only	A user with this card status can only badge a card to gain access and cannot use a PIN code.
Challenger	The Challenger control panel is the basis of the alarm and access control equipment installed at the sites. The Challenger is the main panel that controls remote arming stations, data gathering panels, and relays etc.
CIFS	Common Internet File System
Client	See Forcefield client
Cluster	A Cluster is a grouping of the same type of items (inputs, areas, doors, relays, RASs, DGPs or buildings) that enables many operator functions to be performed more quickly and conveniently. Clusters can be utilised to simplify the simultaneous control of a large number of devices.
Computer Access	An operator of the Forcefield computer system can have access to all or some of the features of Forcefield. The restriction of access to these features is referred to as Computer Access.
CSV	Comma Separated Value data format, typically used to export data to an external spreadsheet or database application. Such applications may require the CSV data to be either raw or formatted: CSV raw data is exported 'as is', with dates not in human-readable format. CSV formatted data is exported with dates converted to human-readable format.
Database	Forcefield databases contain all the information Forcefield and Challenger need in order to maintain control and access functions. Information about users and operators, system equipment, Times and locations are all stored in databases.
De-isolate	A device that has been isolated from the system can be de-isolated, therefore making it part of the security system again.
Device	PIRs, alarms, readers, cameras etc.
DGP	Data Gathering Panels. Devices connected to the Challenger which collect data from other security devices. DGPs expand the number of inputs/relays in a Challenger system and can be installed remote from the Challenger panel.
Disable	To prevent a programmed function being carried out.
Disarm	Changing the status of an Area from armed to disarmed to allow the area to be occupied.
Door Group	A grouping of doors for a common access level, identification and ease of programming. This is a Challenger feature.
DOTL	Door open too long.

Dual Custody	<p>When the Challenger system option dual custody is enabled, two users must enter their codes before access is granted to user programming.</p> <p>When an Intelligent Access Controller is used, dual custody also refers to whether two user cards or PINs are required to gain access to a door or lift. Two users must present their card or PIN to open a door (for example, when a user is identified as a visitor and must be accompanied). In Forcefield, this functionality refers to a card type of Dual.</p>
Download	The transferring of data from Forcefield to Challenger panels.
Duress (keyboard)	A situation where a user is being forced to breach the security system, for example, forced at gunpoint to open a door. The duress facility is reported. This is activated by entering a pre-programmed duress digit in conjunction with a PIN.
Duress system	<p>The Ascom Nira Duress system is comprised of a duress station (connected to Forcefield), duress system locators (static locations within a facility), and a duress transceiver (worn by a personnel such as a guard).</p> <p>If the guard's duress transceiver generates an alarm, the system informs the operator of the guard's location and direction of travel.</p> <p>In addition, the system may be used to page (produce beeps or a siren) when an event occurs.</p>
DVR	Digital Video Recorder or Digital Video Multiplexer Recorder
Dynamic Graphic Display	Any node in the system can display a map of a site with graphical representations of the physical contents of the site or area. These maps display the current status and location of doors, detection and control points and permit actioning and controlling points.
Enable	When programming functions, the Enable action will allow that function to be performed until programmed otherwise.
Event	Each action that occurs in the Forcefield system is recorded as History and each individual occurrence is called an Event.
Event Printer	A printer with this setting will print events in real time. Reports can also be sent to this printer, but only if the printer is set up as a report printer. If so, events will stop being printed to allow for the report. Event printing will resume when the report has finished.
Event window	Displays everything that happens in the security system (subject to the operator's permissions). Each event is dated, timed, and IDs are included where applicable, as is other relevant information.
Expired Status	The status of a card which is outside the dates set for its active use. An expired card will be denied access.
Floor Group	A grouping of floors for identification and ease of programming. This is a Challenger Feature.
Follow-up Alarm	See Alarm Types

Forcefield	Forcefield is multi-operator, multi-tasking, network-enabled software for controlling Challenger panels and high-level interfaces such as CCTV switchers, intercom systems, and more.
Forcefield client	Windows computer that provides operator access to the Forcefield server, connected via LAN/WAN or dial-up.
Forcefield server	QNX computer running Forcefield.
Guard Tour	A Guard Tour is a defined series of checkpoints at which a security guard must check in, within specified time intervals. Failure to check in on time triggers an alarm or other event.
History	The system collects and stores Events as History. Every action performed by an operator and every event received from, or sent to, the field equipment is considered to be an Event.
ID	Identity. Same as Id.
Inactive status	A card which is no longer being used.
Incident	A series of events (starting with an alarm event) belonging to a member. Incidents may be created automatically or manually.
Input	An electrical signal sent from a security device to the Challenger system. These include PIR Detector, Door/Window contact, Smoke detector, Egress button, Key switch, etc.
IP Challenger	A Challenger panel fitted with an IP interface module such as a TS0898 Ethernet Interface or a TS0099 Enhanced Challenger TCP/IP Interface.
Isolate	A device which is Isolated is inhibited from indicating its status to the system and is effectively excluded from functioning as part of the system. Inputs, RASs and DGPs are devices which can be isolated.
IUM	Intelligent User Memory—expanded memory in Challenger equipment
Jump zone	The jump zone is a defined area on a map that, when selected, jumps to another map. The jump zone can be used to zoom from a general map to a more detailed map, or to provide a junction point to display the next section of a large map.
LAN	Local Area Network. The hardware connection linking nodes together for the purpose of sharing data.
LAP	Live Animation Point on a map indicates the position and status of a device under control of Forcefield.
Login	Enter a login name and password at the login window to gain access to the Forcefield system.
Logoff	Allows an operator to exit the Forcefield system but not shut it down. Allows another operator to login to a work station.
Long Access	Allows for a door to be opened for a longer period of time without an alarm being generated. Can be used for physically challenged users.
Lost status	The status of an access card which has been lost. This status will generate an alarm if the card is used.
MAC	Media Access Control

Mag card	Magnetic stripe card
Member	Members are used to define which operators, operator terminals and printers have access to different Items and events in the system. Members are then combined to form member groups.
Member Group	A member group contains a list of members. An operator, terminal or printer is assigned to a member group to restrict their access to items and events relevant to their location and/or level of authority. member groups are also utilized to generate reports.
Node	A computer that is running Forcefield.
NFS	Network File System
NIC	Network Interface Card
NTP	Network Time Protocol
Operator	A person who has a login name and password for access to Forcefield.
PIN	Personal Identification Number used to identify the user to the field equipment system and grant access where applicable. The PIN can be a 4 to 10 digit number.
Point	A device under control of Forcefield including doors, RASs, cameras, nodes, printers, etc.
PPP	Point-to-Point Protocol
Priority	Priorities are set for managing the system events. The preferred order in which the system will display events and the importance of the event will determine its priority.
Privileged	This card function disables the antipassback features on a card. This is usually applicable to users who are senior in an organisation's structure. It also over-rides the disabled reader status.
Profile	See User Profile
Prox card	Proximity card (Tecom 27-bit or Wiegand 26-bit). May be used for Forcefield operator login.
PTZ camera	Pan-Tilt-Zoom camera
QNX	The Forcefield server's operating system.
RAS	Remote Arming Station. See Arming Station.
Region	Regions can consist of doors, readers and remote arming stations. Separate from Challenger-defined areas, a region requires a user to badge their card to both enter and exit a site.
Relay	An output device connected to a Challenger system that is used to control a physical device. For example: sirens, strobes, piezo screamers, door locks, indicator lamps, cameras, etc. Challenger Relays can also be used to interface with lighting, heating, and air-conditioning systems for integrated building management.
Remote Control	Control of a security device using Forcefield rather than using a Remote Arming Station.
Report Printer	A printer with this setting will be able to print reports.

Samba	Open source software providing file and print services across various operating systems.
Sealed	An input device that is NOT activated, for example, door closed.
Sector	The use of Forcefield sectors enable multiple inputs to be associated via the sector number in the inputs' computer category. This lets the inputs generate a sector alarm (also known as perimeter alarm) and for multiple inputs to increase or decrease the alarm priority of the sector alarm, depending on the inputs' alarm and restoral states. Sectors are also used linking of Forcefield events to external events such as a Teleste alarm codes.
Secure	The condition of an area or building when it is armed and unoccupied. The security is turned on.
Secured mode	Use of a special 4-byte password for smart card readers to ensure that a reader cannot be reprogrammed by a configuration card from a different system.
Server	See Forcefield server
Shunt time	The timed inhibiting of an input from being activated when it is in an unsealed condition. for example, a shunt stops a door generating an alarm when opened for a short time.
Shut down	Shut down turns off the Forcefield system safely without losing any information. Not the same as logging off.
Tamper	A situation where a device or associated wiring is tampered with or accidentally damaged. The tamper facility activates an alarm.
Timezone	Refers to Forcefield or Challenger concepts of 'hard' timezones (triggered by defined times and dates) and 'soft' timezones (triggered by events). In Forcefield, timezones are used to give time frames of operation for operators to access the system. In Challenger panel, timezones are used to give time frames of operation to functions and users. There is also a location timezone, used to give Forcefield and Challenger their physical time zone location in relation to GMT. This allows all events to be logged chronologically, irrespective of the time zone of the individual Challenger or Forcefield node.
Trace	A card, with this option set, presented at a reader will attach the word trace to that user in the event log. This allows for that user's movements to be traced, and can be programmed to generate an alarm.
TSV	Tab Separated Value
Unacknowledged Alarm	See Alarm Types
Unlock Door	When a door is in the locked state the Unlock Door command will unlock it.
Unsecured mode	A smart card reader only sees blank (un-programmed) cards with a unique serial number and user-defined cards (the 4-byte security password is not used).
Unsealed	The state of an input device when it is activated. For example: a PIR has detected movement.
Upload	The transferring of data from Challenger panels to Forcefield.

User	A user is a person that holds a Card and/or a Personal Identification Number (PIN) that controls the security system functions (access, secure, etc.) and door functions in a Challenger system. Not to be confused with an operator, who uses Forcefield operator terminals.
User Number	The unique identification number of a user.
User Profile	A collection of user information such as member, date range, position, department, card type, trace, long access, card only, privileged options, and Challenger access.
Valid date	A set of dates between which a user can legally access the security system using a card.
Visitor Status	A visitor can only unlock a door when escorted by a user with Guard authority.
Void status	A user who is programmed in the system but has had their authority denied of any access.
WAN	Wide area network
Watch house mode	<p>A special mode of operation designed for watch houses. All Forcefield nodes to be used in watch house mode must be fitted with monitor, keyboard, and mouse.</p> <p>A Forcefield node is designated as a night switch workstation and other Forcefield nodes are designated as watch house pods. Any Forcefield node not designated as either a pod or a night switch workstation operates in standard mode.</p> <p>Watch house mode enables the night switch workstation to automatically take control of a pod's members when the pod's operator logs off. Conversely, when an operator logs onto a pod, the members are automatically transferred back to the pod.</p>
Workstation	A computer providing access to the Forcefield user interface.

Index

A

- Abnormal Status Report option, 210
- About box, 17
- aca Events option, 250
- Access
 - Alarm Group Report, 145
 - Alarm Groups, 140
 - Door Group Report, 145
 - Door Groups, 142
 - Floor Group Report, 145
 - Floor Groups, 143
 - Modify Profile Access, 144
 - Users By Door Group, 145
 - Users By Floor Group, 145
- access test time, 269
- Activate Shutdown option, 223
- Activation Report option, 152
- activity icon, 10, 17, 18
- Add Event option, 120
- Admin
 - Activate Shutdown, 223
 - Add Event, 120
 - Change Root Password, 223
 - Disable/Enable Workstation, 223
 - Login Message, 224
 - Page Message, 225
 - QNX Shell, 225
 - Reset Operator Lockout, 226
 - Send Operator Message, 226
 - Set System Date/Time, 226
- alarm
 - action text, 58
 - detail, 33
 - follow-up, 35
 - handling, 29
 - highest priority, 61
 - line, 35
 - map, 35
 - screen, 31
 - screen override, 59
 - types, icons for, 33
- Alarm Group Report option, 145
- Alarm Groups option, 140
- Alarm Panel Status
 - Abnormal Status Report, 210

- Challenger Item Status, 211
- Individual Item Status, 211
- Items in State Report, 211
- Alarm Responses option, 187
- alarm response
 - delay, 232
 - order, 232
- Alarms option, 77
- All Storages option, 179
- allow Forcefield shutdown, 177
- applied patches, 215
- Area Control Report option, 153
- Area option, 109
- arming stations, 260
- ASCOM, 182, 183, 184
- Assign Profile to Users option, 146
- Auto Database Backup option, 86
- Auto History Backup & Purge option, 87
- Auto History Export option, 88
- auto popup
 - PTZ control, 175
 - video player control, 176
- auto-allocate user numbers, 48
- AutoCAD, 96
- automatic shutdown, 24

B

- Background Editor option, 96
- backup
 - database, 86
 - Forcefield data, 89
 - history, 87, 90
- Backup Data option, 89
- Backup History option, 90
- backup storage location, 234
- Backups
 - Auto Database Backup, 86
 - Auto History Backup & Purge, 87
 - Auto History Export, 88
 - Backup Data, 89
 - Backup History, 90
 - Convert 4.5.x Database, 91
 - Delete Database Archive, 91
 - Delete History Archive, 92
 - Export History, 92
 - Export History Archive, 92

- Format Disk, 93
- Purge History, 93
- Restore System, 93
- BMP format, 101
- boot agent, 22
- bulk
 - create users, 46
 - delete users, 48
 - modify users, 47
- C**
- Camera control option, 116
- Camera Control option, 116
- Camera Report option, 209
- Cameras option, 206
- Card (User) Report option, 153
- card and PIN always, 262
- card and PIN time, 270
- card learn, 174
- CCTV
 - Camera Report, 209
 - Monitor Report, 209
 - Preset Report, 209
 - Switcher Report, 209
- Challenger
 - areas, 259
 - areas assigned to vaults, 290
 - arming stations, 260
 - auto access – secure, 289
 - auto reset, 273
 - battery test, 294
 - cameras, 293
 - communication options, 273
 - copy, 63, 220
 - custom RAS display, 294
 - Delete Download Buffer, 221
 - detail report, 220
 - DGPs, 263
 - door groups, 142
 - Door/Lift Access, 282
 - Door/Lift Alarm Control, 282
 - Door/Lift Egress, 285
 - Door/Lift Hardware, 284
 - Door/Lift Options, 281
 - doors & lifts, 279
 - Download All, 221
 - Download Challenger Users, 222
 - Download Changes, 222
 - Download User, 222
 - enabled report, 221
 - Ethernet configuration, 298
 - event flags, 278
 - floor groups, 143
 - floors, 290
 - holidays, 290
 - input shunts, 291
 - inputs, 256
 - IUM Card Categories, 220
 - Lift Options, 285
 - macro logic, 295
 - maintenance, 294
 - panel condition events, 296
 - Panel Link, 299
 - Panel Link Event Mapping, 300
 - Panel Link Relay Mapping, 300
 - printer options, 277
 - programming, 217
 - radio options, 297
 - regions, 293
 - relays, 288
 - security password, 295
 - summary report, 221
 - system options, 270
 - text words, 277
 - timers, 269
 - timezones, 278
 - timezones to follow relays, 292
 - upload, 66, 220
 - Upload All Challenger Data, 220
 - user category data, 287
 - user report, 221
- Challenger Detail Report option, 220
- Challenger Enabled Report option, 221
- Challenger ID Alteration option, 216
- Challenger Item Status option, 211
- Challenger option, 111
- Challenger Programming option, 217
- Challenger Summary Report option, 221
- Challenger User Report option, 221
- Change Dialup Password option, 237
- Change Root Password option, 223
- Change Site ID option, 236, 310
- Change Status of User option, 146
- Check Log Report option, 216
- CIFS, 181
- CIFS storage, 234
- clear history, 63
- Clear History option, 63
- Cluster Report option, 188
- Cluster Usage Report option, 188
- Commend intercom, 185
- Commission Node option, 237
- communication analyser, 250
- computer access, 173
- Computer Categories option, 188
- Computer Category Report option, 191
- Computer Category Usage Report option, 192
- Computer Equipment
 - Equipment Report, 178
 - Node, 167
 - Printer Permission, 167
 - Printers, 168
 - Serial & Parallel Ports, 169
 - TCP/IP Hosts, 170
 - TCP/IP Ports, 170
 - UPS, 171
 - Workstation Permissions, 172

- Workstations, 173
 - Computer Status option, 214
 - Configuration
 - Change Dialup Password, 237
 - Change Site ID, 236, 310
 - Commission Node, 237
 - Configuration, 226
 - Copy System to Node, 237
 - Icon Editor, 237
 - Modify License, 239
 - Network Configuration, 239
 - Phindows, 244
 - Service System, 242
 - Set Server Locale, 243
 - speed bar, 243
 - Windows Manager Options, 244
 - Configuration option, 226
 - configuring
 - CCTV/intercom options, 229
 - Challenger poll rate options, 235
 - login options, 229
 - network, 239
 - network details, 241
 - remote workstation options, 235, 236
 - report options, 230
 - TCP/IP addresses, 240
 - user options, 232
 - control
 - intercom, 115
 - intercom calls, 115
 - MultiView, 118
 - Control
 - Area, 109
 - Camera, 116
 - Challenger, 111
 - DGP, 112
 - Door, 110
 - Door Lock Override, 111
 - Floor, 113
 - Input, 113
 - Lift, 114
 - RAS, 114
 - Relay, 115
 - Show DVR Video, 119
 - Convert 4.5.x Database option, 91
 - Convert DXF to Map option, 96
 - copy Challenger, 63, 220
 - Copy Challenger option, 220
 - Copy System to Node option, 237
- D**
- data mirroring, 246, 303
 - database
 - restore, 93
 - Databases
 - Device Locale, 166
 - Email Addresses, 166
 - Holidays, 166
 - daylight saving, 243
 - Debug File Report option, 216
 - default printer, 174
 - default values
 - local, 178
 - workstation, 178
 - delete
 - database archive, 91
 - download buffer, 221
 - history archive, 92
 - unused data, 130
 - Delete Database Archive option, 91
 - Delete Download Buffer option, 221
 - Delete History Archive option, 92
 - Delete Unused Data, 148
 - Delete Unused Data option, 130
 - Deleting analogue cameras, 202
 - departments
 - unused, 130
 - Design Card Layout option, 129
 - device ID names, 67
 - Device Locale option, 166
 - Device Types option, 196
 - Devices option, 195
 - DGP option, 112
 - Disable/Enable Workstation option, 223
 - Disk Storage option, 179
 - Display Map option, 97
 - Display MultiView option, 118
 - Display User Card option, 160
 - Door Access Report option, 154
 - Door Group Report option, 145
 - Door Groups option, 142
 - Door Lock Override option, 111
 - Door Monitor option, 111
 - Door Open Close Times option, 212
 - Door option, 110
 - Door Override Report option, 213
 - Door Status
 - Door Monitor, 211
 - Door Open Close Times, 212
 - Door Override Report, 213
 - Door/Lift Activity option, 122
 - Door/Lift User Activity option, 122
 - Download All option, 221
 - Download Challenger Users option, 222
 - Download Changes option, 222
 - download user, 222
 - Download User option, 130, 222
 - DST, 243
 - dual custody, 272
 - Duress
 - Locator Report, 183
 - Locators, 182
 - Station Report, 184
 - Stations, 182
 - Transmitter Report, 184
 - Transmitters, 183
 - Duress Locators option, 182

Duress Stations option, 182
 Duress Transmitters option, 183
 DVR
 Camera Report, 205
 Cameras, 202
 MultiView, 118, 203
 Preset Report, 206
 Presets, 202
 Report, 206
 DVR Camera Report option, 205
 DVR Cameras option, 202
 DVR Presets option, 202
 DVR Report option, 206
 DVRs option, 201
 DXF format, 96

E

EcoStream WDGP, 268
 Edit Map option, 99
 email address, 166, 228
 Email Addresses option, 166
 email host, 228
 Equipment Report option, 178
 Equipment Status
 List NFS Exports, 214
 List NFS Storage, 180
 Printer Status, 213
 Serial Port Status, 214
 event
 check, 77
 paging, 81
 trigger, 81
 event action
 auto report, 80
 Challenger control, 79
 execute process, 80
 generate alarm, 80
 output data to port, 80
 user data export, 84
 user photo export, 84
 video control, 79
 Event Check option, 77
 Event Check Report option, 84
 Event Group Report option, 195
 event monitor, 36
 display user data, 234
 tool bar, 36
 Event Monitor Information, 234
 Event Paging option, 81
 Event Paging Report option, 85
 Event Report option, 123
 Event Simulator option, 249
 Event Trigger option, 81
 Event Trigger Report option, 85
 Events option, 194
 Expired Profile option, 155
 Expiry Report option, 155
 export

 history, 88, 92
 history archive, 92
 Export History Archive option, 92
 Export History option, 92
 export storage location, 234
 export user data, 233
 Export User Data option, 161
 extended
 alarm groups, 141
 door groups, 142
 floor groups, 144
 timezones, 278

F

firmware version
 8.128, 141, 142, 144, 278
 8.79, 262
 Floor Access Report option, 156
 Floor Group Report option, 145
 Floor Groups option, 143
 Floor option, 113
 Forcefield
 client, 9
 configuration, 226
 icon editor, 237
 shutdown, 223
 speed bar, 18, 243
 title bar, 17
 workspace, 15
 Forcefield Web Toolbox, 240
 Format Disk option, 93

G

Generate IUM Data option, 45
 generating reports, 28
 Graphics
 Background Editor, 96
 Convert DXF to Map, 96
 Display Map, 97
 Edit Map, 99
 Import Bitmap File, 101
 Import LAP Icon, 102
 LAP Editor, 103
 Map Database, 105
 Guard Tour
 Guard Tour Control, 106
 Guard Tour Program, 107
 Guard Tour Report, 109
 overview, 106
 Guard Tour Control option, 106
 Guard Tour Program option, 107
 Guard Tour Report option, 109

H

heartbeat timeout, 298
 help text, 104, 239
 history

- clear, 63
- purge, 93
- History
 - Add Event, 120
 - Door/Lift Activity, 122
 - Door/Lift User Activity, 122
 - Event Report, 123
 - History Config, 121
 - History Report, 123
 - Incident Report, 124
 - Offline History, 124
- History Config option, 121
- History Report option, 123
- holiday
 - adding, 70
 - assigning holiday records, 70, 290
 - Challenger, 290
 - defining holiday records, 70, 166
 - deleting, 71
 - removing, 70
- Holidays option, 166, 290

I

- Icon Editor option, 237
- icons
 - background activity, 17
 - scheduled activity, 18
- ID postfix, 65
- ID prefix, 65
- ID source files, 68
- Idle User Report option, 156
- Import Bitmap File option, 101
- Import LAP Icon option, 102
- import user data, 162, 233
- Import User Data option, 162
- Incident Report option, 124
- incidents, 10, 32, 231
- Individual Item Status option, 211
- Inovonics WDGP, 267
- Input option, 113
- Intercom Master option, 184
- Intercom Slave option, 185
- Intercoms
 - Master, 184
 - Master Report, 186
 - Slave, 185
 - Slave Report, 186
- IP interface, 298
- Issue User Card option, 161
- Items in State Report option, 211
- IUM
 - card category, 219, 220
 - data, 45
 - learn reader, 44, 130, 137
 - software, 219
- IUM Card Categories option, 220

J

- Jacques intercom, 184

L

- LAP Editor option, 103
- LAP Report option, 105
- Last Access By A User option, 157
- learn reader, 44, 130, 137
- licensing, 195
- Lift option, 114
- List NFS Exports option, 214
- List NFS Storage option, 180
- Locator Report option, 183
- log in, 22, 229
- log off, 24, 77
- Logic button, 82, 84
- Login Attempts option, 224
- Login Message option, 224
- login options, 229
- Logoff option, 77

M

- Maintenance Config option, 139
- Maintenance option, 131
- Management Software
 - Alarm Responses, 187
 - Cluster Report, 188
 - Cluster Usage Report, 188
 - Computer Categories, 188
 - Computer Category Report, 191
 - Computer Category Usage Report, 192
 - Event Group Report, 195
 - Events, 194
 - Member Group Report, 193
 - Member Group Usage Report, 194
 - Member Groups, 193
 - Member Report, 193
 - Member Usage Report, 194
 - Members, 192
 - Program Clusters, 187
- map
 - adding a single LAP, 100
 - adding multiple LAPs, 101
 - background, 96
 - display, 97
 - edit, 99
 - file format, 96
- Map Database option, 105
- Master Report option, 186
- Matching Profile option, 151
- Matrix
 - Cameras, 206
 - Monitors, 206
 - Switchers, 208
 - Video Presets, 207
- media player, 128
- Member Group Report option, 193

- Member Group Usage Report option, 194
- member groups, 6, 193
- Member Groups option, 193
- Member Report option, 193
- Member Usage Report option, 194
- members, 6, 192
- Members option, 192
- menu
 - classic, 230
 - Forcefield 6, 230, 308
- minimum call digits, 185
- Modify License option, 239
- Modify Profile Access option, 144
- Modify Status
 - Change Status of User, 146
 - Set Users Offsite, 51
- Monitor Report option, 209
- Monitors option, 206
- Mount Storage option, 225
- MultiView option, 203
- Muster Report option, 158

N

- navigation, 22
- network, 239
- Network Configuration option, 239
- network details, 241
- NFS Exports option, 180
- NFS storage, 181, 234
- NFS Storage option, 181
- Node option, 167
- non-IUM Challenger, 49
- NTP server, 228

O

- Offline History option, 124
- offsite redundancy, 9, 241, 246, 303
- operator
 - lockout, 226
 - password, 165
 - setup, 164
- Operator Menu Permissions option, 164
- Operator Password option, 165
- Operator Permissions option, 163
- Operator Report option, 165
- Operator Setup option, 164
- Operators
 - Menu Permissions, 164
 - Permissions, 163
 - Report, 165
 - Setup, 164
- outputs, 288
- override access, 173
- override alarms, 232
- override member, 165

P

- Page Message option, 225
- patches, 215
- port processes, 169
- positions
 - unused, 130
- Preset Report option, 206, 209
- Presets option, 207
- printer
 - default, 174
- Printer Permission option, 167
- Printer Status option, 213
- Printers option, 168
- Profile Access Report option, 151
- Profile Report option, 152
- profiles
 - unused, 130, 232
- Profiles
 - Assign Profile to Users, 146
 - Matching Profile, 151
 - Profile Access Report, 151
 - Profile Report, 152
 - Program Profile, 147
 - Sync Profile Data, 151
- Program Clusters option, 187
- Program Profile option, 147
- Program Time Zones option, 199
- programming Challenger, 217
- prohibit shared profiles mode, 55
- Purge History option, 93

Q

- QNX, 321
- QNX Shell option, 225

R

- RAS card and PIN time, 270
- RAS option, 114
- raw card data, 45
- Reader Config Card option, 161
- Relay option, 115
- remote control, 42
- report
 - abnormal status, 210
 - alarm group, 145
 - area control, 153
 - camera, 205, 209
 - card, 153
 - card (user), 153
 - Challenger detail, 220
 - Challenger enabled, 221
 - Challenger item status, 211
 - Challenger summary, 221
 - Challenger user, 221
 - cluster, 188
 - computer category, 191
 - computer category usage, 192

- door access, 154
 - door group, 145
 - door open close times, 212
 - door override, 213
 - equipment, 178
 - event, 123
 - event check, 84
 - event group, 195
 - event paging, 85
 - event trigger, 85
 - floor access, 156
 - floor group, 145
 - guard tour, 109
 - history, 123
 - idle user, 156
 - incident, 124
 - individual item status, 211
 - items in state, 211
 - LAP, 105
 - last access by a user, 157
 - locator, 183
 - master, 186
 - matching profile, 151
 - member, 193
 - member group, 193
 - member group usage, 194
 - member usage, 194
 - monitor, 209
 - muster, 158
 - operator, 165
 - preset, 206, 209
 - profile, 152
 - profile access, 151
 - slave, 186
 - station, 184
 - switcher, 209
 - time trigger, 85
 - timezone, 199
 - timezone usage, 199
 - transmitter, 184
 - user, 153
 - user access, 159
 - user activation, 152
 - user expiry, 155
 - user on-site, 159
 - users by alarm group, 145
 - users by door group, 145
 - users by floor group, 145
 - users by region, 160
 - reports, 28
 - system status, 43
 - Reset Operator Lockout option, 226
- S**
- Samba (CIFS) option, 181
 - scan time, 233
 - scheduled activity, 18
 - sector, 80, 82
 - sector alarm, 175, 190, 231, 258, 322
 - secure test time, 269
 - Select Learn Reader option, 130
 - Send Operator Message option, 226
 - Serial & Parallel Ports option, 169
 - Serial Port Status option, 214
 - service packs, 215
 - Service System option, 242
 - Set Server Locale option, 243
 - Set System Date/Time option, 226
 - Set Users Offsite option, 51
 - Setup Programmer option, 161
 - shortcuts, 19
 - Show Ch. User Number option, 162
 - Show DVR Footage
 - Tagged Footage, 125
 - Time Footage, 128
 - Show DVR Video option, 119
 - Show PIN Code option, 140
 - Show System User Number option, 162
 - shutdown
 - automatic, 24
 - Forcefield, 223
 - Slave Report option, 186
 - smart card options, 51
 - Smart Card Programmer
 - Display User Card, 160
 - Issue User Card, 161
 - Reader Config Card, 161
 - Setup Programmer, 161
 - soft timezone
 - assigning, 73
 - removing, 73
 - soft timezones, 292
 - software IUM, 219
 - software keyboard, 23, 175
 - speed bar, 18, 243
 - Speed Bar Configuration option, 243
 - Station Report option, 184
 - Statistics option, 62
 - Status
 - Trace Monitor, 210
 - Status File Utility option, 250
 - Storage
 - All Storages, 179
 - Disk Storage, 179
 - List NFS Storage, 180
 - NFS Exports, 180
 - NFS Storage, 181
 - Samba (CIFS), 181
 - storage devices, 179
 - Switcher Report option, 209
 - Switchers option, 208
 - symbol editor, 237
 - Sync Profile Data option, 151
 - system backup, 89
 - System Backup option, 89
 - System Information option, 251
 - System option, 197

system restore, 93
 System Restore option, 93
 System Status
 Check Log Report, 216
 Computer Status, 214
 Debug File Report, 216
 System Status, 215
 System Status option, 215
 System Sub Types option, 198
 System Types option, 198

T

Tagged Footage option, 125
 TCP/IP addresses, 240
 TCP/IP Hosts option, 170
 TCP/IP Ports option, 170
 Teleste, 80, 82, 190, 206, 207, 208, 209, 312, 322
 templates, 29
 Third Party
 Device Types, 196
 Devices, 195
 System, 197
 System Sub Types, 198
 System Types, 198
 time
 access test, 269
 secure test, 269
 warning, 269
 time allowed in region, 50
 Time Footage option, 128
 Time Trigger option, 82
 Time Trigger Report option, 85
 Time Zone Report option, 199
 Time Zones
 Program Time Zones, 199
 Time Zone Report, 199
 Timezone Usage Report, 199
 timed access, 150
 timed user access, 49
 timezone
 adding, 72
 assigning, 71
 deleting, 72
 removing, 72
 Timezone Usage Report option, 199
 title bar, 17
 Tools
 aca Events, 250
 Event Simulator, 249
 QNX Shell, 225
 Status File Utility, 250
 System Information, 251
 Trace Monitor option, 210
 Transfer User Data
 Export User Data, 161
 Import User Data, 162
 Transmitter Report option, 184

Triggering
 Event Check, 77
 Event Check Report, 84
 Event Paging, 81
 Event Paging Report, 85
 Event Trigger, 81
 Event Trigger Report, 85
 Time Trigger, 82
 Time Trigger Report, 85
 TS0099, 298, 320
 TS0870, 52
 TS0898, 298, 320
 two badge unlock, 282

U

unacknowledged alarms, 31
 uninterruptible power supply, 171
 unique profile per user mode, 56, 138
 unique profiles mode, 55
 unused
 data, 130
 departments, 130
 positions, 130
 profiles, 130
 Unused Data Report option, 158
 Upload All Challenger Data option, 220
 upload Challenger data, 66, 220
 UPS option, 171
 USB storage, 234
 user
 data display, 234
 offset, 49
 profile, 9
 User Access Report option, 159
 user defined data field, 233
 User Maintenance option, 131
 User Maintenance window
 configuring, 21, 139
 defaults, 21
 templates, 21, 57
 User Numbering
 Show Ch. User Number, 162
 Show System User Number, 162
 User On-Site Report option, 159
 User Reports
 Activation Report, 152
 Area Control Report, 153
 Card (User) Report, 153
 Door Access Report, 154
 Expired Profile, 155
 Expiry Report, 155
 Floor Access Report, 156
 Idle User Report, 156
 Last Access By A User, 157
 Muster Report, 158
 Unused Data Report, 158
 User Access Report, 159
 User On-Site Report, 159

- Users By Region Report, 160
- users
 - auto-allocate, 48
 - bulk create, 46
 - bulk delete, 48
 - bulk modify, 47
 - export data, 233
 - import data, 162, 233
 - non-IUM, 49
 - search order, 232
 - set offsite, 50
 - time in region, 50
 - timed access, 49
- Users
 - Delete Unused Data, 130
 - Design Card Layout, 129
 - Download User, 130
 - Maintenance, 131
 - Maintenance Config, 139
 - Select Learn Reader, 130
 - Show PIN Code, 140

- Users By Alarm Group option, 145
- Users By Door Group option, 145
- Users By Floor Group option, 145
- Users By Region Report option, 160

V

- V8 Extended, 218
- Video quality, 205
- Video service, 200

W

- warning time, 269
- watch house, 174, 227, 323
- web server, 240
- Windows Manager Options option, 244
- wireless DGP, 267
- workstation detail button, 215
- Workstation Permissions option, 172
- Workstations option, 173

