Forcefield® Installation and Setup Manual

P/N MAINST-TS9100 • REV 14 • ISS 10APR18

Trademarks and patents

The Forcefield name and logo are trademarks of UTC Fire & Security Australia Pty Ltd.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

UTC Fire & Security Australia Pty Ltd t/a Interlogix
A UTC Climate, Controls & Security company
10 Ferntree Place
Notting Hill, Victoria, 3168, Australia

ACMA compliance

 N4131

Contact information

For contact information, see www.interlogix.com.au.

Content

Important information

This is the *Forcefield® Installation and Setup Manual*. This manual is for use by trained and assessed Forcefield installation technicians and provides the following information:

- Forcefield system overview (see Chapter 2 “System overview” on page 3).
- How to set up the Forcefield server (see Chapter 3 “Setting up Forcefield” on page 9).
- How to install Forcefield on client computers (see Chapter 4 “Installing Forcefield Client” on page 31).
- How to upgrade a Forcefield system by adding modules (see Chapter 5 “Upgrading a Forcefield system” on page 41).
- Typical system applications showing connections between a Forcefield node, Challenger® panels, and other devices (see Chapter 6 “Forcefield system application” on page 49).

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

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

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. See “Improved main menu” on page 4, and 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.

Agency compliance

This product conforms to the standards set by Standards Australia on behalf of the Australian Communications and Media Authority (ACMA).

Notice! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

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

Interlogix advises that only trained Forcefield installation technicians should install or program a Forcefield system. Only trained and assessed Forcefield integration technicians should integrate third-party systems and use the QNX shell to alter system configuration. Forcefield Integration training is required for multi-node use and DVR integration.

Scope of this manual

This manual describes how to set up Forcefield system management hardware and software including the Forcefield server computer, Forcefield client on Windows computers, and how to upgrade an existing Forcefield system. It also describes some typical security system configurations using Challenger panels and peripheral equipment.

It does not describe how to design, install, or configure a security system.

Related documents

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.

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

For details about Challenger programming refer to the following manuals:

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

Refer to the *TS0099 Enhanced Challenger TCP/IP Interface Installation and Programming Guide* for details about setting up IP communications with a Challenger V8 panel.

Chapter 2
System overview

Summary

This chapter describes the Forcefield features of interest to installation technicians. It provides an overview of Forcefield features of interest to installation technicians, how Forcefield can be used in typical security systems, and various configuration options.

Refer to *Key Forcefield Concepts* in the *Forcefield Operators Manual* for an overview of Forcefield.

Content

Key features

Improved main menu

Forcefield version 6.0 or later has a revised main menu layout to help operators quickly navigate the system. The former main menu layout (classic menu) is retained as an alternative so that experienced operators don't need to relearn the system. This manual refers to the classic menu locations of commands.

Enterprise edition

Forcefield version 5.2.0 or later supports the use of 'Enterprise' features, consisting of a high-capacity server, connecting with additional non-controlling nodes, and additional Windows client computers (subject to client licensing). Non-controlling nodes can use either standard or Enterprise hardware. Enterprise hardware can connect with more Challenger panels than standard hardware.

Multi-node capability

Forcefield version 5.1.5 or later can be licensed to operate using a server plus non-controlling nodes.

Backup server facility

Subject to licensing, Forcefield version 6.2 or later supports offsite redundancy (data mirroring). Offsite redundancy replaces DiskShadow redundancy used in Forcefield 6.1.

Interface to CCTV

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

- Legacy DVRs (such as DVMRe, SymDec, and SymSafe).
- DVRs via "video service" applications Video Status Manager (VSM), Video Presentation Client (VPC), and brand-specific plug-in modules.

Refer to the *Forcefield External Interfaces Manual* for the process of installing VSM and VPC, and integrating DVRs and cameras into a Forcefield system via the video service.

Network printing

Either a Forcefield node or a Forcefield Client may print via the network.

Remote computer connectivity

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

Forcefield will also connect to external storage devices allowing backups to be written to remote computer systems by using either NFS or SMB (Server Message Block)/CIFS (Common Internet File System).

Forcefield hardware

Forcefield standard edition

Standard hardware (Figure 1 on page 6) is used for the primary controlling node (and optionally the backup controlling node). The user interface is provided via the Forcefield Client application on Windows computers. A standard Forcefield system can process approximately 10 events per second.

Forcefield Enterprise edition

Rack-mount hardware with RAID storage (Figure 1 on page 6) is used for the primary controlling node (and optionally the backup controlling node). Non-controlling nodes can use any Forcefield hardware. Enterprise hardware can connect with more Challenger panels than standard hardware. The user interface is provided via the Forcefield Client application on Windows computers. A Forcefield Enterprise system can process approximately 20 events per second.

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

Standard hardware

Enterprise rack-mount hardware

Enterprise VM rack-mount hardware

Forcefield Enterprise VM edition

Slim rack-mount hardware with RAID storage and redundant power supplies is used for the primary controlling node (and optionally the backup controlling node). Non-controlling nodes can use any Forcefield hardware. Enterprise VM hardware can connect with more Challenger panels than standard hardware. The user interface is provided via the Forcefield Client application on Windows computers. A Forcefield Enterprise VM system can process approximately 20 events per second. Forcefield Enterprise VM is the only version of Forcefield to run within a virtualized environment by utilizing VMware.

Hardware Setup

Note: Please ensure that the Forcefield Enterprise VM Hardware is correctly connected to power. To operate properly two power supplies are used in the server. Both must be connected to power.

Note: Please also connect a keyboard and monitor to the appropriate ports. The VGA and USB ports exist at both the front and rear of the server. Either set may be used.

1. Ethernet – General: Used by the VM and Forcefield
2. Ethernet – iDRAC: Used by the server to configure and transmit hardware events (e.g. hard drive failure, or power supply failure).

Figure 2: Rear view of the R360 Rack Mount Server

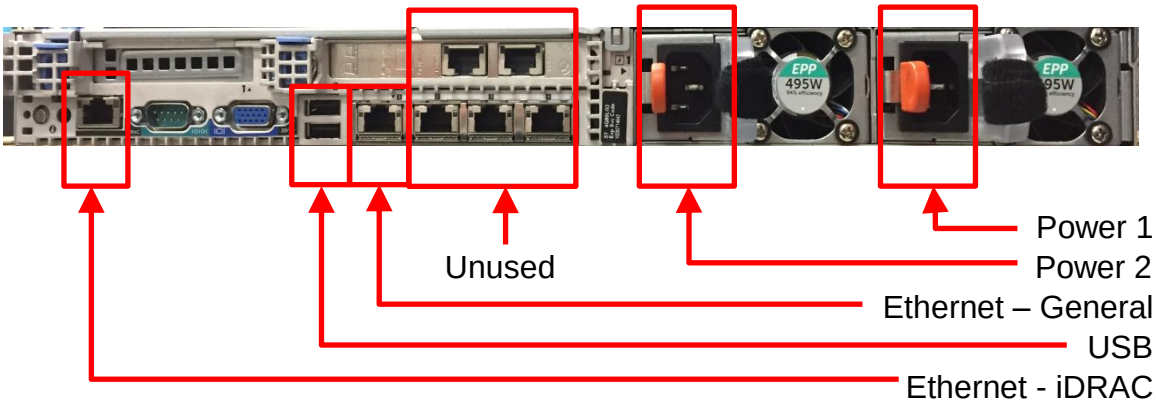


Table 1: Dell PowerEdge R630 Rack Mount Server

Item	Server Requirement
Processor	Intel Xeon ES-2609 v4, 1.7 GHz, 20M Cache
Memory	8 GB RDIMM, 2400MT/s, single rank, x8 Data Width
Hard Disk	2 x 200 GB SSD Write intensive 6 Gbps 2.5 in. Hot-plug drive

Table 2: Client PC Settings

Item	VM requirement
Processor	Core i5 or greater, minimum 2 cores enabled
Memory	2 GB or greater
Hard Disk	60 GB or greater
Video Display	720p Display or higher
LAN	100/1000 MB/s Ethernet
Operating System	Windows 7 or Windows 8.1

Backup controlling node

Forcefield can have a separate computer as a hot standby backup controlling node. If the primary server fails, the backup server automatically takes over, the other nodes automatically connect to the new server. The Forcefield Title Bar displays orange to indicate that Forcefield is running from the backup server. A backup controlling node must not have any Challenger panels or clients connected to it.

A backup controlling node must be the same hardware type as the controlling node (i.e. you cannot have an Enterprise primary controlling node and a standard edition backup controlling node).

Forcefield's automatic change-over functionality includes only Challenger panel IP connections. Other equipment such as printers, video switchers, etc.,

connected to a serial or parallel port on the controlling node will be logically connected to the corresponding port on the backup node.

Note: The physical connection to serial or parallel ports must be handled by third party switching equipment.

System capacities

The capacity of a Forcefield system to connect with client computers and Challenger panels depends on the type of hardware used (standard or Enterprise) and the number of nodes in the system. If one node is set aside as a backup controlling node it must not be connected to any Challenger panels.

Refer to the Forcefield Data Sheet for details.

Chapter 3
Setting up Forcefield

Summary

This chapter describes how to set up the core Forcefield system that runs on Forcefield hardware (see Figure 1 on page 6).

Content

Overview

Refer to *Key Forcefield Concepts* in the *Forcefield Operators Manual* for an overview of Forcefield system types.

The basic Forcefield setup consists of a Forcefield server with QNX and Forcefield installed. This computer is considered to be the server (node 1). The Forcefield server is connected via LAN, WAN or modem to one or more licensed Forcefield clients (Windows computers with Forcefield Client installed).

A Forcefield Enterprise edition server (and backup server, if applicable) uses a rack-mount computer.

The Forcefield system must be licensed in order for it to run, so the installer needs to have a Forcefield License CD or USB device in their possession in order to install, run, and to begin programming the Forcefield system. A Forcefield License can only be used on the specific server and the client site for which is it ordered.

The Forcefield License is created by the distributor after the Forcefield server's serial number and the client site details are known. The installer enters these details on the *Forcefield End User License Information Form* and sends the form to the distributor.

Depending on how quickly the installer needs the Forcefield License, they can opt to order a basic 'zero options' license containing only a single initial Forcefield client license, or they can order a fully-optioned license containing additional modules such as additional clients, multi-node capability, and so on. The fully-optioned license typically takes longer to create than the 'zero options' license.

Also, installers can opt to have the Forcefield license file emailed to them so that they can quickly create their own Forcefield License without waiting for the CD or USB device to be delivered.

Refer to Chapter 5 "Upgrading a Forcefield system" on page 41 for details about expanding the basic Forcefield system by adding nodes and a backup server.

Requirements

Installation software

To set up Forcefield you need the following:

- Forcefield Installation CD or USB device
- Forcefield Licence CD or USB device

Forcefield hardware

The hardware for the Forcefield Server is supplied by Interlogix.

Forcefield clients

The Windows computer(s) must use Windows XP Professional (SP2/SP3), Windows 7 (32 and 64-bit), Windows 8 (32 and 64-bit), or Windows 10 (32 and 64-bit).

Optional hardware

Technical Support modem—any external Hayes-compatible hardware modem.

Initial user interface options

The initial setup of the Forcefield system (including adding the first Forcefield client) is performed from the Forcefield server's user interface, which can be accessed by one of the following methods:

- Direct, by connecting a monitor, keyboard, and mouse to the Forcefield server.

  Note: The keyboard and mouse must be plugged in before powering up the Forcefield server.

- Via the *Forcefield Remote Configuration* application on a Windows computer, by connecting to the Forcefield server at the default IP address of 192.168.0.1. The Forcefield Remote Configuration application is provided on the Forcefield Installation CD or USB device and can be used on a Windows computer after you install Forcefield Client.

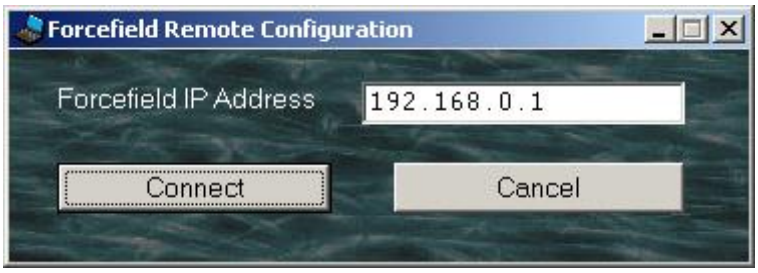
- Forcefield Enterprise VM only: Via the VMware vSphere Client on a Windows computer, by connecting to the Forcefield server at the default IP address of 192.168.0.1. The VMware vSphere Client application is provided on the VMware Installation CD or is available online from http://vsphereclient.vmware.com/vsphereclient/VMware-viclient-all-6.0.0.exe and can be used on a Windows computer after the Forcefield Client has been installed.

If using the *Forcefield Remote Configuration* application, use the following steps.

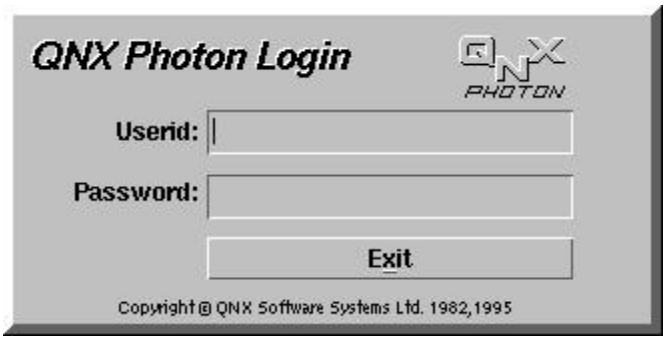
To connect with the Forcefield server and display the user interface:

1. Install Forcefield Client on the Windows computer that will run Forcefield Remote Configuration.
2. Modify the Windows computer's IP configuration settings to enable the computer to connect with the default IP address of 192.168.0.1.
3. Power-up the Forcefield server (or node, if installing a node).

4. On the Windows computer, click Start > Run, browse to FORCEFIELD REMOTECONFIG.EXE in the CD or USB device's Install folder, click Open, and then click OK to start the Forcefield Remote Configuration application.
5. The Forcefield IP Address field displays the default installation IP address of 192.168.0.1.



6. Click Connect to begin a remote session. The QNX Photon Login screen displays, and QNX prompts for a login code and password. Enter the default login code and password. The default login is "root" and the password is "4346".



Note: You should change the password for your protection. Use the Forcefield command **Admin > Change Root Password** to change the QNX root password.

If using the *VMware vSphere Client* application, use the following steps.

Install the VSphere Client and Licensing the Server

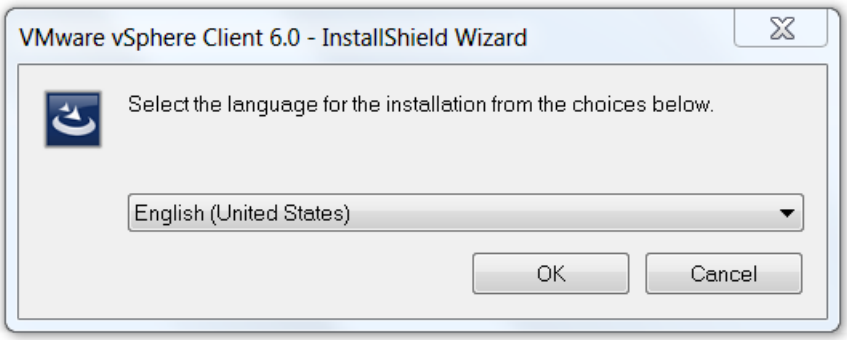
The VSphere client is required to communicate with the ESXi server so that VMs may be created or imported/exported. The client is installed on a computer that is connected to the server via an Ethernet cable (or through the network).

The Client may be downloaded from the internet by clicking in the http address on the ESXi start screen, or found in the CLIENT folder of the VMware installation CD.

Follow the process below to install the VSphere client.

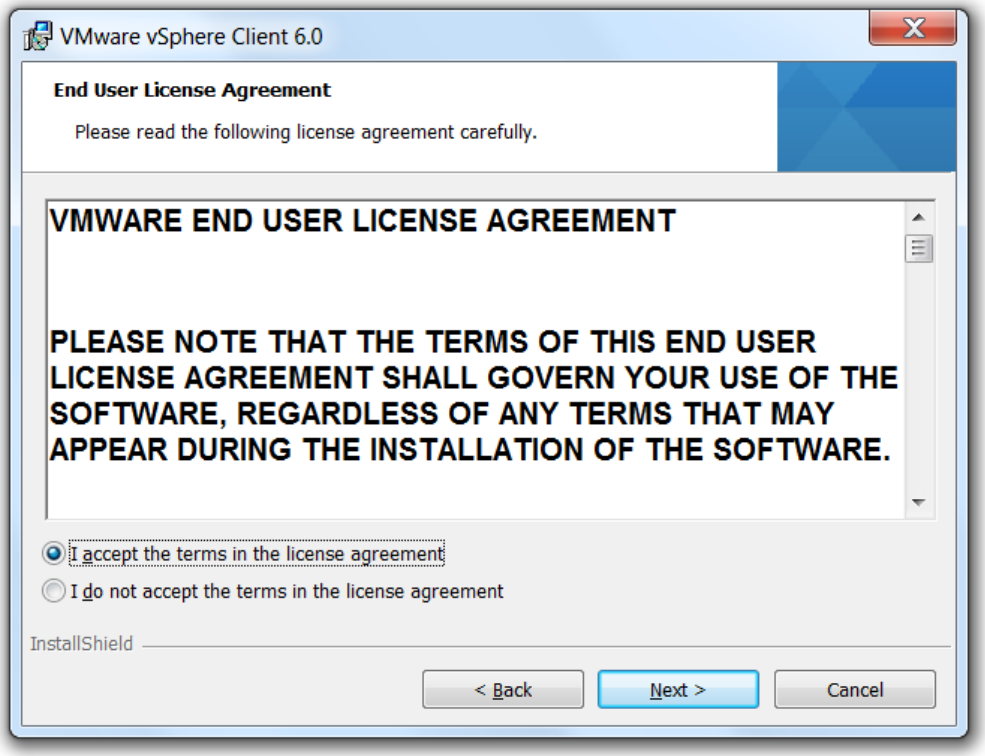
1. Double-click on the installer to start the installation process. The following window appears.

Figure 3: Start of the vSphere client install



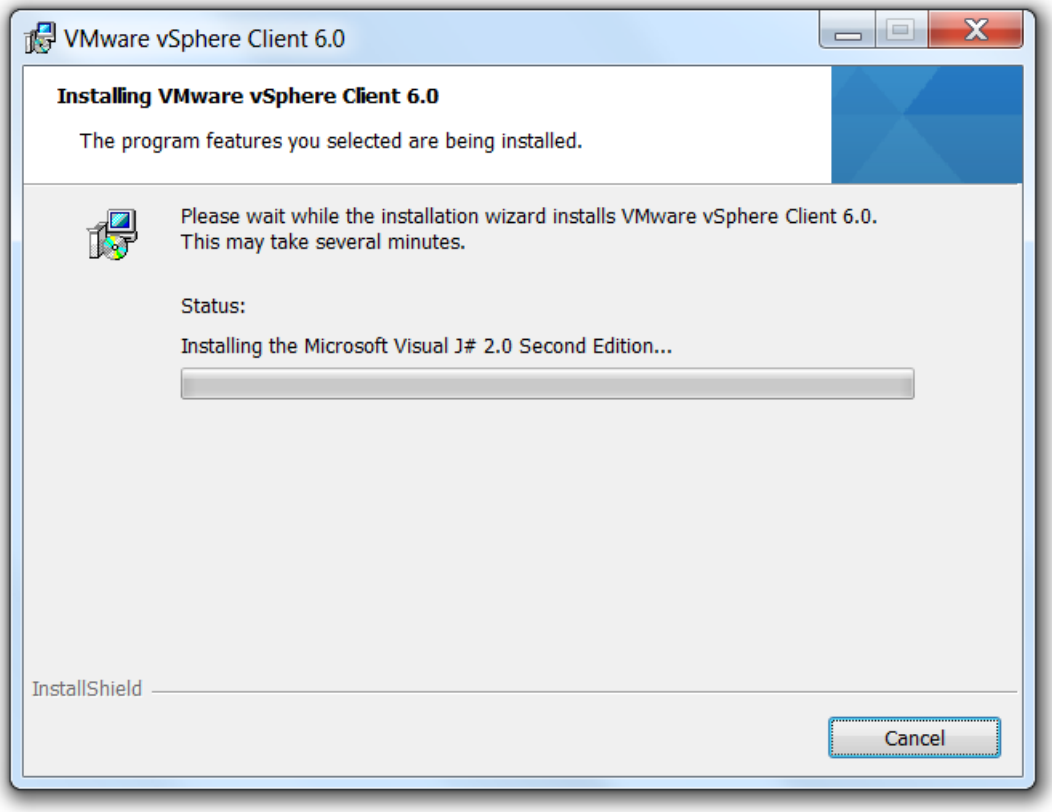
2. The Welcome Window for the vSphere installation appears. Click **Next** and the License window appears. Accept the License and click **Next**.

Figure 4: Accepting the vSphere's license agreement



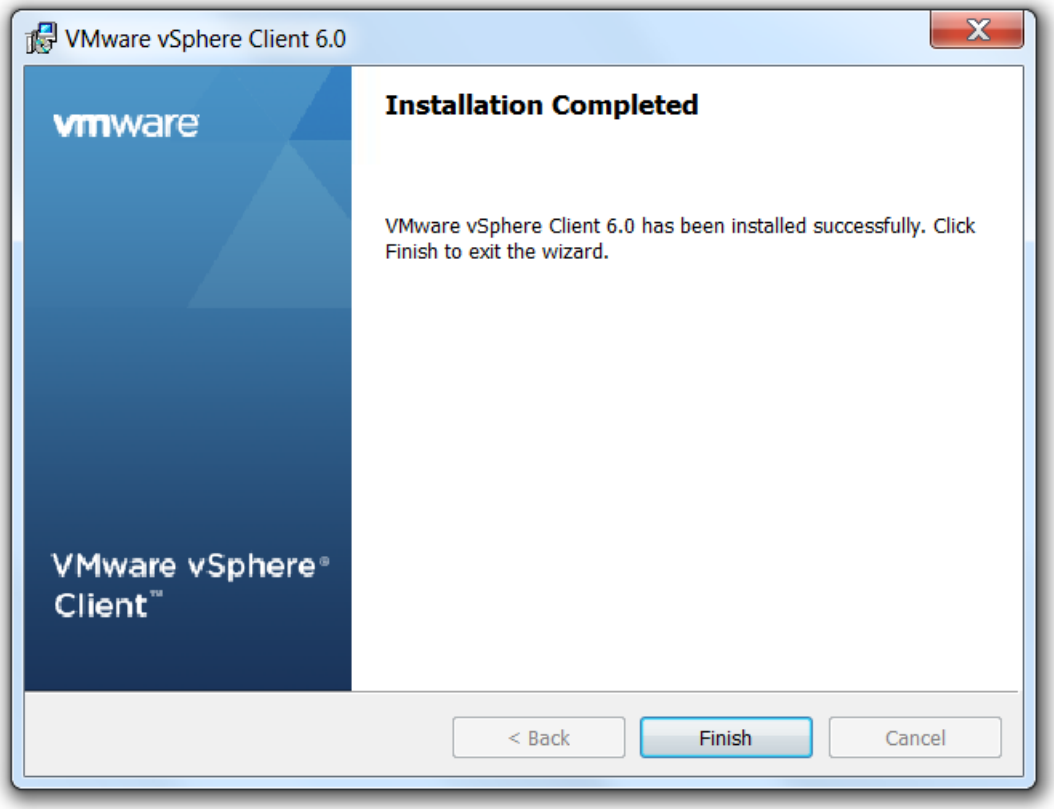
3. Click **Next**, then **Next** and the installation will start. The following progress window will appear.

Figure 5: Installation progress for vSphere client



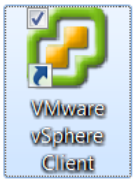
4. When the Install Completed window appears, click **Finish**.

Figure 6: vSphere client install is complete



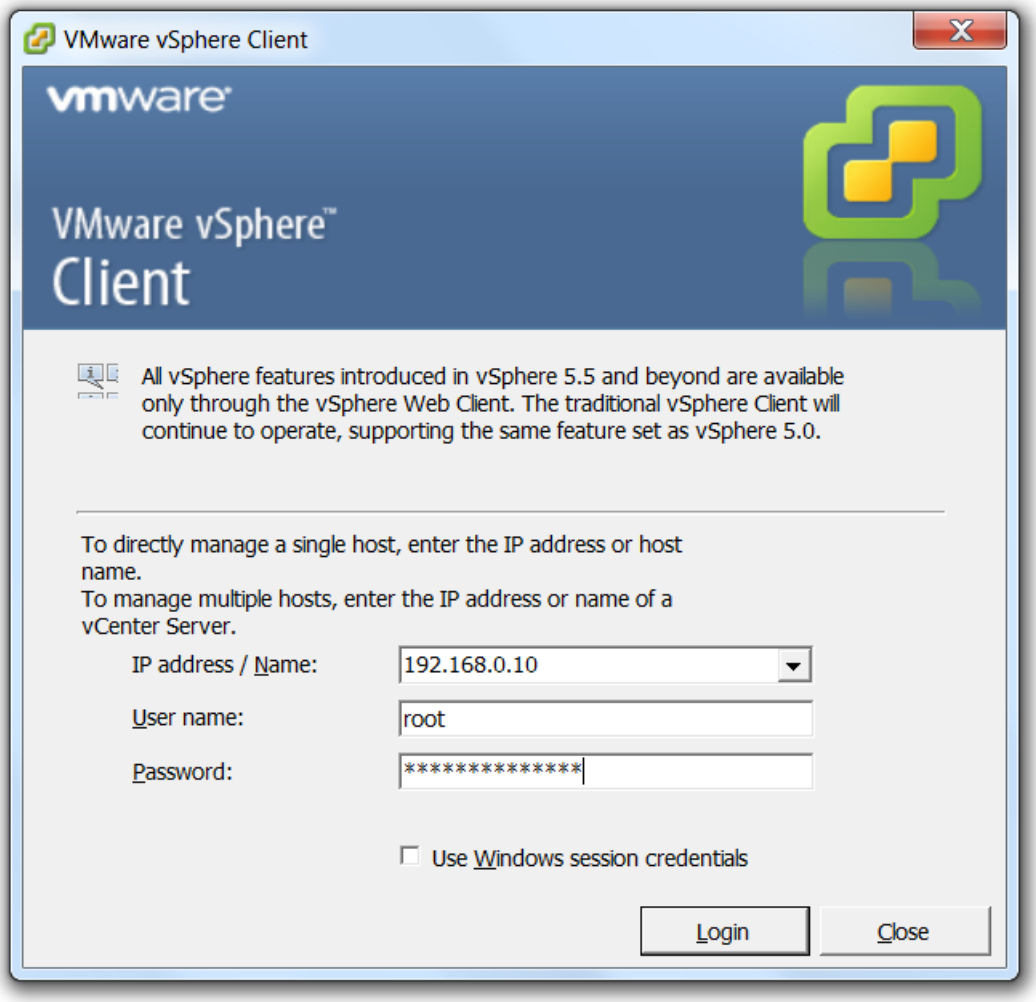
5. Start vSphere by double-clicking on the desktop icon.

Figure 7: Double click this icon on the desktop to start vSphere client



6. Connect vSphere to the server as shown.

Figure 8: Connecting to the server using the vSphere client



IP Address : **192.168.0.10** (as an example)

User Name : **root**

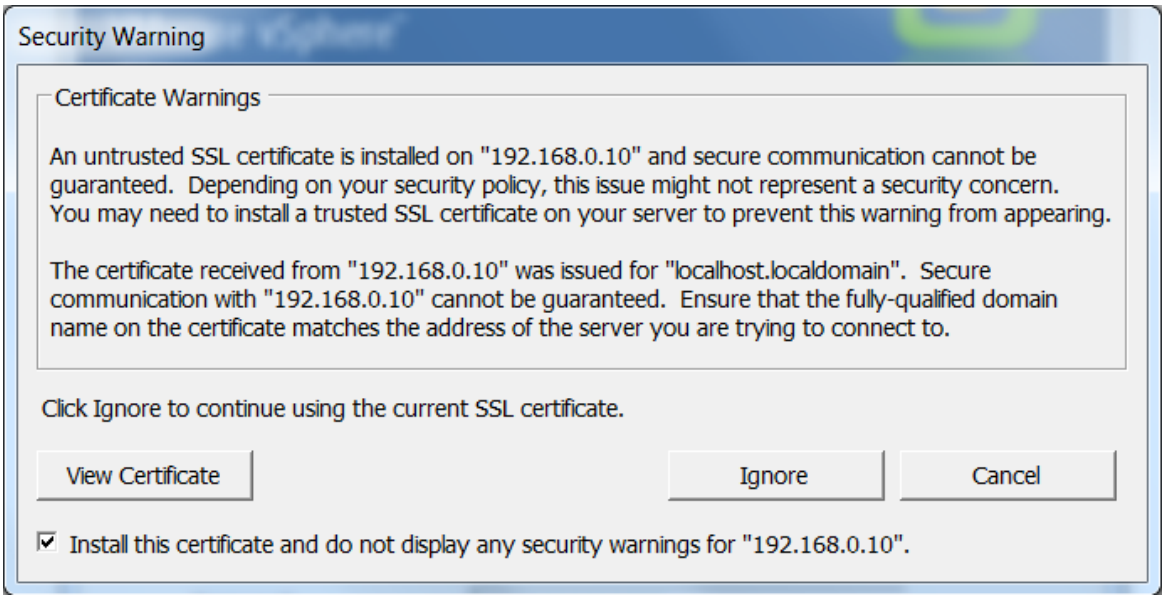
Password : **forcefield4346**

Click the **Login** button.

7. A security certificate warning will pop up as shown below.

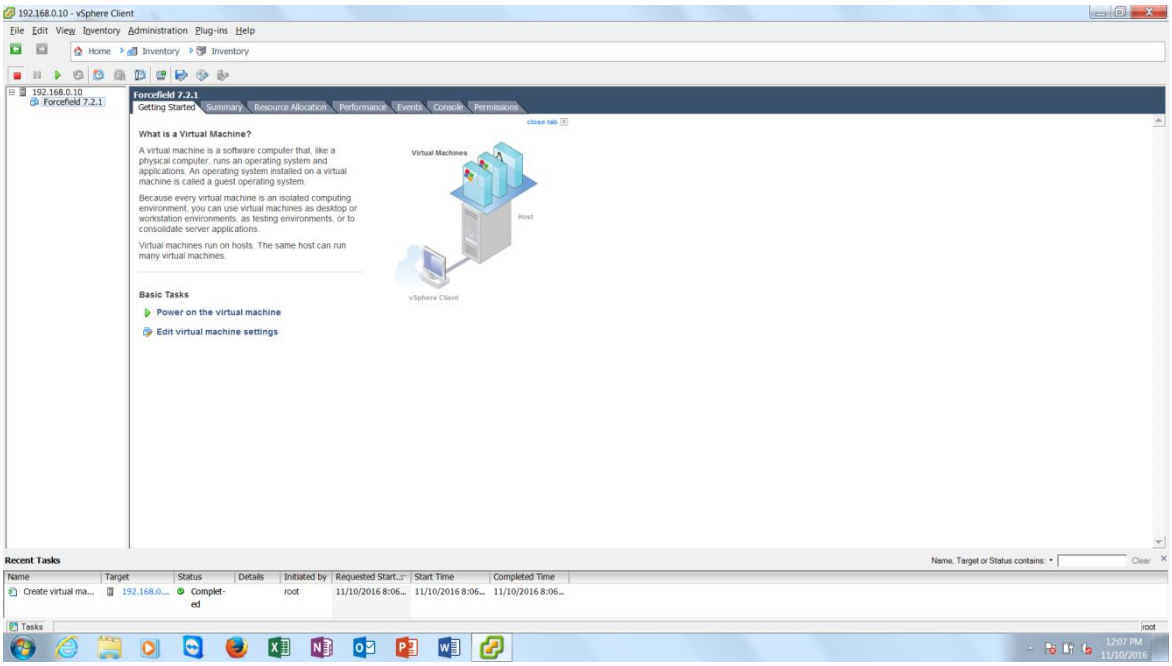
Click on the check box to **Install this certificate…** and click on the **Ignore** button.

Figure 9: Login Security Warning



8. Click on the VM named **Forcefield 7.2.1** in the left hand pane, and then click on **Power on the virtual machine** under the **Getting Started** tab. If you do not see an option to Power On the virtual machine, and instead see options to Power Off and Suspend, then Forcefield is already running.

Figure 10: VM is ready to be started



Clicking on the Console tab displays the Virtual Machine's console.

To interact with the virtual machine, click within the window of the console tab. This makes the keyboard and mouse visible to the Virtual Machine.

To stop interacting, press the CTRL and ALT keys on the left-hand side of the keyboard at the same time. This detaches the keyboard and mouse from the Virtual Machine.

Set-up procedure

Forcefield and Forcefield Enterprise:

The Forcefield server has the following ports at the back:

- 4 x USB (one for keyboard, one for mouse, and two for storage devices)
- LAN 1 connection
- LAN 2 connection (for future use)
- 4 DB9 serial ports (COM1, COM2, COM3 and COM4)
- VGA video port

Forcefield Enterprise VM:

The Forcefield Enterprise VM server has the following ports at the back:

- 2 x USB (mouse and keyboard only)
- Ethernet – General connection
- Ethernet – iDRAC connection
- Ethernet – Unused connections (for future use)
- 1 DB9 serial port (COM1)
- VGA video port

To set up a Forcefield server computer:

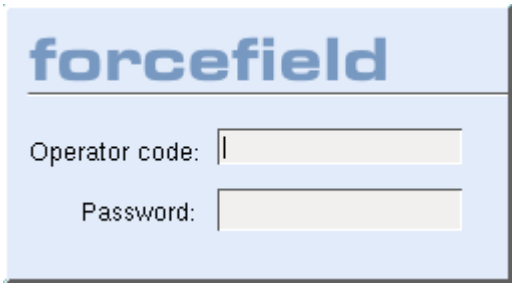
1. Unpack the Forcefield server and place it on a level surface near the required location.

   The Forcefield server is designed for flexibility in mounting arrangements. However, during the setup process you will need to be able to access and use the CD or USB drive.

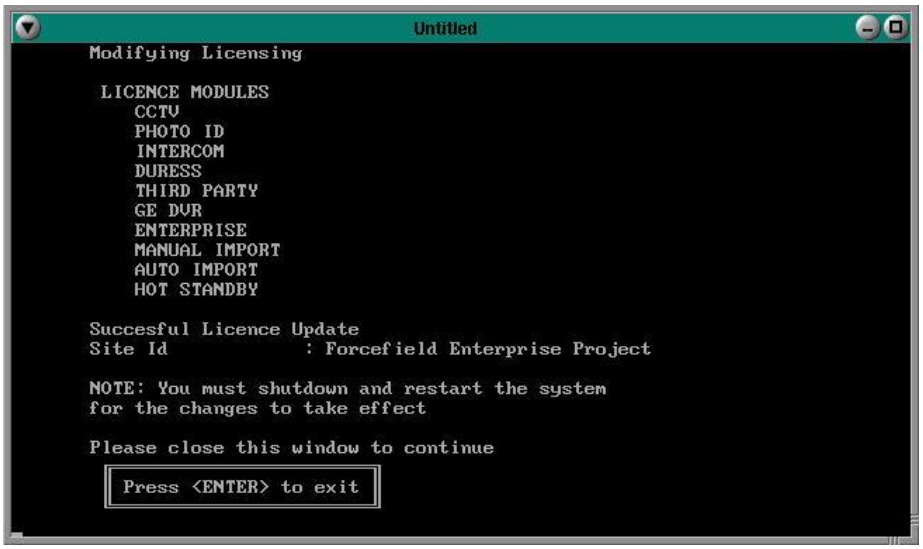
2. Connect, at a minimum, the LAN cable and power supplies.
3. Power-up the Forcefield server (this will take a few minutes).

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

4. Display the Forcefield server's user interface using one of the methods described in "Initial user interface options" on page 11.
5. Forcefield prompts for a login code and password. Enter the default login code and password. The default login is **master** and the password is **4346**. You should change the password for your protection as the default login gives unlimited access to all Forcefield features.



6. Forcefield prompts for the Forcefield License. Insert the Forcefield License into the CD or USB drive of the Forcefield server, and then click Continue. Forcefield displays the details of the licenses to be installed or modified.



7. Close the window to continue.
8. When the CD or USB drive light is out, remove the Forcefield License from the CD or USB drive of the Forcefield server, and store it in a safe location.

What happens next?

After setting up and licensing Forcefield you need to do the following:

- Change the default TCP/IP address to the TCP/IP address that was assigned by the system administrator. See "Configuring TCP/IP addresses" on page 20.
- Create the first Forcefield Workstation record (including a station key). See "Programming a workstation record" on page 33.

- Install the Forcefield Client software on a Windows computer. This process is described in “Installing Forcefield Client” on page 34.
- Use the Preferences window from Start > All Programs > Tecom > Forcefield > Preferences to apply the new station key to the Forcefield client.
- Run Forcefield Client to perform all further operations (including adding more clients).
- If this is a multi-node system, refer to “Adding a node” on page 42.

Configuring TCP/IP addresses

Each node in a Forcefield system is assigned a default IP address, depending on its node number (see “System-wide information record” on page 85).

The process of changing a node’s IP address depends on whether the node is a controlling node (server) or a non-controlling node. This section describes the process of changing a node’s IP address for all roles.

Changing the primary server’s IP address

Use the Forcefield command Admin > Configuration > Network Configuration to change the Forcefield server’s TCP/IP address. Refer to the *Forcefield Operators Manual* for details of using this command.

Changing a non-controlling node’s IP address

During the installation process

The network configuration utility (nwcfg5) runs automatically when a new node is added to a Forcefield system and enables you to assign each node’s IP address. Refer to “Stage 2—Installing the new node” on page 44.

Afterwards at any time

A node’s IP address may be changed via the Admin > Configuration > Network Configuration command. In order to apply this command to the node, use a client connected to the node. Alternatively, if the node doesn’t have a client attached use the *Forcefield Remote Configuration* application on a Windows computer.

Configuring Notification Settings (Forcefield Enterprise VM only)

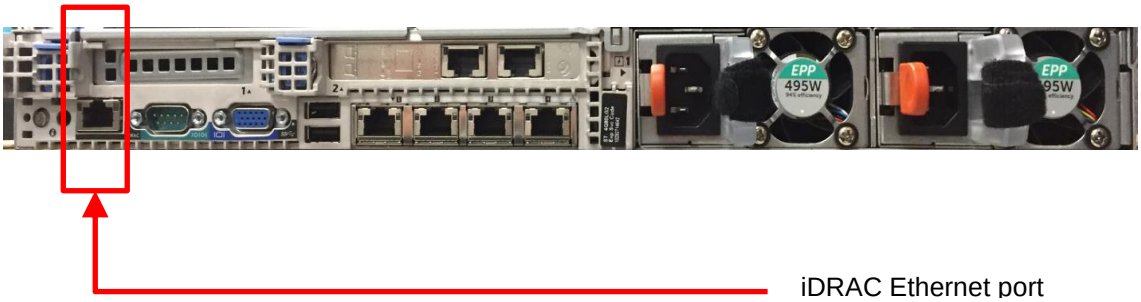
iDRAC Configuration

iDRAC (integrated Dell Remote Access Controller) is a process running under Firmware Control within the server monitor the health of the server hardware. To

monitor the server correctly iDRAC must be configured correctly. Below is a series of steps to configure iDRAC.

Note: iDRAC configuration is done through a computer connected to the iDRAC Ethernet port. The iDRAC Ethernet port is shown in Figure 11below.

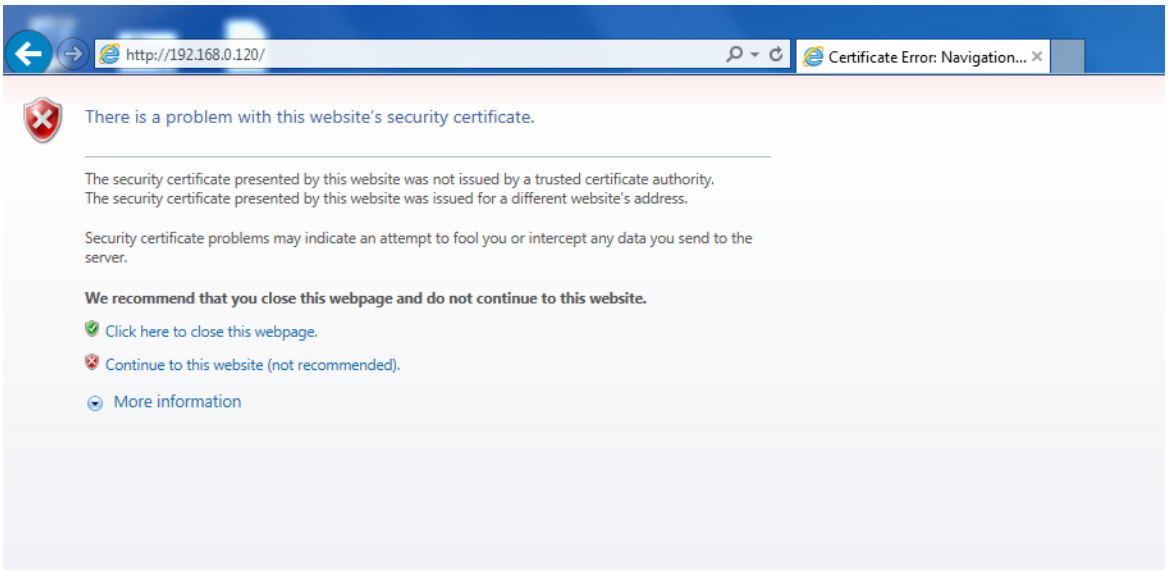
Figure 11: iDRAC Ethernet port



1. Using a web client, such as Internet Explorer, connect to the iDRAC system. Use the IP address as provided by the IT department. For this manual, the following address is used as an example only: 192.168.0.120

   When the security certificate problem page is displayed, click the **Continue to this website (not recommended)** option.

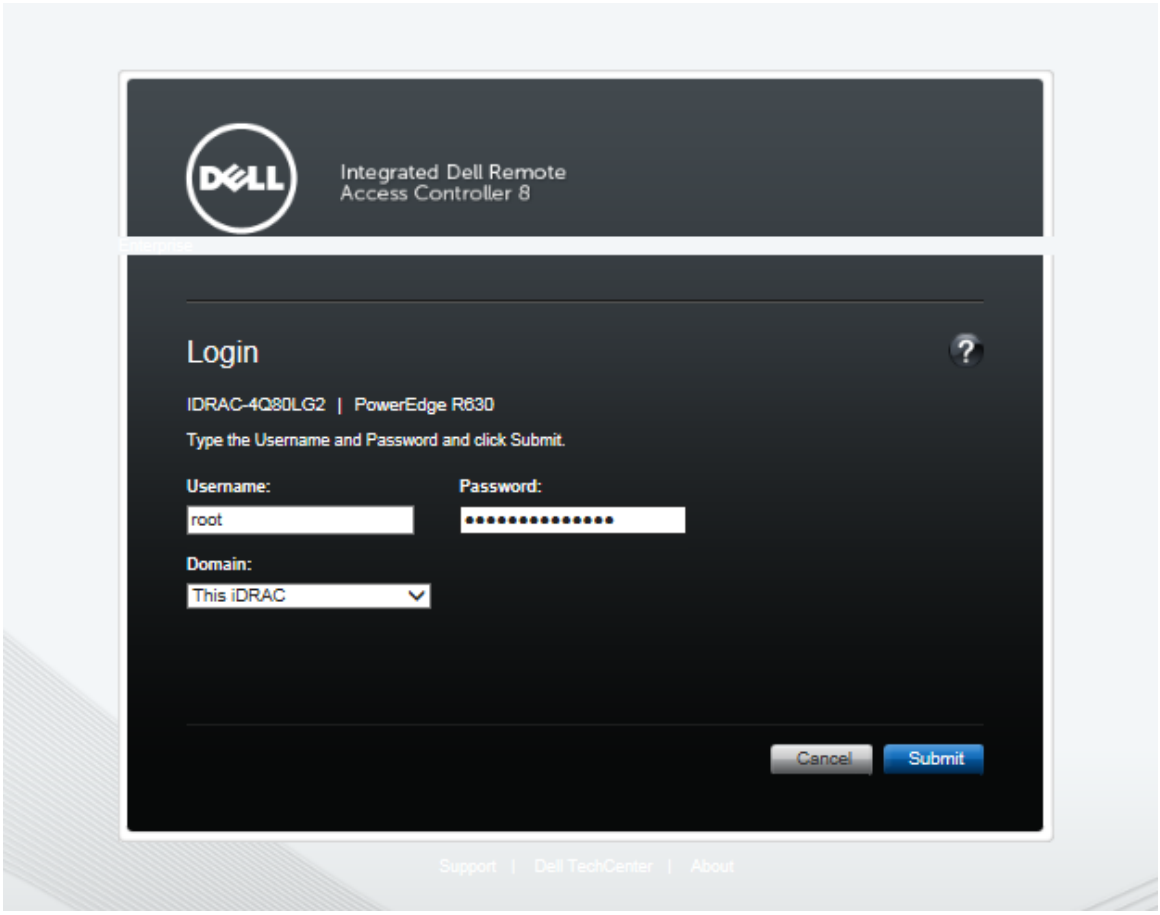
Figure 12: iDRAC website Certificate Problem



2. Log in to the iDRAC system as shown below. Click **Submit**.
   The default username and password information are preset in the iDRAC system:

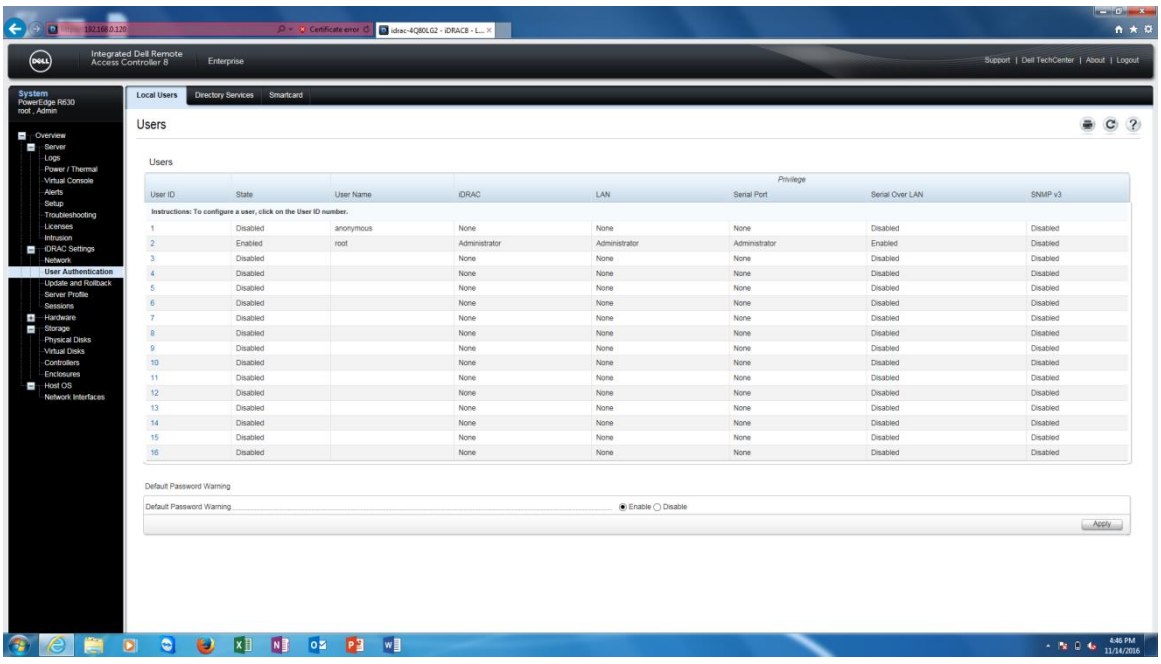
   Username : **root**
   Password : **calvin**

Figure 13: Logging on to iDRAC



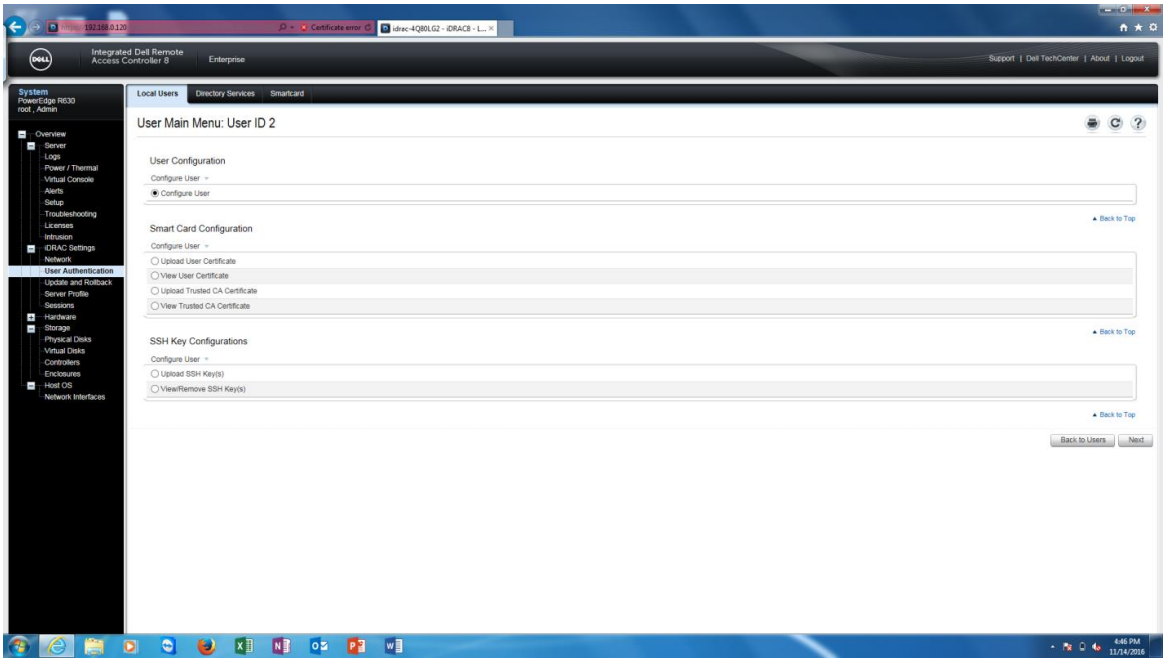
3. Set up the permissions of the user accounts that may log into the iDRAC system. To change the password of the default root user, click on the **User ID** number 2 link.When finished, click **Apply**.

Figure 14: iDRAC user setup



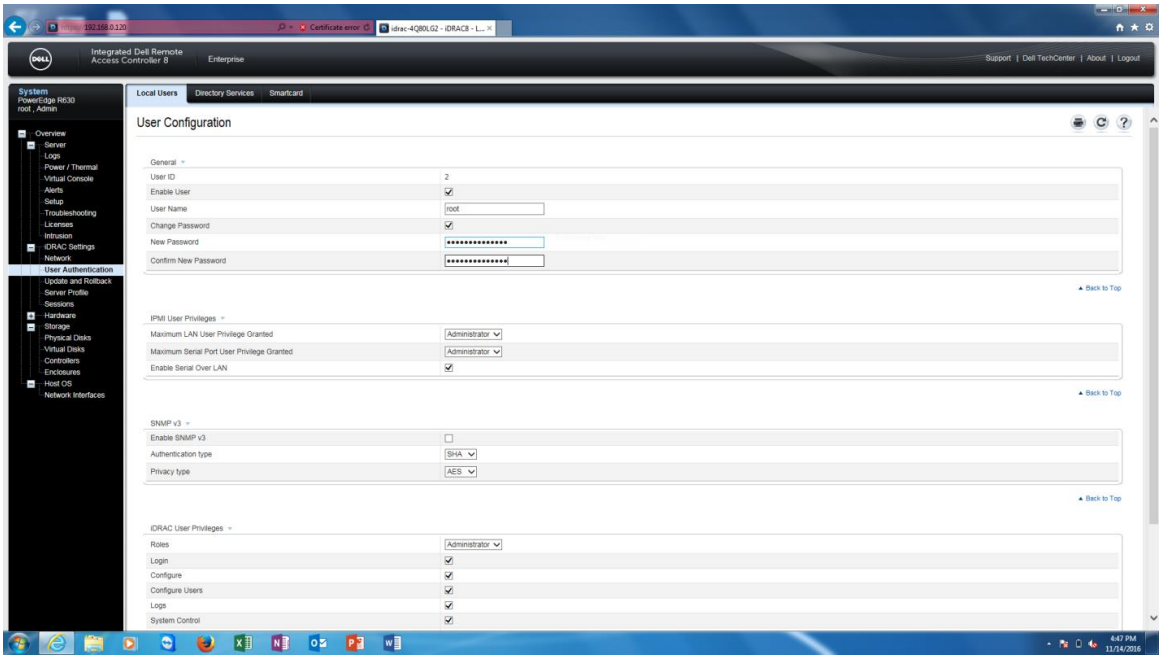
4. To configure the iDRAC user ensure that the Configure user radio button is selected. Click **Next** to countinue.

Figure 15: Getting ready to configure the iDRAC user



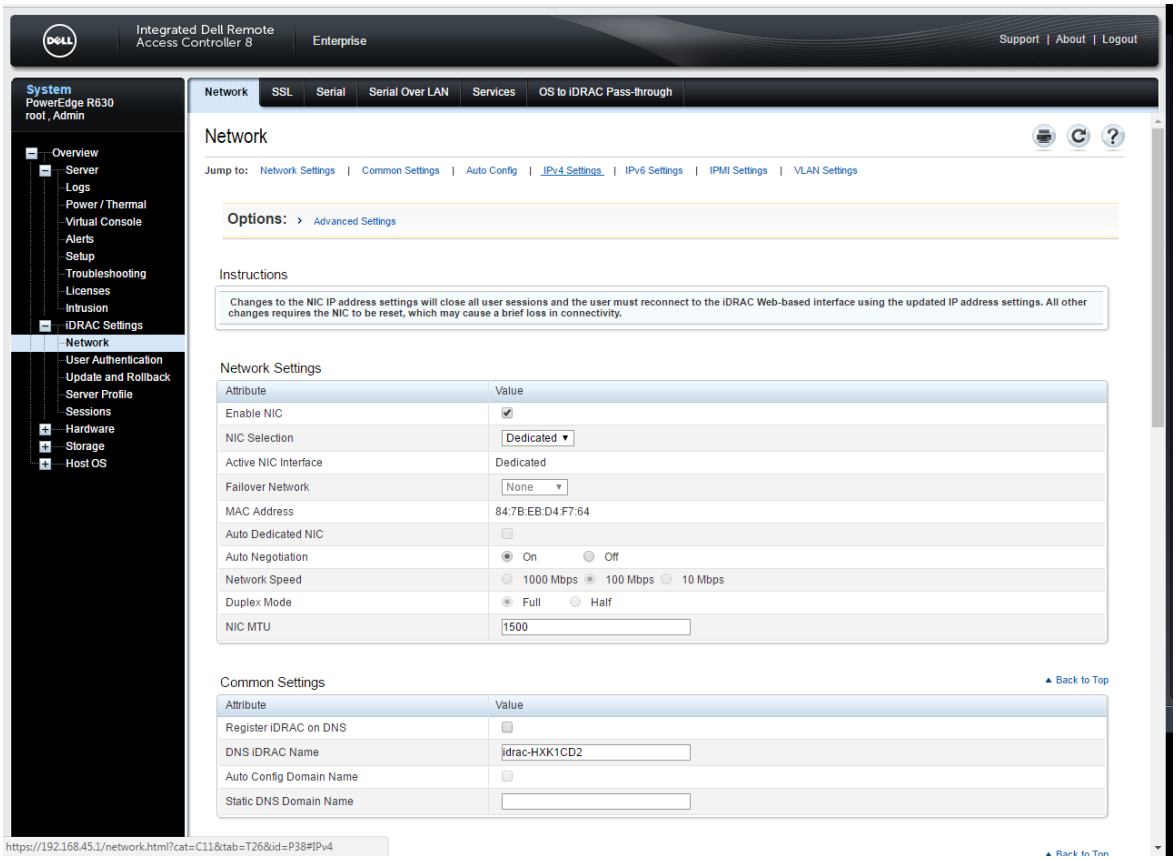
5. The figure below depicts the root user's setting. Note that the Change Password checkbox has been clicked and the new password has been typed in. This is recommended as it ensures that security is maintained , by selecting a password different to the default setting.

Figure 16: root user settings updated



6. Click on the Network link to enable setting up the iDRAC network parameters. This page below shows the Network Settings and Common Settings.

Figure 17: Network and Comment Settings



Network Settings

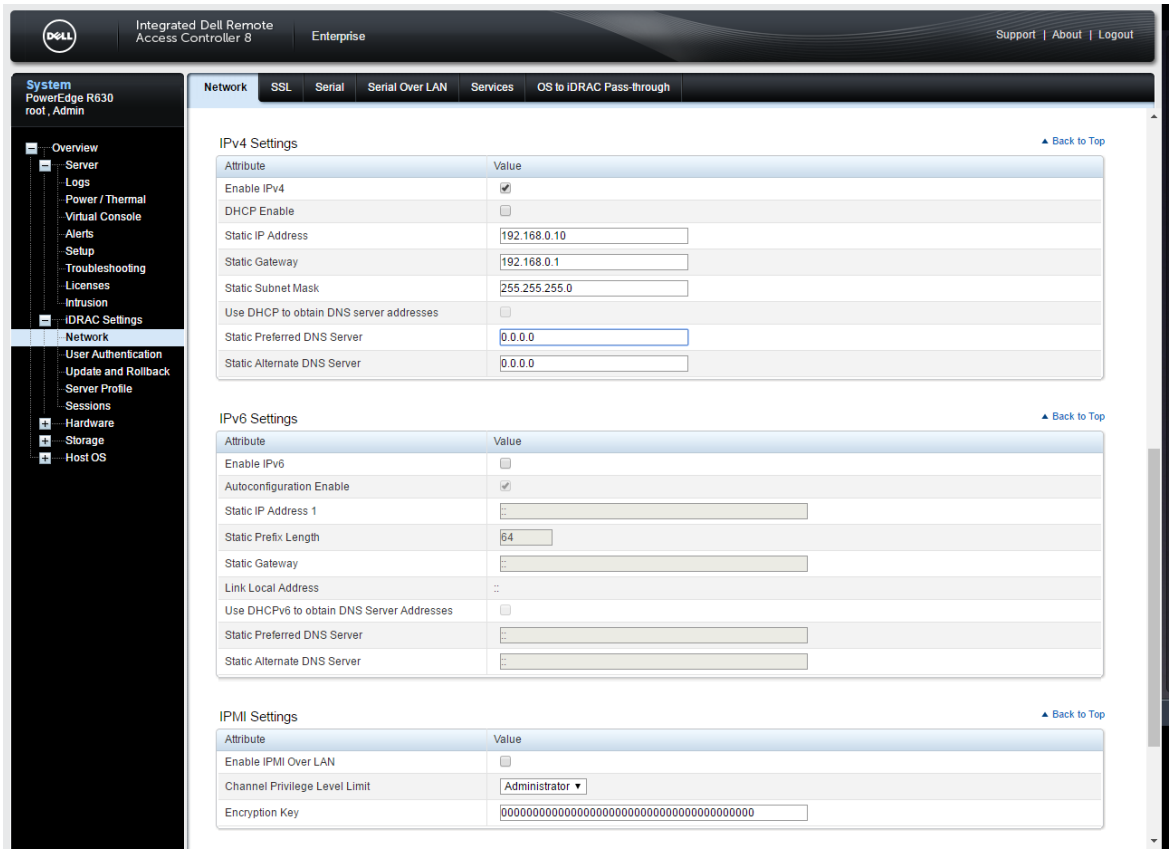
Attribute	Value
Enable NIC	Yes (Check box is selected)
NIC Selection	Dedicated
Active NIC interface	Dedicated
Failover Network	None
MAC Address	(Pre-filled, leave as it is)
Auto Dedicated NIC	No (Check box is NOT selected)
Auto Negotiation	On
Network Speed	100 Mbps
Duplex Mode	Full
NIC MTU	1500

Common Settings

Attribute	Value
Regular iDRAC on DNS	No (Check box is NOT selected)
DNS iDRAC Name	(Pre-filled, leave as it is)
Auto Config Domain Name	No (Check box is NOT selected)
Static DNS Domain Name	(Blank)

7. Scroll down the page to show the IPV4, IPV6, and IPMI Settings.

Figure 18: IPV4, IPV6 and IPMI Settings



IPV4 Settings

Attribute	Value
Enable IPv4	Yes (Check box is selected)
DHCP Enable	No (Check box is NOT selected)
Static IP Address	192.168.0.120
Static Gateway	192.168.0.1
Static Subnet Mask	255.255.255.0
Use DHCP to obtain DNS Server Address	No (Check box is NOT selected)
Static Preferred DNS Server	0.0.0.0
Static Alternate DNS Server	0.0.0.0

IPV6 Settings.

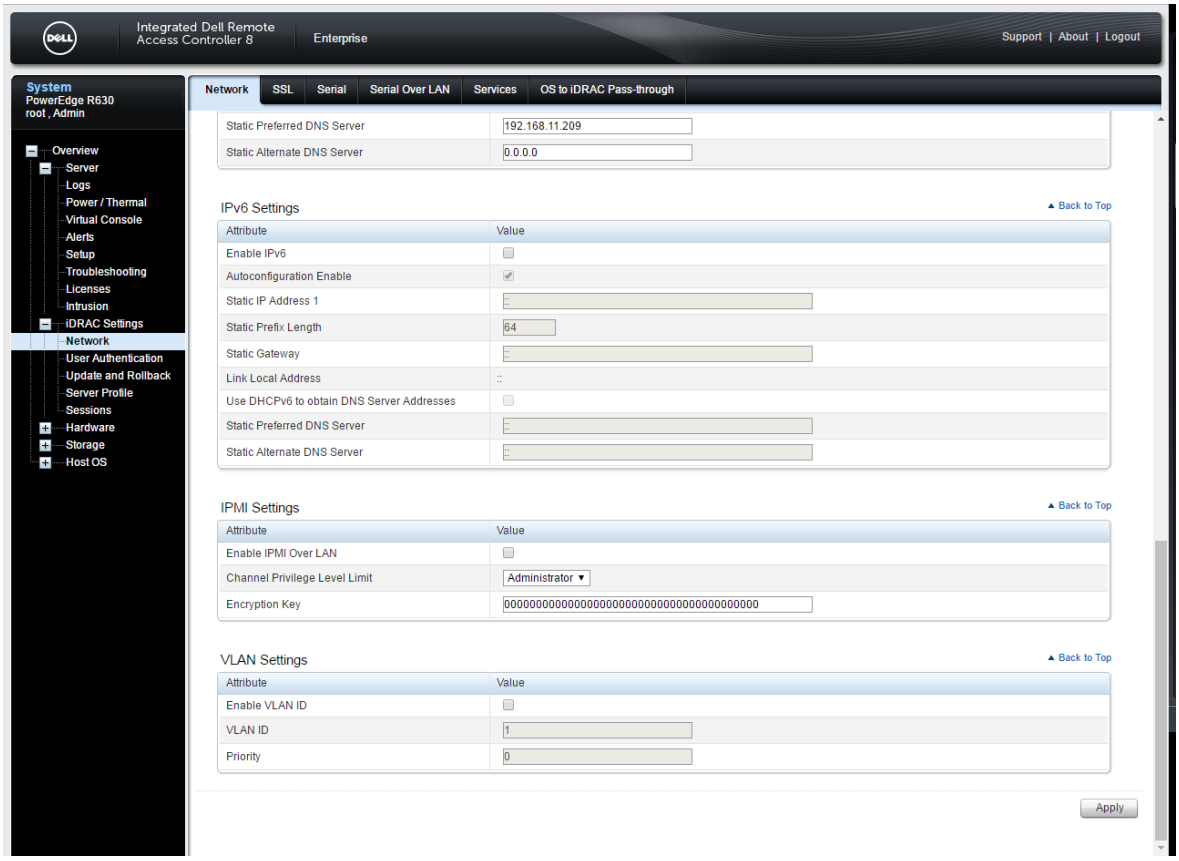
Ensure that the **Enable IPV6** is NOT checked (the check box is not ticked).

IPMI Settings.

Do not modify any IPMI Settings.

8. Scroll down the page to show the VLAN Settings.

Figure 19: VLAN Settings



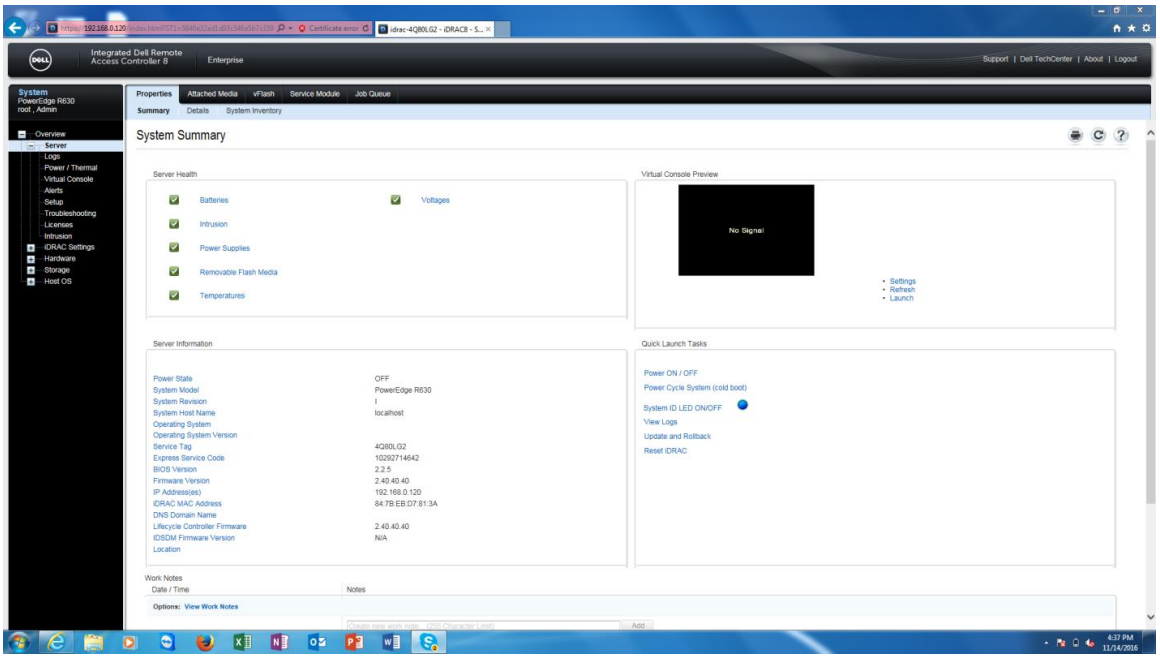
VLAN Settings

Attribute	Value
Enable VLAN ID	No (Check box is NOT selected)
VLAN ID	1
Priority	0

The VLAN settings shown in the table are all default settings.

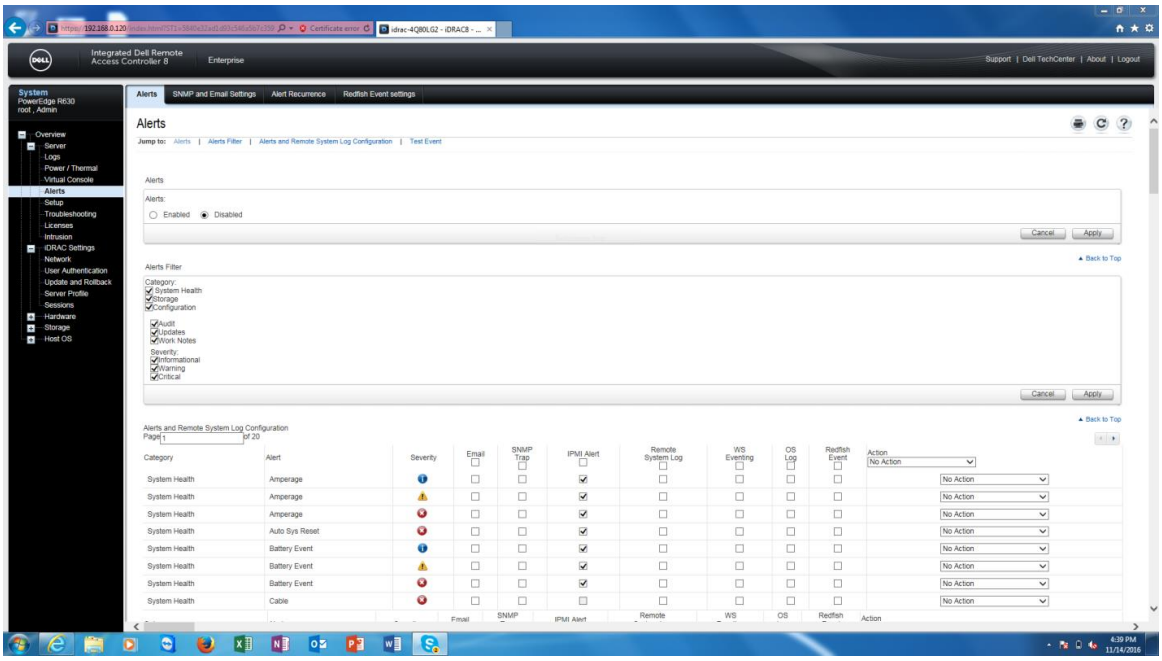
9. At the Server > Properties Summary, ensure the items to be monitored in the Server Health panel are set as shown.

Figure 20: iDRAC System Summary



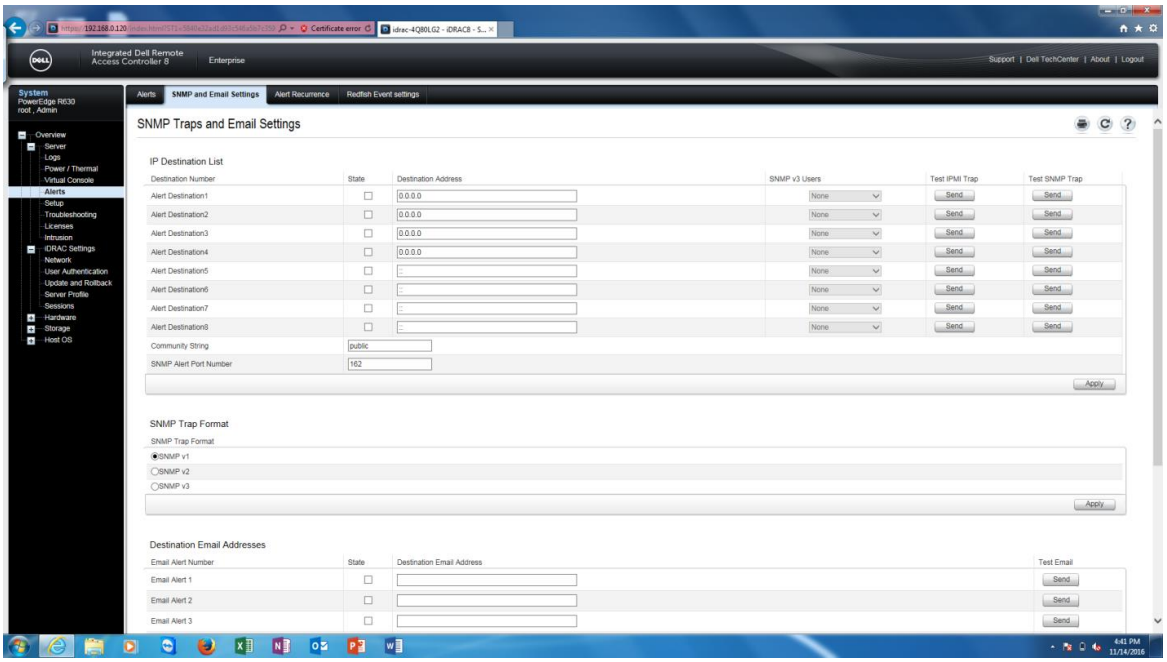
10. Use the Alerts panel to configure alert options. Events can be filtered by type, and description for sending (e.g. PSU failure, RAID events etc), and the method of sending (e.g. SNMP, Email).

Figure 21: iDRAC Alerts setup view



11. In the Alerts > SNMP and Email Settings tab, check that everything is set correctly. The setup may need to be discussed with the IT separtment.

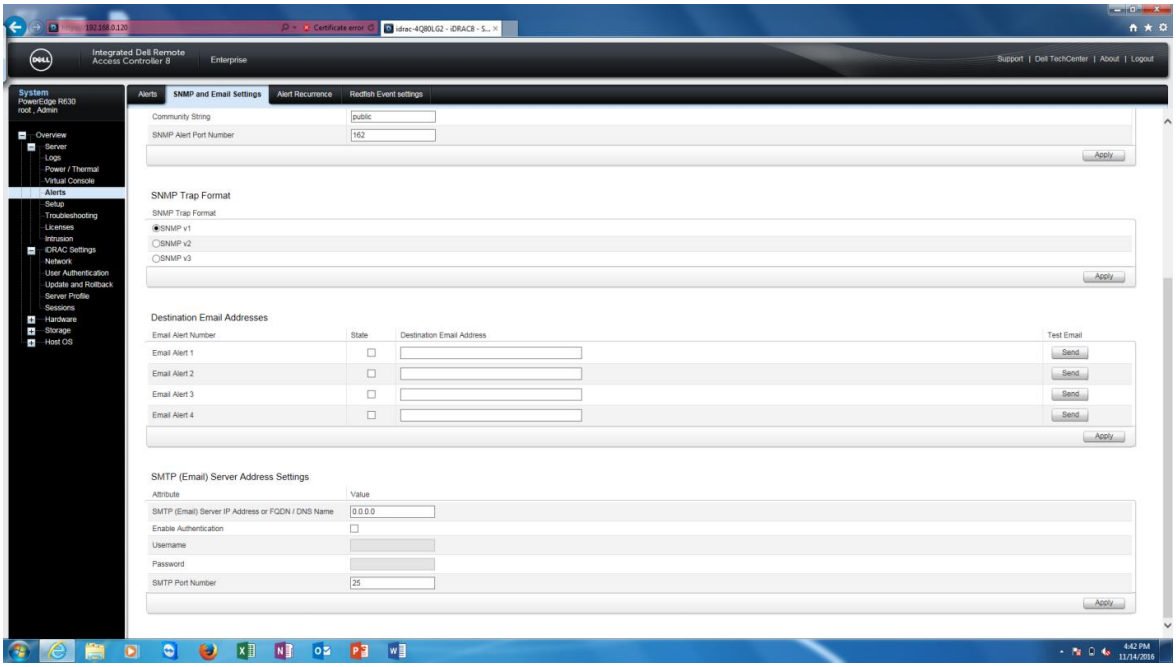
Figure 22: iDRAC Email setting



The correct email settings will be different for each installation site. Please refer to the IT group for the correct email server settings. Note: Ensure email has State checkbox selected.

12. SNMP and Email settings continued. The figure below show the remainder of the email settings page.

Figure 23: Bottom half of email setting view



Note: Please ensure that there is a name in the Static DNS Domain Name in the iDRAC Settings > Network > Common settings. Without this it will not ssend emails.

Chapter 4
Installing Forcefield Client

Summary

This chapter describes how to install Forcefield Client on a Windows computer and communicate with a Forcefield node.

Content

Prerequisites

Installation of Forcefield Client should be done only by trained Forcefield installation technicians, or senior Forcefield operators who have:

- Permissions to create workstations in Forcefield.
- Administrator privileges in Windows.

A Forcefield server must be installed and a Forcefield Workstation record must be created.

Note: 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.

Forcefield Client system requirements

The Windows computer(s) must use Windows XP Professional (SP2/SP3), Windows 7 (32 and 64-bit), Windows 8 (32 and 64-bit), or Windows 10 (32 and 64-bit).

Note: The following IP ports must not be blocked by a firewall or other means:

- TCP port 4868 (Forcefield Client).
- UDP port 5081 (Control Port), or other number assigned for this purpose by the system administrator.
- TCP port 5082 (Transfer Port), or other number assigned for this purpose by the system administrator.
- TCP port 3001 (for Smart Card Programmer, if used), or other number assigned for this purpose by the system administrator. This port number is workstation-specific; the previously-listed port numbers are system-wide.

Refer to “Node-specific information record” on page 86 for the port numbers assigned to the control port and transfer port.

Installation overview

The process of installing a Forcefield Client consists of the following procedures:

- First, install Forcefield Client on a Windows computer. This is required before you can use the *Forcefield Remote Configuration* application. See “Initial installation” on page 35.
- Second, create a Forcefield Workstation record from a Windows computer running the *Forcefield Remote Configuration* application. During this procedure you will need to record certain details that are required later. Use the “Node-specific information record” on page 86 to record the details for each Forcefield Client.

- Third, use the information that you recorded on the worksheet to enable communications with the Forcefield node (the server in this case). See “Connecting the client to the server” on page 39.

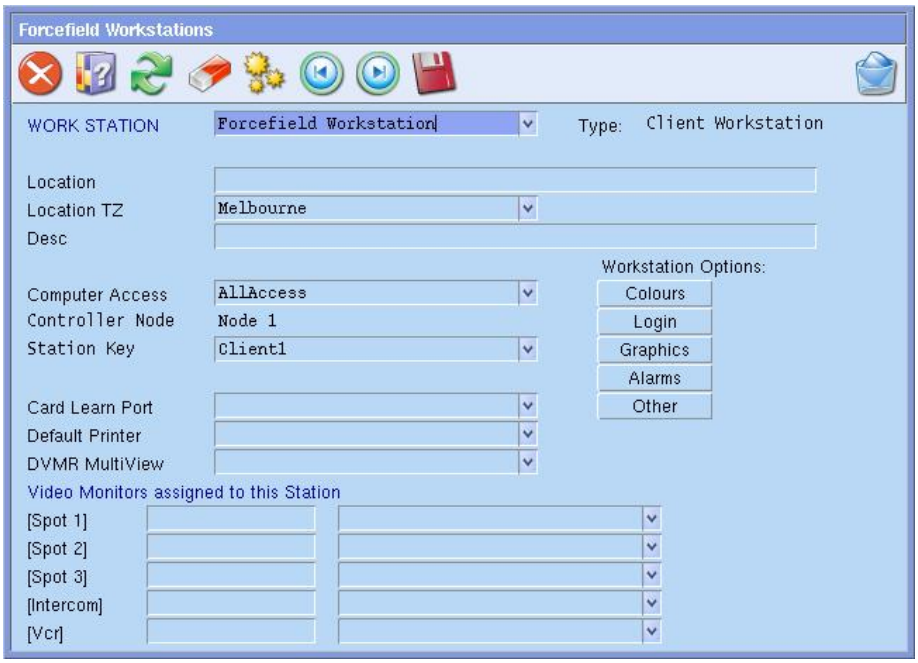
After a first Forcefield client has been installed on a Windows computer and successfully connects to the Forcefield server, you can use the Forcefield client to set up all subsequent Forcefield clients. The *Forcefield Remote Configuration* application is no longer needed.

Programming a workstation record

This procedure describes only the *minimum* details required to create a Forcefield Workstation record. Refer to the *Forcefield Operators Manual* for a detailed description.

To create a Forcefield workstation:

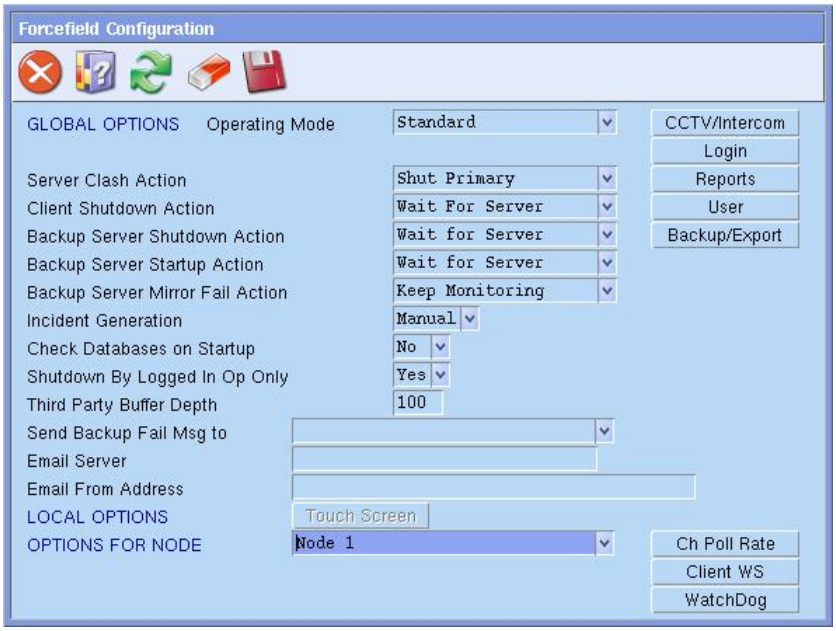
1. In Forcefield, open Databases > Computer Equipment > Workstations to open the Forcefield Workstations window.



2. In the Work Station field, enter a unique name to identify the Forcefield Client to be set up.
3. In the Computer Access field, select a Forcefield Access record to determine what functions will be available.
4. In the Station Key field, type a unique string to identify the workstation.

   Record this detail on the “Node-specific information record” on page 86 to use when installing the Forcefield client. The station key is case-sensitive. It must be used when installing the Forcefield client exactly as it was defined here. It is not possible to search for station keys.

5. Save the workstation record and close the Forcefield Workstations window.
6. Open Admin > Configuration > Configuration to open the Forcefield Configuration window.



7. Click Client WS to open the Client Workstation Config window. The port numbers are displayed automatically. Check with the system administrator that the port numbers are suitable for use. Port 4868 is also required, but is not configurable. Record the port numbers on the “Node-specific information record” on page 86 to use when installing Forcefield Client.
8. Close the Client Workstation Config window and the Forcefield Configuration window.
9. Open Admin > Configuration > Network Configuration and then click Interface Details. The default installation IP address of 192.168.0.1 is for initial set up only.
10. Type the TCP/IP address that was assigned by the system administrator. If required, type the gateway address and netmask that were assigned by the system administrator. Record these details on the “System-wide information record” on page 85 to use when installing Forcefield clients. The IP address must be used by each Forcefield client in order to connect with the Forcefield server (or node, as applicable).

Installing Forcefield Client

Forcefield Client software may be installed via the following options:

- Insert the Forcefield Installation CD (or USB device) in the client computer’s appropriate drive. Install Forcefield from the “Welcome to Forcefield” page. Alternatively, open the Default.htm file on the Installation CD.

- Use the client computer's web browser to open the Forcefield Web Toolbox files over an IP connection to the server when the Web server is enabled (it is disabled by default each time the Forcefield server is started). Copy the FFCinstall.exe file from the Download page. Run the FFCinstall.exe file to install Forcefield.

To install Forcefield from the Web Toolbox:

1. On the Forcefield server, click the Start/Stop Web Server button on the Network Configuration option to start (enable) the Web server.
2. In the client computer's web browser, type nnn.nnn.nnn.nnn in the address bar, and then press Enter (where nnn.nnn.nnn.nnn is the Forcefield server's IP address that was assigned by the system administrator).
3. In the Forcefield Web Toolbox click the Download button to view the Download page.
4. Click Download Forcefield Client, and then click Run.

Refer to “Initial installation” below for the next steps.

Initial installation

In this procedure you will need:

- Forcefield Installation CD or USB device (or IP connection to the Forcefield Web Toolbox on the Forcefield server).
- CD or USB drive in the Windows computer (if needed).
- The Windows computer must have network access to the Forcefield server.

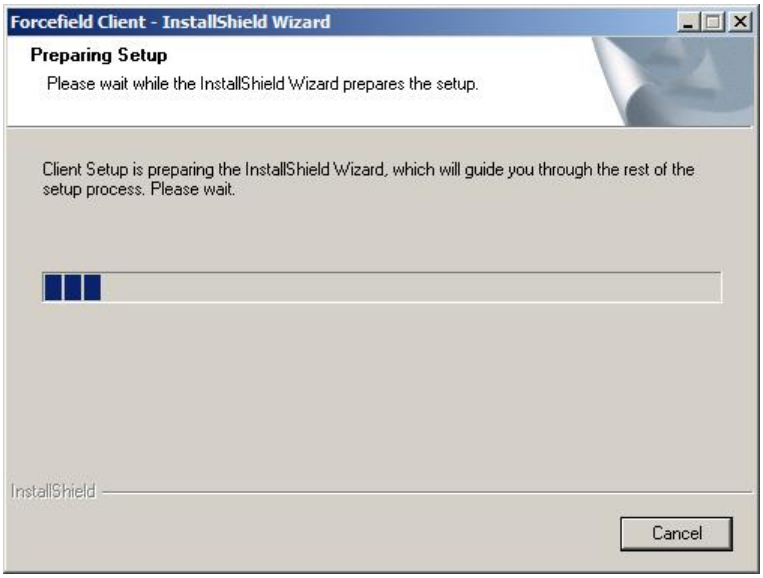
Note: Before you install Forcefield Client on a Windows computer you must first remove any earlier versions, if present. Go to Start > Control Panel > Add or Remove Programs and remove any instances of Forcefield Client.

Use the following steps to install Forcefield Client on a Windows computer from the Forcefield Installation CD or USB device (if using the Forcefield Web Toolbox, refer to instructions on the Download page).

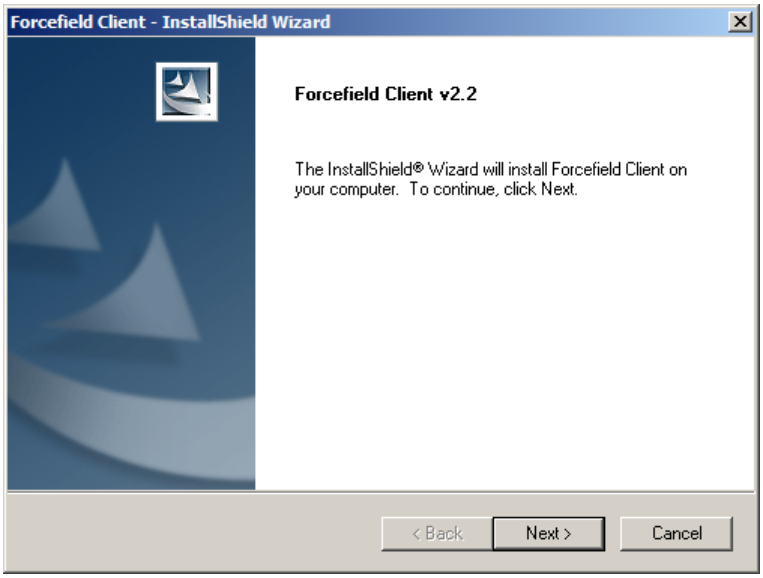
To install Forcefield Client on a Windows computer:

1. Insert the Forcefield Installation CD or USB device into the appropriate drive.
2. The “Welcome to Forcefield” page should automatically open in a browser window. Alternatively, click Start > Run and browse to FFCINSTALL.EXE in the CD or USB device’s Install folder, click Open, and then click OK.

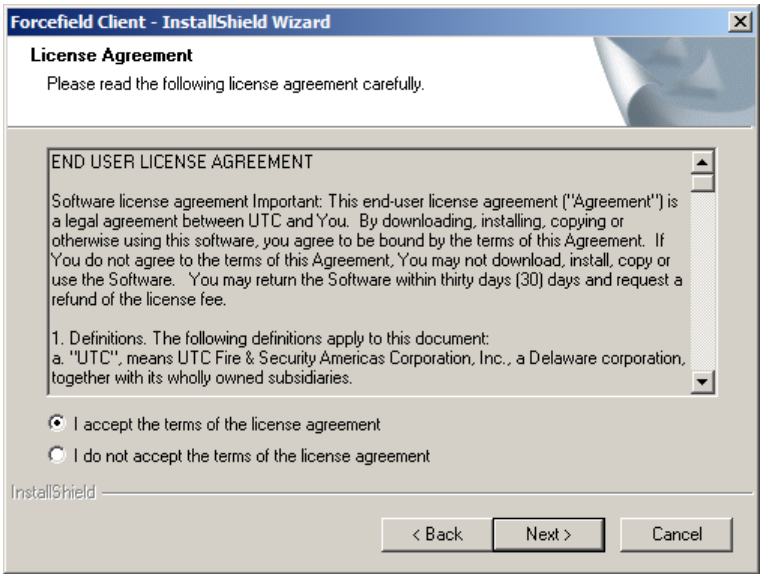
3. InstallShield prepares to install Forcefield Client.



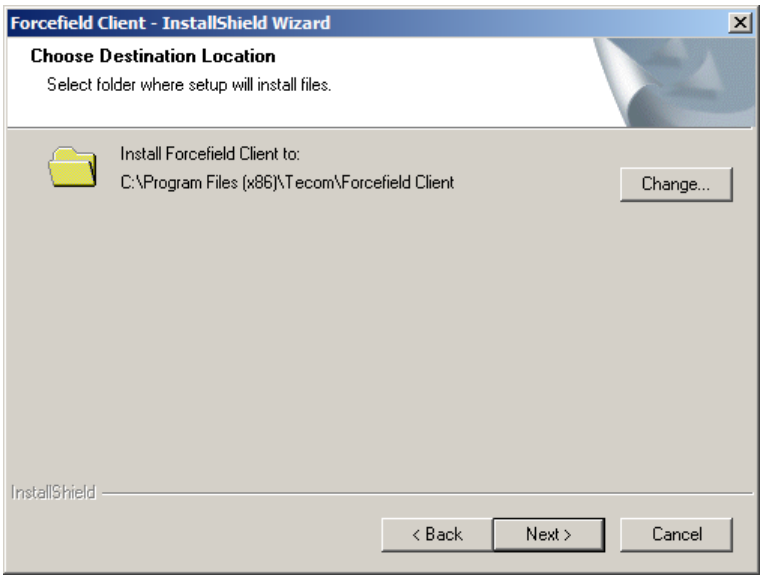
4. InstallShield displays the Forcefield Client welcome screen (version numbers will vary). Click Next to continue.



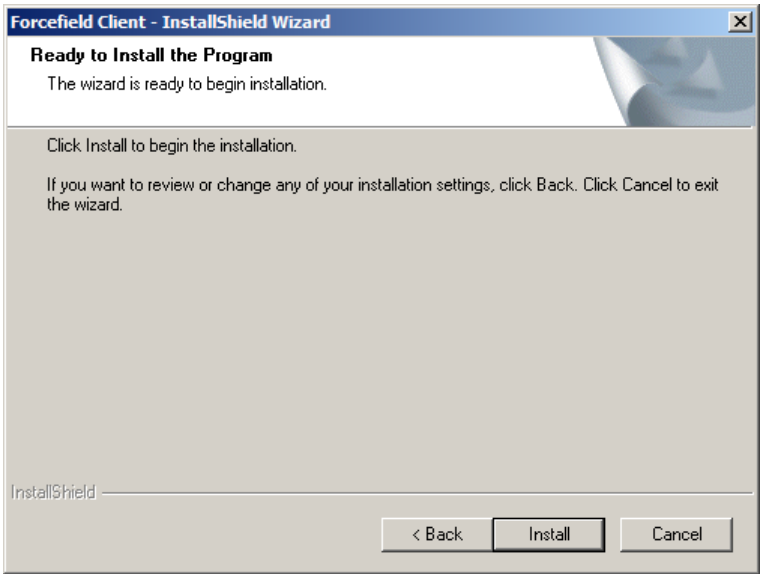
5. InstallShield displays the Forcefield Client License Agreement. Select the I accept… radio button to indicate your acceptance and then click Next.



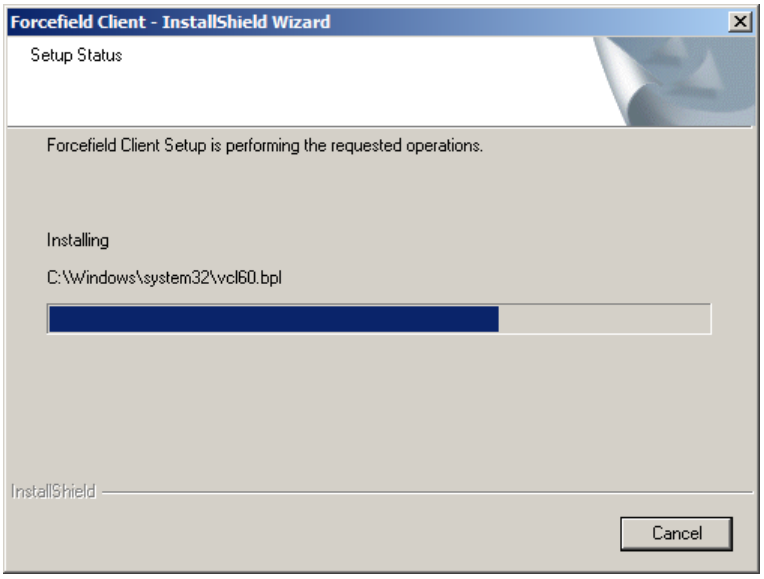
6. InstallShield displays the suggested destination folder. Click Next to continue, or click Change… to select a different location.



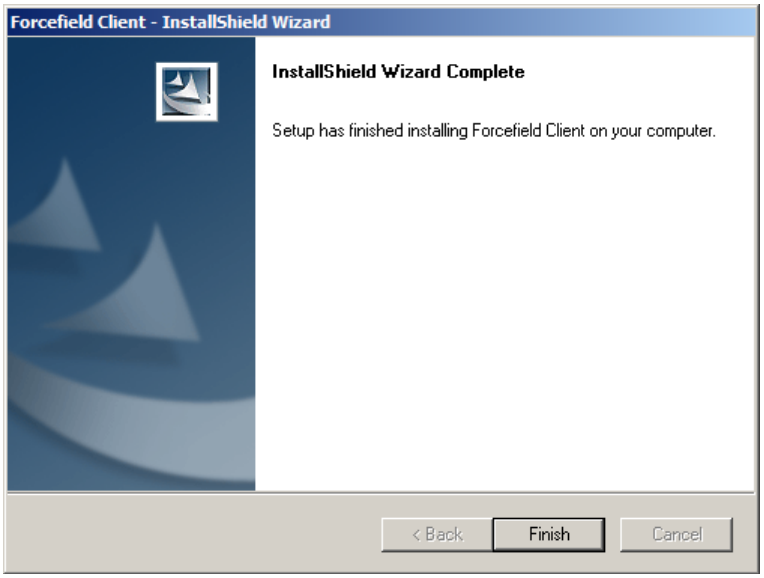
7. If needed, click Back to review or change installation details. Otherwise, click Install to continue.



8. InstallShield installs Forcefield Client files.



9. InstallShield completes the installation. Click Finish to exit.



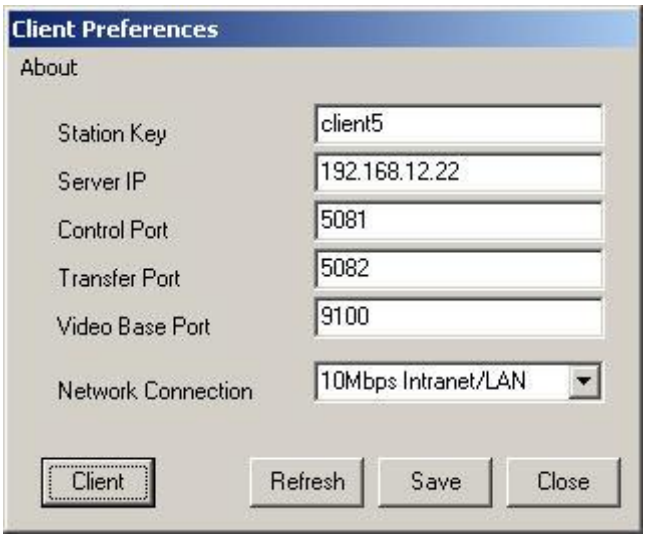
Connecting the client to the server

Prior to performing this procedure, you need to have the following information recorded on the “System-wide information record” on page 85 and the “Node-specific information record” on page 86:

- Station key
- The server’s or node’s IP address that the client will connect to
- Control Port number
- Transfer Port number

To connect to the server (or node, as applicable):

1. Go to Start > All Programs > Tecom > Forcefield > Preferences. The Client Preferences window opens.



2. Type the Forcefield station key in the Station Key field. The station key is case-sensitive and must be entered correctly. It is not possible to search for station keys.
3. Type the server's or node's IP address in the Server IP field.
4. Check the details of the Control Port field against the recorded details.
5. Check the details of the Transfer Port field against the recorded details.
6. Do not change the Video Base Port.
7. Click Save and then click Client to launch Forcefield Client.
8. Remove the Forcefield Installation CD or USB device from the Windows computer, and store it in a safe location.

What happens next?

The Windows menu Start > All Programs > Tecom > Forcefield contains the following applications:

- Client—Opens the Forcefield Client application. Use this option to start Forcefield client.
- Preferences—Opens the Client Preferences window. This window is used during installation or for checking connection faults (see "Troubleshooting client connections" on page 90).

Chapter 5
Upgrading a Forcefield system

Summary

This chapter describes how to modify the Forcefield system by adding nodes.

Content

Overview

A Forcefield system can be modified in a number or ways by purchasing license modules and adding them to the system by using a new License disk. Refer to Key Forcefield Concepts in the *Forcefield Operators Manual* for an overview of Forcefield system configurations.

When additional modules are required, use Admin > Configuration > Modify License to install the module. Refer to the *Forcefield Operators Manual* for details.

This chapter describes the following advanced license modules that are of particular interest to Forcefield installation technicians:

- Multi-node capability (part number TS9115)
- Offsite redundancy capability (part number TS9118)

Notes:

- Installing and using advanced modules require Forcefield installation technicians to be trained and assessed in advanced Forcefield applications such as multi-node use and video integration.
- Restart the Forcefield server after installing a new or modified module license.
- Multi-node operation and hot standby server requires Forcefield version 5.1.5 or later. Offsite redundancy (data mirroring) requires Forcefield version 6.2 or later. If adding these modules to a previously-installed version of Forcefield, you must update your Forcefield software prior to attempting to use new functionality. Contact your distributor for the required software patch, or Forcefield Installation CD or USB device, as applicable.

Adding a node

Additional Forcefield nodes are required if you need to:

- Increase system capacity (more clients or Challenger panels)
- Use a hot standby backup controlling node (backup server)

Note: All Challenger panels connected to the primary controlling node must be upgraded to firmware version V8-C-MFx.8106 (or later). Failure to upgrade the panel firmware may result in very slow event reporting.

A Forcefield multi-node setup consists of at least two computers with QNX and Forcefield installed. One computer is the primary controlling node (node 1) and is connected via LAN to additional QNX computers that are used as nodes 2 and higher.

Each Forcefield node may be licensed for up to 5 Forcefield clients. Standard edition can have up to 8 nodes, and Enterprise edition can have up to 20 nodes.

The number of Challenger panels that can be controlled by the system depends on the type of Forcefield hardware used. Standard edition Forcefield hardware can communicate with up to 32 Challenger panels. Enterprise edition Forcefield hardware can communicate with up to 128 Challenger panels.

When additional panels or clients are required, you must purchase additional licenses.

Refer to the Forcefield Data Sheet for details about system capacity.

Procedures to add a node

Adding a node is a three-stage process:

- The first stage is to prepare the node by licensing it and assigning a node number. This stage can be done off-site (or prior to connecting to the site's LAN) if desired.
- The second stage is to install the prepared node into a Forcefield system that has been licensed for multi-node functionality.
- The third stage is to use a Forcefield client to incorporate the node into the Forcefield system.

Note: Initially, all Forcefield computers have the default installation IP address of 192.168.0.1.

This section assumes that the Forcefield primary controlling node (node 1) has been installed according to Chapter 3 "Setting up Forcefield" on page 9, and describes the additional procedure of installing a non-controlling node into a working Forcefield system (where the primary controlling node's IP address may be the default IP address or an assigned IP address).

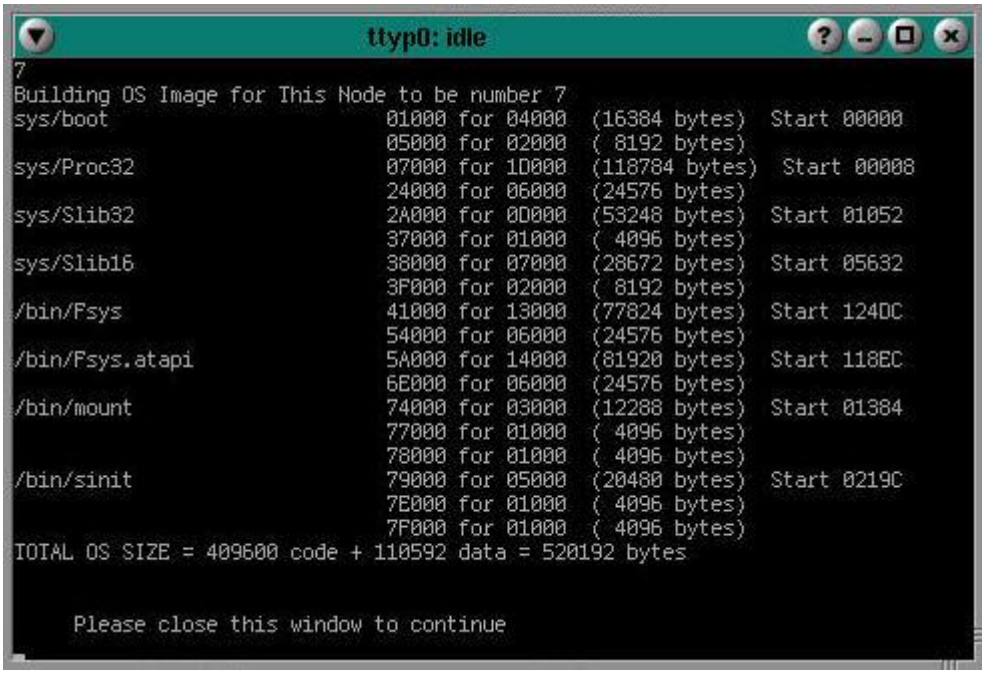
The images used in this section are based on the standard edition multi-node system (8 nodes maximum). Be aware that the Enterprise edition allows up to 20 nodes and the respective images would reflect the increased number.

Stage 1—Preparing the new node

To prepare a new node:

1. Power up the new node (the startup process may take a couple of minutes).
2. Display the Forcefield user interface using one of the methods described in "Initial user interface options" on page 11. The user interface prompts for the Licence CD.
3. Insert the Forcefield License into the CD or USB drive of the new node.
4. On the user interface, click Continue. A window prompts for a node number.

5. Enter the node number in the range 2 to 8 (2 to 20 for Enterprise edition). In response to the new node number, Forcefield displays the summary window.



6. Click the X to close the summary window and reboot the node.

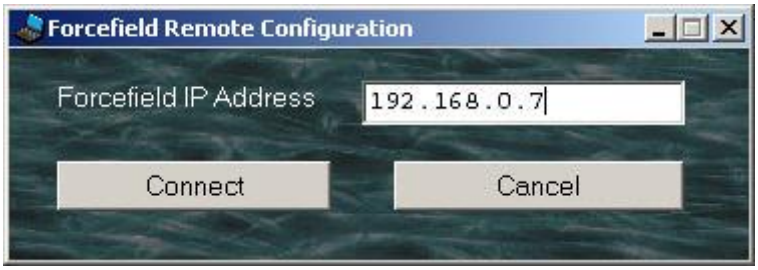
7. Power down the new node and disconnect the cables.

Stage 2—Installing the new node

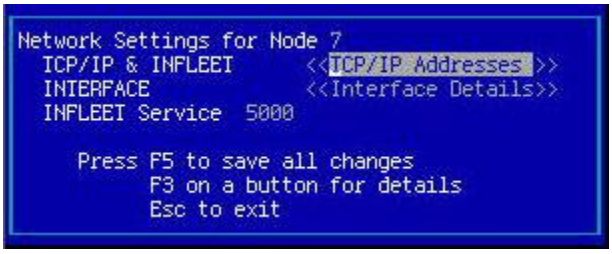
To install a prepared node:

1. Connect the Ethernet port of the new (prepared) node into the LAN used by the currently running Forcefield system.
2. Power up the new node (the startup process may take a couple of minutes).
3. Display the Forcefield user interface using one of the methods described in “Initial user interface options” on page 11.

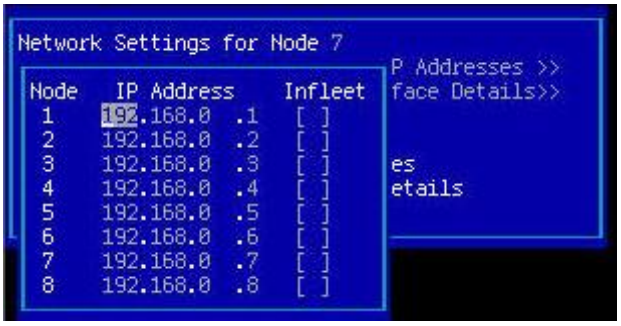
4. The last digit of the default installation IP address is changed to match the node number (e.g. 192.168.0.2, 192.168.0.3, … 192.168.0.20). If using Forcefield Remote Configuration, it will not be able to connect with the node at 192.168.0.1 because the IP address has changed. If you need to connect to the node after it reboots, you must use the new IP address. For example, the following IP address would be used to connect with node 7.



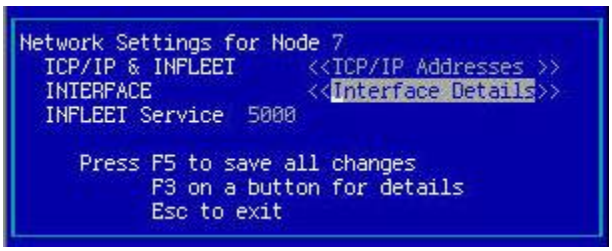
5. The network configuration utility (nwcfg5) runs automatically when a new node is added to a Forcefield system.



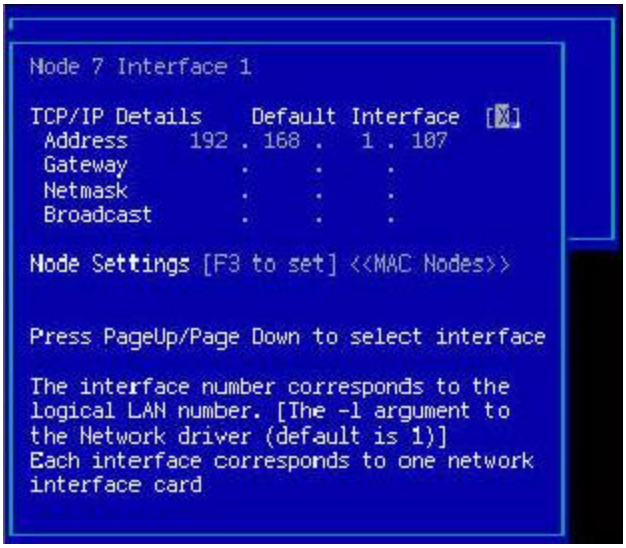
6. Press Esc to accept the default network setting for the node (i.e. in the case of node 7 the IP address is 192.168.0.7). Alternatively, select the << TCP/IP Addresses >> button on the Network Settings for Node screen, and then press F3 to set up TCP/IP.



7. Go to the required node number and input the assigned IP address (refer to “System-wide information record” on page 85). Assign the IP addresses for all nodes in the system, including the backup server (if applicable).
8. When finished, press Esc to return to the Network Settings for Node screen.



9. Select the <<Interface Details>> button on the Network Settings for Node screen, and then press F3 to set up the interface details (as recorded on “System-wide information record” on page 85.



10. When finished, press Esc to return to the Network Settings for Node screen.
11. Press F5 to save all changes. The following window displays.

12. Commission the node. Refer to “Stage 3—Adding the new node to Forcefield” below for details.

Stage 3—Adding the new node to Forcefield

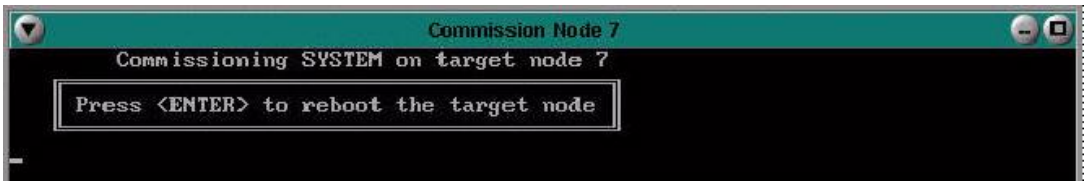
This stage is performed from a Forcefield client (it is assumed that this is an upgrade to an existing system that already has a client).

To add a node to the Forcefield system:

1. Run Forcefield client on the system.

2. Go to Databases > Computer Equipment > Computer and create a record for the new node.

3. Go to Admin > Configuration > Commission Node, select the new node.
4. Click Run. The following window displays.



5. Press ENTER to restart the selected node, run Forcefield on it, and enable communications between the server and the node.

Adding a backup server

Refer to “Appendix B Using offsite redundancy” in the *Forcefield Operators Manual*.

Adding the video service

Forcefield supports DVRs via “video service” applications Video Status Manager (VSM), Video Presentation Client (VPC), and brand-specific plug-in modules.

Refer to the *Forcefield External Interfaces Manual* for the process of installing VSM and VPC, and integrating DVRs and cameras into a Forcefield system via the video service.

Chapter 6
Forcefield system application

Summary

This chapter describes various ways in which Forcefield computers and Challenger panels may be connected.

Content

Overview

In this chapter, the images in Figure 24 below are used to indicate specific equipment.

Please refer to the following sections:

- "Connecting to Challenger Series panels

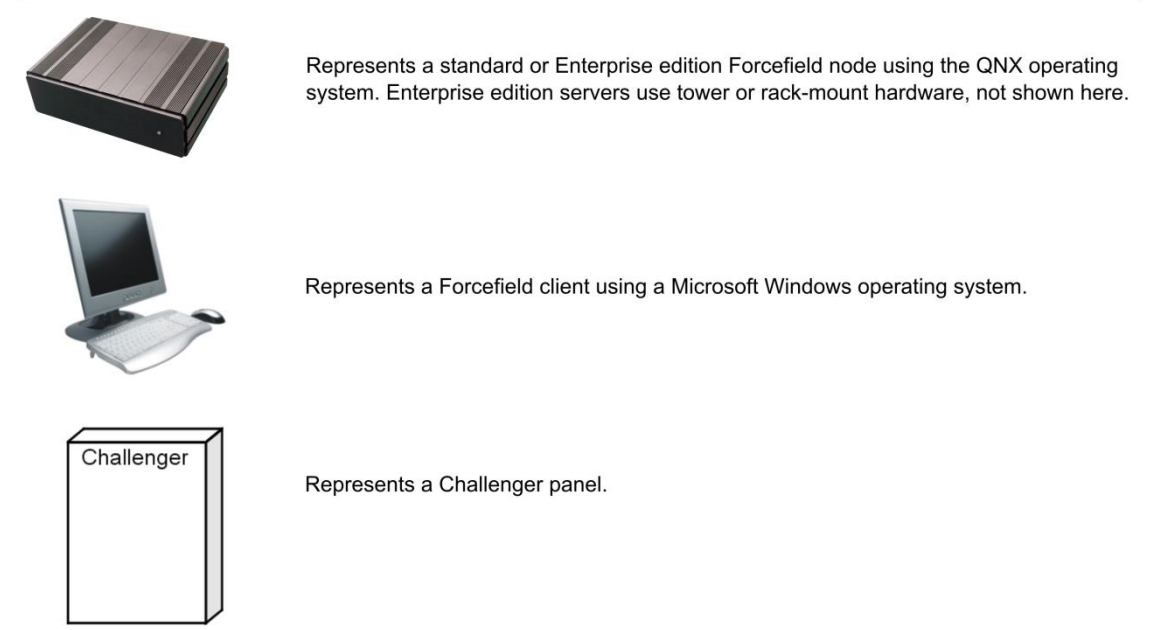
Forcefield can connect with Challenger Series panels in a variety of ways. Refer to the following manuals for detailed information:

- *Challenger Series Installation and Quick Programming Manual*. See “Enabling communications”.
- *Challenger Series Programming Manual*. See “Connecting to management software” and “Configuring IP connections”.
- *Forcefield Operators Manual*. See “Forcefield to Panel IP Settings (Challenger10)” for details about connecting to Challenger Series panels via the “Ethernet (TCP)” communications type.

Connecting to Challenger V8 panels” on page 51

- "Connecting to Challenger Series panels” on page 51

Figure 24: Forcefield equipment symbols



Connecting to Challenger Series panels

Forcefield can connect with Challenger Series panels in a variety of ways. Refer to the following manuals for detailed information:

- *Challenger Series Installation and Quick Programming Manual*. See “Enabling communications”.
- *Challenger Series Programming Manual*. See “Connecting to management software” and “Configuring IP connections”.
- *Forcefield Operators Manual*. See “Forcefield to Panel IP Settings (Challenger10)” for details about connecting to Challenger Series panels via the “Ethernet (TCP)” communications type.

Connecting to Challenger V8 panels

Forcefield can connect to Challenger V8 panels via:

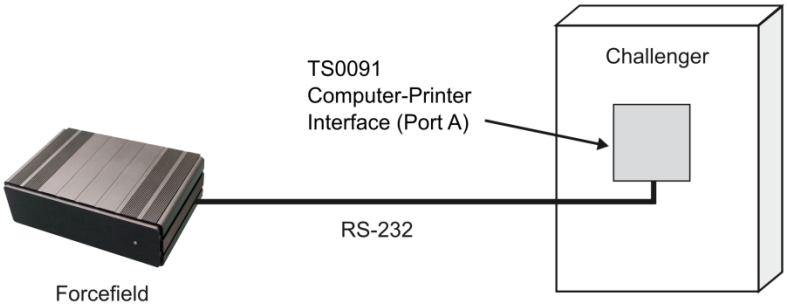
- Direct RS-232 serial connection (see “Direct RS-232 serial connection” on page 52)
- Dialler (see “Dialler connection” on page 54)
- IP communications (see “Ethernet connection” on page 55), see also “Programming UDP/IP mode” on page 59.
- A combination of the above (see “Ethernet connection with backup dialler” on page 56).

TCP/IP is used for communicating with additional Forcefield nodes, polled communication with Challenger (using an IP Interface), and e-mail. UDP/IP is used for event-driven communication with a Challenger (using an IP Interface) in event-driven mode instead of TCP/IP polling mode.

The following diagrams illustrate the various methods in which a Forcefield node may be connected to Challenger V8 panels. Forcefield Client is a client application only and does not connect directly to Challenger panels.

Direct RS-232 serial connection

Figure 25: Connection via RS-232 from Challenger V8 to a serial port on the Forcefield node



To establish a direct connection:

1. Use the Challenger V8 keypad (RAS) to program the Computer Address (Install menu 9: Communication).
2. Use the Challenger V8 keypad (RAS) to program the following options (Install menu 28: Security Password):
   - Password—Set initially to 0000000000.
   - Security Attempts—Set to 255.

   Note: It is advisable to change the settings for the password and security attempts once Forcefield is communicating with the Challenger.
3. Connect the cable from the Challenger to the Forcefield communication port at the required node. See “Connection Details” on page 53 for the wiring diagram appropriate to the Challenger version. (You can use the Forcefield command Status > Serial Port Status to check the connection.)
4. In Forcefield (Databases > Computer Equipment > Ports), program a Challenger communications port of the type Challenger Direct, for the required node. Set the Baud Rate to 4800.
5. In Forcefield (Challenger > Challenger Programming), program a Challenger to have a connection type of Direct Serial, and then select the previously-defined port.
6. Save the Challenger record to establish communication.

Connection Details

Figure 26: Serial connections for Challenger V8

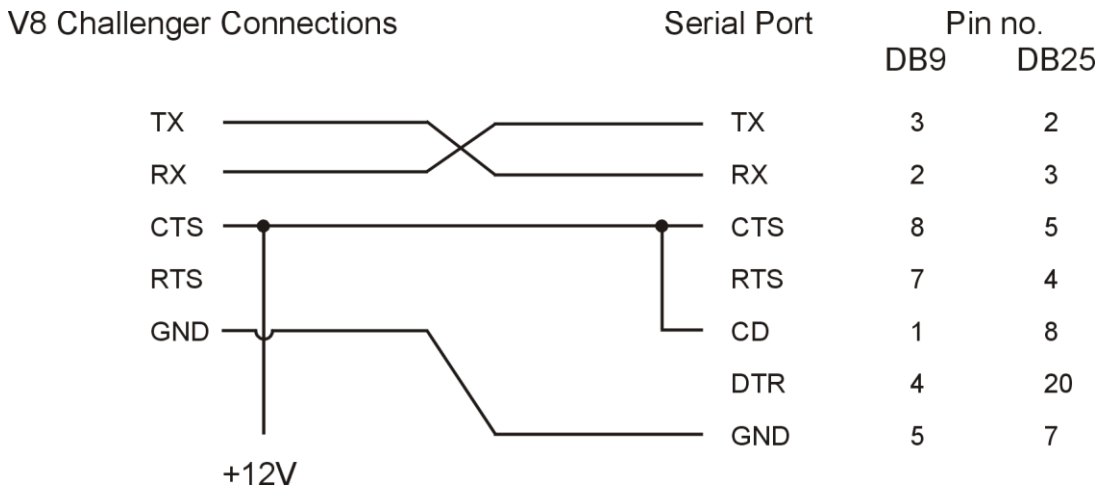
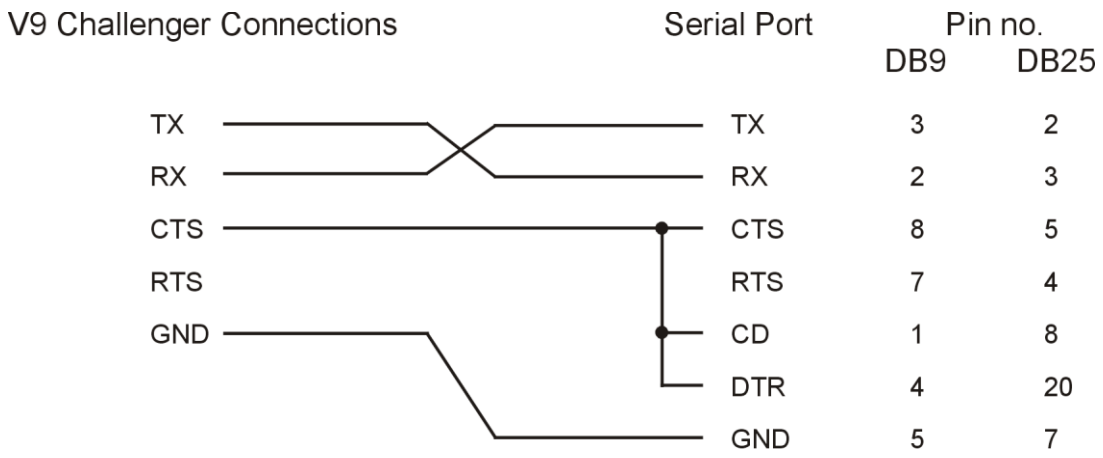
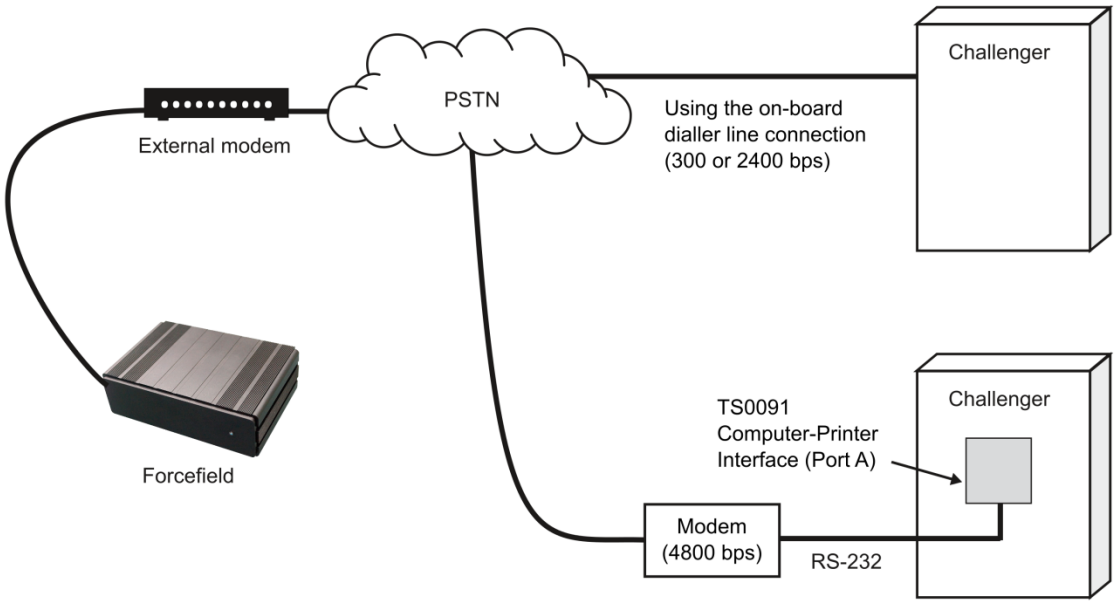


Figure 27: Serial connections for Challenger V9



Dialler connection

Figure 28: Connection via dialler from Challenger V8 panels to serial port on the Forcefield node



Note: The modem must be set so CTS is high when the modem is turned on and CD (carrier detect) is low except when connection is established with the remote modem (e.g. for a Netcomm Smart Modem, the string for CD is: AT&C1).

The number of modems required to handle dial-up Challenger panels depends on how much data each Challenger generates.

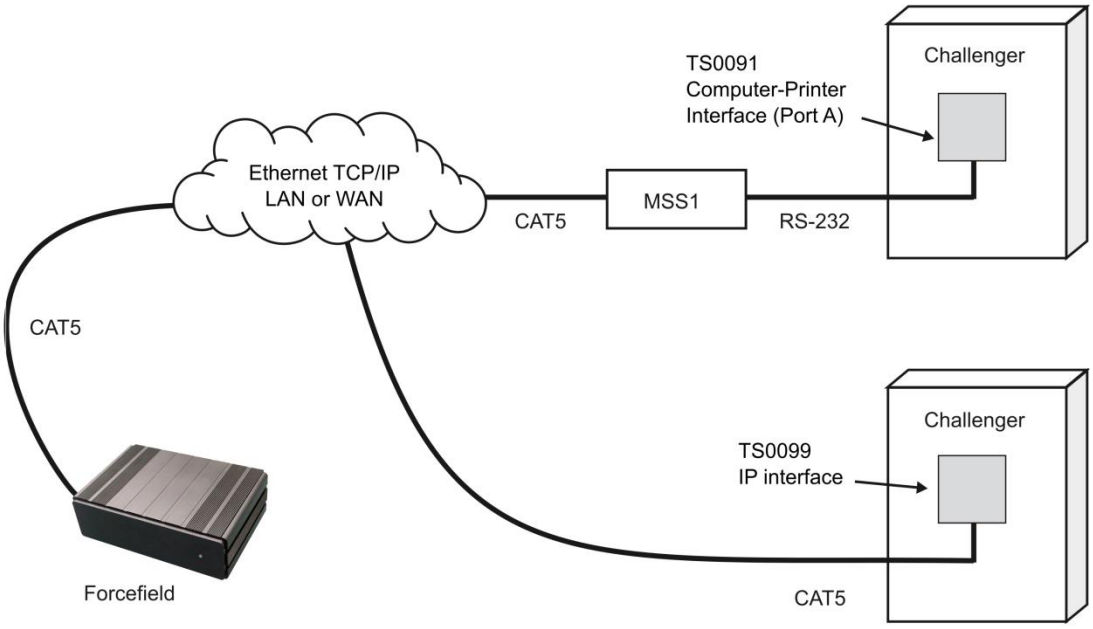
To establish a dialler connection:

1. Use the Challenger V8 keypad (RAS) to program the following options (Install menu 9: Communication Options):
   - Computer Address—Required
   - Computer Phone No.—Required
   - Computer via modem—Required
   - Dial Alarm events instantly—Optional (recommended)
   - Dial Access events instantly—Optional (not recommended)
   - Dial via on board modem—Select, if appropriate
   - Dial via computer port—Select, if appropriate
2. Connect the modem to one of the Forcefield node’s serial ports.

3. In Forcefield (Databases > Computer Equipment > Ports), program a Challenger communications port of the type Challenger Dialler, for the Forcefield node:
   - For Dial Via on board modem, use 300 Baud, 8 bits, no parity, and no handshaking (may be 2400 Baud if supported by the particular Challenger panel).
   - For Dial via Computer Port, use 4800 Baud, 8 bits, no parity, and no handshaking.
4. In Forcefield (Challenger > Challenger Programming), program a Challenger to have a connection type of Dialler 300 or Dialler 2400+ (as appropriate).
5. Enter the AT command for Forcefield to dial the Challenger (e.g. ATDT) and the phone number.
6. Save the Challenger record to make ready for dialler communication.

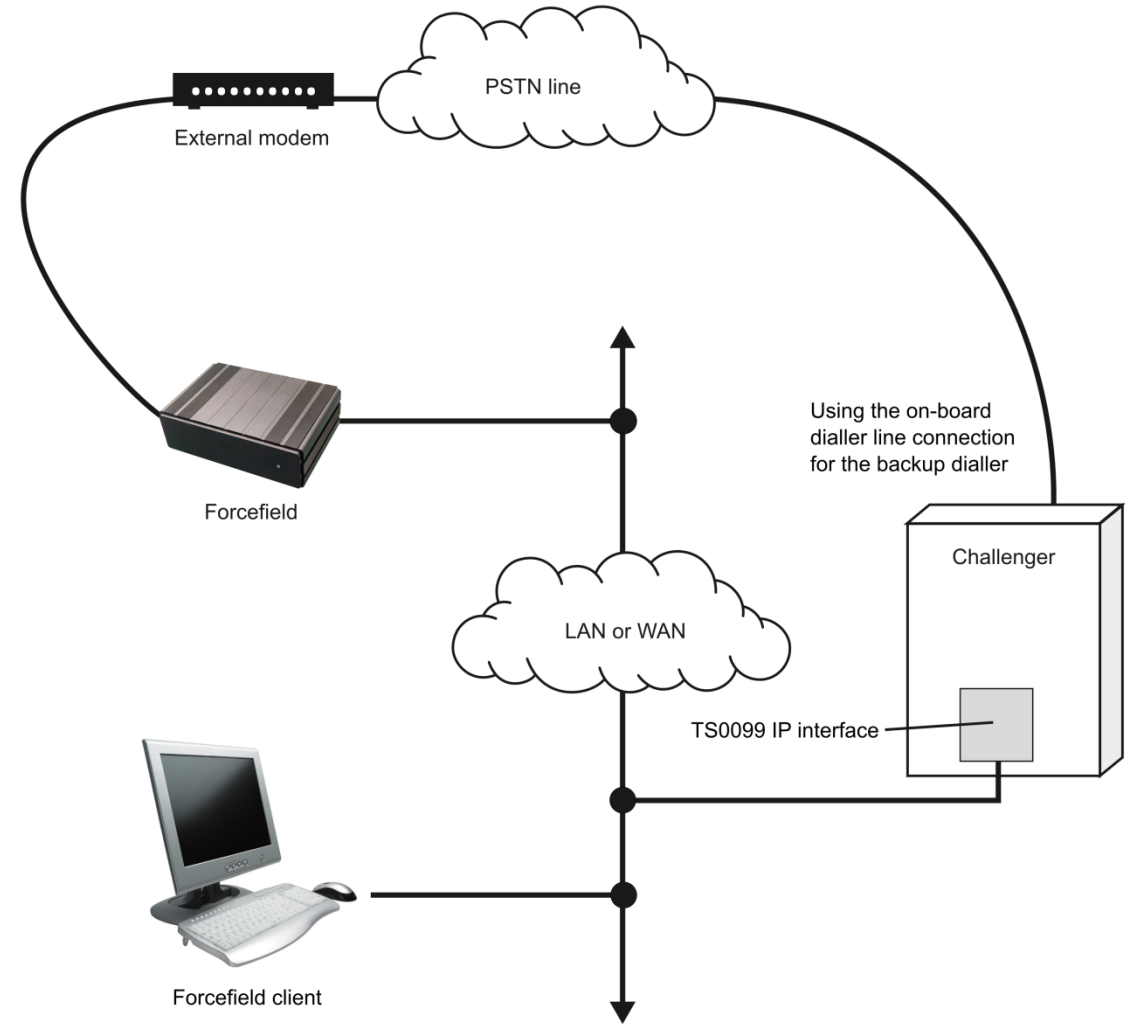
Ethernet connection

Figure 29: TCP/IP connection from Challenger V8 panels to the Forcefield node's LAN port



Ethernet connection with backup dialler

Figure 30: TCP/IP connection from Challenger V8 panels to the Forcefield node's LAN port, with backup dialler



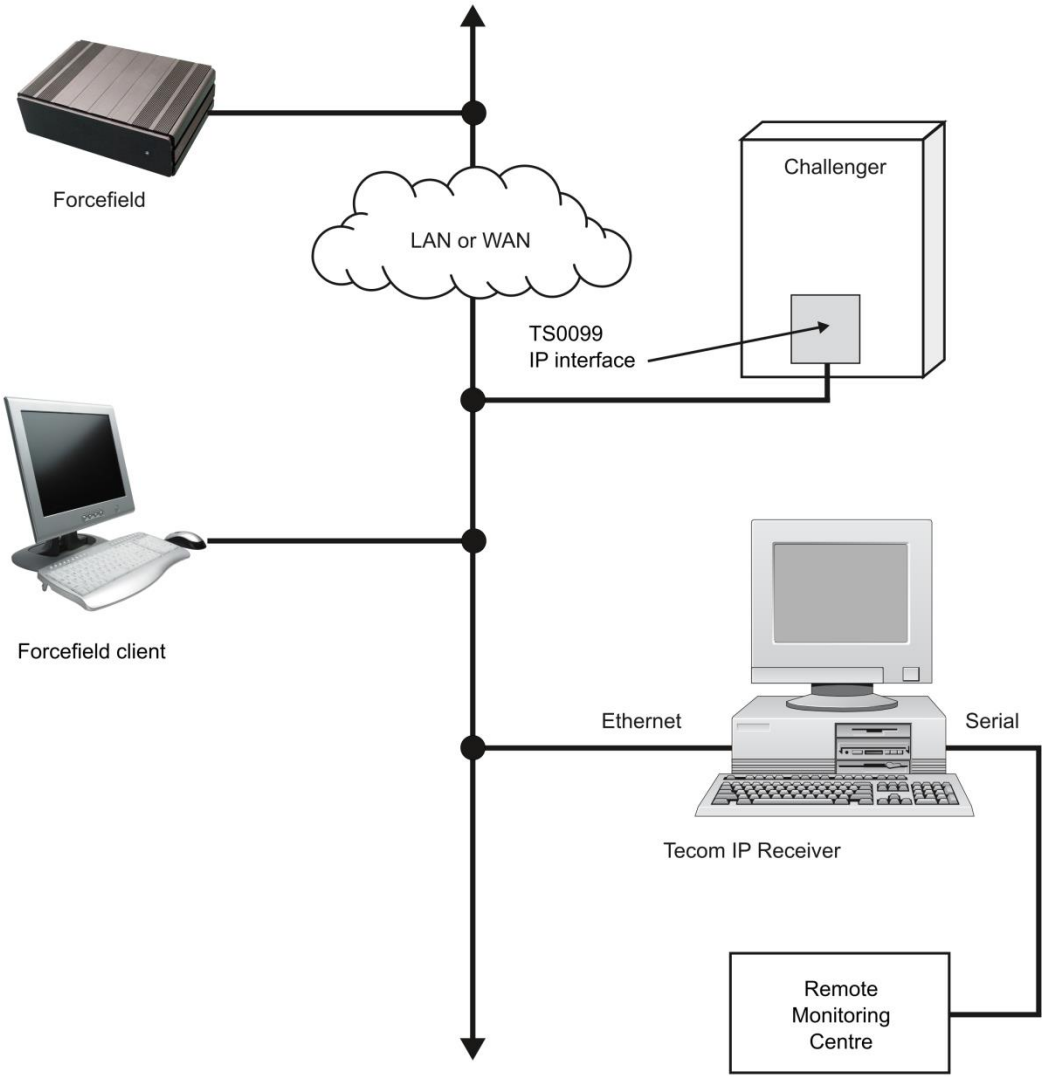
In Figure 30 above Forcefield is used as the access control and security management software to communicate to the Challenger V8 panel via the IP Interface.

A LAN/WAN is used between the Forcefield node's LAN port and the IP Interface's Ethernet port. A Forcefield client is connected using the LAN/WAN.

On the event of a Challenger Ethernet failure, a modem may be connected to one of the Forcefield node's serial ports to receive events from the Challenger panel's onboard dialler via the PSTN.

Ethernet Connection With IP Receiver

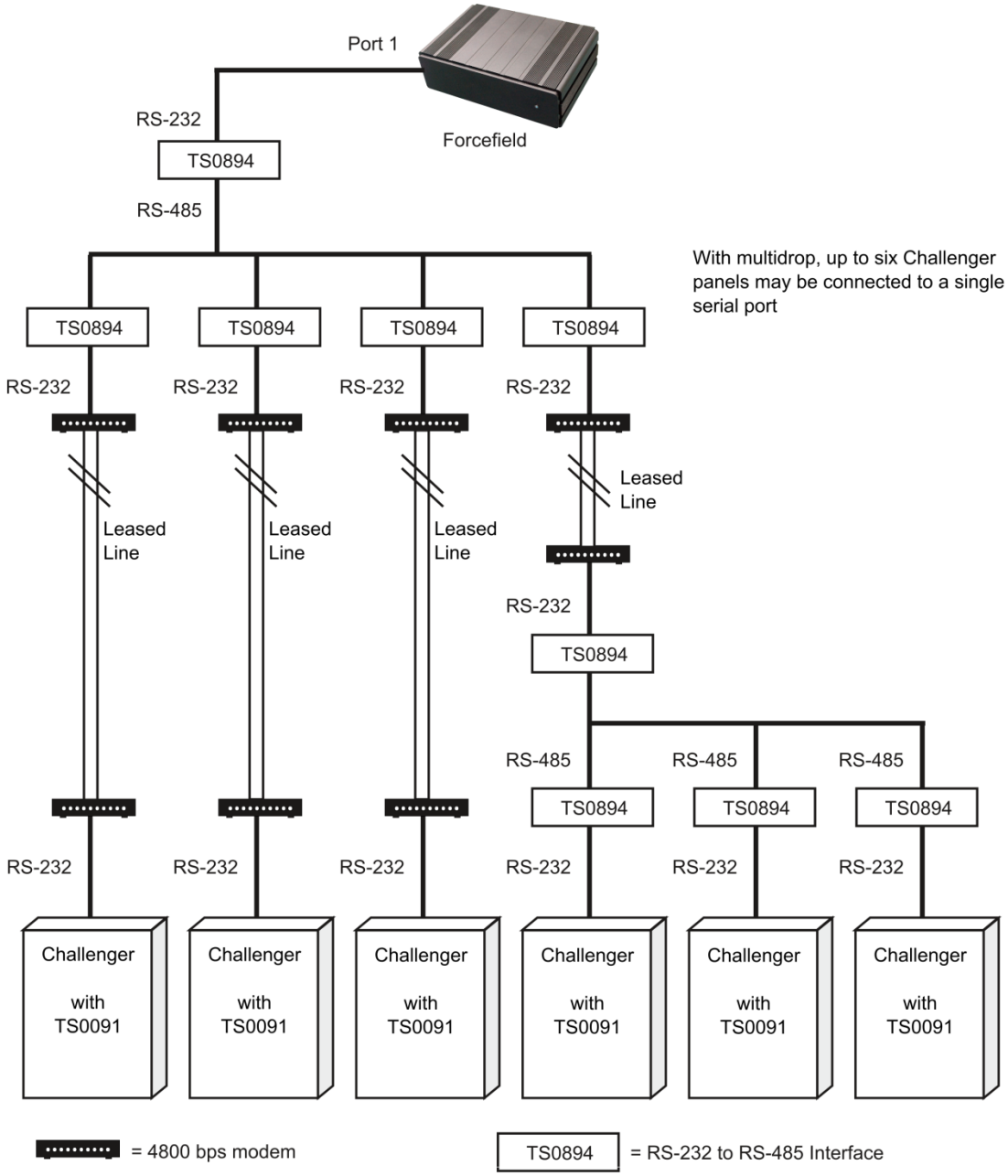
Figure 31: Forcefield node, Challenger V8, and IP Receiver via Ethernet



A Tecom IP Receiver is connected to the LAN/WAN to pass CID events from the Challenger panel to a remote monitoring centre. Forcefield and IP Receiver do not communicate to each other.

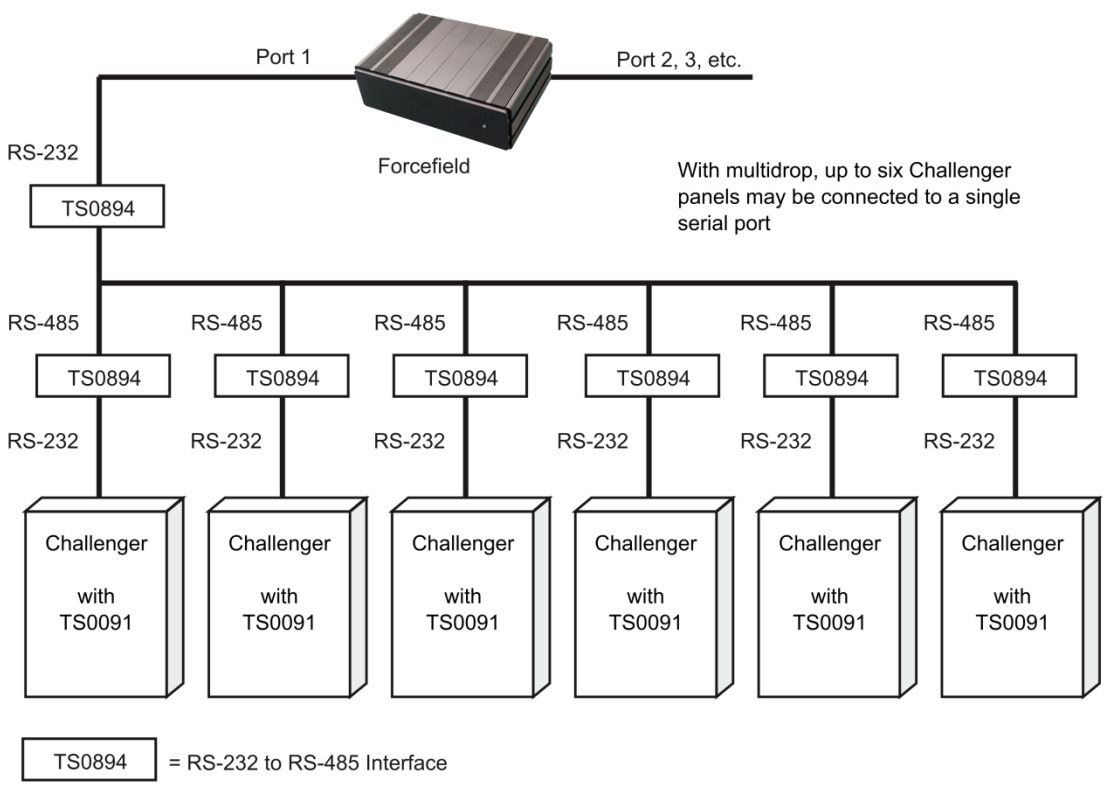
Leased-line multi-drop connection

Figure 32: Leased line multi-drop to a Forcefield node's serial port



RS-485 multi-drop connection

Figure 33: RS-485 multi-drop to a Forcefield node's serial port



Programming UDP/IP mode

Assessed Forcefield Installation Technicians may program Forcefield for event-driven (UDP/IP) IP communications with a Challenger V8 panel (must be fitted with a TS0099 Enhanced Challenger TCP/IP Interface).

In event-driven mode, Forcefield waits to receive Challenger events; thus freeing the network for other data transfers. Forcefield sends a heartbeat signal to each event-driven Challenger panel at intervals nominated by the technician to monitor connectivity. The heartbeat signal is programmed in the Forcefield Ethernet configuration.

In polled (TCP/IP) mode, Forcefield polls the Challenger panels about four times a second for new data. This constant polling can slow the network.

Requirements:

- If you need to communicate with a Challenger V8 panel fitted with an IP Interface, the Challenger panel and interface must be correctly programmed for event-driven connection. Refer to the IP interface installation and programming guide for details.
- Details recorded for the Challenger panel's settings (including Challenger IP address, management software IP address, Gateway IP address and Port number).

Programming port settings

To program port settings:

1. Select Databases > Computer Equipment > TCP/IP Ports.

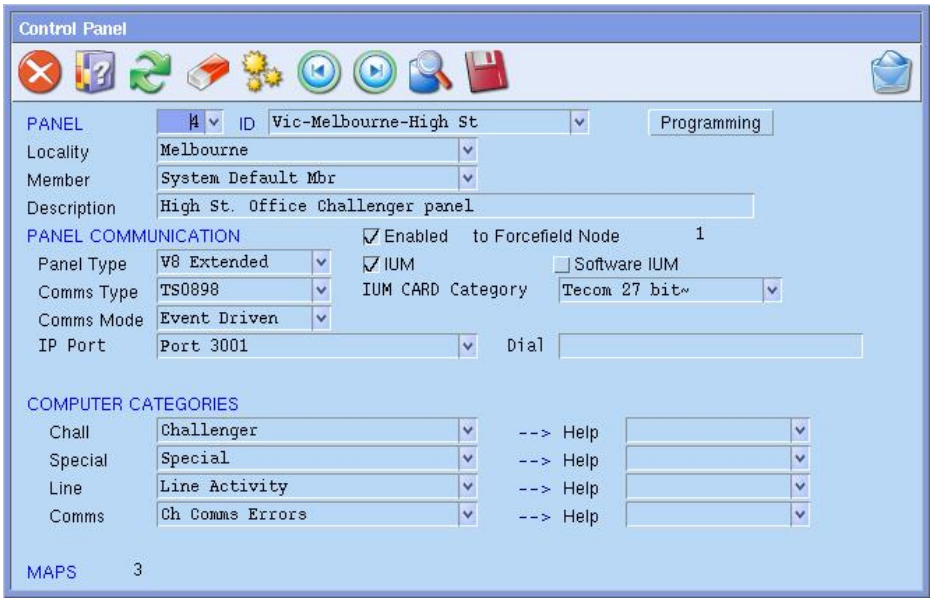
2. Type a name for the port in the IP Port field.
3. Type a port number in the Number field (e.g. 3001). Valid numbers are from 1024 to 65535.
4. Enter the number in the Controlled by System Node field for Forcefield node that will be responsible for this IP port.

Programming Challenger V8 settings

To program Challenger V8 settings:

1. Select Challenger > Program Challengers. The programming window opens.

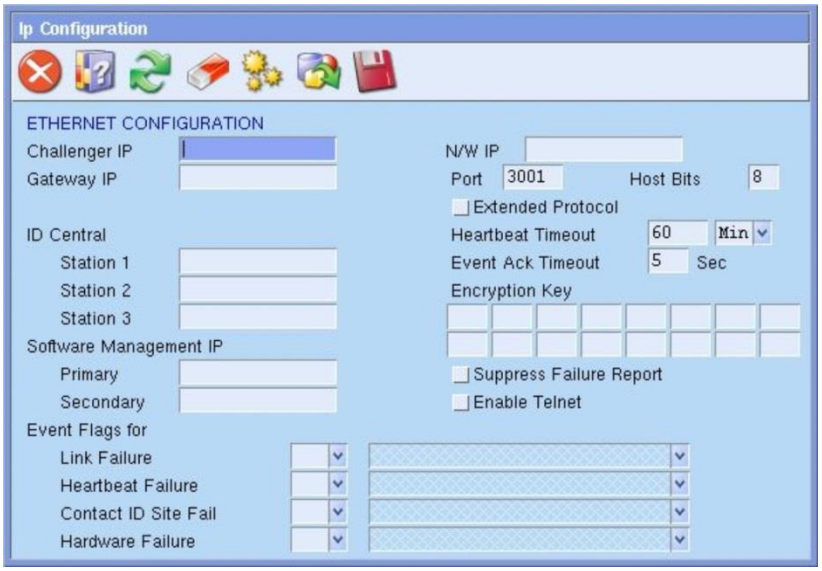
Figure 34: Challenger V8 programming window



2. Set up the Challenger record in Forcefield in the usual manner, and then proceed with the following steps to set up event-driven mode.
3. Tab to the Comms Type field, press F4, and select TS0898 from the list.
4. Tab to Comms Mode and select Event Driven. NOTE: Don’t select Enabled yet. You will do this later.

5. Tab to the IP Port field, press F4 to bring up IP Connect screen, and select the previously-defined port.
6. Press F5 to save the changes for the Challenger, and leave the screen open.
7. Click the Programming button to open the Challenger V8 programming window, and select option ‘Ethernet Configuration’ (shown below).

Figure 35: Challenger V8 Ethernet Configuration window



8. Type the IP addresses for:
   - Challenger IP.
   - Gateway IP.
   - N/W IP, if applicable (refer to the *Forcefield Operators Manual* for details).
   - ID Central Station 1 (SecureStream main receiver, if connected).
   - ID Central Station 2 (SecureStream backup receiver, if connected).
   - ID Central Station 3 (SecureStream disaster receiver, if connected).
   - Software Management IP Primary (Forcefield server). Contact the system administrator for details.
   - Software Management IP Secondary (for offsite redundancy).
9. In the fields Host Bits, Heartbeat Timeout, Event Ack Timeout, type the values as previously programmed into the IP interface from the RAS (menu 19, 47) if applicable. These values must match the values entered at the RAS.
10. Ignore the Extended Protocol check box. Refer to the *Forcefield Operators Manual* for details about this field.
11. Leave Encryption Key fields blank until you know that Forcefield and the IP Challenger are communicating with each another. Press F5 to save, and press ESC twice to return to the main menu.

12. Optional—Select Suppress Failure Report if you wish to stop “report fail” from displaying on an LCD RAS after communication with CID 1 is lost.
13. Select Enable Telnet, if required for TS0898 Ethernet Interface (requires Challenger V8 firmware version 8.112 or later; and does not apply to TS0099 Enhanced Challenger TCP/IP Interface).
14. Press Save to add the changes to the database.
15. Select Challenger > Download Challenger Data > Delete Download Buffer, and the Remove Download Changes window appears.

16. Select the Challenger, and then click F6 to delete the buffer.
17. Close the Remove Download Changes window.
18. Select Challenger > Program Challengers. The Challenger screen opens.
19. Open the record for the Challenger that you previously defined for Event Driven mode.
20. Right-click the Enabled box, and an X displays. Press F5 to save. The Challenger with the IP interface is active and in event-driven mode.
21. Open the Event Monitor window and right-click to select the Challenger programmed. Check the event window to verify that the panel is sending or receiving events.

Programming encryption settings (optional)

To add encryption:

1. After you know that Forcefield and the IP Challenger are communicating with each another, you may need to use the Ethernet Configuration screen to add encryption (see Figure 35 on page 61).
2. Type a number from 1 to 255 in one or more of the Encryption Key fields. Alternatively, to stop encryption, type zero in all Encryption Key fields.
3. Press F5 to save.

Appendix A
Reference

Summary

This appendix contains reference materials and the license agreement for Forcefield's database application.

Content

Re-installation procedure

Forcefield is pre-installed by Interlogix on Forcefield hardware. This section is provided to assist trained Forcefield installation technicians in case Forcefield and QNX software needs to be reinstalled on the Forcefield hardware.

This section uses standard Forcefield hardware (see Figure 1 on page 6) as an example. The specific details and messages displayed on screen will vary depending on the specific hardware used (standard or Enterprise, RAID or non-RAID, and so on).

Note: This is only a guide: it uses sample information. To use the instructions in this section you must also have appropriate knowledge of the particular system.

The hardware type is automatically detected by Application Loader, which displays “If this is not correct, the sysinit and video trap files may need to be altered to ensure the drivers for your hardware are activated.” Contact Technical Support if the detected hardware is not correct.

Note: The process described in this section overwrites all existing data on the Forcefield node. You must back up any data that you need to reuse to external media prior to using this procedure, or you will lose the data.

To reinstall Forcefield you need the following:

- Forcefield Installation CD or USB device
- Forcefield Licence CD or USB device

To re-install Forcefield on standard hardware:

1. Disconnect the server’s network cable.
2. Insert the Forcefield Installation CD or USB device in the Forcefield server’s CD or USB drive.
3. Connect a monitor, keyboard, and mouse to the server.
4. Restart the computer.
5. The monitor displays text similar to the following.

```
************* Application Loader *************

Select one of the following options:
1. Start a QNX Shell & mount system disk.
2. Start a QNX Shell without mounting system disk.
3. Install OS and Application (Warning: Clears System Disk)
```

6. Select option 3 and press ENTER. The monitor displays text similar to the following.

```
************* Application Loader *************

Please wait. Initialising disk.
```

7. As the installation proceeds, the results display (scrolling) on the screen for a considerable length of time. Eventually, the monitor displays text similar to the following.

```
************* Application Loader *************

INSTALLATION COMPLETE

AL has detected a PC type of AEC-6810
If this is not correct, the sysinit and video trap files
may need to be altered to ensure the drivers for your
hardware are activated.

Remove the Application CD

Please type "Shutdown" to reboot.
```

8. Remove the Forcefield Installation CD or USB device from the Forcefield server, type “Shutdown”, and then press ENTER.

The re-installation process is complete. The Forcefield server is now in the same state as when originally received from Interlogix. To continue, refer to “Note: You should change the password for your protection. Use the Forcefield command **Admin > Change Root Password** to change the QNX root password.

If using the *VMware vSphere Client* application, use the following steps.

Install the VSphere Client and Licensing the Server

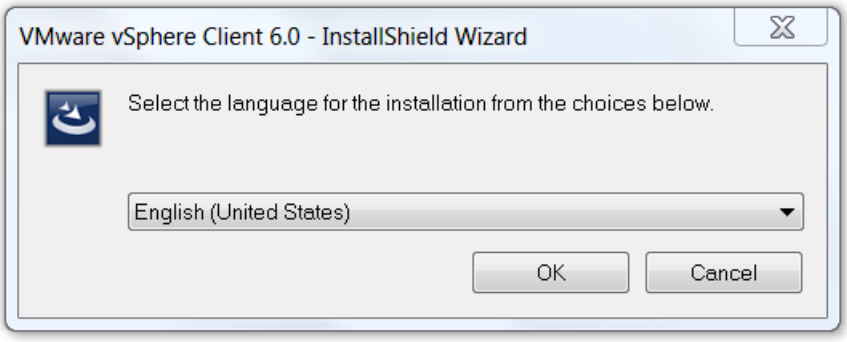
The VSphere client is required to communicate with the ESXi server so that VMs may be created or imported/exported. The client is installed on a computer that is connected to the server via an Ethernet cable (or through the network).

The Client may be downloaded from the internet by clicking in the http address on the ESXi start screen, or found in the CLIENT folder of the VMware installation CD.

Follow the process below to install the VSphere client.

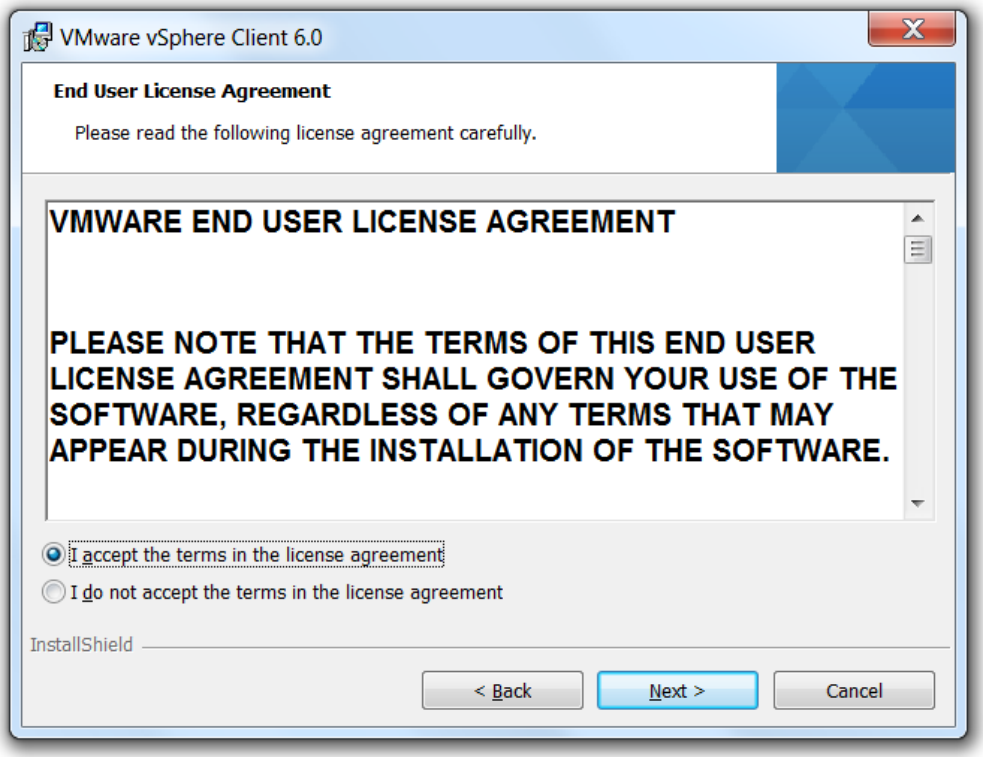
1. Double-click on the installer to start the installation process. The following window appears.

Figure 3: Start of the vSphere client install



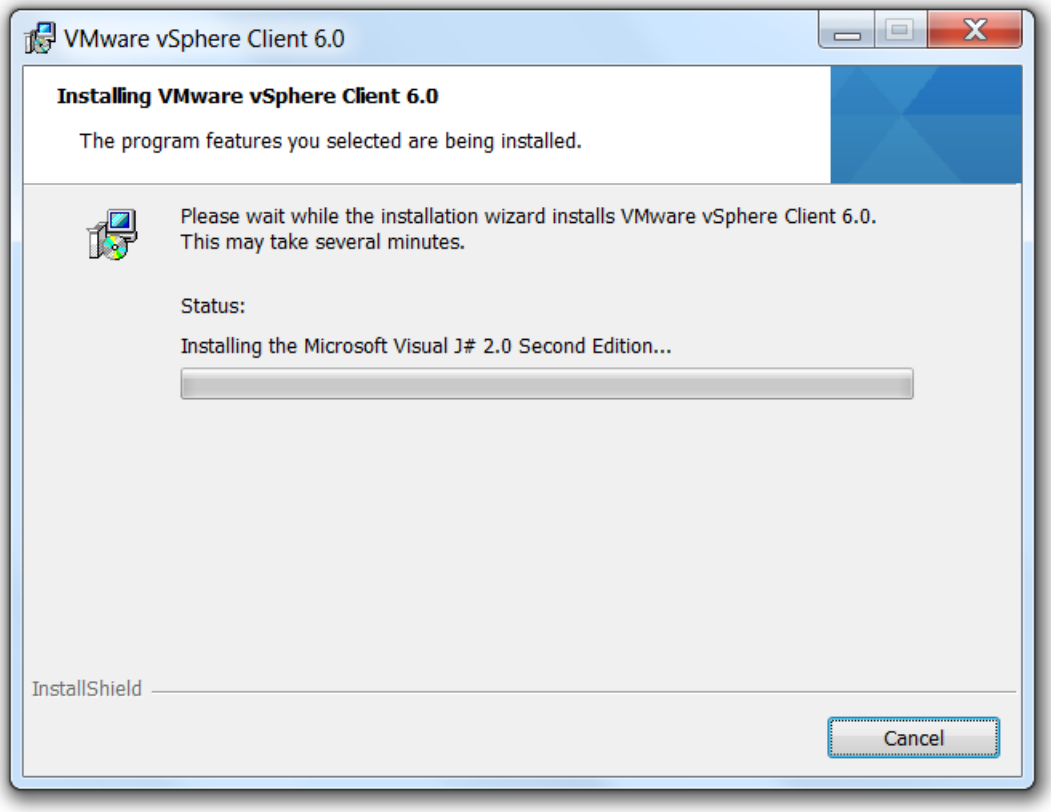
2. The Welcome Window for the vSphere installation appears. Click Next and the License window appears. Accept the License and click Next.

Figure 4: Accepting the vSphere's license agreement



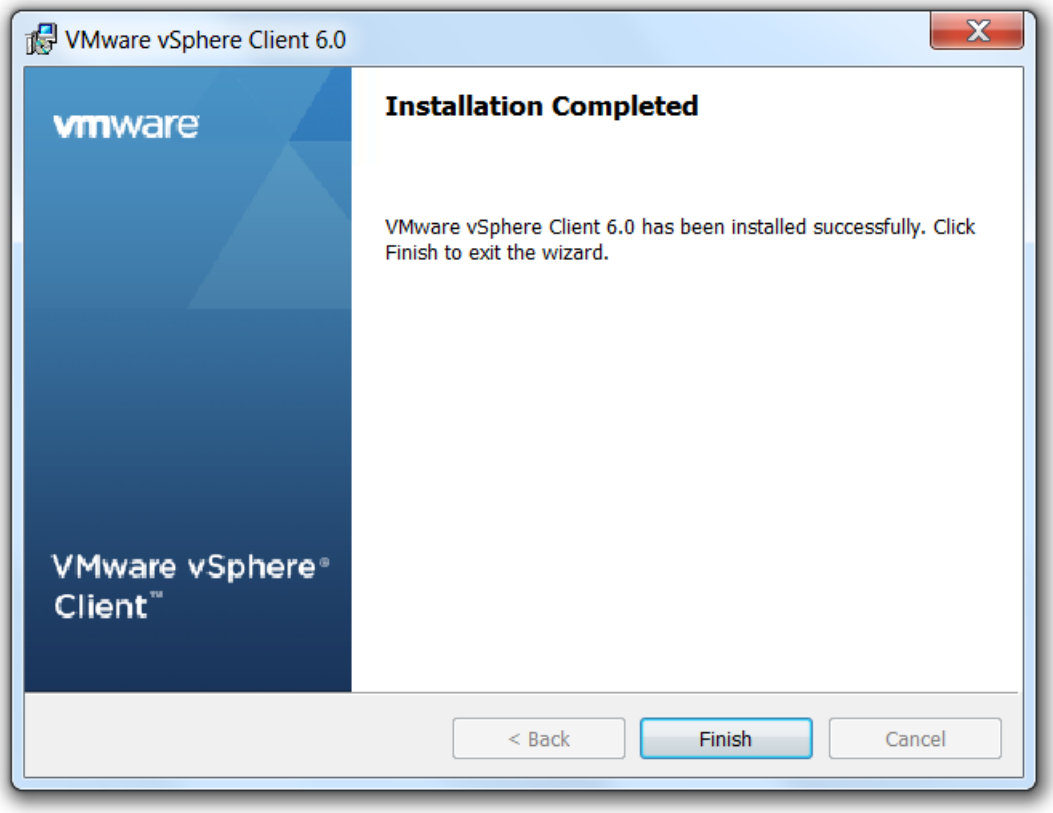
3. Click Next, then Next and the installation will start. The following progress window will appear.

Figure 5: Installation progress for vSphere client



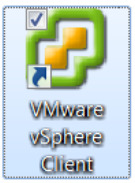
4. When the Install Completed window appears, click Finish.

Figure 6: vSphere client install is complete



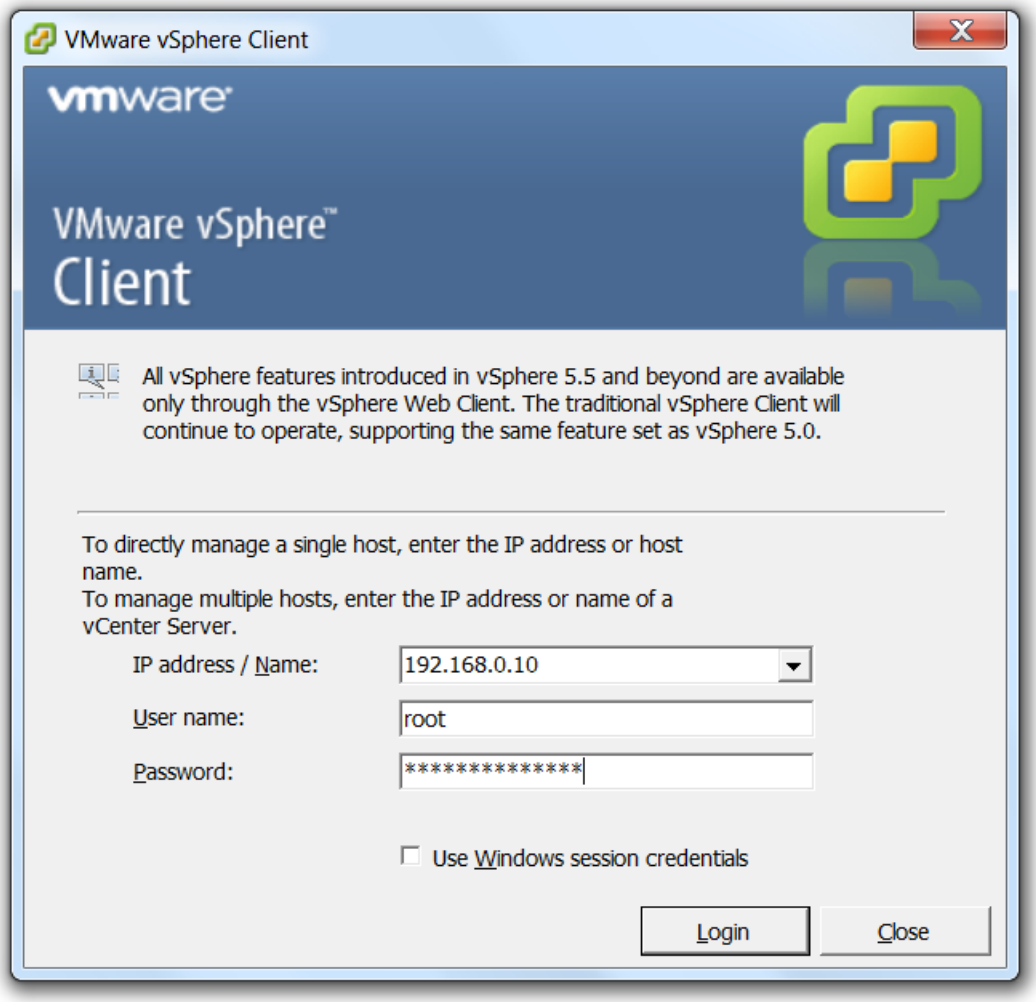
5. Start vSphere by double-clicking on the desktop icon.

Figure 7: Double click this icon on the desktop to start vSphere client



6. Connect vSphere to the server as shown.

Figure 8: Connecting to the server using the vSphere client



IP Address : **192.168.0.10** (as an example)

User Name : **root**

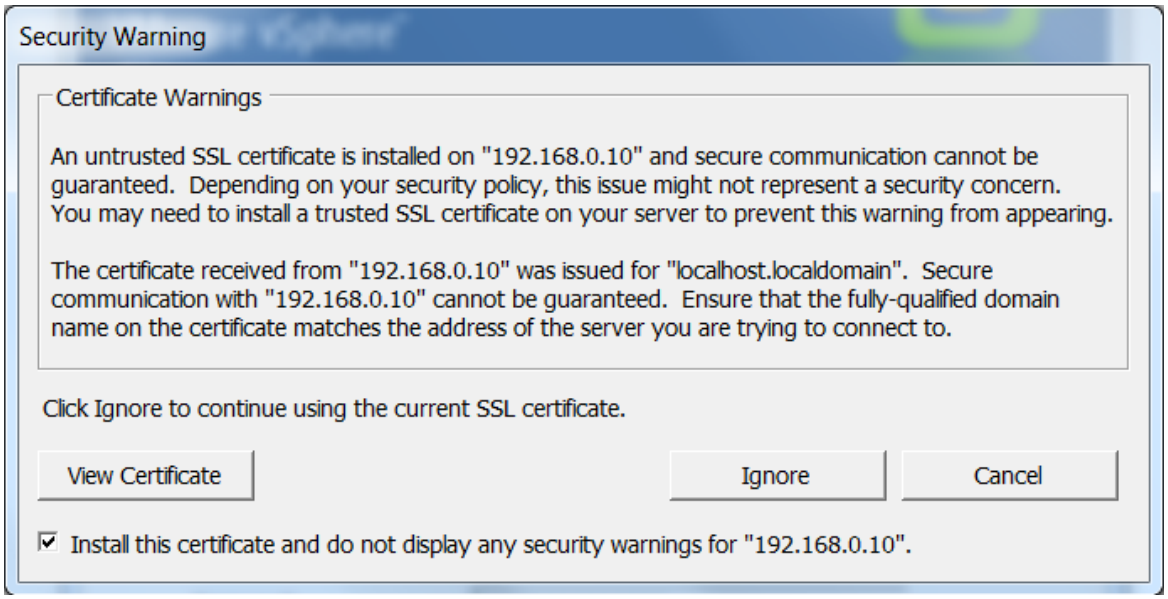
Password : **forcefield4346**

Click the **Login** button.

7. A security certificate warning will pop up as shown below.

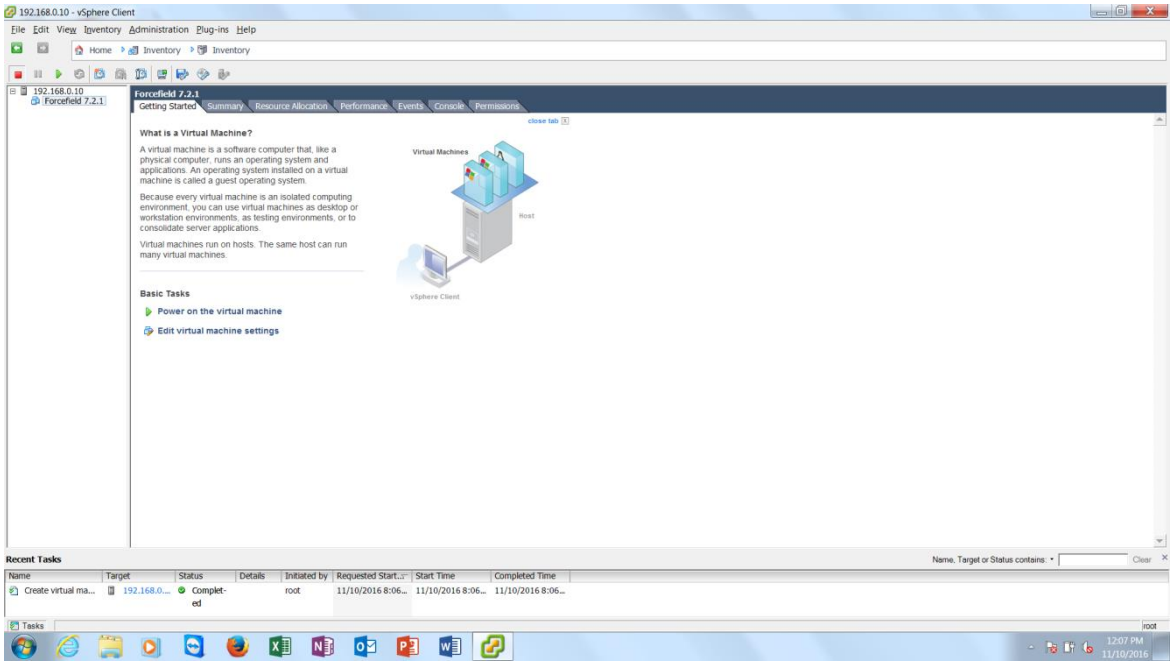
Click on the check box to **Install this certificate…** and click on the **Ignore** button.

Figure 9: Login Security Warning



8. Click on the VM named Forcefield 7.2.1 in the left hand pane, and then click on Power on the virtual machine under the Getting Started tab. If you do not see an option to Power On the virtual machine, and instead see options to Power Off and Suspend, then Forcefield is already running.

Figure 10: VM is ready to be started



Clicking on the Console tab displays the Virtual Machine's console.

To interact with the virtual machine, click within the window of the console tab. This makes the keyboard and mouse visible to the Virtual Machine.

To stop interacting, press the CTRL and ALT keys on the left-hand side of the keyboard at the same time. This detaches the keyboard and mouse from the Virtual Machine.

Set-up procedure” on page 12.

Logging in using proximity cards

An operator must log in to a workstation to start a Forcefield session, and may be required to enter a password on the login screen (the use of a password is a configurable Forcefield option).

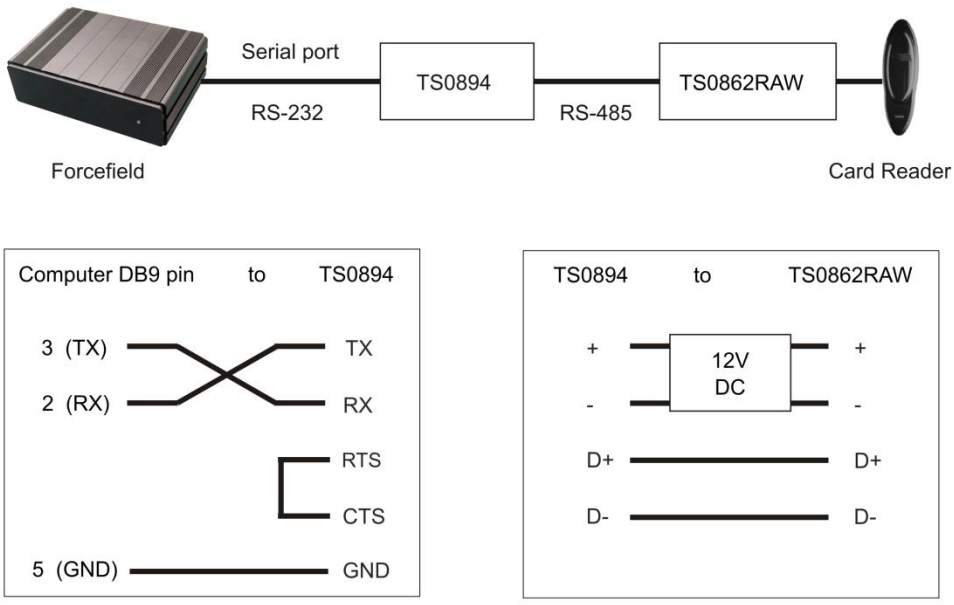
Forcefield may be configured such that the operator logs in by:

- Entering the operator code on the Forcefield login screen.
- Using an access card on a Smart Card Reader.
- Using both the Forcefield login screen and access card on a Smart Card Reader.

Note: Take care when programming card login. Incorrect settings may result in losing the ability to log in to the Forcefield workstation. This is especially critical on a single-node Forcefield system, where you cannot use another Forcefield workstation to correct the error.

This section describes how to set up Forcefield to use access card (proximity card) login.

Figure 36: Equipment and connections required for card login



To set up card login:

1. Connect the Smart Card Reader to the Forcefield node via a TS0862RAW Smart Door Controller and a TS0894 Isolated RS-232 to RS-485 Interface.

   TS0862RAW is a special raw card data version of the TS0862 Smart Door Controller.

2. Use the Databases > Computer Equipment > Ports command to create a port record for the card reader port. The type must be Serial (Other) and communication settings are no handshake, 4800 baud, no parity, and 8 bits.
3. Use the Databases > Computer Equipment > Workstations command to create or modify a workstation record.
4. Click the Login button to open the Workstation Options window.
5. Set the Login by Prox. Card option and program any other options required for login.
6. Close the Workstation Options window.
7. In the Card Login Port field, select the port record created for the card reader port.

Connecting printers

Use the Databases > Computer Equipment > Printers command to set up the following types of printer connections:

- Serial—for use with a serial port on the Forcefield server.
- Parallel—for use with a parallel port on the Forcefield server.
- Network—for use with a network printer. You must specify the host, remote name, and print cap.
- Client—for use with the Forcefield client's default printer (either network or local printer).

Setting up printers

Refer to the *Forcefield Operators Manual* for details of the following commands.

To add a serial or parallel printer to the Forcefield server:

1. Use the Databases > Computer Equipment > Ports command to create a port record (either serial or parallel, as required) for the printer port.
2. Optional—Use the Databases > Computer Equipment > Printer Access command to restrict the use of the printer.
3. Use the Databases > Computer Equipment > Printers command to create a printer record, using the previously defined port and printer access. The selected type must be either serial or parallel, as required.
4. Optional—Use the Databases > Computer Equipment > Workstations command to define the printer as the default workstation printer.
5. Connect the printer to the Forcefield server (see “Connections to Forcefield node” on page 74).

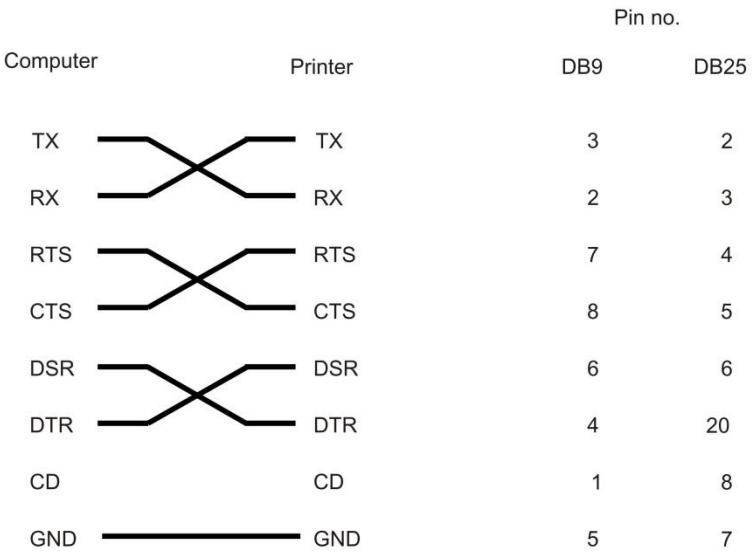
To add the default Windows printer to a Forcefield client:

1. Optional—Use the Databases > Computer Equipment > Printer Access command to restrict the use of the printer.
2. Use the Databases > Computer Equipment > Printers command to create a printer record, using the previously defined printer access. The selected type must be client.
3. Optional—Use the Databases > Computer Equipment > Workstations command to define the printer as the default workstation printer.

Connections to Forcefield node

A standard Centronics cable is used for parallel printers (i.e. a DB25 to Centronics connector). A standard Null modem cable is used for serial printers.

Figure 37: Forcefield node to printer connection details

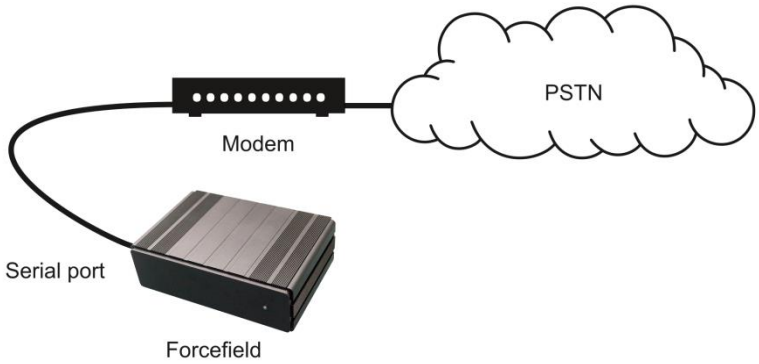


Setting up a technical support modem

To set up a modem:

1. Connect the modem to the Forcefield node via a serial cable (Figure 38 below).
2. Use the Databases > Computer Equipment > Ports command to create a port record for the technical support modem port. The type must be Technical Support.

Figure 38: Connecting a Technical Support modem to a Forcefield node



Programmable keyboards

Forcefield can use a programmable keyboard—or any other keyboard capable of generating the required keystrokes—to implement keyboard macro functionality.

Keyboard macros are Forcefield events named ‘Kbd Macro 1’, ‘Kbd Macro 2’, ‘Kbd Macro 3’, ... up to ‘Kbd Macro 120’ that are used to trigger actions, such as displaying a preset camera view on a monitor when a particular function button on the programmable keyboard is pressed.

Key sequence

All key sequences must start with ALT+, (press the ALT key and the comma key simultaneously), and end with ALT+. (press the ALT key and the full-stop key simultaneously).

After pressing ALT+, use up to three additional key sequences to define up to 120 keyboard macros, and then press ALT+. to end the programming.

- ALT+0 represents the value 0
- ALT+2 represents the value 2
- ALT+3 represents the value 3

  ...
- ALT+9 represents the value 9

For example, to program:

Kbd Macro 1—you must program your keyboard to generate the key sequence:

```
ALT+comma   ALT+1 ALT+ full-stop
```

Kbd Macro 20—you must program your keyboard to generate the key sequence:

```
ALT+comma   ALT+2 ALT+0 ALT+ full-stop
```

The keyboard must generate this sequence in less than 750 milliseconds for it to be recognised as a hot key and not just a sequence of keystrokes.

Raima License Agreement

This product was created using the powerful and fast Raima Database Manager.

RAIMA LICENSE AGREEMENT

*** *IMPORTANT* ***

READ CAREFULLY BEFORE YOU OPEN THE SEALED SOFTWARE MEDIA PACKAGE(S)

If you open the sealed software media package(s), you agree to the terms of this Raima License Agreement.

Raima Corporation will not sell you a license to use the software in the sealed software media package(s) at standard pricing terms unless you agree to all of the terms of this Agreement. If you do not accept the terms of this Agreement, promptly return the unopened software media package(s) and all accompanying materials to the place you obtained them. Raima does not accept contrary terms in Purchase or Sales Orders.

1. PARTIES TO THE LICENSE. This is a legal agreement between you (the “Development Entity” as defined below) and Raima Corporation.

2. SUBJECT MATTER OF THE LICENSE. This Agreement is a novation of all prior agreements and representations between Raima and you regarding all Raima Database Manager and Raima Object Manager software in your possession, including the contents of the sealed media package(s), earlier releases of the software, all accompanying written materials, and prior written agreements whether contained in manuals, sealed media package(s) or otherwise (hereafter referred to as “Products”).

3. LICENSE TO DEVELOP APPLICATION PROGRAM. Raima grants you a limited, perpetual, non-exclusive, nonassignable, nontransferable right to use the Products enclosed in the sealed software media package(s) in source code form (if supplied or in your possession) and object code form to develop one specific computer application program in compiled, linked, executable form (your “Application Program”), provided your Application Program that includes the Product does not constitute a database management system product, a database query product, a database revision product, or an object manager product, which could be used to commercially compete with any Raima Product.

4. LIMITED LICENSE. We base the price of this license, in part, on the operating system environment, hardware platform (including manufacturer, series and model), and maximum number of developers specified in our sales order (including our declarations forms, quotation or invoice). Any person who modifies any aspect (color, text, pixel, etc.) of any application that contains a Raima Product or who links, compiles, or edits code using a Raima Product is considered a “Developer”. The Products may be used only by the number of Developers, in the operating system environment(s) and on the hardware platform(s), specified in the sales order as accepted by Raima. You must purchase additional licenses from Raima for additional Developers, for each Application Program, and for different operating systems or hardware platforms, even from the same hardware manufacturer. You may use the Products only on the number of workstations (defined as the number of Developers) and only in the Application Program declared in the sales order.

5. LICENSE TO MODIFY SOURCE. You may modify and compile the Product source code, if licensed, provided you do not delete copyright notices. All modified versions are part of the licensed Products, subject to this Agreement and the property of Raima. You must deliver to Raima on written request copies of all modifications of, partial replacements of, and extensions to Raima source code. *Raima does not support modified source code.* If you compile the source code for use with an operating system or hardware platform other than as specified in the sales order, you must purchase another license from Raima for that operating system or hardware platform, including larger models of the same platform.

6. LICENSE TO DISTRIBUTE. Provided you conspicuously display the Raima copyright notice and use the Products only in conjunction with your Application Program, you may reproduce and distribute your Application Program royalty free. As part of your Application Program, you may distribute the executable utilities or executable programs within the Products, except ddlp, the Database Definition Language Processor. You may *not* distribute the Product source code unless a special license is purchased from Raima. You may *not* distribute the ddlp program, nor may you replace the ddlp program with another ddlp that creates database dictionaries for the Products, unless you purchase a special license from Raima. You may state in the documentation for your Application Program that you used the Products to create your Application Program. Your Application Program must use the target hardware platform specified in the sales order since Raima bases the pricing for this license, in part, on the CPU you specified.

7. OTHER RESTRICTIONS. These licenses are personal to you, the Development Entity, specified in the sales order. The Development Entity may be an individual or organization. It may be a division or subsidiary of a larger organization or the affiliate of a smaller organization. In any event, Raima grants this license only to the Development Entity named in the sales order and restricts it to the geographical location specified in the sales order. You must separately negotiate licenses for other locations with Raima. You may not use, distribute, or transfer the Products except as allowed by this license. You may not sell, assign, sublicense, lease, or otherwise transfer any part of this license. A sale of a majority of your Development Entity is deemed a transfer. You may not retain copies, even of prior versions of the Products, on termination of this license. Your obligations under this Agreement survive any substitution or termination of the licenses granted by this Agreement.

8. OWNERSHIP AND COPYRIGHT. Raima Corporation or its suppliers own the Product(s). National copyright laws and international treaty provisions protect them. The Products contain proprietary information. You must protect the Products like any other copyrighted material and keep the source code in strict confidence, ensuring that anyone with access to the Products refrains from unauthorized reproduction, use or disclosure. You may make a reasonable number of copies solely for working, backup, or archival purposes, provided you use only one working copy at a time for each licensed CPU. You may not copy in any form the written materials accompanying the Products.

9. INDEMNIFICATION. You agree to indemnify, hold harmless, and defend Raima from any claims, including attorneys' fees, that arise or result from the use or distribution of your Application Program, including any claim that your Application Program infringes the rights of third parties.

10. TERMS AND TERMINATION. After payment in full to Raima, you may terminate this license by returning or destroying all copies of the Product materials in your control and notifying Raima in writing. This license, including your right to use the Products, will terminate automatically if you infringe Raima copyrights or breach this Agreement. Raima may suspend or terminate this license, with 30 days prior notice and opportunity to cure, if you fail to pay any amount due Raima or any Raima distributor, dealer, or subsidiary, including Vista Development Corporation. Termination of your licenses does not impair third party rights in Application Programs already lawfully distributed, nor does termination affect your obligations under this Agreement.

11. LIMITED WARRANTY. Raima warrants that the Products have been accurately recorded on the media and that the media contains no defects. You may return any media which does not meet this warranty within 30 days from the date of shipment to the place where you obtained it, and Raima or its reseller will repair or replace it without charge. *Raima disclaims all other warranties, either expressed or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, and all other remedies for breach of the above warranty. You assume all risks with respect to accuracy, adequacy, quality, reliability, and performance of the Products. All implied warranties which may not be disclaimed are limited to 30 days. Some jurisdictions do not allow limitations on duration of implied warranties, so the above limitation may not apply to you. This limited warranty gives you specific legal rights. You may have other rights, different from the warranty given by Raima.*

12. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. *In no event will Raima, its resellers, or suppliers be liable for consequential damages (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the Products, whether in an action based on contract or tort, including negligence or strict liability, even if you advise Raima of the possibility of such damages. Raima's total liability under this Agreement is limited in the aggregate to amounts you paid for this Product and license.*

13. TECHNICAL SUPPORT. To keep this license in force, technical support, which includes updates (not upgrades to new versions), shall be purchased by the Development Entity annually, in advance, at a price equal to twenty percent of cumulative payments paid to Raima for all Products purchased under this Agreement.

14. U.S. GOVERNMENT RESTRICTED RIGHTS. Raima software and documentation are provided with restricted rights. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR 52.227-14(g)(3) and subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.
Contractor/manufacturer is Raima Corporation, 4800 Columbia Center, 701 Fifth Avenue, Seattle, WA 98104

15. SEVERABILITY. Whenever possible, each provision of this Agreement must be interpreted so as to be valid under applicable law. If any provision is invalid, the remaining provisions remain enforceable.

16. DISPUTES. The laws of the State of Washington, U.S.A., without regard to its conflicts of law rules, control this Agreement, and the United Nations Convention on the International Sale of Goods does not apply. It is enforceable by Raima or its distributors and dealers. Disputes will be finally resolved in arbitration, before one arbitrator, under American Arbitration Association Commercial Arbitration Rules and conducted in Seattle, Washington, U.S.A., or under the UNCITRAL Rules of Arbitration in Stockholm, Sweden, at Raima's option. If conducted in Sweden, the arbitration will be conducted in English, and administered by the Stockholm Chamber of Commerce. The prevailing party in any action related to an alleged infringement of Raima proprietary rights is entitled to recover its costs and expenses, including reasonable attorneys' fees. You consent to personal jurisdiction in the federal and state courts in the State of Washington, U.S.A. A prevailing party may enter judgment on an arbitral award in any court having jurisdiction. These provisions will survive the termination of this Agreement, regardless of the cause of termination.

021398

This product was created using the powerful and fast Raima Database Manager.

Appendix B
Upgrading from Ares

Summary

This appendix describes the typical upgrade paths for migrating from an existing Ares system to a Forcefield Enterprise system.

Content

Overview

The following items are not upgradeable:

- History database (backup any required history files before you upgrade)
- Network configuration file (includes netstart file)
- StartAres script (if system has been configured to use a second hard disk for history)
- Ares system configuration file (i.e. includes Watch House mode, login to graphics, etc.)
- Speed bar configuration
- Auto backup and purge configuration
- If you are using a Versa keyboard, it must be reprogrammed after the upgrade. Refer to “Programmable keyboards” on page 75.

Refer to the following sections for upgrade instructions:

- “Upgrading from Ares 4.5.x” below
- “Upgrading from Ares 4.4.1R” on page 82

Requirements

To set up Forcefield you need the following:

- Forcefield Installation CD or USB device
- Forcefield Licence CD or USB device

Upgrading from Ares 4.5.x

This section describes the process of upgrading an Ares 4.5.x system to Forcefield.

Some Ares 4.5.x systems are configured such that nodes communicate over a WAN. Communication between nodes over a WAN is not recommended due to network performance considerations.

Interlogix recommends that all nodes including the primary and backup servers be on the same network segment so there will be no effect on other general network performance. Consider replacing an Ares 4.5.x non-controlling node (on a LAN or WAN) with a Forcefield client on a Microsoft Windows computer.

Note: Interlogix recommends that only Forcefield hardware is used in a Forcefield system. Customers who choose to reuse Ares hardware may encounter unforseen installation procedures, and possible incompatibilities. Contact Technical Support for details.

Use this upgrade procedure only if you want to upgrade your existing Ares 4.5.x system to Forcefield and wish to retain your existing computer hardware. For best performance, Interlogix recommends that you also upgrade your hardware to Forcefield computer hardware.

In comparison with previous versions, the Forcefield installation process eliminates the need to separately install QNX TCP/IP Runtime, and to program QNX and Forcefield to use TCP/IP.

Before you begin

The upgrade process is not reversible: you cannot roll back to an earlier version. It is recommended that prior to upgrading, you use the Backup History command to backup the Ares history and the Backup Ares Data command to backup the database.

You will need to collect some information about each node (including the controlling node) before you start to upgrade an Ares system. Copy and use the “System-wide information record” on page 85 to assist you in collecting the required information. You will also need to record the following details for each node (if applicable):

- Service Offset (the term is ‘INFLEET Service’ in later versions of Ares).
- Infleet node numbers.
- From the QNX shell, enter netmap, and then record the physical address for the node (the physical address is the MAC address).
- From the QNX shell, enter sin –PNet. and then record the network driver (e.g. Net.rtl).

Note: If the network driver is anything other than Net.rtl, you will need to edit the driver name in the sysinit file.

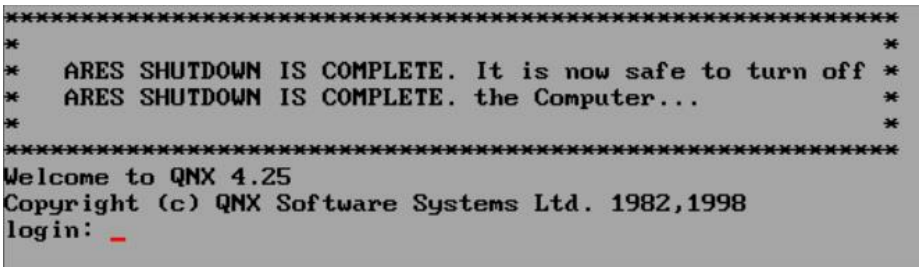
Upgrade process

If this is a multi-node Ares system, upgrade all the client nodes (steps 2 through 11) before you upgrade the controlling node.

To upgrade from Ares 4.5.x to Forcefield:

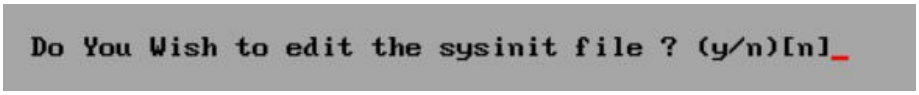
1. Collect the required information about each node on the “System-wide information record” on page 85.
2. If Ares is running, shut down by selecting Administration > ARES Shutdown.
3. Type your login code and press ENTER, and then type your password and press ENTER.

4. Confirm that you want to shutdown, and the QNX screen opens. Wait for a login prompt (see image below) and then go to step 5 below. If you see the // # > prompt instead, then you're already logged on to the QNX shell, so go to step 6.



5. Type root and press ENTER. You may also need to enter the root password if QNX is set up to need one. The default password is 4346.
6. Insert the installation CD and wait for the CD to start.
7. Type /cd0/usr/bin/UpdateARES/cd0 1 0 and press ENTER to install the Ares upgrade files. The string cd0 1 0 is used where the primary controlling node is node 1 and there is no backup controlling node. If there was a backup controlling node and it was node 20, the string would be cd0 1 20.

   Note: QNX is case-sensitive. There is a space between the capital letter S and the forward slash /. The '0' is a zero and not the capital letter 'O'.
8. Ares Upgrade displays a message:



9. Press **N**. Ares completes the upgrade and displays the QNX prompt.

   Note: If the network driver is not Net.rtl, then you must type y, and then press ENTER to open the sysinit file. For example, if the network driver is Net.ether82557, then you would need to change the line in section 5 of the sysinit file from "Net.rtl &" to "Net.ether82557 &".

Upgrading from Ares 4.4.1R

To upgrade from Ares 4.4.1R you must first upgrade to Ares 4.5.x before you can upgrade to Forcefield. Contact Technical Support for details.

Appendix C
Forcefield system information

Summary

This appendix provides worksheets to use when setting up a Forcefield server, Forcefield nodes (if applicable), and installing Forcefield clients.

Content

Collecting information prior to installing

When setting up a Forcefield server, Forcefield nodes (if applicable), and installing Forcefield clients you will need to record the following information about the system:

- System-wide information—you need to know the node number, role, and IP configuration details for each node. See “System-wide information record” on page 85.
- Node-specific information—for each node you need to know the control port and transfer port numbers. See “Node-specific information record” on page 86.
- Client-specific information—for each client you need to know the station key that has been assigned to each workstation. See “Details of node’s clients” on page 86.

Add these details to the following pages.

The roles of Forcefield nodes are indicated by a letter. Roles can be:

- **P** = Primary controlling node
- **B** = Backup controlling node
- **N** = Non-controlling node

System-wide information record

The primary controlling node is 1, and the offsite redundancy site (if used) is also node 1. Non-controlling nodes can be 2 through 20 (8 for standard edition and 20 for Enterprise edition).

Use Table 3 below to record the details for the nodes 1 to 8. If needed, use Table 4 below to record the details for the additional nodes 9 to 20 permitted by Enterprise edition.

Table 3: Node 1 to 8 information for either standard or Enterprise editions

Node	Role	Default IP address	Assigned IP address	Gateway address	Netmask
1	P	192.168.0.1			
2	N	192.168.0.2			
3	N	192.168.0.3			
4	N	192.168.0.4			
5	N	192.168.0.5			
6	N	192.168.0.6			
7	N	192.168.0.7			
8	N	192.168.0.8			

Table 4: Node 9 to 20 information for Enterprise edition only

Node	Role	Default IP address	Assigned IP address	Gateway address	Netmask
9	N	192.168.0.9			
10	N	192.168.0.10			
11	N	192.168.0.11			
12	N	192.168.0.12			
13	N	192.168.0.13			
14	N	192.168.0.14			
15	N	192.168.0.15			
16	N	192.168.0.16			
17	N	192.168.0.17			
18	N	192.168.0.18			
19	N	192.168.0.19			
20	N	192.168.0.20			

Node-specific information record

Each node, except for the optional backup controlling node, can have up to five clients (standard edition) or 20 clients (Enterprise edition). Copy this page for each node that has clients.

Details of node

Refer to “System-wide information record” on page 85 for the node’s assigned IP address, gateway address, and netmask. Record the control port and transfer port numbers.

Table 5: Connection details common to all of the node’s clients

Node no.	Assigned IP address	Control Port	Transfer Port	Video Base Port
				Do not change

Details of node’s clients

Record the station key, and optionally the workstation name, for each of the node’s clients.

Table 6: Connection details specific to each node

Client	Station key	Workstation name (reference only)
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

Client	Station key	Workstation name (reference only)
15		
16		
17		
18		
19		
20		

Appendix D
Troubleshooting

Summary

This appendix contains help for problems that installers may face.

Content

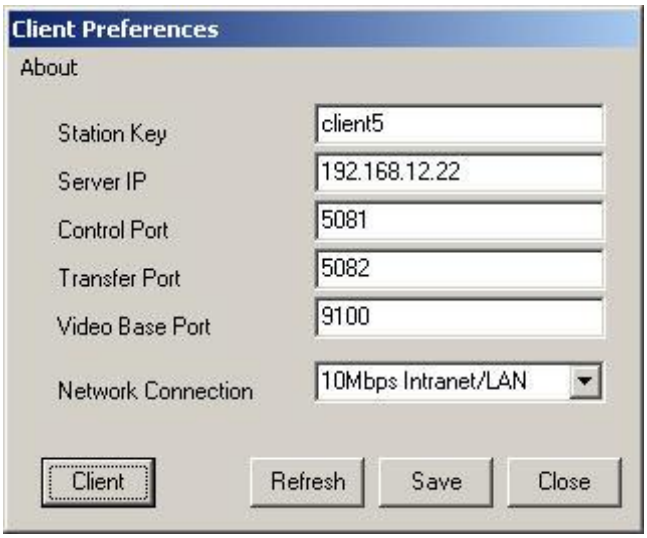
Troubleshooting client connections

The Forcefield client will not be able to connect with the server if the server's IP address is recorded incorrectly in the Preferences window.

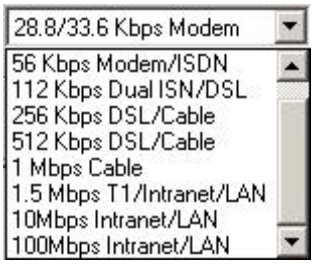
Figure 39: Connection error message

To edit the client preferences:

1. Go to Start > All Programs > Tecom > Forcefield > Preferences to edit the settings selected during installation.



2. Select a network connection speed to suit the type of connection.



Note: If cursor action does not match movements of the mouse, try a slower connection speed.

Troubleshooting servers

When offsite redundancy (data mirroring) is used the Forcefield title bar is colour-coded to indicate various conditions on the primary and mirror servers.

Note: The colours are configurable by the Forcefield system administrator and may be different from the ones indicated below.

The default colours of the primary server's title bar indicate the following:

- Grey—normal operation
- Pink—the mirror server is not running
- Orange—mirror server data transfer fail
- Yellow—mirror server history transfer fail

The default colours of the mirror server's title bar indicate the following:

- Light blue—normal operation
- Light purple—the mirror server has taken over as the primary controlling node
- Pink—mirroring has failed (prior to takeover)