



Forcefield[®] External Interfaces Manual

| | |
|-------------------------------|--|
| Copyright | © 2018 UTC Fire & Security Australia Pty Ltd. All rights reserved. |
| Trademarks and patents | <p>The Forcefield name and logo are trademarks of UTC Fire & Security Australia Pty Ltd.</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 | <p>UTC Fire & Security Australia Pty Ltd t/a Interlogix A UTC Climate, Controls & Security company 10 Ferntree Place Notting Hill, Victoria, 3168, Australia</p> |
| ACMA compliance |  N4131 |
| Contact information | For contact information, see www.interlogix.com.au . |

Content

| | |
|---|-----------|
| Important information..... | iii |
| Chapter 1 Introduction..... | 1 |
| Audience | 2 |
| Scope of this manual | 2 |
| Related documents..... | 2 |
| Before you begin | 3 |
| Chapter 2 Integrating a Smart Card Programmer..... | 5 |
| Installing Smart Card Programmer hardware..... | 6 |
| Smart cards used for access control functionality | 7 |
| Smart cards used for credit functionality | 17 |
| Specifying default values for smart cards..... | 21 |
| Chapter 3 Integrating photo ID..... | 23 |
| Overview | 24 |
| Using Capture..... | 25 |
| Capture device settings | 28 |
| Using Import | 30 |
| Using Card Layout Editor..... | 32 |
| Chapter 4 Integrating automatic event email..... | 43 |
| Overview | 44 |
| Adding an email address | 44 |
| Chapter 5 Integrating intercom..... | 45 |
| Intercom system overview | 46 |
| Forcefield intercom interface..... | 47 |
| Integrating a Commend IP intercom system | 49 |
| Integrating a Jacques intercom system..... | 50 |
| Chapter 6 Integrating paging and duress..... | 53 |
| Integrating Paging | 54 |
| Integrating an Ascom Nira duress system..... | 54 |
| Chapter 7 Integrating CCTV..... | 59 |
| Overview | 60 |
| Video switcher system | 61 |
| DVR systems..... | 65 |
| Teleste Video Management system..... | 74 |
| Chapter 8 Integrating third-party systems..... | 77 |
| Overview | 78 |
| System security | 78 |
| Communications..... | 78 |

| | |
|--|------------|
| Message formats | 79 |
| Third-party system example | 80 |
| Chapter 9 Integrating external user data | 83 |
| Setting up an export/import folder on a Windows computer | 84 |
| Exporting user records | 90 |
| Preparing user data for importing | 91 |
| User data file field names | 95 |
| Generating raw card data | 97 |
| Auto-populating raw card data fields..... | 97 |
| Importing user records..... | 98 |
| Troubleshooting the import process..... | 99 |
| Appendix A User data file formats | 101 |
| Export file formats | 102 |
| Import file formats..... | 112 |
| Appendix B History export data formats..... | 127 |
| Structure of history database record..... | 128 |
| Export raw | 128 |
| Export formatted..... | 129 |
| Appendix C Integrating legacy DVRs | 131 |
| Overview | 132 |
| Legacy DVR integration process | 133 |
| Forcefield-legacy DVR hardware requirements | 135 |
| Application notes | 139 |
| Appendix D Integrating DVRs | 141 |
| Overview | 142 |
| DVR integration process..... | 143 |
| Setting up the video server..... | 144 |
| Setting up video clients..... | 145 |
| Setting up the video service..... | 146 |
| Glossary..... | 149 |

Important information

This is the Forcefield® External Interfaces Manual. This document includes an overview of the product and detailed instructions explaining:

- How to set up external interfaces such as CCTV, duress, intercom, paging, email, and photo ID.
- How to program Smart Cards and use Photo ID and the Card Layout Editor.
- How to export user data to and import user data from external locations.

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

- Installation and programming of Challenger® security systems
- The appropriate level of Forcefield trained and assessed certification (L1 Forcefield, L2 Integration, and L3 Enterprise).

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

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 refers to the classic menu locations of commands. A Forcefield 6 system can use either the Forcefield 6 menu structure or the classic menu structure. For example, the Computer Categories command is in different locations in each menu system:

- In the classic menu structure, go to Databases > Management Software > Computer Categories > Computer Categories.
- In the Forcefield 6 menu structure, go to Administration > Forcefield Setup > Computer Categories.

See the *Forcefield Operators Manual* for details.

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Interlogix 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 chapter describes the intended user of this manual, what it covers, and what other documents may be required.

Content

- Audience 2
- Scope of this manual 2
- Related documents 2
- Before you begin 3

Audience

This manual is for use by trained Forcefield integration technicians and Forcefield operators. It provides reference material for setting up external interfaces such as CCTV, duress, intercom, paging, email, and photo ID.

It also provides reference material for programming Smart Cards and using Photo ID and the Card Layout Editor.

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.

Forcefield hardware for both standard edition and Enterprise edition is represented by an image of standard Forcefield hardware.

Figure 1: Representation of Forcefield hardware



Related documents

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

Refer to the *Forcefield Operators Manual* for introductory material (including key concepts), command reference, and descriptions of Forcefield programming tasks typically performed by trained Forcefield installation technicians, as well as tasks performed by Forcefield operators.

For details about Challenger programming refer to the following Challenger Programming manuals:

- For Challenger10, ChallengerSE, or ChallengerLE panels, see the *Challenger Series Programming Manual*.
- For earlier versions of Challenger panels, see the *Challenger V8 & V9 Programming Manual*.

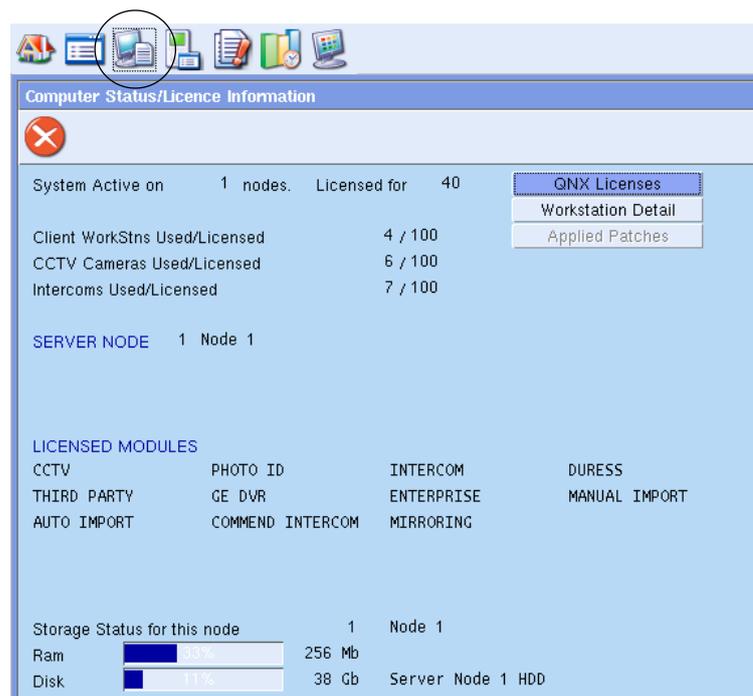
For details about setting up IP communications in Challenger V8 panels, refer to the *TS0099 Enhanced Challenger TCP/IP Interface Installation and Programming Guide*.

Before you begin

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 2: Computer Status window



If the module you need is not listed, then you must purchase and install a license (except for Interlogix video switchers, which do not require a CCTV license module).

Chapter 2

Integrating a Smart Card Programmer

Summary

This section describes how to use a Smart Card Programmer connected to either a Forcefield node or a Forcefield client computer.

Refer to Chapter 3 “Integrating photo ID” on page 23 for details about using Photo ID on a Forcefield client computer.

Content

| | |
|---|----|
| Installing Smart Card Programmer hardware..... | 6 |
| Requirements | 6 |
| Procedure for a client..... | 6 |
| Procedure for a node | 6 |
| Smart cards used for access control functionality | 7 |
| Setting up the Smart Card Programmer | 7 |
| Smart Card Programmer options | 8 |
| Firmware version recall..... | 9 |
| Changing the COM port number | 10 |
| Creating a reader configuration card..... | 10 |
| Reader configuration card options (user access) | 11 |
| Display user card information..... | 14 |
| Issuing user cards (typical) | 15 |
| Smart cards used for credit functionality | 17 |
| Installing Smart Card programmer hardware | 17 |
| Setting up the Smart Card programmer (credit use)..... | 17 |
| Creating a reader configuration card (credit use) | 17 |
| Issuing user cards (credit use) | 19 |
| Programming user credits (credit use) | 20 |
| Programming access data (credit use)..... | 20 |
| Specifying default values for smart cards | 21 |

Installing Smart Card Programmer hardware

Install a Smart Card Programmer on a Forcefield client or a Forcefield Enterprise node where card programming will be performed. See “Procedure for a client” below or “Procedure for a node” below, as required.

Requirements

- Smart Card Programmer, serial cable, power pack.
- Unused serial port on the client or node computer.
- User interface (such as a monitor, keyboard, and mouse).

Procedure for a client

Install a Smart Card Programmer on a Forcefield client where card programming will be performed.

To install Smart Card Programmer hardware:

1. Connect the serial cable to a free serial port on the Forcefield client to be used for programming cards. Connect the other end to the connection marked “RS-232” on the Smart Card Programmer.
2. Connect the power pack to the Smart Card Programmer, and then connect the power pack to mains power.

Procedure for a node

Install a Smart Card Programmer on a Forcefield node where card programming will be performed.

Note: The node computer must have a user interface (such as a monitor, keyboard, and mouse).

To install Smart Card Programmer hardware:

1. Connect the serial cable to a free serial port on the node to be used for programming cards. Connect the other end to the connection marked “RS-232” on the Smart Card Programmer.
2. Connect the power pack to the Smart Card Programmer, and then connect the power pack to mains power.
3. Create a port record in Forcefield for the Smart Card. Enter an ID for the Smart Card Programmer, for example, ‘Node 1 Smart Card Programmer’. See the *Forcefield Operators Manual* for details.
4. Select “SmartCard Programmer” as the port type.
5. Enter the node number for the port. The Smart Card Programmer can only program cards on the same node that it’s installed on.

6. Select the System (QNX) ID for the hardware device (serial port), for example ser2= serial port 2. All serial ports are listed, not just available ports.
7. Click Save, and then close the port record.
8. Setup the Smart Card Programmer using the SmartCard Programmer port record. See “Setting up the Smart Card Programmer” below.

Smart cards used for access control functionality

This section describes the options on the Card Programmer Properties screen that apply only to using Smart Cards for access control purposes instead of for credit purposes.

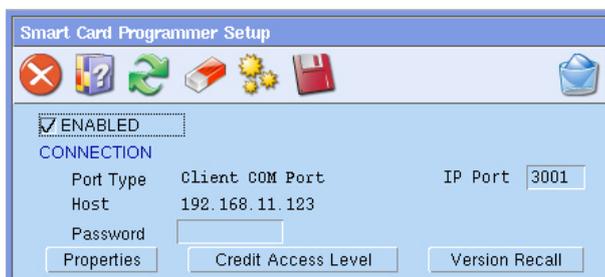
Setting up the Smart Card Programmer

Use the Smart Card Programmer Properties Setup options to program the Smart Card Programmer in Forcefield.

This procedure assumes the Smart Card Programmer hardware was successfully installed.

To program the Smart Card Programmer:

1. Select Users > Smart Card Programmer > Setup Programmer.



2. Type the Forcefield client’s IP port number in the IP Port field. The port must not be blocked by a firewall or other means. By default Forcefield uses COM1 on the Forcefield client to communicate with the Smart Card Programmer. If you need to use a different port, see “Changing the COM port number” on page 10.
3. Type the connection password in the Password field. The connection password can be up to 10 digits (the default password is all zeros). Forcefield uses this password to connect with the Smart Card Programmer. To change the connection password, click Properties.
4. Right-click Enabled to enable the Smart Card Programmer.

- Click Save (F5) to save. If the installation was successful, the LED on the Smart Card Programmer will be orange, and then the programmer can now send or receive data. In addition, a Software Terminal Server icon displays in the Windows system tray, similar to below.



See the following sections for details about the buttons on the Smart Card Programmer Setup window:

- The Properties button is described in “Smart Card Programmer options” below.
- The Credit Access Level button is described in “Smart cards used for credit functionality” on page 17.
- The Version Recall button is described in “Firmware version recall” on page 9.

Smart Card Programmer options

After connecting to the Smart Card Programmer, Forcefield can be used to program the Smart Card Programmer options. This section describes the options on the Card Programmer Properties screen.

From the main menu select: Users > Smart Card Programmer > Setup Programmer, and then click Properties.

Figure 3: Programmer Properties window (Smart Card Programmer)



Click Save (F5) to save and change the properties when finished, and to return to the Smart Card Programmer Setup screen.

Default and upload buttons

If the programmer is online, click Default to display the factory default settings (the factory default programmer password is 38.33.123.42).

Alternatively, click Upload to display the Smart Card Programmer's current settings.

Connection password

The optional connection password helps to ensure that only the authorised operator can use this Smart Card Programmer.

The connection password can be up to 10 digits and can be modified at any time.

Card password lock

Select the Card Password Lock button if you wish to prevent the security password from ever being deleted from the cards. This prevents a card being blanked completely.

Programmer password

Type a password (also known as the security password or 4-byte code) in the range of 0 to 127 in each field.

Note: For higher security, we can issue a unique, read-only, security password using values in the range of 128 to 255 (requires a TS0870PSC Configuration Card).

The Smart Card Programmer stores the password and writes the same number to the cards. Only cards with the same security password can be erased or blanked if the card programmer's security password matches that on the card. This number must also match the security password stored in the Smart Card reader for the cards to work.

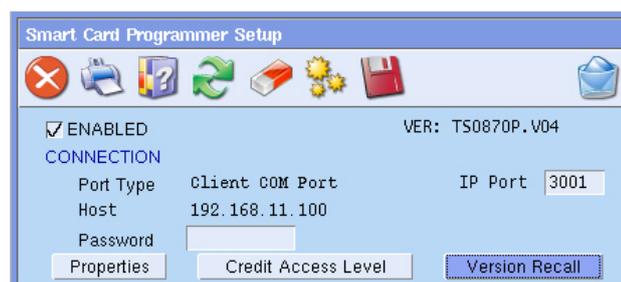
Site code limits

Type the details for the site code limits (or ranges). Up to ten site code limits can be stored in the programmer. Site codes outside of these limits cannot be programmed into user cards.

Firmware version recall

From the main menu select: Users > Smart Card Programmer > Setup Programmer, and then click Version Recall to display the Smart Card Programmer firmware version (in this case V.04).

Figure 4: Smart Card Programmer Setup window (example IP address used)



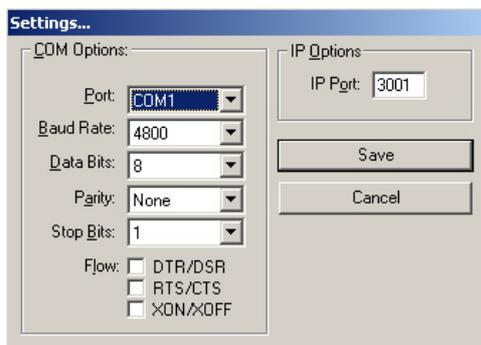
Changing the COM port number

By default Forcefield uses COM1 on the Forcefield client to communicate with a Smart Card Programmer.

Note: The Smart Card Programmer must first be enabled using the Setup Programmer command (see “Setting up the Smart Card Programmer” on page 7).

To change the Smart Card Programmer port number, if necessary:

1. Right-click the Software Terminal Server icon in the Windows system tray, and then select Disable.
2. Right-click the Software Terminal Server icon, and then select Settings.



3. Click the Port arrow, and then select the required port number. The port must not be blocked by a firewall or other means.
4. Change the required settings, and then click Save.
5. Right-click the Software Terminal Server icon in the Windows system tray, and then select Enable.

Creating a reader configuration card

Smart Card readers can be programmed two ways:

- By use of an LCD RAS to access the Install menu options for programming the reader.
- By use of a reader configuration card, programmed for the specific Smart Card reader. A reader configuration card is required to program cards in secured mode (using the 4-byte security password). This is the only means of transferring the 4-byte code to a reader.

Different options are required on a reader configuration card depending on whether the reader is being used for access control or for credit functionality.

See the appropriate Smart Card Reader Installation Guide for instructions to change the reader default values.

The Smart Card reader is 'online' only when directly connected to a Challenger LAN, or an Intelligent Door/Lift Controller LAN.

To create a reader configuration card:

1. From the main menu select Users > Smart Card Programmer > Reader Config Card (Figure 5 on page 12). See Table 1 below for a description of the buttons at the bottom of the screen.
2. Select the Reader Configuration Card options, as required (see “Reader configuration card options (user access)” below).
3. Place a configuration card or a blank card on the Smart Card Programmer.
4. Double-click Read to check that the card is either a reader configuration card or a blank card.
5. Double-click Write to transfer the selected options to the reader configuration card. A successful write produces two beeps; write denied produces seven beeps. Some options (marked with *) are not supported by the reader-equipped CA1115 or CA1116 RASs.

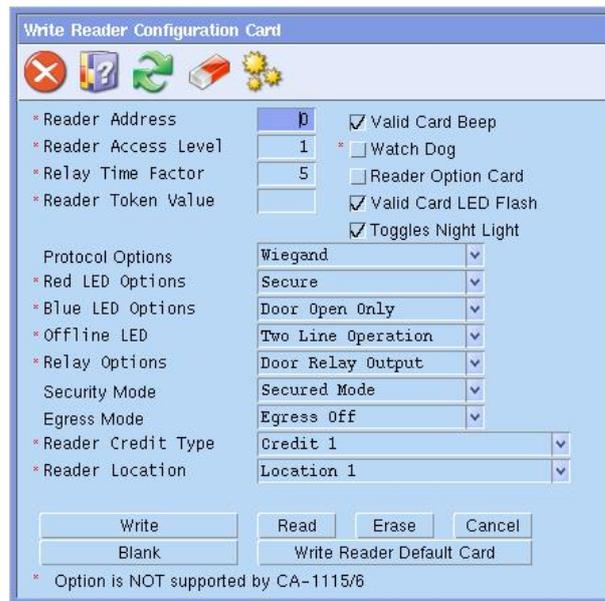
Table 1: Reader Configuration Card window buttons

| Button | Details |
|---------|---|
| Write | Attempts to transfer the data displayed on the screen to the card. Use this action to program a card. The Smart Card Programmer emits two beeps to indicate a successful write and seven beeps to indicate that writing was denied. |
| Read | Reads and displays the data (if any) currently programmed onto the card. Use this action to check a card's current details. The Smart Card Programmer emits two beeps to indicate a successful operation. |
| Erase | Deletes the data from the card, but leaves the site security code intact. The Smart Card Programmer emits two beeps to indicate a successful operation. |
| Default | Writes a default configuration card that will program readers to factory settings. The Smart Card Programmer emits two beeps to indicate a successful operation. |
| Cancel | Cancels the current operation. |
| Blank | Deletes the data and the site security code from the card (available only if the card password lock was switched off when the card was written). The Smart Card Programmer emits two beeps to indicate a successful operation. |

Reader configuration card options (user access)

This section describes the options on the Write Reader Configuration Card window (Figure 5 on page 12) for access use instead of for credit use.

You will need to create a Reader Configuration Card for each reader to be polled on the Challenger LAN, or an Intelligent Door/Lift Controller LAN, where the programmable options differ from the factory default values (i.e. if you have 16 readers with addresses 1 through 16, you will need to program 16 different reader configuration cards).

Figure 5: Reader Configuration Card window

Reader address

If the reader is on a Challenger LAN, or an Intelligent Door/Lift Controller LAN, type a number from 1 to 16 in the Reader Address field to specify the Smart Card reader address.

Leave the address field blank:

- For readers such as CA1115 or CA1116 that have their RAS addresses set via DIP switches.
- To create a reader configuration card to program readers without using a fixed reader address. The reader address would be set during address programming mode, in which the reader configuration card is used to select the required address from a series of coded beeps. Refer to the Smart Card Reader's Installation and Programming Manual for details.

Valid card beep

Optional—If selected, the reader will beep once when valid Smart Card is badged at the reader (in addition to any other beeps).

Watch dog

Optional—If selected, 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 (configuration) card

Optional—If selected, 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—If selected, the reader's LED gives a short flash when a valid card is badged.

Toggles night light

Optional—If selected, the blue LED remains lit, with low intensity, at all times regardless of whether the red LED is on or off.

Protocol options

Select the required protocol:

- **Wiegand mode**—Card data is generated in the Wiegand protocol. The information on the card decides which format can be used, for example: Tecom ASP or Standard 26-bit Wiegand format.
- **Magnetic Stripe**—Card data is generated in the Track-2 magnetic stripe format. A 'card present' signal is available on the relay output (violet wire) if selected by configuration card (see "Relay options" on page 14).

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 mag-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—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.

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

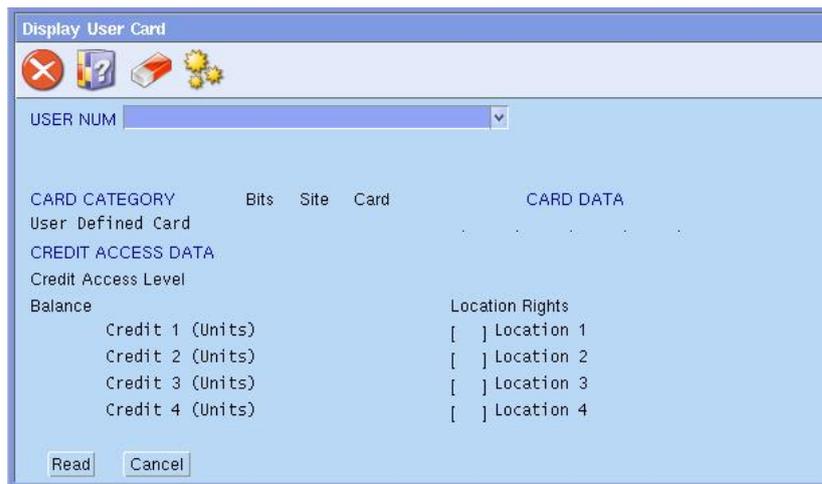
Select one of the following egress mode options:

- Egress off
- Standard Egress
- Egress and Arm/disarm

Display user card information

Forcefield operators may need to check the data written to a card. Open the Display User Card window (Figure 6 on page 15).

Figure 6: Display User Card window



To display user card information:

1. From the main menu select Users > Smart Card Programmer > Display User Card.
2. Place the card on the Smart Card Programmer. Double-click Read to display information stored on the card.

Issuing user cards (typical)

From the main menu select Users > Smart Card Programmer > Issue User Card.

Figure 7: Issue User Card window



Authorised Forcefield operators may perform the following card actions described in Table 2 below when issuing user access cards.

Table 2: Issue User Card window buttons

| Button | Details |
|--------|---|
| Read | Reads and displays the data (if any) currently programmed onto the card. Use this action to check a card's current details. The Smart Card Programmer emits two beeps to indicate a successful operation. |

| Button | Details |
|--------|---|
| Write | Attempts to transfer the data displayed on the screen to the card. Use this action to program a card. The Smart Card Programmer emits two beeps to indicate a successful write and seven beeps to indicate that writing was denied. |
| Erase | Deletes the data from the card, but leaves the site security code intact. The Smart Card Programmer emits two beeps to indicate a successful operation. |
| Blank | Deletes the data and the site security code from the card (available only if the card password lock was switched off when the card was written). The Smart Card Programmer emits two beeps to indicate a successful operation. |
| Cancel | Cancels the current operation. |

The uses of the other buttons are described in “Issuing user cards (credit use)” on page 19.

Note: Default values for bits and site fields may be specified in Admin > Configuration > Configuration > User (Global). Doing so enables you to select only the user for system default cards, and then the raw card data will be automatically calculated from the default settings. See “Specifying default values for smart cards” on page 21 for details.

To issue user cards:

1. From the main menu select Users > Smart Card Programmer > Issue User Card (Figure 7 on page 15).
2. For IUM systems: select a user number and card category. The raw card data will appear.
— OR —
For non-IUM systems: enter the card format (Bits field), the site code (Site field), and the card number (Card field) to create the raw card data. If the card format is other than 26-bit or 27-bit, then you must also enter the six bytes of card data.
3. Place a blank card on the Smart Card Programmer.
4. Double-click Write to program the card. The Smart Card Programmer emits two beeps to indicate a successful write or seven beeps to indicate that writing was denied.

Smart cards used for credit functionality

This section describes the options on the Card Programmer Properties screen that apply only to using Smart Cards for credit purposes instead of for access control purposes.

Installing Smart Card programmer hardware

Refer to the section “Installing Smart Card Programmer hardware” on page 6 for details.

Setting up the Smart Card programmer (credit use)

The procedures described in this section are used in addition to the procedures described in “Setting up the Smart Card Programmer” on page 7.

From the main menu select Users > Smart Card Programmer > Setup Programmer, and then click Credit Access Level to display the Credit Access Level Descriptions window.

Figure 8: Credit Access Level Descriptions window (Smart Card Programmer)

Type the details for the credit field, and then its location details (e.g. Credit 1 and Location 1). This screen records existing credit information for each account and location (this information also appears in the Write Credits Units screen).

Click Save (F5) when finished to return to the Smart Card Programmer Setup screen.

Creating a reader configuration card (credit use)

Smart Card readers can be programmed in the following ways:

- By use of a RAS.
- By use of a reader configuration card programmed for the specific Smart Card reader.

- By use of a reader configuration card programmed without an address (the reader address is set during address programming mode, in which the reader configuration card is used to select the required address from a series of coded beeps).

Different options are required on a reader configuration card depending on whether the reader is being used for:

- Access control functions (see “Reader configuration card options (user access)” on page 11).
- Credit functions (this section).

Refer to the applicable smart card reader’s installation guide for instructions to change the reader default values.

Reader configuration card options (credit use)

This section describes the options on the Reader Configuration Card window (Figure 5 on page 12) pertaining to credit use instead of access use.

Reader access level

If the configuration card is to be used for programming smart card ‘credit’ readers (e.g. for a photocopier or drinks dispenser), type a number from 1 to 16 in the Reader Access Level field to define the readers’ access level (16 is the highest).

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

If applicable, type a number from 1 to 256 to specify the relay time factor. The relay time factor modifies the pulse width output of the pulsed relay option and the energised time for the timed relay.

Reader token value

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

If applicable, type a number in the range of 1 to 65534 to specify the reader’s token value.

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).

Relay options

Select the relay option:

- **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 on a configuration card (see Relay Time Factor).
- **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 Tecom 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 Tecom smart card is badged next, with or without credits.

Reader credit type

Select the reader credit type that the reader will use.

Reader location

Select the reader's location.

Issuing user cards (credit use)

This section applies to programming smart card readers used for 'credit' (e.g. for a photocopier or drinks dispenser).

Authorised Forcefield operators may perform the following card actions described in Table 3 below when issuing user access cards.

Table 3: Issue User Card window buttons

| Button | Details |
|--------------|---|
| Read | Reads and displays the data (if any) currently programmed onto the card. Use this action to check a card's current details. The Smart Card Programmer emits two beeps to indicate a successful operation. |
| Write | Attempts to transfer the data displayed on the screen to the card. Use this action to program a card. The Smart Card Programmer emits two beeps to indicate a successful write and seven beeps to indicate that writing was denied. |
| Erase | Deletes the data from the card, but leaves the site security code intact. The Smart Card Programmer emits two beeps to indicate a successful operation. |
| Credit units | Add credit units to cards or deduct credit units from cards. |

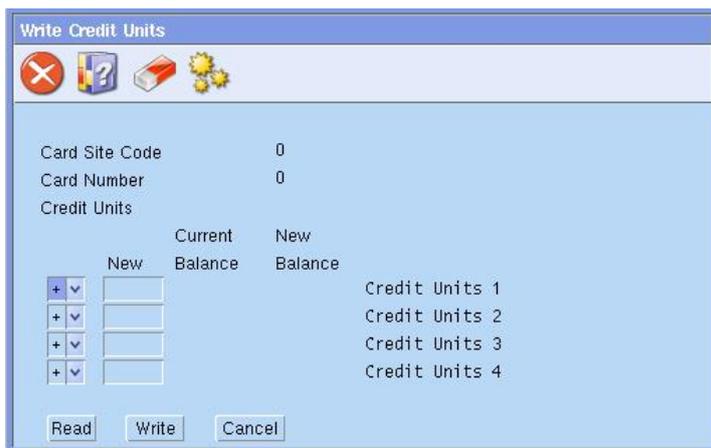
| Button | Details |
|-------------|--|
| Access data | Set the card access levels |
| Blank | Deletes the data and the site security code from the card (available only if the card password lock was switched off when the card was written). The Smart Card Programmer emits two beeps to indicate a successful operation. |
| Cancel | Cancels the current operation. |

Programming user credits (credit use)

This section applies to programming smart card readers used for 'credit' (e.g. for a photocopier or drinks dispenser).

To program user credits:

1. Starting from the Issue User Card window (Figure 7 on page 15), and with a card placed on the Smart Card Programmer, click Credit Units, and then the following screen displays.



2. Double-click Read to check the card's credit details.
3. Type new values in the New fields to add credit units to cards or deduct credit units from the card's current balance.
4. Click Write and then click Esc to return to the Issue Card screen.

Programming access data (credit use)

This section applies to programming smart card readers used for 'credit' (e.g. for a photocopier or drinks dispenser).

To program access data:

1. Starting from the Issue User Card window (Figure 7 on page 15), and with a card placed on the Smart Card Programmer, click Access Data, and then the following screen displays.



2. Double-click Read to check the card's credit details.
3. Type a number from 1 to 16 in the Credit Access Level field to define the access level (16 is the highest) for devices using the credit option. 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 3 cannot use the photocopier.
4. Select the Location rights to permit the use of credits at the selected location(s).
5. Double-click Write, then click Esc.

Specifying default values for smart cards

Use this option to specify global default values for site code and card bits for use in issuing smart cards.

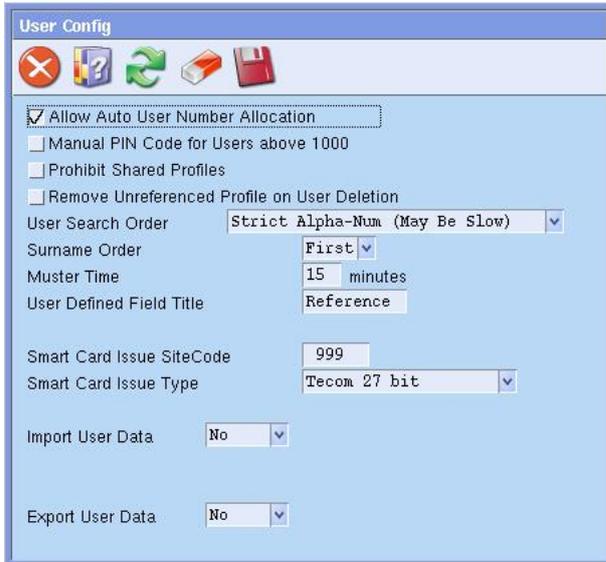
Specifying default values enables you to select only the user for system default cards, and then the raw card data will be automatically calculated from the default settings.

Note: The Forcefield workstation may be configured to use workstation-specific default values which override the global default values, see the Workstation Options—Other section in the *Forcefield Operators Manual*.

To program default site code and card bit values:

1. From the main menu select: Admin > Configuration > Configuration to open the Forcefield Configuration window.

2. Click the User button. The User Config screen displays.



3. Type the site code number in the Smart Card Issue SiteCode field.
4. Select the required Smart Card Issue Type.
5. Click Save.

Chapter 3

Integrating photo ID

Summary

This section describes how to use Photo ID on a Forcefield client computer.

Content

| | |
|--|----|
| Overview | 24 |
| Using Capture | 25 |
| Capture device settings | 28 |
| Using Import..... | 30 |
| Using Card Layout Editor | 32 |
| Forcefield client Card Layout Editor Window..... | 32 |
| Creating a Card Layout..... | 35 |

Overview

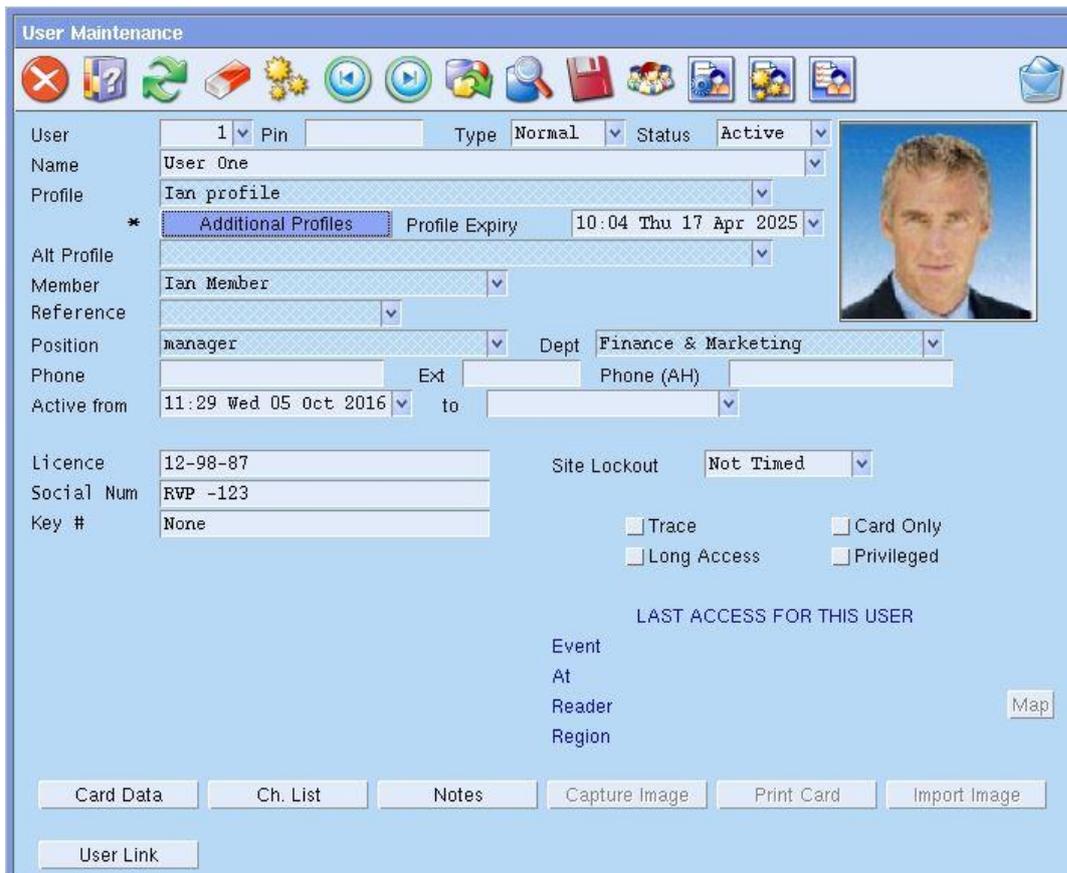
Photo ID user card design and printing facilities are provided for Forcefield client computers only.

Note: The Forcefield client must have the Capture, Import, and Issue options enabled. See the Workstation Options—Other section in the *Forcefield Operators Manual*.

An enabled Forcefield client displays the following buttons on the User Maintenance window (Figure 9 below):

- Capture — Enables you to capture an image from a video camera, see “Using Import” on page 30.
- Import — Enables you to import an image file, see “Forcefield client Card Layout Editor Window” on page 32.
- Print Card — Opens the print preview window for printing the user’s card. The use of this command is described in the *Forcefield Operators Manual*.

Figure 9: User Maintenance window



Using Capture

The use of Capture on a Forcefield client requires the workstation is set up with:

- A video camera.
- A video capture card, driver, and associated software.

In other words, the client must be receiving a video signal in order for an image to be captured.

To capture an image from a video input:

1. In the User Maintenance window, click the Capture button to select and prepare an image file.



2. Right-click the image to change the capture device options (see "Capture device settings" on page 28).
3. Click Capture to collect five images (two per second).

4. Click the still image in the sequence of five that you like best. The large image is the live view from the camera.



5. The selected image displays in the Import User Image window.

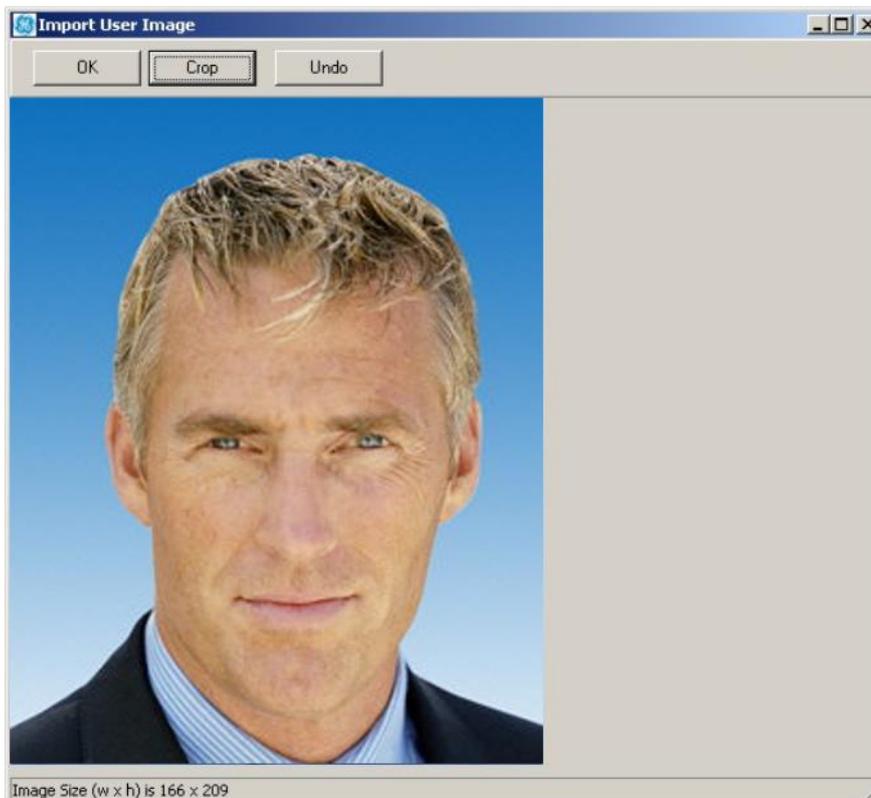


6. If the displayed image isn't suitable, return to step 1 and select a new image.
7. Click OK to accept the captured image, as is.

- Alternatively, click and drag inside the image to crop it. The dragged area image size in pixels displays at the bottom of the window.



- Click Crop to crop the image to the defined size.



- Click OK to save the file. The new image is saved with the user number (e.g. 22.jpg for user number 22).

Capture device settings

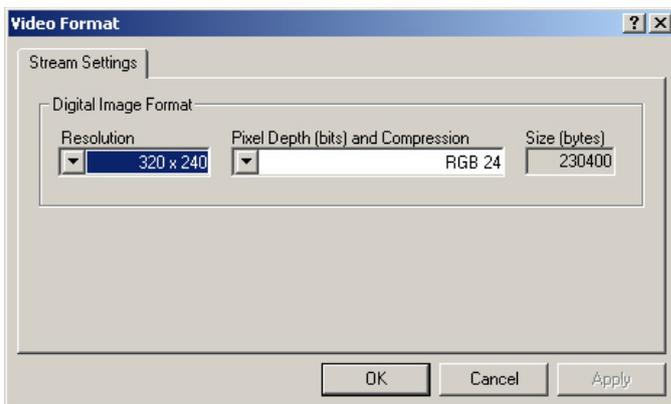
In the Capture User Image window (Figure 10 below) right-click the main image to change the device settings.

Figure 10: Capture User Image window right-click menu

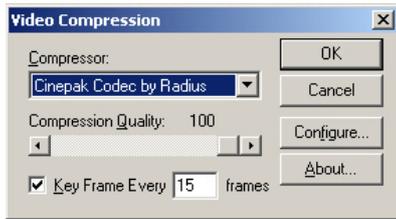


From the right-click menu select the following options:

- Preview (default setting) to use video preview mode to preview the live video before doing the capture.
- Overlay to use video overlay mode (if supported by your system) to preview the live video before doing the capture. Overlay mode provides real time video and better image quality than video preview mode.
- Driver Dialogs > Format to change the image format from the Video Format dialogue box.

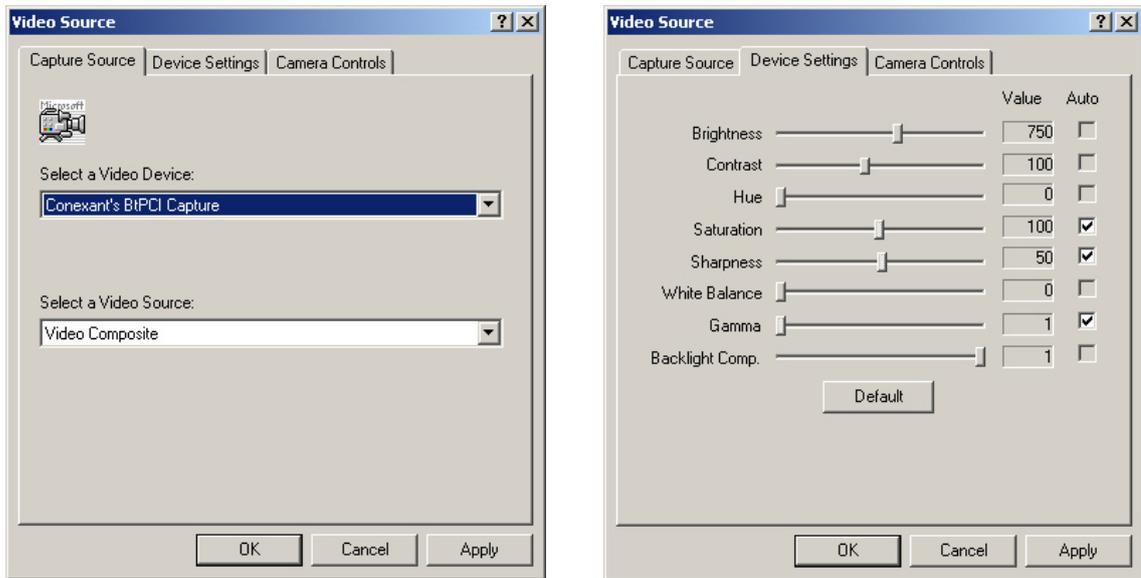


- Driver Dialogs > Compression to change the image compression options from the Video Compression dialogue box.

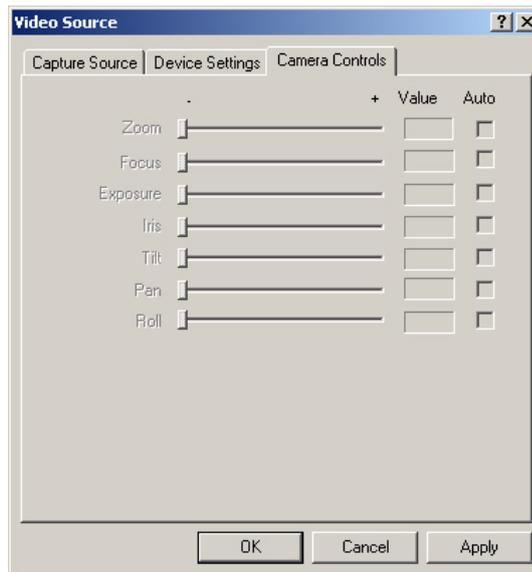


- Driver Dialogs > Source to change the video source options from the Video Source dialogue box (Figure 11 below).

Figure 11: Video Source dialogue box tabs



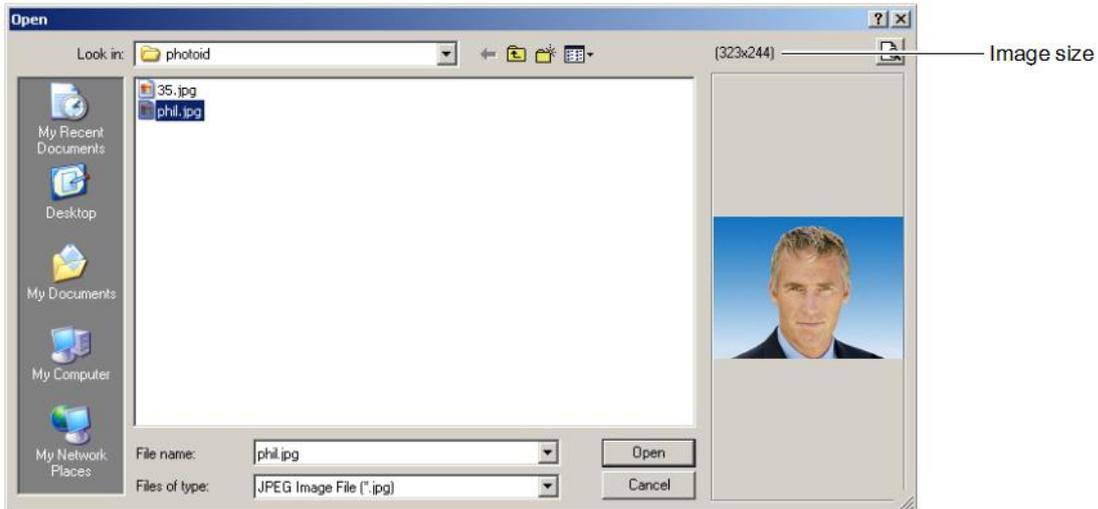
The Camera Controls tab is enabled for PTZ cameras only



Using Import

To import an image:

1. In the User Maintenance window, click the Import button to select and prepare an existing image file.



2. Select a .jpeg or .jpg file and click Open. The selected image displays in the Import User Image window.

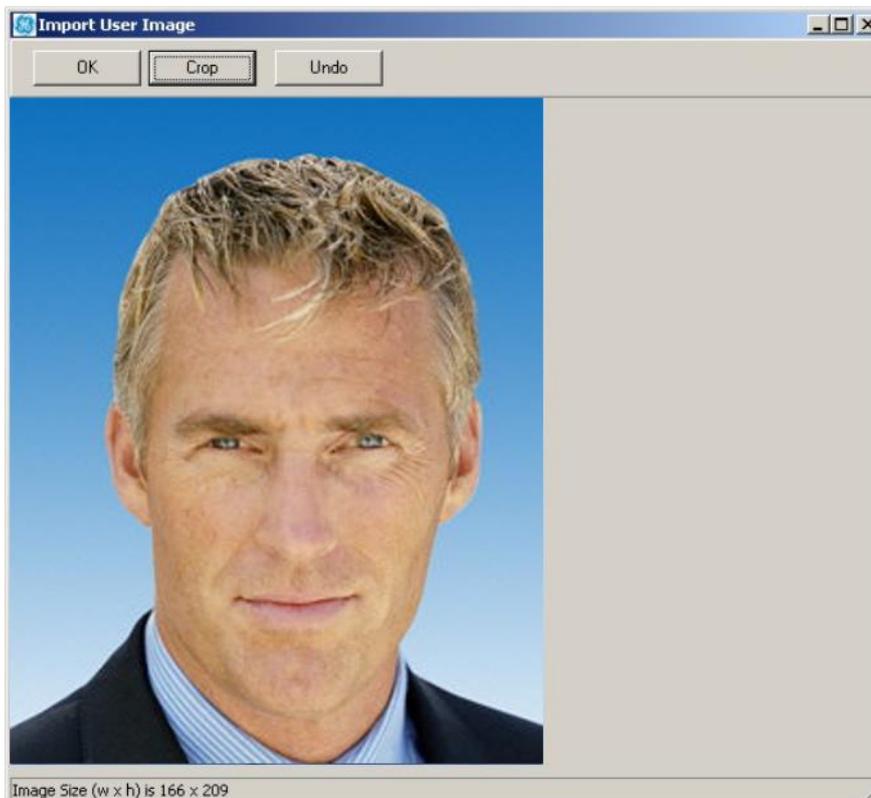


3. Click OK to accept the captured image, as is.

- Alternatively, click and drag inside the image to crop it. The dragged area image size in pixels displays at the bottom of the window.



- Click Crop to crop the image to the defined size.



- Click OK to save the file. The new image is saved with the user number (e.g. 22.jpg for user number 22).

Using Card Layout Editor

Use this command on a Forcefield client to create or modify user card layouts.

Forcefield enables you to create a number of different user card layouts, each of which must be assigned to a department. Departments are created and applied to users in Users > Maintenance.

For example, you might want to use a different coloured background on the card to identify contractors. To do so, you would need to create an appropriate department named, e.g. 'contractor', and then create a card layout with a coloured background for the 'contractor' department.

The Forcefield client Card Layout Editor allows you to:

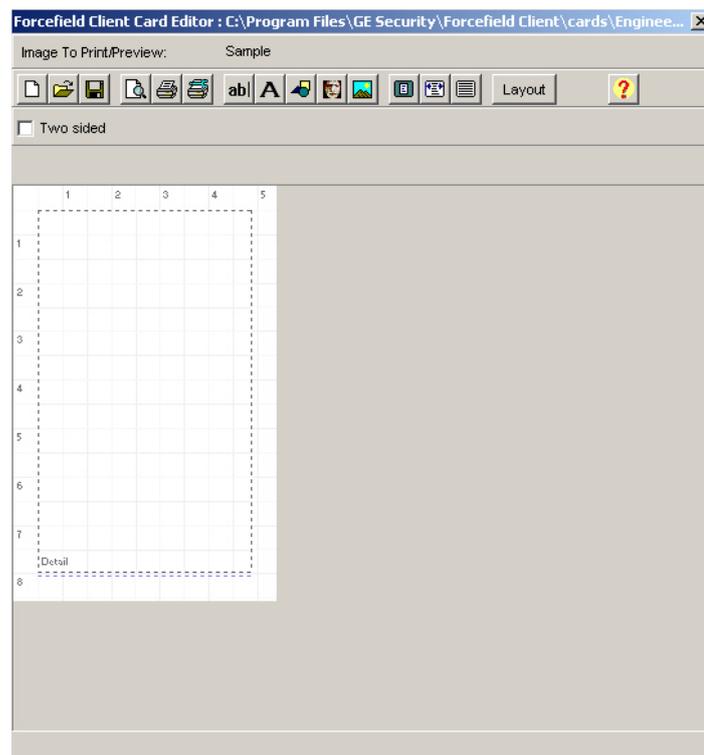
- Automatically add user details to each card from the users database.
- Add text labels
- Add shapes, database images, backgrounds and graphics, and format these
- Save the card layout
- Print photo ID cards on a card printer.

Forcefield client Card Layout Editor Window

Use the command Users > Design Card Layout to open the User Card Layout window. Select the required department and then click Design to launch the Forcefield client Card Layout Editor.

If you need to create a department, you can open the User Profiles window or the User Maintenance window, and then double-click the Department field.

Figure 12: Card Layout Editor window



Commands

The Forcefield client Card Layout Editor uses a right-click menu to access commands. The right-click menu commands are:

- Send to Back—places the selected object behind all others.
- Bring to Front—places the selected object in front of all others.
- New—create a new layout design.
- Open—opens a previously-created layout.
- Save—saves the current layout displayed on screen.
- Save As—saves the current layout displayed on screen, with the option of changing the file name.
- Close—closes the current layout displayed on screen (Forcefield client Card Layout Editor remains open).

Toolbar Buttons

The Forcefield client Card Layout Editor window Figure 12 above has a row of toolbar buttons. From left to right, the buttons are described in Table 4 on page 34.

Table 4: Card Layout Editor toolbar buttons

| Name | Function |
|----------------------|--|
| New Report | Create a new layout design. |
| Load Report | Opens a previously-created layout. |
| Save Report | Saves the current layout displayed on screen. |
| Print Preview | Displays the results of current layout based on default data. |
| Print | Prints the results of current layout based on default data. |
| Printer Setup | Select the Windows system printer that you want to print the card on. |
| Add database field | Click the button and then click inside the dotted border on the card image to add a database field (variable text). A row of editing buttons displays (Figure 13 on page 35). Note the <i>fx</i> button for adding database fields and expressions. |
| Add label | Click the button and then click inside the dotted border on the card image to add a label field (fixed text). A row of editing buttons displays (Figure 13 on page 35). |
| Add shape | Click the button and then click inside the dotted border on the card image to add a shape. A row of shape editing buttons displays (Figure 14 on page 35). Click a button to change the shape. |
| Add user image | Click the button and then click inside the dotted border on the card image to add the user image contained in user records. |
| Add image/background | Click the button and then click inside the dotted border on the card image to add a fixed image such as a background or logo. A Load Image button and a row of selection boxes displays (Figure 15 on page 35). |
| Zoom to fit | Click to adjust the card image to fit the Forcefield client Card Layout Editor window. |
| Zoom to width | Click to adjust the card image to fit the width of the Forcefield client Card Layout Editor window. |
| Zoom to 100% | Click to adjust the card image to view at actual size. |
| Card layout settings | Click to open the Report Settings window. |

Depending on the function selected, a second row of buttons displays Figure 13 on page 35, Figure 14 on page 35, or Figure 15 on page 35).

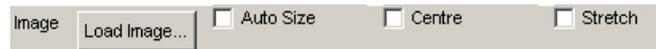
Figure 13: Additional formatting buttons



Figure 14: Shape editing buttons



Figure 15: Load Image button and selection boxes



Creating a Card Layout

To create a photo ID card layout:

1. Unless already done so, create a department to which both the card layout and users can be assigned. Departments are created and applied to users in Users > Maintenance.
2. Select Users > Design Card Layout to open the User Card Layout window.
3. Select the required department and then click Design to launch the Forcefield client Card Layout Editor.
4. Click the Card layout settings button to open the Report Settings window. Ensure that the dimensions are correct for the cards you need to use. See “Setting up the card layout” on page 36 for details.
5. Optionally, if you have duplex card printer (one than prints on both sides of the Photo ID card) and want to create a two-sided layout, select Two sided on the Card Layout Editor window (see Figure 12 on page 33).
6. Add a user image to be loaded from user records when issued cards are previewed or printed. Adjust the size and location of the image as required. See “Adding a user image” on page 36 for details.
7. Optionally, add a background image or other images. Use the right-click command Send to Back to place the image behind all others. Adjust the size and location of the image as required. See “Adding a background image” on page 37 for details.
8. Optionally, add a shape. Adjust the shape, colour, size, and location of the shape as required. See “Adding a shape” on page 37 for details.
9. Add any required text labels to the card and format the text as needed. These labels will print on every card for the particular department. See “Adding text labels” on page 37 for details.
10. Add any required database fields to the card and format the text as needed. These fields will load text from the user records for issued cards. See “Adding database fields” on page 38 for details.

11. Click the Print Preview button to preview a card layout based on default data.
12. When finished editing the card layout, save the layout and exit.

Note: The first time you save a file from Card Layout Editor you may need to navigate to the location of the cards folder.

Setting up the card layout

Ensure that the card layout settings are correct for the cards you need to use. Click the Card layout settings button to open the Report Settings window.

The four main areas on Report Settings window are:

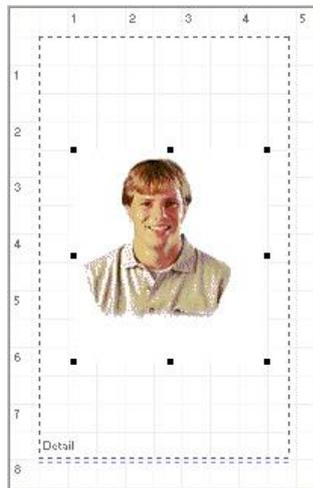
- Paper size: The average access or Photo ID card size is around 54mm x 86mm (portrait is a tall layout, landscape is a wide layout.)
- Margins: Sets the distance of the border from the edge of the card layout. Columns can also be set up on the card to help you position elements in the layout. Columns won't print in your final Photo ID card.
- Other: Use these settings to set the default font for the card layout labels.
- Page frame: This is the dotted grey line on the card layout, which (if selected) prints as a line around the edge of the layout. You can adjust its width, and distance from the edge with the margin settings. If you want no frame to appear, leave the page frame boxes empty. The frame is invisible unless you preview the layout.

Adding a user image

Click the Add user image button and then click inside the dotted border on the card image to add user images from user records.

Card Layout Editor initially uses a default user image as a placeholder. The image is placed inside of a rectangular frame, which has resizing handles when selected.

Figure 16: Card Layout Editor user image preview window



Adding a background image

Click the Add image/background button and then click inside the dotted border on the card image to add a fixed image such as a background or logo.

A Load Image button and a row of selection boxes displays on the toolbar (Figure 15 on page 35):

- Load Image button—click to browse to the image file.
- Auto size—resizes image to its original size.
- Centre—if the image has been shrunk, selecting this displays the image in the centre.
- Stretch—Makes the entire image fit into the box you have defined, dragging the edges.

Adding a shape

Shapes, such as squares, circles and lines can be added and formatted in the card layout editor to print on the card.

Click the Add shape button and then click inside the dotted border on the card image to add a shape. Card Layout Editor initially places a square on the card layout and displays a row of shape editing buttons displays (Figure 14 on page 35). Click a button to change the shape:

- Square (may be filled with colour)
- Circle (may be filled with colour)
- Single vertical line
- Single horizontal line
- Two parallel horizontal lines
- Two parallel vertical lines
- Change the colour of the line
- Change the colour of the fill

Adding text labels

To add text labels to the card layout:

1. Click the Add label button and then click inside the dotted border on the card image to add a label field (fixed text). The text '(none)' is added to the card layout (and displays in the editing field), and a row of formatting buttons displays (Figure 13 on page 35).
2. Replace the text '(none)' in the editing field with the required label text, and then click the [button to accept the changes.
3. Click a formatting button to make the text bold, italic, underlined, etc.
4. Click and drag the text on the card layout image to position it.

5. Click the Print Preview button to preview a card layout based on default data.
6. When finished editing the card layout, save the layout and exit.

Note: The first time you save a file from Card Layout Editor you may need to navigate to the location of the cards folder.

Adding database fields

By using the Add database field button you can get Forcefield to extract user details automatically from the database, and print each user's data on their card. In the following procedure we'll add users' first and last names to a card layout.

To add database fields to the card layout:

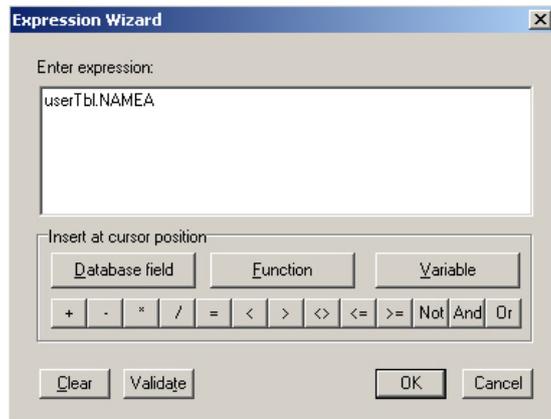
1. Click the Add database field button and then click inside the dotted border on the card image to add a database field (variable text). A row of formatting buttons displays (Figure 13 on page 35). Note the fx button for adding database fields and expressions.
2. Click the fx button to open the Expression Wizard.



3. Click the Database field button to select a database field (see "Database field mapping" on page 40 for details).



4. Select a database field and click OK. The field is added to the Enter expression window. The field NAMEA is the first part of the user name (up to the first space), and the field NAMEB is the second part of the user name (even if the second part uses a space).

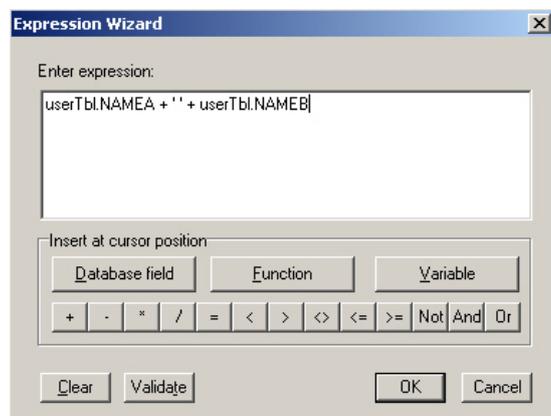


5. Click Validate to verify the expression.



Next, we'll add a space to separate the first and second parts of the name. Spaces, or any other fixed text, is not a database field and so must be enclosed between two apostrophes.

6. Click the + button to add another element to the expression.
7. Type ' for the first apostrophe to enclose the fixed text.
8. Press the spacebar for the space between the first and second parts of the name (the space is fixed text: other characters could be used).
9. Type ' for the second apostrophe (ending the fixed text).
10. Click the + button to add another element to the expression.
11. Repeat step 3 to select and add the database field NAMEB.



12. Click the Validate button to check the results for the currently selected user.



13. Click OK to close the validation window.

14. Click a formatting button to make the text bold, italic, underlined, etc., as required.

15. When finished editing the expression, click OK to close the Expression Wizard.

16. Click the Print Preview button to preview a card layout based on default data.

17. When finished editing the card layout, save the layout and exit.

Note: The first time you save a file from Card Layout Editor you may need to navigate to the location of the cards folder.

The Expression Wizard has many more features than described here. If you need help using the Expression Wizard, please contact technical support.

Database field mapping

The database fields displayed in Expression Wizard correspond to the User Maintenance window as described in Table 5 below.

Table 5: Relationship between Expression Wizard data and User data

| Expression Wizard field | User Maintenance window field |
|-------------------------|--|
| NAMEA | First part of the name field (up to the first space) |
| NAMEB | Second part of the name field (even if the second part uses a space, e.g. 'Van Dam') |
| POSITION | Position |
| DEPARTMENT | Department |
| USERDEFINED | The label of this field in the User Maintenance window is determined by the setting in Admin > Configuration > Configuration > User button > User Defined Field Title value. |
| PHONE | Phone |
| EXT | Ext |
| AFTHOURS | Phone (AH) |
| USERNUMBER | User |

| Expression Wizard field | User Maintenance window field |
|--------------------------------|--|
| MEMBER_DATA_1 | Value of the field on the User Maintenance window, the label of which is the value of the Data 1 field for the user's member. |
| ... | As above for Data 2 through Data 9 fields. |
| MEMBER_DATA_10 | Value of the field on the User Maintenance window, the label of which is the value of the Data 10 field for the user's member. |
| USER_STATUS | Status |
| USER_TYPE | Type |
| PROFILE | Profile |
| PROF_END_DATE | Profile end date (day month year) |
| ALT_PROFILE | Alt Profile |
| MEMBER | Member |
| BEGIN_DATE | Active from date (day month year) |
| EXPIRY_DATE | Active to date (day month year) |
| TRACE | Prints "Traced" if the user flag Trace is checked. |
| CARD_ONLY | Prints "Card Only" if the user flag Card Only is checked. |
| LONG_ACCESS | Prints "Long Access" if the user flag Long Access is checked. |
| PRIVILEGED | Prints "Privileged" if the user flag Privileged is checked. |
| LOCKOUT_TYPE | Prints the programmed lockout type (e.g. "Not Timed"). |

Chapter 4

Integrating automatic event email

Summary

This chapter describes how to set up Forcefield to send email messages when alarms or other events are detected.

Content

| | |
|-------------------------------|----|
| Overview | 44 |
| Adding an email address | 44 |

Overview

Forcefield can be set up to send email messages when an event occurs. One or more emails can be sent with each event.

Example of automatic email message text (where “Collins_3” is the Challenger ID and “Vic/CollinsSt/L3_RmE17” is the Area ID):

```
16/06/2004 15:48:51 Incident 4773 Alarm  
Vic/CollinsSt/L3_RmE17  
Reported from Collins_3 at 16/06/2004 15:48:51
```

In this procedure, it is necessary to create a new Computer Category (or alter one that was previously created). Computer Categories tell Forcefield how to handle events. Forcefield has default Computer Categories that cannot be modified, and because they cannot be modified it is necessary to create a new Computer Category that can be modified.

Complete the following tasks to set up automatic email messages:

1. Save the email server IP address in Admin > Configuration > Forcefield Configuration.
2. Add the email address(es) in the Forcefield email address book. This is described in “Adding an email address” below.
3. Set up a new computer category for events with email. This is described in “Adding a computer category for paging or email support” on page 58.
4. Program the Challenger device to use the new computer category. This is described in the *Forcefield Operators Manual*, see Challenger > Challenger Programming.
5. Create a page or email event trigger. This is described in “Creating a ‘Paging By Event’ trigger” on page 58.

Adding an email address

Add new email addresses to the Forcefield email address book. Email addresses have a number, ID, and email address.

Email addresses from the Forcefield email address book can be selected to automatically receive notification of pre-defined events.

To add an e-mail address to the Forcefield email address book:

1. Select Databases > Email Addresses. The email address screen displays.
2. Enter an ID (e.g. Fred Jones) and the email address.
3. Press F5 to save.

Chapter 5

Integrating intercom

Summary

This chapter describes how to program Forcefield to be used with one of the following types of intercom equipment:

- Commend GE 800 IP intercom
- Jacques 550 Series analogue intercom

It does not explain how to design, install, or implement an intercom system.

Note: In order to use these features, you must purchase and install the appropriate intercom license modules.

Content

| | |
|---|----|
| Intercom system overview | 46 |
| Forcefield intercom interface | 47 |
| Using the Forcefield graphical maps | 47 |
| Using the Forcefield Speed Bar intercom buttons | 48 |
| Integrating a Commend IP intercom system | 49 |
| Integrating a Jacques intercom system | 50 |

Intercom system overview

From Forcefield’s point of view, intercom systems consist of intercom masters and intercom slaves. Intercom masters are used by operators to answer calls that come from intercom slaves and from other intercom masters.

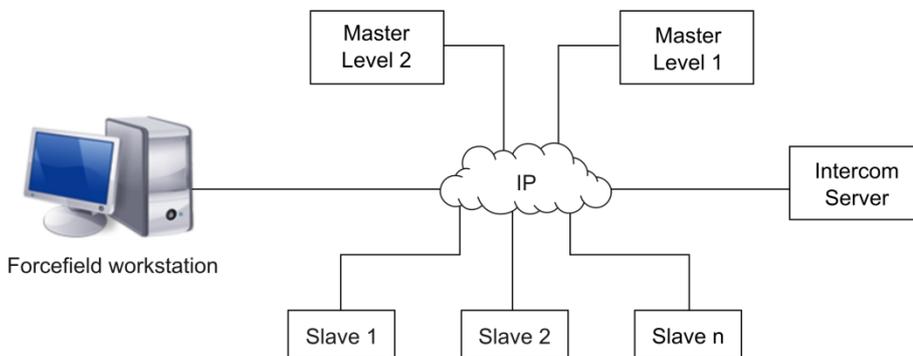
There can be two levels of intercom masters, numbered 1 (lowest authority) and 2 (highest authority). Both levels of intercom masters can receive calls from slave intercoms. When an intercom master level 1 operator is logged off, all calls that would normally go to an intercom master level 1 are automatically diverted to the intercom master level 2.

Intercom slaves are the system’s remote units, typically located near doors, to provide a means of requesting two-way communication. The functionality of intercom slaves varies depending on the hardware and the intended purpose. For example, an intercom slave might be configured to be only a public address (PA) annunciator, to provide background music, and so on.

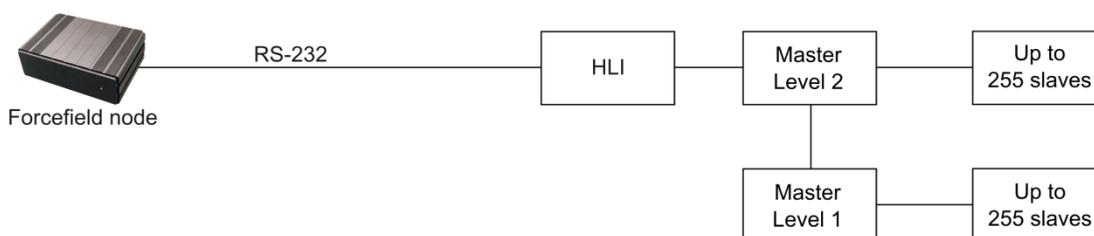
Forcefield provides an integrated user interface for the intercom system. A Forcefield operator can answer or initiate calls via intercom LAPs placed on graphical maps. New calls can be displayed as flashing icons on the Speed Bar, and the operator can immediately go to the associated map when answering a call. Multiple calls are queued for the operator’s attention by priority and sequence.

Figure 17: Comparison of intercom system topologies

Topology of a Commend GE 800 IP intercom system



Topology of a Jacques 550 intercom system



Forcefield intercom interface

The intercom system is used on Forcefield via the following graphical elements:

- Each intercom is represented by a Live Animation Point (LAP) image on a Forcefield graphical map.
- Forcefield Speed Bar buttons allow quick access to calls, the intercom map, and for radio and call volume controls.

Using the Forcefield graphical maps

Intercom masters and slaves can be added to Forcefield maps, where each intercom's location is marked by an icon.

Intercom calls to a Forcefield workstation are made by pressing a call button on a slave unit (or by initiating a call from another audio workstation). When a call is requested, the associated intercom LAP flashes pink, and the "Go To Intercom Map" button on the Forcefield Speed Bar also flashes pink. When flashing, the intercom is said to be waiting.

If an additional intercom call is requested whilst the intercom is waiting, Forcefield automatically queues the call. Waiting calls are displayed according to the intercom system used:

- For Jacques intercoms Forcefield indicates one call waiting at a time, in the sequence initiated.
- For Commend intercoms Forcefield indicates all waiting calls simultaneously. Calls are answered in priority and sequence order, when answered via the "New Alarm or Call" Speed Bar button.

Click the flashing intercom LAP on the map to automatically:

- Switch the video camera assigned to the intercom to the workstation's intercom monitor.
- Open the intercom's call channel.

Note: The intercom monitor is defined on a workstation basis. Use the Databases > Computer Equipment > Workstations command, and then click the Video button, to create a title to be displayed on Graphics Map for the intercom monitor, and to select the monitor to be used.

When not flashing, the intercom is said to be inactive. The operator selects an inactive intercom icon to switch the camera associated with the intercom to the intercom monitor. The options available to the operator are as follows:

- Cancel. Closes the menu.
- Open Call. The options associated with an active call become available.
- Open Door. Opens the door. The intercom monitors are cleared after a configurable period. The system may be configured to require a confirmation for the open door command.

- Audio Monitor On. Starts audio monitoring of a selected intercom.
- Audio Monitor Off. Stops audio monitoring of a selected intercom.
- Disable Call Button. Disables the call button and set the intercom icon to yellow. The option toggles to 'Enable Call Button' to reverse the command. For Commend intercoms, an alarm periodically reminds the operator that the intercom is isolated (configured in Admin > Configuration > Configuration > CCTV/Intercom).

The active call options available to the operator are as follows:

- Close Call. Ends the call and clears the intercom monitors after a configurable period.
- Open Door. Opens the door and immediately closes the call. The intercom monitors are cleared after a configurable period. The system may be configured to require a confirmation for the open door command.

Using the Forcefield Speed Bar intercom buttons

The Forcefield Integration Technician must add the buttons listed in Table 6 below to the Forcefield Speed Bar. Configuring the Forcefield Speed Bar is described in the *Forcefield Operators Manual*.

Table 6: Forcefield Speed Bar intercom buttons

| Button | Operation |
|---------------------------|---|
| Go To Intercom Map | Flashes pink when an intercom call is waiting to be answered. The operator clicks the button to go to the map containing the icon of the intercom that is currently waiting to be answered. |
| Intercom Radio 1 | Radio channel 1 selection |
| Intercom Radio 2 | Radio channel 2 selection |
| Intercom Radio 3 | Radio channel 3 selection |
| Intercom Radio Off | Turns off the radio |
| Intercom Volume Down | Reduces the radio volume |
| Intercom Volume Up | Increases the radio volume |
| Intercom Call Volume Down | Reduces the current call volume |
| Intercom Call Volume Up | Increases the current call volume |

Integrating a Commend IP intercom system

To integrate a Commend intercom system, you'll need to understand the following basic concepts.

- The Commend intercom system used by Forcefield is a multi-level hierarchical system. Forcefield supports levels 1 and 2 intercom masters.
- Forcefield communicates with the intercom system via IP to a Commend GE 800 Intercom Server.
- A Forcefield TCP/IP host record is used to store the connection details (IP address) of the Commend GE 800 Intercom Server.
- Intercom masters level 1 are located near Forcefield client workstations and can communicate with other intercom masters and slaves via IP.
- When a Forcefield operator at an intercom master level 1 is logged off, all intercom calls to the intercom master level 1 are automatically diverted to the intercom master level 2.
- Slave intercoms are located near doors or in rooms and communicate with the intercom masters via IP.

The first step is to set up the intercom records for masters and slaves. Then, build a map in Forcefield showing the position of the intercoms. For more information about setting up maps, see the *Forcefield Operators Manual*.

Integration steps

Unless already done so, create a Forcefield TCP/IP host record with the IP address of the Commend GE 800 Intercom Server.

See the *Forcefield Operators Manual* for more information on configuring ports.

The overall process of integrating a Commend intercom system is as follows:

1. Select Databases > Intercoms > Intercom Master. The Intercom Master screen displays.
2. Program the intercom master level 2 and give it an ID.
3. In the Comms Port/Host field select the TCP/IP host record for the Commend GE 800 Intercom Server.
4. Program any intercom masters level 1 and specify the intercom master level 2 ID in the Higher Master field.
5. Select Databases > Intercoms > Intercom Slave. The Intercom Slave screen displays.
6. Program intercom slaves and specify the appropriate intercom master's ID in the Master field.

Integrating a Jacques intercom system

To integrate a Jacques intercom system, you'll need to understand the following basic concepts.

- The Jacques intercom system used by Forcefield is a multi-level hierarchical system. Forcefield supports levels 1 and 2 master intercoms.
- Forcefield communicates with intercom consoles or control units via a single intercom master level 2 connected to one of the Forcefield node's serial ports via a Jacques HLI.
- A Forcefield serial port record is used to store the connection details of the Jacques intercom system.
- Up to 14 intercom masters level 1 are located near Forcefield clients workstations and are connected to the intercom master level 2.
- An intercom master level 1 can make intercom calls only to its intercom slaves or to the intercom master level 2.
- When a Forcefield operator at an intercom master level 1 is logged off, all intercom calls to the intercom master level 1 are automatically diverted to the intercom master level 2.
- Slave intercoms are located near doors or in rooms and communicate with the intercom masters.

The first step is to set up the intercom records for masters and slaves. Then, build a map in Forcefield showing the position of the intercoms. For more information about setting up maps, see the *Forcefield Operators Manual*.

Integration steps

Integrate a Jacques intercom system so that operators can respond to and make calls on Jacques intercom systems.

Unless already done so, create an intercom port with the appropriate values from the intercom system. The required values are:

- Port type = Intercom
- Node = The node number that the Intercom is connected to
- Handshake = None
- Baud = 9600
- Parity = None
- Data Bits = 8

See the *Forcefield Operators Manual* for more information on configuring ports.

The overall process of integrating a Jacques intercom system is as follows:

1. Select Databases > Intercoms > Intercom Master. The Intercom Master screen displays.
2. Program the intercom master level 2 and give it an ID.

3. In the Comms Port/Host field select the Com port record for the Jacques intercom system.
4. Program any intercom masters level 1 and specify the intercom master level 2 ID in the Higher Master field.
5. Select Databases > Intercoms > Intercom Slave. The Intercom Slave screen displays.
6. Program intercom slaves and specify the appropriate intercom master's ID in the Master field.

Chapter 6

Integrating paging and duress

Summary

This chapter describes how to set up Forcefield to send automatic email messages or to page an Ascom Nira paging system when an event occurs.

Note: In order to use these features, you must purchase and install the TS9112 Pager/Duress license module.

Content

| | |
|--|----|
| Integrating Paging | 54 |
| Integrating an Ascom Nira duress system | 54 |
| Duress system overview | 54 |
| Adding a Computer Category for duress support | 56 |
| Adding an Ascom Nira duress station | 56 |
| Adding an Ascom Nira duress system locator | 57 |
| Adding an Ascom Nira duress transceiver | 57 |
| Adding a computer category for paging or email support | 58 |
| Creating a 'Paging By Event' trigger | 58 |

Integrating Paging

In this procedure, it is necessary to create a new Computer Category (or alter one that was previously created). Computer Categories tell Forcefield how to handle events. Forcefield has default Computer Categories that cannot be modified, and because they cannot be modified it is necessary to create a new Computer Category that can be modified.

To set up automatic email messages or duress system paging:

1. Integrate the Ascom Nira system into Forcefield. Refer to “Integrating an Ascom Nira duress system” below.
2. Set up a new computer category for events with paging. Refer to “Adding a computer category for paging or email support” on page 58.
3. Program the Challenger device to use the new computer category. Refer to Challenger Programming in the *Forcefield Operators Manual*.
4. Create a ‘Paging by Event’ trigger. Refer to “Creating a ‘Paging By Event’ trigger” on page 58.

Integrating an Ascom Nira duress system

This guide describes how to integrate Ascom Nira system devices into Forcefield. It does not explain how install or implement Ascom Nira system devices.

The task of integrating an Ascom Nira Duress system consists of the following procedures, to be performed in the following sequence:

1. “Adding a Computer Category for duress support” on page 56
2. “Adding an Ascom Nira duress station” on page 56
3. “Adding an Ascom Nira duress system locator” on page 57
4. “Adding an Ascom Nira duress transceiver” on page 57
5. “Adding a computer category for paging or email support” on page 58
6. “Creating a ‘Paging By Event’ trigger” on page 58

Duress system overview

The duress system uses the following components:

- A duress station connected to a Forcefield computer.
- A number of duress system locators placed at various locations in a facility. Each locator is identified by an ID code on the equipment.
- A duress transceiver (or transmitter), typically worn at the waist, by personnel required to move through the facility. Each transceiver is identified by an ID code on the equipment.

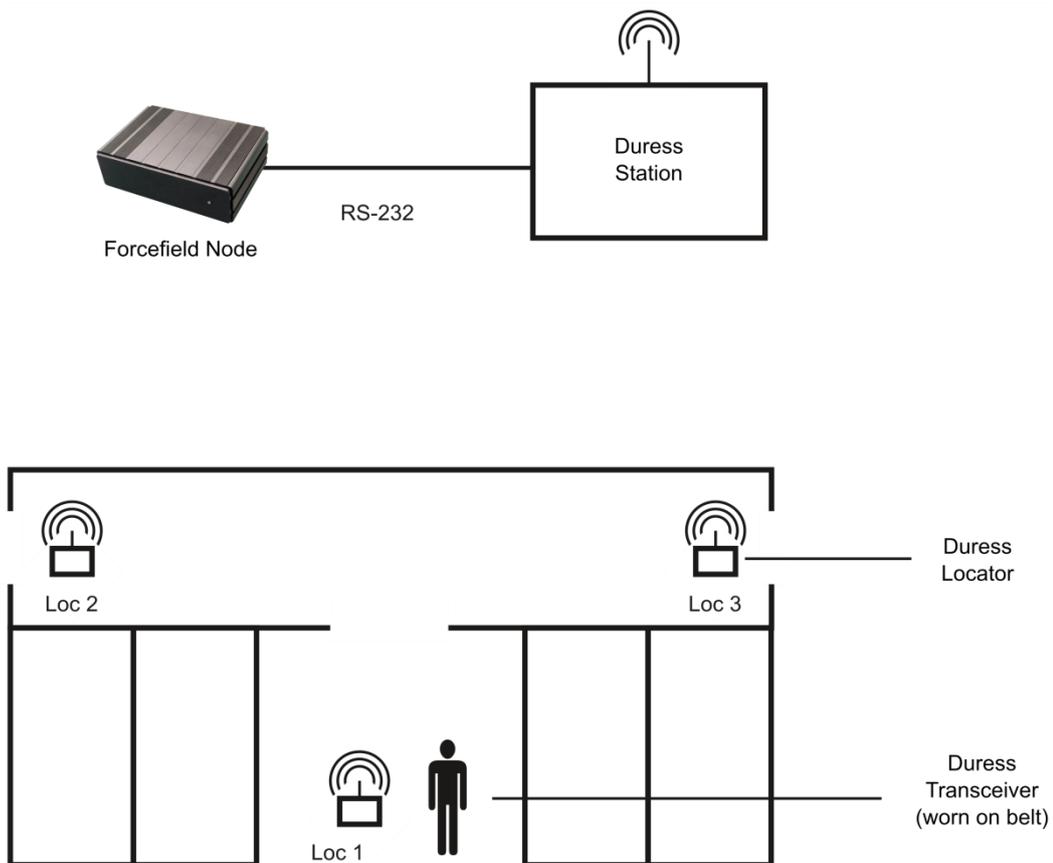
Each time a person wearing a duress transceiver passes a duress locator, the transceiver receives a location from the locator. If an alarm occurs (such as “Man Down”, “Alarm Button Pressed”, “No Motion”, etc.) the location and the previous location are sent to the duress station. Forcefield uses the two locations to change the colours of the relevant duress locator icons on the alarm map so that the operator has an indication of the wearer’s position and direction of travel.

When a duress alarm occurs, the duress station communicates with the Forcefield system and provides:

- The type of alarm (including duress button press, transceiver pulled off, person down, person not moving, person too long at one locator).
- Identity of transceiver.
- Present location.
- Previous location.

The duress system keeps track of two consecutive locations in order to indicate direction of travel as well as present location (Figure 18 below).

Figure 18: Duress system overview



Adding a Computer Category for duress support

In this procedure, it is necessary to create a new Computer Category (or alter one that was previously created). Computer Categories tell Forcefield how to handle events. Forcefield has default Computer Categories that cannot be modified, and because they cannot be modified it is necessary to create a new Computer Category that can be modified.

Note: You must create a new Computer Category. As part of this procedure, you'll need to select each type of duress alarm event, and then clear the Restoral Required field because Ascom Nira does not generate alarm restoral events.

To create a new computer category for Ascom Nira duress:

1. Select Databases > Management Software > Computer Categories > Computer Categories. The Computer Categories screen displays.
2. Click the Computer Category field, type a new name for the Computer Category, and then press ENTER. Forcefield displays a Category type selection list.
3. Select the Category Type "Duress" 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 (e.g. Personal Monitor Alarm) for which you want to program the event settings.
6. Right-click the Restoral Required box to clear it.
7. Press F5 to save the changes.

Adding an Ascom Nira duress station

Unless already done so, create a new Duress Computer Category, which has the Restoral Required box cleared. See "Adding a Computer Category for duress support" above.

Unless already done so, create a duress port with the appropriate values from the duress station. The required values are:

- Port type = Duress
- Node = The node number that the Duress Station is connected to
- Handshake = None
- Baud = 9600
- Parity = Even
- Data Bits = 8

See the *Forcefield Operators Manual* for more information on configuring ports.

To add an Ascom Nira duress station:

1. Select Databases > Duress > Duress Stations.
2. Select or add a duress system, e.g. New Ascom Nira.
3. Click the protocol arrow, and select Ascom 960.
4. In the System ID field, type an Ascom Nira System ID (hex value supplied by Ascom Nira).
5. Select port, member, computer category, etc.
6. Press F5 to save.

Adding an Ascom Nira duress system locator**To add an Ascom Nira duress system locator:**

1. Select Databases > Duress > Duress Locators.
2. Select a duress system.
3. Select an address and ID.
4. Enter a description of the locator.
5. Press F5 to save the record.

Adding an Ascom Nira duress transceiver

Unless already done so, create a new Duress Computer Category, which has the Restoral Required box cleared. See “Adding a Computer Category for duress support” on page 56.

To add an Ascom Nira duress transmitter:

1. Select Database > Duress > Duress Transmitter.
2. From the Duress transmitter screen select a duress system.
3. Type the identity (supplied by Ascom Nira).
4. Select an ID from the ID field.
5. Click the Type arrow, and then select the type of transmitter. If you select U922 (which has two-way communication), then call number fields are provided.
6. Select a duress type of computer category that has been amended to not require restorals for the alarm conditions. The Ascom Nira does not generate alarm restoral events.
7. Press F5 to save the record.

Adding a computer category for paging or email support

In this procedure, it is necessary to create a new Computer Category (or alter one that was previously created). Computer Categories tell Forcefield how to handle events. Forcefield has default Computer Categories that cannot be modified, and because they cannot be modified, it is necessary to create a new Computer Category that can be modified.

As part of this procedure, you'll need to select the type of event, and then select Allow Paging (not applicable to some event types).

To create a new computer category to page or email on events:

1. Select Databases > Management Software > Computer Categories > Computer Categories. The Computer Categories screen displays.
2. Click the ID field, type a new name for the Computer Category, 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 (e.g. Duress) for which you want to program the event settings.
6. Right-click the Allow Paging box to select it.
7. Press F5 to save the changes.

Creating a 'Paging By Event' trigger

Program a Paging by Event trigger to page an Ascom Nira duress system or to send an email.

To create an event trigger:

1. Select Triggering > Event Paging, and then the Paging by Event screen displays.
2. Type a new ID or select one.
3. Type a new description for the event.
4. Click the Page on Event arrow, and then select an event type.
5. Press F5 to save the changes.
6. Click Destinations, and then the Paging Destination screen displays.
7. Complete the ID, type, and address fields.
8. For the type of output, select Ascom Duress or Email address. If you select Ascom Duress, also select an alarm option from the list (e.g. the number of beeps or a siren).
9. Press F5 to save the changes. Complete a new paging destination screen for each email destination you need to add.

Chapter 7

Integrating CCTV

Summary

This chapter describes how to integrate Forcefield with closed-circuit television (CCTV) systems.

Content

| | |
|---|----|
| Overview | 60 |
| Video switcher system..... | 61 |
| Overall process..... | 62 |
| Automatically displaying CCTV images for alarms | 63 |
| Controlling CCTV from Forcefield events | 64 |
| DVR systems | 65 |
| Creating a computer category..... | 65 |
| Using the DVR system..... | 65 |
| Viewing CCTV footage from a DVR | 66 |
| Controlling the DVR from Forcefield events | 72 |
| Viewing exported video footage | 72 |
| Teleste Video Management system..... | 74 |
| Overview..... | 74 |
| Integrating Teleste into Forcefield | 74 |

Overview

In Forcefield, the term “CCTV” includes video delivered via a video switcher, legacy DVRs, video service DVRs, and Teleste Video Management system.

The term “video service” refers to the use of plug-in modules to support CCTV equipment from various manufacturers.

Forcefield can be integrated with the following CCTV systems:

- **Video Switcher.** A video switcher is connected via RS-232 to the Forcefield node. External monitor(s) must be used to display CCTV footage. Refer to “Video switcher system” on page 61 for details.
- **Legacy DVRs.** Forcefield client can interface via Ethernet (IP) connections to legacy DVRs (such as DVMRe, SymDec, and SymSafe). Legacy DVRs are supported natively in Forcefield. Refer to “DVR system” on page 65 and Appendix C “Integrating legacy DVRs” on page 131 for details.
- **Video Service DVRs.** Forcefield client can interface via Ethernet (IP) connections to DVRs supported via plug-in modules. Refer to “DVR system” on page 65 and Appendix D “Integrating DVRs” on page 141 for details.
- **Teleste Video Management system.** Forcefield client can interface via IP connection to Teleste. Refer to “Teleste Video Management system” on page 74 for details.

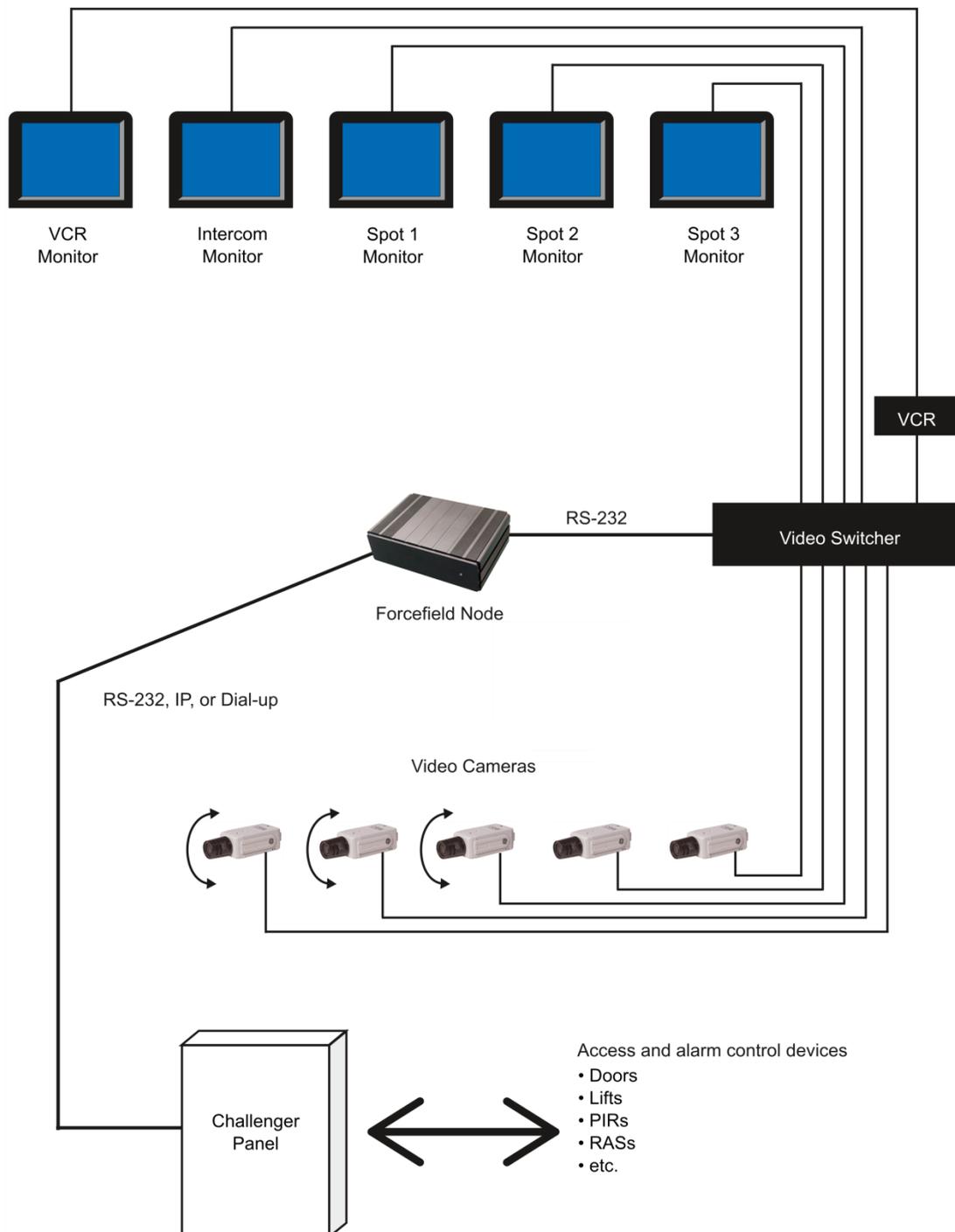
In order to use these features, you must purchase and install the appropriate license modules. Refer to the Forcefield datasheet for details.

Notes:

- Restart the Forcefield server after installing a new or modified license module.
- DVR integration requires the appropriate versions of Forcefield client. Before you install Forcefield client on a Windows computer you must first remove any earlier versions, if present. Go to Start > Control Panel > Add or Remove Programs and remove any instances of Forcefield client. (Record the station key and other details for reuse from the Client Preferences screen before you remove Forcefield client.)

Video switcher system

Figure 19: System diagram of basic CCTV system



The video switcher must be physically connected to the Forcefield node, but the CCTV system is controlled from Forcefield clients.

The optional VCR monitor is selected from the pop-up menu for a camera LAP. When selected, the signal from the selected camera is routed through the VCR, and then the workstation's VCR monitor displays the image that is being recorded.

Overall process

This section describes the overall process of integrating video switcher CCTV devices into Forcefield.

Refer to the Databases > Video > Matrix Video menu section in the *Forcefield Operators Manual* for details about programming video cameras, monitors, camera presets, and switchers. The information provided in this section is only a summary.

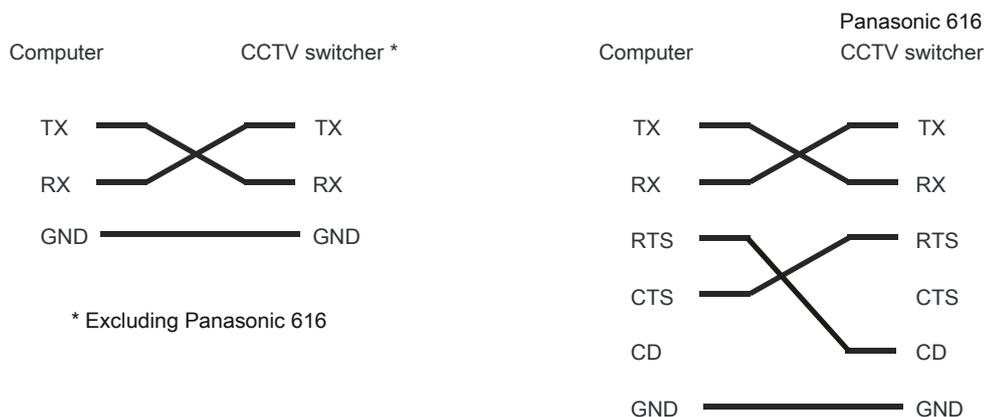
Overall process for integrating CCTV into Forcefield:

1. Use the Databases > Video > Matrix Video > Switchers command to program a CCTV switcher. Leave the Enabled selection unchecked so that you can program the CCTV switcher, cameras, monitors and presets before actually physically connecting the equipment to the Forcefield system.
2. If not previously done, define a video switcher port.
3. Use the Databases > Video > Matrix Video > Cameras command to program a video camera. Select the CCTV switcher (defined in step 1) to which this camera is connected, and specify whether the camera has pan-tilt-zoom (PTZ) control.
4. If applicable, use the Databases > Video > Matrix Video > Presets command to program and name predefined views for PTZ cameras (defined in step 2). TIP: The names that you assign to a presets 1 through 5 are added to the camera's pop-up menu on maps displaying the camera.
5. Use the Databases > Video > Matrix Video > Monitors command to program the video monitors. Select the CCTV switcher (defined in step 1) to which this monitor is connected.
6. Use the Databases > Computer Equipment > Workstations command, and then click the Other button to ensure that the Disable CCTV Control selection is not checked.
7. Use the Databases > Computer Equipment > Workstations command to specify the video monitors to be used by the workstation. TIP: The first programmed spot monitor is used to display the image from the camera associated with the point in alarm when the operator views the Alarm Detail screen. From the Forcefield Workstations window, click the Alarms button and then select Switch Cam. to Mon. on Detail.
8. If applicable, use the Databases > Computer Equipment > Workstations command to select the intercom monitor to display the feed from the intercom camera and to create a title to be displayed on the Graphics Map for the intercom monitor.
9. If applicable, use the Databases > Computer Equipment > Workstations command to select the VCR monitor to be used to display the feed from the VCR.

10. Use the Admin > Configuration > Forcefield Configuration command, and then click the CCTV/Intercom button to configure the following options:
 - Door Open Blank Camera Delay. When the operator opens a door associated with an Intercom from a graphics map, the monitor displays video from the associated camera. This value is the number of seconds until 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.
11. Use the Databases > Computer Equipment > Ports command and configure a Forcefield node port as follows:
 - The port type is VideoSwitcher RS232
 - Configuration settings to suit the switcher (e.g. at the time of writing, the settings for a Kalatel KTD-348 are: no handshake, 9600 baud, no parity, 8 data bits).
12. Connect the cameras, monitors, and switchers to the Forcefield system.

The switcher must be connected to the correct serial port on the Forcefield node via an RS-232 cable. Details of serial port connections are described in Figure 20 below.
13. Use the Databases > Video > Matrix Video > Switchers command, and then check the Enabled selection to enable a CCTV switcher.

Figure 20: CCTV switcher wiring connections



Automatically displaying CCTV images for alarms

Forcefield can automatically display video images on a spot monitor in response to an alarm when the operator opens the alarm detail screen.

Briefly, the following must be in place:

- The workstation must be programmed to have at least one spot monitor (Databases > Computer Equipment > Workstations).

- The workstation must be set up to switch the camera to the spot monitor in response to an alarm. From the Forcefield Workstations window, click the Alarms button and select Switch Cam. to Mon. on Detail.
- The field device in alarm must be programmed to have a video camera (and optionally a preset view). If a preset view is not programmed, then Forcefield will display the camera's preset view 1.

See also “Controlling CCTV from Forcefield events” below for details of using other events to automatically display video images on a spot monitor.

Controlling CCTV from Forcefield events

In addition to displaying video in response to an alarm (see “Automatically displaying CCTV images for alarms” on page 63), you can also program Forcefield to automatically perform CCTV operations when particular events occur. For example, if a door is opened, Forcefield can automatically aim a PTZ camera at the door and display an image on a monitor at the operator's workstation.

This section describes the overall process of programming Forcefield to operate CCTV equipment.

Refer to the Triggering menu section in the *Forcefield Operators Manual* for details about actions associated with video control events.

The overall process for programming Forcefield for CCTV control is:

1. Use the Triggering > Event Trigger command to program an action to be activated by the notification of a Forcefield event (e.g. Door Forced alarm).
2. Click the Action button on the Triggering By Event window to program an action.
3. Program the options required to activate the camera and CCTV switcher to display a preset view when the specified Forcefield event occurs.
4. Click the Action arrow, and then select “Cam to Preset (Matrix)”.
5. Optionally, use the Admin > Tools > Event Simulator command to simulate the specified Forcefield event and to check for the intended outcome.
6. Alternatively, generate the Forcefield event using the actual hardware to check for the intended outcome.

DVR systems

Forcefield 7.1 can be used with the following types of DVR systems:

- Legacy DVRs (such as DVMRe, SymDec, and SymSafe). For integration details, see Appendix C “Integrating legacy DVRs” on page 131.
- DVRs via plug-in modules. For integration details, see Appendix D “Integrating DVRs” on page 141.

Creating a computer category

Computer categories tell Forcefield how to handle events.

An event can be used to send an event tag to a DVR. In order to do so, you must create a computer category that can be edited (the standard computer categories are read-only ‘templates’).

The particular type of computer category that you create will be based on the type of equipment (e.g. arming station, door, etc.) that you want to use.

For any given computer category and event, there are two items that you need to program for use with a DVR:

- Select Mgt s/w to tag DVR if Forcefield is to send text to DVR to be recorded as a tag for the event.
- Edit (if required) the event text for the event. The event text will be sent as part of the tag to the DVR when the event occurs.

Using the DVR system

Forcefield can perform the following tasks in relation to a DVR system:

- In response to events, Forcefield sends text to the DVR to be recorded along with video footage from a camera associated with the event. The text can be generated by Forcefield or by a high-level interface such as an intercom system.
- A Forcefield operator working at a Forcefield client computer can display live or recorded footage from a DVR.
- When viewing live footage from a PTZ camera, the operator can control the camera’s view.
- A Forcefield operator working at a Forcefield client computer can search for and display video footage identified by text recorded with the video footage on a DVR.
- When viewing recorded footage, the operator can control the speed and direction of the playback.

Viewing CCTV footage from a DVR

A Forcefield system may interface via Ethernet (IP) connection to a Digital Video Recorder (DVR) and associated CCTV video cameras.

Authorised operators can:

- Access live and recorded video footage from maps (see “Using maps to display video” below).
- 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.
- Display up to 16 images of DVR video on a single screen using multiview. Refer to the section View Groups menu in the *Forcefield Operators Manual* for details.

Note: In order for Forcefield to initiate the recording and tagging of the recorded DVR camera footage for Challenger events such as using a reader, the computer category entry for the event must have the “Mgt s/w to tag DVR” option selected, and the computer category must be assigned to the device. Also, the device (such as an input) generating the event must also have an associated DVR camera programmed in the Video Cam field, as per the example shown in Figure 21 on page 67.

Using the History menu to display video

The History > Show DVR Footage menu contains the following sub-menus:

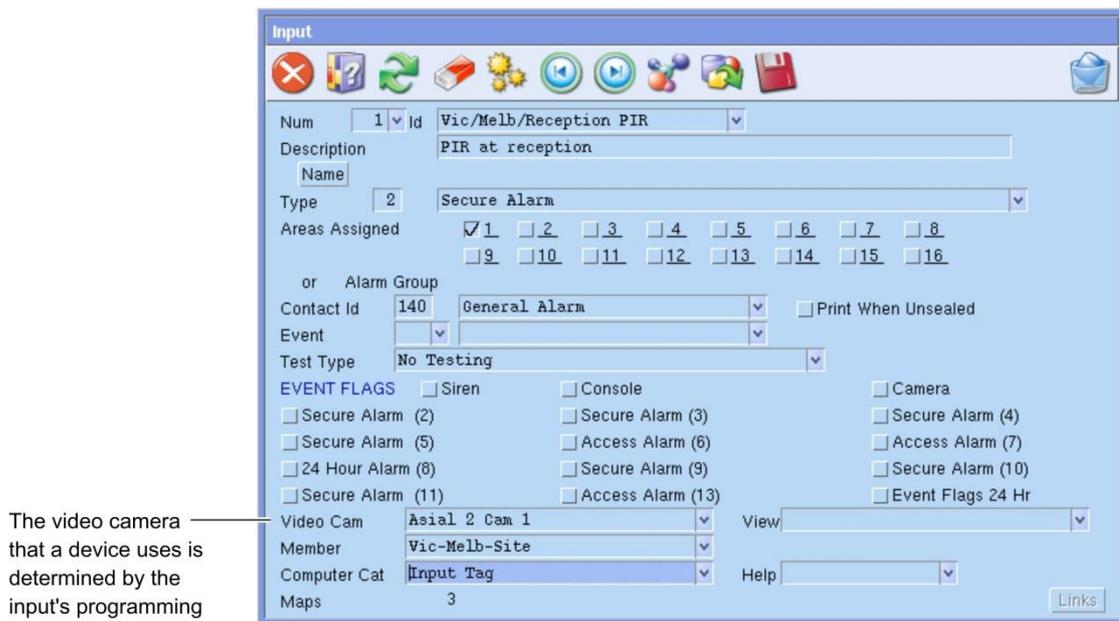
- Tagged Footage
- Time Footage

Refer to History > Show DVR Footage menu in the *Forcefield Operators Manual* for details about using these commands.

Using maps to display video

Maps can contain Challenger equipment devices that have been programmed with an associated DVR video camera (see Figure 21 on page 67 for example).

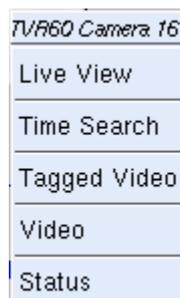
Figure 21: Challenger input device programming



The following steps describe how to find and display video by using the LAP menu Video option (see Graphics > Display map in the *Forcefield Operators Manual*).

Click the LAP image for any device that has a video camera associated with it. The LAP menu displays (Figure 22 below).

Figure 22: LAP menu for a Challenger device programmed with an associated video camera



Click a LAP menu option to perform the following tasks:

- Select Live View to display a live view from the camera (see “Using the LAP menu to display a live view” on page 68)
- Select Time Search to display the Play DVR Time Footage window (“Using the LAP menu to search by time” on page 69)
- Select Tagged Video to display the Tagged Video time span menu (“Using the LAP menu to search by tag” on page 69)
- Select Video to display the Live View option menu (“Using the LAP menu to select a live view” on page 71)

- Select Status to check the current state of the camera.

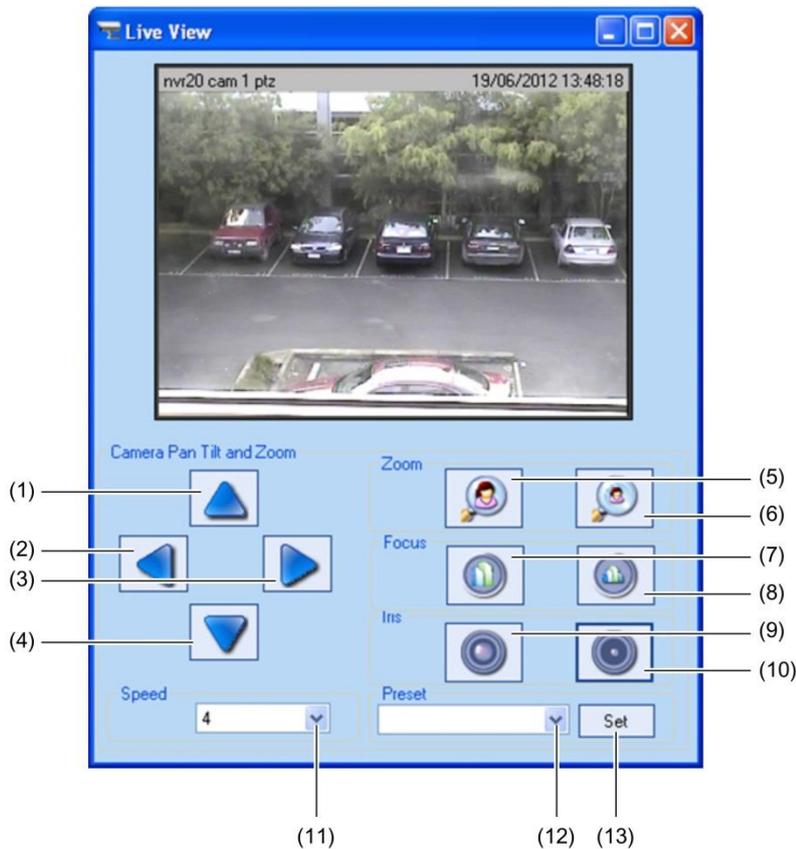
Using the LAP menu to display a live view

Click the LAP image for any device that has a video camera associated with it, and then select Live View.

Note: Figure 23 below indicates a live camera view for a legacy DVR. Live and recorded views for a video service DVR use a video console. Refer to “Show Video Console” in *Forcefield Operators Manual*, REV 14 (or higher) for details of the video console’s interface and controls.

If the camera is a pan-tilt-zoom (PTZ) camera, you can use the controls in Live View.

Figure 23: Live Camera View window for a PTZ camera (for legacy DVR camera)

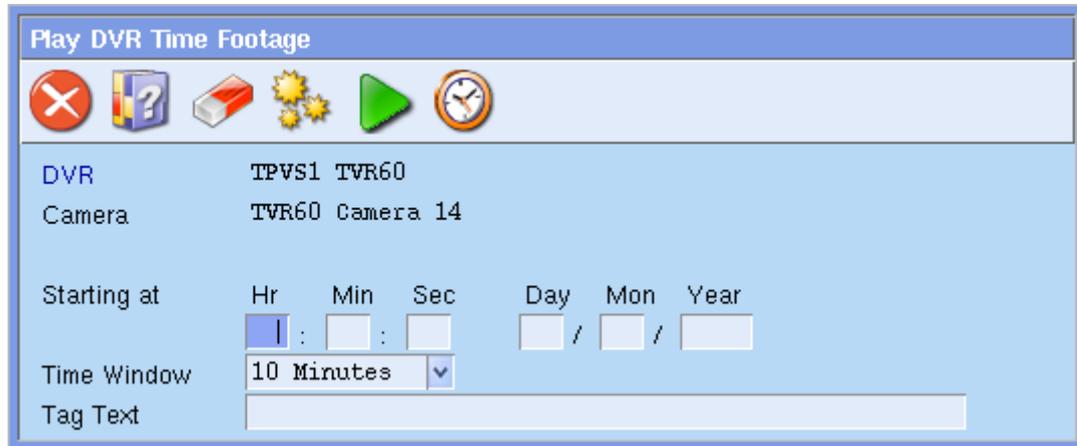


- | | |
|----------------|---|
| (1) Tilt up | (8) Focus far |
| (2) Pan left | (9) Increase iris (increase the amount of light passing through the lens) |
| (3) Pan right | (10) Reduce iris (reduce the amount of light passing through the lens) |
| (4) Tilt down | (11) Click to select a camera movement speed |
| (5) Zoom in | (12) Click to select a preset |
| (6) Zoom out | (13) Click to save a changed preset |
| (7) Focus near | |

Using the LAP menu to search by time

Click the LAP image for any device that has a video camera associated with it, and then select Time Search.

Figure 24: Play DVR Time Footage window



Using the LAP menu to search by tag

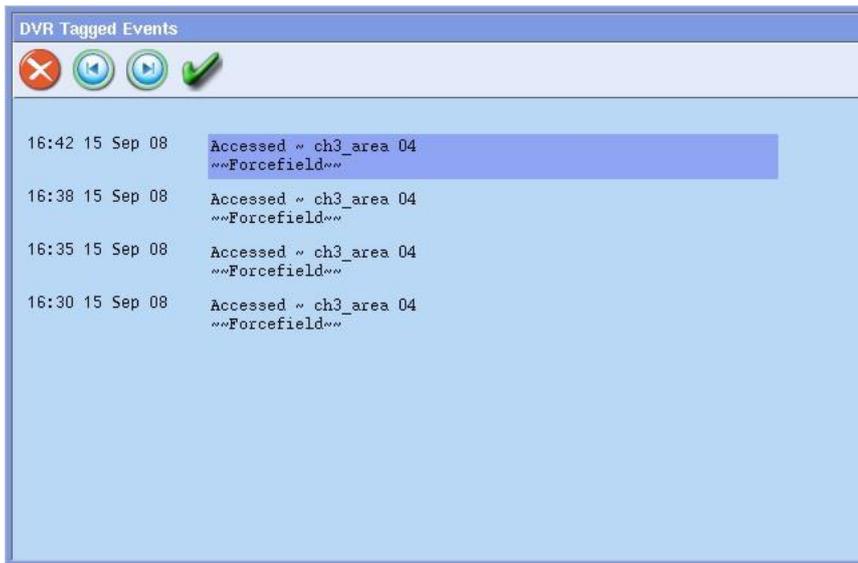
Click the LAP image for any device that has a video camera associated with it, and then select Tagged Video.

Figure 25: Tagged Video time span menu



If recorded video is found within the selected time span, a list of events during that time displays (Figure 26 on page 70).

Figure 26: DVR Tagged Events list



Click an event text field to launch the DVR Recorded Video window (see Figure 27 on page 71).

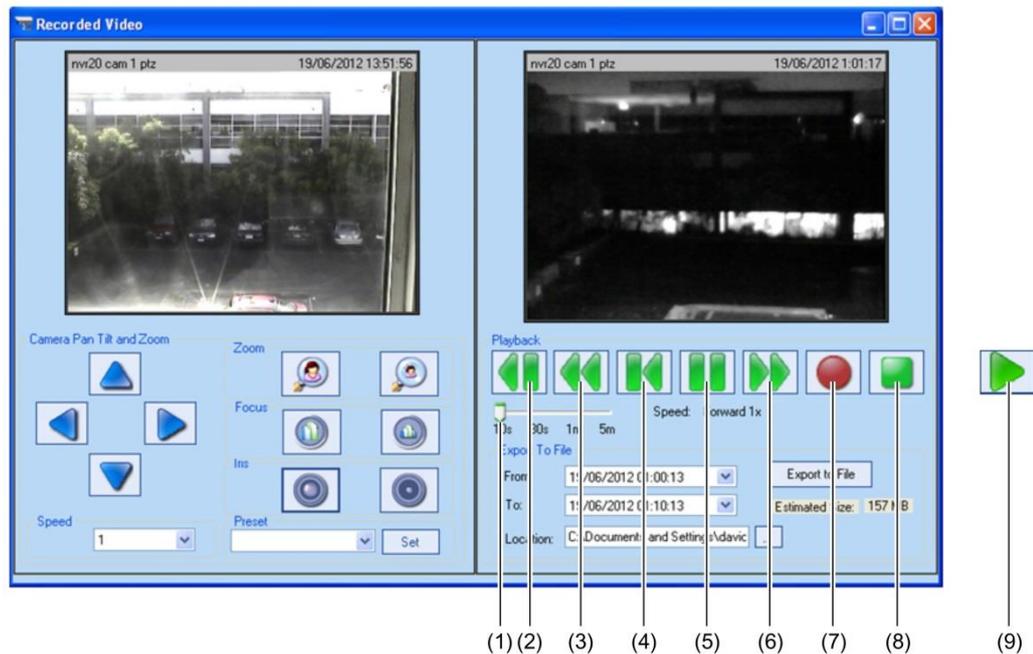
Note: Figure 27 on page 71 indicates a recorded video view for a legacy DVR. Live and recorded views for a video service DVR use a video console. Refer to “Show Video Console” in *Forcefield Operators Manual*, REV 14 (or higher) for details of the video console’s interface and controls.

The DVR 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. Refer to Figure 23 on page 68 for details of the PTZ controls.

Use the VCR buttons to rewind, play backward, play forward, and pause (stop).

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 72 for details.

Figure 27: Recorded Video window (for legacy DVR camera)

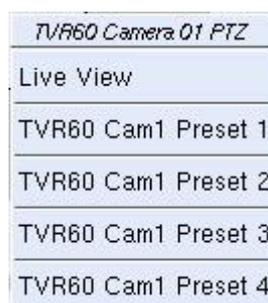


- (1) Jump interval slider
- (2) Jump back by 10 s, 30 s, 1 m, or 5 m, as set by the jump interval slider
- (3) Rewind
- (4) Rewind to the beginning of the event
- (5) Pause (when paused, the Play forward button displays)
- (6) Play fast forward by the multiplier displayed below the button (for example, 2x)
- (7) Mark the start of footage segment to export (the operator must have edit permissions on the Show DVR Footage functions)
- (8) Mark the stop of recorded footage to export, and then to select a storage location for the file
- (9) Play forward (when playing, the Pause button displays)

Using the LAP menu to select a live view

Click the LAP image for any device that has a video camera associated with it, and then select Video.

Figure 28: Live View option menu (options vary depending on assigned presets)



Controlling the DVR from Forcefield events

You can program Forcefield to automatically perform CCTV operations when particular events occur. For example, if a door is opened, Forcefield can automatically aim a PTZ camera at the door and display an image on a Forcefield client workstation.

This section describes the overall process of programming Forcefield to operate CCTV equipment.

Refer to the Triggering menu section in the *Forcefield Operators Manual* for details about actions associated with video control events.

The following is the overall process for programming Forcefield for CCTV control:

1. Use the Triggering > Event Trigger command to program an action to be activated by the notification of a Forcefield event (e.g. Door Forced alarm).
2. Click the Action button on the Triggering By Event window to program an action.
3. Program the options required to activate the PTZ camera and DVR to display a preset view when the specified Forcefield event occurs.
4. Click the Action field and select, for example, Set Multi View.



You must already have the required multi view record programmed. See the Databases > Video > DVR Video > Multiview section in the *Forcefield Operators Manual* for details.

5. Optionally, use the Admin > Tools > Event Simulator command to simulate the specified Forcefield event and to check for the intended outcome. Alternatively, generate the Forcefield event using the actual hardware to check for the intended outcome.

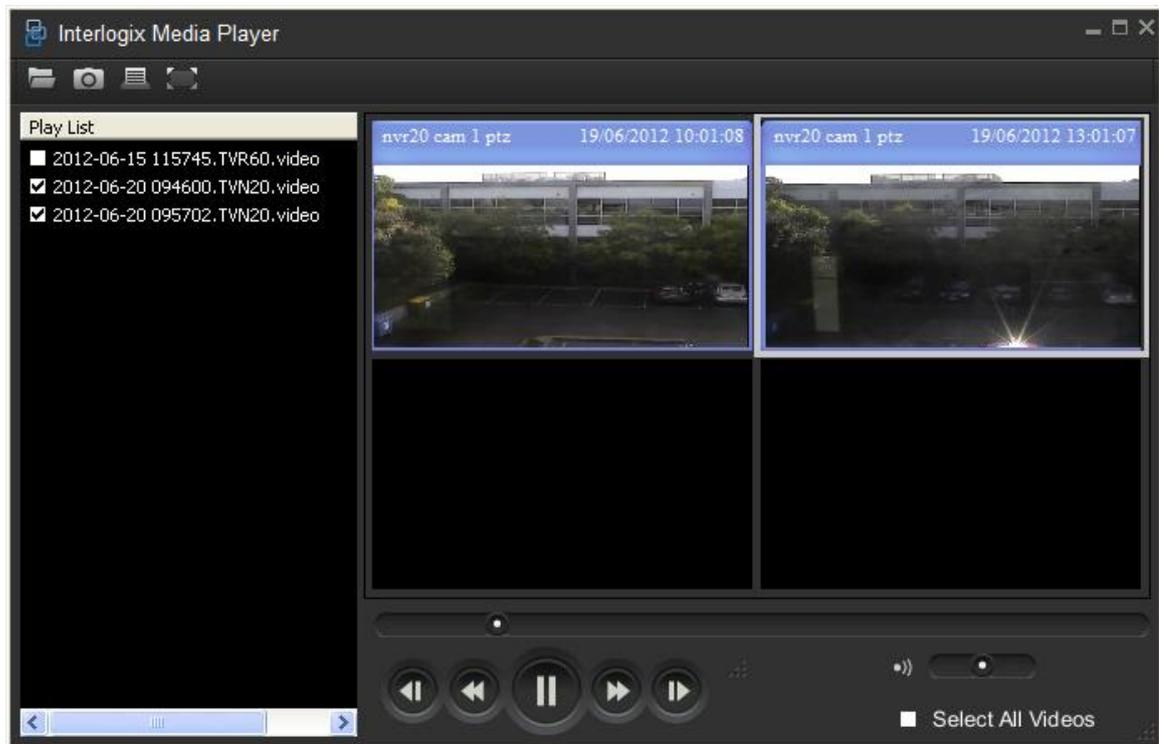
Viewing exported video footage

The media player is a standalone player that can be used to replay any video clip that has been exported using Forcefield. Copy the player's .exe file and .bin file to media in the same folder as the video clips for authorities. It has a zero footprint – meaning it does not require installation to a machine.

Run the media player's .exe file to display a play list of exported files in the same folder (or use the Open File icon to find a video file).

Note: The export of video footage may not be supported on some third-party video products.

Figure 29: Media Player



Teleste Video Management system

This section describes the process of integrating a Teleste Video Management system into Forcefield 6.2 and later.

Overview

A Teleste Video Management system typically comprises:

- CCTV cameras
- Video encoder (providing IP connection to Teleste Server)
- Teleste Server (with VMX Client and VMX Config applications)
- One or more instances of XReceiver (grid of monitors connected to the Teleste Server)
- IP connection to external application (Forcefield client workstations)
- Operating stations (Forcefield client workstations with Teleste remote XReceiver application and ffdshow codec installed)

In addition to XReceiver, running natively on the Teleste Server, each Forcefield client workstation can host remote XReceivers to display video images on the workstation's monitors (suitable IP connection and graphics card required). We recommend NVIDIA® brand video cards.

A multicast IP connection is required between the Teleste Server and the Forcefield workstation in order to display video using XReceiver.

To integrate Teleste into Forcefield, you will need information from the VMX Config application on the Teleste Server. It is assumed that the Teleste system was previously configured and records, such as monitors, cameras, PTZ camera presets, and users, already exist.

Integrating Teleste into Forcefield

The following is the overall process for programming Forcefield to display and control a Teleste Video Management system.

- 1. Create a TCP/IP host record:** In Forcefield use the Databases > Computer Equipment > TCP/IP Hosts command to create a record for the Teleste Video Switcher. The "Address" field must match the "Address" field in VMX Config (Main Group > Master Server > Setup window).
- 2. Create a video switcher record:** In Forcefield use the Databases > Video > Matrix Video > Switchers command to create a new record name, for example "Teleste". Use the license key and hash key associated with your Teleste license. For the "IP Address" field, select the previously-created TCP/IP Host record.

3. **Create video monitor records:** “Monitor” refers to a picture tile on a display and not the display itself. In Forcefield use the Databases > Video > Matrix Video > Monitors command to create a new record. For the “Switcher” field, select the previously-created Teleste video switcher record. The “Teleste Monitor Id” field must match the “Display ID” field in VMX Config (Main Group > Receiver > Monitor > Setup window).
4. **Create monitor group records:** “Monitor group” is a grid of picture tiles on a display. In Forcefield use the Databases > Video > Matrix Video > Monitors Group command to create a new record, select a physical layout, and then save the record.
5. **Assign video monitors to the group:** Click Monitor Assignment to assign a video monitor to each of the picture tiles in the grid.
6. **Create video camera records:** In Forcefield use the Databases > Video > Matrix Video > Cameras command to create a new record. For the “Switcher” field, select the previously-created Teleste video switcher record. The “Teleste Camera Id” field must match the “Camera ID” field in VMX Config (Main Group > Encoder 1 > Camera window).
7. **Create presets for PTZ cameras:** In Forcefield use the Databases > Video > Matrix Video > Presets command to create a new record. The “Teleste Name” field must match the “Position name” field in VMX Config (Main Group > Encoder 1 > Camera > Preset window). This field is case sensitive.
8. **Configure workstation video options:** In Forcefield use the Databases > Computer Equipment > Workstations command to open a Forcefield workstation record, and then click Video to assign video monitor groups and video monitors to the workstation. The “Video Command Operator” field must match a Teleste user record.
9. **Reactivate the switcher driver:** After making any changes to CCTV configuration, you need to reactivate the driver that talks to the switcher. In Forcefield use the Databases > Video > Matrix Video > Switchers command to open the Teleste video switcher record. Clear the Enabled check box, and then save the record. Check the Enabled check box, and then save the record again.

Chapter 8

Integrating third-party systems

Summary

This chapter describes the basics of integrating certain third-party systems into Forcefield. These systems require the TS9116 Third Party license module.

This chapter does not include the following topics:

- Third-party user link control system (User Link). Refer to the *Forcefield Operators Manual* for details about using the User Link Systems menu.
- Third-party video integration. Refer to Appendix D “Integrating DVRs” on page 141.

Forcefield version 5.1.0 and later can be integrated with third-party devices, so that Forcefield can send event data to, and receive messages from, external systems. Third-party integration enables Forcefield to perform actions via the event triggering system. Refer to Event Trigger in the *Forcefield Operators Manual* for details.

Note: In order to use these features, you must purchase and install the TS9116 Third Party Integration license module.

Content

| | |
|--|----|
| Overview | 78 |
| System security | 78 |
| Communications..... | 78 |
| Message formats..... | 79 |
| Forcefield to third-party system | 79 |
| Third-party system to Forcefield..... | 79 |
| Third-party system example | 80 |
| System definition | 80 |
| Device definition | 81 |

Overview

A third-party system is an external system which can communicate with Forcefield using the Forcefield third-party system protocol.

Refer to the *Forcefield Operators Manual* for details of Forcefield menu options, and refer to the *Third-Party System Protocol Document* for details about technical requirements. The *Third-Party System Protocol Document* is provided after licensing of third-party integration.

The third-party system must be assigned a type in Databases > Third Party > System Types, and is optionally assigned a sub-type in Databases > Third Party > System Sub Types.

A third-party sends events to Forcefield. The third-party device must be assigned a type in Databases > Third Party > Device Types.

Forcefield supports up to 99 types of third-party system (nine types may be connected simultaneously).

Each third-party system can have up to:

- 99 system sub-types
- 99 device types
- a total of 65,535 devices

System security

Both the third-party system (Databases > Third Party > System) and third-party devices (Databases > Third Party > Devices) are assigned a member in order for the normal member partitioning to occur.

The third-party system is assigned a Forcefield operator login and password (Operators > Operators) in order to control access.

The third-party system's operator record is assigned an access (Operators > Access) in order to control by member group and timezone which events are to be sent to the third-party system.

Communications

Forcefield communicates with third-party systems via serial RS-232 or TCP/UDP. Only one third-party system is allowed per communications channel.

In order to control the amount of data that Forcefield sends to a third-party system, a buffer depth setting is provided on the Admin > Configuration > Configuration screen. Older data will overflow the buffer and be discarded, and only recent data will be sent to the third-party system. The buffer depth is global to all third-party systems used by Forcefield.

The following communication parameters are programmed in Databases > Third Party > System:

- **ACK Timeout:** Both Forcefield and the third-party system must acknowledge data transmission within the ack timeout time.
- **Retry Attempts:** Determines the number of retries permitted. Data transmission may be retried up to the number of retry attempts when data transmission has not been acknowledged within the ack timeout time.
- **Heartbeat:** Determines the heartbeat period. During periods of inactivity, Forcefield will send heartbeats to the third-party system to ensure it is still active.
- **Time Synchronisation:** Determines whether Forcefield or the third-party system is allowed to set the time of the other, or no time synchronisation is to occur.

The third-party system must log in to Forcefield with a valid operator login and password. No data transmission will occur unless the third-party system has successfully logged in.

Message formats

Forcefield to third-party system

Forcefield will send a particular event to a third-party system when the event's computer category is programmed to print the event.

The following data types may be used, and are programmed in Databases > Third Party > System:

- Short form binary
- History record in native record format
- History record in CSV format

Refer to the *Third-Party System Protocol Document* for details.

Third-party system to Forcefield

The message from the third-party system is the device number and an index into the device's computer category. Forcefield uses this information to perform actions through the event triggering mechanism.

Third-party system example

System definition

The third-party system:

- Is a watering controller.
- Communicates to Forcefield via a serial RS-232 interface.
- Is to receive Forcefield events only during business hours for messages of the 'Watering Member' member group.
- The received event format is to be short form binary.
- Will send events to Forcefield to indicate faulty or fixed watering solenoids and to notify of watering on or off operations.
- Does not require time synchronisation between Forcefield and the watering system.

To set up the third-party system:

1. Create a serial port record of type 'Other', and name it, for example, 'Ser 1- TP Port'.
2. Create a printer access record, for example, 'Watering Access', with a 'Watering Member' member group, and a timezone of 'Business Hours'.
3. Create a third-party system type record and name it, for example, 'Coyote Watering Controller'.
4. Create a computer category record from the 'General' type, and name it, for example, 'Watering Sys Comp Cat'.
5. Create a third-party system record with the following values:
 - Num is a value from 1 to 9.
 - ID is a unique name, such as 'Coyote Watering System'.
 - Type is 'Coyote Watering Controller'.
 - A valid locality.
 - Channel type of RS-232, serial port of 'Ser 1- TP Port'.
 - ACK timeout, retry attempts and heartbeat as required.
 - Select 'Sends Events'.
 - Select 'Receives Events' in format 'Short Form Binary'.
 - Set access to 'Watering Access'.
 - Set member as appropriate.
 - Set computer category to 'Watering Sys Comp Cat'.
 - Set time sync to 'None'.

6. At this stage leave Enabled blank.

Device definition

It is now necessary to create a device record for each device of this system that is to send data to Forcefield.

The watering system devices are to report notify events as well as alarm and restoral events so a computer category record of type 'Other: AlarmRestNotify' and named, for example 'Watering Solenoid' is required.

Let's say each solenoid can generate the following alarm/restore events:

- Fault - open circuit
- Restore - open circuit
- Fault - short circuit
- Restore - short circuit
- Fault - watering failure
- Restore - watering failure

Let's say each solenoid can generate the following notify events:

- Watering
- Not Watering
- Pre-set Moisture Level Reached.

Table 7 below depicts a possible computer category layout (the indexes start from zero, so the third item is index 2).

Table 7: Computer category example

| Event | Event type | Change event text to | Index |
|------------|-----------------|---|-------|
| Event 2177 | Alarm Event 1 | 'Fault - open circuit' | 0 |
| Event 2178 | Restore Event 1 | 'Restore - open circuit' | 1 |
| Event 2179 | Notify Event 1 | 'Watering' | 2 |
| Event 2180 | Notify Event 2 | 'Not Watering' | 3 |
| Event 2181 | Alarm Event 2 | 'Fault - short circuit' | 4 |
| Event 2182 | Restore Event 2 | 'Restore - short circuit' | 5 |
| Event 2183 | Notify Event 3 | 'Preset Moisture Level Reached' | 6 |
| Event 2184 | Notify Event 4 | Event 2184 is not used because it's a notify event and can't be used for alarms or restorals. | 7 |

| Event | Event type | Change event text to | Index |
|------------|-----------------|------------------------------|-------|
| Event 2185 | Alarm Event 3 | 'Fault - Watering Failure' | 8 |
| Event 2186 | Restore Event 3 | 'Restore - Watering Failure' | 9 |

When the third-party system wants to send a message (see *Forcefield Third Party Integration Protocol* document for details) denoting, for example, 'Fault - short circuit', it sends a message with an index of 4. When the third-party system wants to send a message denoting Watering it sends a message with an index of 2.

Create a third-party device record with the following values:

- System is 'Coyote Watering System'.
- Enter a number for the device.
- Enter an ID for the device, Forcefield will use this ID for history, etc.
- Enter appropriate descriptions and locations.
- Select an appropriate member.
- Use the computer category record created above (see Table 7 on page 81).

Repeat for each device of the third-party system. Each device may be of a different type and have a different computer category.

Forcefield only uses the device number and the index of the computer category to identify the event from the third-party system. This may be used to generate actions within Forcefield itself.

Chapter 9

Integrating external user data

Summary

This chapter describes how to set up Forcefield to export or import user data.

Content

| | |
|--|----|
| Setting up an export/import folder on a Windows computer | 84 |
| Overview..... | 84 |
| Preparing the Windows computer | 84 |
| Creating a user account..... | 86 |
| Creating a shared export/import folder | 87 |
| Creating SMB (CIFS) storage in Forcefield | 88 |
| Troubleshooting CIFS connections | 90 |
| Exporting user records | 90 |
| Preparing user data for importing | 91 |
| Using Microsoft Excel | 91 |
| User data file field names | 95 |
| Generating raw card data | 97 |
| Auto-populating raw card data fields..... | 97 |
| Importing user records..... | 98 |
| Troubleshooting the import process..... | 99 |

Setting up an export/import folder on a Windows computer

This section describes the process of setting up a shared folder on a Windows 7 or Windows 8.1 computer and accessing it from Forcefield to export or import user data.

Overview

Sharing the folder a Windows computer uses SMB (Server Message Block) protocol, also referred to as CIFS (Common Internet File System).

Forcefield uses an “SMB (CIFS) Connected Storage” record to define a connection to a shared folder on the Windows computer (such as a Forcefield Client computer) via a user name and password (created for this purpose).

Sharing a folder in a Windows 7 or Windows 8.1 environment (Professional, Ultimate or Enterprise editions) involves a number of procedures, as described in the following sections:

- “Preparing the Windows computer” below
- “Creating a user account” on page 86
- “Creating a shared export/import folder” on page 87
- “Creating SMB (CIFS) storage in Forcefield” on page 88

Preparing the Windows computer

The following descriptions are based on Windows 7, and may differ for Windows 8.1. Refer to Windows help if needed.

Note: Restart the computer after completing the procedures in this section.

Share files

Use the Network and Sharing Center to enable file sharing.

To enable file sharing:

1. From the Control Panel, select Network and Sharing Center, and then click “Change advanced sharing settings” in the left-hand panel.
2. In the File and Printer sharing option, click the “Turn on file and printer sharing” radio button.
3. Click “Save changes” at the bottom of the page.

Note: If you can't see the “Save changes” button at the bottom of the page, use the scroll bars to navigate. If you use the keyboard arrow keys to scroll, then you may accidentally change the settings. If this happens, click Cancel and start over.

Configure security settings

Use the Local Group Policy Editor (gpedit.msc) to configure security settings so that communications from Forcefield are not blocked.

To configure the security settings:

1. Run C:\Windows\System32\gpedit.msc to open the Local Group Policy Editor.
2. Navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
3. The policy “Microsoft network server: Digitally sign communications (always)” must be set to “Disabled”.
4. The policy “Microsoft network client: Digitally sign communications (always)” must be set to “Disabled”.
5. The policy “Network Security: LAN Manager authentication level” must not refuse LM (for example, use “Send LM & NTLM – use NTLMv2 session security if negotiated”).
6. Exit from the Local Group Policy Editor.

Configure local security policies in Windows Registry

Use the Registry Editor (regedit.exe) to configure security policies to accommodate the version of SMB used by Forcefield.

Note: Additional steps are required for Windows 8.1 (they do no harm if applied to Windows 7, but are not required).

To edit the registry for Windows 7 or Windows 8.1:

1. Run C:\Windows\regedit.exe to open the Registry Editor.
2. Navigate to HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Lsa.
3. In the right-hand pane, right-click “LmCompatibilityLevel”, and then select Modify. Change the Value data to 1, and then click OK.
4. In the right-hand pane, right-click “NoLmHash”, and then select Modify. Change the Value data to 0, and then click OK.

Additional steps required for Windows 8.1:

5. Navigate to HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > LanmanServer.
6. In the left-hand pane, right-click Parameter and then select New > DWORD (32-bit) Value.
7. Type “smb1”, and then press ENTER.
8. In the right-hand pane, right-click “smb1”, and then select Modify. Change the Value data to 1, and then click OK.

9. In the left-hand pane, right-click Parameter and then select New > DWORD (32-bit) Value.
10. Type “smb2”, and then press ENTER.
11. In the right-hand pane, right-click “smb2”, and then select Modify. Change the Value data to 1, and then click OK.

When finished editing the Registry for either Windows 7 or Windows 8.1, exit from the Registry Editor and then restart the computer.

Creating a user account

We recommend that you create a local user account on the Windows computer for the purpose of accessing the shared export/import folder via Forcefield.

Notes:

- The user name and password are visible to anyone viewing the “SMB (CIFS) Connected Storage” record in Forcefield, so it may be inappropriate to use an actual operator’s Windows login as the user account.
- It is possible to create a local user account on the Windows computer with a password that does not meet the complexity requirements to allow Forcefield to access the shared folder. The password complexity requirements are listed in step 6.

To create a local user:

1. From the Control Panel, select Administrative Tools, and then double-click Computer Management.
2. In the left-hand pane of the Computer Management window, navigate to System Tools > Local Users and Groups, and then click Users.
3. Click Action > New User... to display the New User dialogue box (Figure 30 on page 87).
4. Enter a name in the User name field to identify this local user account.
5. Optionally describe the purpose of the user in the Description field.
6. Enter a password that’s 6 to 14 characters in length, contains both upper- and lower-case letters, contains at least one numeral (0 to 9), and contains at least one special character (such as @, #, \$). The password must not be the same as the user name.

Note: Numerals must be non-consecutive (for example, ‘1357’).

7. Enter the password a second time in the Confirm password field.
8. Click to populate the “User cannot change password” check box and the “Password never expires” check box. The other check boxes must be cleared.
9. Click Create.

Figure 30: New User dialogue box

New User

User name: import

Full name:

Description: Forcefield CIFS user

Password: ●●●●●●

Confirm password: ●●●●●●

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

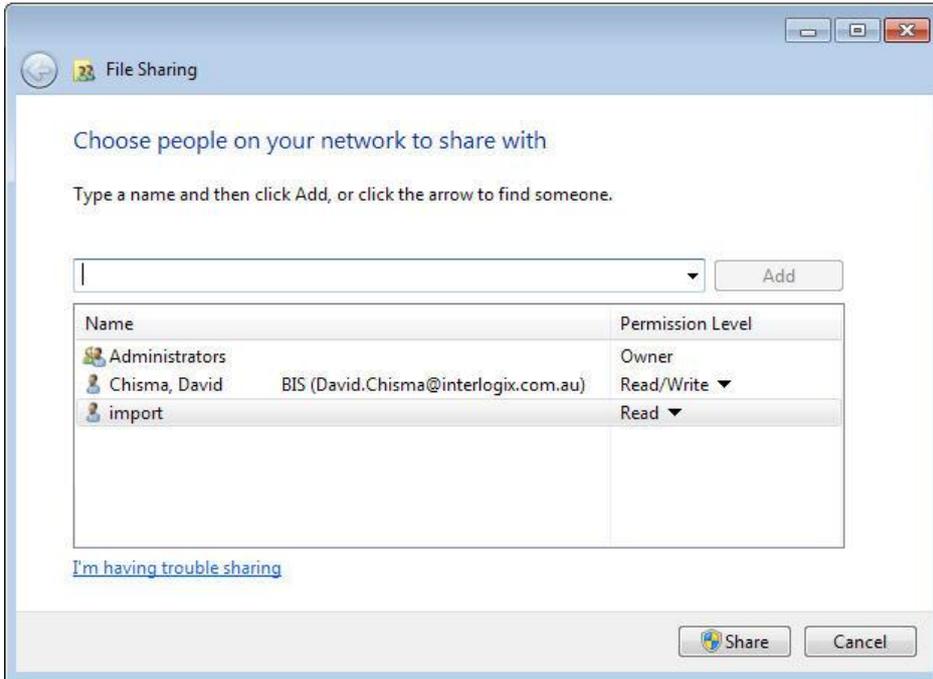
Help Create Close

Creating a shared export/import folder

To create a folder and share it with the local user:

1. Create a folder to be shared with Forcefield, for example “C:\transfer”.
2. Right-click the folder, and then select Share with > Specific people...

3. In the File Sharing dialogue box, type the name of the local user in the text field, and then click Add. In the following image, the user name “import” has been added to the list of users with a permission level of Read.



4. Click the Permission Level arrow to the right of the local user name, and then select Read/Write.
5. Click Share, and then click Done.

Creating SMB (CIFS) storage in Forcefield

In order to access a shared folder on a Windows computer from Forcefield via your network, you need to know the following:

- The Windows computer name and IP address (specifically the IP address of the computer’s connection to the Forcefield node).
- The shared folder name.
- The name and password of the Windows local user account.

To create an SMB storage:

1. In Forcefield select Databases > Computer Equipment > Storage > SMB (CIFS) to open the SMB (CIFS) Connected Storage window (Figure 31 on page 89).

Figure 31: SMB (CIFS) Connected Storage



2. Create a new SMB storage record containing the following details:
 - Type a name for the record in the CIFS ID field.
 - Click the Node arrow, and then select the Forcefield node number that is to make the connection.
 - Type a number of seconds in the Check field. The Forcefield node will periodically attempt to write a file to the share location at the defined interval in order to maintain the connection. If the node has more than one SMB storage record with different Check values, then the lowest (non-zero) value will be used for all records.
 - Type the Windows computer name followed by a colon and the IP address in the Machine field.
 - Type the share folder name in the Share field.
 - Type the Windows user name in the User field.
 - Type the Windows password in the Passwd field (this password is visible, not cloaked).
3. Click Save. Forcefield displays a test connection prompt (see Figure 32 on page 90).
4. At the test connection prompt, click Yes to check the connection. If successful, Forcefield opens a connection and displays a Continue button.

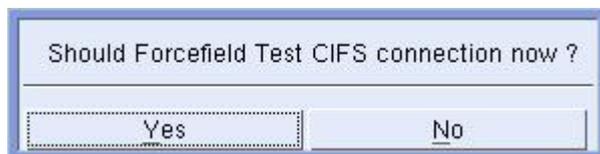


5. Click Continue to close the test window when successful. If not successful, recheck your steps in this procedure, or see “Troubleshooting CIFS connections” on page 90.

Troubleshooting CIFS connections

When you click Save in the CIFS Storage window Forcefield displays a test connection prompt (Figure 32 below). Click Yes to perform a connection test.

Figure 32: CIFS test prompt



Error messages are displayed if the connection attempt is unsuccessful. If more than one fault exists, an error message is displayed for only the first error encountered, even if other errors exist. For example, if both the machine name and the user password are wrong, you receive an error message for only the machine name until you correct it and test the connection again.

Table 8 below lists the error messages you might see.

Table 8: CIFS mount error messages

| Sequence | Error message | Probable cause |
|----------|---|--|
| 1 | Mount failed: Connection timed out | Error in machine IP address |
| 2 | Mount failed: No such device or address | Error in machine name |
| 3 | Mount failed: Permission denied | Error in Windows user name or password |
| 4 | Mount failed: No such file or directory | Error in share folder name |

Exporting user records

Before you can export user records you need to have set up a storage location, such as a CIFS storage on a Windows computer (see “Setting up an export/import folder on a Windows computer” on page 84).

To export user records:

1. Go to Users > Transfer User Data > Export User Data to open the User Export window.
2. Select the criteria to define the records you want to export and then click the Export To arrow.
3. Click the in format arrow, and then select the data format required (e.g. CSV).
4. Select the remote storage location.
5. Click Run to execute.

In the case of a CSV file export, Forcefield creates a file named userexp.csv in the remote storage location. In the case of a TSV file export, Forcefield creates a file named userexp.tsv in the remote storage location.

See also “Export file data format” on page 102.

Preparing user data for importing

User data may be created or exported from a variety of applications for use in Forcefield, as long as they conform to the specifications listed in Table 10 on page 114.

The use of various applications and methods to prepare data is outside of Our control and outside of the scope of this document. However, this section does provide some guidelines to assist you in preparing data.

We do not recommend the use of one external application over another. Responsibility for maintaining data integrity lies with the operator.

Using Microsoft Excel

Microsoft Excel is commonly used for manipulating tabular data. Note the following cautions:

- You can't work in form view because Excel (depending on version) does not support forms with more than 32 data fields (user data has at least 71 data fields). User data displayed in Excel occupies at least 71 columns (see “User data file field names” on page 95).
- Take care to avoid changing Forcefield time and date fields into Excel time and date format by opening the file incorrectly (e.g. by double-clicking a .CSV file in Windows Explorer). Such changes may result in errors or a loss of data.

Opening user data in Excel

This section describes a method of using Microsoft Excel to open a user data file and save it as an Excel file. This example uses a .TSV file; the process is similar for a .CSV file.

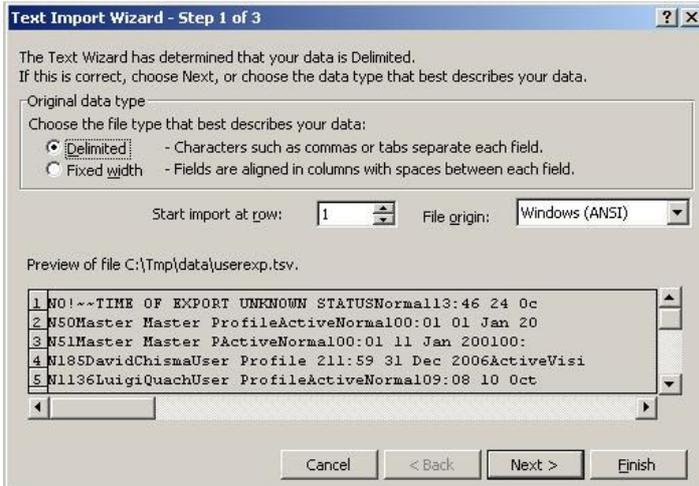
To open user records in Excel:

1. Prepare a user import file that conforms to Table 10 on page 114. In this example we'll use the results of a user export operation named `userexp.tsv`.

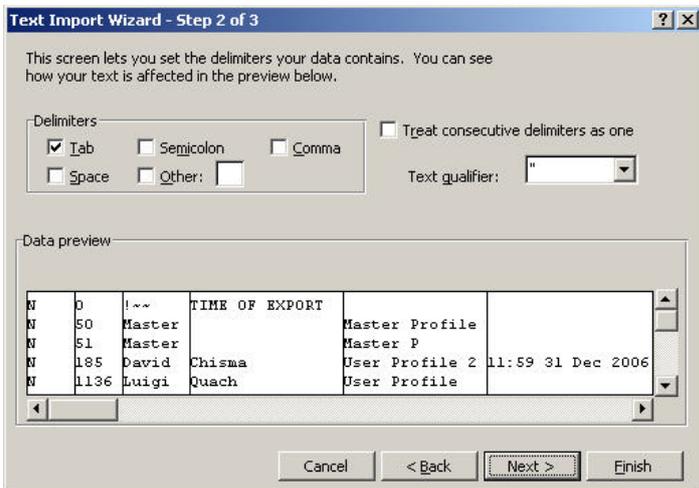
Note: It is recommended to use file extensions such as .TSV or .IMP, because Excel launches the Text Import Wizard, which is required to prepare data files correctly. If you open a .CSV file, Excel will automatically reformat the date columns incorrectly. If you need to edit a .CSV file, first change the file extension from .CSV to .IMP.

2. In Microsoft Excel, use File > Open to begin to open the `userexp.tsv` file. Excel displays the Text Import Wizard.

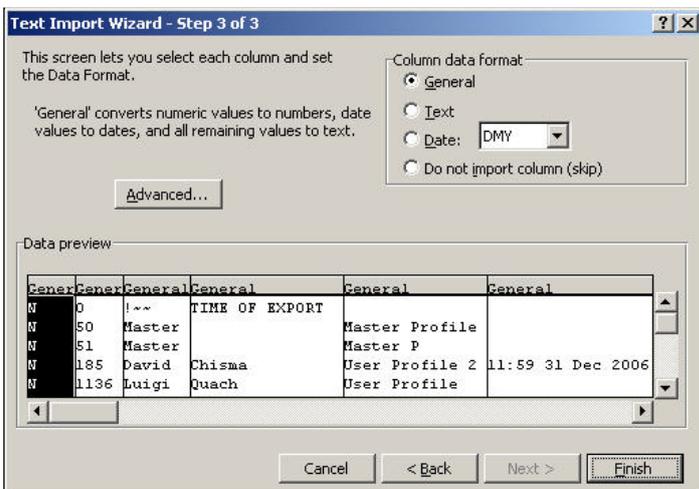
3. Select Delimited and click Next.



4. For TSV format, select Tab and click Next. For CSV format, select Comma and click Next.



5. Excel allows you to change the data format of each column. You must change the format of the three date columns (column 6, 14, and 15) even if they contain no data.



6. Scroll across to the first date in column 6 (Profile Expiry Date) and change the Column data format from General to Text.



7. Scroll across to the two remaining date columns (14 and 15) and change the format from General to Text.
8. Raw card data can be omitted and created in Forcefield later. See “Generating raw card data” on page 97 and “Auto-populating raw card data fields” on page 97.
9. Click Finish to open the file in Excel.



10. Use File > Save As to save the file as an Excel file (.XLS), if required.

Row 1, produced in the export process, may be deleted or left as is. It will be ignored if used in an import file.

Due to limitations in Excel, you will not be able to insert a row with heading names (unless you delete it prior to exporting data), nor will you be able to convert the spreadsheet into a form.

Creating user data from Excel

This section describes a method of using Microsoft Excel to edit or create the required user.imp file, for importing into Forcefield.

To create a user.imp from Excel:

1. Open the Excel file created using the process described in “Opening user data in Excel” on page 91.

2. Edit and save the data as required, so that it conforms to Table 10 on page 114.
3. Use File > Save As to save the file in .CSV format (for example newdata.csv).
4. In Windows Explorer, rename the file newdata.csv to user.imp.
5. Place the user.imp file in the remote storage location, as defined in “Setting up an export/import folder on a Windows computer” on page 84.

User data file field names

Field names are provided to assist in creating forms for data handling, for example as temporary column headings in Microsoft Excel or as field labels in Microsoft Access (or other application).

Refer to Table 10 on page 114 for detailed information about each of the fields.

Use the following field names if additional profiles are not required for users.

| | | |
|------------------------|-------------------|------------------------|
| 1. Import Action | 2. User Number | 3. Name |
| 4. Name | 5. Profile | 6. Profile Expiry Date |
| 7. Alternate Profile | 8. Status | 9. Type |
| 10. Privileged | 11. Long Access | 12. Card Only |
| 13. Trace User | 14. Begin Date | 15. End Date |
| 16. PIN | 17. Member | 18. Def Field |
| 19. Department | 20. Position | 21. Phone |
| 22. Ph Ext | 23. Phone AH | 24. Lockout Type |
| 25. Lockout Time | 26. User Data 1 | 27. User Data 2 |
| 28. User Data 3 | 29. User Data 4 | 30. User Data 5 |
| 31. User Data 6 | 32. User Data 7 | 33. User Data 8 |
| 34. User Data 9 | 35. User Data 10 | |
| 36. User Card Category | 37. Raw Card Data | 38. Total Bits |
| 39. User Card Category | 40. Raw Card Data | 41. Total Bits |
| 42. User Card Category | 43. Raw Card Data | 44. Total Bits |
| 45. User Card Category | 46. Raw Card Data | 47. Total Bits |
| 48. User Card Category | 49. Raw Card Data | 50. Total Bits |
| 51. User Card Category | 52. Raw Card Data | 53. Total Bits |
| 54. User Card Category | 55. Raw Card Data | 56. Total Bits |
| 57. User Card Category | 58. Raw Card Data | 59. Total Bits |
| 60. User Card Category | 61. Raw Card Data | 62. Total Bits |
| 63. User Card Category | 64. Raw Card Data | 65. Total Bits |
| 66. User Card Category | 67. Raw Card Data | 68. Total Bits |
| 69. User Card Category | 70. Raw Card Data | 71. Total Bits |

The following 16 additional fields are used for user link data (omit if not needed):

| | |
|----------------------|-----------------------|
| 72. User Link Server | 73. User Link Profile |
| 74. User Link Server | 75. User Link Profile |
| 76. User Link Server | 77. User Link Profile |
| 78. User Link Server | 79. User Link Profile |
| 80. User Link Server | 81. User Link Profile |
| 82. User Link Server | 83. User Link Profile |
| 84. User Link Server | 85. User Link Profile |
| 86. User Link Server | 87. User Link Profile |

Use the following field names if additional profiles are required for users. The list includes the 27 fields (9 sets of 3) for additional profiles.

| | | |
|-----------------------------|-----------------------------------|---------------------------------|
| 1. Import Action | 2. User Number | 3. Name |
| 4. Name | 5. Profile | |
| 6. Additional Profile Name | 7. Additional Profile Start Date | 8. Additional Profile End Date |
| 9. Additional Profile Name | 10. Additional Profile Start Date | 11. Additional Profile End Date |
| 12. Additional Profile Name | 13. Additional Profile Start Date | 14. Additional Profile End Date |
| 15. Additional Profile Name | 16. Additional Profile Start Date | 17. Additional Profile End Date |
| 18. Additional Profile Name | 19. Additional Profile Start Date | 20. Additional Profile End Date |
| 21. Additional Profile Name | 22. Additional Profile Start Date | 23. Additional Profile End Date |
| 24. Additional Profile Name | 25. Additional Profile Start Date | 26. Additional Profile End Date |
| 27. Additional Profile Name | 28. Additional Profile Start Date | 29. Additional Profile End Date |
| 30. Additional Profile Name | 31. Additional Profile Start Date | 32. Additional Profile End Date |
| 33. Profile Expiry Date | 34. Alternate Profile | 35. Status |
| 36. Type | 37. Privileged | 38. Long Access |
| 39. Card Only | 40. Trace User | 41. Begin Date |
| 42. End Date | 43. PIN | 44. Member |
| 45. Def Field | 46. Department | 47. Position |
| 48. Phone | 49. Ph Ext | 50. Phone AH |
| 51. Lockout Type | 52. Lockout Time | 53. User Data 1 |
| 54. User Data 2 | 55. User Data 3 | 56. User Data 4 |
| 57. User Data 5 | 58. User Data 6 | 59. User Data 7 |
| 60. User Data 8 | 61. User Data 9 | 62. User Data 10 |
| 63. User Card Category | 64. Raw Card Data | 65. Total Bits |
| 66. User Card Category | 67. Raw Card Data | 68. Total Bits |
| 69. User Card Category | 70. Raw Card Data | 71. Total Bits |
| 72. User Card Category | 73. Raw Card Data | 74. Total Bits |
| 75. User Card Category | 76. Raw Card Data | 77. Total Bits |
| 78. User Card Category | 79. Raw Card Data | 80. Total Bits |
| 81. User Card Category | 82. Raw Card Data | 83. Total Bits |
| 84. User Card Category | 85. Raw Card Data | 86. Total Bits |
| 87. User Card Category | 88. Raw Card Data | 89. Total Bits |
| 90. User Card Category | 91. Raw Card Data | 92. Total Bits |
| 93. User Card Category | 94. Raw Card Data | 95. Total Bits |
| 96. User Card Category | 97. Raw Card Data | 98. Total Bits |

The following 16 additional fields are used for user link data (omit if not needed):

| | |
|-----------------------|------------------------|
| 99. User Link Server | 100. User Link Profile |
| 101. User Link Server | 102. User Link Profile |
| 103. User Link Server | 104. User Link Profile |
| 105. User Link Server | 106. User Link Profile |
| 107. User Link Server | 108. User Link Profile |
| 109. User Link Server | 110. User Link Profile |
| 111. User Link Server | 112. User Link Profile |
| 113. User Link Server | 114. User Link Profile |

Generating raw card data

Forcefield can automatically generate raw card data (RCD) for imported user records (fields 36 to 71, or 63 to 98 if additional profiles are present). This means the creator of the user.imp file does not need to enter the raw card data into the spreadsheet.

Automatic raw card data generation occurs only in the following circumstances:

- There is no raw card data in the user.imp file (fields 36 to 71 are blank, or if additional profiles are present, fields 63 to 98 are blank) for this user.
- There is currently no raw card data in the database for this user and card category.
- The calculated raw card data does not already exist in the database for any other user.
- The Challengers to which the user will be downloaded have a standard card category (a card category that ends with a tilde character '~'). If a non-standard card category is used, the raw card data fields will all contain zeros.
- The Challenger has site code A specified in Challenger system options.

A user's generated raw card data is based on the first Challenger assigned to the user (determined by the profile access). The raw card data is calculated from the following:

- User number
- User offset (if applicable)
- Site code A
- Site code A offset (if applicable)

Once raw card data is automatically generated, the same raw card data will then be assigned to subsequent Challengers having the same card category regardless of the Challenger's Site Code A (they should all be the same).

Auto-populating raw card data fields

Forcefield can automatically populate the raw card data for the standard card categories (marked with a tilde, such as Tecom 27 bit~), when the site code and card number are known.

To use this feature, do the following for each of the required sets of three data fields:

1. In the User Card Category field, enter the required standard card category. See row 36 in Table 10 on page 114 for example. Each card category can only be used once per user record.

2. In the Raw Card Data field, set the first value to the site code (e.g. 136) and the second value to the card number (e.g. 15). Using the example values, the Raw Card Data would appear in the import file as “136.15.0.0.0.0”. See row 37 in Table 10 on page 114 for example.
3. In the Total Bits field, set the value to 255. See row 38 in Table 10 on page 114 for example.

Each set of three data fields must be populated in turn without gaps or any subsequent data will be ignored.

Importing user records

Before you can import user records you need to have set up a storage location, such as a CIFS storage on a Windows computer (see “Setting up an export/import folder on a Windows computer” on page 84).

User records must be in a specific format before they can be used in Forcefield. Refer to “Import file data format” on page 112 for details.

To import user records:

1. Prepare a user import file in either .TSV or .CSV format and name it ‘user.imp’. See “Preparing user data for importing” on page 91 for details.
2. Place the user.imp file in the remote storage location.
3. Go to Users > Transfer User Data > Import User Data to open the User Import window.
4. Select the remote storage location.
5. Click the Report to arrow, and then select the reporting location (e.g. screen).
6. Click Run to execute.

Troubleshooting the import process

If the user.imp file is missing, or if it's incorrectly named, Forcefield will generate an 'Unable to Open File' alarm and the import process will be terminated.

If the operation runs successfully, view the generated report to see any error messages generated from the user.imp file. The following is a list of common faults and associated error messages listed in the report viewer.

Rejected – Action not Add or Delete: The user record did not begin with an A or a D.

Rejected – User Profile Invalid: The user profile does not exist in Forcefield. Check the spelling in the user.imp file, or create the user profile in Forcefield, as required.

Rejected – Invalid Member: The member does not exist in Forcefield. Check the spelling in the user.imp file, or create the member in Forcefield, as required.

Rejected – IUM Card Category Invalid: The IUM card category does not exist in Forcefield. Check the spelling in the user.imp file, or create the card category in Forcefield, as required.

Rejected: Followed by details for the rejection, such as card data or PIN code already in use by another user.

Data format error on line n: If any of the required data fields are missing, Forcefield abandons changes to the user's record and all subsequent records in the file.

Time or date input format error: The data in the date and time fields is not correct, for example, the file has been converted to Excel format "31/12/2006 11:59" instead of "11:59 31 Dec 2006".

Appendix A

User data file formats

Summary

This appendix describes the data file requirements to copy or export Forcefield user data from the Forcefield user database to storage media or an NFS or CIFS connected computer.

Content

| | |
|---|-----|
| Export file formats | 102 |
| Export method | 102 |
| Export file data format..... | 102 |
| Import file formats..... | 112 |
| Import method..... | 112 |
| Status report | 112 |
| Import file data format..... | 112 |
| Importing profiles in Unique Profile Per User mode..... | 126 |

Export file formats

This section relates to the Export User Data option.

Export method

The export method may be manual or automatic (Forcefield Configuration determines which one is used).

Note: In order to use automatic user export, you must purchase and install the TS9119 Auto User Import/Export license module.

Manual export

- Initiated by an operator from the Forcefield menu.
- Export data is copied to the storage media selected by the operator.
- The file may not contain all Forcefield users. Only those users who meet the export criteria selected by the operator will be in the file regardless of file format.
- The export data file is regenerated on every manual export.

Automatic export

- Can only be directed to NFS/CIFS mounted storage.
- Every time a user is added, modified or deleted, Forcefield will amend or create the export data file.
- For CSV format a new record will be appended to the end of the file, thus a record that is first created, then modified, and then deleted will appear in the file three times.
- It is the responsibility of the remote computer system to remove the file periodically.

Note: The only valid user data on a delete is the user number.

Export file data format

When performing manual exports, user data is exported from Forcefield in either CSV or TSV formats. These formats are described in the following sections.

CSV (comma separated value) format

The file created is userexp.csv. In this format there is 1 text line per user with data in double quotes separated by commas.

For example, "datafield1","datafield2","....", "datafield n", in the order listed in Table 9 on page 103.

TSV (tab separated value) format

File created is userexp.tsv. In this format there is 1 text line per user with data separated by tabs.

For example, datafield1<TAB>datafield2<TAB>.. ..<TAB>datafield, in the order listed in Table 9 below

Note: For manual exports, there is a record for user zero. This user does not exist—this record contains the date the export was performed (in the begin and end date fields).

The number of fields exported for a user depends on whether the user has additional profiles and/or user link data. If the user has neither, then 72 fields are exported. If the user has additional profiles, then 27 extra fields (9 sets of 3) will be exported. If the user has user link data, then 16 extra fields (8 sets of 2) will be exported. Thus:

- A user with neither additional profiles or user link data will have 72 fields
- A user with additional profiles but no user link data will have 99 fields
- A user with user link data but no additional profiles will have 88 fields
- A user with additional profiles and user link data will have 115 fields

Note: Each user may be exported with a different number of fields.

Note: The field numbers in the following table vary according to whether additional profiles are used.

Table 9: CSV and TSV export file field descriptions

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|---------------------|--|
| 1 | 1 | Export Action | "N" | Values include: <ul style="list-style-type: none"> • N—no data change, only for a Manually generated export • A—user has been added • M—user has been modified • D—user has been deleted |
| 2 | 2 | Date | "14:15 21 Jan 2014" | The date of the entry. Note: Applicable only to Automatic Export file format |
| 3 | 3 | User Number | "1" | The Forcefield user number range is 1 to 999,999. |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|---------------------|--|
| 4 | 4 | Name | "Fred" | User first name or surname, order depends on Forcefield configuration. |
| 5 | 5 | Name | "Smith" | User first name or surname, order depends on Forcefield configuration. |
| 6 | 6 | Profile | "Engineering Staff" | The primary profile that the user is assigned to, e.g. 'Cleaners'. This determines the Challenger access the user has. |

The following 9 sets of 3 data fields contain additional profile information for the user (if applicable).

| | | | | |
|--|----|-------------------------------|---------------------|-----------------------------------|
| | 7 | Additional Profile Name | "Profile name" | Name of additional profile |
| | 8 | Additional Profile Start Date | "14:15 21 Jan 2014" | Start date of additional profile |
| | 9 | Additional Profile End Date | "11:00 23 Mar 2014" | End date of additional profile |
| | 10 | Additional Profile Name | See field 7 | See field 7 (additional profiles) |
| | 11 | Additional Profile Start Date | See field 8 | See field 8 (additional profiles) |
| | 12 | Additional Profile End Date | See field 9 | See field 9 (additional profiles) |
| | 13 | Additional Profile Name | See field 7 | See field 7 (additional profiles) |
| | 14 | Additional Profile Start Date | See field 8 | See field 8 (additional profiles) |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|---------------------|---|-------------------------------|---------------------|-----------------------------------|
| | 15 | Additional Profile End Date | See field 9 | See field 9 (additional profiles) |
| | 16 | Additional Profile Name | See field 7 | See field 7 (additional profiles) |
| | 17 | Additional Profile Start Date | See field 8 | See field 8 (additional profiles) |
| | 18 | Additional Profile End Date | See field 9 | See field 9 (additional profiles) |
| | 19 | Additional Profile Name | See field 7 | See field 7 (additional profiles) |
| | 20 | Additional Profile Start Date | See field 8 | See field 8 (additional profiles) |
| | 21 | Additional Profile End Date | See field 9 | See field 9 (additional profiles) |
| | 22 | Additional Profile Name | See field 7 | See field 7 (additional profiles) |
| | 23 | Additional Profile Start Date | See field 8 | See field 8 (additional profiles) |
| | 24 | Additional Profile End Date | See field 9 | See field 9 (additional profiles) |
| | 25 | Additional Profile Name | See field 7 | See field 7 (additional profiles) |
| | 26 | Additional Profile Start Date | See field 8 | See field 8 (additional profiles) |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------------------|-------------------------------|---|
| | 27 | Additional Profile End Date | See field 9 | See field 9 (additional profiles) |
| | 28 | Additional Profile Name | See field 7 | See field 7 (additional profiles) |
| | 29 | Additional Profile Start Date | See field 8 | See field 8 (additional profiles) |
| | 30 | Additional Profile End Date | See field 9 | See field 9 (additional profiles) |
| | 31 | Additional Profile Name | See field 7 | See field 7 (additional profiles) |
| | 32 | Additional Profile Start Date | See field 8 | See field 8 (additional profiles) |
| | 33 | Additional Profile End Date | See field 9 | See field 9 (additional profiles) |
| 7 | 34 | Profile Expiry Date | "11:00 23 Mar 2014" | A date after which the profile no longer applies. Blank means the profile never expires. |
| 8 | 35 | Alternate Profile | "Engineering Staff - No Labs" | The profile that the user is assigned to when the primary profile expires. If blank, then the user would have no Challenger access after the expiry date. |
| 9 | 36 | Status | "Active" | Values include: <ul style="list-style-type: none"> • Inactive • Active • Void • Lost • Expired |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|---------------------|---|
| 10 | 37 | Type | "Normal" | Values include: <ul style="list-style-type: none"> • Normal • Visitor • Guard • Dual |
| 11 | 38 | Privileged | "" | Blank means 'does not apply' |
| 12 | 39 | Long Access | "Long Access" | Blank means 'does not apply' |
| 13 | 40 | Card Only | "" | Blank means 'does not apply' |
| 14 | 41 | Trace User | "1" | Blank means 'does not apply' |
| 15 | 42 | Begin Date | "11:00 15 Mar 2012" | The date when the user becomes valid. |
| 16 | 43 | End Date | "14:15 21 Jan 2017" | The date when the user becomes expired. |
| 17 | 44 | PIN | "1111" | User's PIN code. |
| 18 | 45 | Member | "Administration" | All users belong to a member, this determines where any alarm messages will be directed, and which operators have access to this user's data. |
| 19 | 46 | Def Field | "reference num" | This field contains data pertinent to all users on this site. |
| 20 | 47 | Department | "" | |
| 21 | 48 | Position | "" | |
| 22 | 49 | Phone | "phone1" | |
| 23 | 50 | Ph Ext | "1234" | |
| 24 | 51 | Phone AH | "home phone" | |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|---|------------------------------------|--------------------|---------------|--|
| 25 | 52 | Lockout Type | "Not Timed" | Values include: <ul style="list-style-type: none"> • Not Timed • From On Site • From Off Site |
| 26 | 53 | Lockout Time | "0" | Lockout time in minutes |
| The following 10 data fields contain data as determined by the member that the user belongs to. | | | | |
| 27 | 54 | User Data 1 | "" | |
| 28 | 55 | User Data 2 | "" | |
| 29 | 56 | User Data 3 | "" | |
| 30 | 57 | User Data 4 | "" | |
| 31 | 58 | User Data 5 | "" | |
| 32 | 59 | User Data 6 | "" | |
| 33 | 60 | User Data 7 | "" | |
| 34 | 61 | User Data 8 | "" | |
| 35 | 62 | User Data 9 | "" | |
| 36 | 63 | User Data 10 | "" | |
| The following 12 sets of 3 data fields contain the card data for the user. | | | | |
| 37 | 64 | User Card Category | "C 36 bit" | The Card Category assigned to this card data. |
| 38 | 65 | Raw Card Data | "0.1.0.0.2.0" | The raw card data. |
| 39 | 66 | Total Bits | "36" | The number of bits of card data. |
| 40 | 67 | User Card Category | See field 37 | See field 37 |
| 41 | 68 | Raw Card Data | See field 38 | See field 38 |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|---------------------|---|--------------------------|---------------------|--------------------|
| 42 | 69 | Total Bits | See field 39 | See field 39 |
| 43 | 70 | User Card Category | See field 37 | See field 37 |
| 44 | 71 | Raw Card Data | See field 38 | See field 38 |
| 45 | 72 | Total Bits | See field 39 | See field 39 |
| 46 | 73 | User Card Category | See field 37 | See field 37 |
| 47 | 74 | Raw Card Data | See field 38 | See field 38 |
| 48 | 75 | Total Bits | See field 39 | See field 39 |
| 49 | 76 | User Card Category | See field 37 | See field 37 |
| 50 | 77 | Raw Card Data | See field 38 | See field 38 |
| 51 | 78 | Total Bits | See field 39 | See field 39 |
| 52 | 79 | User Card Category | See field 37 | See field 37 |
| 53 | 80 | Raw Card Data | See field 38 | See field 38 |
| 54 | 81 | Total Bits | See field 39 | See field 39 |
| 55 | 82 | User Card Category | See field 37 | See field 37 |
| 56 | 83 | Raw Card Data | See field 38 | See field 38 |
| 57 | 84 | Total Bits | See field 39 | See field 39 |
| 58 | 85 | User Card Category | See field 37 | See field 37 |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|---|---|--------------------------|---------------------|--------------------|
| 59 | 86 | Raw Card Data | See field 38 | See field 38 |
| 60 | 87 | Total Bits | See field 39 | See field 39 |
| 61 | 88 | User Card Category | See field 37 | See field 37 |
| 62 | 89 | Raw Card Data | See field 38 | See field 38 |
| 63 | 90 | Total Bits | See field 39 | See field 39 |
| 64 | 91 | User Card Category | See field 37 | See field 37 |
| 65 | 92 | Raw Card Data | See field 38 | See field 38 |
| 66 | 93 | Total Bits | See field 39 | See field 39 |
| 67 | 94 | User Card Category | See field 37 | See field 37 |
| 68 | 95 | Raw Card Data | See field 38 | See field 38 |
| 69 | 96 | Total Bits | See field 39 | See field 39 |
| 70 | 97 | User Card Category | See field 37 | See field 37 |
| 71 | 98 | Raw Card Data | See field 38 | See field 38 |
| 72 | 99 | Total Bits | See field 39 | See field 39 |
| The following 8 sets of 2 data fields contain user link data (if applicable). | | | | |
| 73 | 100 | User Link Server | “server name” | |
| 74 | 101 | User Link Profile | “profile name” | |
| 75 | 102 | User Link Server | “server name” | |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|---------------------|---|--------------------------|---------------------|--------------------|
| 76 | 103 | User Link Profile | "profile name" | |
| 77 | 104 | User Link Server | "server name" | |
| 78 | 105 | User Link Profile | "profile name" | |
| 79 | 106 | User Link Server | "server name" | |
| 80 | 107 | User Link Profile | "profile name" | |
| 81 | 108 | User Link Server | "server name" | |
| 82 | 109 | User Link Profile | "profile name" | |
| 83 | 110 | User Link Server | "server name" | |
| 84 | 111 | User Link Profile | "profile name" | |
| 85 | 112 | User Link Server | "server name" | |
| 86 | 113 | User Link Profile | "profile name" | |
| 87 | 114 | User Link Server | "server name" | |
| 88 | 115 | User Link Profile | "profile name" | |

Import file formats

This section relates to Forcefield menu option Users > Transfer User Data > Import User Data.

This functionality is provided in order to copy or import Forcefield user data from storage media or an NFS/CIFS connected computer into the Forcefield user database.

See also “Preparing user data for importing” on page 91.

Import method

The import method may be manual or automatic (Forcefield Configuration determines which one is used).

Note: In order to use automatic user import, you must purchase and install the TS9119 Auto User Import/Export license module.

Manual import

- Initiated by an operator from the Forcefield menu.
- Forcefield will attempt to read the file user.imp on the storage selected by the operator.
- If located on the Forcefield computer, the location must be /usr/ares/user/import.

Automatic import

- Automatic imports can only be directed from NFS/CIFS mounted storage.
- Forcefield will periodically scan the nominated directory for the file user.imp, process the file, and then remove it.

Status report

A report will be generated indicating status of import for each user record in the import file which is rejected or has its data modified.

Individual records may be rejected for a variety of reasons, or data may be truncated if imported data fields are too long.

Import file data format

User data may be imported into Forcefield in either CSV or TSV formats. These formats are described in the following sections.

CSV (comma separated value) format

In this format there is 1 text line per user with data in fields separated by commas, in the order listed in Table 10 on page 114.

Data containing commas must be contained in double quotes, for example, A,12432, Manufacturing, "Smith, Jane", Girl Friday.

TSV (tab separated value) format

In this format the data fields are separated by TAB characters, e.g. A<TAB>12432<TAB>Manufacturing<TAB>Smith, Jane<TAB>Girl Friday, in the order listed in Table 10 on page 114.

Forcefield always exports dates using the format “hh:mm dd Mon yyyy”, with single space characters between the minute and day fields, the day and month fields, and the month and year fields. For example, “11:23 19 Mar 2007”. Upon import, Forcefield accepts the above date format, as well as “dd/mm/yyyy hh:mm”, with single space characters between the year and hour fields. For example, “19/03/2007 11:23”.

The number of fields required in the import file depends on whether the user has additional profiles and/or user link data. If the user has neither, then 71 fields are required. If the user has additional profiles, then 27 extra fields (9 sets of 3) will be required. In each case, all of the fields must be present even if they contain no data. If the user has user link data, then 16 extra fields (8 sets of 2) will be required. Thus:

- A user with neither additional profiles or user link data will require 71 fields.
- A user with additional profiles but no user link data will require 98 fields.
- A user with user link data but no additional profiles will require 87 fields.
- A user with additional profiles and user link data will require 114 fields

User link info for a user is only altered if the user link fields are present in the import file. To remove user link data for a user, the user link fields must be present and be blank. Thus, if there are 71 or 98 fields in the import file for a user, then the user link data for that user will remain unaltered. If there are 87 or 114 fields in the import file, then any existing user link data for that user is removed and then added from the import file, even if blank.

Additional profile information for a user is always changed to reflect what is in the import file. If additional profile information is not present in the import file for a user (i.e. there are 71 or 87 fields) then that user will lose any existing additional profile data.

Note: If a user has additional profiles in the import file that are not present in the Forcefield profile database, then that user will not be imported.

Note: The field numbers in the following table vary according to whether additional profiles are present.

Table 10: CSV and TSV import file field descriptions

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|--------------|--|
| 1 | 1 | Import Action | "A" | <p>Values include:</p> <ul style="list-style-type: none"> • A—user to be added (or modified if it already exists) • D—user to be deleted <p>Any other character is ignored and the data is not processed.</p> |
| 2 | 2 | User Number | "1" | <p>The Forcefield user number range is 1 to 999,999.</p> <p>Mandatory field. For a delete, this is the only field required to contain data.</p> |
| 3 | 3 | First Name | "Fred" | <p>Up to 30 characters.</p> <p>The first name and/or surname fields must contain data or the action will be rejected.</p> <p>First name and surname will be concatenated in Forcefield to form one name field (up to 60 characters total).</p> |
| 4 | 4 | Surname | "Smith" | <p>Up to 30 characters.</p> <p>The first name and/or surname fields must contain data or the action will be rejected.</p> <p>First name and surname will be concatenated in Forcefield to form one name field (up to 60 characters total).</p> |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|---------------------|--|
| 5 | 5 | Profile | "Engineering Staff" | <p>The profile that the user is assigned to, e.g. 'Cleaners'. This determines the Challenger access the user has.</p> <p>The user's member, card type, trace flag, dates, department and position will be determined by the profile, unless the corresponding data fields are contained in the fields in this file.</p> <p>Notes:</p> <ul style="list-style-type: none"> The user's profile must already exist in Forcefield or the user record will not be imported. The report lists 'User Profile Invalid' for the user. When modifying a user, use "~" (or leave blank) to keep the pre-existing value. |

The following 9 sets of 3 data fields contain additional profile information for the user (if applicable).

| | | | | |
|--|----|-------------------------------|---------------------|-----------------------------------|
| | 6 | Additional Profile Name | "Profile name" | Name of additional profile |
| | 7 | Additional Profile Start Date | "14:15 21 Jan 2014" | Start date of additional profile |
| | 8 | Additional Profile End Date | "11:00 23 Mar 2014" | End date of additional profile |
| | 9 | Additional Profile Name | See field 7 | See field 6 (additional profiles) |
| | 10 | Additional Profile Start Date | See field 8 | See field 7 (additional profiles) |
| | 11 | Additional Profile End Date | See field 9 | See field 8 (additional profiles) |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|---------------------|---|-------------------------------|---------------------|-----------------------------------|
| | 12 | Additional Profile Name | See field 7 | See field 6 (additional profiles) |
| | 13 | Additional Profile Start Date | See field 8 | See field 7 (additional profiles) |
| | 14 | Additional Profile End Date | See field 9 | See field 8 (additional profiles) |
| | 15 | Additional Profile Name | See field 7 | See field 6 (additional profiles) |
| | 16 | Additional Profile Start Date | See field 8 | See field 7 (additional profiles) |
| | 17 | Additional Profile End Date | See field 9 | See field 8 (additional profiles) |
| | 18 | Additional Profile Name | See field 7 | See field 6 (additional profiles) |
| | 19 | Additional Profile Start Date | See field 8 | See field 7 (additional profiles) |
| | 20 | Additional Profile End Date | See field 9 | See field 8 (additional profiles) |
| | 21 | Additional Profile Name | See field 7 | See field 6 (additional profiles) |
| | 22 | Additional Profile Start Date | See field 8 | See field 7 (additional profiles) |
| | 23 | Additional Profile End Date | See field 9 | See field 8 (additional profiles) |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------------------|---------------------|---|
| | 24 | Additional Profile Name | See field 7 | See field 6 (additional profiles) |
| | 25 | Additional Profile Start Date | See field 8 | See field 7 (additional profiles) |
| | 26 | Additional Profile End Date | See field 9 | See field 8 (additional profiles) |
| | 27 | Additional Profile Name | See field 7 | See field 6 (additional profiles) |
| | 28 | Additional Profile Start Date | See field 8 | See field 7 (additional profiles) |
| | 29 | Additional Profile End Date | See field 9 | See field 8 (additional profiles) |
| | 30 | Additional Profile Name | See field 7 | See field 6 (additional profiles) |
| | 31 | Additional Profile Start Date | See field 8 | See field 7 (additional profiles) |
| | 32 | Additional Profile End Date | See field 9 | See field 8 (additional profiles) |
| 6 | 33 | Profile Expiry Date | "11:23 19 Mar 2015" | A date after which the profile no longer applies. When adding a user leave this field blank if you do not want the profile to expire. Note: When modifying a user, use "~" (or leave blank) to keep the pre-existing value. |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|-------------------------------|--|
| 7 | 34 | Alternate Profile | "Engineering Staff - No Labs" | The profile that the user is assigned to when the primary profile expires. If blank, then the user would have no Challenger access after the expiry date. Note: When modifying a user, use "~" (or leave blank) to keep the pre-existing value. |
| 8 | 35 | Status | " Void" | Values include: <ul style="list-style-type: none"> • Void • Lost The user's status will be determined by Forcefield, unless the value here is Lost or Void. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 9 | 36 | Type | "Normal" | Values include: <ul style="list-style-type: none"> • Normal • Visitor • Guard • Dual Note: When modifying a user, use "~" to keep the pre-existing value. |
| 10 | 37 | Privileged | "" | Blank means 'does not apply'. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 11 | 38 | Long Access | "Long Access" | Blank means 'does not apply'. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 12 | 39 | Card Only | "" | Blank means 'does not apply'. Note: When modifying a user, use "~" to keep the pre-existing value. |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|---------------------|---|
| 13 | 40 | Trace User | "1" | Blank means 'does not apply'. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 14 | 41 | Begin Date | "11:23 19 Mar 2014" | The time and date when the user becomes valid. Leave blank to use the time and date of importing (adding or modifying). Note: When modifying a user, use "~" to keep the pre-existing value. |
| 15 | 42 | End Date | "11:23 19 Mar 2014" | The time and date when the user becomes expired. Leave blank if you do not want the user to expire (adding or modifying). Note: When modifying a user, use "~" to keep the pre-existing value. |
| 16 | 43 | PIN | "1111" | User's PIN code, 4 to 10 digits. Note: When modifying a user, use "~" to keep the pre-existing value. Leave this field blank if you want to delete the pre-existing PIN. |
| 17 | 44 | Member | "Administration" | Up to 30 characters. All users belong to a member, this determines where any alarm messages will be directed, and which operators have access to this user's data. Notes: <ul style="list-style-type: none"> The member must already exist in Forcefield. User data field labels are not imported. When modifying a user, use "~" (or leave blank) to keep the pre-existing value. |
| 18 | 45 | Def Field | "reference num" | Up to 20 characters. This field contains data pertinent to all users on this site. |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|--------------|---|
| 19 | 46 | Department | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 20 | 47 | Position | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 21 | 48 | Phone | "phone1" | Up to 11 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 22 | 49 | Ph Ext | "1234" | Up to 4 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 23 | 50 | Phone AH | "home phone" | Up to 17 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 24 | 51 | Lockout Type | "Not Timed" | Values include: <ul style="list-style-type: none"> • Not Timed • From On Site • From Off Site Note: When modifying a user, use "~" (or leave blank) to keep the pre-existing value. |
| 25 | 52 | Lockout Time | "0" | Lockout time in minutes (0 to 65535). Note: When modifying a user, use "~" (or leave blank) to keep the pre-existing value. |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|---|------------------------------------|-------------------|--------------|---|
| <p>The following 10 optional user data fields contain data as determined by the member that the user belongs to. User data field labels (defined via the member programming window) are not imported.</p> <p>Note: User data is displayed in Forcefield only if the operator's member allows it.</p> | | | | |
| 26 | 53 | User Data 1 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 27 | 54 | User Data 2 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 28 | 55 | User Data 3 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 29 | 56 | User Data 4 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 30 | 57 | User Data 5 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 31 | 58 | User Data 6 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 32 | 59 | User Data 7 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 33 | 60 | User Data 8 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--|------------------------------------|--------------------|------------------|---|
| 34 | 61 | User Data 9 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| 35 | 62 | User Data 10 | "" | Up to 30 characters. Note: When modifying a user, use "~" to keep the pre-existing value. |
| <p>There can be up to 12 sets of card data for a user (each set has 3 data fields). Note: If any of the 3 data field sets are blank, then all subsequent card data will be ignored.</p> | | | | |
| 36 | 63 | User Card Category | "Tecom 27 bit~" | Up to 20 characters. Notes: <ul style="list-style-type: none"> The card category must already exist in Forcefield. Each card category can only be used once per user record. When modifying a user, use "~" to keep the pre-existing values in the three data field sets. |
| 37 | 64 | Raw Card Data | "136.15.0.0.0.0" | Raw card data in format xxx.xxx.xxx.xxx.xxx.xxx. See also "Generating raw card data" on page 97 and "Auto-populating raw card data fields" on page 97. |
| 38 | 65 | Total Bits | "27" | The number of bits of the card data used: 1 to 48, or 255: <ul style="list-style-type: none"> For up to 48 bits (IUM users) then only raw card data is used. For 255 bits, then the raw card data will start with the site code and card number, e.g. "136.12345.0.0.0.0", where 136 is the site code and 12345 is the card number. |
| 39 | 66 | User Card Category | See field 36 | See field 36 |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|---------------------|---|--------------------------|---------------------|--------------------|
| 40 | 67 | Raw Card Data | See field 37 | See field 37 |
| 41 | 68 | Total Bits | See field 38 | See field 38 |
| 42 | 69 | User Card Category | See field 36 | See field 36 |
| 43 | 70 | Raw Card Data | See field 37 | See field 37 |
| 44 | 71 | Total Bits | See field 38 | See field 38 |
| 45 | 72 | User Card Category | See field 36 | See field 36 |
| 46 | 73 | Raw Card Data | See field 37 | See field 37 |
| 47 | 74 | Total Bits | See field 38 | See field 38 |
| 48 | 75 | User Card Category | See field 36 | See field 36 |
| 49 | 76 | Raw Card Data | See field 37 | See field 37 |
| 50 | 77 | Total Bits | See field 38 | See field 38 |
| 51 | 78 | User Card Category | See field 36 | See field 36 |
| 52 | 79 | Raw Card Data | See field 37 | See field 37 |
| 53 | 80 | Total Bits | See field 38 | See field 38 |
| 54 | 81 | User Card Category | See field 36 | See field 36 |
| 55 | 82 | Raw Card Data | See field 37 | See field 37 |
| 56 | 83 | Total Bits | See field 38 | See field 38 |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--|------------------------------------|--------------------|---------------|--|
| 57 | 84 | User Card Category | See field 36 | See field 36 |
| 58 | 85 | Raw Card Data | See field 37 | See field 37 |
| 59 | 86 | Total Bits | See field 38 | See field 38 |
| 60 | 87 | User Card Category | See field 36 | See field 36 |
| 61 | 88 | Raw Card Data | See field 37 | See field 37 |
| 62 | 89 | Total Bits | See field 38 | See field 38 |
| 63 | 90 | User Card Category | See field 36 | See field 36 |
| 64 | 91 | Raw Card Data | See field 37 | See field 37 |
| 65 | 92 | Total Bits | See field 38 | See field 38 |
| 66 | 93 | User Card Category | See field 36 | See field 36 |
| 67 | 94 | Raw Card Data | See field 37 | See field 37 |
| 68 | 95 | Total Bits | See field 38 | See field 38 |
| 69 | 96 | User Card Category | See field 36 | See field 36 |
| 70 | 97 | Raw Card Data | See field 37 | See field 37 |
| 71 | 98 | Total Bits | See field 38 | See field 38 |
| There can be up to 8 sets of user link data for a user (each set has 2 data fields). | | | | |
| 72 | 99 | User Link Server | “server name” | User Link Server ID as previously defined in Forcefield (up to 30 characters). |

| Field number | Field number (additional profiles) | Field description | Sample value | Description |
|--------------|------------------------------------|-------------------|----------------|---|
| 73 | 100 | User Link Profile | “profile name” | User Link Profile name as previously defined in Forcefield (up to 40 characters). |
| 74 | 101 | User Link Server | See field 72 | See field 72 |
| 75 | 102 | User Link Profile | See field 73 | See field 73 |
| 76 | 103 | User Link Server | See field 72 | See field 72 |
| 77 | 104 | User Link Profile | See field 73 | See field 73 |
| 78 | 105 | User Link Server | See field 72 | See field 72 |
| 79 | 106 | User Link Profile | See field 73 | See field 73 |
| 80 | 107 | User Link Server | See field 72 | See field 72 |
| 81 | 108 | User Link Profile | See field 73 | See field 73 |
| 82 | 109 | User Link Server | See field 72 | See field 72 |
| 83 | 110 | User Link Profile | See field 73 | See field 73 |
| 84 | 111 | User Link Server | See field 72 | See field 72 |
| 85 | 112 | User Link Profile | See field 73 | See field 73 |
| 86 | 113 | User Link Server | See field 72 | See field 72 |
| 87 | 114 | User Link Profile | See field 73 | See field 73 |

Importing profiles in Unique Profile Per User mode

Forcefield may be configured to operate in Unique Profile Per User mode, where user profiles (and alternative user profiles) are locked to user records. For example, user 1 can have only “User 1 Profile|” and optionally “User 1 Alt Profile|”.

The effect of Unique Profile Per User mode on user import is:

- If the import file contains profile and alternative profile names in the format “User xx Profile|” and “User xx Alt Profile|” (where xx is the user number), the profile will be imported if the name already exists in Forcefield.
- If the import file contains profile and alternative profile names that do not match the required format, the profile and alternative profile are used as templates, whose contents are used to either modify an existing profile record or to create a new record with the correct Id (as applicable).

For example, the import file contains a profile for user number 495 named “Head Office” and an alternative profile named “Head Office plus Warehouse”.

During the import process Forcefield will create or modify the profile “User 495 Profile|” whose contents will mirror the contents of “Head Office” and the alternative profile “User 495 Alt Profile|” whose contents will mirror that of “Head Office plus Warehouse”.

Appendix B

History export data formats

Summary

This appendix describes the format of exported history data files.

Content

| | |
|---|-----|
| Structure of history database record..... | 128 |
| Export raw..... | 128 |
| Export formatted..... | 129 |

Structure of history database record

| | | |
|----------------|---------------------|---|
| unsigned long | Hist_Unit | // Unit Number of device |
| unsigned short | Hist_Node | // origin node of event |
| unsigned long | Hist_Incident | // Event number |
| unsigned short | Hist_Sequence | // sequence of event within same event number |
| unsigned short | Hist_Priority | // priority of event |
| unsigned long | Hist_AresTime | // Time Computer got event |
| unsigned char | Hist_AresTmDST | // set if event occurred in daylight savings time |
| unsigned long | Hist_ChTime | // Challenger event time if applicable |
| unsigned char | Hist_ChTmDST | // set if event occurred in daylight savings time |
| unsigned short | Hist_EventState | // index into computer category |
| char | Hist_StateText[31] | // event text e.g. Tamper |
| unsigned short | Hist_Job | // not currently used |
| unsigned short | Hist_Mbr | // member number |
| char | Hist_MbrId[31] | // member name |
| unsigned short | Hist_EventType | // Forcefield event type |
| unsigned short | Hist_PointClass | // class of originating device e.g. Input |
| char | Hist_Point[31] | // name of originating device |
| char | Hist_SecPoint[41] | // name of secondary device, e.g. duress locator |
| char | Hist_Text[81] | // history text |
| unsigned long | Hist_User_Num | // User number if applicable |
| unsigned short | Hist_User_Mbr | // User member if applicable |
| char | Hist_User_or_Op[31] | // User or Operator name |
| char | Hist_WsId[31] | // Workstation name |

Note: Time fields are in UNIX format, i.e. number of seconds since midnight Jan 01, 1970.

Export raw

All fields in the above structure are exported “as is”. For example:

```
1020300000,2,107924,0,8,1087867013,0,0,0,1,"OPERATOR LOGIN",0,1024,"~Default-
MbrGrp",898,0,"Node 2 Console","", "",0,0,"Master(Default Master)", ""
80,0,107871,0,4,1087827426,0,0,0,0,"COMPUTER EVENT",0,1024,"~Default-
MbrGrp",1281,0,"","", "Time Change Detected. Node 2",0,0,"", ""
```

Export formatted

Time fields are readable. For example:

```
107924,"Tue Jun 22 11:16:53 2004 ","","OPERATOR LOGIN","~Default-MbrGrp","Node 2  
Console","","",0,"Master(Default Master)",""
```

```
107871,"Tue Jun 22 00:17:06 2004 ","","COMPUTER EVENT","~Default-MbrGrp","","","Time  
Change Detected. Node 2",0,"",""
```

The fields exported are:

- incident
- computer time
- challenger time
- state text
- member id
- point id
- secondary point id
- text
- user number
- operator or user name
- workstation name

Appendix C

Integrating legacy DVRs

Summary

This appendix describes the hardware requirements and limitations of integrating Forcefield to legacy DVRs, including *SymDec™ 16 plus 4* DVR or *SymSafe Pro™* DVRs. We refer to either of these products as legacy DVRs.

Note: Refer to Appendix D “Integrating DVRs” on page 141 for current video products.

Content

| | |
|---|-----|
| Overview | 132 |
| Legacy DVR integration process | 133 |
| Before you begin..... | 134 |
| Overall process..... | 134 |
| Limitations | 135 |
| Forcefield programming | 135 |
| Forcefield-legacy DVR hardware requirements | 135 |
| Recommended hardware..... | 136 |
| Combined hardware list | 137 |
| Application notes..... | 139 |
| CPU usage | 139 |
| Loss of video stream..... | 139 |
| Forcefield user interface | 140 |
| Supported video hardware | 140 |

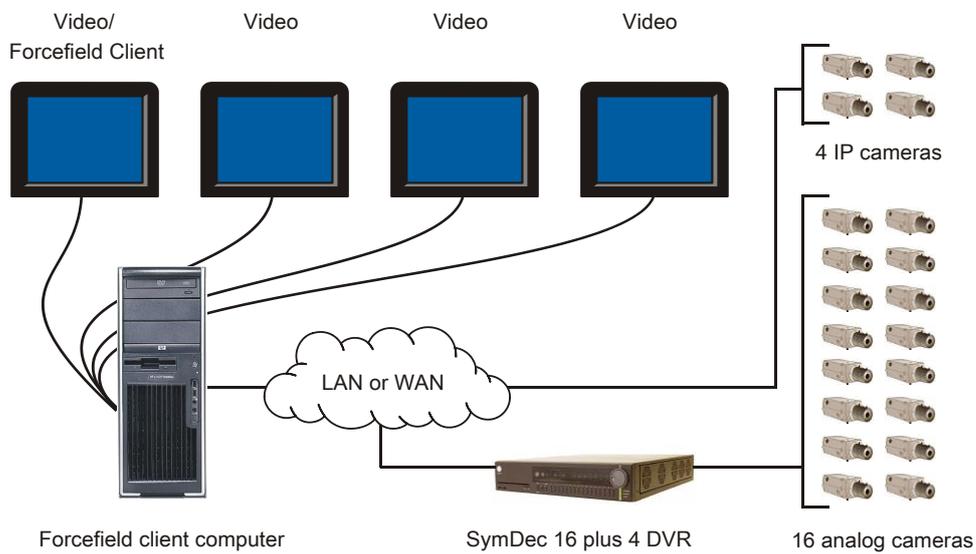
Overview

A Forcefield Client computer can display video image streams from SymDec™ 16 plus 4 digital video recorder (DVR) and SymSafe Pro™ DVR in multiview windows as well as live view and recorded view windows on one or more computer monitors. Collectively, we refer to these products as “legacy DVR”.

Legacy DVRs allow you to record full-size D1 images in real time on analogue channels and on IP channels (subject to hardware and network capabilities).

Forcefield multiview can be configured to display the views from up to 32 cameras on up to four monitors. Multiple instances of Forcefield multiview windows can be displayed simultaneously, using multiple computer monitors (Figure 33 below).

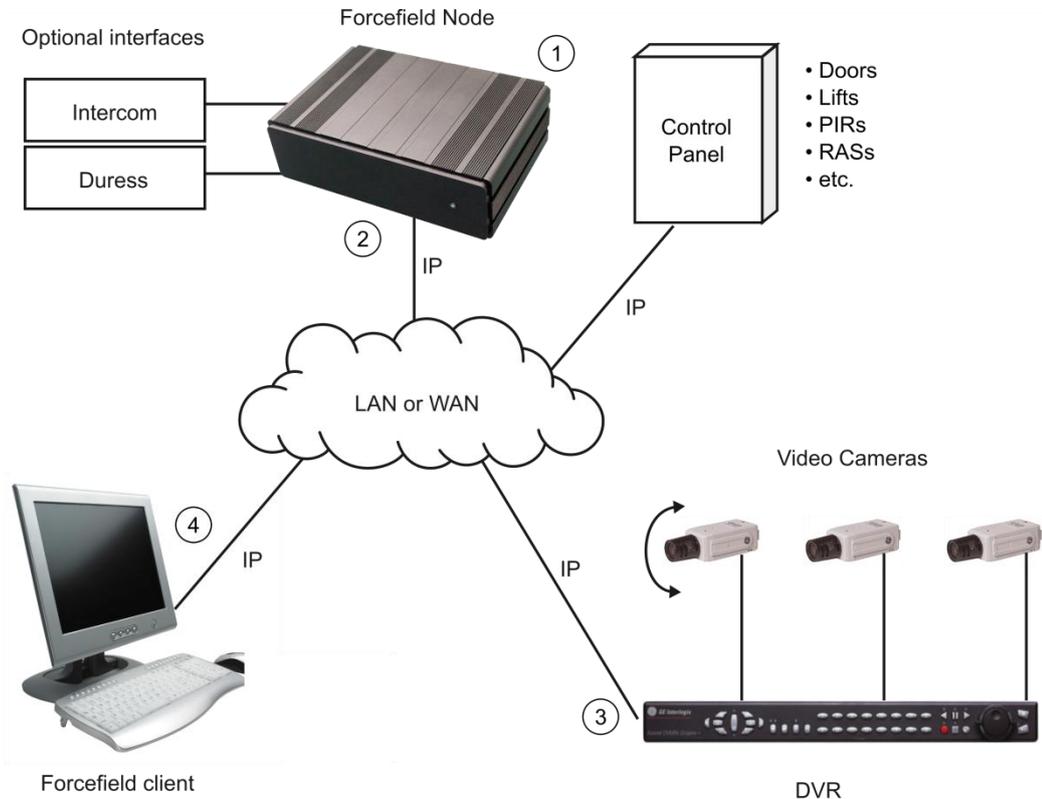
Figure 33: Forcefield client computer with multiple monitor video card



Each digital video view displayed by Forcefield is processed by the Forcefield client computer’s CPU from data received from legacy DVR via the IP network. As a result, the processing power of the Forcefield client computer’s CPU limits the number of digital video views that can be displayed simultaneously. Refer to the following specific recommendations concerning suitable hardware and software configurations.

The (discontinued) range of supported legacy DVR products includes SymDec 16 plus 4 or SymSafe Pro DVRs.

Figure 34: Overview of legacy DVR interface



1. The Forcefield node receives events from a Challenger panel or from other interfaces, as defined by computer categories created for this purpose. The image represents both standard and Enterprise Forcefield hardware.
2. The legacy DVR is connected to the Forcefield node via an Ethernet port. A TCP/IP host address is defined for this purpose. The IP connection to the Forcefield node does not carry digital video.
3. Forcefield sends event tags (associated with a camera) to the legacy DVR. The event tag is recorded with the camera's digital video footage.
4. A Forcefield operator on a Windows computer can view live video and/or recorded video directly from the legacy DVR (not via the Forcefield node's IP connection). Events can be found quickly by searching for text tags.

Legacy DVR integration process

This section describes the overall process of integrating legacy DVR devices into Forcefield.

Refer to the Databases > Video > DVR Video menu section in the *Forcefield Operators Manual* for details about programming DVRs, cameras, monitors, and presets. The information provided in this section is only a summary.

Before you begin

In order to use legacy DVR functionality you need the following:

- The Forcefield system must be licensed for DVR integration. The TS9117 Interlogix DVR license module is required, and the installer must be trained for Forcefield Integration.
- The Forcefield server computer must have Forcefield software version 6.0.2, or later, installed. Forcefield software version 6.0.1 may be used provided that the Forcefield client computer has Forcefield Client software version 1.0.7.30, or later, installed.
- The SymDec 16 plus 4 DVR must have firmware V1.51E, or later, installed (provided on the Forcefield Installation CD or USB device). The SymSafe Pro DVR must have firmware V1.30B, or later, installed. For firmware updates, check the Video Surveillance Web page at <http://utcssecurityproducts.com/Customersupport/Pages/VideoSurveillance.aspx>

The ability of a Forcefield Client computer to display video is subject to the computer's hardware, operating system, video card, and network bandwidth.

Overall process

The overall process for integrating a legacy DVR into Forcefield is:

1. Use the Databases > Computer Equipment > TCP IP Hosts command to create a TCP/IP Host record for the IP host for legacy DVRs. Note the Host ID.
2. Use the Admin > Configuration > Configuration command to open the Forcefield Configuration window, and then click the CCTV/Intercom button. Configure a time for the "DVR: Tagging By Mgt. SW Delay" option.
3. Use the Databases > Video > DVR Video > DVRs command to program a DVR:
 - Click the Type arrow, and then select DVMRe or SymDec/SymSafe (as applicable) for legacy DVRs.
 - Click the IP Address field, and then select the appropriate Host ID.
 - Leave the Enabled selection unchecked so that you can program the DVR, cameras, monitors and presets before actually physically connecting the equipment to the Forcefield system.
4. Use the Databases > Video > DVR Video > DVR Cameras command to program a video camera. Select the DVR to which this camera is connected, and specify whether the camera has pan-tilt-zoom (PTZ) control.
5. If applicable, use the Databases > Video > DVR Video > DVR Presets command to program and name predefined views for PTZ cameras.

Tip: The names that you assign to a presets 1 through 5 are added to the camera's pop-up menu on maps displaying the camera.

6. Connect the DVR to the network.
7. Use the Databases > Video > DVR Video > DVRs command, and then check the Enabled selection to enable a DVR.

Limitations

Some customers may experience problems integrating legacy DVRs with Forcefield client computers, especially when viewing multiple video streams. To avoid problems, customers will need to use only the recommended hardware and software configurations described in this Appendix (see “Forcefield-legacy DVR hardware requirements” below). In particular:

- Camera presets are not supported for cameras connected to the legacy DVR’s IP ports.
- If a Forcefield Client computer’s operating system is upgraded (for example from Windows XP SP3 to Windows Vista) video pop-up functionality may not work. If so, you may need to reinstall the latest version of Forcefield client software on the client computer.

Forcefield programming

SymSafe Pro DVR uses the same programming in Forcefield as SymDec 16 plus 4 DVR. For example, in the DVR programming window, select “SymDec/SymSafe” to use either SymDec 16 plus 4 DVR or SymSafe Pro DVR.

SymSafe Pro DVRs are available in 4, 8, and 16 channel models. Consider the model when programming or using Forcefield multiview windows.

Forcefield-legacy DVR hardware requirements

The Forcefield client application supports the use of legacy DVR to display multiview video on multiple computer monitors. The number of video streams and monitors that can be used depends on:

- The image resolution. We test at full-size D1 resolution in order to test the worst-case scenario.
- The frame rate (fps) used. A lower frame rate typically enables you to view more video streams.
- The Forcefield client computer’s hardware specifications.

Notes:

- This section contains references to legacy Windows operating systems and legacy computer hardware. We will not update this legacy section to accommodate current versions.

- You must use the specified hardware (or better) in order to benefit from the software's capabilities. The increased video performance of Forcefield 6.0 requires different hardware configurations than those required for Forcefield 5.3. If you upgrade to Forcefield 6.0 software on version 5.3 hardware, you will not be able to use all of the added functionality.

The recommended configurations for Forcefield client computers using legacy DVRs can be found in the following locations:

- Refer to *Technical Bulletin 20080905-TS9100* for details of using SymDec 16 plus 4 DVR with Forcefield 5.3. These hardware configurations can be used for Forcefield 6.0, but the increased video performance that Forcefield 6.0 supports requires the hardware described in this section.
- Refer to this appendix for details of using legacy DVRs with Forcefield 6.0.

Refer to the "Combined hardware list" on page 137 for a summary of hardware combinations that may be used with Forcefield 6.0. This list applies to both SymDec 16 plus 4 DVR and SymSafe Pro DVR, except as noted.

Recommended hardware

We have tested and approved specific configurations of Forcefield client computer hardware, network configurations, and monitors. In each case, a 1000 Mb/s network connection is provided, and all monitors are set to a screen resolution of 1280 by 1024 pixels.

Note: Any unused monitors must not be enabled or they will consume resources. To disable unused monitors, use the Display option in Windows Control Panel to open the Display Properties window (Settings tab).

The minimum specification for a Forcefield client computer integrated with legacy DVR depends on the number of simultaneous video streams you need to view.

Refer to the following sections for a summary of minimum and high-performance applications.

Minimum legacy DVR use

A Forcefield client computer that is to be used only for displaying live and recorded views (not multiview) from a legacy DVR must have the following specifications:

- Processor: Intel Pentium 4, 1.6 GHz or faster
- Operating system: Windows XP (SP2) or Windows Vista (SP1)
- RAM: 256 MB or larger
- HDD: 120 GB or larger (7200 rpm minimum)
- Video Card: 1 x 64 MB or larger
- Monitor: 1
- Simultaneous video streams: 2

Maximum legacy DVR use

A Forcefield client computer that is to be used for displaying live and recorded views of up to 32 video streams on up to four monitors from multiple legacy DVRs must have the following specifications:

- Processor: Intel Core 2 Quad, 2.40 GHz or faster
- Operating system: Windows XP (SP2) or Windows Vista (SP1)
- RAM: 4 GB or larger
- HDD: 120 GB or larger (7200 rpm minimum)
- Video Cards: 2 x NVIDIA chipset with 512 MB or larger (for example, Quadro FX 1700)
- Monitors: 1 to 4
- Simultaneous video streams: 16 per monitor, 32 maximum

Combined hardware list

This section describes the video performance that you can expect from Forcefield 6.0 for various computer hardware configurations, at full-size D1 resolution, and for two frame rate selections. For intermediate frame rates such as 12.5 fps, the performance will fall between the specifications listed.

The hardware configurations listed in the this section may be used to display video image streams from legacy DVR in multiview windows.

Table 11 on page 138 lists the computer hardware recommended for use with Forcefield 6.0. The following configurations were tested:

Computer A: HP xw4600, Intel Core 2 Quad Q6600, Windows XP SP2, 4 GB RAM

Computer B: HP xw4600, Intel Core 2 Quad Q6600, Windows Vista SP1, 4 GB RAM

Table 12 on page 138 lists the computer hardware recommended for use with Forcefield 5.3 but may be used with Forcefield 6.0. The following configurations were tested:

Computer C: HP xw6600, Quad-Core Xeon 3.00 GHz, Windows XP, 4 GB RAM

Computer D: HP xw4600, Quad-Core Xeon 2.40 GHz, Windows XP, 4 GB RAM

Computer E: HP xw4600, Quad-Core Xeon 2.40 GHz, Windows Vista SP1, 4 GB RAM

The “Max. on one (remaining)” columns indicate the maximum number of video streams that can be displayed on one monitor, with the remaining streams available indicated in brackets. For example, 16 (16) indicates that 16 video streams can be displayed on one monitor and 16 remaining streams can be displayed on additional monitors.

The “Monitors” columns indicate the maximum number of monitors, including any monitors required to display the Forcefield operator interface, if needed.

Table 11: Video performance for Forcefield 6.0 using recommended hardware

| Computer configuration | Video card 1 Video card 2 (if used) | Monitors | Frame rate (D1) | Total video streams | Max. on one (remaining) |
|------------------------|--|----------|-----------------|---------------------|-------------------------|
| A | NVIDIA Quadro FX-1700 No second card | 2 | 25 fps | 10 | 10 (0) |
| | | 2 | 8.3 fps | 32 | 16 (16) |
| A | NVIDIA Quadro FX-1700 NVIDIA Quadro FX-1700 | 4 | 25 fps | 10 | 10 (0) |
| | | 4 | 8.3 fps | 32 | 16 (16) |
| A | NVIDIA Quadro FX-1700 NVIDIA Quadro NVS440 | 6 | 25 fps | 10 | 10 (0) |
| | | 6 | 8.3 fps | 32 | 16 (16) |
| B | NVIDIA Quadro FX-1700 No second card | 2 | 25 fps | 12 | 12 (0) |
| | | 2 | 8.3 fps | 20 | 12 (8) |

Table 12: Video performance for Forcefield 6.0 using Forcefield 5.3 hardware

| Computer configuration | Video card 1 Video card 2 (if used) | Monitors | Frame rate (D1) | Total video streams | Max. on one (remaining) |
|------------------------|--|----------|-----------------|---------------------|-------------------------|
| C | NVIDIA Quadro NVS440 NVIDIA Quadro NVS440 | 8 | 25 fps | 8 | 1 (7) |
| | | 5 | 5 fps | 20 | 4 (16) |
| D | NVIDIA Quadro NVS440 No second card | 4 | 25 fps | 9 | 4 (5) |
| | | 4 | 5 fps | 12 | 4 (8) |
| E | NVIDIA Quadro NVS440 No second card | 4 | 25 fps | 8 | 4 (4) |
| | | 4 | 5 fps | 12 | 4 (8) |

Notes:

- Remember that in any configuration, you may need to use one monitor to operate Forcefield if the client computer is not dedicated to displaying video.
- Programming camera multiviews to display different views frequently (short dwell time) may exceed the CPU resources as tested in this document.
- You must ensure that the fps rate in event and alarm conditions does not exceed the ability of the computer to display video. Systems were tested with static camera multiviews, so that camera views did not change after a programmed dwell time.
- SymSafe Pro DVRs are available in 4, 8, and 16 channel models. If using SymSafe Pro instead of SymDec 16 plus 4, the maximum number of video streams may be limited by the number of channels available in your SymSafe Pro model.

- SymSafe Pro DVRs at D1 resolution have a maximum supported frame rate of 12.5 fps per camera.
- If recommended hardware is not available, use hardware with equivalent or better specifications. For example, HP Z400 may be used in place of HP xw4600; HP Z600 may be used in place of HP xw6600; and the video card NVS450 may be used in place of NVS440.
- Use Windows XP for best performance in displaying multiple video streams as compared to Windows Vista on a given computer.

Computer hardware specifications and capabilities may change. Check our Web site at www.interlogix.com.au for updates as they become available.

Application notes

CPU usage

For video streaming to work effectively, it's important that the Forcefield computer's CPU isn't overloaded. Forcefield monitors the computer's CPU usage for each view in a multiview window. If the CPU usage exceeds 90% for more than 20 seconds, Forcefield will close one or more video streams and display the message "Stopped due to high CPU usage" in place of the closed view. This process repeats after 20 seconds, so in cases where multiple video streams are causing (or coinciding with) excessive CPU usage, additional streams may close starting roughly 40 seconds from the first stream closing.

When configuring your system, We recommend that you use the Windows Task Manager, Performance tab, to monitor CPU usage when all video streams are displayed, and all cameras configured at the fps rate that will be used in event or alarm conditions (refer to the legacy DVR's user manual for details).

Note: Configure your system such that the CPU usage will not exceed 90% for more than 20 seconds, or Forcefield will turn off one or more video streams.

Loss of video stream

When streaming from the legacy DVR stops on any particular stream for a period of five seconds, that particular window will display a black background and will display "No video stream received from SymDec". If streaming restores, the window will return to displaying the camera view. Note that this can also appear if the UDP ports are blocked by a firewall.

Forcefield user interface

Forcefield's legacy DVR interface differs slightly from the DVMRe interface, as follows:

- The Skip Backward and Skip Forward buttons allow a user to jump backward or forward by a configurable number of seconds (5 to 300, the default is 20). Press either button multiple times to make multiple jumps. Forcefield starts playing forward automatically after making a jump. Adjust the number of seconds skipped by dragging the track bar (below the buttons) to the left or right.
- The Play Reverse button isn't available. Use the Skip Backward button instead.
- Playback speed is not applicable to SymDec.

Supported video hardware

Forcefield 6.0 (and later) supports only Legend IP PTZ dome cameras and SymNet IP encoder/decoder.

Appendix D

Integrating DVRs

Summary

This appendix describes how to integrate CCTV equipment that uses the Interlogix video service and plug-in modules.

Content

| | |
|--------------------------------------|-----|
| Overview | 142 |
| DVR integration process..... | 143 |
| Before you begin..... | 143 |
| Setting up the video server | 144 |
| Installing VSM..... | 144 |
| Installing VSM plug-in modules..... | 145 |
| Setting up video clients..... | 145 |
| Installing VPC | 145 |
| Installing VPC plug-in modules | 146 |
| Setting up the video service..... | 146 |

Overview

“Video service” refers to the use of plug-in modules to support CCTV equipment from various manufacturers.

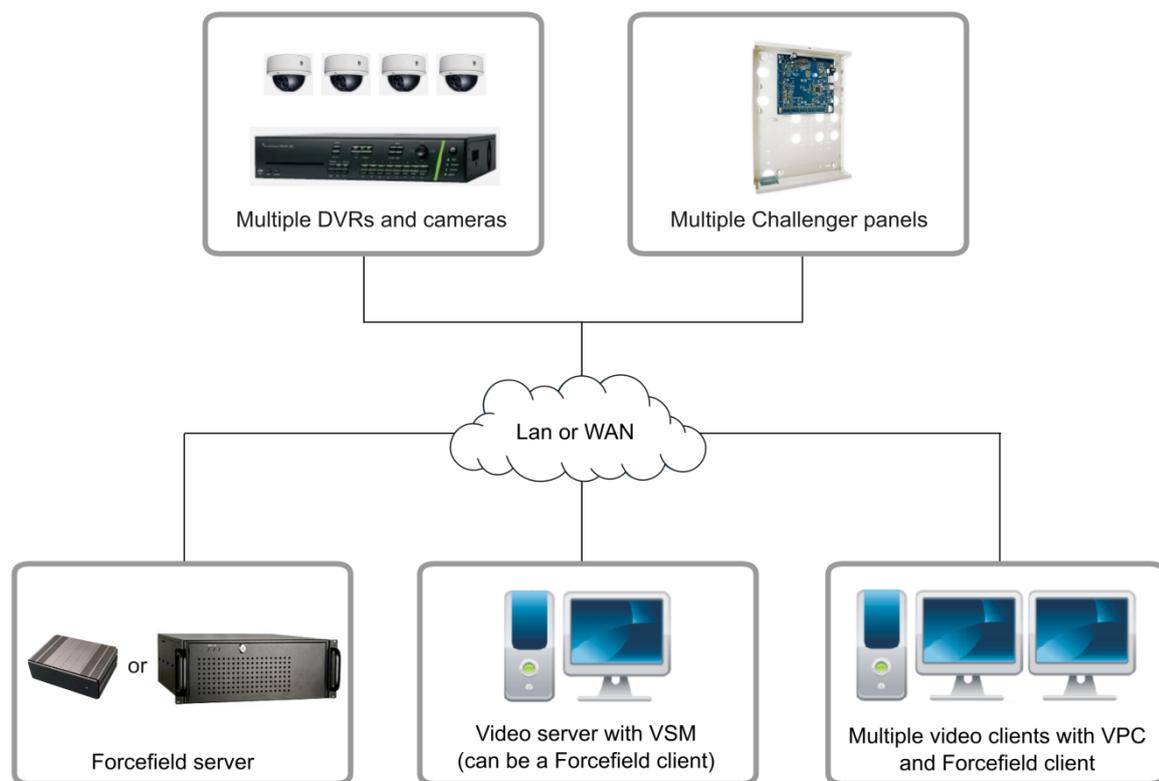
Legacy equipment such as DVMRe, SymDec, and SymSafe are supported natively in Forcefield and do not use add-on video service applications. Refer to Appendix C “Integrating legacy DVRs” on page 131.

Forcefield 7.1 (and later) uses add-on video service applications (each with one or more brand-specific video plug-in modules) to provide the interface between Forcefield and CCTV devices.

- Video Status Manager (VSM) and brand-specific VSM plug-in modules must be installed on one Windows computer per Forcefield system. The computer with VSM is the video server.
- Video Presentation Client (VPC) and brand-specific VPC plug-in modules must be installed on each Forcefield client computer that is used for controlling or viewing video. Each computer with VPC is a video client.

Refer to Figure 35 below for an illustration of a Forcefield system with separate computers used as the video server (VSM) and video clients (VPC). Alternatively, the VSM and VPC and Forcefield client can be installed on the same computer.

Figure 35: Overview of DVR integration



DVR integration process

This section describes the process of integrating DVRs and cameras into a Forcefield system via the video service.

The information provided in this section is only a summary. Refer to the *Forcefield Operators Manual* for details about programming the following options:

- Databases > Video menu section for programming the video service.
- Databases > Video > DVR Video menu section for programming DVRs, cameras, and presets.

For the video service record, you will need to have:

- A TCP/IP host port for the video service connection between the video server computer and any video client computers.
- A unique “Session ID” used in the video service record, and in the VSM and VPC configuration windows.
- The VSM port number (default is 9300).

For the DVR record, you will need to have:

- In the case of TruVision DVRs, you must specify the type via the model name (such as “Type=TVR60”) in the DVR record’s “Other” field.
- The video service’s “Session ID”.
- A custom computer category that you created (that does not require restoral for any events).
- The DVR’s IP address, port, protocol, user name and password.

Before you begin

In order to use video service functionality you need the following:

- The use of video service DVRs requires at least one of TS91716 16-camera license module or TS91732 32-camera license module.
- The Forcefield server computer must have Forcefield software version 7.1.0, or later, installed. The Forcefield client computer must have Client version 2.1.1, or later, installed.
- Any computer with VSM and/or VPC must also have Microsoft .NET Framework 4 installed.
- Plug-in modules may have other specific requirements. Refer to the plug-in module’s datasheet for details.
- DVRs must have correct firmware. Check the manufacturer’s web site for updates.

Refer to the applicable DVR datasheets for workstation hardware requirements.

Setting up the video server

One Windows computer per Forcefield system must be the video server.

We recommend that the video server is also a Forcefield client because the VSM gets the address of the primary and mirror nodes from the registry keys provided by the Forcefield client.

Install the VSM and then the brand-specific VSM plug-ins, as described in the following sections.

Installing VSM

Install VSM on a Forcefield client computer (or other Windows computer). The computer must have Microsoft .NET Framework 4 installed.

Note: If VSM has been previously installed on this computer, then remove it before reinstalling.

Make note of the following details:

- Forcefield site name (exactly as licensed, and displayed in the top left of the Forcefield window).
- The unique “Session ID” used in the video service record, and in the VSM and VPC configuration windows.
- The server’s VSM port number (default is 9300)

To install VSM:

1. From the Forcefield Web Toolbox (Installation page), click “Install Video Status Manager (VSM)”. Alternatively, browse to the Install folder and run “VSMinstall.exe”. The “Welcome to the Video Status Manager Service Setup Wizard” displays. Click Next to continue.
2. Type the server’s VSM port number (default is 9300).
3. Type the Forcefield site ID (exactly as licensed, and displayed in the top left of the Forcefield window).
4. Type the “Session ID” (also used in the video service record), and then click Next to continue.
5. Accept the suggested installation folder, and then click Next to continue. Alternatively, click Browse to select a different location before clicking Next.
6. When the “Installation Complete” message displays, click Close.

To edit the details after installation, click Start > All Programs > Video Status Manager Configuration.

Installing VSM plug-in modules

Visit our website at www.interlogix.com.au for brand-specific plug-ins and installation instructions.

Setting up video clients

Each Forcefield client computer that is used for controlling or viewing video must have VPC installed.

Notes:

- Video client computers must have User Account Control set to “never notify”. To verify or change the User Account Control settings go to Control Panel > System and Security > Action Center.
- When starting a video client computer (Forcefield Client), you must log in as a user with Administrator privileges in Windows.

If you intend to install both VSM and VPC on the same computer, then follow the instructions in “Setting up the video server” on page 144 before you proceed.

Installing VPC

Install VPC on each Forcefield client computer where video is required. Each computer must have Microsoft .NET Framework 4 installed.

Note: If VPC has been previously installed on this computer, then remove it before reinstalling.

To install VPC:

1. From the Forcefield Web Toolbox (Installation page), click “Install Video Presentation Client (VPC)”. Alternatively, browse to the Install folder and run “VPCinstall.exe”. The “Welcome to the Tecom Video Presentation Client Setup Wizard” displays. Click Next to continue.
2. Enter the details noted in “Installing VSM” on page 144, except for the client’s VPC port number (default is 9200). Do not use the same port number as the server.
3. In the Video Status Manager Server field enter the video server’s IP address (or type “localhost” if VPC and VSM are on the same computer).
4. Accept the suggested installation folder, and then click Next to continue. Alternatively, click Browse to select a different location before clicking Next.
5. At the Confirm Installation screen, click Next to continue.
6. When finished, an “Installation Complete” message displays.
7. Click Close.

To edit the details after installation, click Start > All Programs > Video Presentation Client Configuration.

Installing VPC plug-in modules

Visit our website at www.interlogix.com.au for brand-specific plug-ins and installation instructions.

Setting up the video service

To set up the video service:

1. Use the Databases > Video > Video Service command to create a Video Service record.
2. Type a unique name for this video service record in the ID field.
Note: Cameras, Monitors, Presets, Matrix Switchers, DVRs and Video Service records are kept in the same database, the Id must be unique across all of these devices.
3. Type a description for this video service record in the Desc field.
4. Click the Type arrow and select Interlogix.
5. Click the Address arrow, and then select the previously-defined Host ID (select the TCP/IP Host record for the VSM computer's IP address).
6. In the session ID field type the session password defined in "Installing VSM" on page 144.
7. In the Port field type the server's VSM port number (default is 9300).
8. Right-click the Enabled check box to populate it.
9. Use the Admin > Configuration > Configuration command to open the Forcefield Configuration window, and then click the CCTV/Intercom button.
 - In the Video Service VPC Port field, type the port number (default is 9200) that the VPC will use to listen for data.
 - Configure a time for the "DVR: Tagging By Mgt. S/W Delay" option.

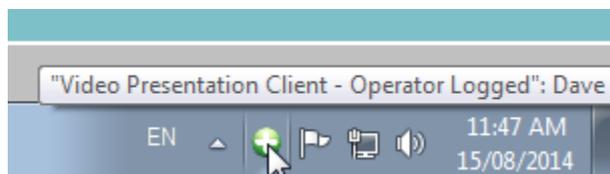
Checking the VPC connection:

Any time a Forcefield client is started, VPC starts and attempts to connect with Forcefield. The VPC icon in the Windows taskbar (Figure 36 on page 147) can display three states:

- A red icon with an x indicates that VPC cannot connect with Forcefield.
- A blue icon with a – indicates that VPC is connected with Forcefield, but there is no Forcefield operator logged in.

- A green icon with a + indicates that VPC is connected with Forcefield, and there is a Forcefield operator logged in.

Figure 36: Video Presentation Client icon



Notes:

- The video service must be defined and enabled.
- At least one (video service) DVR must be enabled before the video service can connect to the video server.
- The taskbar must display a blue or green icon with a + before you can connect to DVRs or cameras.

Refer to the *Forcefield Operators Manual* for details about programming DVRs, DVR cameras, and DVR camera presets.

Glossary

| | |
|-------------------------|--|
| Ascom Nira | Brand name for Ascom Nira 960 duress system. |
| Capture | Use of a video camera connected to a Forcefield client to capture an image for use in a Photo ID system. |
| Card Layout Editor | Photo ID user card design application for Forcefield clients. |
| CCTV | Closed Circuit Television |
| CCTV switcher | Part of the CCTV system, a CCTV switcher (connected to Forcefield) controls video cameras and monitors. |
| Duress | <p>The Ascom Nira 960 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 |
| Email | Forcefield can be set up to send an email message to a specified recipient when an event occurs. |
| Intercom | <p>The Jacques 550 Series intercom system is comprised of master and slave intercoms that interface with Forcefield.</p> <p>The Forcefield intercom interface is comprised of icons on maps and Speed Bar buttons to control volume.</p> <p>The operator clicks the icon to open the intercom channel and to switch the intercom video camera to the workstation's intercom monitor.</p> |
| Intercom Level 1 Master | Part of the Jacques 550 Series intercom system, level 1 masters are located near Forcefield workstations and are connected to the Level 2 master. Level 1 masters serve as intercoms for Forcefield operators. |
| Intercom Level 2 Master | Part of the Jacques 550 Series intercom system, a single Level 2 master is connected to a Forcefield comm port. The Level 2 master serves as the intercom for the Forcefield supervisor. |
| Intercom Slave | Part of the Jacques 550 Series intercom system, each intercom master can have up to 255 slave units. Intercom calls are requested by pressing a call button. |
| LAP | Live Animation Point indicates position and status of a device under control of Forcefield. |
| NVR | Network video recorder |

| | |
|----------------|--|
| Paging | Forcefield can be set up to page via the Ascom Nira Duress system when an event occurs. A page is a text message which can be announced by a series of beeps or a siren, or not announced. |
| Photo ID | Photo ID user card design and printing facilities are provided for Forcefield clients. |
| PTZ camera | Pan-Tilt-Zoom video camera |
| Legacy DVR | SymDec™ 16 plus 4 DVR or SymSafe Pro™ DVR |
| Third-party | An external system which can communicate with Forcefield using the Forcefield third-party system protocol. |
| TruVision | Interlogix range of cost-effective video surveillance DVRs and cameras. |
| TVR | TruVision DVR |
| User Link | User mapping between Forcefield and a third-party user link control system (for example, a lift system). |
| Video switcher | See CCTV switcher |
