ADPRO Video Central Platinum

Setup and Configuration Manual

March 2022
Doc. 19116_22
Software version 3.06

Honeywell

Disclaimer

The contents of this document are provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label. This document is subject to copyright owned by Xtralis. You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify, or publish any contents of this document without the express prior written consent of Xtralis.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Xtralis. All proper health and safety precautions must be taken during the installation, commissioning, and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Xtralis is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Xtralis accredited training course can install, test and maintain the system.

Liability

You agree to install, configure, and use the products strictly in accordance with the User Manual and product documents available from Xtralis.

Xtralis is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits, or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation, or advice given by or on behalf of Xtralis or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Xtralis in relation to the products is limited to:
(i) in the case of services, the cost of having the services supplied again; or
(ii) in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Xtralis harmless for any claim, cost, demand, or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

Trade Name Statement

ADPRO, Xchange, FastTrace, iFT, eFT, iFT-E, iFT Gateway, IntrusionTrace, LoiterTrace, XO, iTrace, iCommand, iCommission, iPIR, and FMST are trademarks and/or registered trademarks of Honeywell and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Your use of this document does not constitute or create a licence or any other right to use the name and/or trademark and/or label.

Document Conventions

The following typographic conventions are used in this document.

Convention	Description
Bold	Used to denote: emphasis Used for names of menus, menu options, toolbar buttons
Italics	Used to denote: references to other parts of this document or other documents. Used for the result of an action

The following icons are used in this document.

Icon	Description
	Note. This icon indicates information of special interest that will help the reader make full use of the product, optimise performance, etc. Failure to read the note will not result in physical harm to the reader, or damage to equipment or data.
	Caution! This icon indicates danger to equipment. The danger can be loss of data, physical damage to the equipment, or permanent corruption of configuration details.
	Warning! This icon indicates danger of physical harm to the reader. Not following instructions may lead to death or permanent injury.
	Warning! This icon indicates danger of electric shock. This may lead to death or permanent injury.
	Warning! This icon indicates that there is a danger of inhaling dangerous substances. This may lead to death or permanent injury.

https://www.security.honeywell.com

Contents

1 What's New 8

2 Setup and Configuration 13

2.1 Start and Login for Single User 13
2.2 Start and Login for Multi User 13
2.3 Login as User 14
2.3.1 Initial Login 14
2.3.2 Changing the Password 14
2.4 HeiTel Setup 15
2.4.1 Setup of CamControl Server 15
2.4.2 Opening the HeiTel CamControl Server 16
2.4.3 Opening the HeiTel VS-Videochannel 17
2.4.4 HeiTel Unit Programming 18
2.4.5 HeiTel Operational Limitations 22
2.4.6 HeiTel or VCP Features not Supported by Video Central Platinum when HeiTel Units are in Use 22
2.5 Licensing 23
2.5.1 Unlicensed Video Central Platinum 23
2.5.2 Licensing via Hardware Dongle 23
2.5.3 Licensing via Software Key 23
2.5.4 HeiTel CamControl Server Licensing 24
2.6 Adding or Editing Sites 24
2.6.1 Adding New Sites 24
2.6.1.1 Transmitter Details 24
2.6.1.2 Events Details 28
2.6.1.3 SitePulse Details 35
2.6.1.4 Notification Details 36
2.6.1.5 Owner Details 38
2.6.1.6 Location Details 41
2.6.1.7 Site Images 41
2.6.1.8 Diagrams 42
2.6.1.9 Fire Contacts 43
2.6.1.10 Quick Access Buttons 44
2.6.2 Adding New HeiTel Sites 47
2.6.3 Editing Site Details 47
2.6.4 System Monitor Message Configuration 48
2.7 Suspending, Restoring and Deleting Sites 49
2.7.1 Suspending a Site 49
2.7.2 Restoring a Site 50
2.7.3 Deleting a Site 50
2.8 Users Groups and Graphs 50
2.8.1 Adding and Editing Users 50
2.8.1.1 Adding Users 50
2.8.1.2 Editing User Details 53
2.8.1.3 Suspending Users 53
2.8.1.4 Restoring Users 54
2.8.2 Adding or Editing Groups 54
2.8.2.1 Adding New Groups 54
2.8.2.2 Editing Group Details 57
2.8.2.3 Deleting Groups 57
2.9 Displaying Graphs 58
2.10 Comments 58
2.10.1 Adding Pre-defined Comments 59
2.10.2 Deleting Comments 59

2.10.3 Adding Quick Access Buttons (QAB) 59
2.11 General Options 63
2.11.1 Mandatory Site Acknowledgement 63
2.11.2 Resource Monitor 64
2.11.3 Alarm Server Port 64
2.11.4 Event Type Hiding 64
2.11.5 ASL Site Priority 65
2.11.6 Site Description 65
2.11.7 GPS Settings 65
2.11.8 Import Conflict Action 65
2.12 User Interface Options 65
2.12.1 Event Notifications 66
2.12.1.1 Description of Event Notification Options 66
2.12.1.2 Examples 67
2.12.1.3 Alarm Notification Volume 69
2.12.2 Event History 70
2.12.3 Bounding Box Setup 70
2.12.3.1 Alarm Images 70
2.12.3.2 Live / Review 71
2.12.4 Remote Control 71
2.12.5 Language Setup 71
2.12.6 Quad Alarm Configuration 72
2.12.7 Joystick Settings 72
2.12.8 Enabling Auto Maximise on Event 73
2.12.9 Global Maps Auto Start 73
2.12.10 Column Visibility 74
2.12.11 Active Sites List Options 74
2.13 Local Audio Setup (Play audio file to site) 75
2.14 ADPRO XO Device Setup Options 75
2.14.1 Ethernet / PPP 75
2.14.2 Alarm Transmission 76
2.14.3 Alarm Profile 76
2.14.4 Input/Output Behaviour 76
2.14.5 Quad Image Interval 77
2.14.6 ADPRO XO Device Audio Setting 77
2.15 Central Monitoring Station Integration 77
2.15.1 Basic Integration 77
2.15.1.1 Overview of Basic Integration 77
2.15.1.2 Unknown Alarm Events 78
2.15.1.3 Communication with the CMSC 78
2.15.1.4 Heartbeat 78
2.15.2 Setup of Basic Integration 79
2.15.2.1 Modifying the Translation Table 80
2.15.3 VCP UI Controller 81
2.15.3.1 Introduction 81
2.15.3.2 Using VCP Controllers 82
2.15.3.3 Enabling the VCP UI Controller 83
2.15.3.4 The VCPUIController Syntax 83
2.15.3.5 VCP UI Controller Settings 84
2.15.3.6 Testing the VCP UI Controller 84
2.15.3.7 Usage 84
2.16 VCP Configuration Files and Folders 85
2.17 Report Manager 86
2.17.1 Accessing Reports 86
2.17.1.1 Accessing Report Manager via Video Central Platinum 86
2.17.1.2 Direct Access via Internet Explorer Web Browser 86
2.17.1.3 Hidden Reports 86

2.17.2 Configuring the Windows Firewall 88
2.17.2.1 Opening Inbound Port 80 88
2.17.3 Adding Users for Reporting 91
2.18 Creating a new Report Based on an Existing Report 96
2.18.1 Changing Report Parameters 98
2.18.1.1 Text and Background Colour 101
2.18.2 Changing the Report Banner 102
2.19 Task Scheduling 102
2.19.1 Archiving Task Schedule 103
2.19.2 Reporting Task Schedule 105
2.19.2.1 Integrated Reporting 107
2.20 Private Wall Setup and Configuration 107
2.20.1 Create a Default Guard Tour 108
2.20.1.1 Default Guard Tour with One Screen 109
2.20.1.2 Default Guard Tour with Multiple Screens 112
2.20.2 Create a Guard Tour with Multiple Screens 113
2.20.2.1 Edit a Guard Tour Screen 114
2.20.2.2 Set the Screen Split 115
2.20.2.3 Set the Screen Delay 115
2.20.2.4 Set the Camera for Each Screen Cameo 116
2.20.2.5 Complete Editing the Guard Tour Screen 116
2.20.2.6 Remove Screens 117
2.20.3 Edit an Existing Guard Tour 118
2.20.3.1 Create a New Screen 119
2.20.3.2 Edit Screens 119
2.20.3.3 Remove Screens 119
2.20.4 Remove a Guard Tour 119
2.20.5 Complete a full Guard Tour Wizard Loop to Save Changes 120
2.20.6 Video Performance 121
2.20.7 Protection Mode 121
2.20.8 Guard Tour Guidelines 122
2.21 Diagrams 122
2.21.1 Creating and Editing Diagrams 122
2.21.1.1 Background Element 123
2.21.1.2 Interactive Elements 124
2.21.2 Interactive Diagram Browser 125
2.21.2.1 Camera 125
2.21.2.2 Fire Detector 126
2.21.2.3 PIR Detector 128
2.21.2.4 HotSpot 129
2.21.2.5 Input 129
2.21.2.6 Output 130
2.21.2.7 Button 131
2.21.3 Creating and Editing User Routines 131
2.21.4 User Interface Control Commands 132
2.21.4.1 Command Syntax 133
2.21.4.2 Basic Commands 135
2.21.4.3 Advanced Commands 136
2.21.4.4 Variables 137
2.21.4.5 Parameter Variables 137
2.21.4.6 Expressions 138
2.21.4.7 Conditional Blocks 139
2.21.4.8 Modes of Operation 140
2.21.4.9 Error Handling 140
2.21.4.10 System Symbols 142
2.21.4.11 Macro Example 143
2.22 Global Maps 146

2.22.1 Settings 147
2.22.2 Advanced Settings 148
2.23 Scenarios 149
2.23.1 Add a Site to the VCP Database 149
2.23.2 Suspend a Site 150
2.23.3 Restore a Site 151
2.23.4 Delete a Site and its Events 152
2.23.5 Add User 154
2.23.6 Suspend User 156

1 What's New

Feature	Description	Section Reference
New in 3.02.09		
Extended Operator Audit	Additional operator audit data was added.	Operational Manual, 2.28.7.2, Audit Log Descriptions
32 camera support	32 cameras are now supported.	NA
Fisheye Camera support	Fisheye cameras can be viewed in VCP.	Operational Manual, 2.22.12, Viewing a Fisheye (360°) Camera
New in 3.04		
Support for HeiTel in Diagrams	Diagrams now support HeiTel devices.	Setup and Configuration Manual, 2.22, Diagrams
Private Wall HeiTel support	The private wall now allows to show video from HeiTel devices.	Setup and Configuration Manual, 2.4.4, HeiTel Unit Programming
HeiTel GPS support	VCP supports tracking HeiTel GPS devices by using the Global Maps application.	Setup and Configuration Manual, 2.11.7, GPS Settings, 2.12.10, Global Maps Auto Start Operational Manual, 2.46, Global Maps
Live Video Snapshot support for HeiTel	It is now possible to take live video snapshots when streaming video from HeiTel devices.	Operational Manual, 2.22.10, Saving a Live Image
Talk-to-Site Audio File support for HeiTel	Audio files (mp3 and wav) can be configured for Talk-to-Site with HeiTel devices.	Setup and Configuration Manual, 2.13, Local Audio Setup (Play audio file to site)
HeiTel HTConnect support	VCP HeiTel sites can be configured to use HTConnect to connect to the associated devices.	Setup and Configuration Manual, 2.4.1, Setup of CamControl Server, 2.4.4, HeiTel Unit Programming
Bounding Box Configuration	The type of bounding boxes that are shown for alarm images (quad images) and live and review video can be selected.	Setup and Configuration Manual, 2.12.3, Bounding Box Setup
Event Monitoring	It is now possible to monitor events for occurrence, i.e. to check whether a given event has occurred within an expected timeframe.	Setup and Configuration Manual, 2.6.1.2.7, Event Monitoring Settings
Enhanced Database and Disk Size Warnings	Database and disk size warnings have been improved. Warnings will be repeated periodically if the issue at hand is not dealt with. If the issue becomes critical, the system monitor site cannot be cleared until the issue has been dealt with.	Database and Maintenance Manual, 2.1.4, Hard Drive Warnings, 2.1.5, Database Warnings
ASL Customisation	ASL column locations can now be changed. It is now possible to select which ASL columns are visible.	Setup and Configuration Manual, 2.12.11, Column Visibility
Time on ASL	The time how long a site is sitting on the ASL is displayed in a new ASL column "Accumulated Time".	Operational Manual, 2.16.1, ASL Explanation

Feature	Description	Section Reference
Additional Reports	Additional reports are available: • "User Response Report 2", for viewing average response time. • "User Response By Event", shows individual alarms and associated details. • "User Response By Event Type", shows alarms and associated details per sensor. • "User Response By Transmitter", shows alarms and associated details per transmitter. • "Isolations By Sensor", shows isolations and associated details per sensor. • "User Response By User", shows alarms and associated details per user. "User Response Key Metrics", shows user response key metrics.	Operational Manual, 2.45, Reports
New Export/Import of VCP Server Configuration	A new export/import mechanism allows to export/import VCP Server configuration (site details, user details, event priorities…) to/from an XML file. In order to prevent unexpected overwriting of data during import, an import rule can be set which defines how configuration data should be imported. A task is added to the Task Scheduler to allow for automated and scheduled export of the server configuration. A tool exists to convert the VCP legacy export files to the new XML format.	Setup and Configuration Manual, 2.11.8, Import Conflict Action Database and Maintenance Manual, 2.1.18, Exporting and Importing Site and User Data
System Monitor Message Selection	Now System Monitor messages can be enabled or disabled. The System Monitor site will not appear on the ASL for disabled messages.	Setup and Configuration Manual, 2.6.5, System Monitor Message Configuration
Troubleshooting FAQ for Setup	In case VCP setup fails, a troubleshooting FAQ is displayed.	NA
Language Selection in Active Language	The list of languages is now displayed in the language that is active.	Setup and Configuration Manual, 2.12.6, Language Setup
Event Comment enhancement	When adding comment on an event, the Event Comment dialog now contains some information which summarises the event at hand.	Operational Manual, 2.27, Entering Comments
Diagram Guard Tour enhancement	Additional diagram commands are added to allow to switch to the next or previous guard tour sequence: Video(MULTI,NEXTSEQUENCE) Video(MULTI,PREVIOUSSEQUENCE)	Setup and Configuration Manual, 2.22.4.1.1, Live Video Control
Enhanced Review on 20+ Channels	When reviewing more than 20 channels, the user can now switch between the first 20 cameras (cam 1–20) and last 12 cameras (cam 21–32).	Operational Manual, 2.43.9.3, Reviewing More than 20 Cameras
VCP Server autostart upon crash	It is now possible to configure VCP Server to automatically restart after the program has crashed.	Setup and Configuration Manual, 2.2, Start and Login for Multi User

Feature	Description	Section Reference
Guard Tour enhancement	The “All Cameras” guard tour option automatically selects the best camera layout for displaying all cameras on the device.	Operational Manual, 2.23, Conducting a Guard Tour
Enhanced PTZ Configuration	An option is added to allow to invert the Y-axis when controlling PTZ via a joystick. An option is added to show an indication of the centre of the screen when using PTZ.	Setup and Configuration Manual, 2.12.8, Joystick Settings
Support for new XO events	Added support for XO PIR events. Added support for “STORAGE INSUFFICIENT” event.	NA
Diagrams Workbits support	Diagrams now support XO device workbits.	Setup and Configuration Manual, 2.22, Diagrams
VCP SecureViewer Fisheye Cam enhancement	The VCP SecureViewer now supports dewarping exported fisheye camera video.	Secure Viewer User Manual, 4.3.16, Viewing a Fisheye (360°) Camera
Basic Integration enhancement	Basic Integration now supports sending event deactivation codes.	Setup and Configuration Manual, 2.15.2.1, Modifying the Translation Table
Enhanced Performance	Overall enhanced performance by database optimisation and caching.	NA
New in 3.05		
Additional Language	Added Polish translation.	NA
Archiving	Improved error notification in case archiving fails due to insufficient disk space.	NA
Configurable alarm images location.	Added support for setting the path to the EventExtraData folder in the SystemData table.	2.16 VCP Configuration Files and Folders
Configurable SQL Server edition and instance name.	It is now possible to select a pre-installed SQL database instance when installing VCP. Supported instances are SQL 2008 R2, SQL 2014, SQL 2016, and SQL 2017. The user is not forced to use “XTRALIS_CYCLOPS” as the name of the SQL Server instance.	VCP Installation Manual
Configuration files relocated	VCP related configuration files have been moved to the “ADPRO VCP” folder under the common application data folder. E.g. “C:\ProgramData\ADPRO VCP”. The configuration files include vcp_bi.ini, VCPClientConfig.xml, VCPAppLauncherConfig.xml, ADPROSW.config and GPSMapsSettings.xml.	2.16 VCP Configuration Files and Folders
Consolidated configuration file location	Temporary, backup and log files are moved to subfolders under the Common \ “ADPRO VCP” folder.	2.16 VCP Configuration Files and Folders
Convert export busy indication.	Tool now shows wait cursor while conversion is busy.	NA

Feature	Description	Section Reference
Enhanced Camera I/O	The camera I/O status page has been redesigned, allowing to isolate individual camera points.	Operational Manual 2.19.3 Camera I/O
Enhanced event search	Added a column to the Event Search dialog, showing the cameras associated with the event. Added a new search option in the Event Search dialog, to search for events linked with a specific camera.	VCP Operational Manual 2.42.1.3 EventSearch Results – Event tab
Enhanced IP configuration	Improved the appearance of the IP Configuration window that is displayed if the VCP UI is launched with a misconfigured bind-to-IP address.	NA
Event Detail	For the SITE CONNECT, SITE SELECT, SITE RELEASE, SITE DISCONNECT and SITE ACKNOWLEDGEMENT events, the Events list now contains the user name in the Detector Text column.	VCP Operational Manual 2.32
Event Search	In the VCP Event Viewer, which is launched via Event Search, the Next or Previous button used for cycling through alarm images, is disabled if there are no subsequent images to show.	NA
NetIO digital tamper event.	Added support for the new NetIO digital tamper events that are available on XO 4.2.	NA
New Bind To network settings	Added ability to configure .NET remoting client socket (bind-to-address and client port) for VCP Video Wall, Global Maps application, and the ADPRO Media Server. This provides the ability to better finetune these applications to the needs of an environment where network communication is more restricted.	NA
iRespond feature removed.	Removed iRespond functionality from setup and menues.	NA
VCP Feedback tool removed.	Removed the VCP feedback tool from setup and menues.	NA
Secure Viewer	Added extra diagnostic logging to the Secure Viewer Extractor post-extract processing.	NA
Separated SQL instance installation.	Installation of the SQL Server instance, that is required for installing the VCP related databases, has been separated from the VCP setup. The VCP setup no longer integrates installation of SQL server into the VCP setup process. The wizard still does provide a link on the prerequisites page, which allows to run the setup for SQL Server 2014 Express with Advanced Services. SQL Server setup then runs with default configuration settings.	VCP Installation Manual

Feature	Description	Section Reference
Simplified Bounding-Box Configuration	To avoid confusion with the colour of bounding boxes, colour configuration for quad alarm bounding has been removed.	2.12.13.1 Alarm Images
Site Overview	The Site Armed/Disarmed status on the Site Overview page is now updated on the fly, upon receiving a “SYSTEM ARMED” event from the unit. Prerequisite for this to work properly, is to use an alarm profile where the “End of alarm tx” checkbox is ticked, on the unit. If required, the “SYSTEM ARMED” event can be hidden from the ASL, using Sensor Monitoring.	VCP Operational Manual 2.2.1
Support for Windows 10 64 bit, Windows Server 2012 Windows Server 2016 operating systems	VCP can run user interfaces and servers on these operating systems.	NA
Updated default database - SQL Server 2014 Express	VCP setup now comes with SQL Server 2014 Express with Advanced Services. On the setup wizard’s prerequisites page, the setup provides the ability to install SQL Server 2014 Express with Advanced Services, if the user did not select a valid existing SQL Server instance. **Note**: VCP is qualified up to SQL Server 2016 Express.	VCP Installation Manual
Video Wall network configuration	VCP Video Wall can now be configured not to require a ping reply from VCP Server before it attempts to connect to the Server. By default, the Video Wall does not connect to the Server if it doesn’t receive a ping reply.	VCP Video Wall Manual 9.2
New in 3.06		
P2P support	The option to enable P2P instead of the IP connection. The IP Address and Host Name fields disappear if this option is selected and P2P License ID field appears. Enter the license key with 20 alphanumeric characters.	Setup and Configuration Manual 2.6.1.1
Support for secure streaming	Select this checkbox to enable encrypted video streaming.	Setup and Configuration Manual 2.6.1.1
Upgrade to SQL Server 2019	VCP installs SQL Server 2019 Express and SQL Report Server 2019 Express (SQL Server Reporting Services-SSRS) for 64-bit operating systems (if there is no previous SQL Server installation). Install the Reporting Server only after installing the SQL Server. There is no change in the installation procedure for 32-bit operating systems, and VCP will install SQL Server 2014 in this case (for backward compatibility).	NA

Note: Wherever **ADPRO device** or **ADPRO XO device** is mentioned in this document, it applies to the FastTrace 2 Series devices, iFT Series devices, and eFT Series devices unless specifically mentioned otherwise.

2 Setup and Configuration

2.1 Start and Login for Single User

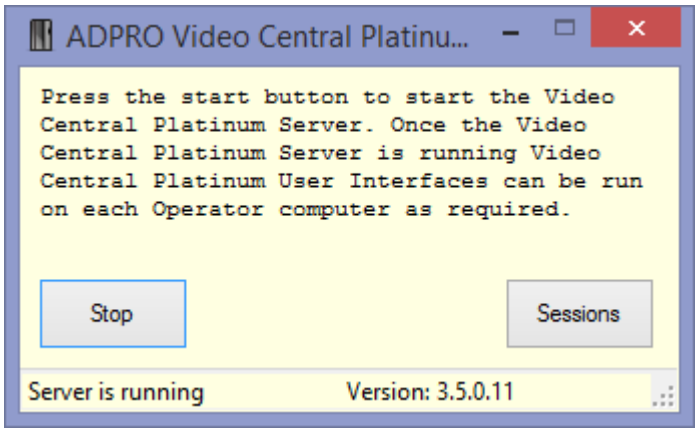
In a single user installation, start the Server and User Interface together by either clicking the **Video Central Platinum** icon  on the Desktop or accessing Start > Programs > Xtralis > Video Central Platinum > Video Central Platinum. After a short pause the Server and User Interface will start and the ADPRO Video Central Platinum Server application will be displayed. Do not click the **Stop** button on the Server. The Server maybe minimized during operation.

After a short delay the User Interface will display the Active Sites List and the system is ready for User Login.

2.2 Start and Login for Multi User

As a multi user installation, the Video Central Platinum Server and User Interface will start automatically when the PC is started. The User Interface dialog will be displayed ready for User Login once the Server has completed its start process and connected to the User Interface(s).

If the Server or User Interface has been manually stopped or closed they will need to be re-started manually. If stopped the server can be started by clicking the **Start** button on the Server application. Double click the desktop icons to start the Video Central Platinum Server  then the User Interface  or alternatively use the Windows Start Menu.



This screen will remain active whilst the Server is running but may be minimized.

Note: there is an option to have the VCP Server restart automatically in case the program crashes. To enable the option, set the following value in the VCPServerConfig.xml file:

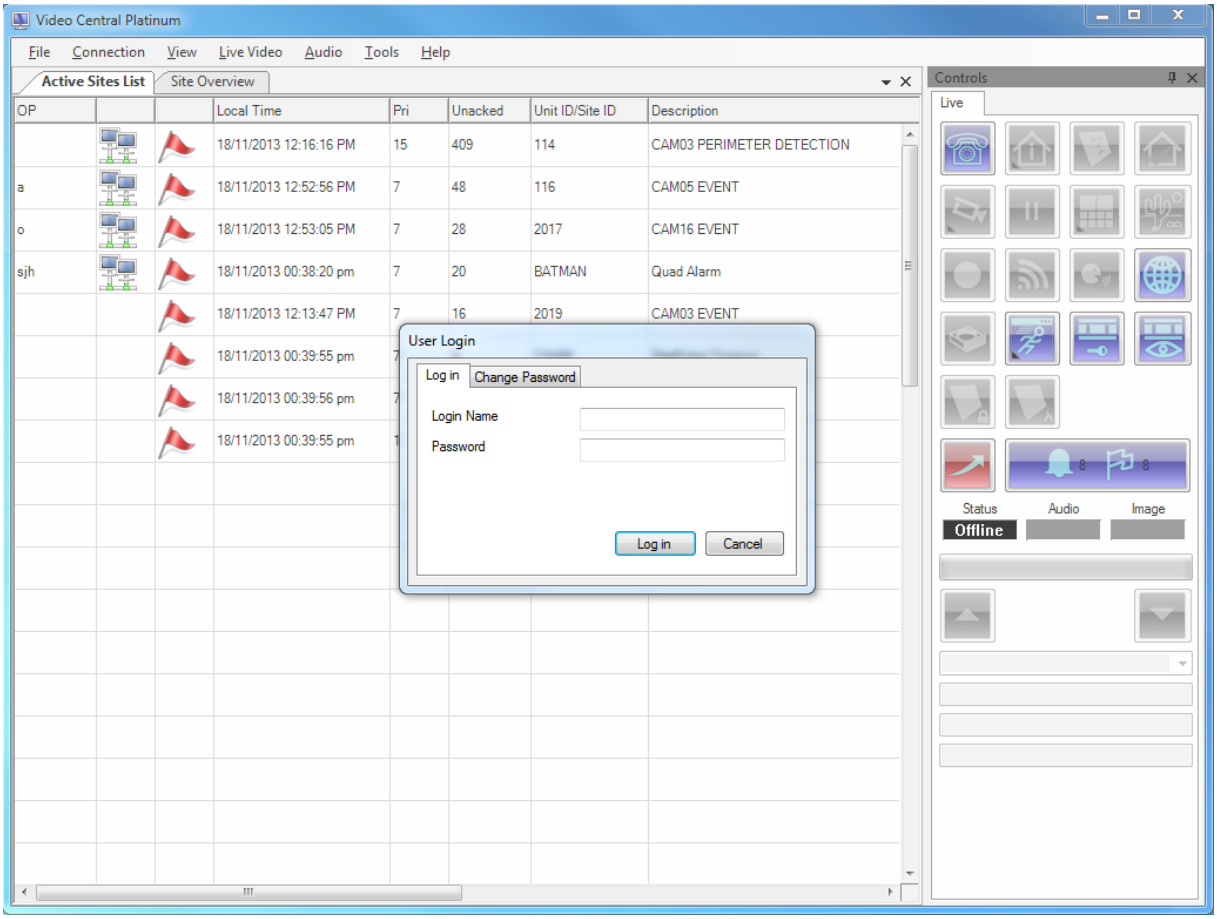
<Configuration>
<RestartOnCrash>YES</RestartOnCrash>
</Configuration>

If the <RestartOnCrash> element is omitted, or if set to NO, the VCP Server program will not automatically restart after it has crashed.

The VCPServerConfig.xml is located in the folder where the database is installed. The default folder is: C:\VCP\VCPDataRoot

2.3 Login as User

Login for Single and Multi User facilities begins at the User Interface dialog.



Click anywhere on the User Interface and the User Login dialog will be displayed.

2.3.1 Initial Login

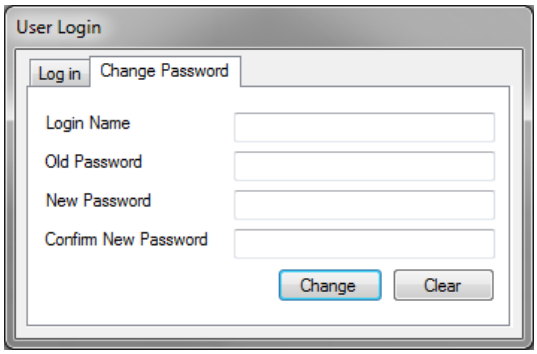
For initial login enter the following defaults in lower case:

Login Name: admin

Password: password

2.3.2 Changing the Password

To change the password after entering defaults, select the Change Password tab.



Re-enter the Login Name and the Old (default) Password.

Now enter a New Password, which may be alphanumeric and is case sensitive.

Confirm the New Password then click **Change** to complete the process.

You may also change the password at any stage by accessing Tools > Change Password.

2.4 HeiTel Setup

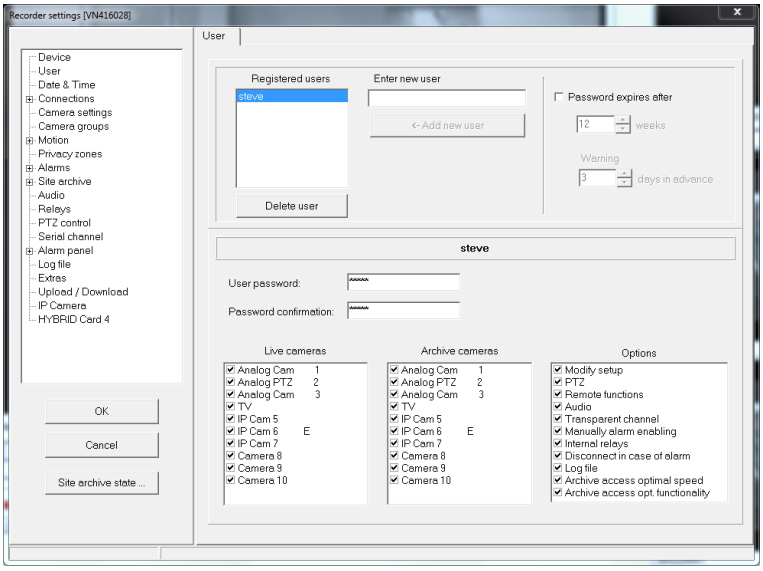
The Video Central Platinum (VCP) installation process installs the necessary HeiTel CamControl Server components on the Video Central Platinum (VCP) Server PC. All connections to HeiTel transmitters from VCP User Interfaces are made transparently through the CamControl Server which is running on the VCP Server PC in the background.

When the VCP Server is run the HeiTel components will be automatically started and use control port 5500, audio port 8100 and video ports 8010 to 8020 by default.

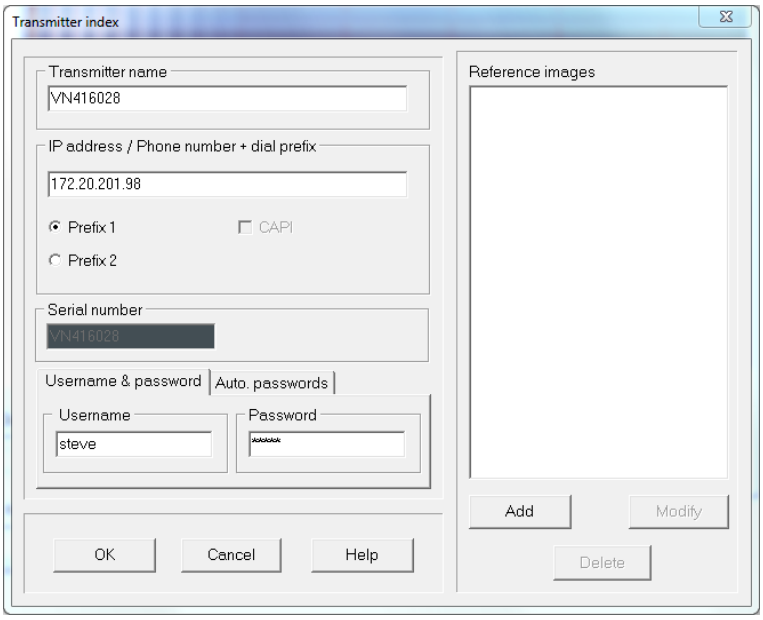
If connections to HeiTel transmitters were previously working, and have now stopped working, check both the CamControl Server and VS-Videochannel have not been manually closed. If either have been closed, stop and close the VCP Server then re-start the VCP Server.

2.4.1 Setup of CamControl Server

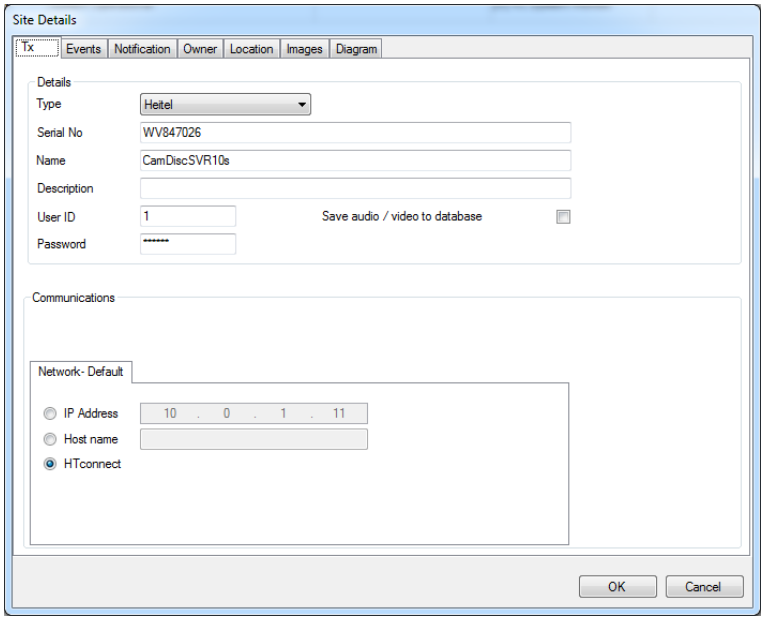
By default there is no setup required of the CamControl Server. However when users have been programmed in the HeiTel unit as shown below and alarms are monitored by Video Central Platinum, the HeiTel site must be added to the CamControl Server as well as Video Central Platinum Site Details.



Site programmed in the CamControl Server with username and password.



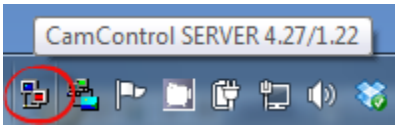
Site Programmed in VCP Site Details programming with user ID (username) and password. You can connect to the unit by IP address, by hostname, or by HTconnect.



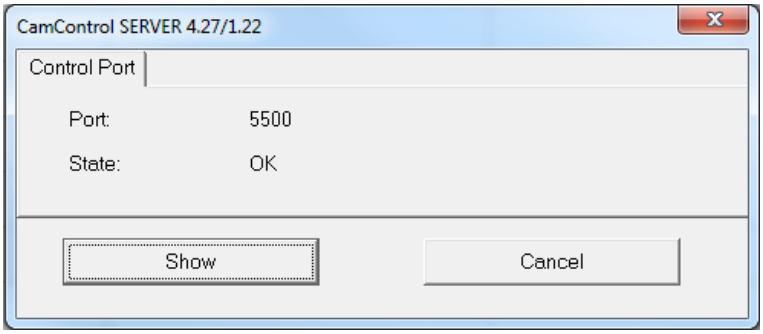
The CamControl Server or HeiTel Client are required to configure the HeiTel transmitters initially. See HeiTel manuals for further detail.

2.4.2 Opening the HeiTel CamControl Server

From the Windows task bar left click on the CamControl Server icon to open.

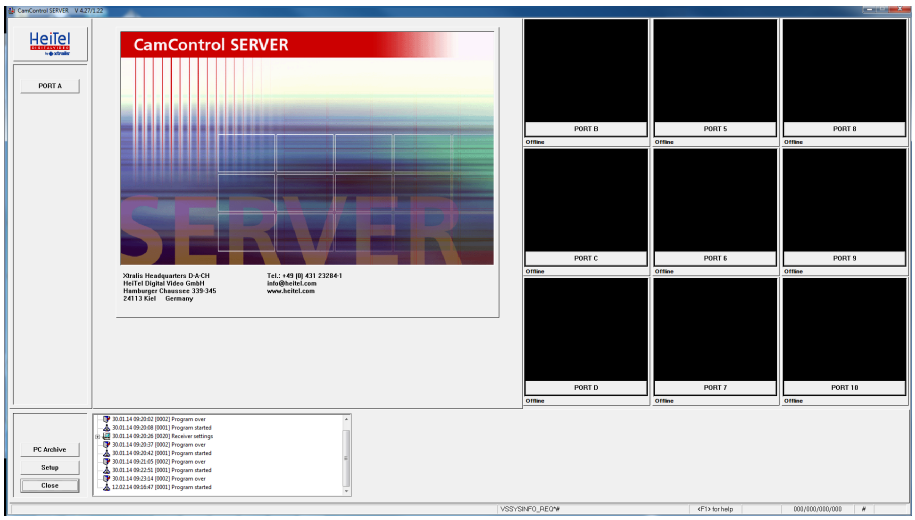


The CamControl Server dialog will be displayed.



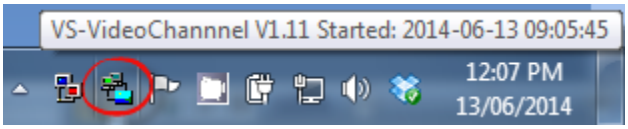
Select the Show button to display the CamControl Server application. The CamControl Server application can be used to connect to HeiTel transmitters for initial setup. See HeiTel manuals for further detail.

When finished ensure the minimize button is selected and **DO NOT** close the dialog with '**X**'.



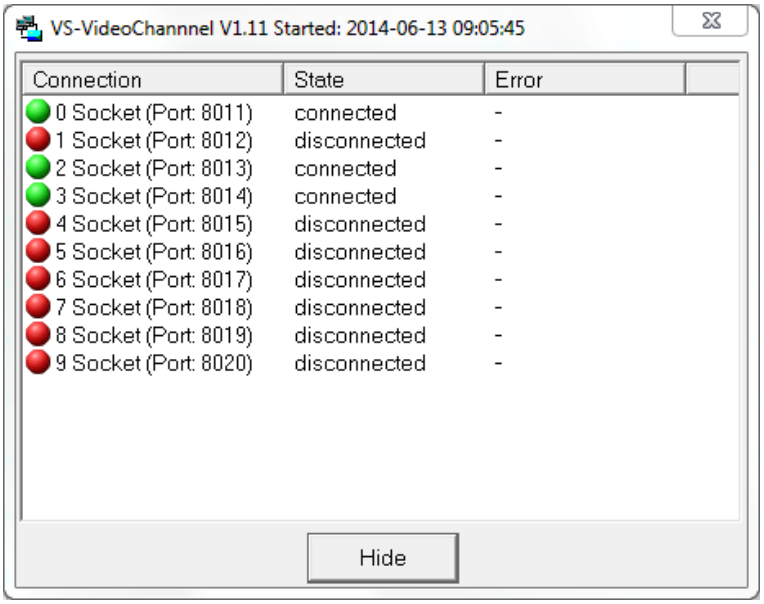
2.4.3 Opening the HeiTel VS-Videochannel

From the Windows task bar right click on the VS-Videochannel icon then select ‘Show VS-Videochannel‘ to open.



The VS-Videochannel dialog shows the connection status of the video streams from HeiTel transmitters. See HeiTel manuals for further detail.

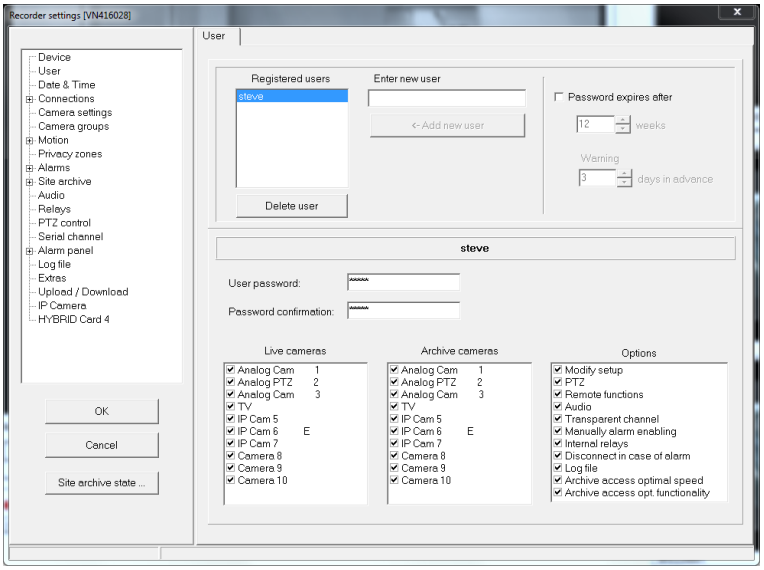
When finished ensure the hide button is selected and **DO NOT** close the dialog with ‘**X**’.



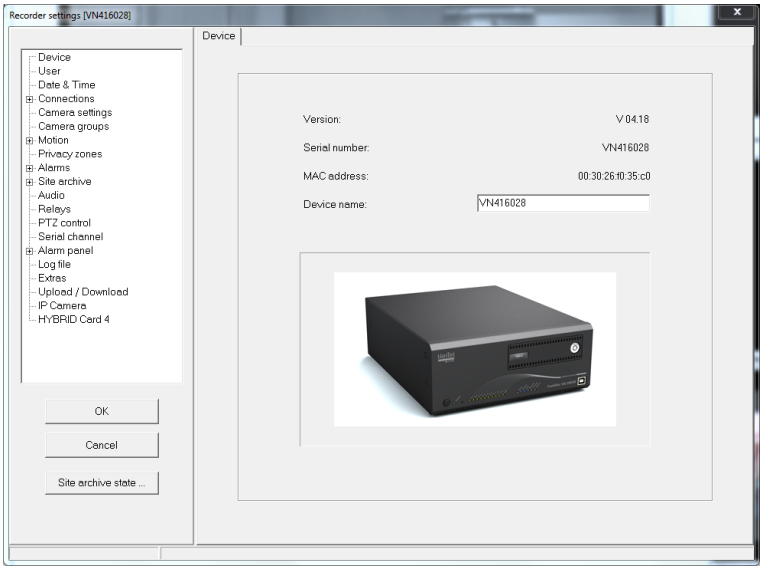
2.4.4 HeiTel Unit Programming

The following specific settings are required in the HeiTel programming in order for Video Central Platinum to operate either correctly, or provide similar behaviour to an ADPRO XO device.

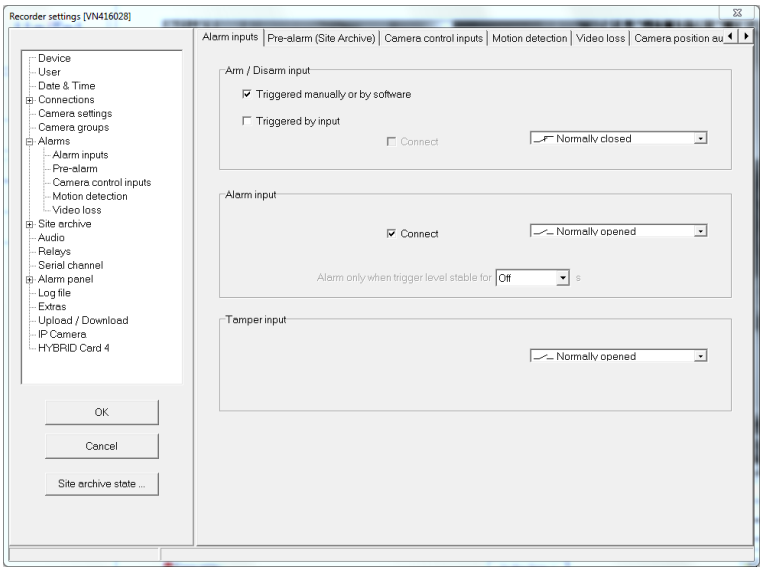
- Registered users - User name (for alarms, programmed as User ID in VCP). Only if HeiTel unit programmed for security.



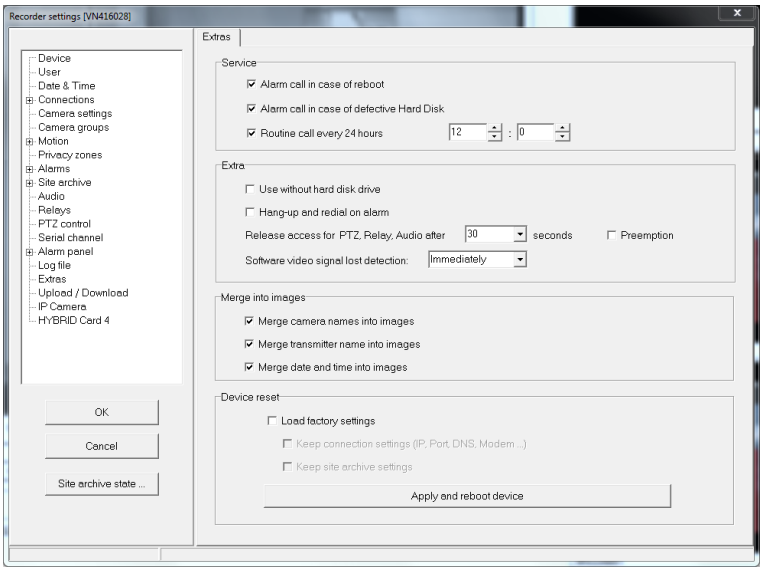
- Device name. (for alarms, programmed as Unit ID in VCP)



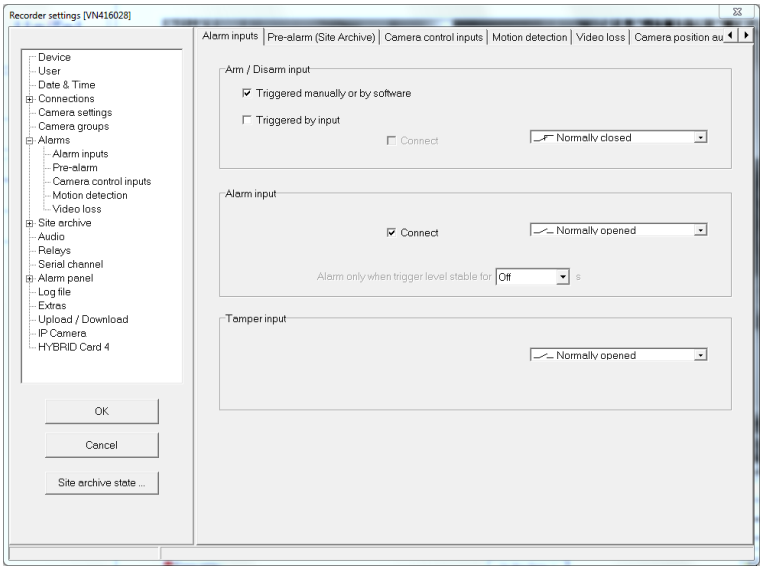
- Alarm Input – Connect On. (for alarm activation events to be sent to VCP)



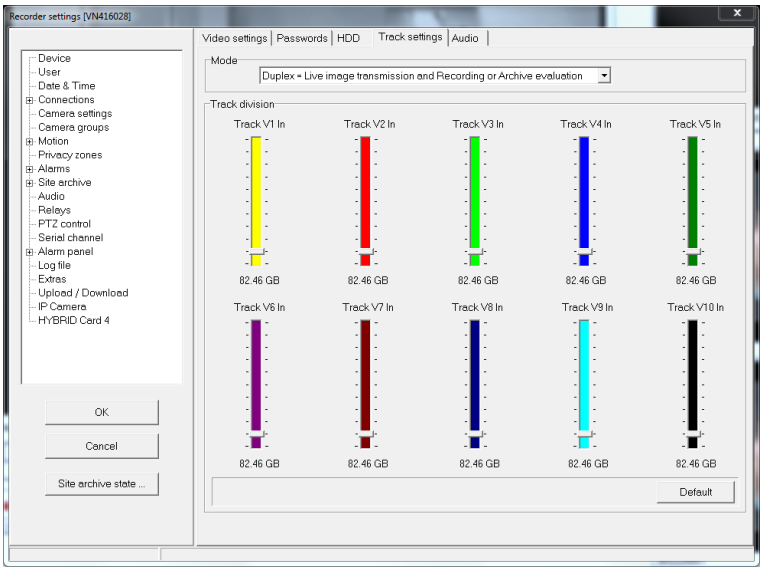
- Pre-emption Off. (for VCP to retain control of audio)



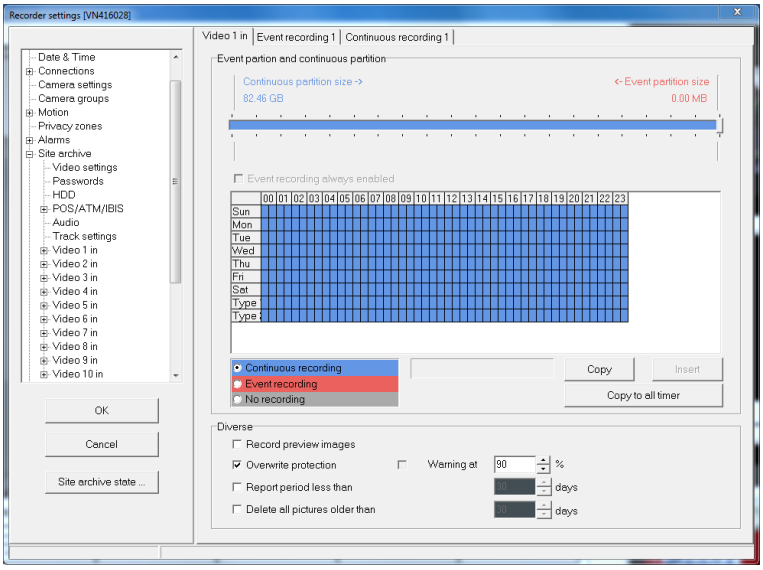
- Trigger Manually or by Software On (for arm/disarm control via VCP)

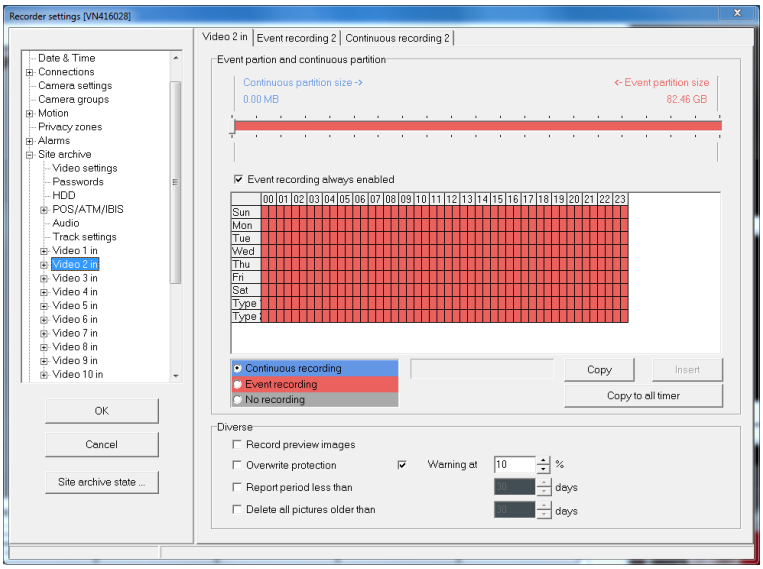


- Duplex Mode (for review mode)

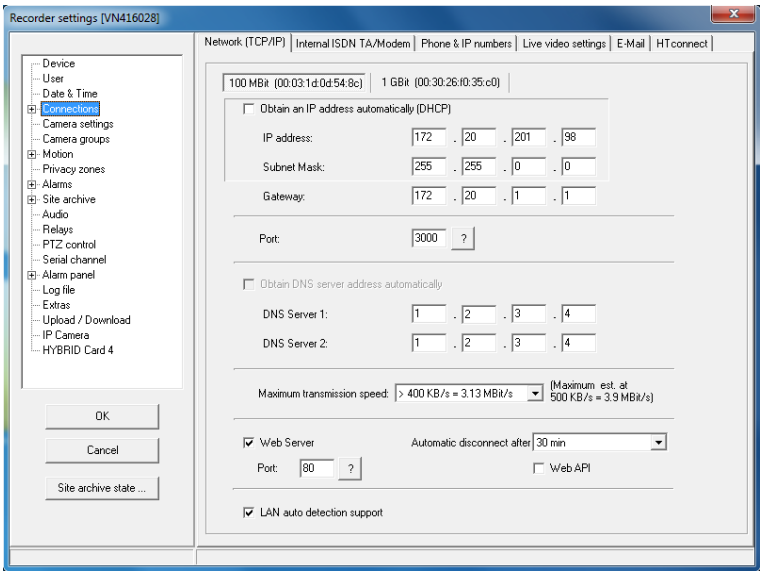


- Continuous only or event only recording (for review mode)

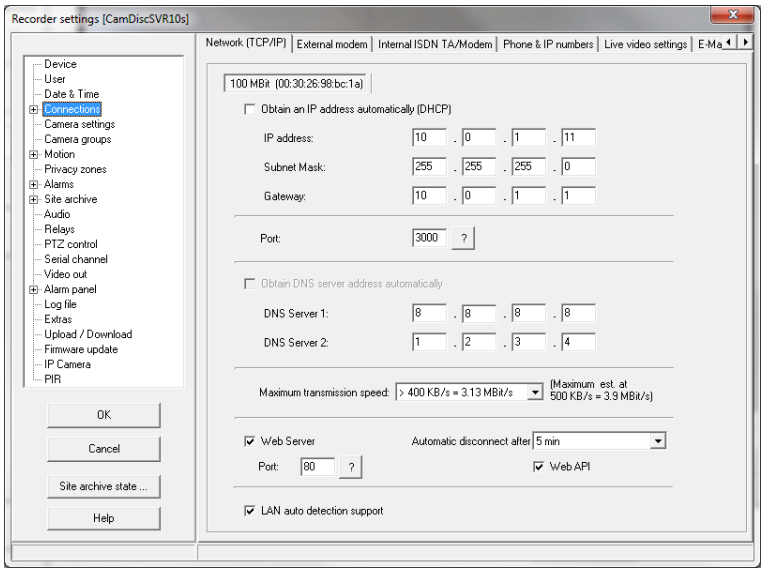




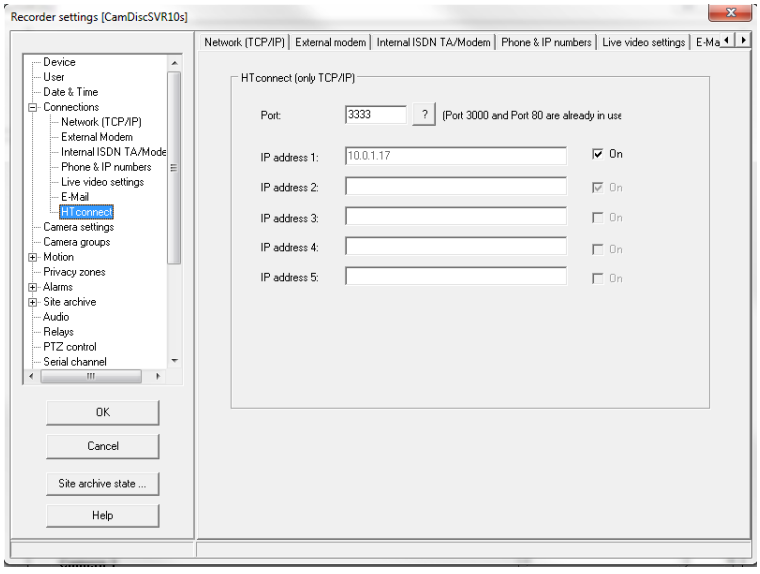
- Web Server On and Port (for iRespond)



- Web API On (for Private and Video Wall)



- To set up an HTconnect connection: in the screenshot below, IP address 1 represents an alarm receiver. The address can be modified from the Phone & IP numbers page. For more information on configuring HTconnect, see HeiTel manuals.



2.4.5 HeiTel Operational Limitations

Active Sites List

- Detector text and Fire fields will be blank as these are ADPRO XO device specific.

Alarms

- Detector text, Indicator and Fire fields will be blank as these are ADPRO XO device specific.
- Cannot associate more than one camera per event.

Arm/disarm

- Arm/disarm will not operate if HeiTel is not set for software control.

Inputs/Outputs

- CIO Relays cannot be controlled.
- Activating CIO Inputs displays HeiTel inputs as ON also when they are actually OFF.
- Relay status will be displayed however if set to something like ‘on when in alarm’ the software control will not operate.
- IO Summary bars not implemented in VCP for HeiTel.

Update Rate for Guard Tour

- Update rate is approx. ½ second per camera. Each camera is updated sequentially.

Audio

- No audio switching as HeiTel only has one channel.

PTZ

- PTZ is enabled for all IP cameras even if they do not have PTZ.

Review Mode

- Limited to camera type searches one camera at a time.
- Due to duplex mode setting requirement HeiTel will not record while a VCP user is in review mode.
- Limited to continuous only recording and event only recording.

2.4.6 HeiTel or VCP Features not Supported by Video Central Platinum when HeiTel Units are in Use

- IO Summary bars.
- Zone Isolate.
- Fire IO Status.
- Fire Contacts.
- Transmit Audio File to Site.
- CMS Priority.
- HeiTel Device Recall Alarm Type.
- HeiTel Pre-Alarm.
- HeiTel Routine Call (SitePulse).
- Review Mode Audio.
- Bounding boxes.
- Serial Communications.
- Backup Communications.
- Output Quick Access Buttons.
- Bi-directional RS232.

2.5 Licensing

After login, system licensing must be conducted via a hardware dongle or a software license key. To display the Feature Licensing dialog select Tools > Administration > Licensing.

2.5.1 Unlicensed Video Central Platinum

If Video Central Platinum is not licensed it runs in Video Central Platinum Lite Mode. Lite mode provides the following limitations;

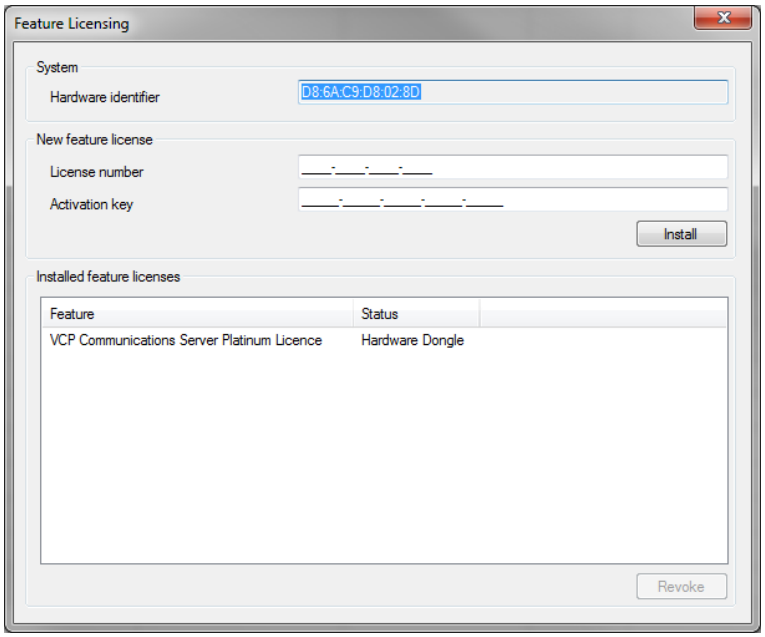
Only the User Interface on the Video Central Platinum Server will connect to the Video Central Platinum Server. No remote User Interfaces will connect to the Video Central Platinum Server.

No Diagrams.

No Video Wall.

2.5.2 Licensing via Hardware Dongle

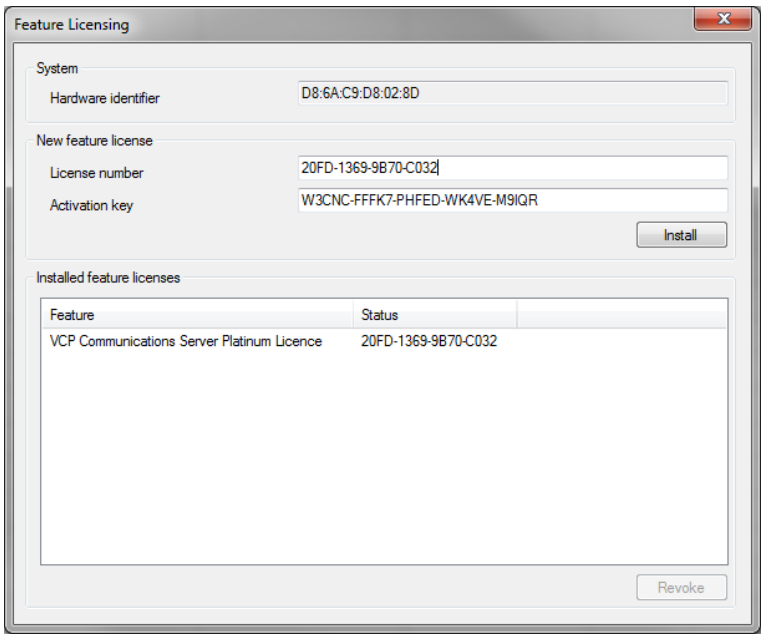
Insert the Video Central Platinum dongle and the Feature column will display ‘VCP Communications Server Platinum License’ and Status will display ‘Hardware Dongle’.



2.5.3 Licensing via Software Key

On the Feature Licensing dialog under New Feature License enter the License Number and the Activation Key then click **Install**. After a short delay the Feature column will display ‘VCP Communications Server Platinum License’ and Status will display the license number.

The Hardware Identifier, which is unique to the PC, is used in conjunction with the License Number to create the Activation Key.



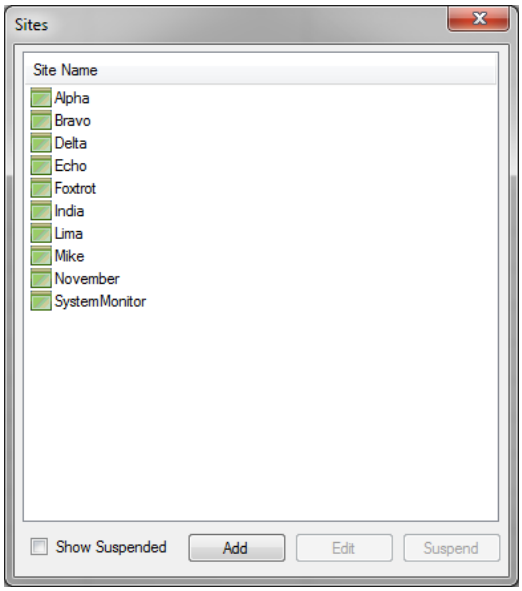
2.5.4 HeiTel CamControl Server Licensing

The HeiTel CamControl Server version 4.27 or better does not require a license. Previous versions require a HeiTel dongle.

2.6 Adding or Editing Sites

2.6.1 Adding New Sites

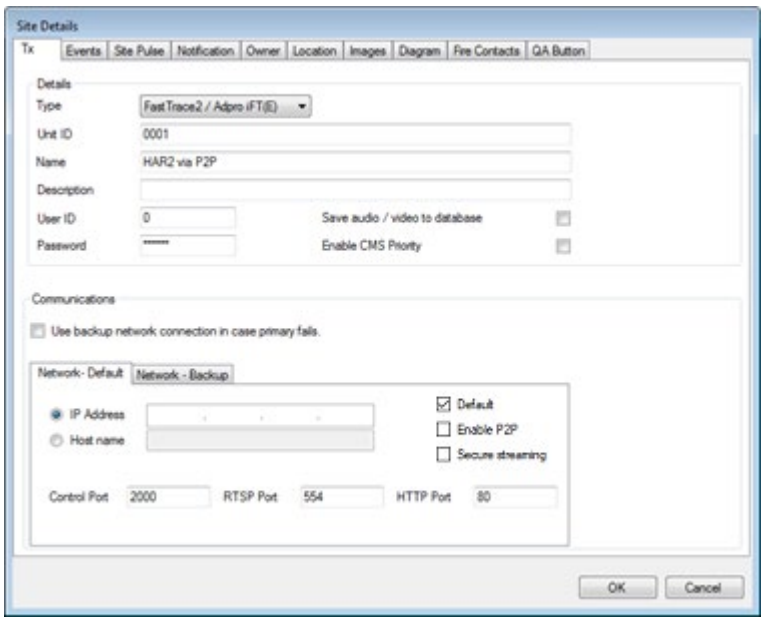
From the Active Sites List access Tools > Administration > Sites to display the Sites dialog.



Click the **Add** button and the Site Details dialog will be displayed.

2.6.1.1 Transmitter Details

Select the **Tx** tab to enter site and communication details.



This dialog is used to define the site name, identification and set communication details.

Unit ID: This is a unique identifier for receiving alarms from the ADPRO XO device. This setting must match the Unit ID set in the ADPRO XO device settings.

Site Name (Name): Enter a unique and easily identifiable site name. This setting must **match the Site Name set in the ADPRO XO device settings**.

User ID and Password: These are security features used to log into the ADPRO XO device. This setting must match the User ID and Password set in the ADPRO XO device settings.

Site Description: Flexible text that can be used to describe the site, location or account for example with up to 50 characters.

Save audio / video to database: Set this check box to automatically save the audiovisual data streams to the database as events. When the check box is clear the audiovisual stream can be saved to the database manually.

Important: Recording will not be performed irrespective of the Save audio / video to database setting if the user does not have permission. Refer to Section 2.8.2 Adding or Editing Groups for further details.

When it is recording, the database will record whatever the operator sees, hears, and/or says.

An audiovisual event lasts for a maximum of 5 minutes, which ensures that exported video events are kept to a manageable size. A new audiovisual event is triggered when the channel or video type changes, as selected from the Guard Tour list, and when 5 minutes has elapsed.

Enable CMS Priority: When enabled CMS Priority allows the first connected CMS (Video Central Platinum System) to automatically take control of the sites PTZ, Local Audio and Video Quality settings. Other CMS systems that may connect to the site will not be able to control the PTZ, Local Audio and Video Quality settings and the respective icons will appear ghosted. Once the CMS with control has acknowledged or disconnected the site other CMS may take control. If CMS Priority is not enabled the CMS will not automatically take control of the features when a connection is made either via alarms or manual connection to the site. This can however be done manually through the Video Central Platinum User Interface if no CMS has control. See the Video Central Platinum Operational Manual for details.

Use backup network connection in case primary fails: This option enables you to set a second IP Address or Host Name, which alarms will be received on if the primary (network - default) cannot be reached. Also, connections to the site will first attempt the network - default connection method. If this method fails the backup method will automatically be attempted. A System Monitor (SystemMonitor Site) event will be generated if the primary connection fails and the backup connection is attempted.

Default: Determines if the Network or Network Backup communications is used first. If the Network Tab is set as default, default will appear on the tab. If default is not present it indicates network backup is set as the default. Note if Network is set as default then the Network communications settings will be used first for validation of incoming alarms or outgoing connections to the site. If a connection cannot be established the Network Backup will be used if “Use backup network connection in case primary fails” is enabled. Alternatively, if Network Backup is set as the default its communication settings will be used for validation of

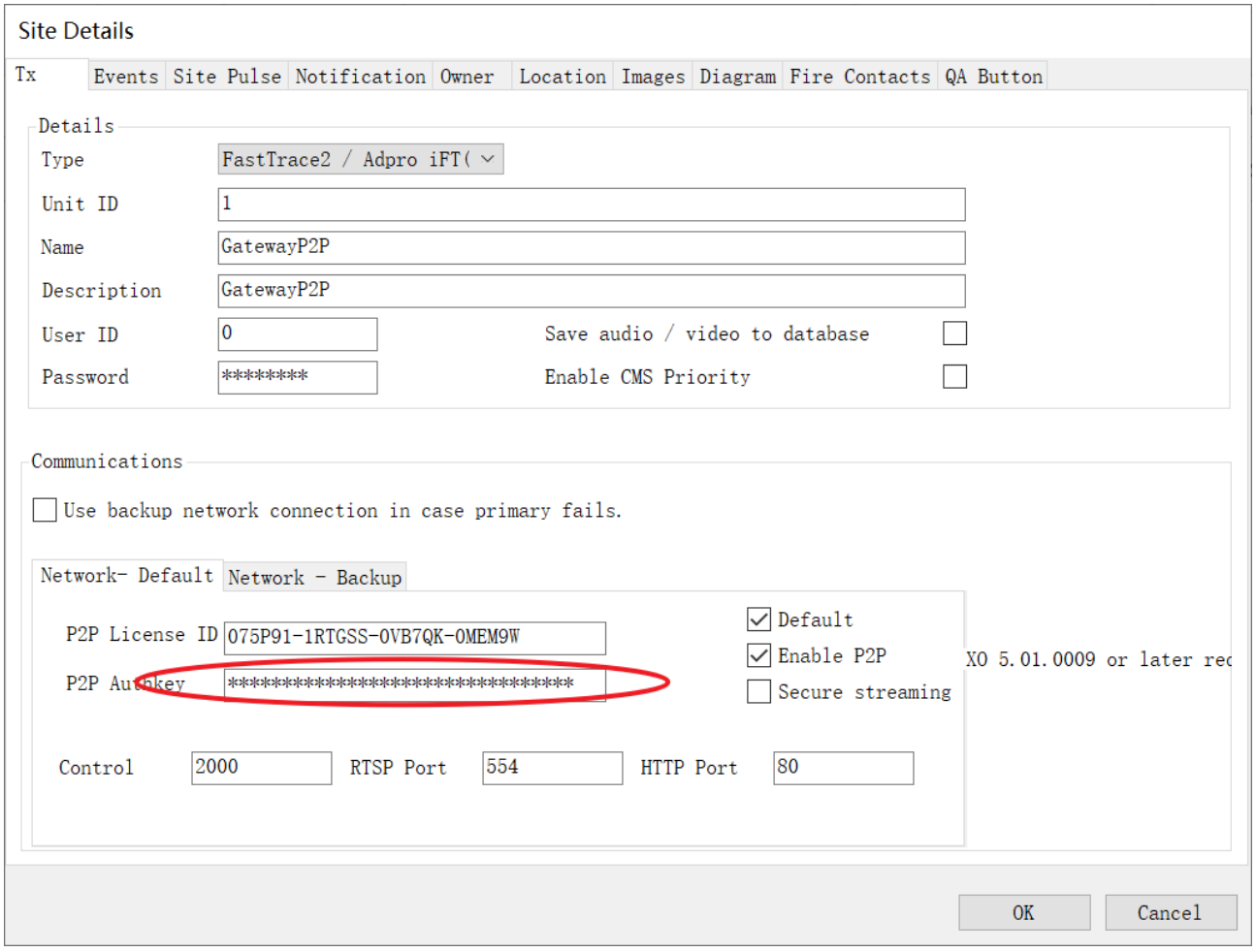
incoming alarms or outgoing connections to the site. Note if the Network Backup settings fail the Network communications settings will not be used and the overall connection attempt will fail leading to a System Monitor (SystemMonitor Site) event.

Network Tab (Note default will appear on this tab if set):

1. IP Address: This is the ADPRO XO device IP Address.
2. Host Name: This is the ADPRO XO device Host Name as setup through a Doman Name System (DNS). DNS is typically used for communication devices where the IP Address changes such as with 3G devices.

Note: The devices with XO5 firmware support P2P connections. To get the P2P license key, add the XO device to Xchange2 and click **Activate your P2P license** on the **Manage Products** page for the device to get the TUTK license code. Copy it to the clipboard by clicking the text icon and use it for device connection in VCP. For more details, see *Xchange2 User Guide*.

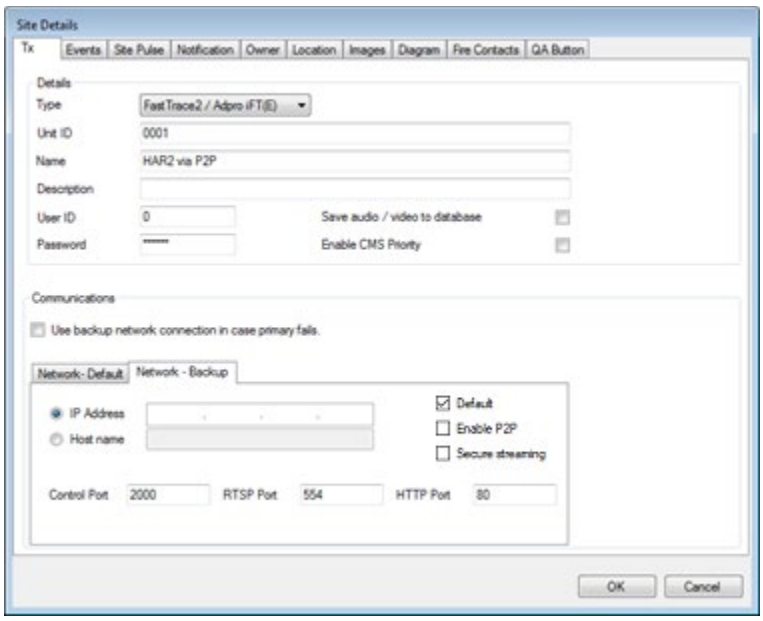
3. Enable P2P: The option to enable P2P instead of the IP connection. The IP Address and Host Name fields disappear if this option is selected and P2P License ID and P2P Authkey fields appear. Enter the P2P license ID and P2P Authkey. The P2P Authkey is obtained from the XO client. For more details, see *P2P Setup Guide*.
4. Secure streaming: Select this checkbox to enable encrypted video streaming.



5. Control Port: Port used by Video Central Platinum to send commands to the ADPRO XO device.
6. RTSP Port: Port used to receive video from the ADPRO XO device.
7. HTTP Port: Port used for ADPRO XO device Setup or HeiTel iRespond.

Network Backup Tab:

This tab is only enabled when the 'Use backup network connection in case primary fails' option is used. It allows for a backup IP Address or Host Name on which to receive alarms and make outgoing connections to the site if the primary Network – Default IP Address or Host Name fails.



1. IP Address: This is the ADPRO XO device IP Address.
2. Host Name: This is the ADPRO XO device Host Name as setup through a Doman Name System (DNS). DNS is typically used for communication devices where the IP Address changes as with 3G devices.
3. Enable P2P: The option to enable P2P instead of the IP connection. The IP Address and Host Name fields disappear if this option is selected and P2P License ID field appears. Enter the P2P license key obtained from Xchange2.

   Note: The P2P license ID can be different for the Default and the Backup.
4. Control Port: Port used by Video Central Platinum to send commands to the ADPRO XO device.
5. RTSP Port: Port used to receive video from the ADPRO XO device.
6. HTTP Port: Port used for ADPRO XO device Setup.

Note: Information must be exactly as entered via the ADPRO XO Client Setup Interface. The Unit ID and Site Name in the Video Central Platinum setup must match the valid Unit ID and Site Name in the ADPRO XO client.

Note: Ports should only be changed if a conflict occurs with another application. If ports are changed within Video Central Platinum, they will also need to be set via the ADPRO XO device Setup to match.

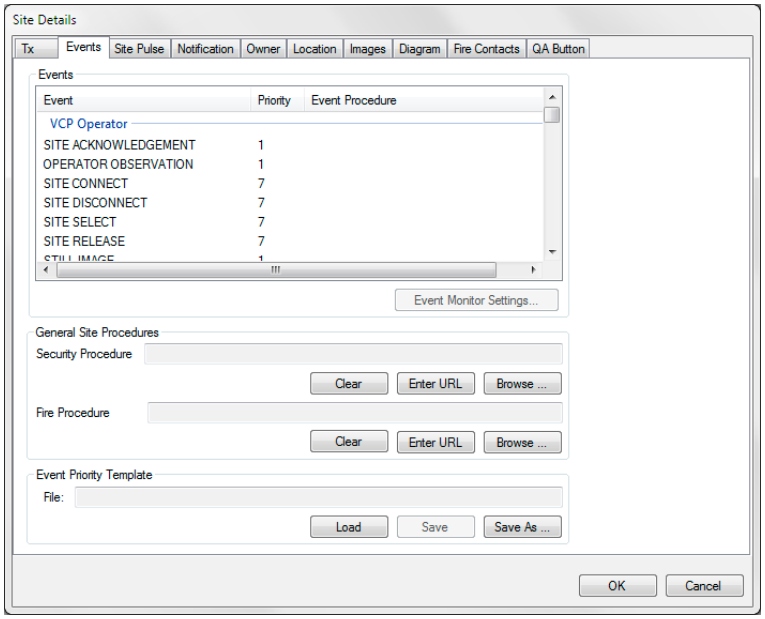
Note: If a Host Name is required typically due to the use of a 3G communications service for example it must first be setup via a Domain Name System Service provider. This service maps a unique and constant name to the communication devices IP Address. If the IP Address of the device changes the service will automatically update the Host Name to IP Address mapping ensuring a connection to the site can always be established.

Note: If the audio port is changed within the ADPRO XO device Setup, Video Central Platinum will automatically utilize the new port set.

Note: Video Wall cannot use Network – Backup communication settings. Only the Network communication settings will be used.

2.6.1.2 Events Details

Select the **Events** tab to set the priorities of events and assign procedures, or to configure event monitoring.



2.6.1.2.1 Assigning Event Priorities

The Event column is a global list of all events. The Priority column allows an order of importance to be assigned to each event. Priorities range from 15 (highest) to 0 (lowest).

When an event occurs, the figure in the Priority column will determine where that site and event will appear on the Active Sites List. By default, any event of priority 15 will be displayed at the top and others will be listed in descending order of priority. However, you can specify a different sorting order in the ASL Site Priority setting in the Database General Options screen (Tools > Administration > Database > General).

To assign a priority to an event, scroll up or down the list, click to select an event and enter the required number in the Priority column.

2.6.1.2.2 Save and Load Event Priority Templates

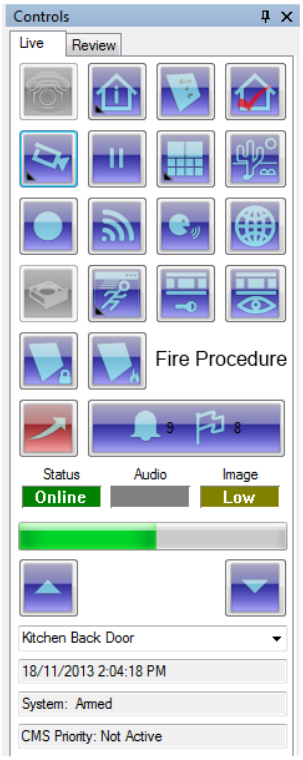
The **Save** and **Save As** buttons allow the event priority list for a site to be saved for re-use. This is useful when entering similar priority details across several sites. After assigning event priorities for a particular site, click **Save As** then browse to a location where the list is to be saved. Enter a file name then click **Save**. The file path and filename with extension '.ep' will be displayed in the Event Priority Template dialog.

To re-use the event priority list for another site, click **Load** then browse to the saved file and click **Open**. This will open a copy of the Site Details with the file path and name displayed in the Event priority Template dialog. This copy may then be modified and renamed to suit a different site.

2.6.1.2.3 Security Procedure / Fire Procedure

Procedures are instructions to Installers/Operators on a given alarm. These instructions may include contact details, instructions, maps, or steps to resolve issues. Procedures can be displayed in response to a site's Security and Fire events in either text format, pictorial or html formats. The events display the procedure in the Security or Fire Procedure tab/window once it has been opened.

While in Live View mode for a site, click the **Security Procedure** or **Fire Procedure** button in the Controls panel to open the Security/Fire Procedure tab/window for that site.



After a site has been configured it has a default Web URL (Web page) or other compatible file associated with security class and/or fire class events.

For Security and Fire events, when an event is clicked on in the Events tab the default procedure for its class of events will be displayed, unless a specific procedure has been configured to display for that site event.

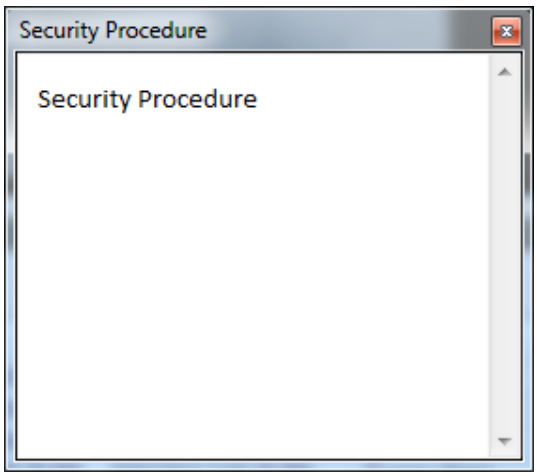
For Video Central Platinum events, when an event is clicked on in the Events tab the last procedure is displayed again unless a procedure has been configured for that particular event, in which case the configured resource (file or URL) will be displayed.

2.6.1.2.4 Security and Fire Procedure requirements for Files and Web URLs

When setting a Web URL or file to be launched from a site event you must ensure that the VCP UI PC, and the logged in operator, will have the security permissions needed to view that URL. The compatible file types are listed in the table below. Files must be less than 200 MB in size.

File Type	Control Type Used
URL	Web Browser
Txt	Web Browser
html	Web Browser
htm	Web Browser
xhtml	Web Browser
png	Web Browser
bmp	Web Browser
jpg	Web Browser
jpeg	Web Browser
gif	Web Browser
tif	Web Browser
yuv	Web Browser
pdf	Web Browser with PDF Plug-in *
rtf	Rich Text

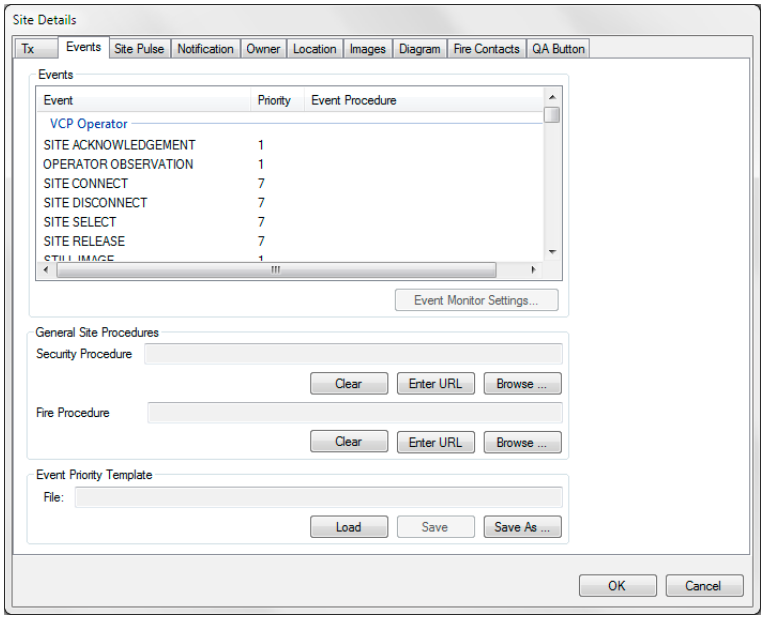
*PDF Plug-in must be installed on the PC.



2.6.1.2.5 Setting the Default Procedures for Security and Fire events

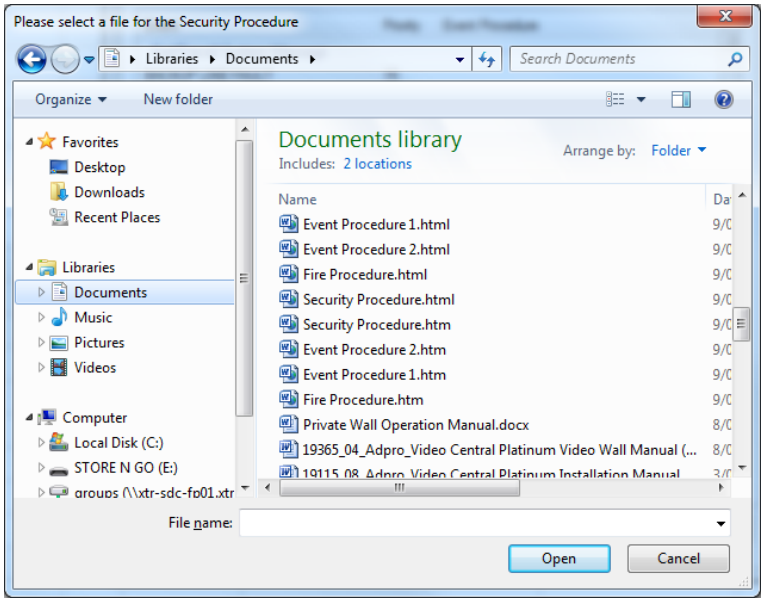
While in the Active Sites List, from the main menu select Tools > Administration > Sites. Video Central Platinum will display the Sites window. Select the site to configure and click **Edit**. The Site Details window will be displayed.

Click the **Events** tab.

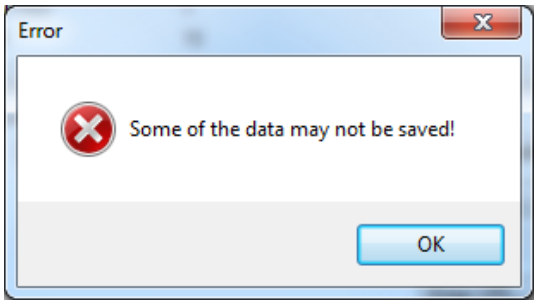


To set the Web URL for a Security Procedure or Fire Procedure click the appropriate **Enter URL** button and enter a web location as you would enter it in the Internet Explorer address bar.

To set a file as the resource, click **Browse** and locate the file within the browse window.



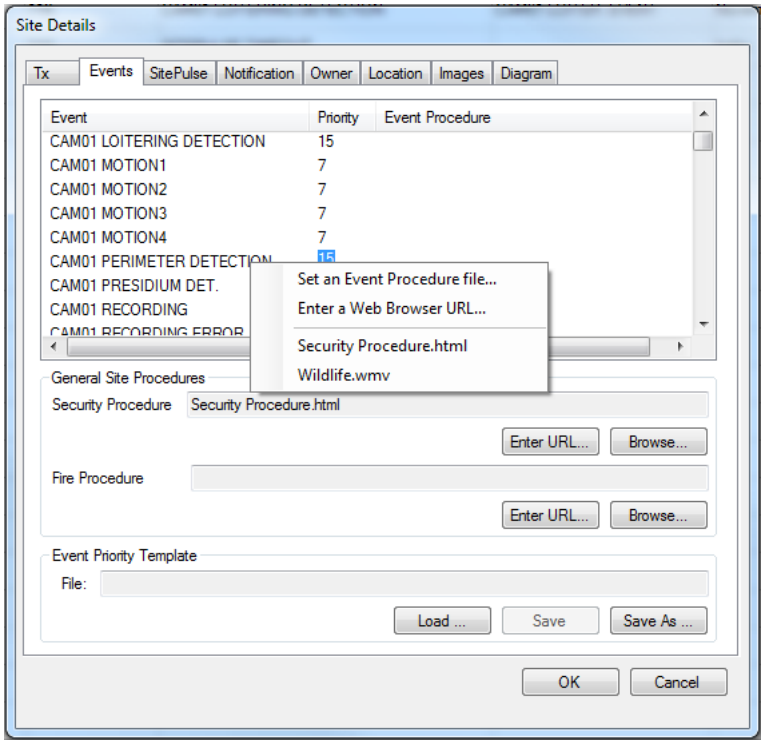
If the selected file is too big it will not be copied to the Video Central Platinum Server and a warning will inform you that the operation has failed.



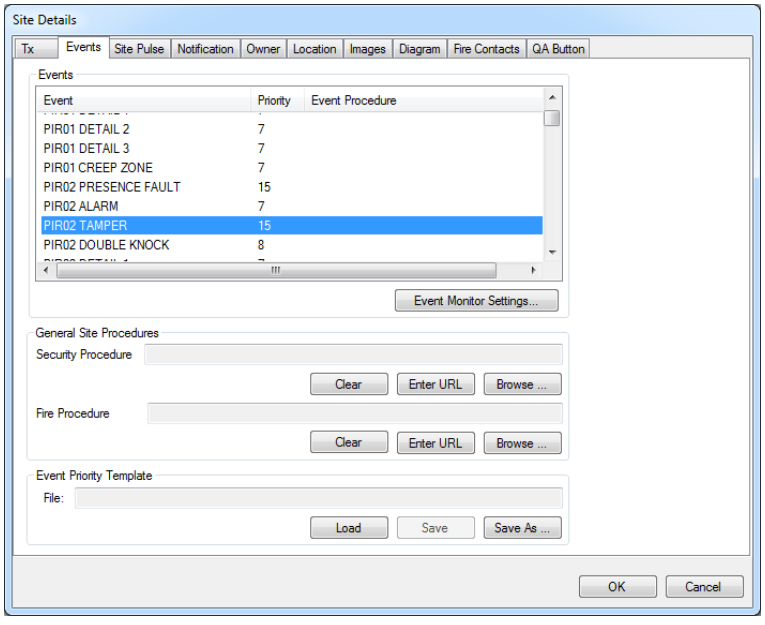
2.6.1.2.6 Setting Event procedures for specific Site Events

Each site event can have their event procedure set rather than have all security class events show the default security procedure and all fire class events show the default fire procedure.

To set a procedure for an event open using the Site Details, click the **Events** tab and scroll to the desired event. **Right-click** on the event name. Video Central Platinum will present a context menu from which you can set a file or web URL as the resource for this event then click **OK**.



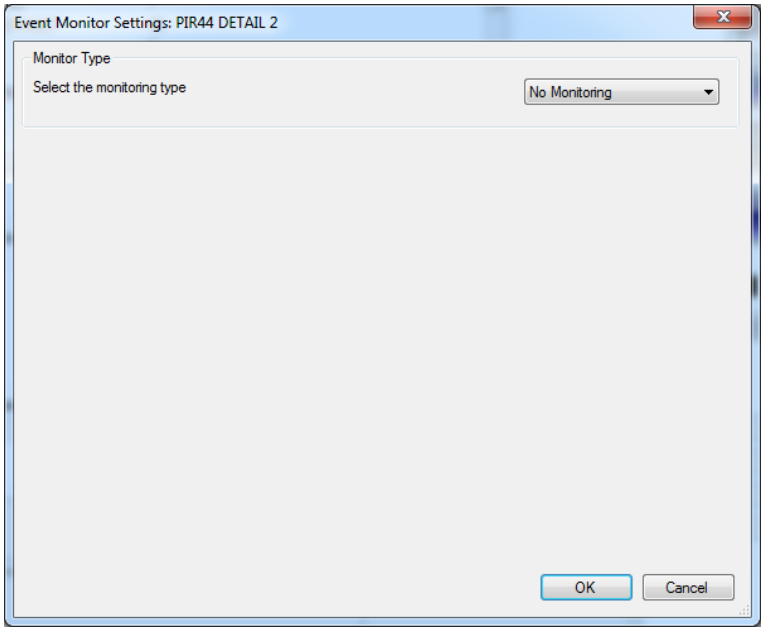
2.6.1.2.7 Event Monitoring Settings



Select a device site event from the Events list.

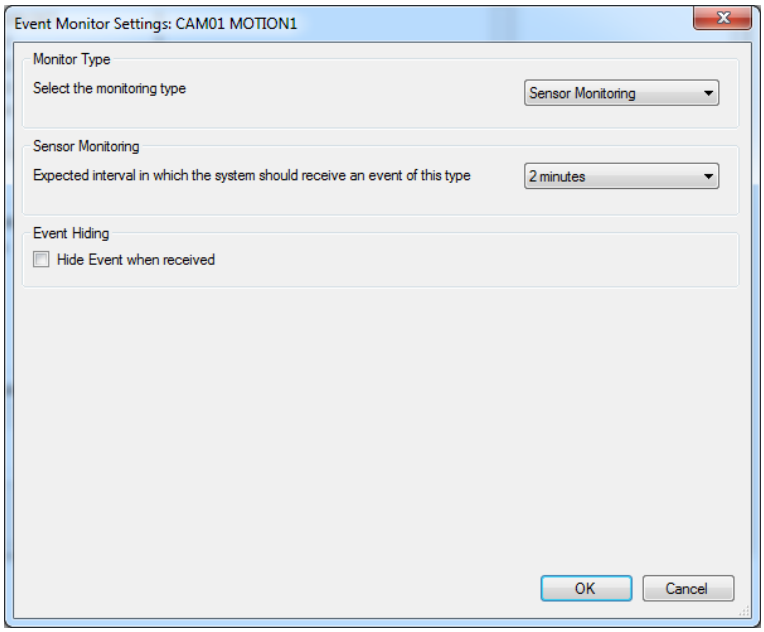
Note: some events are not generated by the site device, but rather by VCP itself. It is only possible to monitor device site events. The Event Monitor Settings button will only be enabled when selecting a device site event from the Events list.

After selecting the event to monitor, click the Event Monitor Settings button. This will open the Event Monitor Settings screen.



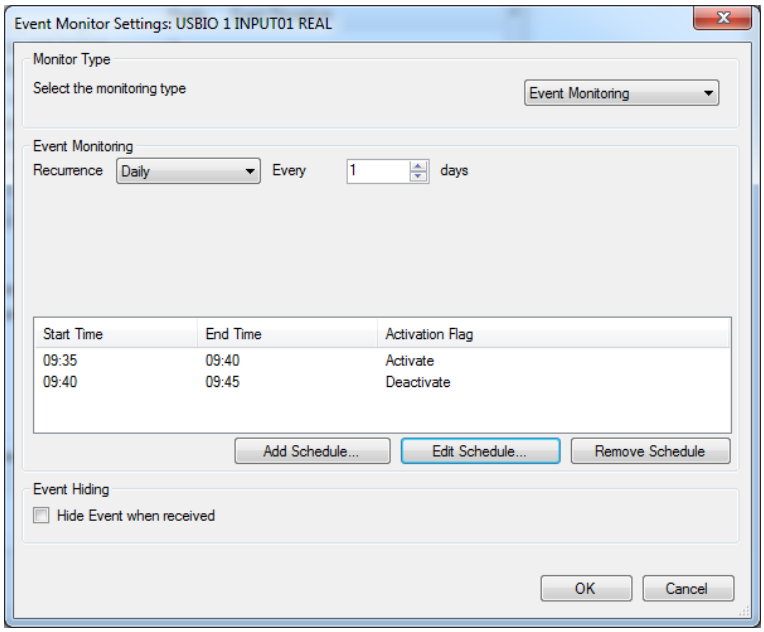
The following options for monitoring are available:

- **No Monitoring**: can be used to clear any of the other monitoring settings.
- **Sensor Monitoring**: allows to select an interval in which the event is expected to occur. If the event does not occur within the specified interval, a SENSOR PULSE TIMEOUT alarm will appear on the Active Sites List.
  There is also an option to hide the event when received. If this option is checked, the event that is being monitored will not appear on the ASL when it occurs.

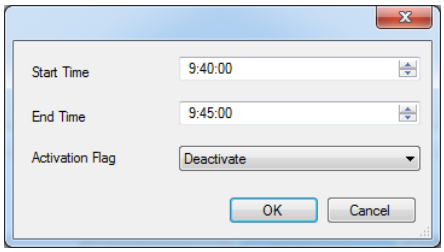


- **Event Monitoring**: allows to select a timespan in which an event is expected to occur. A timespan is defined by a schedule, which has a start and end time. Different timespans can be added, by adding extra schedules.
  - The Recurrence setting allows to set the days on which the event monitoring is active.
  - If event monitoring is active for a given event, then if this event is not received within the timespan indicated by a schedule, a “MONITORED EVENT UNRECEIVED” event will appear on the system monitor, i.e. the related site will appear on the ASL with a “MONITORED EVENT UNRECEIVED” event.
  - If the monitored event is received outside of the scheduled time span, then a “MONITORED EVENT RECEIVED AT UNSCHEDULED TIME” event will appear on the ASL.

- If the “Hide event when received” checkbox is ticked, then the event that is being monitored will not appear on the ASL if it occurs.



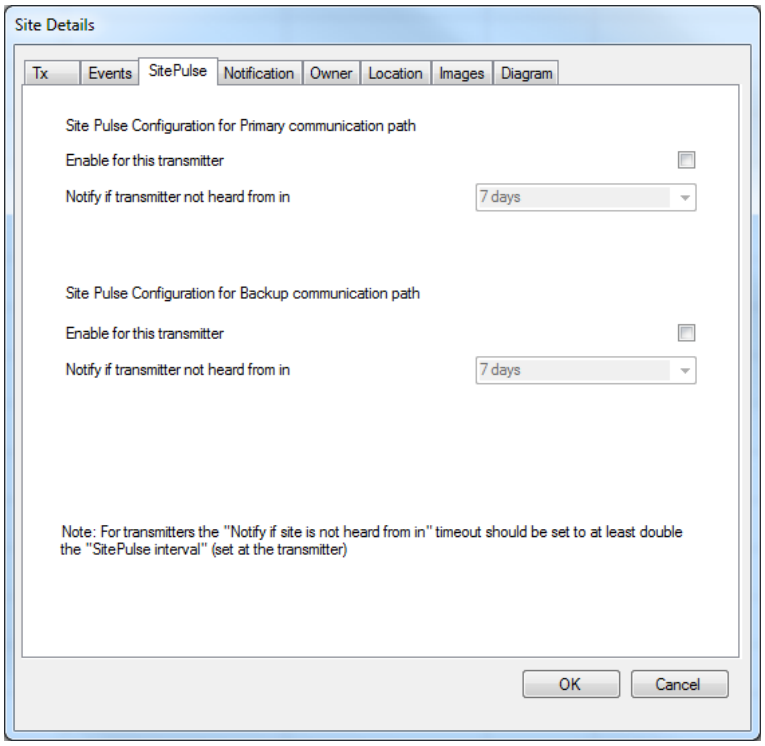
Below is the **Add/Edit Schedule** screen. It allows to set a start and end time for the schedule. You can also set an activation flag. The activation flag indicates whether the event monitoring should check on event activation, event deactivation, or both, when monitoring this event.



2.6.1.3 SitePulse Details

Select the **SitePulse** tab to set the time period after which a non-responsive transmitter notification will be made.

The SitePulse feature monitors connection with the ADPRO XO device. If Video Central Platinum does not receive a reset within the specified time period, a SitePulse event will be generated. This normally indicates a fault with either the communication network or the ADPRO XO device.



2.6.1.3.1 Site Pulse Configuration for Primary communication Path

Check the ‘Enable for this transmitter’ dialog to enable the SitePulse feature.

Select a time period from the ‘Notify if transmitter not heard from in’ list.

The SitePulse timer will be reset if any of the following occurs:

- a user connects to the site
- a user remains connected to the site
- an event is received from the site
- the life check event is sent from the ADPRO XO device.

The life check event is programmed at the ADPRO XO device as the Line Test feature. It is recommended that the ‘Notify if transmitter not heard from in’ time is set to at least double that of the Line Test Interval that is programmed into the ADPRO XO device.

The site pulse setting applies to the XO primary life check message (XO event code 0034).

At the XO side this site pulse is configured via System > Behaviour > Alarm Transmission > CMS Alarm Transmission > Primary Alarm Transmission > Line test (Site Pulse).

This VCP Site Pulse setting also applies to the XO Parallel Alarm Transmission 1- and 2-line tests.

2.6.1.3.2 Site Pulse Configuration for Backup communication Path

The Site Pulse feature can also be applied to the Backup Communication Path.

Check the ‘Enable for this transmitter’ dialog to enable the SitePulse feature.

Select a time period from the ‘Notify if transmitter not heard from in’ list.

The SitePulse timer will be reset if any of the following occurs:

- a user connects to the site
- a user remains connected to the site
- an event is received from the site
- the life check event is sent from the ADPRO XO device.

The life check event is programmed at the ADPRO XO device as the Line Test feature. It is recommended that the 'Notify if transmitter not heard from in' time is set to at least double that of the Line Test Interval that is programmed into the ADPRO XO device.

The site pulse setting applies to the XO backup life check message (XO event code 0035).

At the XO side this site pulse is configured via System > Behaviour > Alarm Transmission > CMS Alarm Transmission > Secondary Alarm Transmission > Line test (Site Pulse).

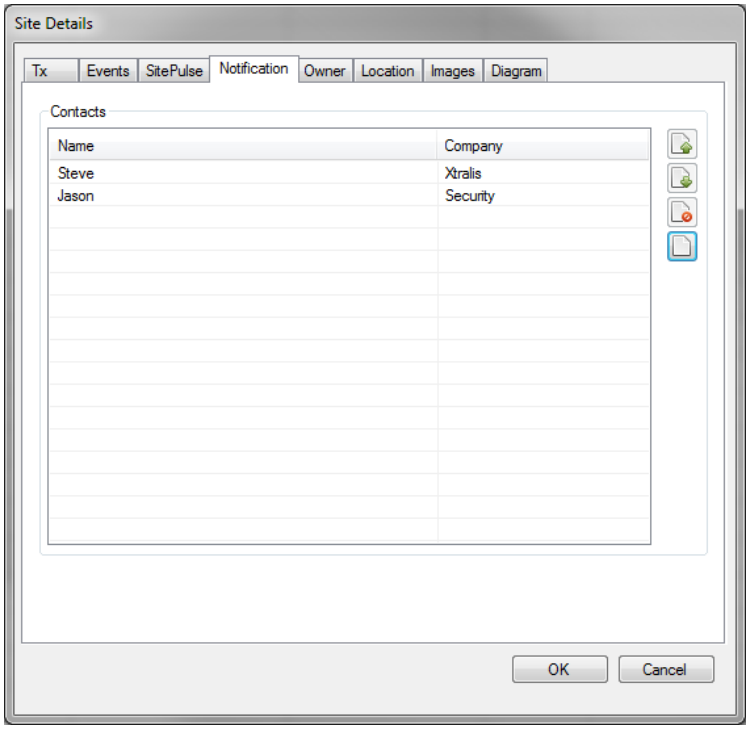
2.6.1.4 Notification Details

Select the **Notification** tab to create a list of people that may be contacted if an event occurs. The contact names and company details are displayed on the Site Details dialog, Notification tab but are created and edited on the Site Notification Contact dialog.

In Operational Mode, Notification details are displayed on the Site Details dialog.

To create a new contact from the Notification tab, click the  icon and the Site Notification Contact dialog will be displayed, opening at the General tab

Important: Never use the pipe character (|) when entering data as it is used to determine the separation of data when an export is performed.

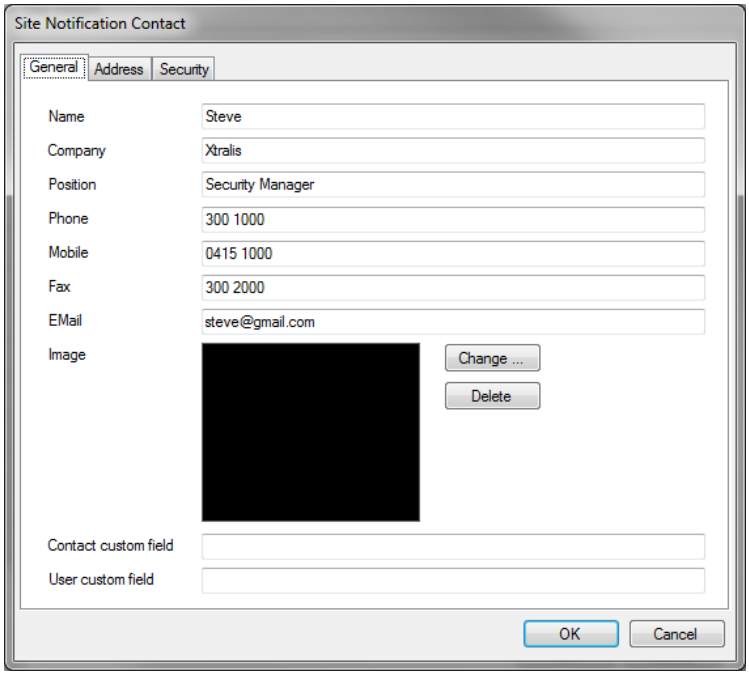


In the Site Notification Contact dialog, **General** tab, enter the name and company of the contact. These are the minimum requirements before the contact will be listed. Tab down to other boxes and enter relevant details including phone and fax numbers.

The Image box allows a photo of the contact to be displayed. To add a stored image click **Change** and navigate to the relevant location.

To replace the image, click **Delete** then **Change** to locate the new image.

The Contact and the User custom fields are unassigned and may be used for adding notes. When complete select the Address tab.



Under the **Address** tab enter the site Address (street number and suburb), City and State names, then the Zip or post code of the Contact.

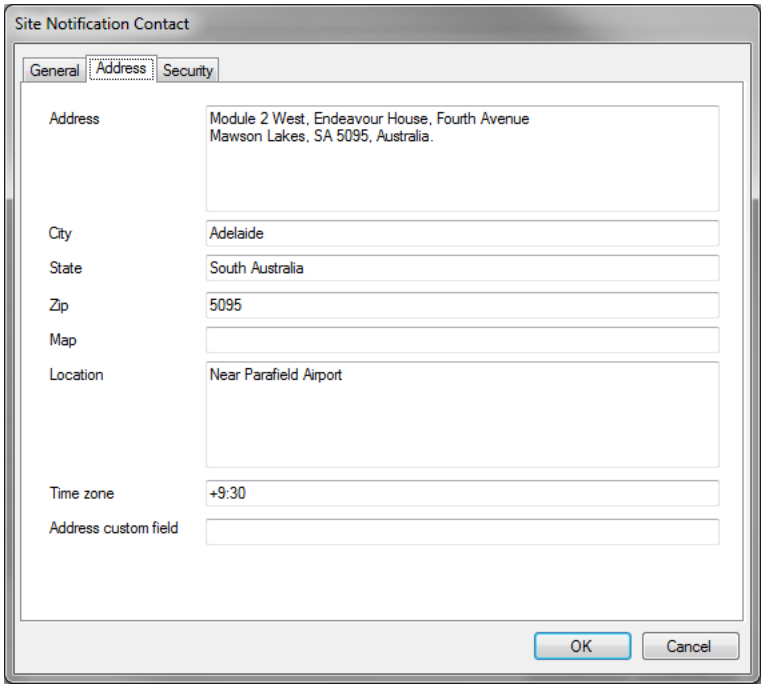
In the Map text box enter a map reference, GPS coordinates, or other location specification.

In the Location text box enter a description of the site location and how to go there.

In the Time Zone text box enter any time difference between the monitoring station and site. For example, +2.00 indicates the site is two hours ahead of the monitoring station.

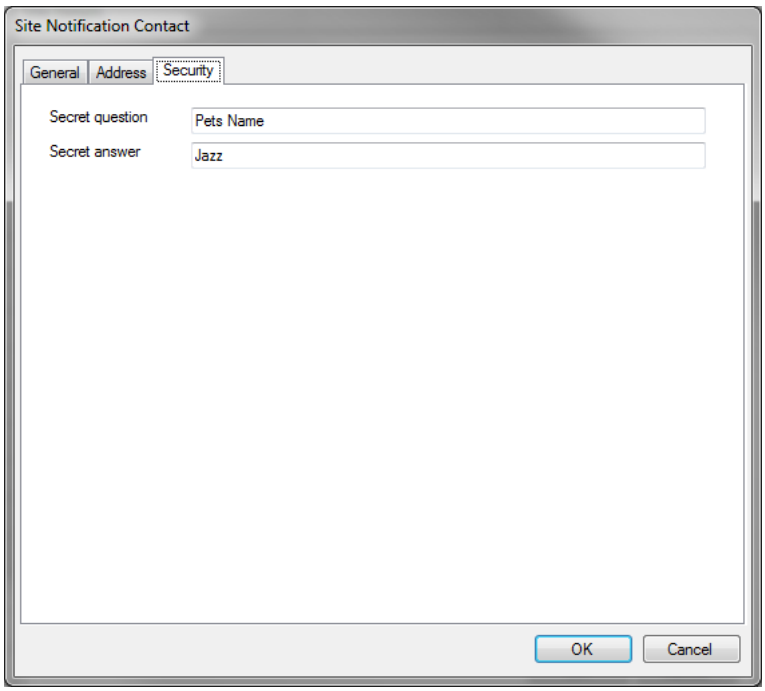
The Address custom field is unassigned and may be used for adding notes.

When complete select the **Security** tab.



Under the Security tab enter a Secret Question and the Secret Answer. This will be used to validate the identity of anyone calling the Contact from the monitoring station.

When complete, click **OK** and the Notification dialog will re-display, now populated with the names of contacts and their companies.



To set the order in which listed people are to be contacted, select each in turn then click the or button to move them up or down the priority list.

To delete a contact, select the icon.

When complete select the **Owner** tab.

2.6.1.5 Owner Details

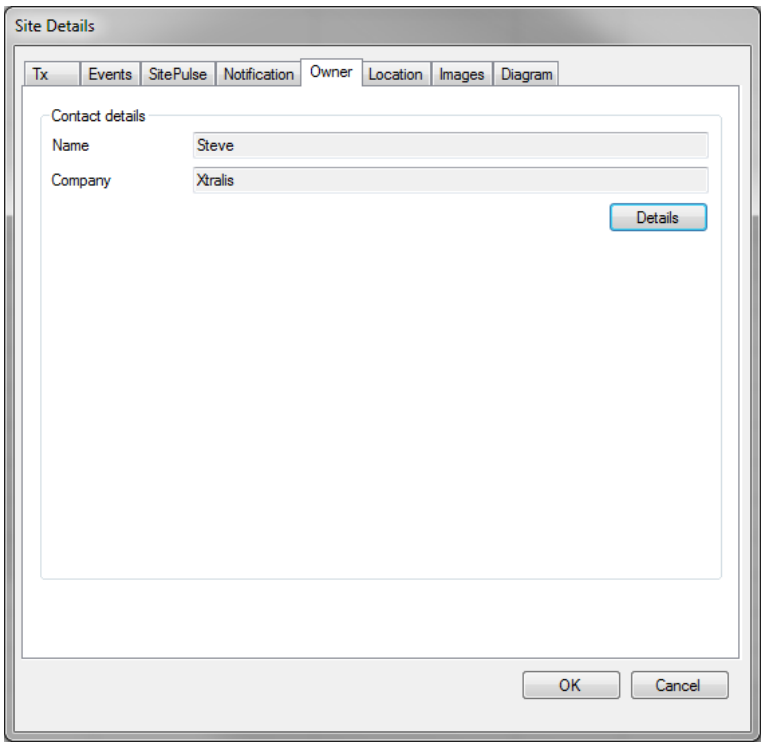
In Operational Mode, Owner Details are displayed on the Site Details dialog.

Select the Owner tab to register details of the site's owner.

The owner's Name and Company are displayed under the Owner tab but are created and edited on the Site Owner dialog.

Click the **Details** button to display the Site Owner dialog, opening at the General tab.

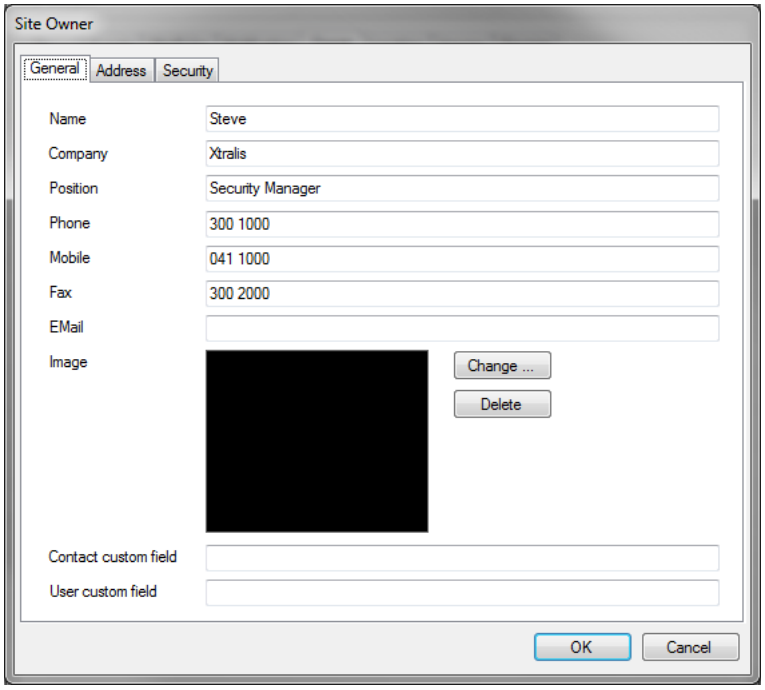
Important: Never use the pipe character (|) when entering data as it is used to determine the separation of data when an export is performed.



Under the General tab enter the owner's name and company title. These are the minimum requirements before the contact will be listed. Tab down to other boxes and enter relevant details including phone and fax numbers.

The Image box allows a photo of the owner to be displayed. To add a stored image click Change and navigate to the relevant location.

To replace the image, click **Delete** then **Change** to locate the new image.
The Contact and the User custom fields are unassigned and may be used for adding notes. When complete select the **Address** tab.



Under the **Address** tab enter the site Address (street number and suburb), City and State names, then the Zip or post code.

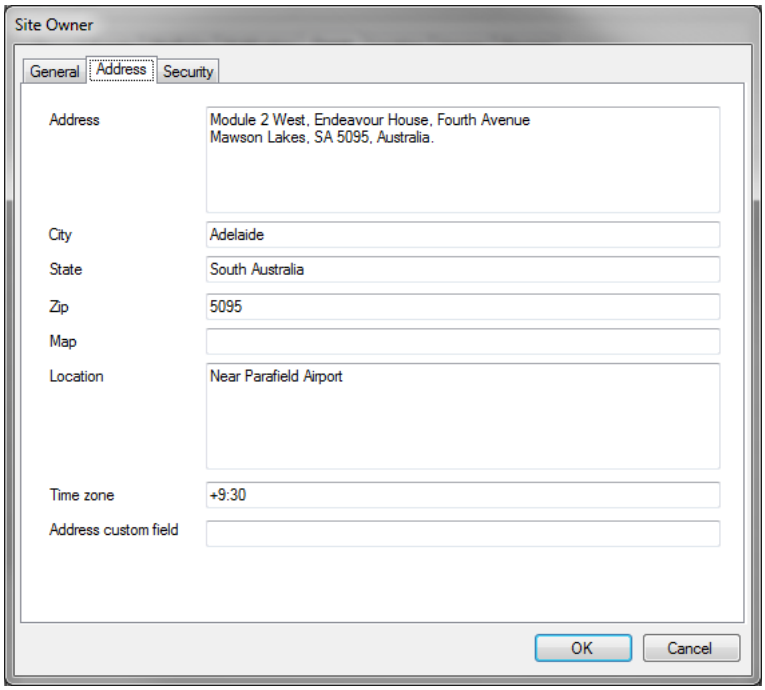
In the Map text box enter a map reference, GPS coordinates, or other location specification of the site.

In the Location text box enter a description of the site location and how to go there.

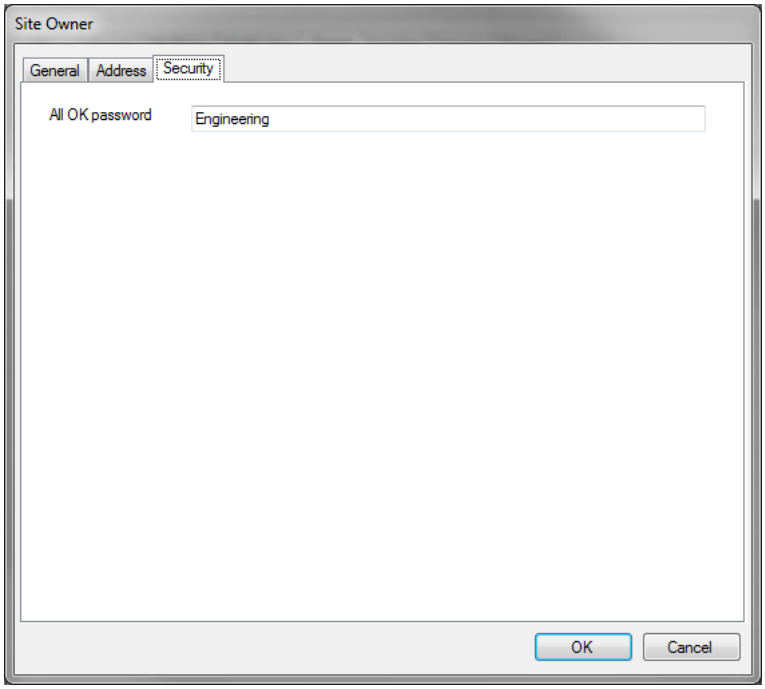
In the Time Zone text box enter any time difference between the monitoring station and site. For example, -2.00 indicates the site is two hours behind the monitoring station.

The Address custom field is unassigned and may be used for adding notes.

When complete select the **Security** tab.



Under the **Security** tab enter a password that will be used to validate the identity of anyone calling the monitoring station from the site and confirm that everything is satisfactory. Click **OK** to enter the details under the Owner tab then select the **Location** tab.



2.6.1.6 Location Details

In Operational Mode, Location Details are displayed on the Site Details dialog.

Location Details are displayed on the Site Details dialog in Operational Mode.

Under the **Location** tab enter the site Address (street number and suburb), City and State names, then the Zip or post code at which the ADPRO XO device transmitter is located.

In the Map text box enter a map reference, GPS coordinates, or other location specification.

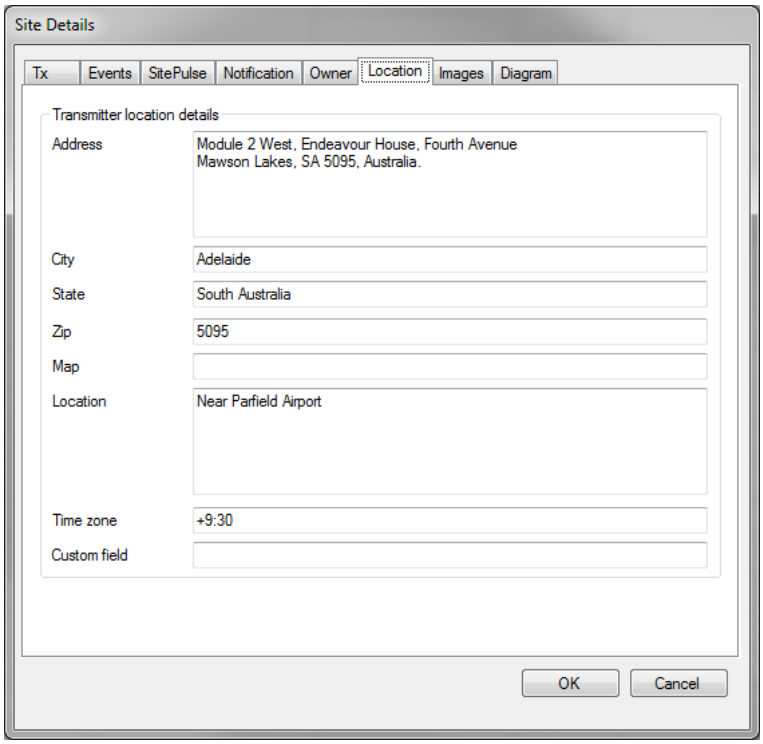
In the Location text box enter a description of the site location and how to go there.

In the Time Zone text box enter any time difference between the monitoring station and site. For example, +2.00 indicates the site is two hours ahead of the monitoring station.

The Custom field is unassigned and may be used for adding notes.

When complete select the Images tab.

Important: Never use the pipe character (|) when entering data as it is used to determine the separation of data when an export is performed.



2.6.1.7 Site Images

In Operational Mode, Site Images are displayed on the Site Details dialog.

Images may be used to display static pictures from the installed cameras as references.

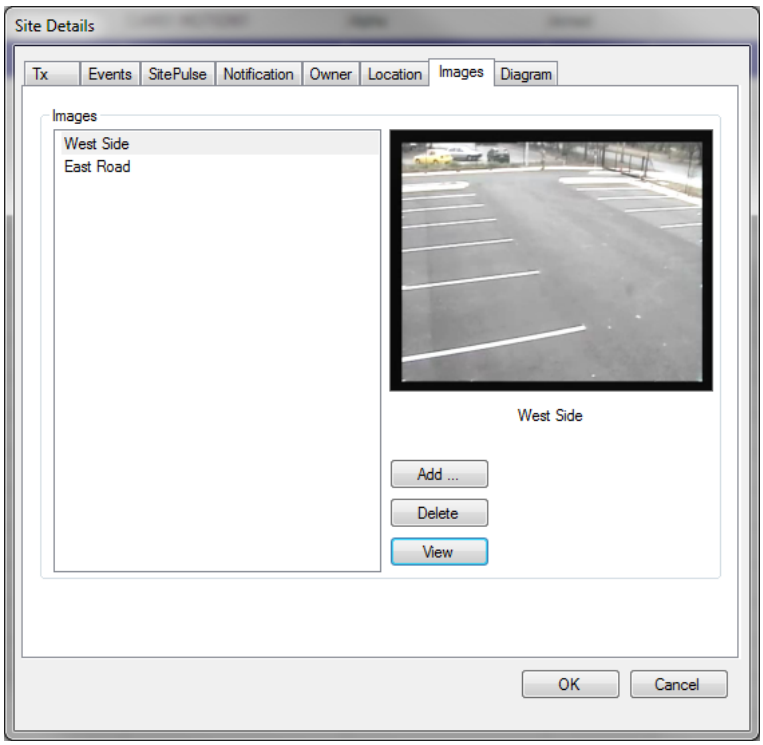
To add a new image click **Add** and the Windows Open dialog will be displayed. Browse to the required file then click **Open** and the Picture Title dialog box will be displayed. Do not change the Filename but enter a meaningful name for the image in the Title box. Click **OK** and the name will be entered in the Images list.

To preview an image select its name on the Images list then click **View**. The image and name will be displayed.

To delete an image select on the Images list then click **Delete**.

If a diagram is to be associated with the site, click the **Diagrams** tab and proceed as described below.

If no diagram is to be associated with the site click **OK** and the Active Sites dialog will be displayed.

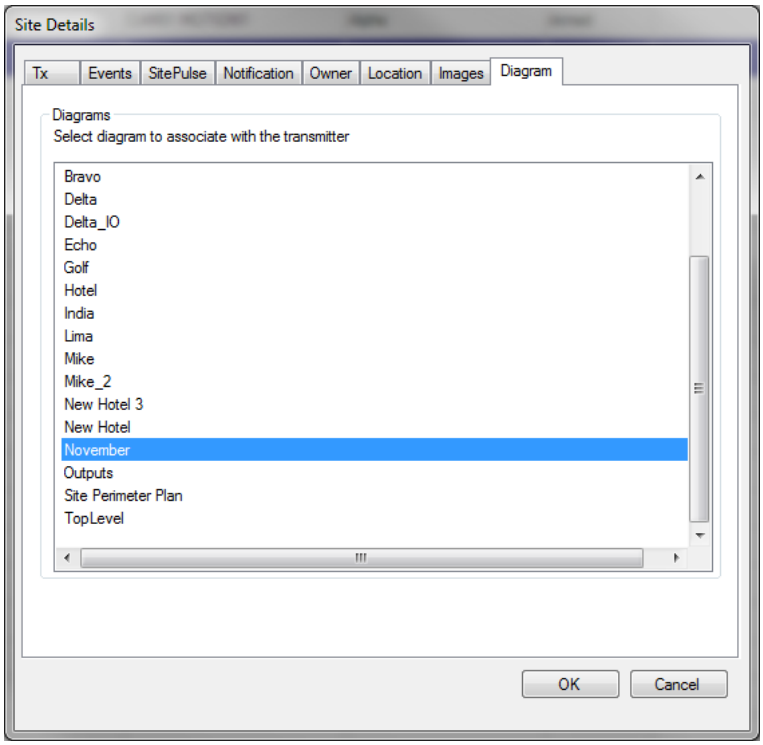


2.6.1.8 Diagrams

Diagrams must first be created using the Video Central Platinum Diagram Editor.

The Interactive Diagrams feature will attempt to load the map associated with the site when a connection is made. If no Site Diagrams have been associated with the site, the top level map will be loaded.

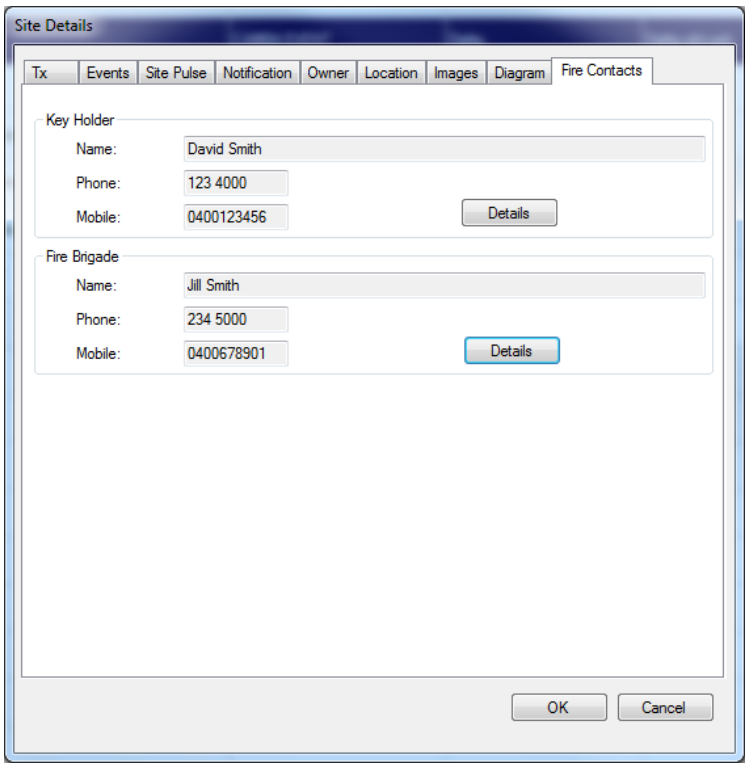
To associate a Diagram with a site, highlight the name from the Diagrams list then click **OK**.



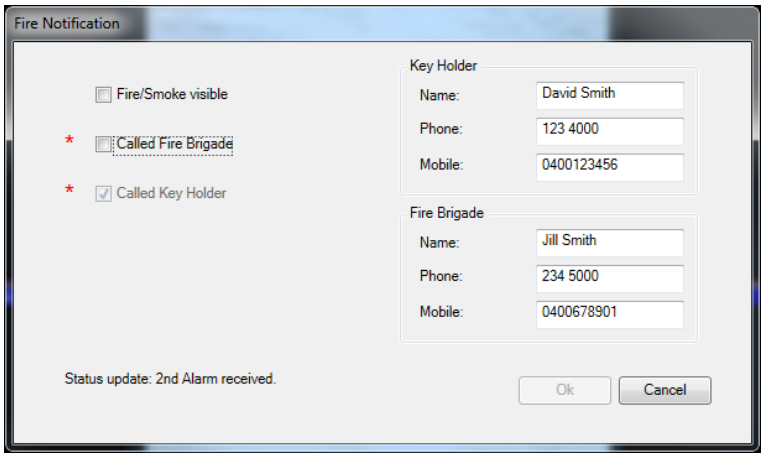
To create Diagrams refer to Section 2.21.

2.6.1.9 Fire Contacts

Fire contacts are displayed on the fire notification dialog when a fire event is processed by an operator progressing the state from ‘Call Keyholder’ to ‘Called Key holder’ and ‘Call Fire Brigade’ to ‘Called Fire Brigade’. Note while all details fields can be set only the Name, Phone and Mobile fields are displayed on the fire notification dialog.



Fire Notification Dialog Example

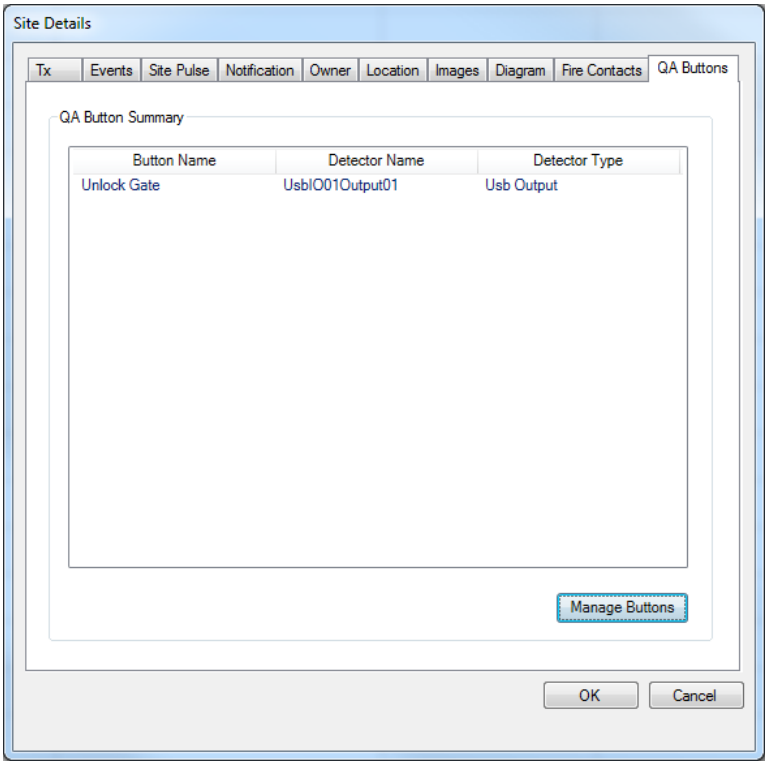


2.6.1.10 Quick Access Buttons

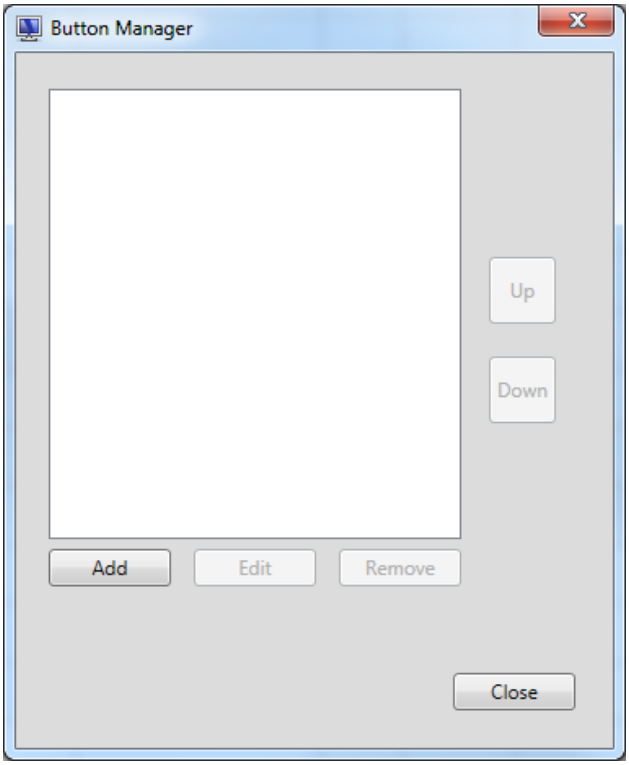
Site level Quick Access Buttons (QAB) allow the following functions to be programmed and allocated to a button.

- Control Outputs.

The programmed buttons are displayed on the event list when the respective site is selected. To add a QAB select the ‘Manage Buttons’ button within the QA Buttons tab.

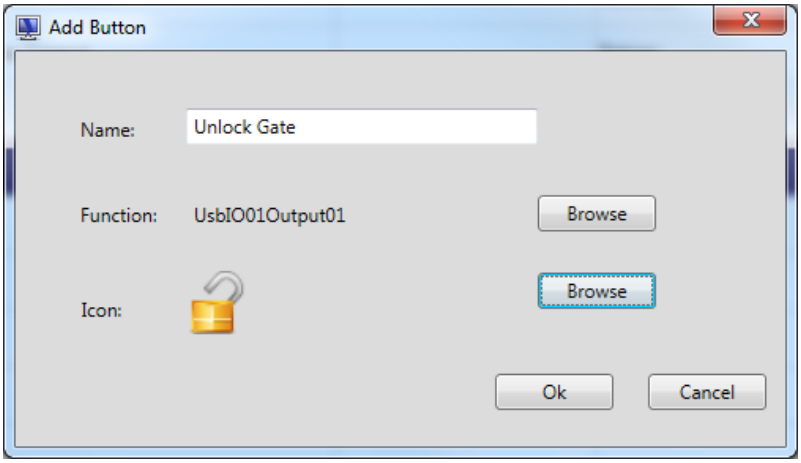


The button manager dialog will be displayed. Select the ‘Add’ button.

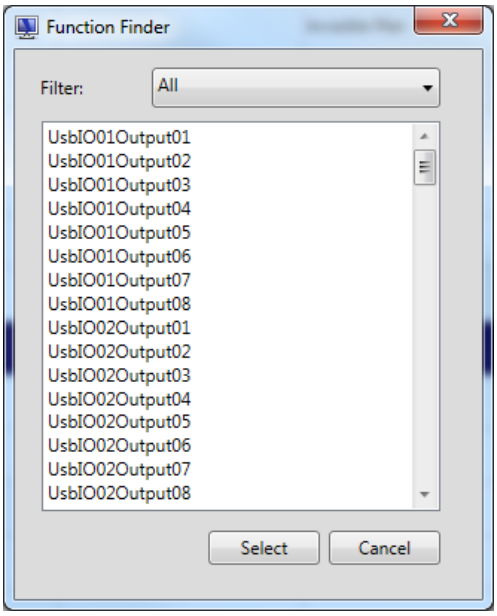


The Add button dialog will be displayed. Enter a name for the button (this will be displayed as hover text when the mouse is over the icon) and browse for an icon. The icon should ideally be 32x32 and in one of these formats; BMP, PNG, GIF, ICO.

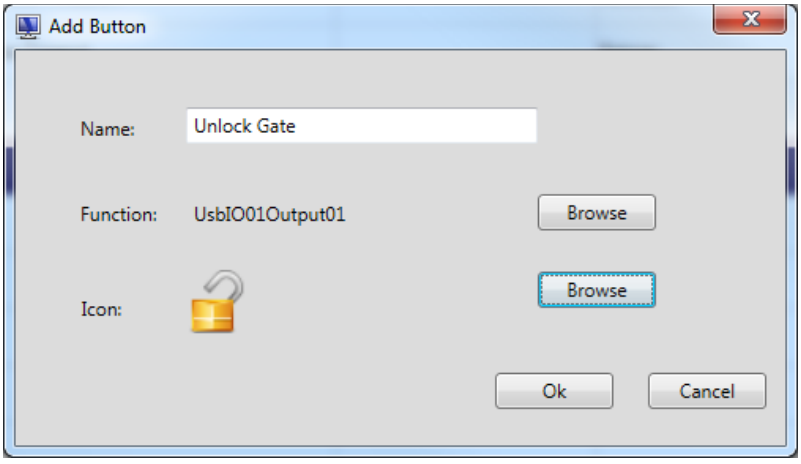
A large selection of icons are available for use on the VCP DVD under the following directory; \Support\Icons. Note these icons are only licensed for use within VCP.



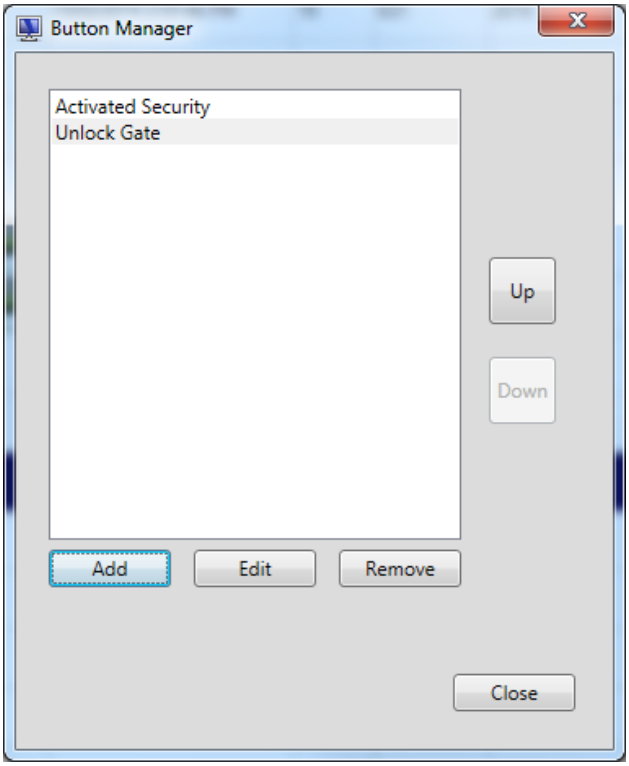
Select the ‘Browse’ button and allocate the USB or NET IO function to be activated when the button is selected in site view mode. Click on the function and press the ‘Select’ button. The Add button dialog will be displayed



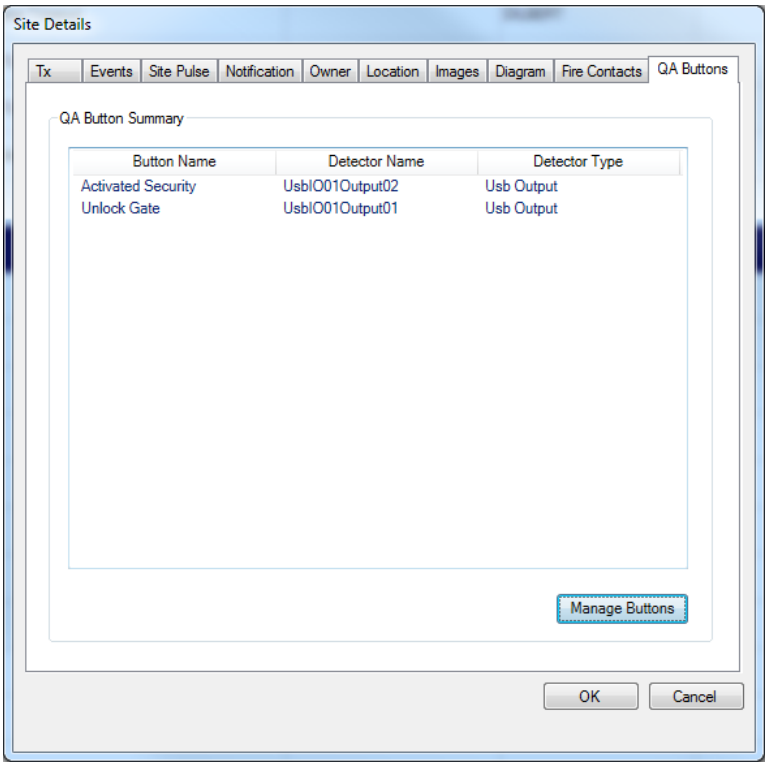
Select ‘OK’ and the Button Manager dialog will be displayed



Close the button manager and the Site details, QA button tab will be displayed.



Select the ‘OK’ button to complete and save the programming.

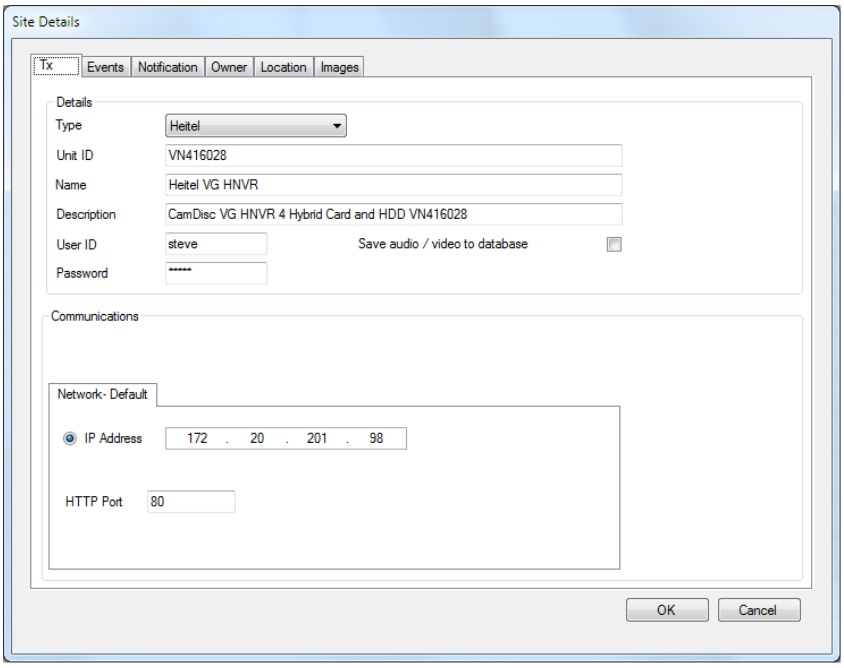


2.6.2 Adding New HeiTel Sites

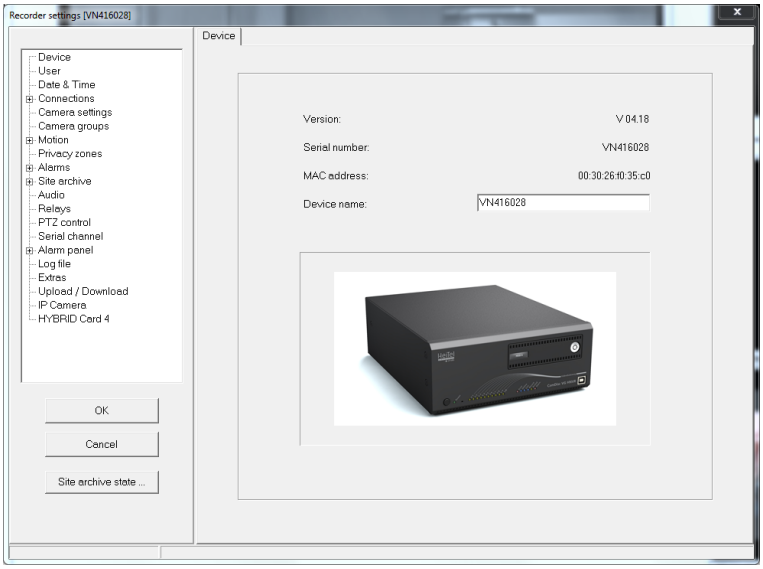
The process for adding HeiTel sites is the same as the procedures for ADPRO XO device sites as detailed from section 2.6. Since HeiTel support is limited to network connectivity the options are reduced.

Note: The Unit ID programming in VCP Site Details must match what is programmed in the HeiTel unit as the Device Name. It is recommended to use the HeiTel unit serial number as the device name.

Also see 2.4.1, Setup of CamControl Server for setup details if users have been programmed in the HeiTel unit.



HeiTel device name programming.



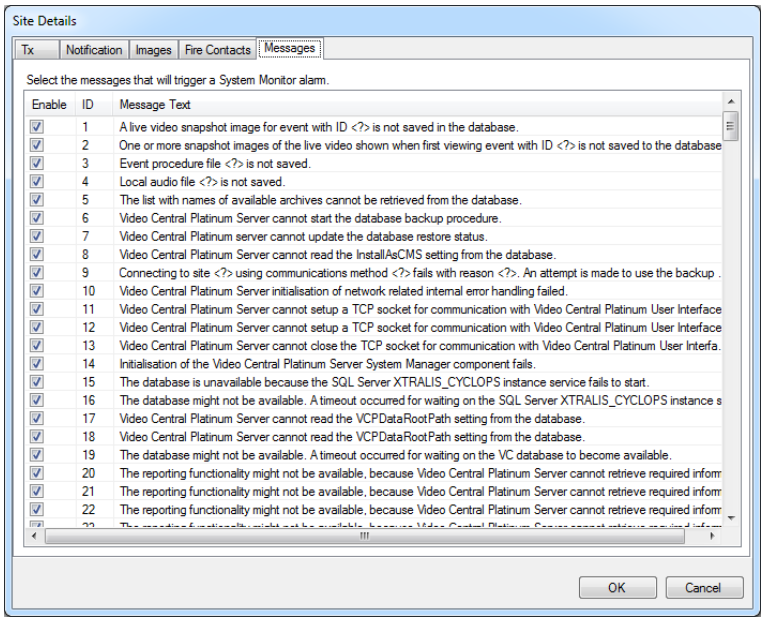
2.6.3 Editing Site Details

Access the Sites dialog via Tools > Administration > Sites then select the site to be edited and the **Edit** button will activate. Click **Edit** and the Site Details dialog will be displayed.

Make changes to this dialog as described in Section 2.6.1 Adding New Sites then click **OK** to save and exit.

2.6.4 System Monitor Message Configuration

System monitor messages can be enabled or disabled via the System Monitor site details' Messages tab.



If a message is enabled, a system monitor entry will appear on the ASL for this message.

If a message is disabled, there will be no system monitor entry on the ASL. However, the message will still be stored in the database, and will be listed as an acknowledged event on the System Monitor site.

An operator action will be logged when the user enables or disables a system monitor message.

Each system monitor event, that can be enabled/disabled, is uniquely identified by a message ID. This message ID will also be part of the message that is displayed on the System Monitor site.

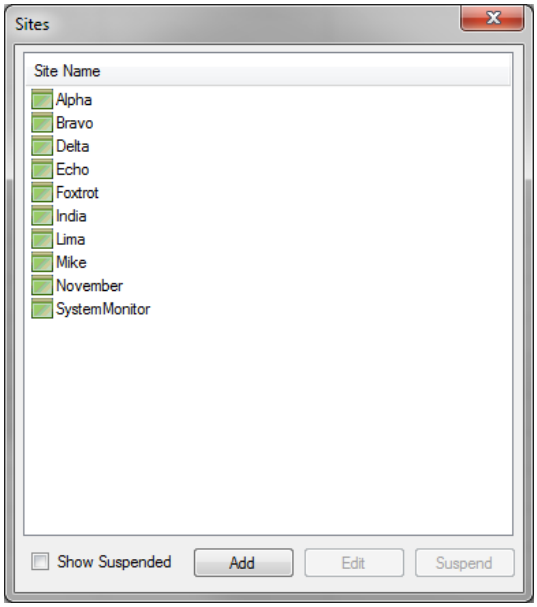
2.7 Suspending, Restoring and Deleting Sites

2.7.1 Suspending a Site

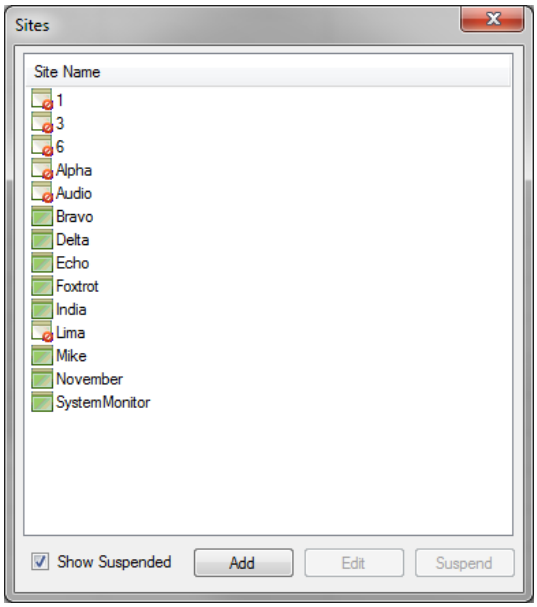
If a site is no longer required it may be suspended. Suspending a site means it will no longer be displayed within the ‘Connect to Site’ list. However it will not be deleted from the database and may be restored at a later date.

Access the Sites dialog via Tools > Administration > Sites.

To suspend a site, select the name under Site Name then click **Suspend**.

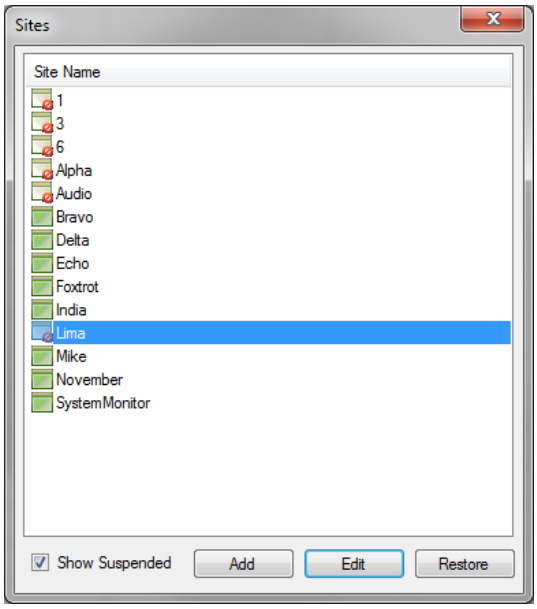


To view all suspended sites, check the Show Suspended dialog, which will be updated to show any suspended sites as ‘Lima’ in the example below.



2.7.2 Restoring a Site

To restore a site, select the name under Site Name then click **Restore**.



2.7.3 Deleting a Site

Sites and their associated events may be deleted at any time or as a scheduled task. Both methods use the Task Schedule Wizard, refer to the Maintenance Manual.

Note: Deleting a site will delete all alarm data including images.

2.8 Users Groups and Graphs

At a Central Monitoring Station (CMS) a User is any individual registered to access Video Central Platinum. Each User is assigned to a Group during setup. The Group to which the User is assigned is based on their area and level of responsibility. Some groups are predefined in Video Central Platinum and new groups can be created. If a new Group is required it must be created before Users can be assigned to it.

The relationship between Users and Groups is displayed in a Graph.

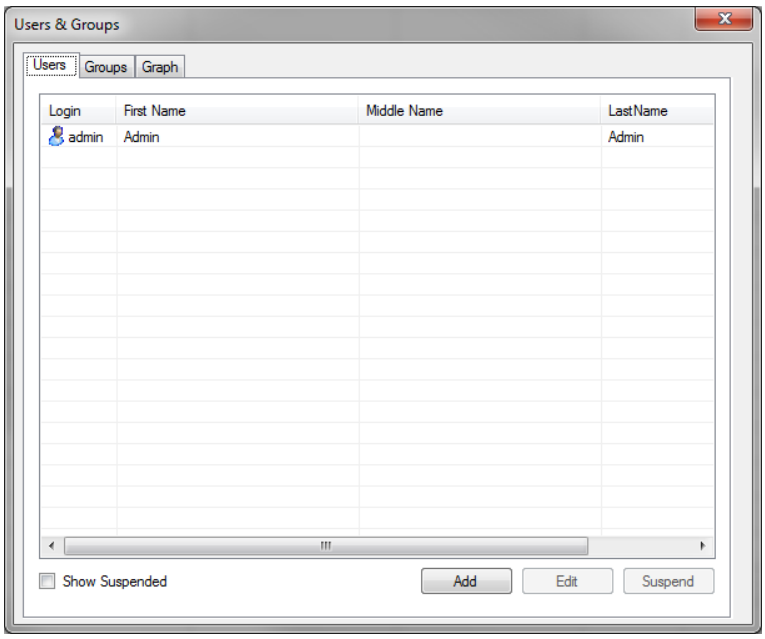
2.8.1 Adding and Editing Users

New Users can be added, details can be changed, or Users may be suspended.

2.8.1.1 Adding Users

Note: The default admin user password should be changed to maintain security.

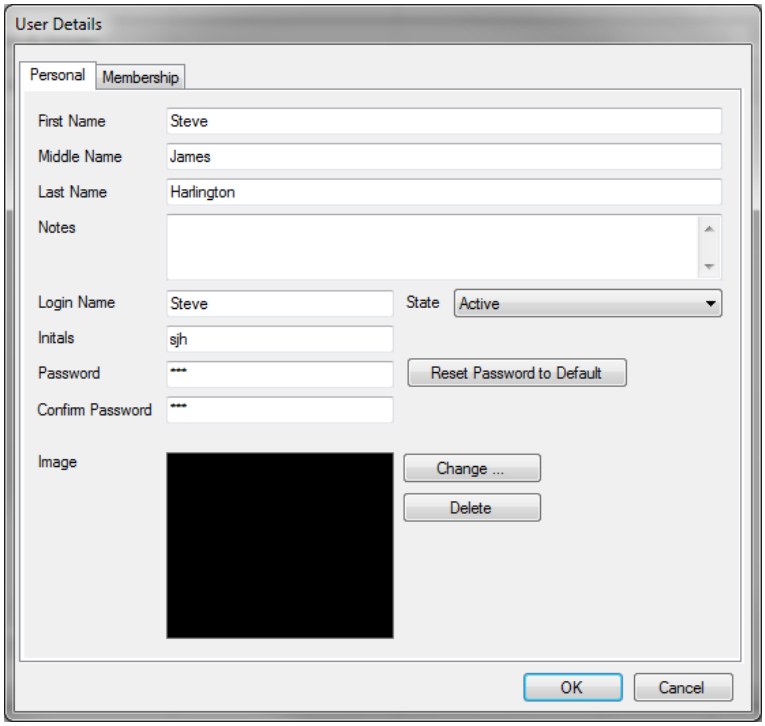
Access the Users and Groups dialog via Tools > Administration > Users & Groups. The Users tab will display all registered users. Click **Add** to display the User Details dialog.



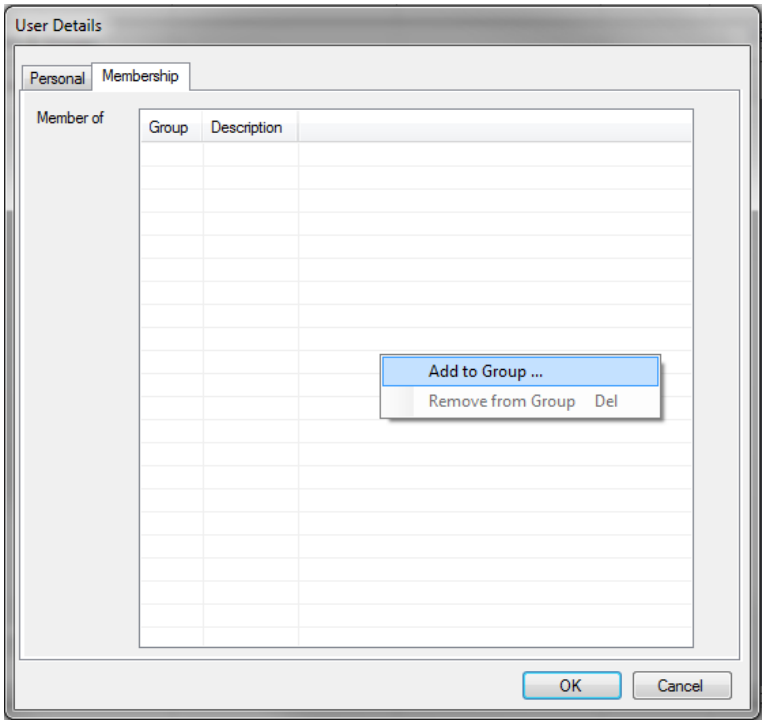
Under the Personal tab enter the new user's full name, login name, initials, and password. Select their state as being Active and make relevant notes such as their position or area of responsibility.

To add the user's photo click **Change** and navigate to the stored image.

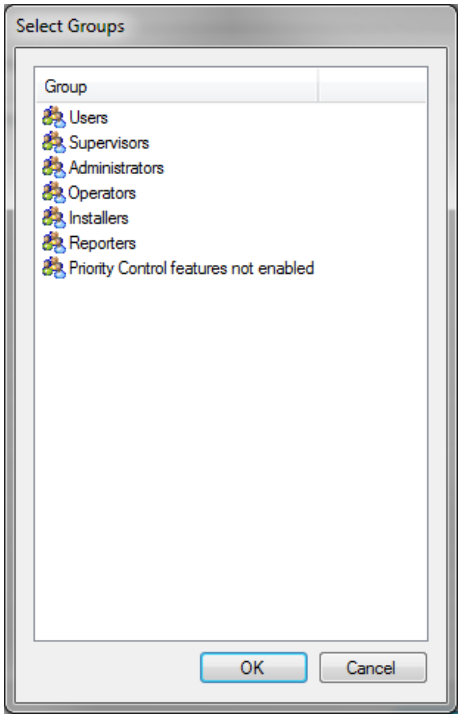
To remove any existing image click **Delete**.



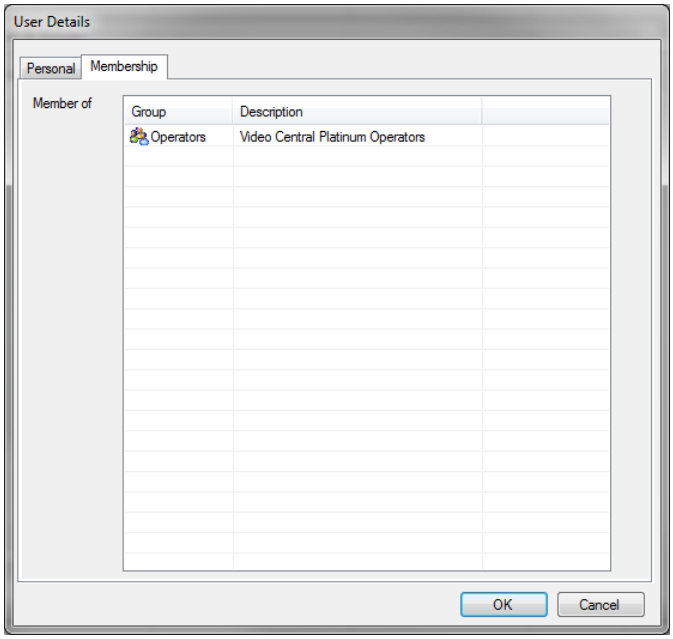
To assign the new user to a Membership group select the Membership tab, right click in the Group/Description area and a selection box will be displayed. Select Add to Group, click **OK** and the Select Groups dialog will be displayed.



The Select Groups dialog lists all Groups within Video Central Platinum. Select the group to which the new user is to be allocated then click **OK.**



The User Details, Membership dialog and the Users and Groups, User dialog will both display the group to which the new User has been allocated.



2.8.1.2 Editing User Details

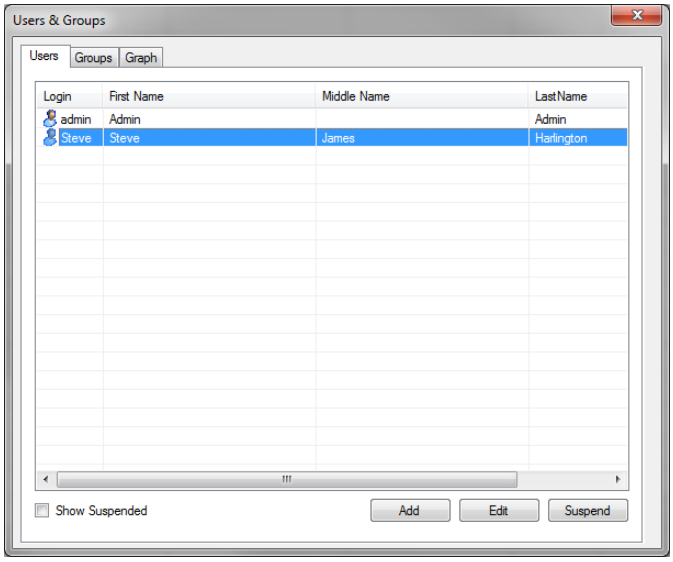
Access the Users and Groups dialog via Tools > Administration > Users & Groups. Under the Users tab select the user whose details are to be edited and the **Edit** button will activate. Click **Edit** and the User Details dialog will be displayed. Make the necessary changes then click **OK** to save and exit.

2.8.1.3 Suspending Users

Suspending Users removes their login from the Users and Groups list and from the Graph. To suspend a User, access the Users and Groups dialog, select the relevant row and click **Suspend**.

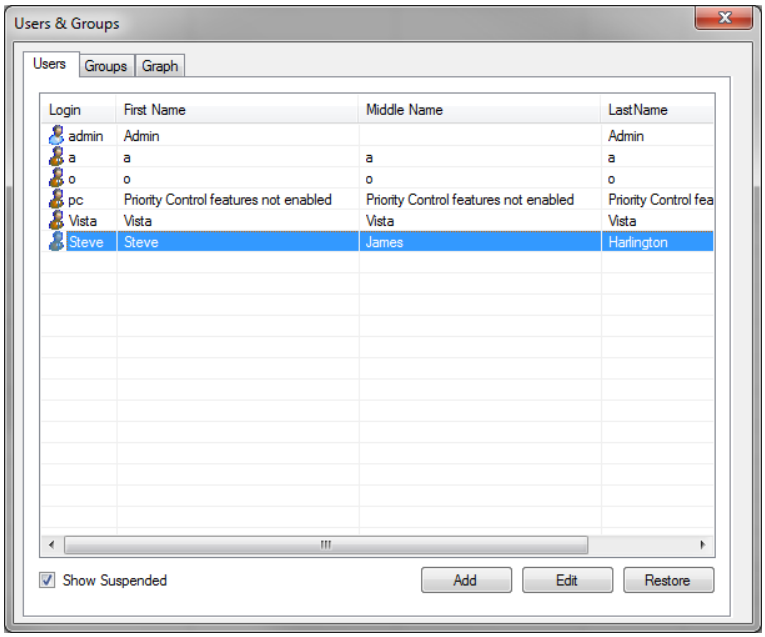
To display suspended Users in the list, check the 'Show Suspended' box. The suspended User's name will still be displayed in the list with the suspended status indicated by a change in the icon colour.

Details of suspended Users remain in the database and may be restored at any time.



2.8.1.4 Restoring Users

To restore a suspended User, access the Users and Groups dialog, select the ‘show suspended’ check box and then select the relevant row and click **Restore**.



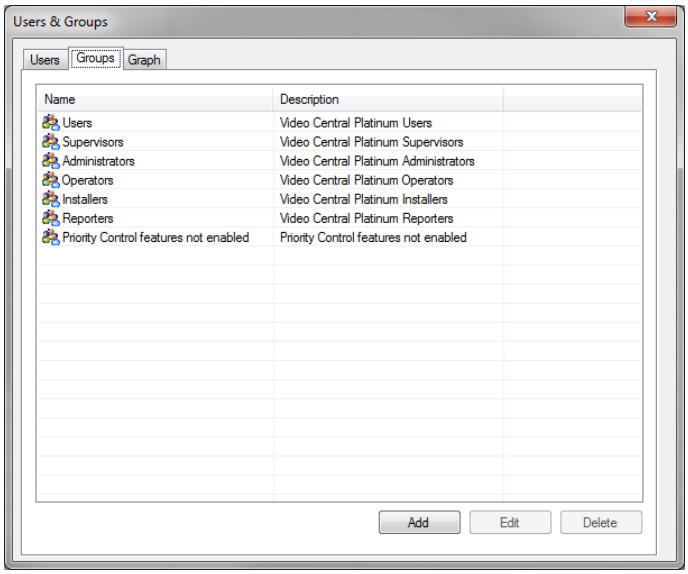
2.8.2 Adding or Editing Groups

New Groups can be added, their details may be changed, or they may be deleted from the system.

2.8.2.1 Adding New Groups

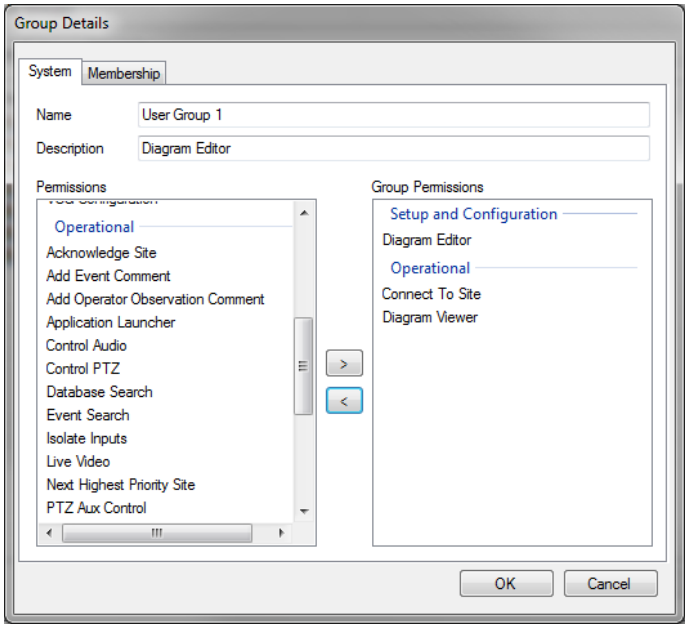
Access the Users and Groups dialog via Tools > Administration > Users & Groups. Select the Groups tab to display a list of all existing groups.

Note: Administrators, Operators, Installers, Users, Supervisors, and Reporters are predefined groups that appear on the list by default. Other groups may be created to suit the structure of the CMS. To create a new Group click **Add** and the Group Details dialog will be displayed.



Enter an appropriate name for the new Group and a description such as its area of responsibility.

Assign permissions for the Group by selecting from the Permissions list and adding to Group Permissions using the **'>'** key.

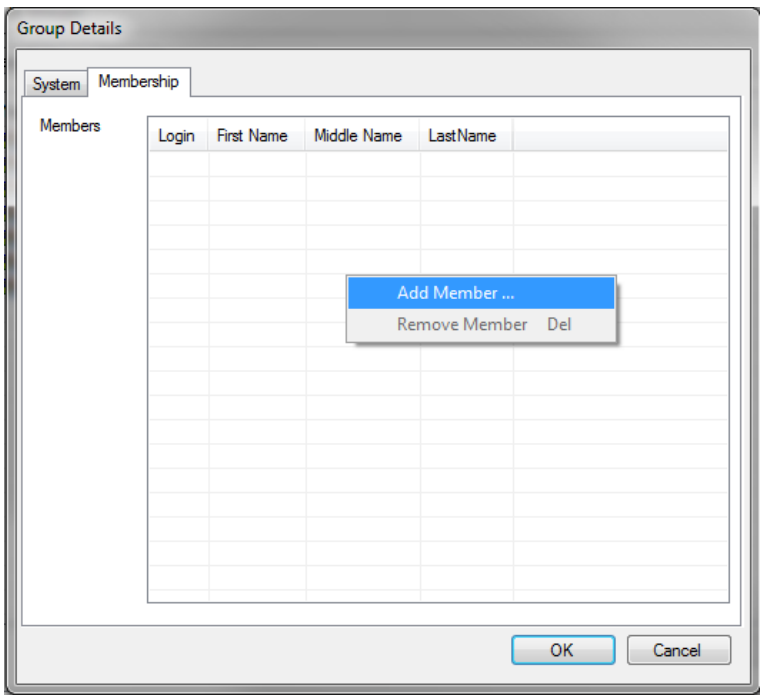


Permissions that are available to each group are defined in the following table:

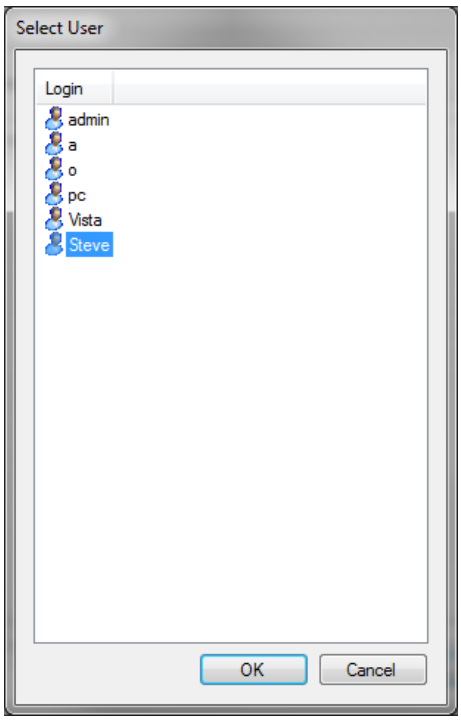
Feature	Administrator	Installer	Supervisor	Operator	User	Reporter
Setup and Configuration						
Basic Integration	✓	✓				
Change Password	✓	✓				
Diagram Editor	✓	✓				
Edit Site Records	✓	✓				
Edit User Records	✓	✓				
General Options	✓	✓				
Licence Features	✓	✓				
Modify PTZ Preset	✓	✓	✓			
Predefined Comments	✓	✓				
Private Wall Setup	✓	✓				
Setup Transmitter	✓	✓				
Task Scheduling	✓	✓				
User Interface Options	✓	✓				
Video Quality Setup	✓					
Operational						
Acknowledge Site	✓	✓	✓	✓	✓	
Add Event Comment	✓		✓	✓	✓	
Add Operator Observation Comment	✓		✓	✓	✓	
Application Launcher	✓	✓	✓	✓	✓	
Connect to Site	✓	✓	✓	✓	✓	
Control Audio	✓	✓	✓	✓	✓	
Control PTZ	✓	✓	✓	✓	✓	
Database Search	✓	✓	✓	✓		
Diagram Viewer	✓	✓	✓	✓	✓	

Feature	Administrator	Installer	Supervisor	Operator	User	Reporter
Event Hiding	✓	✓	✓	✓	✓	
Event Search	✓	✓	✓	✓		
Fire Reset	✓	✓	✓			
Fire Status	✓	✓	✓	✓	✓	
Isolate Inputs	✓		✓	✓		
Live Video	✓	✓	✓	✓	✓	
Next Highest Priority Site	✓	✓	✓	✓	✓	
Private Wall Operation	✓	✓	✓	✓	✓	
PTZ Aux Control	✓	✓	✓	✓		
QAB Functions	✓		✓	✓	✓	
Record Video	✓	✓	✓	✓		
Remote Arm/Disarm Site	✓		✓	✓		
Reports	✓	✓	✓			✓
Review Mode	✓	✓	✓	✓		
Save Still Image	✓	✓	✓	✓		
Site and Event Procedures	✓	✓	✓	✓	✓	
Site Details	✓	✓	✓	✓	✓	
Video Wall	✓	✓	✓	✓	✓	
View Inputs/Set Outputs	✓	✓	✓	✓	✓	
Maintenance						
Archive Database	✓		✓			
Maintain Database	✓		✓			

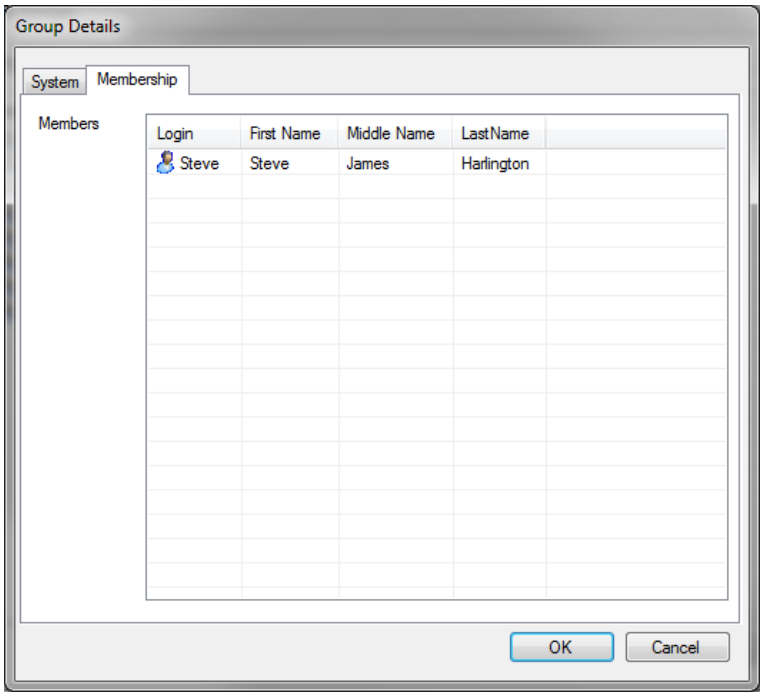
Add members to the Group by clicking the **Membership** tab, right clicking in the Membership dialog then selecting Add Member. The Select User dialog will be displayed.



Select the User then click **OK**.



The new member will be displayed in the Users & Groups dialog.



2.8.2.2 Editing Group Details

Access the Users and Groups dialog via Tools > Administration > Users & Groups. Under the Groups tab select the Group whose details are to be edited and the **Edit** button will activate. Click **Edit** and the Group Details dialog will be displayed. Make the necessary changes then click **OK** to save and exit.

2.8.2.3 Deleting Groups

Any Group that was created during setup can be deleted by selecting the Group name under the Groups tab and clicking **Delete**.

Of the predefined groups only Users and Supervisors can be deleted.

2.9 Displaying Graphs

A Graph gives a convenient visual representation of the mapping between Users and Groups at a Central Monitoring Station (CMS).

- The left column lists all groups - both predefined and newly created.
- The right column shows the Login names of all registered Users.
- The linkages show the Group or Groups to which each User belongs, noting that a User may belong to more than one Group.

Graphs are automatically created as users and groups are entered during setup. The mapping may be modified by re-allocating Users to Groups via the Users and Groups dialog tabs or by changing the Graph directly.

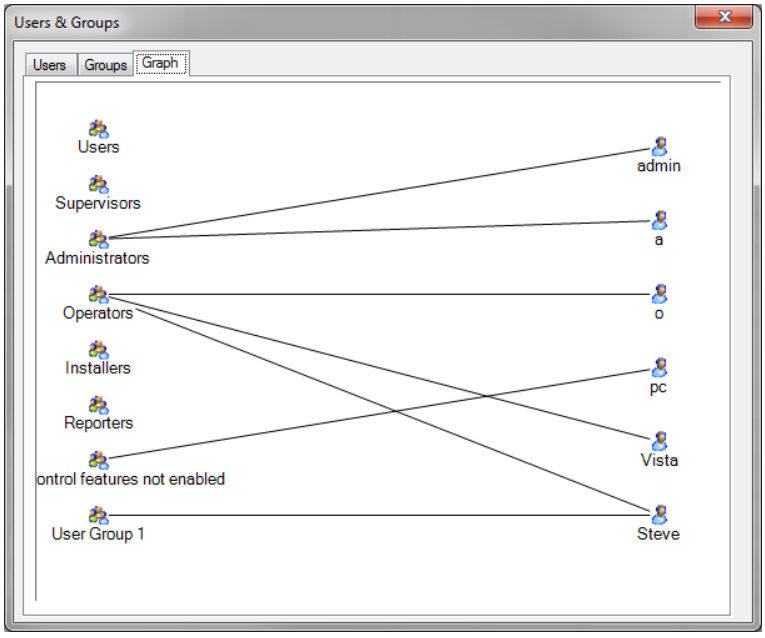
The Graph may be changed by dragging and dropping User or Group icons or by drawing and deleting linkages.

To change the position of an icon click on the title text then drag to the position required. The linkages between icons will remain intact wherever they are moved.

To create a new link, click on an icon graphic (not the text) then drag to another icon graphic to form a link. The icons will remain in place but a line will now connect them.

To delete a link, click to select the line then press the PC's Delete key.

Note: A User or a Group cannot be deleted directly from the Graph but only via the Users and Groups dialog.



2.10 Comments

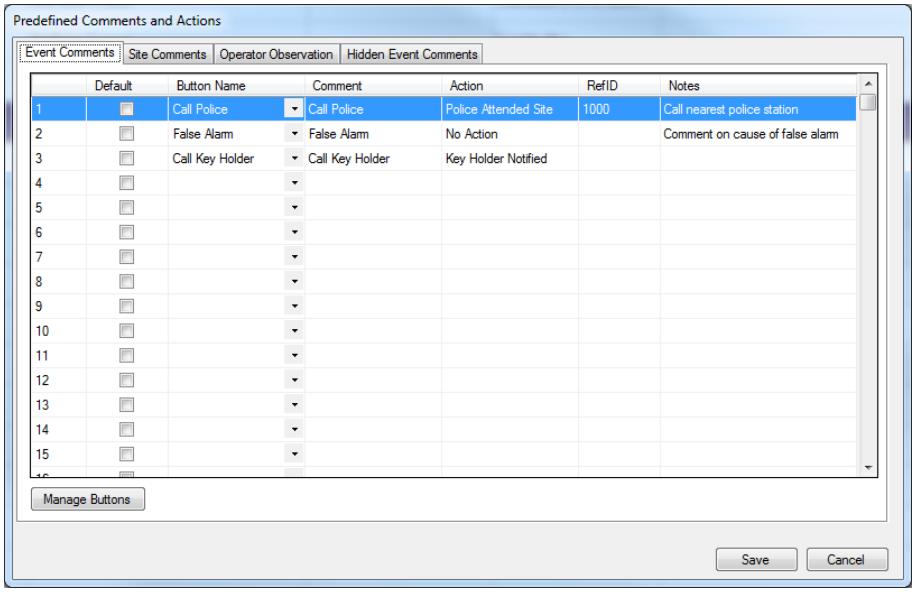
Four comment types can be entered by operators when viewing sites and responding to events:

- Event Comment – a comment related to a particular event.
- Site Acknowledgement Comment – entered when acknowledging a site at which alarms are present.
- Operator Observation – a general observation about the site.
- Hidden Event Comment – option when hiding an event type for a period of time.

2.10.1 Adding Pre-defined Comments

Predefining a list of comments and actions during setup allows them to be quickly allocated by operators.

Create predefined lists of Comments and Actions via the Active Sites List by selecting Tools > Administration > Database > Comments and the Predefined Comments and Actions dialog will be displayed.



Select each tab in turn and enter lists of possible Event Comments, Site Acknowledgement Comments, Operator Observation, and Hidden Event Comments. Click in the next blank space in the fields and enter the required text.

If wished, one comment in each group may be set as default by checking the adjacent default box.

For each comment and comment type a comment, action, reference (typically a number), and note can be added. Each comment can also be associated with a quick access button. See section 2.10.3.

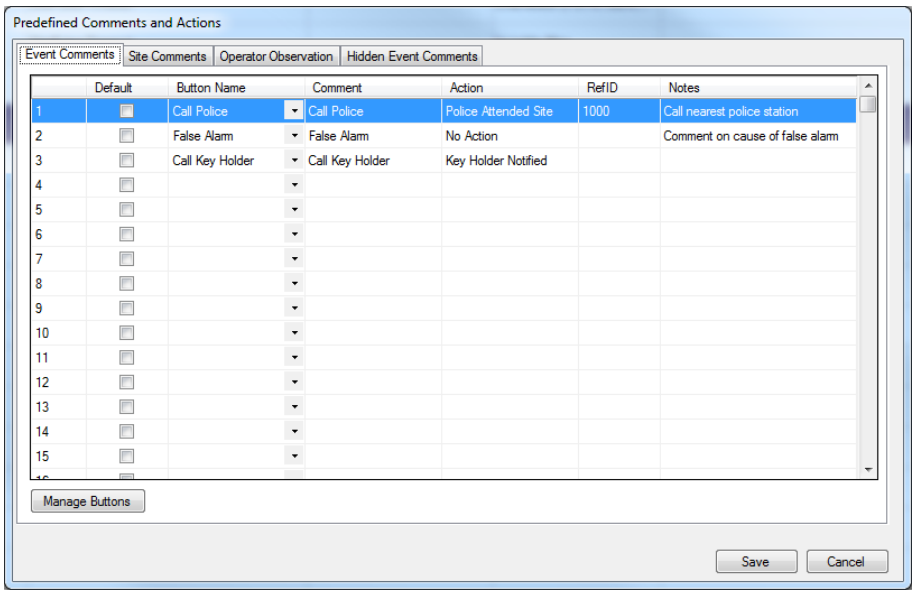
2.10.2 Deleting Comments

To delete comments remove all text from all fields including any associated QABs.

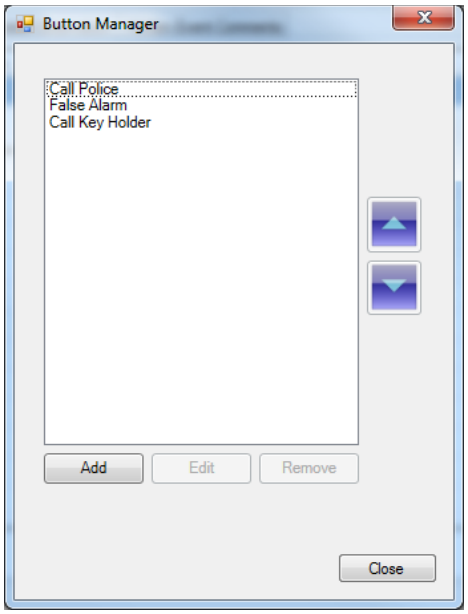
2.10.3 Adding Quick Access Buttons (QAB)

Each comment can be associated with a QAB which is represented as an icon in operational mode. Selecting icons in operational mode auto populates all fields for the respective comment. Up to 20 QABs can be setup for use for each comment type.

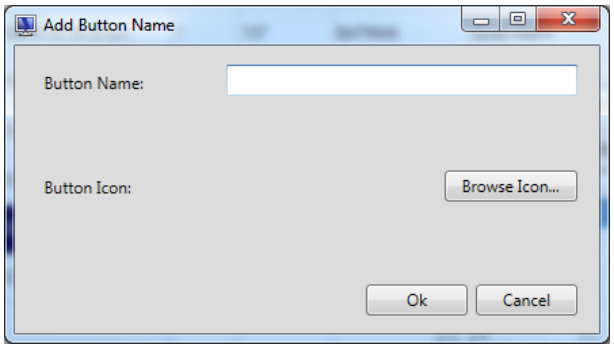
To add a QAB first select the required comment type tab (Event Comments, Site Acknowledgement Comments, Operator Observation and Hidden Event Comments) then select the ‘Manage Buttons’ button.



The Button Manager dialog will be displayed.

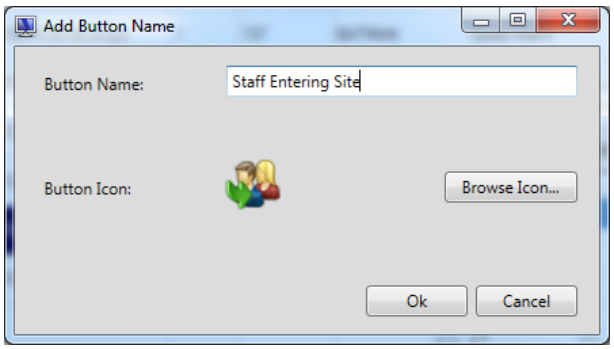


Select the ‘Add’ button and the add button dialog will be displayed.

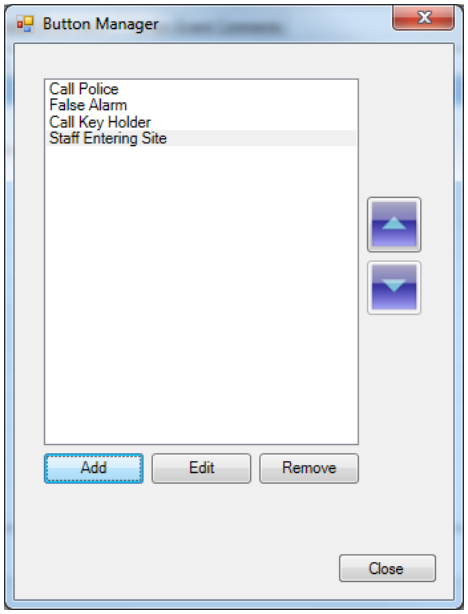


Enter a name for the button (this will be displayed as hover text when the mouse is over the icon) and browse for an icon. The icon should ideally be 32x32 and in one of these formats; BMP, PNG, GIF, ICO.

A large selection of icons are available for use on the VCP DVD under the following directory; \Support\Icons. Note these icons are only licensed for use within VCP.

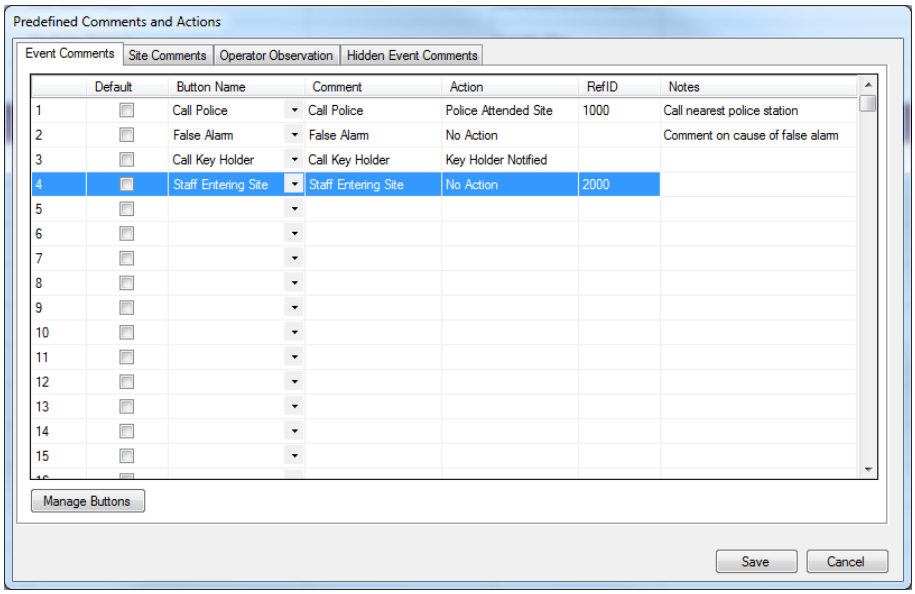


Once ‘OK’ has been selected the button for the selected comment type will be available for use.

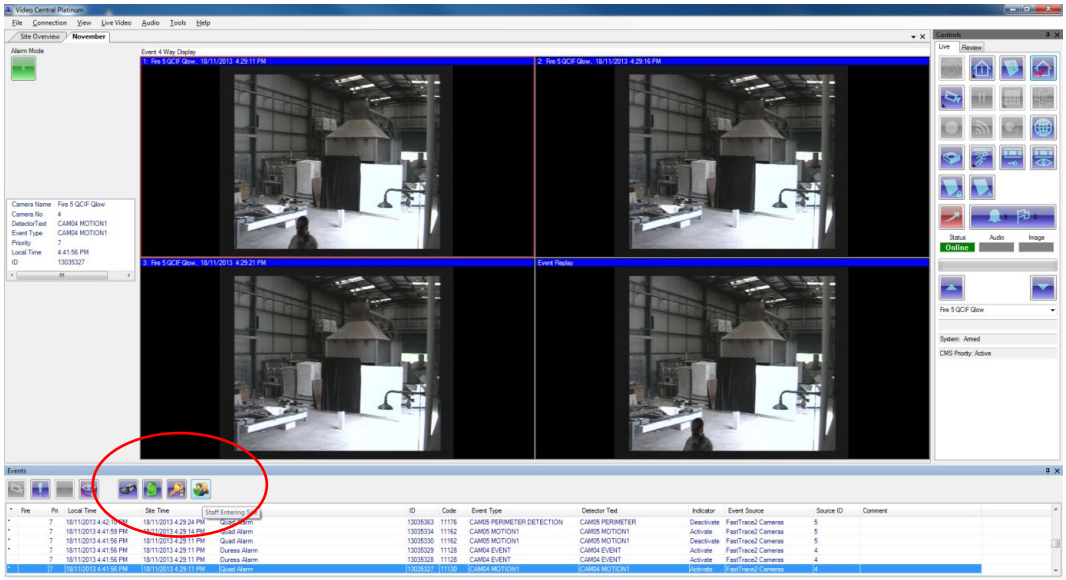


Select ‘Close’ to exit and return back to the Predefined Comments and Actions dialog.

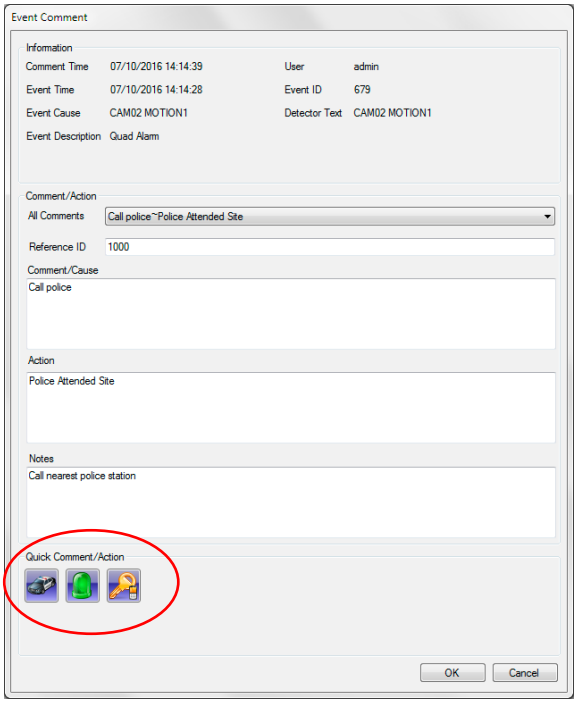
To associate a button with a comment select the drop down list within the ‘Button Name’ column and choose the required button.



Once the setup has been completed QABs will appear on their respective dialogs. The event comment QAB will also appear on top of the event list.



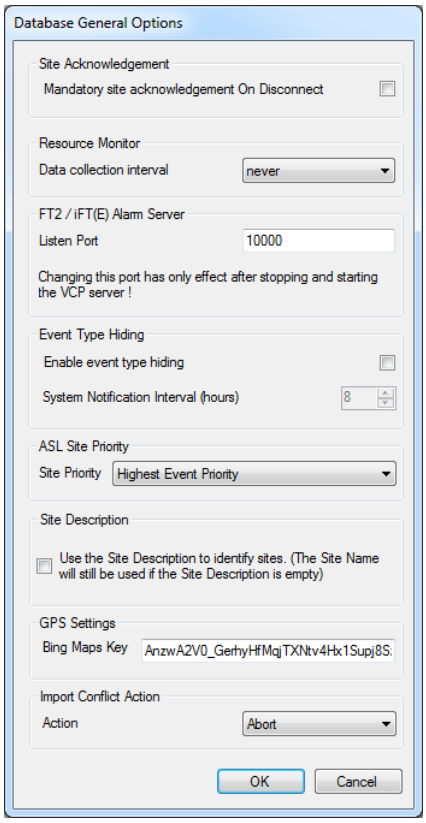
Event Comment Dialog Example;



2.11 General Options

General Options allows selection of mandatory site acknowledgement on disconnect, enabling of the Resource Monitor, ability to set the port on which alarms are received from the ADPRO XO device, enable the ability to hide events, set the Active Sites List (ASL) site priority or sort order, enable use of the Site Description to identify sites, set the Global Maps application Bing Maps key, and set the desired Import Conflict Action.

Access General Options via Tools > Admin > Database > General which; will display the Database General Options dialog.

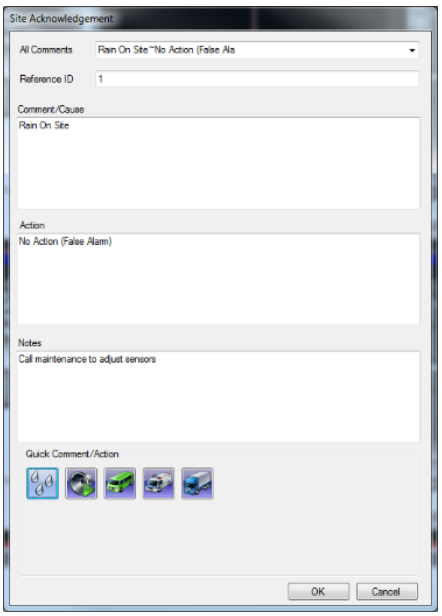


2.11.1 Mandatory Site Acknowledgement

The Site Acknowledgement comments dialog will be displayed when disconnecting from a site if this feature is enabled. If not enabled, disconnecting from the site will return directly to the Active Sites dialog.

Check the ‘Mandatory Site Acknowledgement on Disconnect’ dialog then click **OK**.

When disconnecting from a site with the feature enabled, a Site Acknowledgement dialog as the example shown below will be displayed.



2.11.2 Resource Monitor

This section describes how to enable the Resource Monitor and select the data collection interval during setup.

For a description of Resource Monitor functions, refer to 19118 Video Central Platinum Database and Maintenance Manual.

Access the data collection interval setting via Tools > Database > General. The Database General options dialog will be displayed.

The default value is ‘never’ which means the Resource Monitor is inactive. Setting the interval to any other value will activate the automatic data collection function. Select a time period from the drop down list, which ranges from one second to one hour, then click **OK**.

Note: Setting the Data Collection Interval to less than five seconds may reduce the performance of a heavily loaded system.

2.11.3 Alarm Server Port

Alarms are received on port 10,000 by default. If another application conflicts with this port it can be changed to another value. If the port value is changed, the setup of all ADPRO XO devices will need to be changed to match and the Video Central Platinum Server restarted.

2.11.4 Event Type Hiding

When the hide event from operator feature is turned on icons will appear on the top of the event list to enable the operator the ability to temporally hide events. The operator will be able to select an event in the event list and choose to hide the event type from operators for a period of time. While the event type is hidden and these event types are received by VCP they will be automatically acknowledged meaning the site will not appear in the Active Sites List if only these types are received. In site view mode the events shall appear as history events in the event list. The user may also reset the hide timer to re-enable the display of events prior to the natural timer expiration. By default, every 8 hours a sysmonitor event shall be created for hidden event types as a reminder. This interval can by modified through the System Notification Interval setting. If an operator arms a site when event types are hidden the option to rest will be provided. Hidden events are not sent out of the basic integration port.

This feature would be typically used when detectors become faulty causing a high false alarm load.

2.11.5 ASL Site Priority

In previous versions of Video Central Platinum (VCP) the Active Sites List sorting was based upon the Highest Priority and Time. The ASL Site Priority (or sort order) can now be set to;

- Highest Priority and Time
- Highest Unacknowledged Event Count
- Oldest Event Time
- Newest Event Time

When the Next Highest Priority button is selected in VCP the site selected will be based on the ASL Site Priority sort order. This feature is compatible with ADPRO XO, HeiTel, and Legacy sites.

2.11.6 Site Description

If this setting is enabled, instead of the site name, the site description will be used by the VCP User Interface for representing the site. Site name and site description are set in the Site Details dialog (see section 2.6).

2.11.7 GPS Settings

Set a Microsoft Bing Maps key here, in case usage of the Global Maps application is required. A Bing Maps key is required by the Global Maps application to be able to access the Bing map servers. To get a key you can visit https://www.bingmapsportal.com, or https://www.microsoft.com/maps/default.aspx.

2.11.8 Import Conflict Action

This setting is used to specify the action to perform when running into a conflict during import of VCP Server configuration data. A conflict can be considered as a situation where after the import the database would contain duplicate and/or conflicting data.

The following options exist:

- **Abort**: will stop the import. Any data that is already successfully imported at that point will not be rolled back.
- **Skip**: will skip the conflicting import data entry and continue with the next import entry.
- **Overwrite**: will overwrite the database data with the data from the import.

There are two types of import entries: site details and user details.

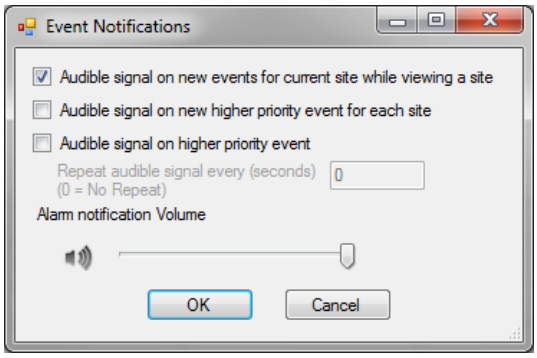
2.12 User Interface Options

Access via the Active Sites List by selecting Tools > User Interface Options;

- Event Notifications
- Event History
- Bounding Box Setup
- Remote Control
- Language Setup
- Quad Alarm Configuration
- Joystick Settings
- Global Maps Auto Start
- Column Visibility
- Active Sites List Options.

2.12.1 Event Notifications

Event notifications controls the audible annunciation of events.



2.12.1.1 Description of Event Notification Options

Option	Active Sites List (ASL)	Site View Mode
Audible signal on new events for current site while in site view mode.	not applicable.	Audio signal is played once for each new event for the site the operator is currently viewing.
Audible signal on new higher priority event for each site This option is mutually exclusive with *Audible signal on highest priority event*.	Play priority sound once if an event comes in for a site with a higher priority than the previous highest event priority for this site.	Play priority sound once if • an event comes in for another site with a higher priority than the previous highest priority event for this other site, *and* • the new event on the other site has a priority > highest event priority of site currently being viewed.
Audible signal on higher priority event This option is mutually exclusive with *Audible signal on new higher priority event for each site*.	Play priority sound once if an event comes in with a higher priority than the previous highest event priority.	Play priority sound once if • the event belongs to another site than the site currently being viewed, *and* • the event priority > highest event priority of site currently being viewed, *and* • the event has a priority > previous highest event priority.
Repeat audible signal Allows to enter a signal repeat interval t in seconds. This field is only enabled if *Audible signal on highest priority event* is checked.	Plays the priority sound for the highest priority event every t seconds. A value of 0 disables the repeat.	Plays the priority sound for the highest priority event every t seconds if • the event belongs to another site than the site currently being viewed, *and* • the event priority > highest event priority of site currently being viewed.

2.12.1.2 Examples

* Example 1

Audible signal on new events for current site while in site view mode ON
Audible signal on new higher priority event for each site OFF
Audible signal on higher priority event OFF
Repeat audible signal 0 (disabled on UI)

Currently viewing site A
site A priority 5 alarm => priority 5 sound
site A priority 3 alarm => priority 3 sound
site A priority 7 alarm => priority 7 sound
site B priority 8 alarm => no sound

* Example 2

Audible signal on new events for current site while in site view mode ON
Audible signal on new higher priority event for each site ON
Audible signal on higher priority event OFF (disabled on UI)
Repeat audible signal 0 (disabled on UI)

Currently viewing ASL
No alarms on ASL
site A priority 5 alarm => priority 5 sound
site A priority 3 alarm => no sound
site A priority 7 alarm => priority 7 sound
site B priority 2 alarm => priority 2 sound
site C priority 8 sound => priority 8 sound
site C priority 8 sound => no sound

Connect to site A
site A priority 5 alarm => priority 5 sound
site A priority 3 alarm => priority 3 sound
site A priority 7 alarm => priority 7 sound
site C priority 8 alarm => no sound
site B priority 6 alarm => no sound
site B priority 7 alarm => no sound
site C priority 9 alarm => priority 9 sound

* Example 3

Audible signal on new events for current site while in site view mode OFF
Audible signal on new higher priority event for each site OFF (disabled on UI)
Audible signal on higher priority event ON
Repeat audible signal 0

Currently viewing ASL
No alarms on ASL
site A priority 5 alarm => priority 5 sound
site A priority 3 alarm => no sound
site A priority 7 alarm => priority 7 sound
site B priority 2 alarm => no sound
site C priority 8 sound => priority 8 sound
site C priority 8 sound => no sound

Connect to site A
site A priority 5 alarm => no sound
site A priority 3 alarm => no sound
site A priority 7 alarm => no sound
site C priority 8 alarm => no sound
site B priority 6 alarm => no sound
site B priority 7 alarm => no sound
site C priority 9 alarm => priority 9 sound
site A priority 10 alarm => no sound

* Example 4

Audible signal on new events for current site while in site view mode ON
Audible signal on new higher priority event for each site OFF (disabled on UI)
Audible signal on higher priority event ON
Repeat audible signal 5

Currently viewing ASL
No alarms on ASL
site A priority 5 alarm => priority 5 sound
every 5 seconds play priority 5 sound (start first play 5 seconds after receiving event)
site A priority 3 alarm => no sound
site A priority 7 alarm => priority 7 sound
every 5 seconds play priority 7 sound
site B priority 2 alarm => no sound

site C priority 8 sound => priority 8 sound

every 5 seconds play priority 8 sound

site C priority 8 sound => no sound

Connect to site A

keep playing priority 8 sound every 5 seconds

site A priority 5 alarm => priority 5 sound

site A priority 3 alarm => priority 3 sound

site A priority 7 alarm => priority 7 sound

site C priority 8 alarm => no sound

site B priority 6 alarm => no sound

site B priority 7 alarm => no sound

site C priority 9 alarm => priority 9 sound

every 5 seconds play priority 9 sound

site A priority 10 alarm => priority 10 sound

stop repeating priority 9 sound

site C priority 10 alarm => no sound

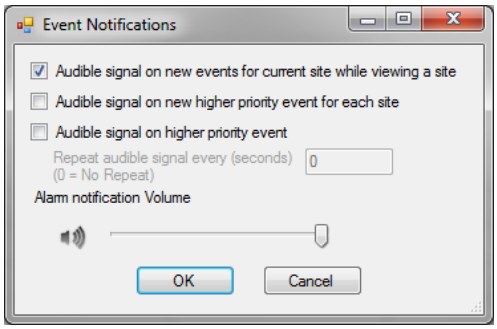
site C priority 11 alarm => priority 11 sound

every 5 seconds play priority 11 sound

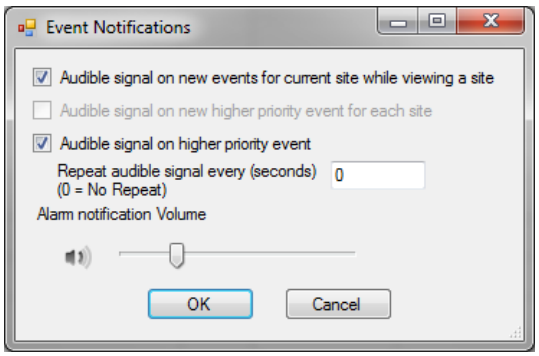
2.12.1.3 Alarm Notification Volume

The alarm notification volume allows each user interface to adjust the volume so the event notification and site audio volume match in level.

1. Connect to a site and turn on site audio. Adjust the computers volume through Windows until the required level is set.
2. Disconnect from the site.
3. From the Video Central Platinum User Interface select Tools > User Interface Options > Event Notifications and the Event Notifications options will be displayed.



4. Adjust the Alarm Notification Volume by dragging the slider control to the left to match the volume of the site audio. Typically between a quarter and half volume will be suitable.



5. Repeat the process for each Video Central Platinum User Interface.

2.12.2 Event History

The Event History dialog controls the retrieval and display of past events within the Events List whilst in Site View mode. After retrieval these are displayed in the selected Historic Event Colour at the bottom of the Events list.

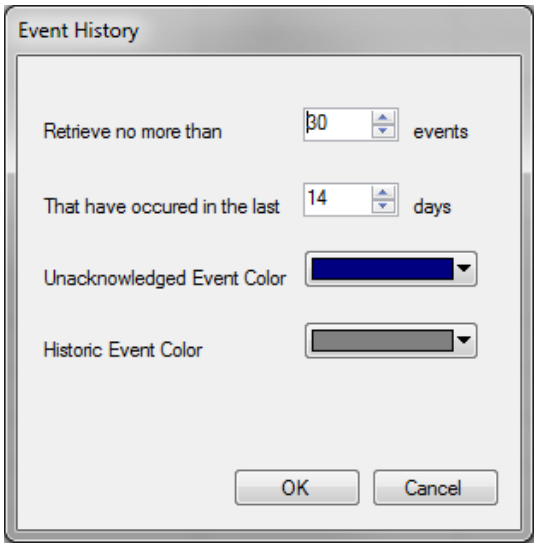
Set the maximum number of history events to be retrieved and displayed in the Event List using the ‘Retrieve no more than xxx events’ thumbwheel.

Set the retrieval time period using the ‘That have occurred in the last xxx days’ thumbwheel. This will determine how far back in time the historic events will be included in the Events List.

Choose a colour for unacknowledged or active events via ‘Unacknowledged Event Colour’.

Choose a colour for historic events via ‘Historic Event Colour’ then click **OK**.

Note: The colour of the events will be red for Live Alarms if the user does not have access to the camera.



2.12.3 Bounding Box Setup

2.12.3.1 Alarm Images

The bounding box feature allows detection tracking to be displayed within quad and duress alarms for ADPRO XO Fire Detection, Perimeter Detection, and Loitering event types. This feature is available for the respective event types displayed within Site View Mode and Event Search.

Note: Fire Detection, Perimeter Detection, and Loitering are licensed features of ADPRO XO.

Important: Bounding boxes will only be displayed for the ADPRO XO Perimeter Detection and Loitering event types if the ADPRO XO device is fitted with version 2.03 or greater. For Fire Detection, version 2.04 or greater is required.

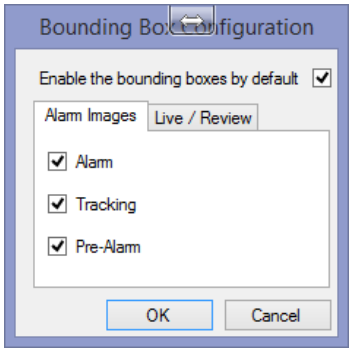
Setup is performed through the Tools > User Interface Options > Bounding Box Setup. The ‘Enable the bounding boxes by default’ option controls the display of tracking or bounding boxes on quad and duress

Fire Detection, Perimeter Detection and Loitering event types displayed in Site View Mode. It turns on display of bounding boxes when Video Central Platinum is started if the check box is selected.

Once Video Central Platinum is running and in Site View Mode the bounding boxes can be manually turned on or off as required for Site View Mode Alarms through the Video Central Platinum User Interface either via the Ctrl – B shortcut key or the View > Bounding Boxes menu.

The Alarm Images bounding box setup allows to enable or disable analytics bounding box types individually. Check or uncheck the individual checkboxes to do so. Note that the “Enable the bounding boxes by default” setting overrules the individual settings: if you disable this option, no bounding boxes will be shown. When it is enabled, the bounding boxes will show as configured.

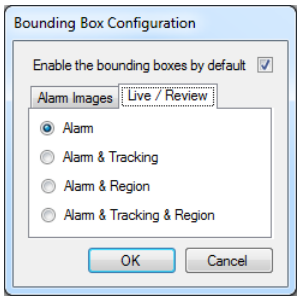
Note: Bounding boxes are always displayed when displaying, exporting or printing through the Event Search feature (Tools > Event Search). Since the bounding boxes are not part of the raw image bounding boxes cannot be displayed within incident reports.



2.12.3.2 Live / Review

The Live/Review setup is about enabling/disabling bounding boxes when viewing live video, or when reviewing recorded video.

Live/Review setup only allows a limited number of combinations. Therefore, the options are provided as a number of radio buttons. There are 3 types of analytics bounding boxes for live and review: Alarm, Tracking, and Region. The radio buttons represent the combinations which are supported by the XO SDK. The SDK also does not allow to change the bounding box colours for live and review video.



2.12.4 Remote Control

Refer to VCP UI Controller 2.15.3.

2.12.5 Language Setup

The language can be set to the following options within each Video Central User Interface. (English, French, Dutch, German, Chinese, Japanese, Polish)

Note while most text is translated there are some limitations;

- All text that comes from the database is not translated (Active Sites List and Event List for example).
- Diagram Editor left hand object pane and Macro Language.
- Live Video and Alarm Replay Viewer accessed from Event Search.
- Secure Viewer.

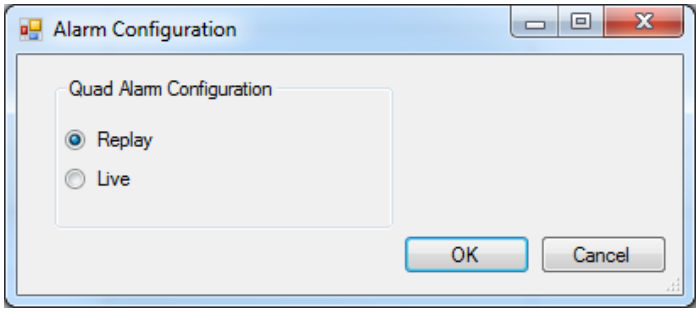


When selecting a language it might be important to take into account the sub language. While the sub language generally would refer to a variant of the parent language, this is not the case for VCP.
E.g. selecting a different sub language for English will not change the English translation used in VCP. However, changing the sub language will affect regional settings that are used for displaying certain information such as dates for example. The format of dates can be important when ordering data from different sources. For example when the Active Sites List contains entries from VCP sites. If ordering of the ASL is based on date information, then it is important that VCP uses the same regional settings.

2.12.6 Quad Alarm Configuration

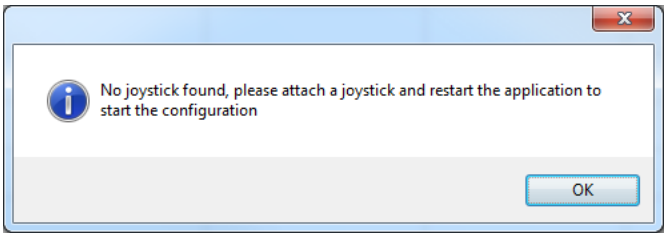
The behaviour for the fourth alarm quad can be setup to display either;

- a replay of the first three alarm images
- a live view of the camera channel in alarm.

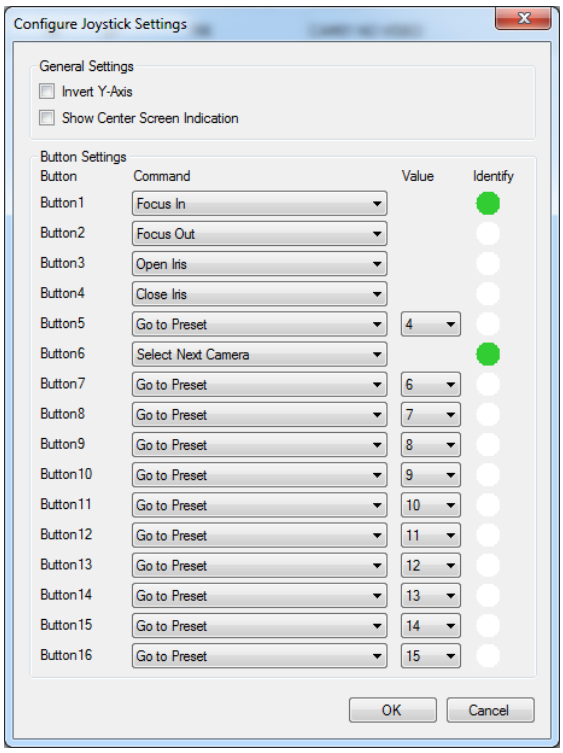


2.12.7 Joystick Settings

A joystick can be connected to the user interface PC to control PTZ camera stations. The joystick must be connected prior to starting Video Central Platinum.



The action buttons on the joystick can be assigned to PTZ functions. Use the configure joystick buttons dialog to setup the joystick. Clicking a joystick action button will cause the corresponding button in the setup to highlight the identity green.



Select the “Invert Y-Axis” checkbox to invert the up/down movement when using PTZ.

Select the “Show Center Screen Indication” checkbox to display a crosshair at the centre of the screen, when using PTZ.

2.12.8 Enabling Auto Maximise on Event

If Video Central Platinum is minimised, a function is provided whereby it is automatically maximised when an event occurs. This function is disabled by default and if required, must be enabled as follows:

Access the file VCPClientConfig.xml.

The location of this depends on the operating system of the computer in use:

- C:\ProgramData\ADPRO VCP\VCPClientConfig.xml

Open in Notepad.

Under ‘UserInterfaceOptions’ locate the command string:
<VCPClientMaximisedWhenAlarm>**false**</VCPClientMaximisedWhenAlarm>.

Change the word ‘**false’** to ‘**true’** then save and exit Notepad**.** The auto maximise function will now be active.

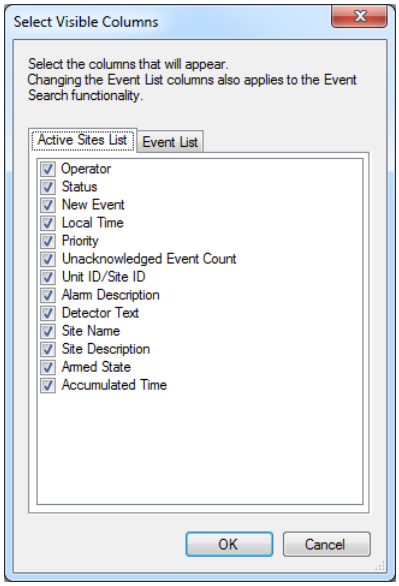
2.12.9 Global Maps Auto Start

If the Global Maps Auto Start flag is set, the Global Maps application will automatically start when launching the VCP User Interface application. Likewise, it will automatically close when shutting down the VCP User Interface application. If there is a checkmark next to this setting on the menu item (Tools > User Interface Options > Global Maps Auto Start), it means auto start is enabled.

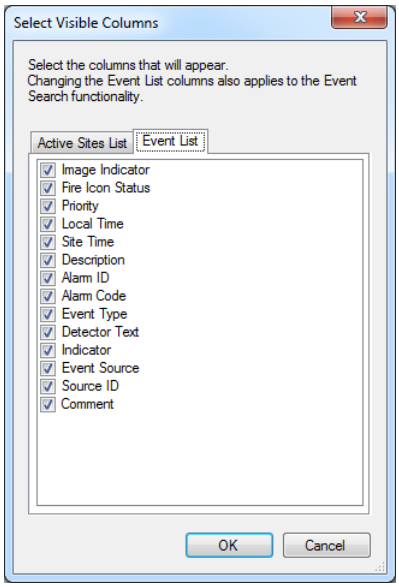
2.12.10 Column Visibility

This option allows to select which columns need to be visible on the Active Sites List, and on the Event List which is used in site view mode and for event search.

Configurable columns on the Active Sites List:

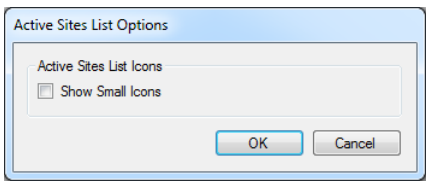


Configurable columns on the Event List:



2.12.11 Active Sites List Options

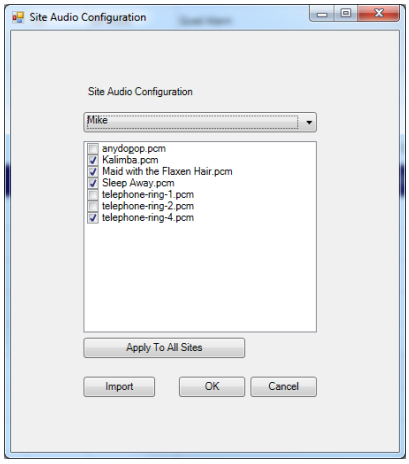
This option allows to set the site of the icons that are used on the ASL, either 32x32 icons or 16x16 icons (small icons). When using small icons, more ASL row entries will be visible without needing to scroll down the list.



2.13 Local Audio Setup (Play audio file to site)

Select Tools > Administration >Local Audio Setup to import audio files and associate them with the required sites. Once audio files are associated with sites they will appear when an operator right clicks on the Local Audio button  in site view mode. To setup;

- Import all required audio files (files must be .mp3 or .wav format)
- Select a site then check the required checkboxes.
- If these setting are required for all sites select the 'Apply To All Sites' button.
- Select the next site are repeat the process.



2.14 ADPRO XO Device Setup Options

All ADPRO XO device setup options are set via the XO Client. The XO Client can be run from the Windows Desktop or from within Video Central Platinum. To access the XO Client from within Video Central Platinum Connect to the respective Site and select the Site Actions Icon followed by Installer Menu. The XO Client will then launch within a Web Browser.

The following ADPRO XO device settings are important as they affect the ability for Video Central Platinum to connect or receive alarms from an ADPRO XO device.

Note: The default XO Client UserName is '0' and Password is '666777'.

2.14.1 Ethernet / PPP

The Ethernet/PPP settings determine the IP Address and port connection information of the ADPRO XO device. The following settings are mandatory:

- IP Address
- RTSP Port
- Control Port
- Web Server Port.

Set the parameters as follows:

When programming a site in Video Central Platinum set the IP Address to match that set at the ADPRO XO device.

The RTSP Port is fixed at 554 and must not be changed.

The Control Port is fixed at 2000 and must not be changed.

The Web Server Port is fixed at 80 and must not be changed.

2.14.2 Alarm Transmission

The alarm transmission settings determine the IP address and connection information when the ADPRO XO device needs to connect to Video Central Platinum to send alarms. The following settings are mandatory:

- Activate Alarm Transmission
- Destination IP Address.
- Destination IP Port
- CMS ID
- ADPRO XO device Unit ID
- Site Name

Set the parameters as follows:

- Typically, Primary Ethernet.
- IP Address of the Video Central Platinum Server.
- The Destination IP Port is fixed at 10000 and must not be changed.
- The CMS ID is fixed at 3141593 and must not be changed.
- The Unit ID programmed at the ADPRO XO device must be set the same when programming a Video Central Platinum Site. The Unit ID must be unique.
- The Site Name programmed at the ADPRO XO device must be set the same when programming a Video Central Platinum Site. The Site Name must be unique.

2.14.3 Alarm Profile

Alarm profiles are associated with input/outputs behaviour and determine:

When an alarm is sent to Video Central Platinum depending on the arm/disarm state.

What communications medium is used.

If a Repeat Tx alarm event is to be sent.

If a trigger deactivate event is to be sent. If this option is programmed off, a single event will be sent to Video Central Platinum per trigger which will be listed as an activate event within the Video Central Platinum event list indicator column. If programmed on, two events will be sent to Video Central Platinum per trigger which will be listed as an activate and deactivate event within the Video Central Platinum event list indicator column.

In order for Video Central Platinum to receive alarms the profile associated with the input/output behaviour must have the following minimum settings:

Operational State typically Armed.

Alarm Behaviour, Armed and Primary Transmission checkbox selected.

2.14.4 Input/Output Behaviour

The input/output behaviour setup of the ADPRO XO device determines:

What alarm (event) type is sent to Video Central Platinum as determined by the alarm profile.

What logic determines the activation of an input/output that are sent to Video Central Platinum.

What alarm type is sent to Video Central Platinum (Quad, Live or Duress).

What video channel is associated with the input/output.

Note: Input/outputs are referred to as alarm or event types at Video Central Platinum.

In order for Video Central Platinum to receive alarms correctly the following setup should be programmed:

Alarm Profile as setup previously. Normally the Normal Profile would be used.

Program the logic that determines when the trigger is activated. Normally for example the CAM01 Event Input/Output would be associated with either the CAM01 MOTION1, USB-1 INPUT01 Real, Digital Input E0001 or CAM01 Presidium Det.

Set the Camera View Style as either Quad, Live or Duress alarm type.

Associate one of more Cameras.

Note: If no camera is associated with an input/output type the alarm will be displayed within the Video Central Platinum event list description column as Quad Alarm – No images available.

2.14.5 Quad Image Interval

The quad image interval determines the period between the three static images captured at the ADPRO XO device for quad alarms. The site global default value is .2 second however this value can be altered up to 5 seconds.

Note: If this value is changed the Video Central Platinum Server will need to be re-started.

2.14.6 ADPRO XO Device Audio Setting

ADPRO XO device Audio uses 32 Mbits of bandwidth, therefore if your network connection has less than 256 MHz of bandwidth, and if audio is not used, it is highly recommended that you turn off each of the channels in the ADPRO XO device Audio section.

2.15 Central Monitoring Station Integration

2.15.1 Basic Integration

2.15.1.1 Overview of Basic Integration

Basic Integration configures Video Central Platinum to communicate with a Central Monitoring Station Computer (CMSC) via a serial communications link or TCP/IP socket. Events are translated into ADEMCO Contact ID or SIA codes and sent to the CMS via a communications link. The CMSC displays these codes in the same way as events from a commercial alarm panel.

The CMSC software can log all alarm events thus providing one central database for events and reporting of all systems.

Day to day operation involves minimal attention from Video Central Platinum Operators. Events with no associated video are automatically logged to the database and passed to the CMSC. These events are dealt with and acknowledged at the CMSC workstation in the same fashion as the CMSC operator would normally deal with alarms. These events do not appear at Video Central.

Events with video are also automatically logged to the database and passed to the CMSC but require review and acknowledgement on the Video Central Platinum workstation as well as acknowledgment at the CMSC workstation.

Note: Events with video do not require review or acknowledgement at Video Central Platinum if the AcknowledgeQuadAlarms = Yes option is set.

When video events are received from a site, or an operator is connected live to a site, the site is placed on the ‘Active Sites List’. If there is more than one active site, there will be more than one site on the list. The operator is able to view events by selecting a site from the list.

The site can be acknowledged, which will remove it from the list, or the operator can put it back on the list to be acknowledged later. The operator is then free to select another site from the list or connect live to another site. The Video Central Platinum Operator has to acknowledge the site once and this will automatically acknowledge all events for that site.

Note: Only events with video images or sites that are on line will appear in the list. If a site sends events without video images, the site will only appear in the list while the event is being downloaded. Once the event has been downloaded it will be passed to the CMSC and the site will disappear from the list.

When Video Central Platinum is started, the system establishes the link using protocols defined during installation. If the communications link fails, the following message may be displayed:

‘The connection to the Central Monitoring Station is no longer available’.

The link may be unavailable for a number of reasons: The CMSC may be busy, the link cable may be disconnected, or the TCP/IP connection is not established. Video Central Platinum will continue to receive

and process events and log data. Outstanding events will be queued and sent to the CMSC when the problem has been rectified. The following messages may be displayed:

'The connection to the Central Monitoring Station is back online' or

'The connection parameters have changed'.

Note: If CMSC if offline for any reason, it should be quickly brought back online or Basic Integration should be turned off on the Video Central Platinum Server PC by reconfiguring the product. This will eliminate any potential problems with the queuing of events if CMSC is offline for long periods of time.

2.15.1.2 Unknown Alarm Events

If the ADPRO XO firmware is newer than the installed version of Video Central Platinum (VCP) then the ADPRO XO device could be capable of sending alarm events to VCP that are not understood or supported. In this scenario the basic integration module by default will translate these events into the following ADEMCO or SIA events;

Ademco - Unknown Event=E354,E754,None

SIA - Unknown Event=UA,UA,None

To resolve this issue the following options are available;

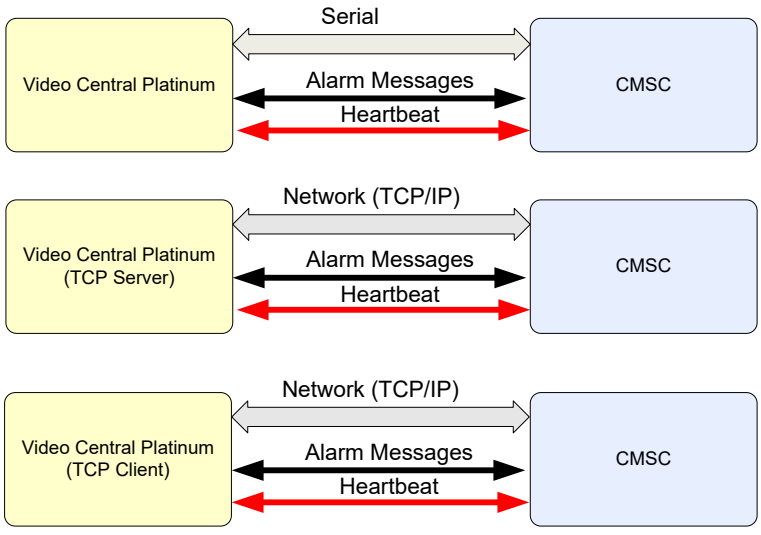
- Change the ADPRO XO setup to stop the unsupported events from being sent to VCP.
- Downgrade the ADPRO XO firmware to the version that is compatible with your current VCP version.
- If available upgrade VCP to the version that supports the current ADPRO XO firmware.
- Continue to accept the unknown events and manage this scenario within your third-party CMS software.

2.15.1.3 Communication with the CMSC

If a Com Port is selected, a null-modem cable with full hardware handshaking is required to connect between the Com Port as defined in the Basic Integration Setup on the Video Central Platinum PC and the Com Port defined by the CMSC software as being a port to receive an ADEMCO or SIA receiver.

The CMSC software will define the Com Port parameters such as baud rate and parity. The CMSC software will also define a Receiver number, Line Card group, and Group number.

Alternatively, TCP/IP may be used for sending the alarm information.



2.15.1.4 Heartbeat

During normal operation, Video Central Platinum transmits a Heartbeat Character (usually a capital S) at regular intervals. The CMSC acknowledges the Heartbeat Character within the programmed time period with a Heartbeat Response.

If Video Central Platinum does not receive a Heartbeat within the programmed time period, an error message will be displayed on all workstations connected to the Server PC. This will announce that the connection to the CMSC is no longer available.

When a valid Heartbeat is received, an announcement that the CMSC is back online will be sent to all workstations.

2.15.2 Setup of Basic Integration

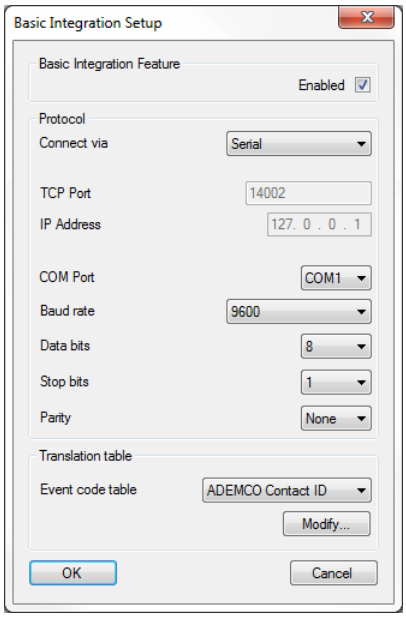
Access the Basic Integration Setup dialog via Tools > Admin > Basic Integration Setup.

Turn on the Basic Integration feature by selecting the 'Enabled' checkbox.

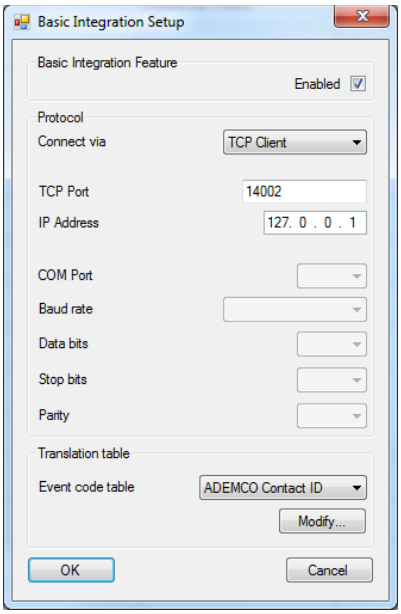
Set the Protocol via the 'Connect via' dialog. Select from Serial, TCP Client, or TCP Server.

Ensure that any serial port selected will not be used by other devices such as modems or terminal adaptors.

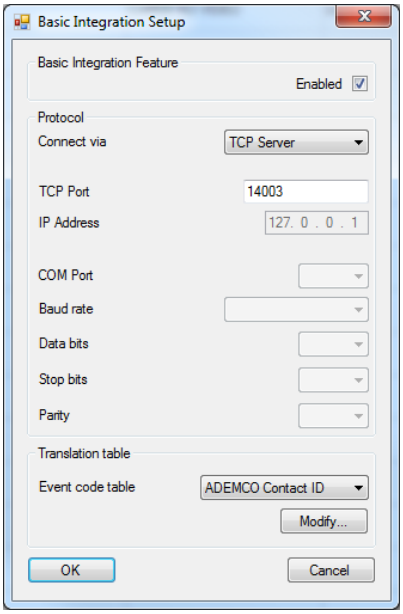
If connecting via Serial: select the COM Port, Baud Rate, Data Bits, Stop Bits, and Parity type.



If connecting via TCP Client enter the TCP Port and IP Address.



If connecting via TCP Server enter the Port Number.



From the Translation Table area choose the Event Code Table type as either SIA or ADEMCO Contact ID.

If you wish to modify the Translation Table click **Modify** and the Modify Translation Table dialog will be displayed with codes appropriate to the selected Event Code Table Type, SIA or ADEMCO Contact ID, will be displayed.

If modification is not required, click **OK** to save settings and exit Basic Integration Setup.

2.15.2.1 Modifying the Translation Table

The Translation Table contains all the events the system can receive and their equivalent codes. The Receiver number, Line Card group and Group number are defined in the translation table.

The Receiver Number, Line Card Group and Group Number must be amended for the specific Central Station configuration if using a protocol that uses these fields (<RN>, <LCG> or <GP>).

The Video Central Platinum Fault Reporting Site ID is that which Video Central Platinum will assume if sending any Video Central Platinum-based faults.

The Comm Fault Code is the event code that will be sent if a communications-based failure occurs.

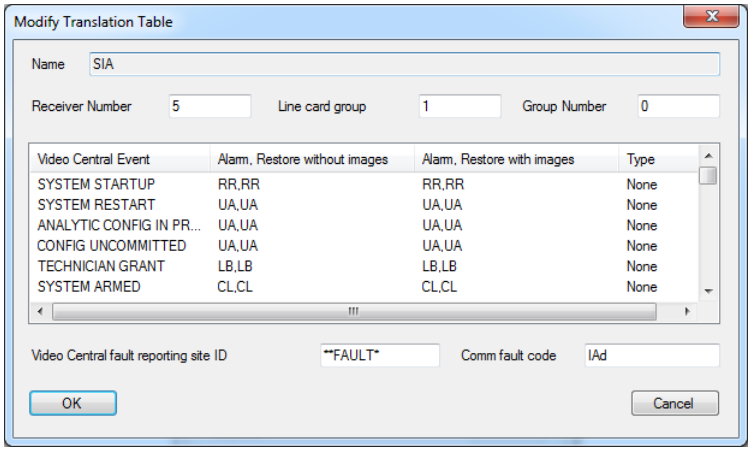
Event Codes for all other alarm types can also be amended. Most ADEMCO events have two codes associated:

- an alarm with associated images
- an alarm without associated images.

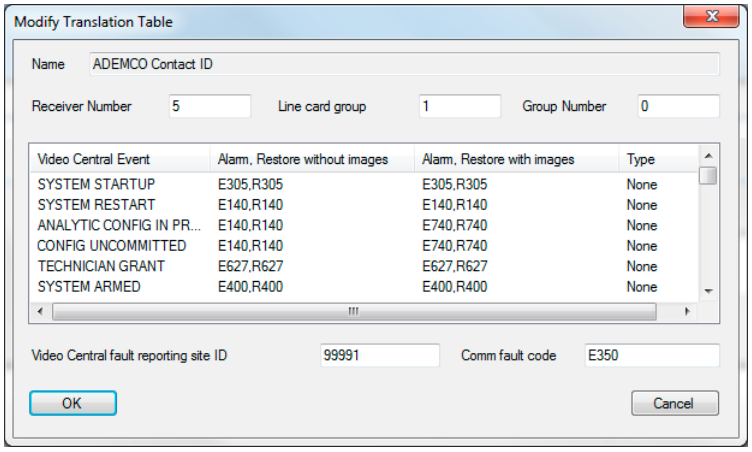
The default codes for alarms with no images are typically industry standard codes whilst the default codes for alarms with images are typically the same code plus 600. For example a code E130 without images becomes a code E730 with images).

It is also possible to set an alarm restore code. An alarm restore code will be used if the alarm is no longer active. The alarm code fields in the Modify Translation Table, have the format “<alarm activation code>,<alarm deactivation code>”.

Modify Translation Table – SIA codes



Modify Translation Table – ADEMCO Contact ID codes



The following parameters may be modified by entering the appropriate data:

- Receiver Number
- Line Card Group
- Group Number
- Video Central Platinum Fault Reporting Site ID
- Comm Fault Code.

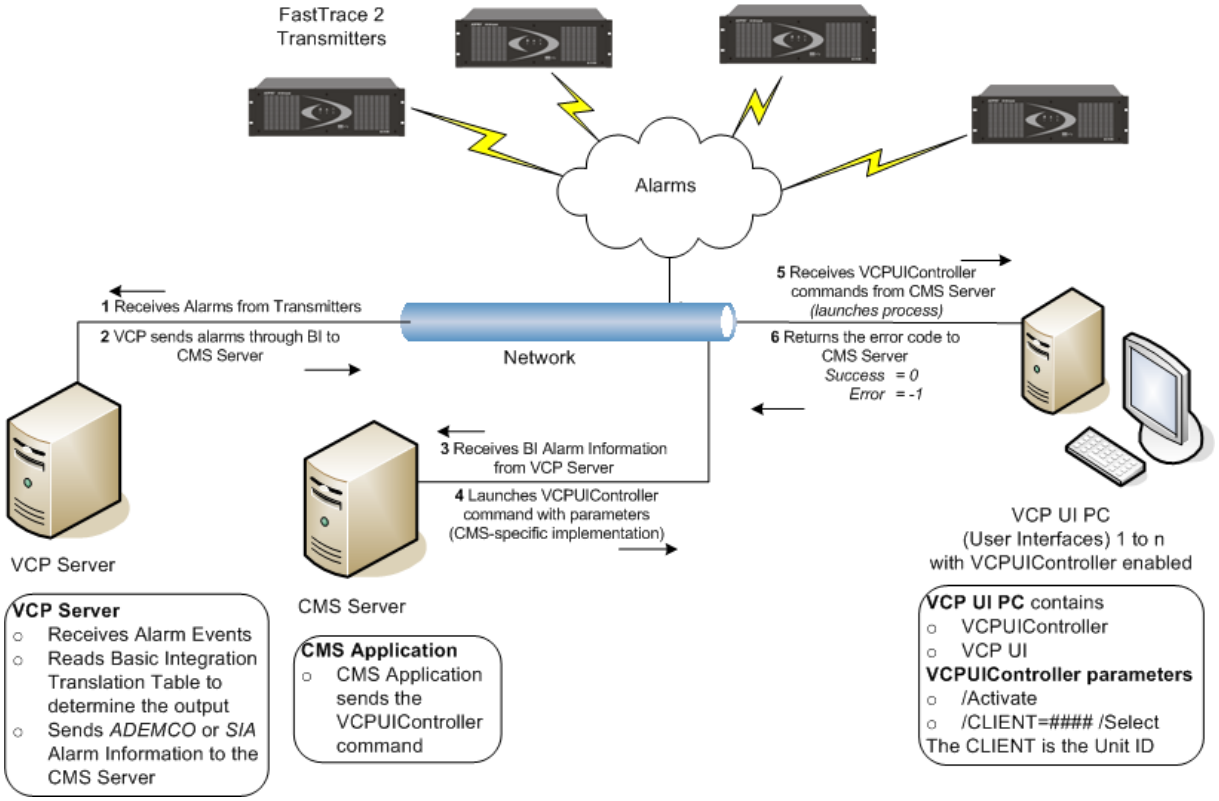
2.15.3 VCP UI Controller

2.15.3.1 Introduction

The VCP UI Controller is typically used in conjunction with Basic Integration. The VCP UI Controller enables an authorised Central Monitoring Station (CMS) computer to activate (maximise) the VCP UI application, select a site from its Active Sites List and display it.

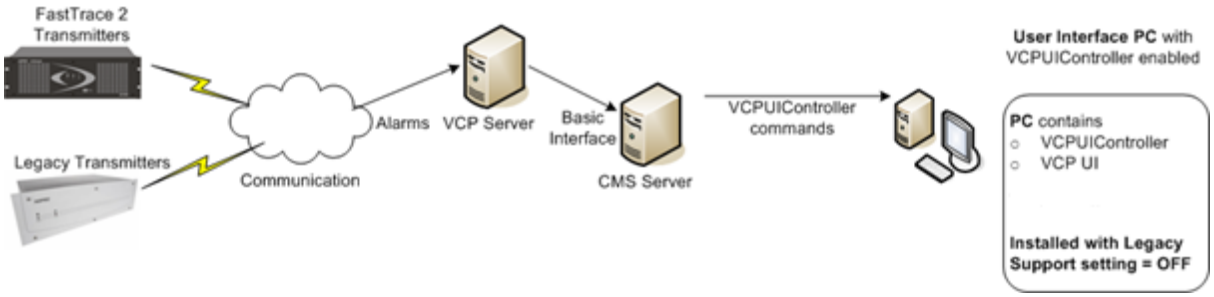
The VCP Server receives alarms from transmitters and sends alarm information to the CMS Server, encoded in the ADEMCO or SIA format, as indicated by settings in the Basic Integration Translation Table. When an alarm event for a site has accompanying video data the CMS can send the VCPUIController.exe command, with the appropriate parameters, to display the video from the alarm site.

The illustration below shows a system with ADPRO FastTrace 2 Series devices. ADPRO iFT Series devices and HeiTel are also possible.



2.15.3.2 Using VCP Controllers

The VCP UI Controller controls the Video Central Platinum User Interface (VCP). The illustration below shows a system with ADPRO FastTrace 2 Series devices. ADPRO iFT Series devices are also possible.

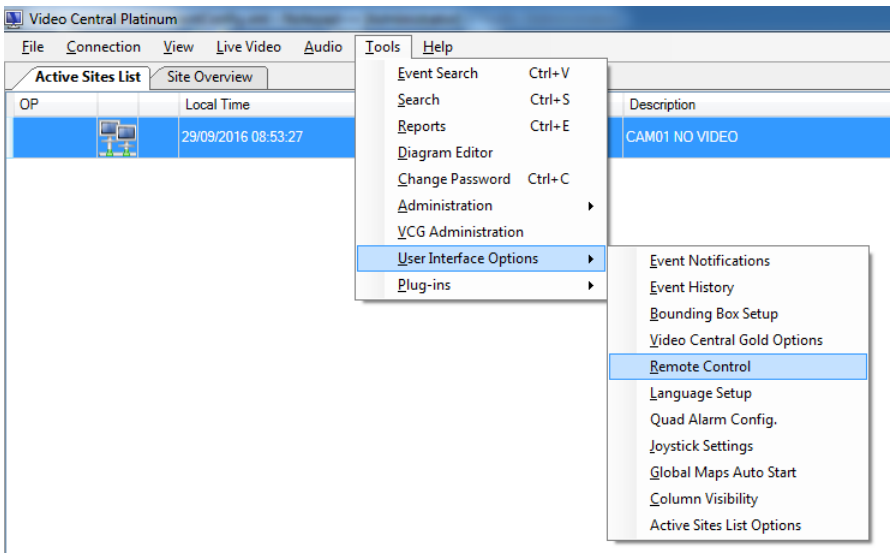


The VCP UI Controller runs on the same host as the VCP UI. For the VCP UI Controller to control the VCP UI on a PC the VCP UI operator must be logged in to the VCP UI and its *Remote Control* option must be enabled.

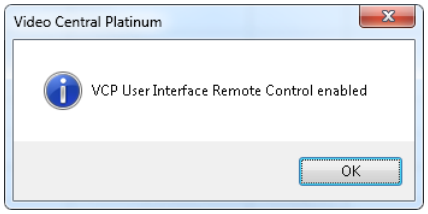
2.15.3.3 Enabling the VCP UI Controller

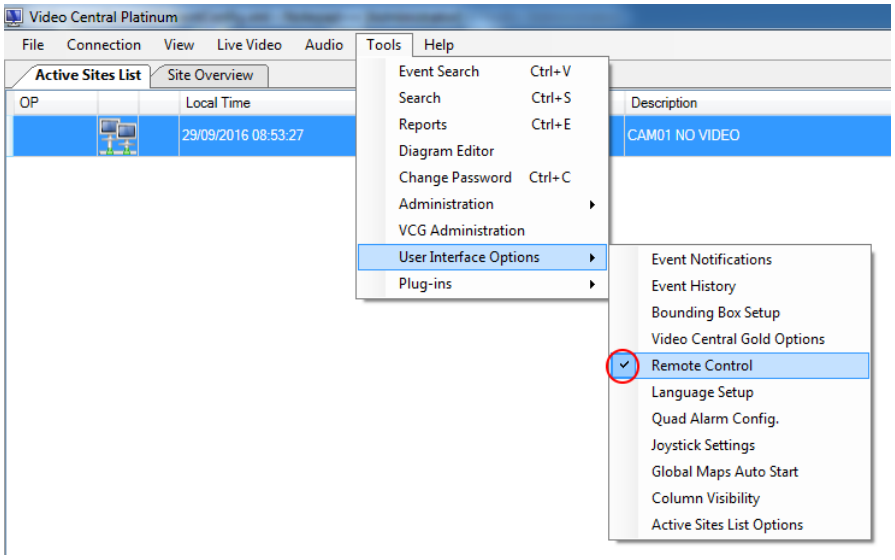
To enable the VCP UI Control on a VCP UI PC, from the VCP UI main menu select:

Tools > User Interface Options > Remote Control



When the option is enabled the VCP UI will display a confirmation dialog and the menu will show that the option has been enabled.





2.15.3.4 The VCPUIController Syntax

The VCP UI Controller is found in the VCP UI installation location. By default this is:

C:\VCP\Client\UIController\VCPUIController.exe

The VCPUIController.exe has three commands:

- Activate = put the VCP UI in the foreground with its main window maximised.
- Client = specifies which site to select, which is identified by the Unit ID, as programmed in the VCP Site Details from the Active Sites List (ASL).
- Select = Select the VCP site and display the video events on the Site tab.

When the command is executed it will return a result code of 0 or –1.

- result = 0 means the command succeeded
- result = -1 means the command failed.

2.15.3.5 VCP UI Controller Settings

When a site is selected while another site is being viewed in the VCP UI, the active site is pushed back to the Active Sites List (ASL) and then the selected site is displayed. If the selected site is not displayed because the time required to make the switch from one site to the next is too long, and the attempt to switch times out, the timeout period can be altered. The default timeout period is 7 seconds.

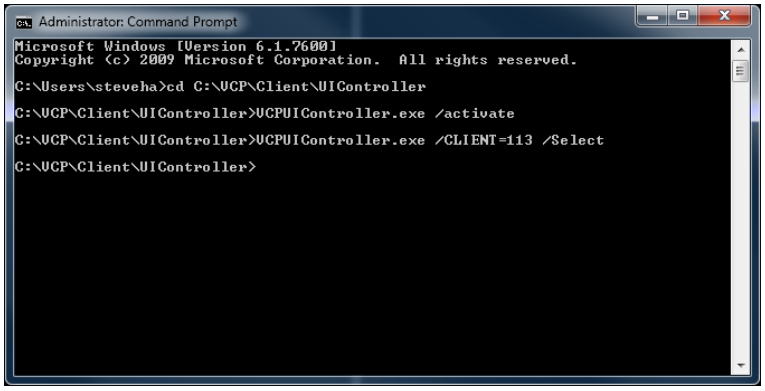
The timeout setting is contained in the VCPClientConfig.xml file, located at “C:\ProgramData\ADPRO VCP\VCPClientConfig.xml”. The XML tag containing the timeout value is “<TimeoutDisconnectFromSite>” and the value is given in milliseconds, such that the default 7-second timeout setting is 7000.

2.15.3.6 Testing the VCP UI Controller

The VCPUIController.exe command can be sent manually in a console from the VCP UI PC to confirm that the site Unit ID is correct and the VCPUIController command is bringing up a site from the VCP UI Active Sites list.

2.15.3.7 Usage

- REM Activate the VCP UI, bring it to the foreground and maximise it
- C:\VCP\Client\UIController\VCPUIController.exe /Activate
- REM Select VCP site where #### is the site Unit ID
- C:\VCP\Client\UIController\VCPUIController.exe /CLIENT=#### /Select



2.16 VCP Configuration Files and Folders

- **VCP related configuration files** have been moved to the “ADPRO VCP” folder under the common application data folder. E.g. “C:\ProgramData\ADPRO VCP”.

  The configuration files include

File	Configuration Purpose
ADPROSW.config and	Video Wall
GPSMapsSettings.xml.	Global Maps
vcp_bi.ini,	Basic Integration
VCPAppLauncherConfig.xml,	User interface, 3rd party application launcher
VCPClientConfig.xml,	VCP client

- **Temporary, backup and log files** are moved to subfolders under the “ADPRO VCP” folder. The “ADPRO VCP” folder resides under the common application data folder.

  The following folders are now used by VCP:

<CommmonApplicationData folder>\ADPRO VCP
Used for storing VCP configuration files, and other files that do not belong in any of the subfolders.
<CommmonApplicationData folder>\ADPRO VCP\Temp
Used for temporary files, i.e. files that are supposed to be cleaned up by VCP.
<CommmonApplicationData folder>\ADPRO VCP\Temp\SavedAlarms
Used by the XO Alarm Server SDK for temporary caching alarm information.
<CommmonApplicationData folder>\ADPRO VCP\Backup
Used by VCP for storing backups of config files, etc.
<CommmonApplicationData folder>\ADPRO VCP\Logs\Server
Contains VCP Server rolling log.
<CommmonApplicationData folder>\ADPRO VCP\Logs\Client
Contains VCP UI rolling log.
<CommmonApplicationData folder>\ADPRO VCP\Logs\VideoWall
Contains VCP VW rolling log.
<CommmonApplicationData folder>\ADPRO VCP\Logs\GlobalMaps
Contains Global Maps application rolling log

  These files contain the application settings that have been entered either via the installation, added manually, or set by using the application and describe how your system should function.

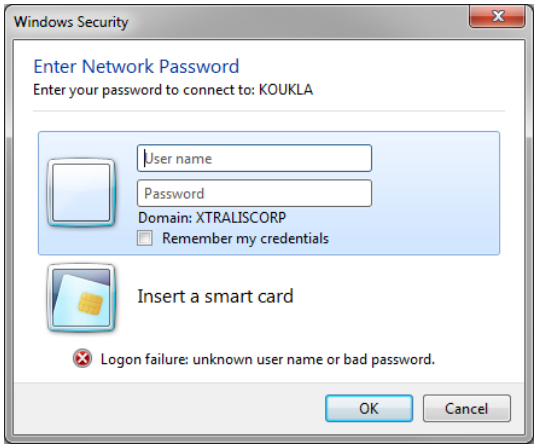
  Technical support may ask for these files when working with you to resolve an issue.

2.17 Report Manager

2.17.1 Accessing Reports

2.17.1.1 Accessing Report Manager via Video Central Platinum

From the Video Central Platinum Client select Tools > Reports. As Reporting Services uses Windows Authentication you may be prompted to enter a user name and password. These are as your Windows Domain or Workgroup user account details. If User Account Control (UAC) is on, the direct access method maybe required to allow access to normal administrators or other users.



2.17.1.2 Direct Access via Internet Explorer Web Browser

Local access via http://127.0.0.1/Reports_XTRALIS_CYCLOPS

Remote Server via http://<server ip >/Reports_XTRALIS_CYCLOPS

Example: http://172.20.254.1/Reports_XTRALIS_CYCLOPS

Example: http://172.20.254.1/Reports_MY _INSTANCE_NAME

Note: If UAC is on, Internet Explorer must be run with elevated admin rights. To run Internet Explorer with elevated rights from within Start > All Programs right-click on the **Internet Explorer** shortcut icon and select “Run As Administrator”.

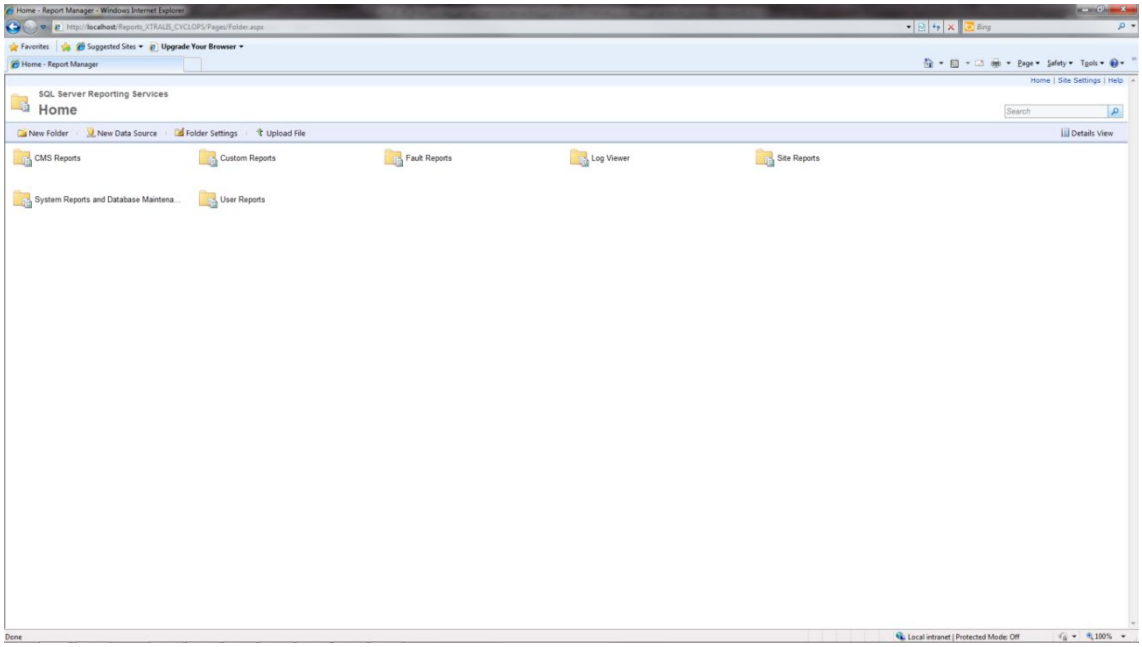
To display the Report Manager dialog within an Internet Explorer (IE) web browser enter the following:

- http://localhost/Reports_XTRALIS_CYCLOPS

2.17.1.3 Hidden Reports

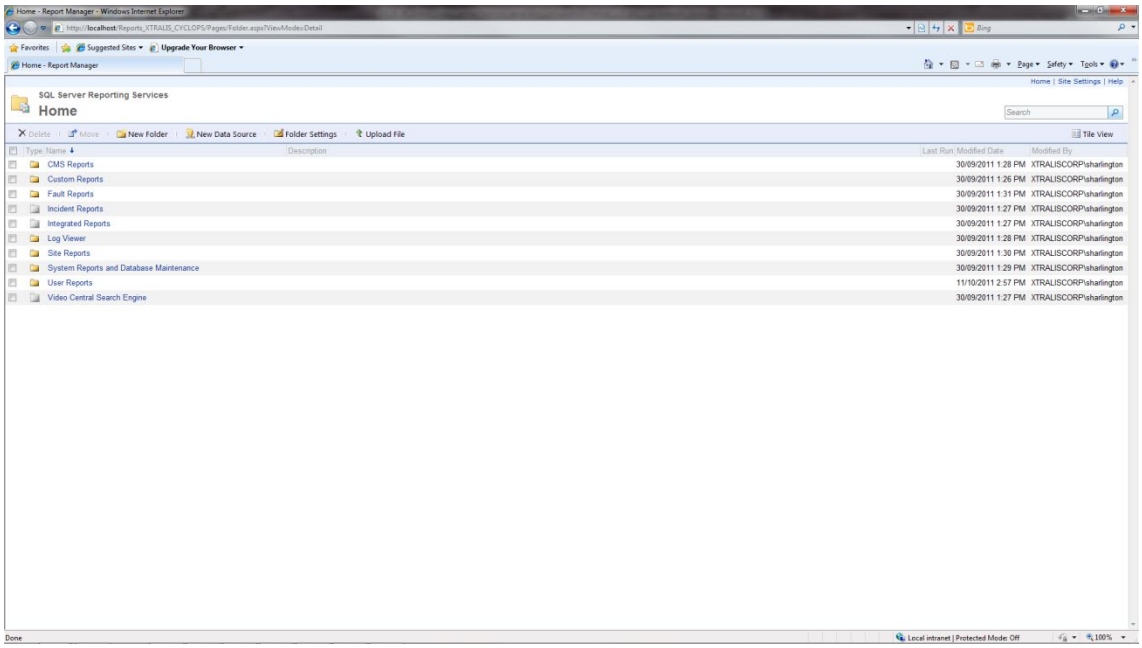
Entire Report Folders and some Reports that are executed from within Video Central Platinum and are therefore important to the operation of the system are hidden in Report Manager within **Tile View**. This is done to reduce the risk of users moving or deleting reports that provide features in Video Central Platinum.

Tile View:

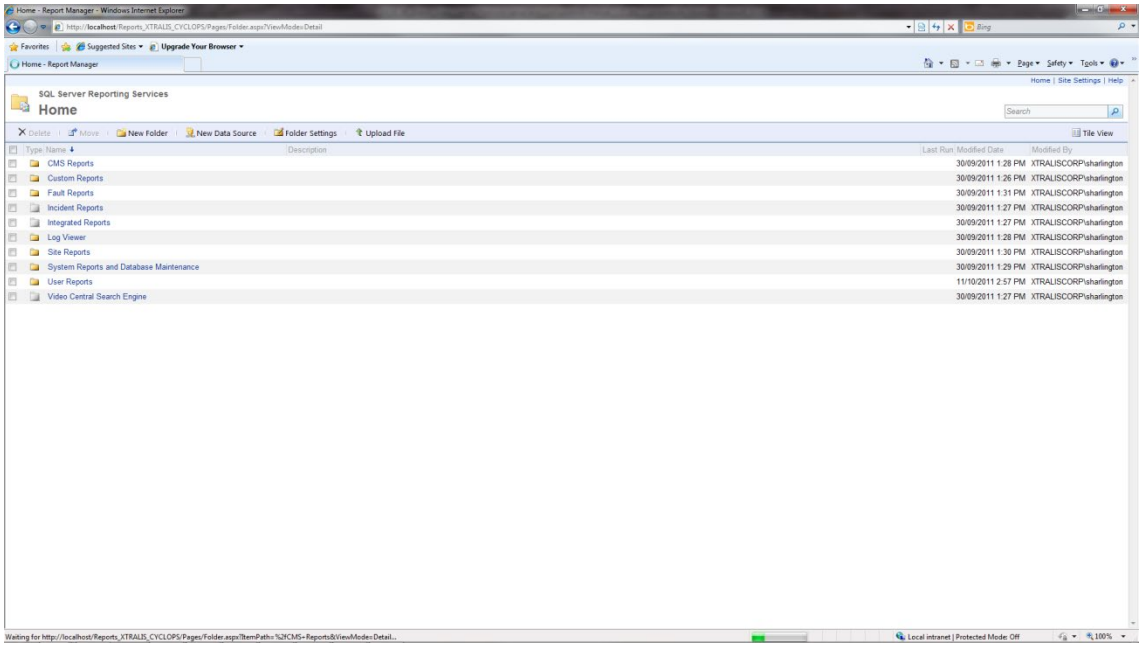


Select the **Details View** option to change the display. The hidden Report Folders are displayed with a Grey Icon.

Details View:



Selecting the **CMS Reports Folder** for example shows hidden reports with a Grey Icon.



2.17.2 Configuring the Windows Firewall

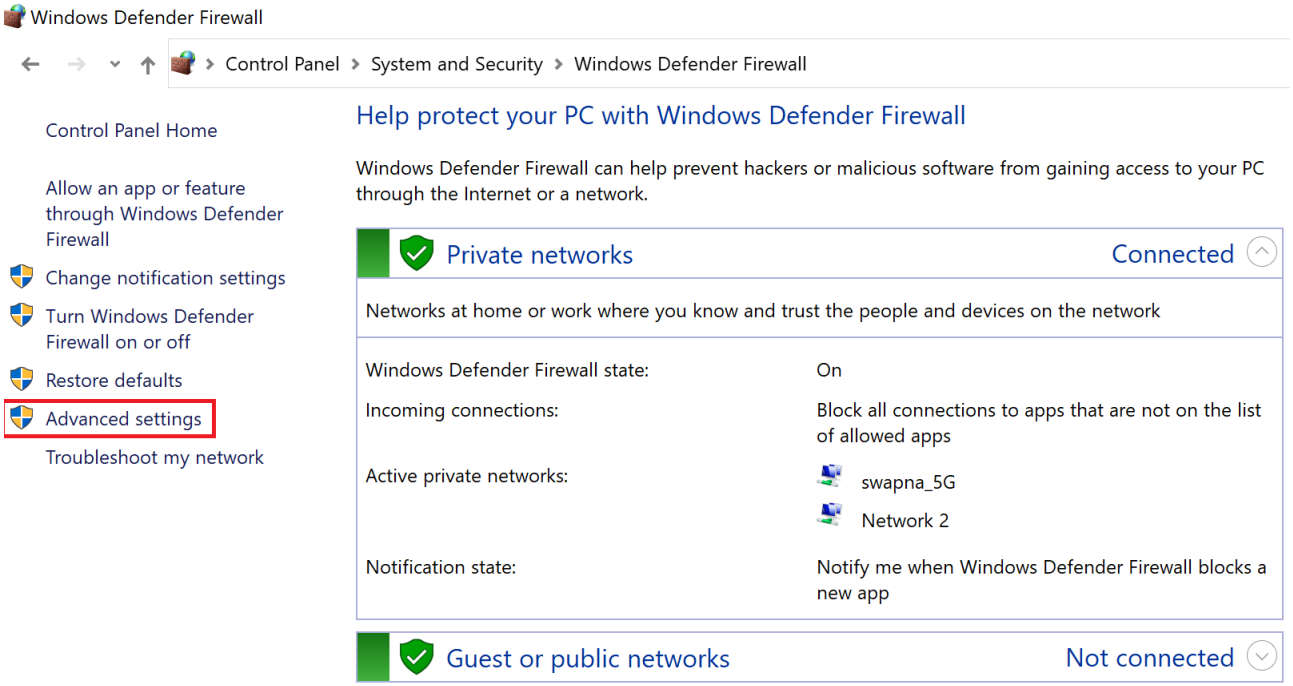
If you are using an alternative to Windows Firewall, ensure and port 80 is open.

The configuration of Windows Firewall varies according to operating system type.

2.17.2.1 Opening Inbound Port 80

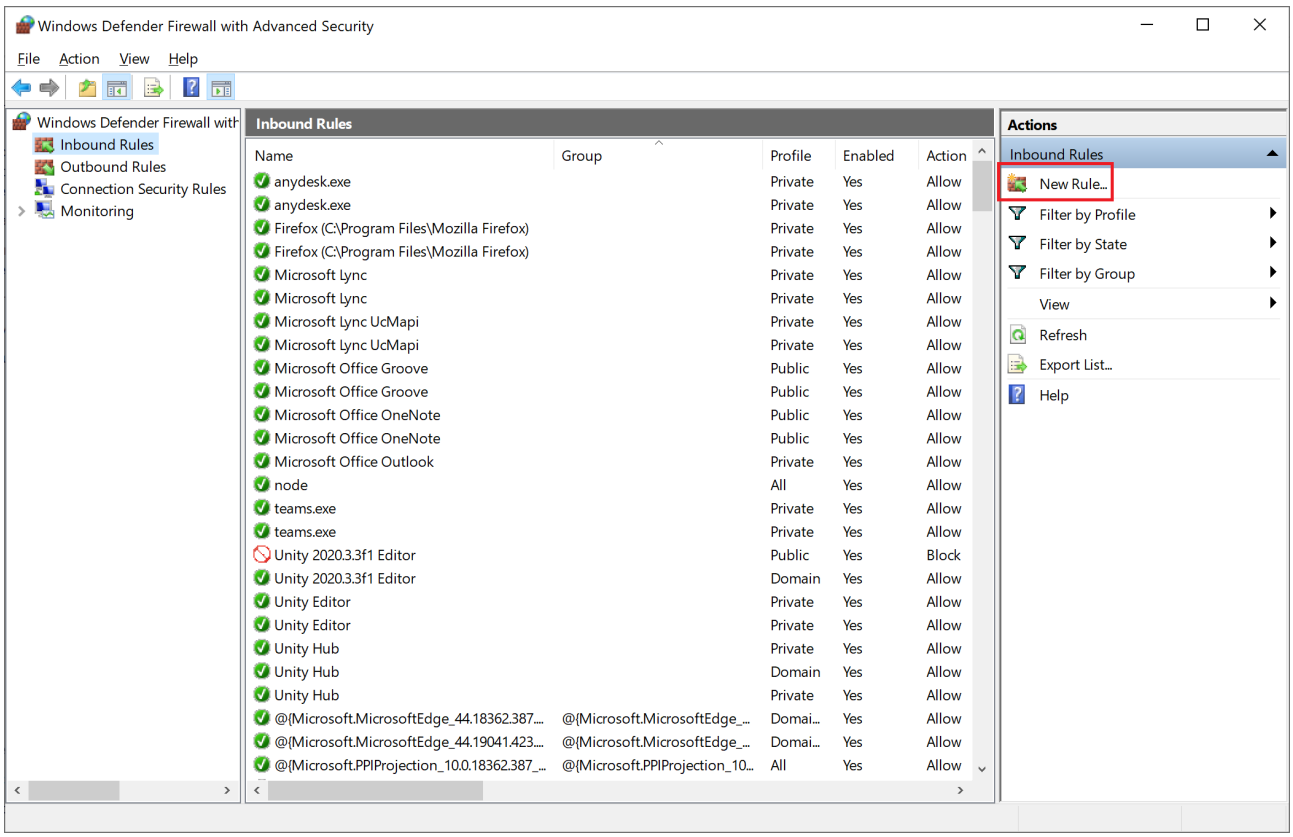
Microsoft SQL Server Reporting Services requires Port 80 open for inbound connections to enable Report Manager to operate.

Access the Windows Firewall dialog via Start > Control Panel > System and Security > Windows Defender Firewall then select Advanced Settings.

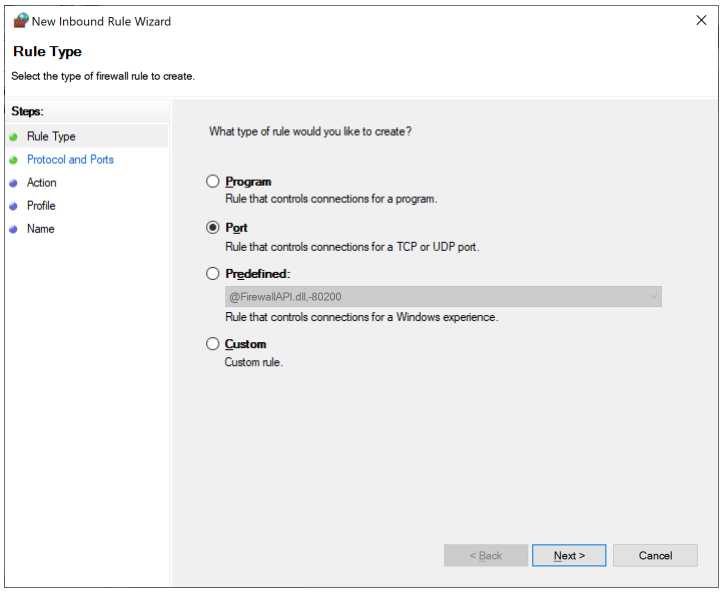


In the Windows Defender Firewall with Advanced Security dialog, select Inbound Rules.

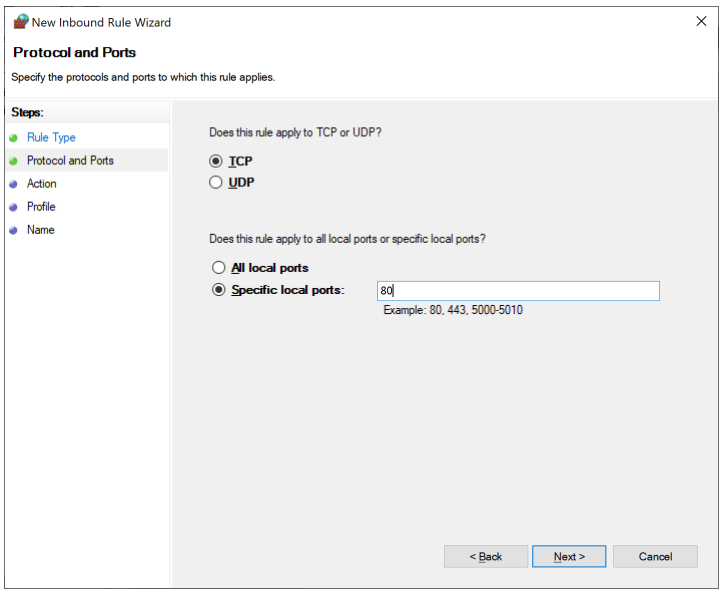
In the **Actions** list, click **New Rule** to start the New Inbound Rule Wizard.



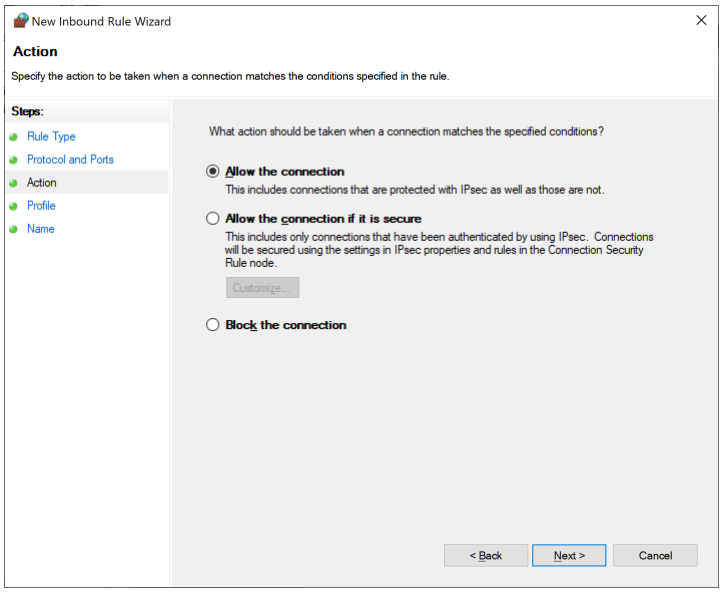
In the New Inbound Rule Wizard. select Port then click **Next** to display the Protocol and Ports dialog.



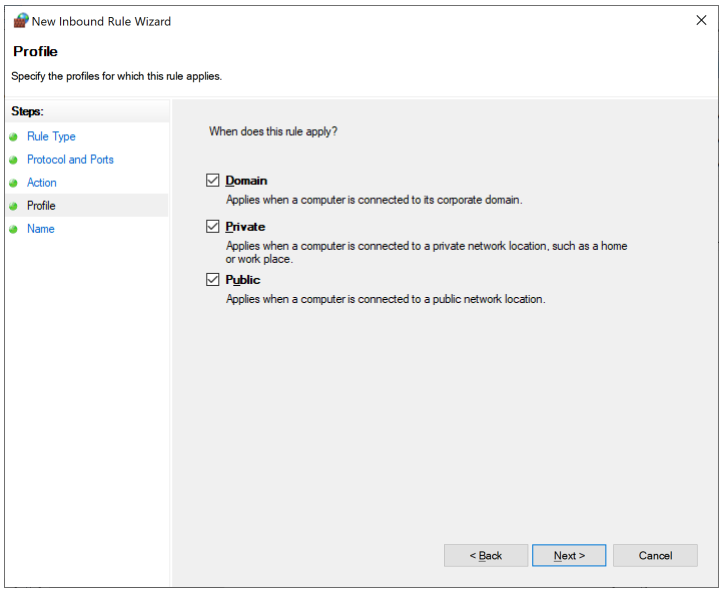
Enter 80 in Specific Local Ports then click **Next** to display the Action dialog.



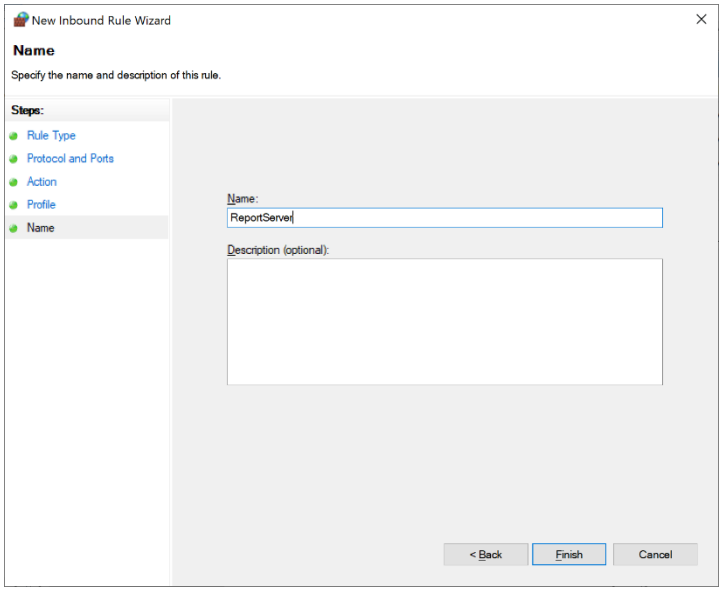
In the Action dialog, select Allow the Connection and click **Next** to display the Profile dialog.



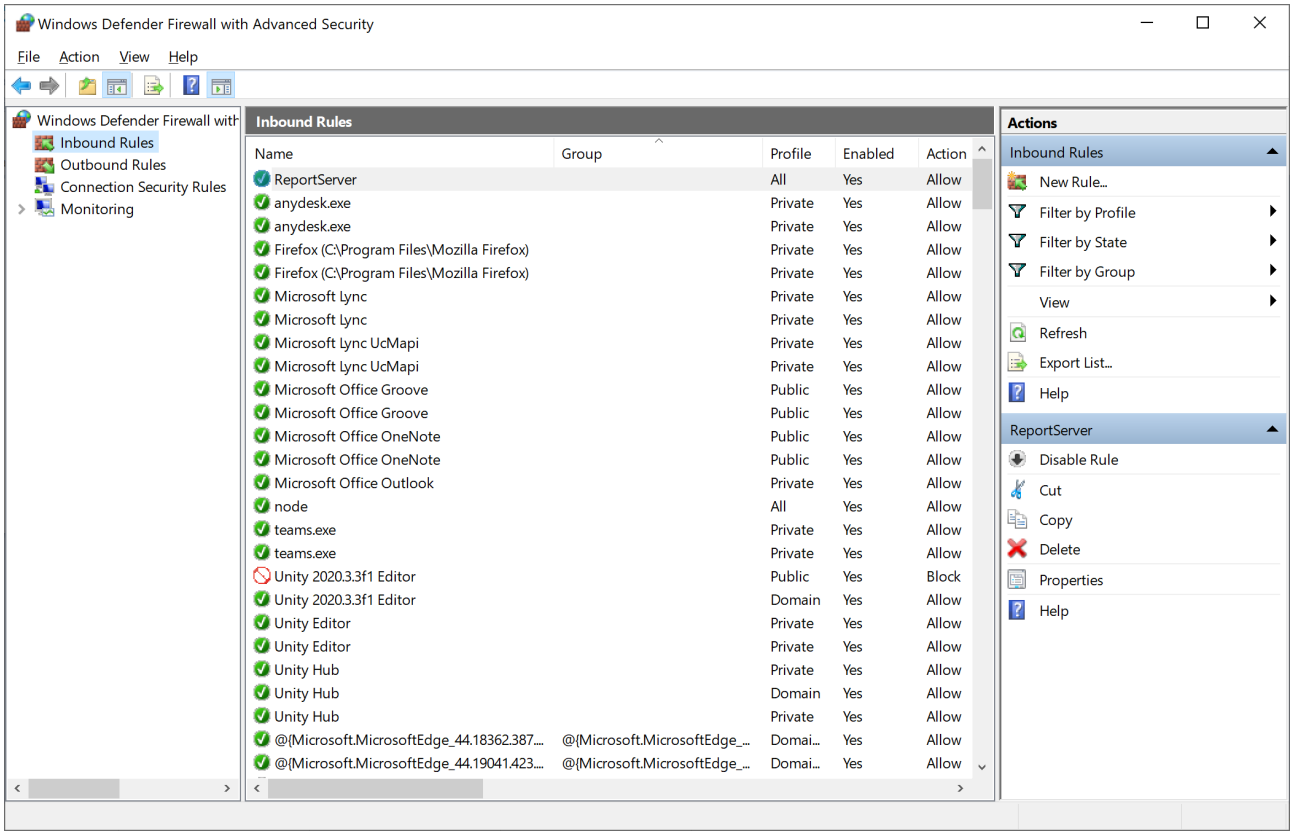
In the Profile dialog, under ‘When does this rule apply?’ select Domain, Private and Public then click **Next** to display the Name dialog.



In the Name dialog enter a name for the rule then click **Finish** to re-display the Windows Firewall with advanced Security dialog.



The new rule will be displayed. Close Windows Firewall.



For related information, visit https://docs.microsoft.com/en-us/sql/reporting-services/report-server/configure-a-firewall-for-report-server-access?view=sql-server-ver15

2.17.3 Adding Users for Reporting

By default only local administrators have access to Report Manager. If User Account Control (UAC) is turned on, Internet Explorer must be run with elevated admin rights. To run Internet Explorer with elevated rights from within Start > All Programs right click on the **Internet Explorer** shortcut icon and select “Run As Administrator”.

Users or User Groups should be added through Report Manager via Internet Explorer prior to using the Reports Menu or any report listed below through the Video Central Platinum User Interface.

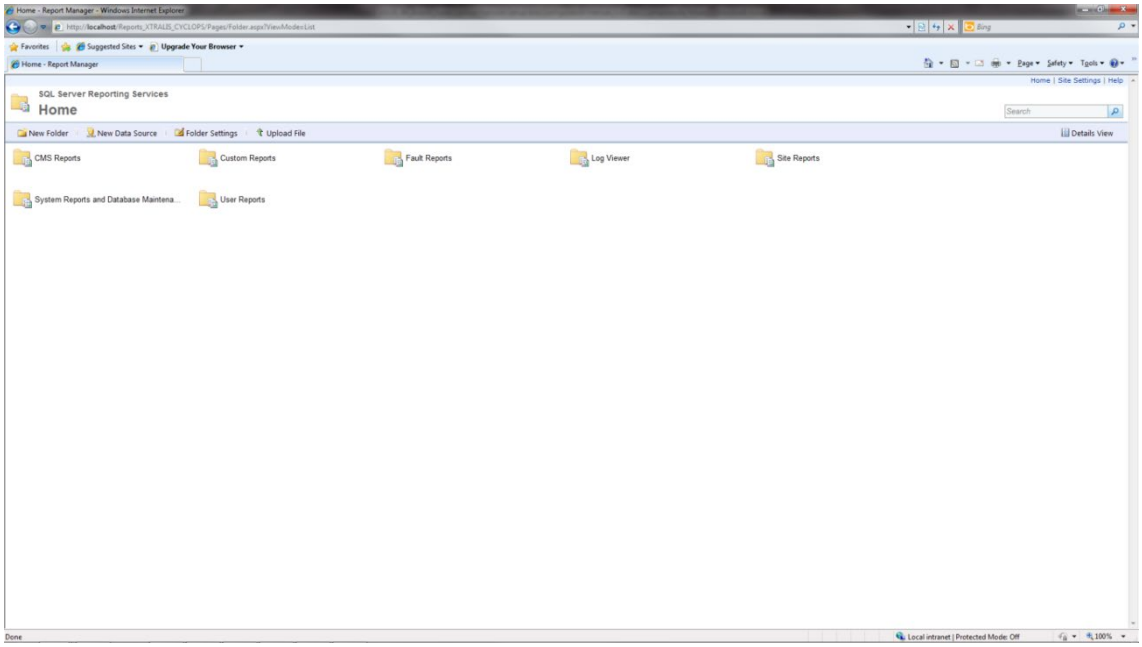
If you are unable to access the reports, visit https://www.mssqltips.com/sqlservertip/3144/sql-server-reporting-services-report-manager-site-permissions-error-after-installation/ for possible solutions.

The following example demonstrates how to add top-level permissions for either a specific user or user group. Report Manager allows permissions for reports or report folders to be set at any item level allowing full control over access.

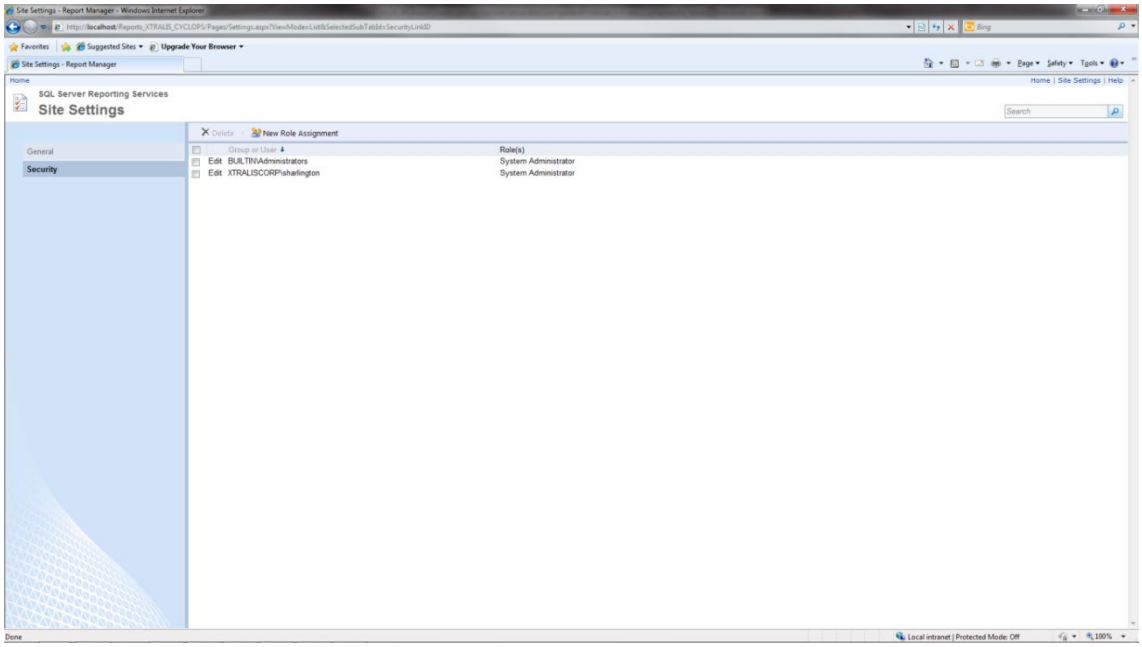
The following Video Central Platinum features are supplied via embedded reports and so appropriate access maybe required for each Video Central Platinum Operator.

- Tools > Search
- Site Actions > Site Details
- Application Launcher > View Site and User Notes.
- Application Launcher > Live Report
- Application Launcher > Incident Report
- Application Launcher > Resource Monitor Report
- Application Launcher > User Response Report
- Application Launcher > Operator Actions Audit Trail
- Application Launcher > Hidden Event Types

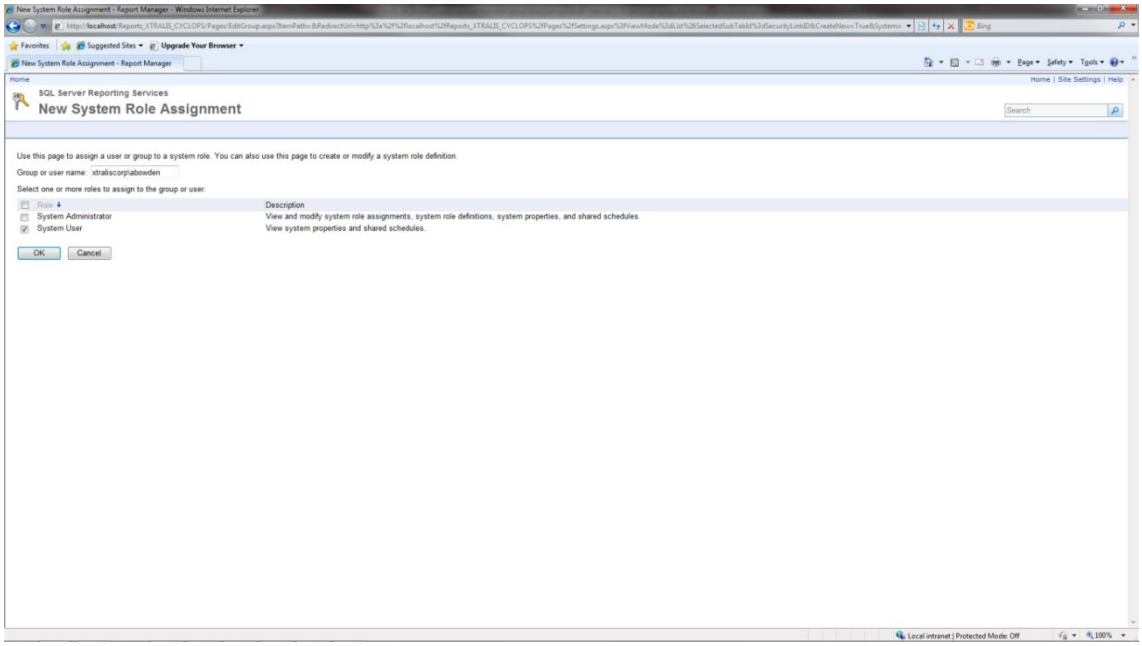
At the top right of the Report Manager dialog click **Site Settings** and the Site Settings page, General tab will be displayed.



In the Site Settings dialog, click the **Security** tab and the Site Settings Security dialog will be displayed.



On the Site Settings, Security dialog click **New Role Assignment** and the New System Role Assignment page will be displayed.

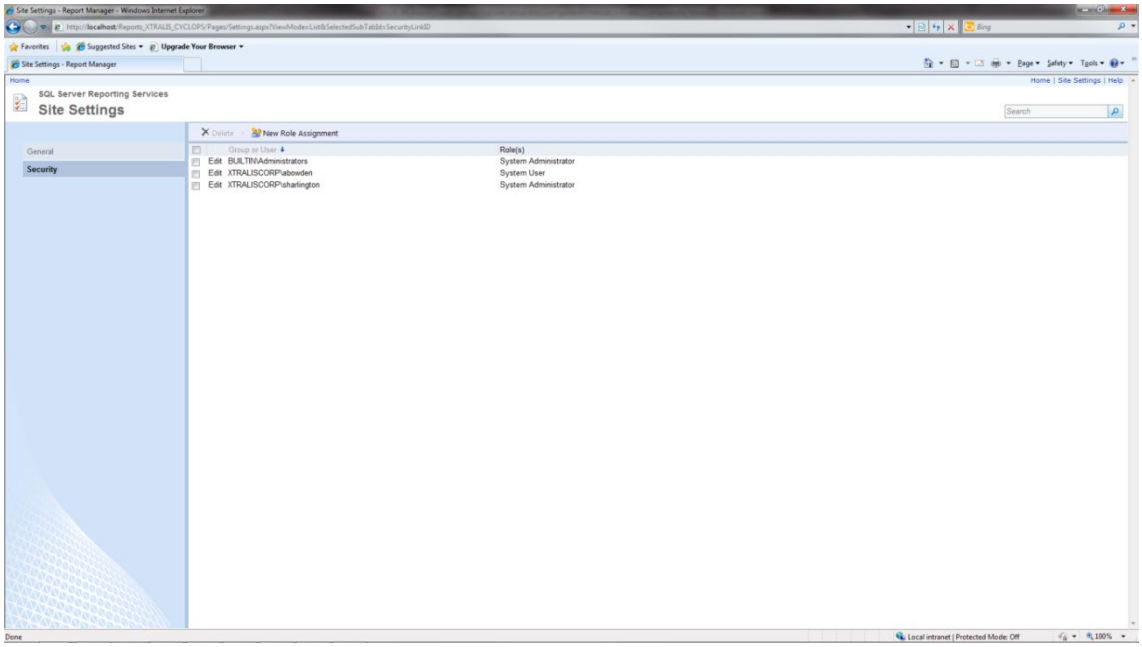


In the **New System Role Assignment** page, enter a valid Group or User name then assign a role by checking either System Administrator or System User.

Valid examples of names are:

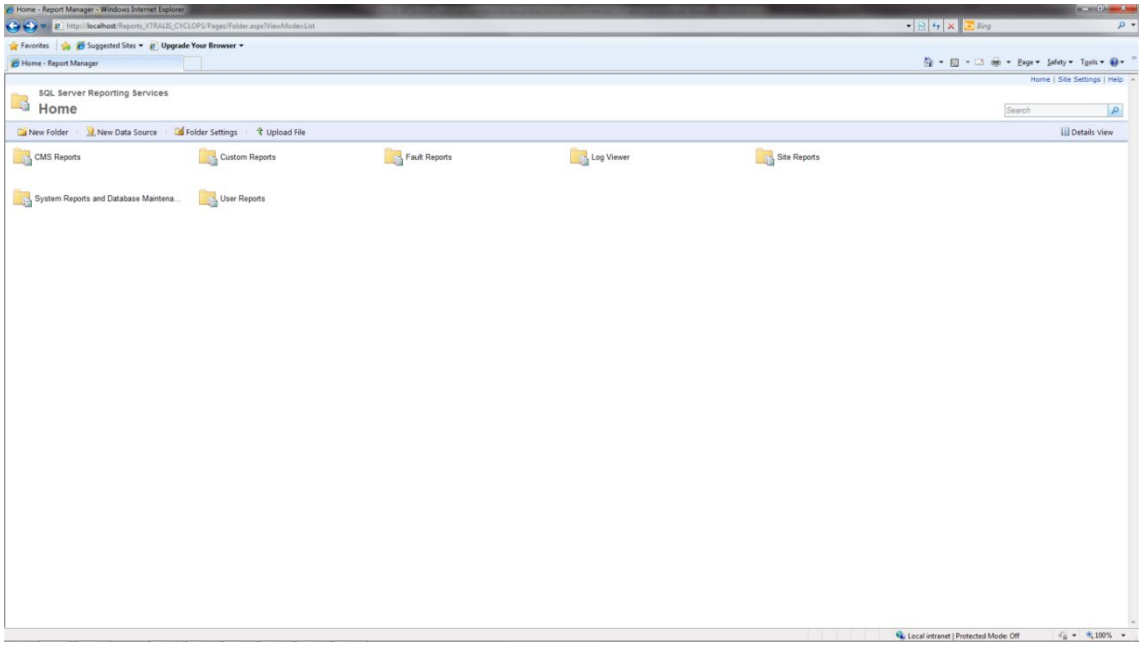
- Domain Name\User Group: adpro.com.au\domain users
- Domain Name\User: adpro.com.au\jimb
- Workgroup Name\User Group: mypcname\users
- Workgroup Name\User: mypcname\jimb.

Click **OK** and the Site Settings page, showing the new Group or User, will be displayed.

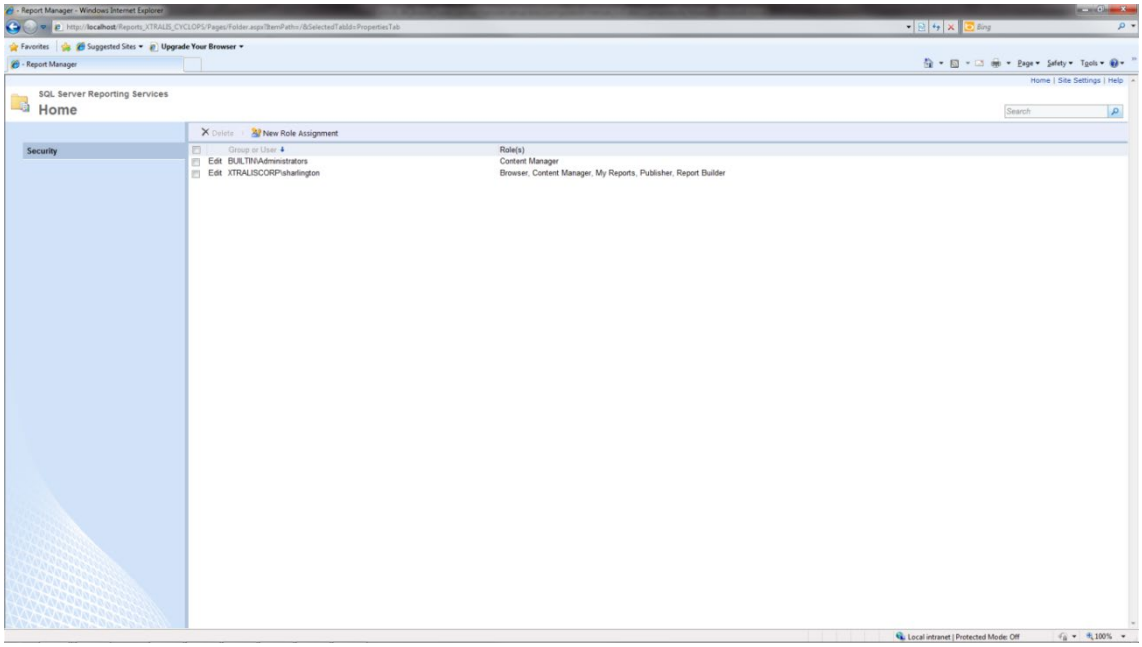


If editing of Groups or User is required in Site Settings, refer to Help.

Select **Home** to display the Home page.

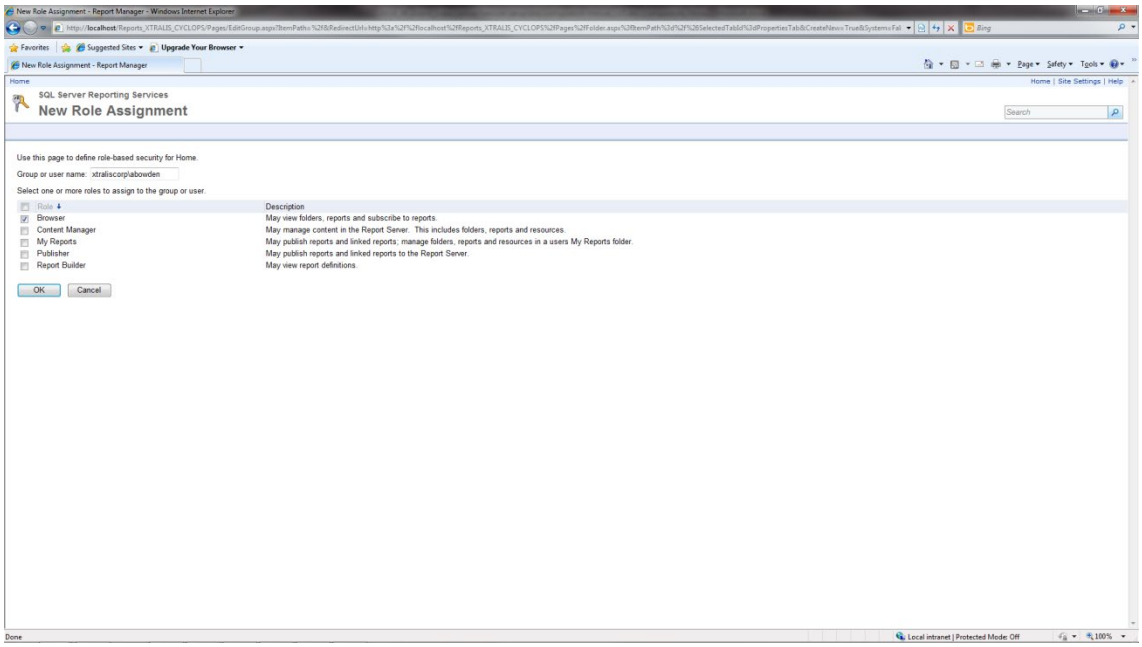


Select **Folder Settings** to display the security settings.

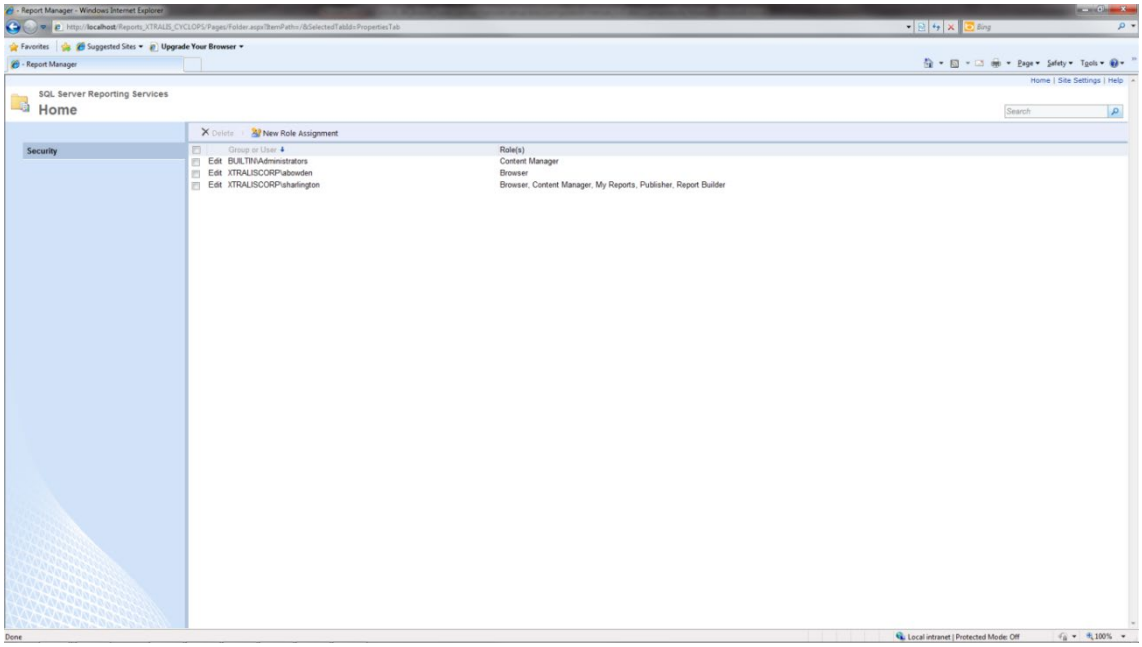


In the Security settings page select **New Role Assignment** then repeat the previous process but now adding the appropriate role to Users or Groups.

Enter the Group or User name then check the appropriate Role boxes to allocate permissions. Click **OK** to return to the Home page.

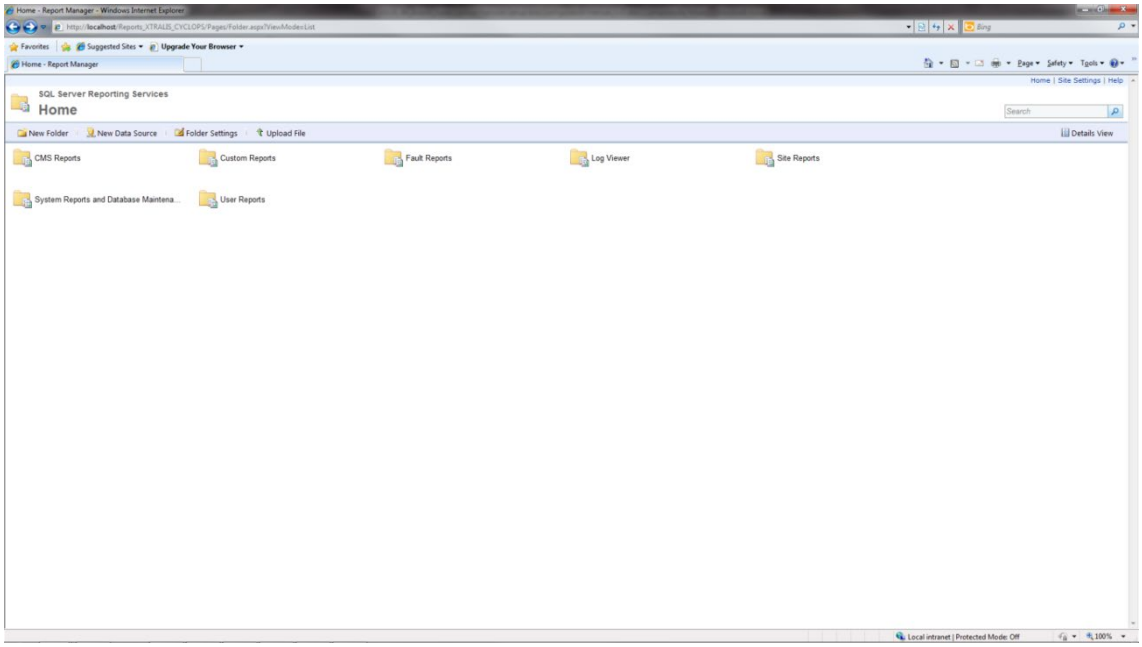


The Security settings page shows the new User or Group with the role or roles defined.

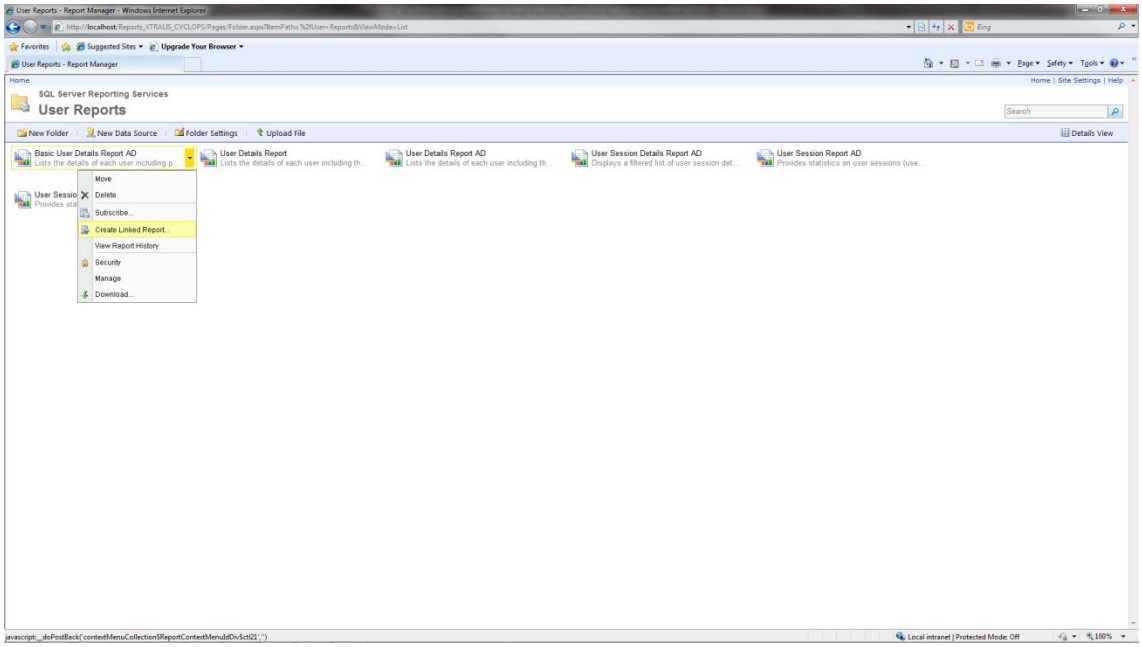


2.18 Creating a new Report Based on an Existing Report

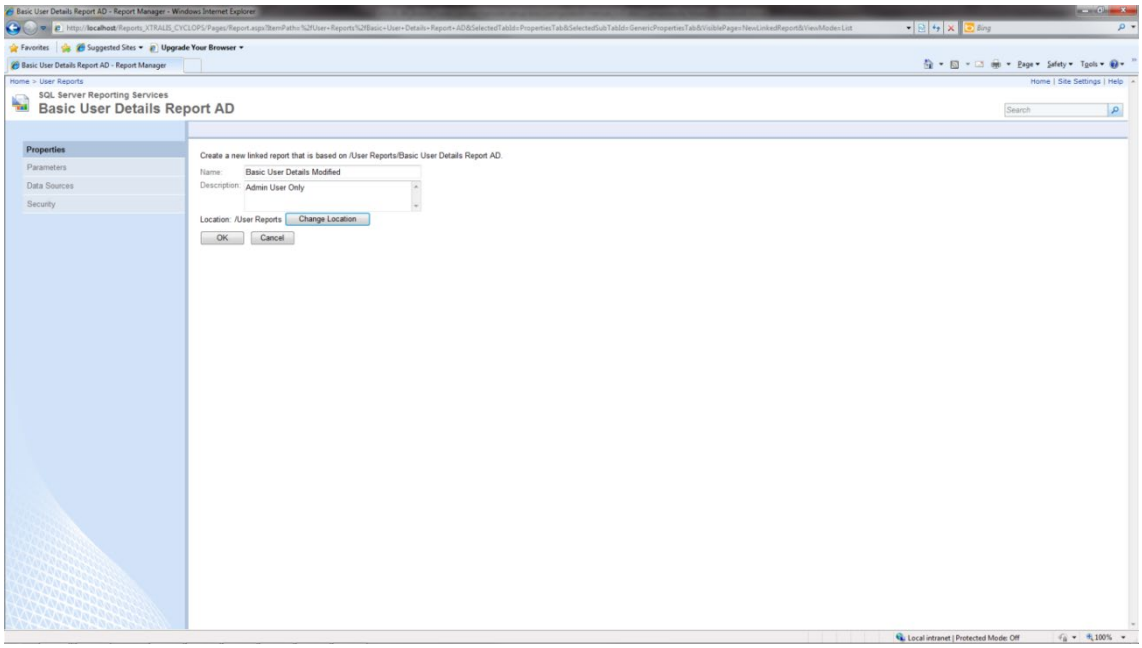
From the Home page click on the folder that contains the report on which the new report is to be based. The folder, displaying report titles and a synopsis of each, will open. In the following example the folder chosen is User Reports and the report is Basic User Details Report AD.



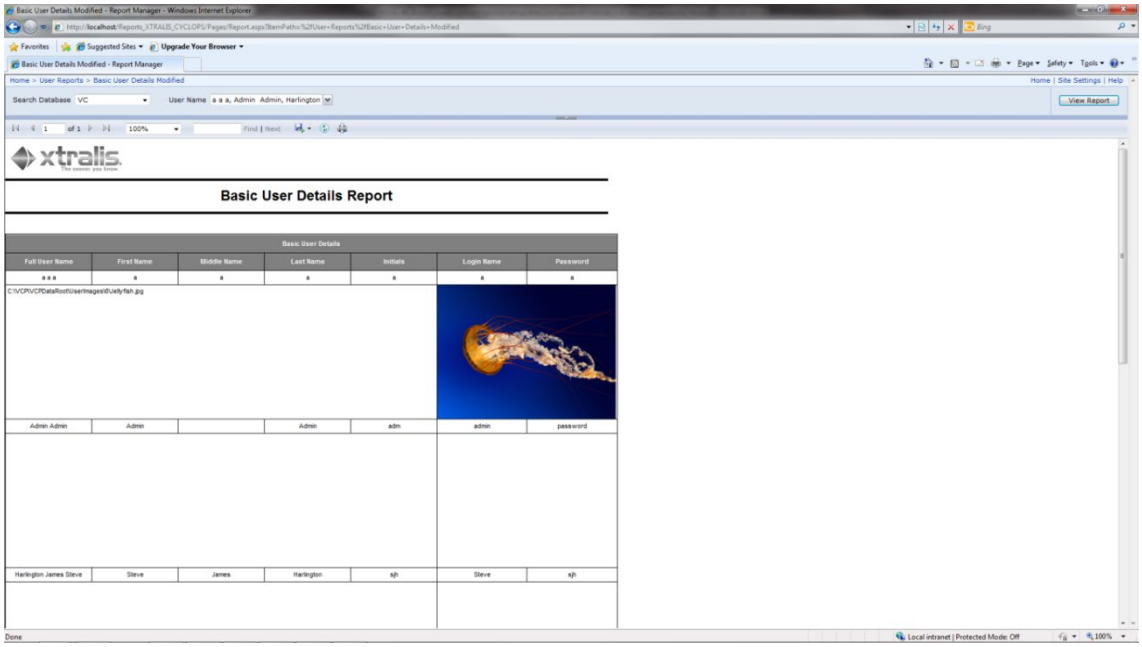
In the User Reports page click the drop down list to the right of the required title and the options will be displayed. Select the **Create Linked Report** option.



In the Properties view enter details of the new report such as a name and description. The default location may be changed by clicking **Change Location** and browsing to the required folder.



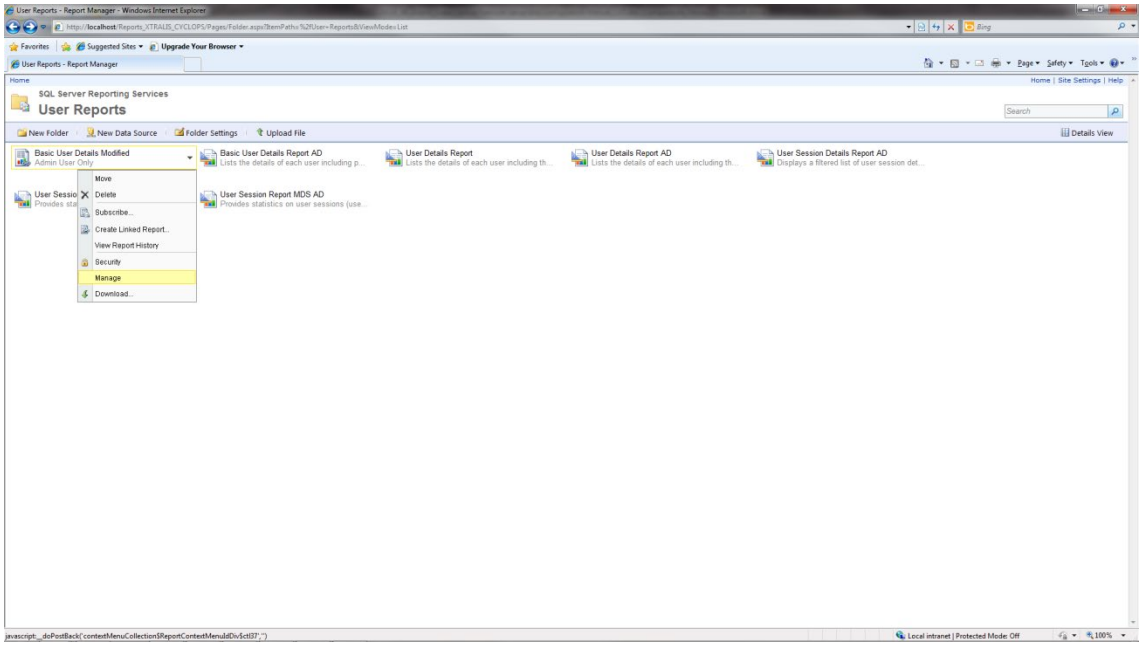
When complete click **OK** and the new report 'Basic User Details Modified' will be executed and displayed.



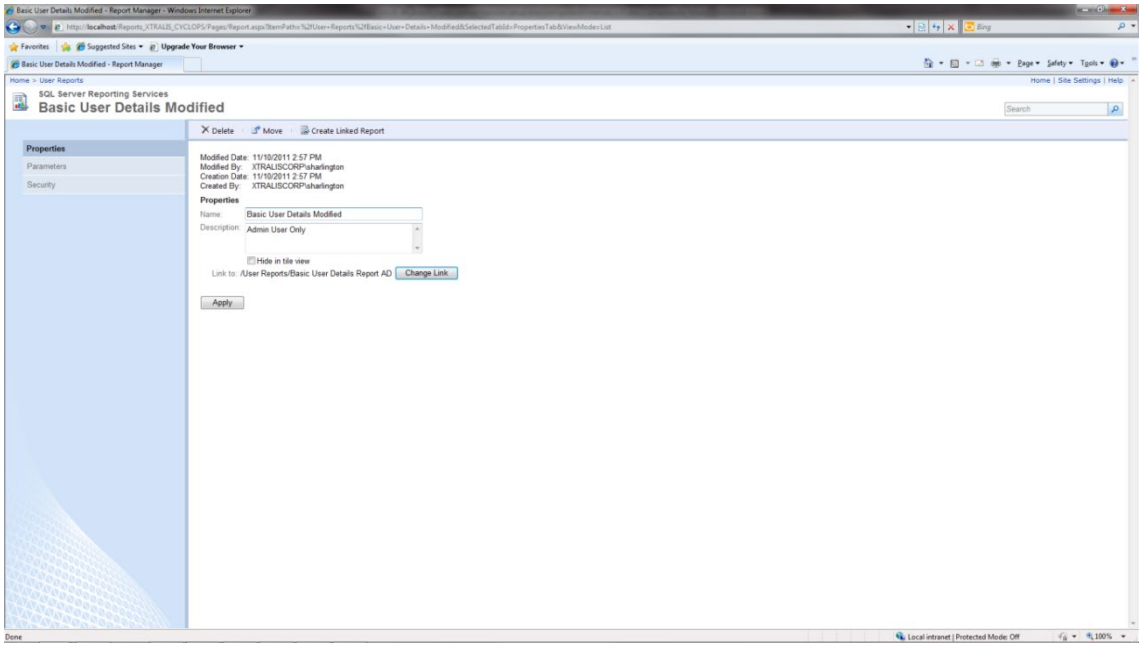
So far the report is identical to the original. To change parameters in the new report Refer to Section 2.18.1, Changing Report Parameters.

2.18.1 Changing Report Parameters

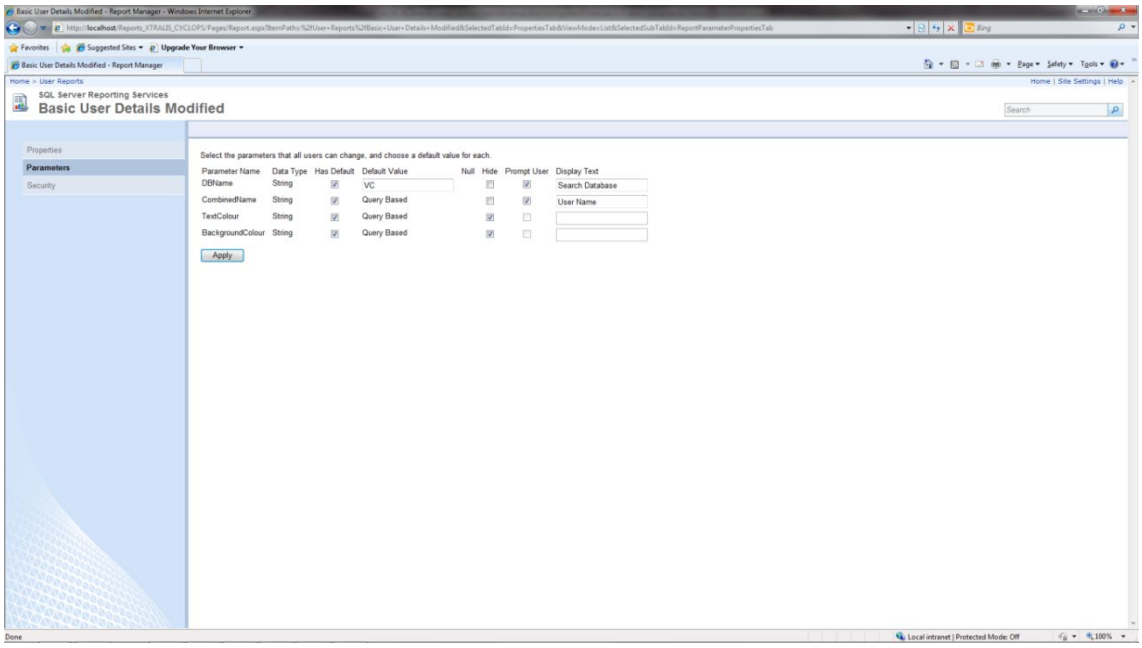
To change parameters of the new report, click the drop-down list to the right of the required title and the options will be displayed. Select the **Manage** option.



The properties page will be displayed.



Select the **Parameters** option and the parameters page will be displayed.

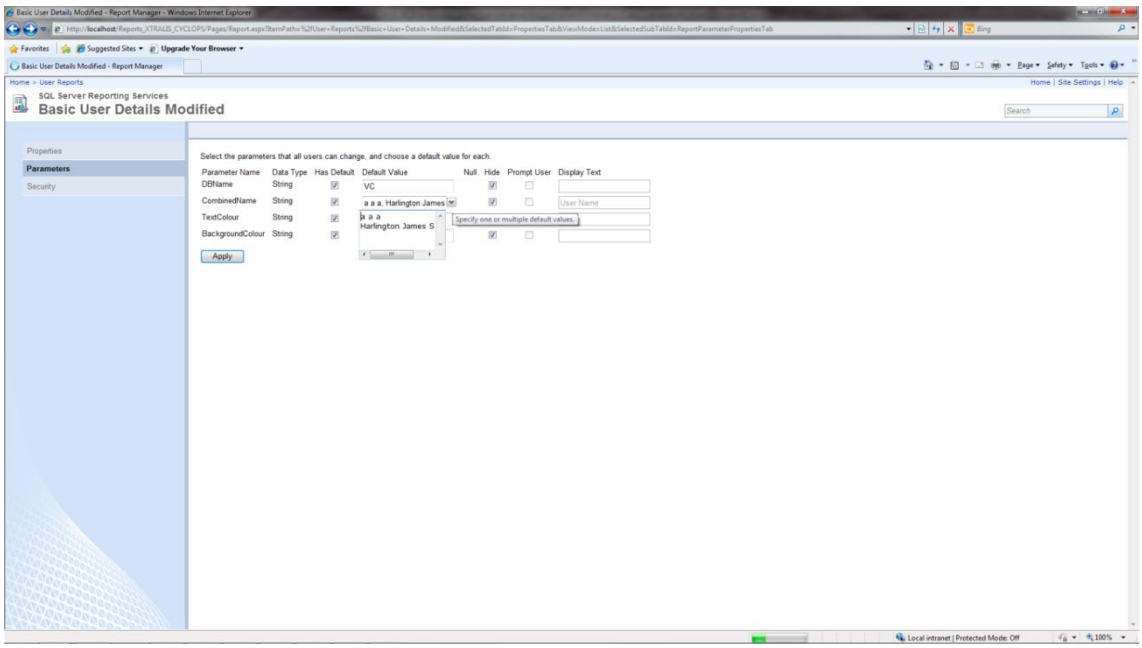


Note: Any changes must use valid names. Check valid name options via the drop down lists that are accessible in View mode.

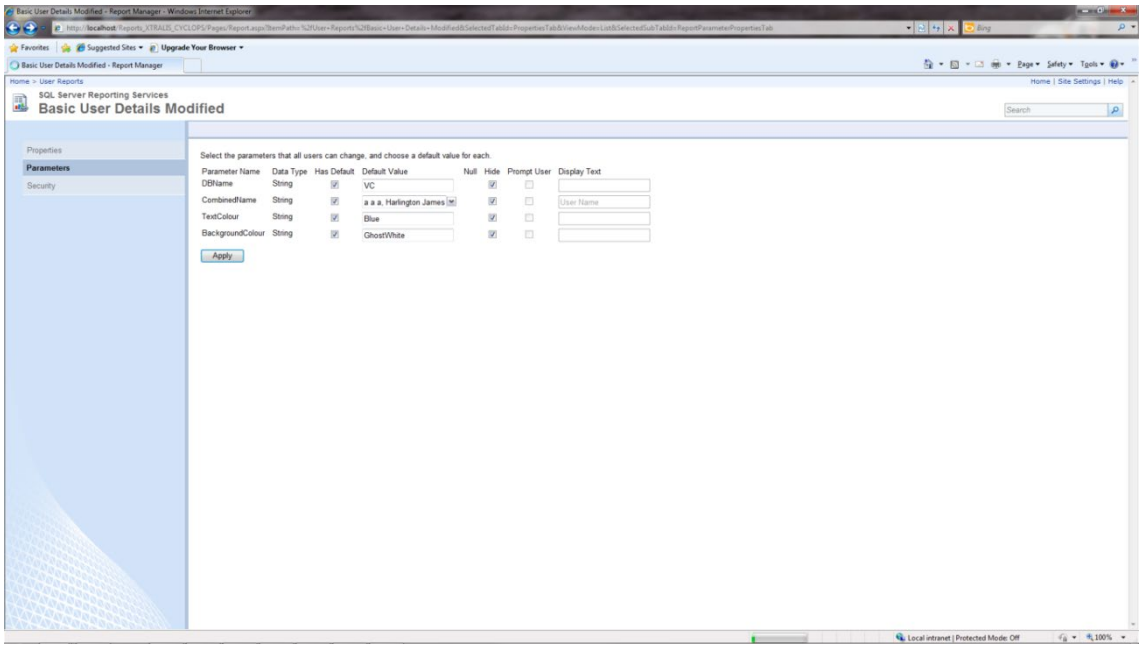
To change a Default Value, uncheck the **Has Default box** and click **Apply**. Re-check the **Has Default box** and click **Apply again**. An entry box will now appear under the Default Value. Change the Default Value as required then click **Apply**.

If any box has been left blank but an entry is mandatory, the comment ‘A value is required’ will be displayed.

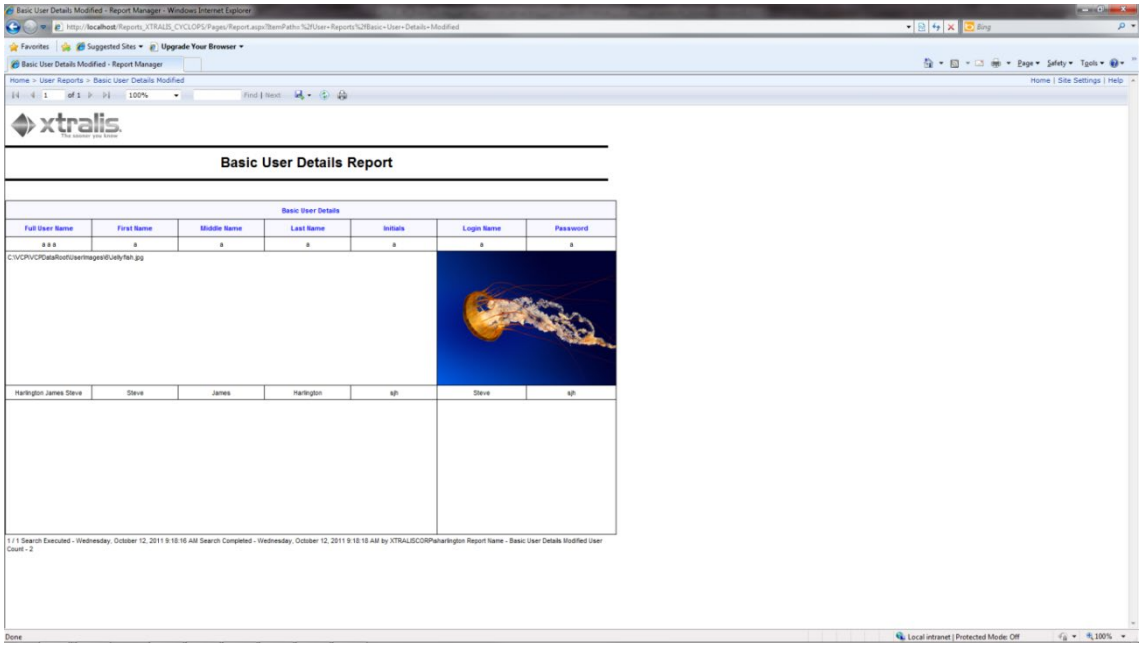
To change the Display Text, ensure the Prompt User box is checked, enter a valid name then click **Apply**. To leave the Display Text blank, uncheck the Prompt User box.



Once the default values have been set the parameters can be hidden from the user enabling the report to automatically run with the desired input. Check the **Hide box** and un-check the **Prompt User box** if this is required and select **Apply**. Select the **Report Name** on the top left hand side of the report to run the Basic User Details Modified report.



The Basic User Details Modified report will be displayed limited to the two users selected via the CombinedName input. Also note the report did not allow for any user input in this case.



2.18.1.1 Text and Background Colour

Valid options for Text Colour and Background Colour parameters are:

Transparent, White, GhostWhite, Snow, AntiqueWhite, NavajoWhite, WhiteSmoke, OldLace, FloralWhite, Ivory,

Black, DimGray, Gray, DarkGray, Silver, LightGrey, Gainsbro,

SlateGray, LightSlateGray, SlateBlue, DarkSlateBlue, MediumSlateBlue,

DarkKhaki, Beige, Brown, Chocolate, SaddleBrown, SandyBrown, PeachPuff, Peru, Linen, Bisque, DarkOrange, BurlyWood, Tan,

BlanchedAlmond, PapayaWhip, Moccasin, Orange, Wheat, DarkGoldenRod, GoldenRod, CornSilk, Gold, Khaki, LemonChiffon, PaleGoldenRod, LightGoldenRodYellow, Yellow, LightYellow,

Olive, OliveDrab, YellowGreen,DarkOliveGreen,GreenYellow, Chartreuse, LawnGreen, DarkSeaGreen, LightGreen, ForestGreen, LimeGreen, PaleGreen, DarkGreen, Green, Lime, Honeydew, SeaGreen, MediumSeaGreen, SpringGreen, MintCream, MediumSpringGreen,

Maroon, Red, DarkRed, IndianRed, Firebrick, Coral, LightCoral, RosyBrown, MistyRose, Salmon, Tomato, DarkSalmon, OrangeRed, LightSalmon, Sienna, SeaShell,

MediumAquamarine, Aquamarine, Turquoise, LightSeaGreen, MediumTurquoise, DarkSlateGray, PaleTurquoise, Teal, DarkCyan, Cyan, Aqua, LightCyan, Azure, DarkTurquoise,

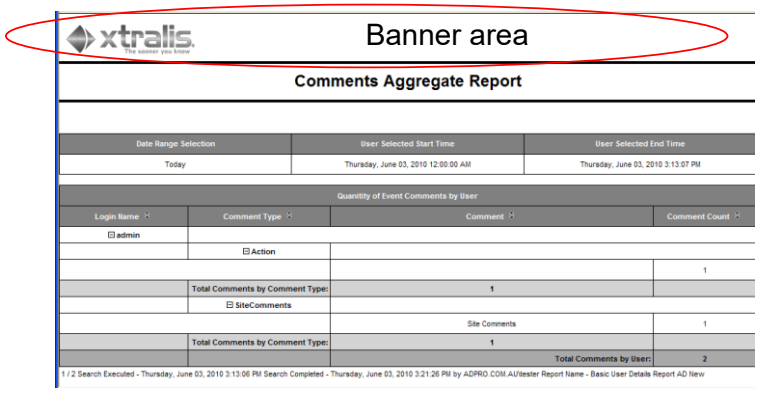
Blue, CadetBlue, PowderBlue, LightBlue, DeepSkyBlue, SkyBlue, LightSkyBlue, SteelBlue, AliceBlue, DodgerBlue, LightSteelBlue, CornFlowerBlue, RoyalBlue, MidnightBlue, Navy, DarkBlue, MediumBlue,

MediumPurple, BlueViolet, Indigo, DarkOrchid, DarkViolet, MediumOrchid, Thistle, Plum, Violet, Purple, DarkMagenta, Fuchsia, Magenta, Orchid, MediumVioletRed, DeepPink, HotPink, Lavender, LavenderBlush, PaleVioletRed, Crimson, Pink, LightPink.

2.18.2 Changing the Report Banner

To change the banner of a report, browse to the banner image location in the PC on which the database is installed. The default location is: C:\VCP\VCPDataRoot.

In the \VCPRS folder locate the file Report Banner.png. To change the banner, replace this image file but retain the name Report Banner.png. Image type can be jpg, bmp, png, or gif.

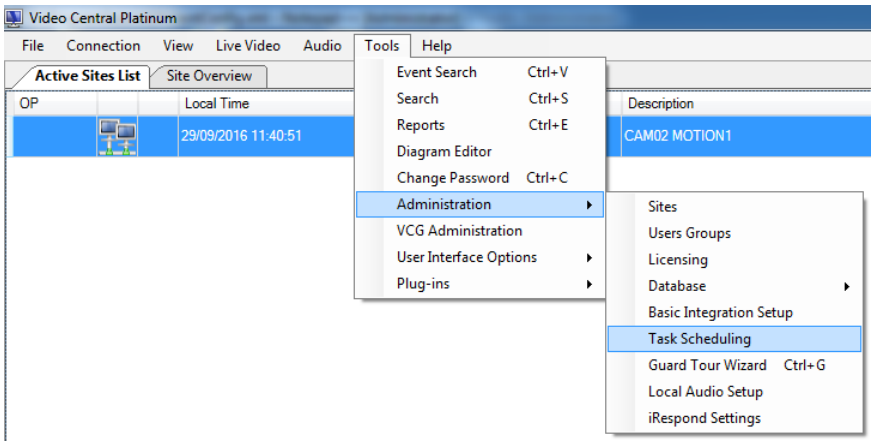


2.19 Task Scheduling

Task scheduling is a facility whereby generation of reports and archiving (backing up) of data are run according to a schedule at predetermined times.

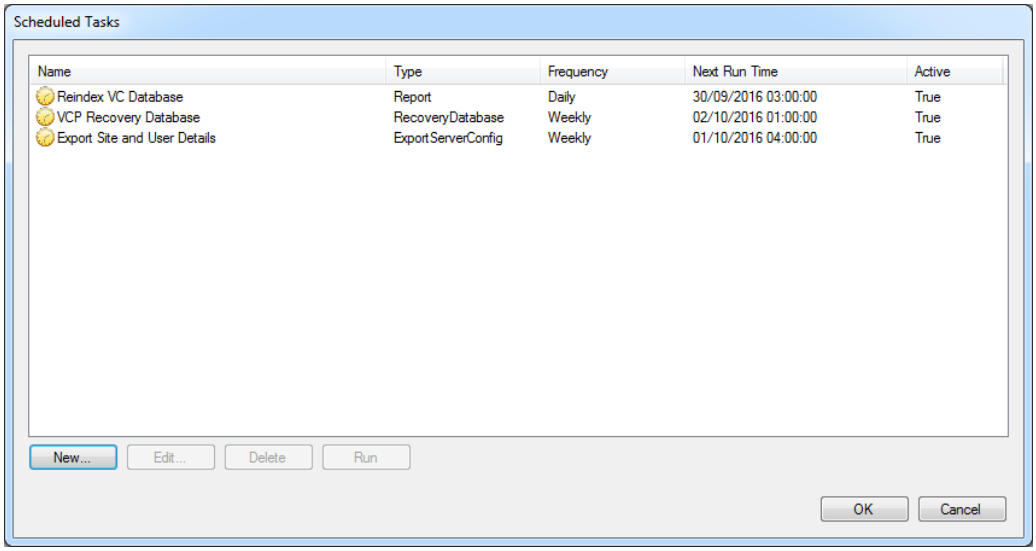
This facility can also be used to delete selected sites and associated events, either immediately or at a scheduled frequency. This function is described in ADPRO Video Central Platinum Database and Maintenance Manual, Doc 19118.

Access the Task Schedule Wizard via Tools > Administration > Task Scheduling and the Scheduled Tasks list will be displayed.

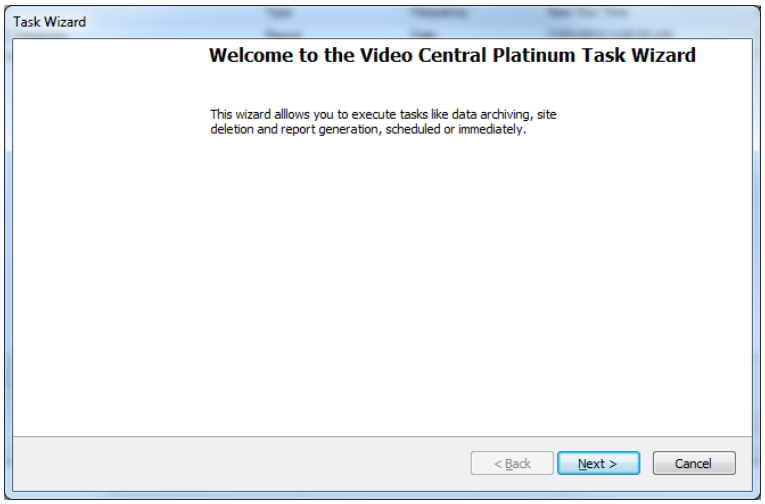


The Scheduled Tasks box below contains some examples of scheduled tasks.

To schedule a new task, click **New**. To edit, delete or run an existing task, select the task, then click the required icon and follow the prompts.



The Video Central Platinum Schedule Wizard Welcome screen will be displayed.



Click **Next** and the Wizard will guide you through the steps for creating schedules to archive and/or report.

2.19.1 Archiving Task Schedule

It is recommended that Archiving be scheduled to take place at times when it is known that the system is least busy because the archiving process will affect system performance.

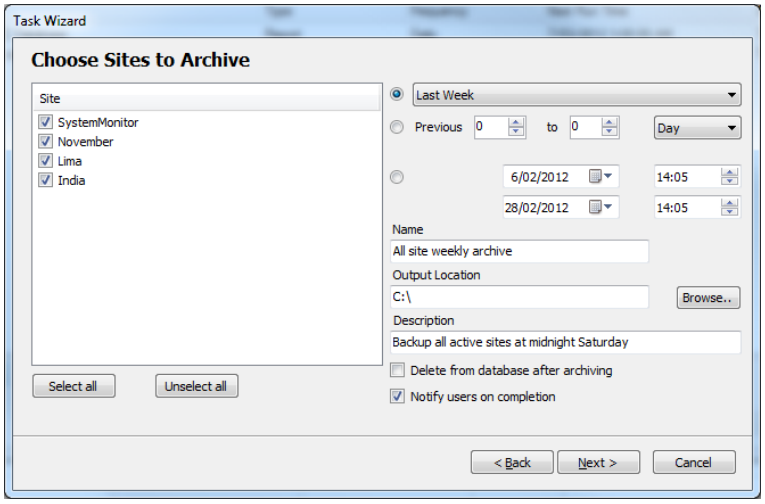
From the Choose Task type dialog select **Archive** then click **Next** and the Choose Sites to Archive dialog will be displayed.

In this dialog, the sites to archive, the archiving time period, and the output location for the archive can be specified.

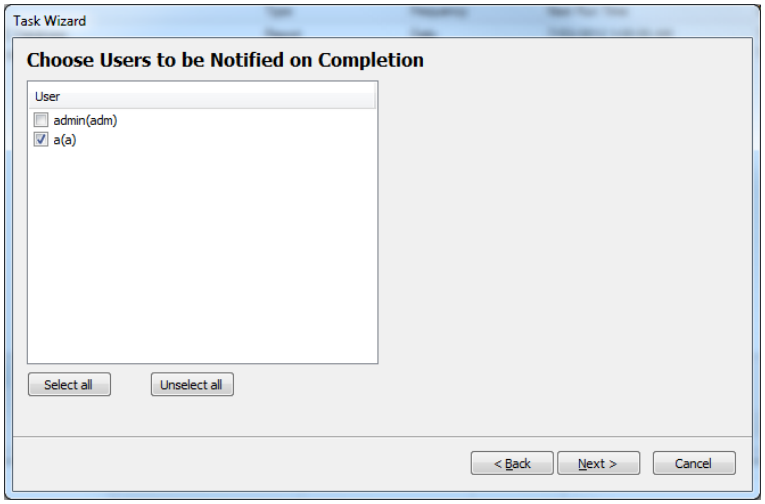
Check the button next to the type of time option required. Three types are available:

- Current or last day, week or month
- Previous interval of days, weeks, months, or years.
- Interval between specified dates and times

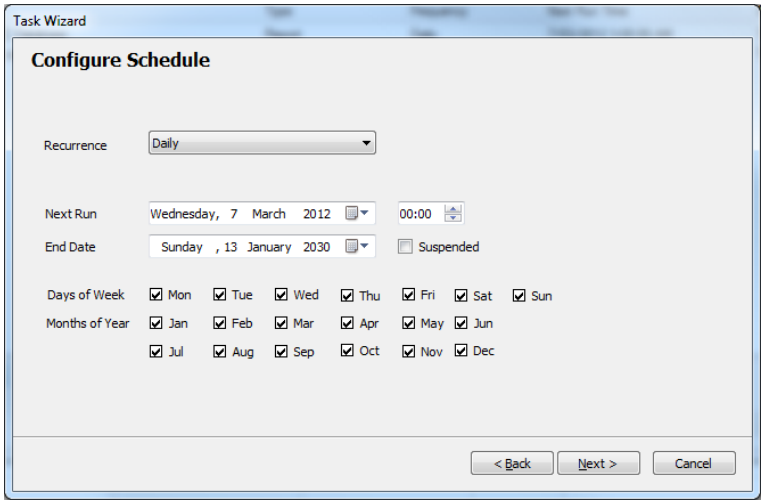
Choose a suitable name and a description for the task then browse to the location in which the archived data is to be stored. The following example shows that the previous week's data for all sites is to be archived at midnight each Saturday. Click **Next**.



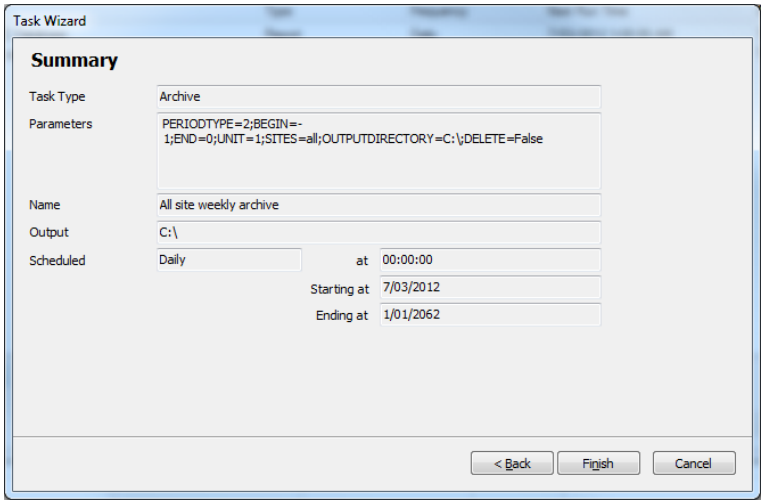
Notify users on completion button is checked by default. This allows users to be chosen to be notified on the completion of a task. Select the user groups as required then click **Next**.



In the Configure Schedule dialog, specify how often the task is to run and the time period over which this is effective then uncheck any days or months when the task is not to run.



Click **Next** to complete the Wizard and display the Summary.



Click **Finish**.

2.19.2 Reporting Task Schedule

It is recommended that the running of scheduled system reports takes place at times when it is known that the system is least busy because the compiling of reports will affect system performance.

Important: To execute a report via the task scheduler successfully all parameters (filters) must be set on the report. By default some of the reports listed within the report list do not have all the parameters set. As such if you wish to run one of these reports check the report executes through report manager first, then if required set the parameters that have not yet been set as outlined in Changing Report Parameters, Section 2.18.1.

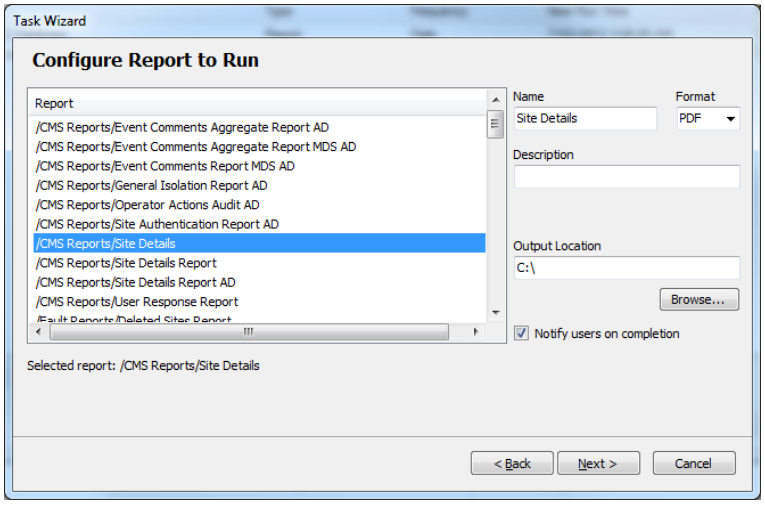
From the Choose Task type dialog select **Report** then click **Next** and Configure Report to Run dialog will be displayed.

In this dialog, the report to run, its format and the output location can be specified.

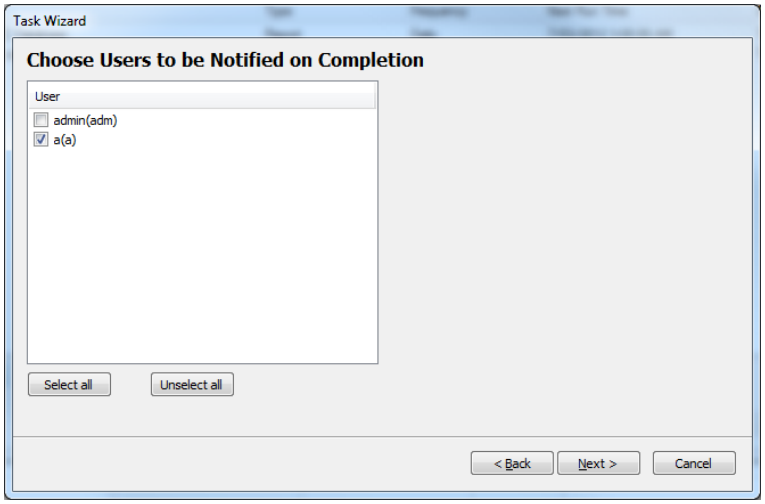
Select the report to run from the Report list.

Choose a suitable name and a description for the task and the format for the report then browse to the location in which the report is to be stored.

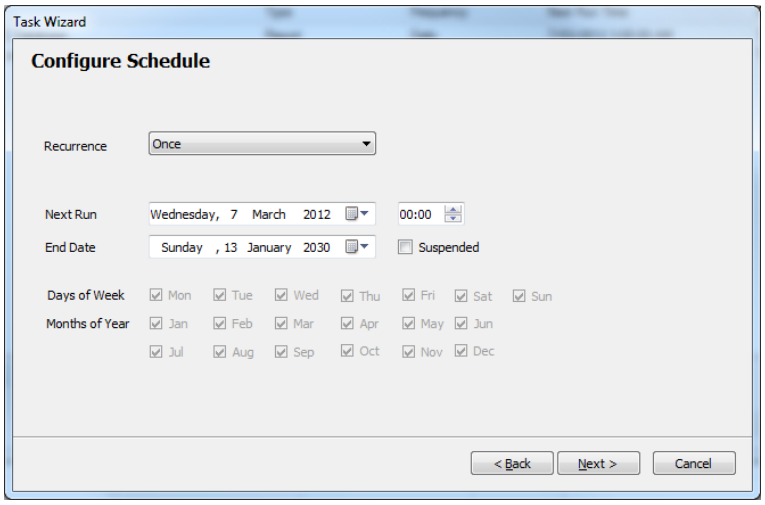
The following example shows that a site details report is to be created daily at midnight as a pdf file. The output format can be changed to either PDF, Excel or Word formats. Click **Next** to display the Configure Schedule dialog.



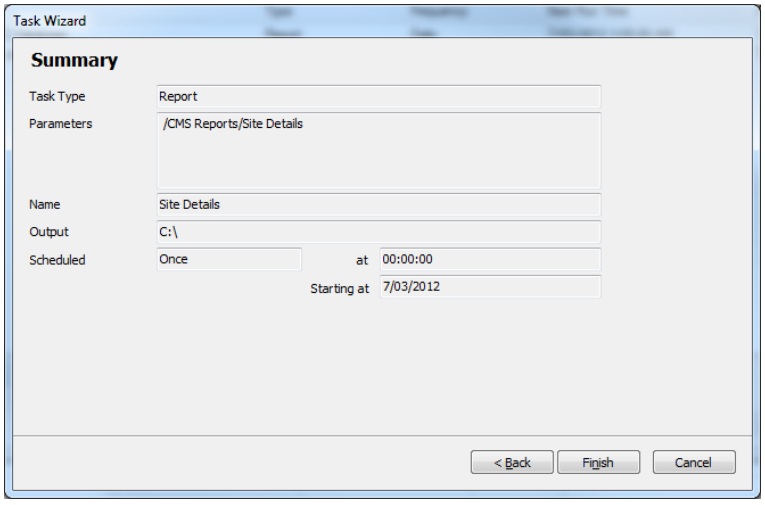
Notify users on completion button is checked by default. This allows users to be chosen to be notified on the completion of a task. Select the user groups as required then click **Next**.



In the Configure Schedule dialog, specify how often the task is to run and the time period over which this is effective then uncheck any days or months when the task is not to run.



Click **Next** to complete the Wizard and display the Summary.



Click **Finish**.

2.19.2.1 Integrated Reporting

Integrated reports provide a method for Video Central Platinum Reporting to integrate data from Video Central Platinum Databases into single reports.

Integrated reports are designed to run from the task scheduler. Note while the reports exist within Report Manager they are not designed to run from this location directly without a level of manual pre-processing. The task scheduler performs the required tasks and pre-processing in order for the reports to obtain data from Video Central Platinum Databases.

2.19.2.1.1 Pre-requisites

Video Central Platinum is installed.

2.19.2.1.2 Integrated Report Type and Location

CMS_User Reports – Provides detail from the User Details and Access Level.

Customer_Site Reports - Provides detail from the Site Details, Communication Details and Contact Details.

Event_Activity Reports - Provides detail from the Alarms/Events and reporting generated aggregate results.

Integrated reports of each type must reside under the following Report Manager/Server folder structure;

/Integrated Reports/CMS_User

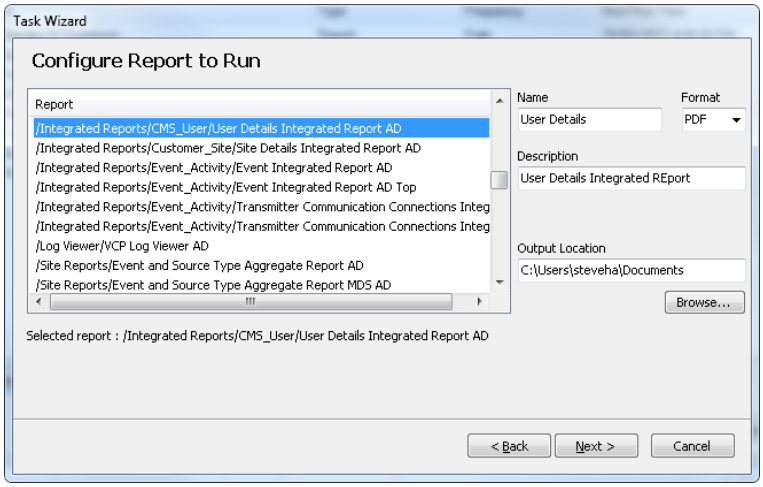
/Integrated Reports/ Customer_Site

/Integrated Reports/ Event_Activity

When an Event_Activity type report is executed, the date/time frame used for the search is that of the VCP Report Template for the VCP database.

2.19.2.1.3 Running an Integrated Report

Follow the process as outlined in Reporting Task Schedule, Section 2.19.2 and select one of the Integrated Reports. They can be identified by their path name and typically file name.



2.20 Private Wall Setup and Configuration

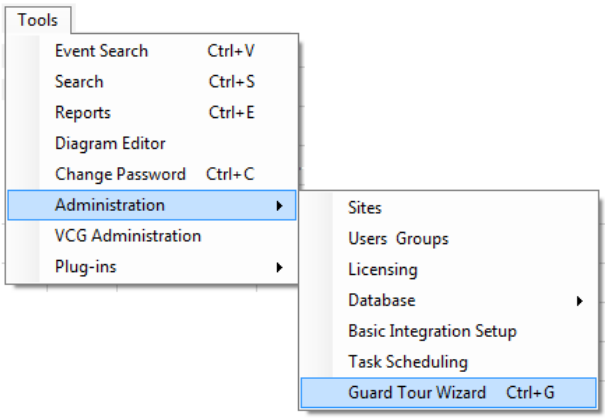
Private Wall is a core feature included with Video Central Platinum. It enables the operator to view one or more Guard Tours of any combination of cameras from their available sites on one monitor. A Guard Tour consists of one or more screens displaying video in one or more cameos.

Note: Private Wall connects directly to the alarm site, not via the Video Central Platinum. The following ports need to remain open in the Firewall and/or router settings:

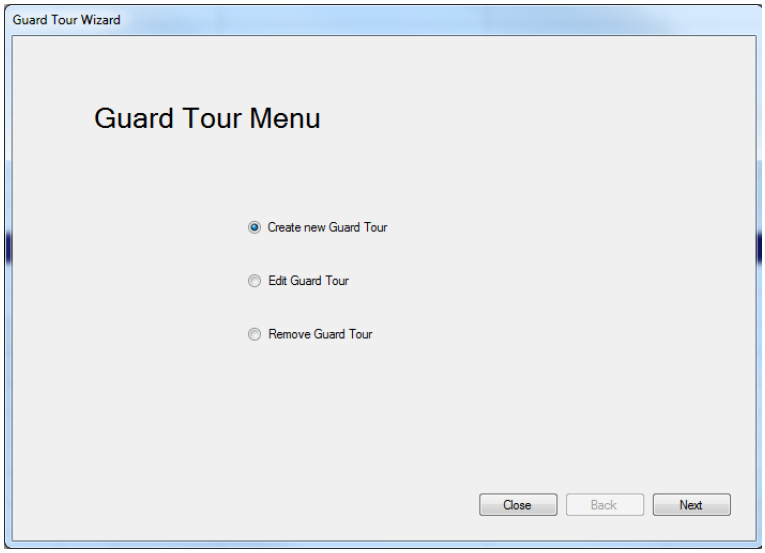
- Control Port: 2000
- RTSP Port: 554

If a Video Central Platinum user has permission to create and use the Private Wall feature they will see the **Private Wall** button enabled in their Controls box. Private Wall Guard Tours are created with the Guard Tour Wizard.

While in the Active Sites List, Private Wall users can launch the Guard Tour Wizard by selecting Tools > Administration > Guard Tour Wizard from the main menu.



The Guard Tour Wizard opens with the Guard Tour Menu screen, displaying options to Create a new Guard Tour; Edit an existing Guard Tour or Remove a Guard Tour.

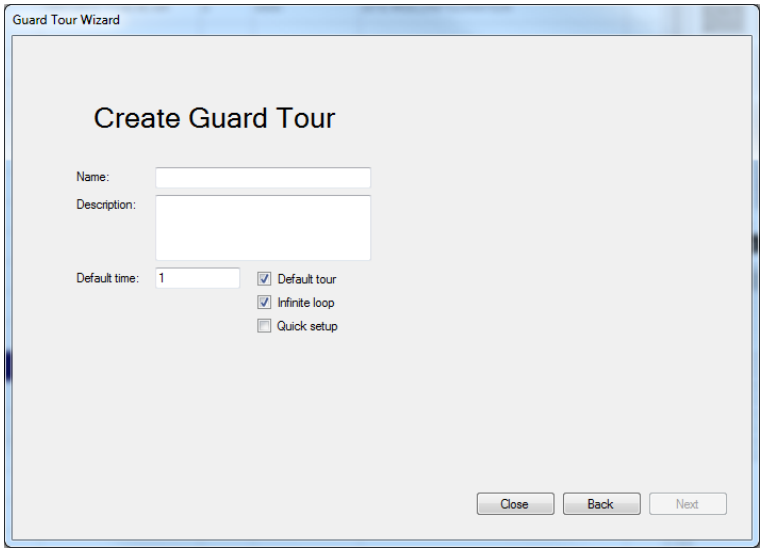


2.20.1 Create a Default Guard Tour

Launch the Guard Tour Wizard to create a default Guard Tour for Private Wall to display. While in the Active Sites List, select Tools > Administration > Guard Tour Wizard from the main menu. The Guard Tour Wizard will display the Guard Tour Menu screen.

From the Guard Tour Menu screen select the “Create new Guard Tour” option and click on the **Next** button. The Create Guard Tour screen will display fields to define the new Guard Tour.

Enter the Name and Description and click in the **Default tour** checkbox.

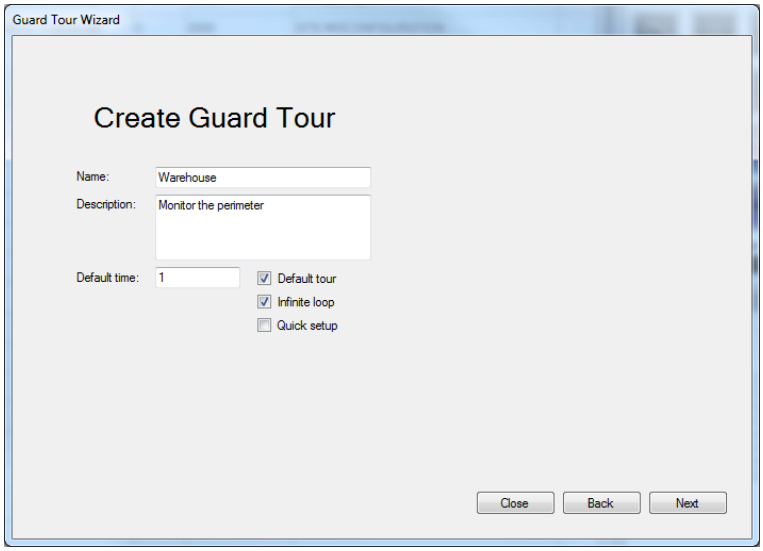


Click in the **Infinite loop** checkbox if you want this tour to run continuously.

Default time should normally be set to 1 second.

2.20.1.1 Default Guard Tour with One Screen

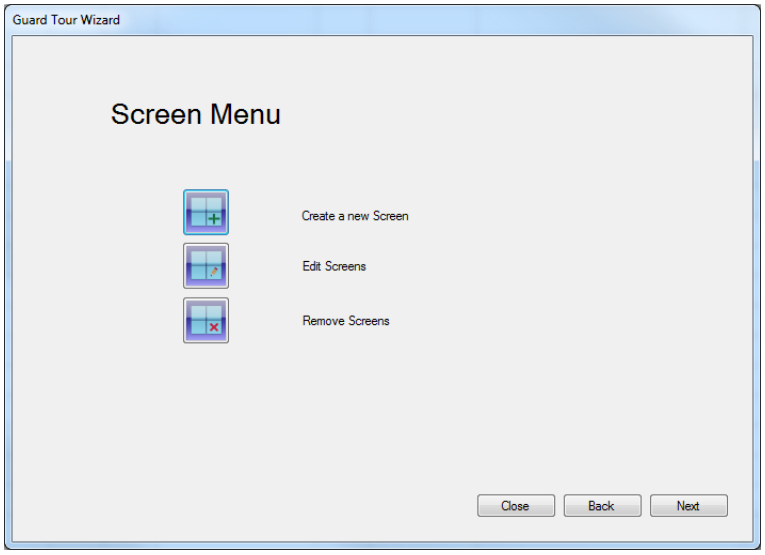
From the Create Guard Tour screen a Guard Tour containing one screen can be created. The screen can have up to twenty cameos and it can be set to display continuously.



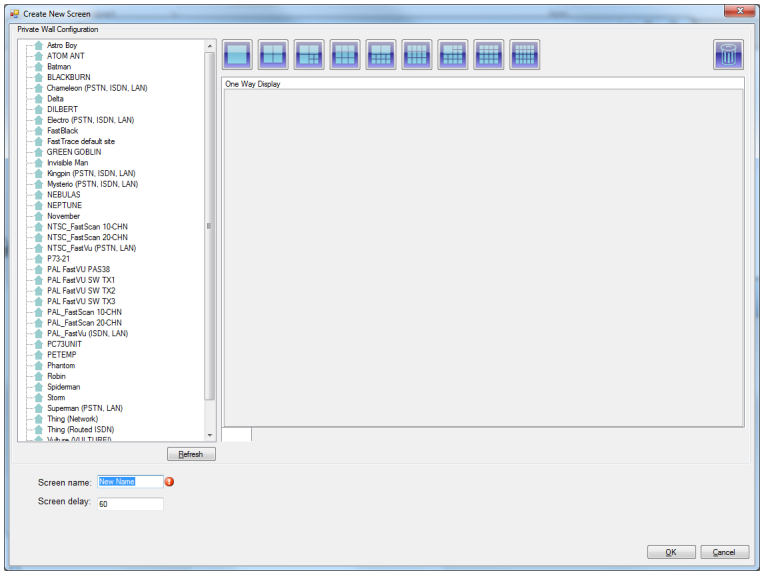
Click **Next** after the detail for this Guard Tour has been entered.

If you click **Close** you will be asked if you want to abort the current operation and you will be advised that all changes since the last full loop will be lost.

When the Screen Menu is displayed click **Create a new Screen**.



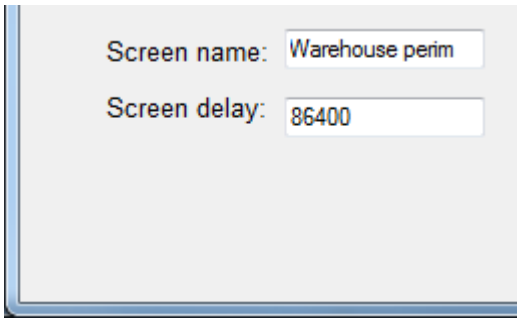
The Guard Tour Wizard displays the Create New Screen window, showing a tree view of the available Sites on its left side, the screen split on the right side and both the Screen name and Screen delay at the bottom left of the screen



Click on one of the icons above the view of the screen split to alter the number of cameos the screen will display.

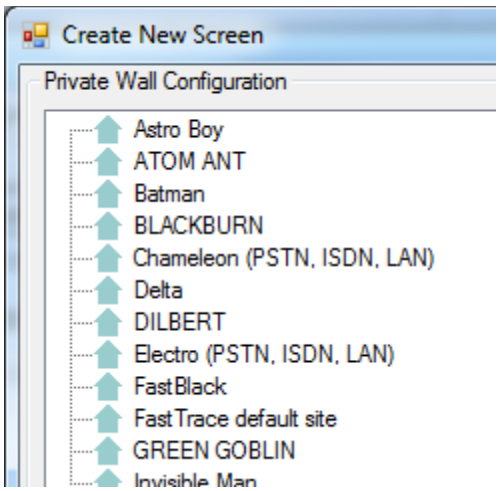


Edit the Screen name and Screen delay as required. The Screen delay is its display time in seconds. After this period Private Wall will display the next screen in the Guard Tour.



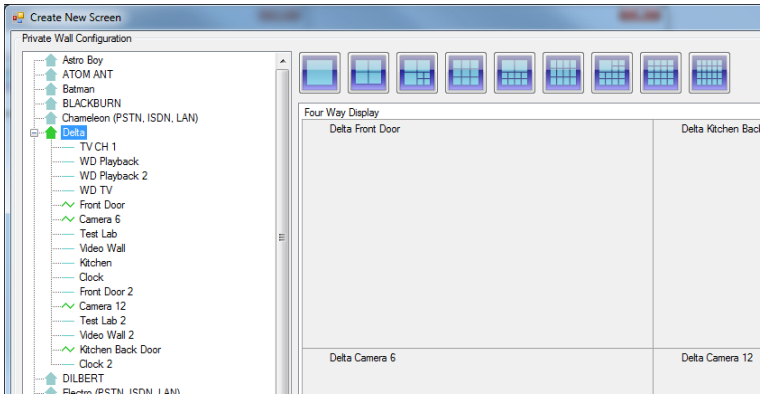
Set the Screen delay to 86400, which is the number of seconds per day for a screen to display continuously throughout the day. For further explanation, refer to Section 2.20.8 Guard Tour Guidelines.

Double-click on a Site from the tree view of available sites to connect to it, making its cameras available to be shown on the Guard Tour screen cameos.



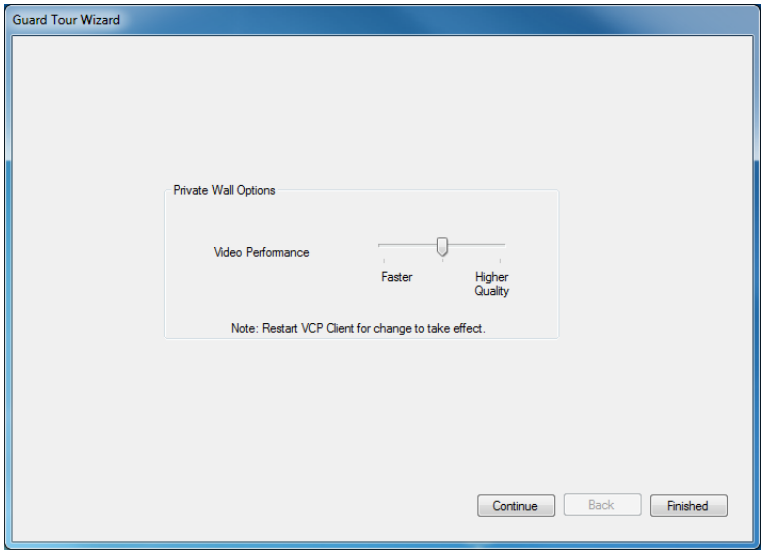
When the icon changes from plain blue  to blue with a '+' to its left  the site cameras are available. Click on the '+'  to view the site's available cameras.

Drag cameras to cameos and drop them individually, or simply drag the **site** icon  to the first available cameo and the cameras will populate the screen cameos sequentially. When the connection is made the site icon will change colour from blue to green; the connected cameras will display as branches in the site tree with green 'connected' icons  and the unconnected cameras will continue to display as site tree branches with blue 'available' icons .



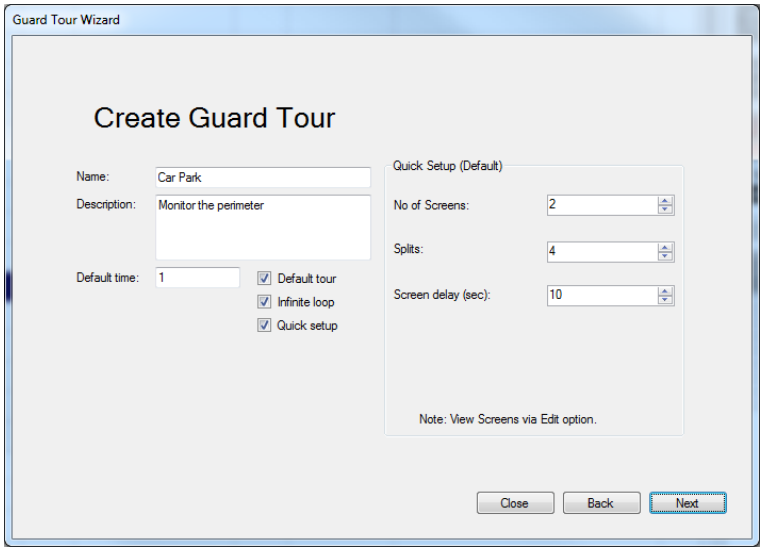
When the camera has been set for each cameo, click **OK** to save the screen with these settings. If you do not want to save the screen click **Cancel** instead. The Guard Tour Wizard will display the Screen Menu.

Click **Next** and when the Guard Tour Wizard displays the final screen click **Finished**.



2.20.1.2 Default Guard Tour with Multiple Screens

To create a default Guard Tour with multiple screens select Tools > Administration > Guard Tour Wizard from the main menu to open the Guard Tour Menu. Select Create new Guard Tour to open the Create Guard Tour screen.



Enter the Name, Description and Default time. The Default time should normally be set to 1.

Select the Default tour option.

Select Infinite loop to display the first screen again at the end of the last screen display for this Guard Tour. The Private Wall always displays a blank screen while the Default time period is counting down before it displays the first Guard Tour screen.

Select Quick setup to set a number of screens with the same number of splits and screen delays per screen. The screen delay is the number of seconds the screen will display its cameos before closing. These defaults can be edited at any time.

Click **Next**. The Guard Tour Wizard will display the Screen Menu. Click **Edit Screens** to set the screen properties, as described in Section 2.20.2.1.

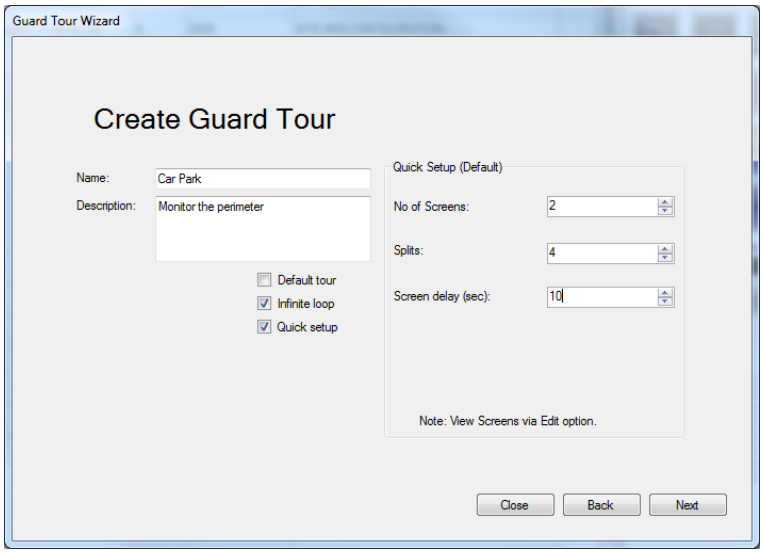
2.20.2 Create a Guard Tour with Multiple Screens

Launch the Guard Tour Wizard to create a Guard Tour with multiple screens for Private Wall to display. While in the Active Sites List, select Tools > Administration > Guard Tour Wizard from the main menu. The Guard Tour Wizard will display the Guard Tour Menu screen.

From the Guard Tour Menu screen select the “Create new Guard Tour” option and click on the **Next** button. The Create Guard Tour screen will display fields to define the new Guard Tour.

Enter the Name, Description and select the **Quick setup** option. Extra fields will be displayed.

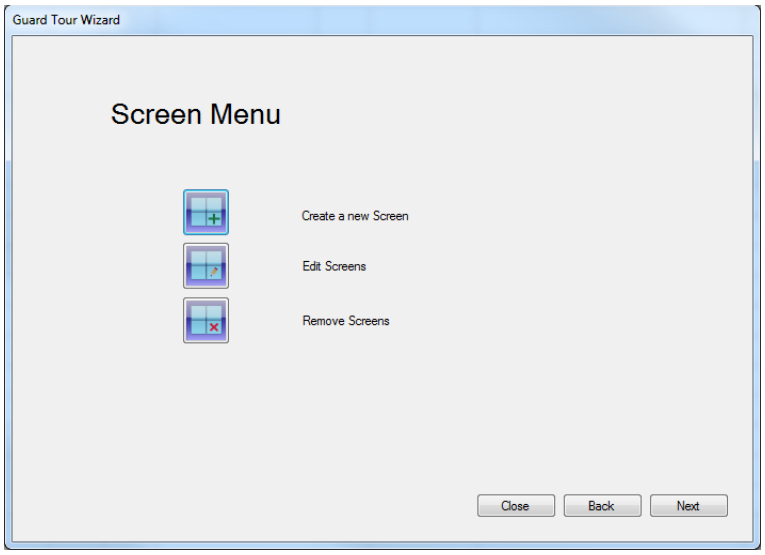
Enter the No of Screens, Splits, and Screen delay fields to set a number of screens with a default number of splits and a default screen delay for those screens.



Click **Next** and the Screen Menu will be displayed.

If you click Close you will be asked if you are sure you want to abort the current operation because your Guard Tour Wizard changes will be lost.

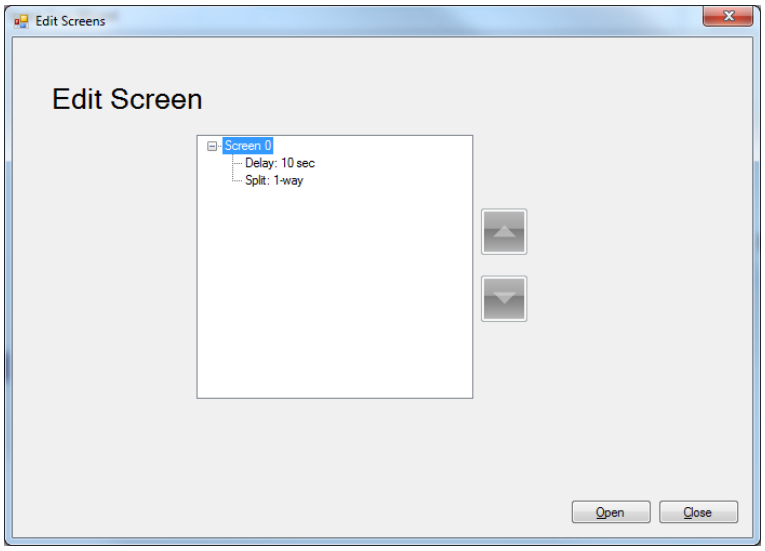
Complete a full Guard Tour Wizard Loop to Save Changes.



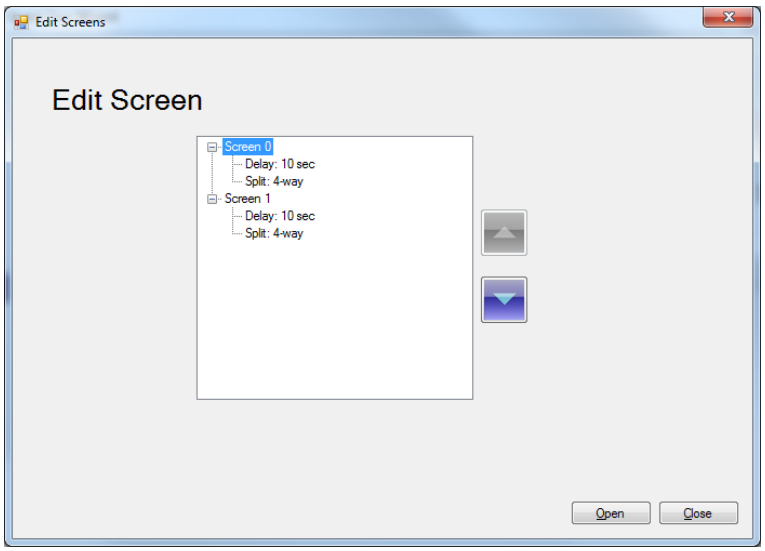
Edit each of the Guard Tour screens, as described in the Section 2.20.2.1

2.20.2.1 Edit a Guard Tour Screen

From the Guard Tour Wizard Screen Menu click **Edit Screens** to open the Edit Screens window. If the Guard Tour contains one screen click **Open** to display its detail in the Edit Screen window.

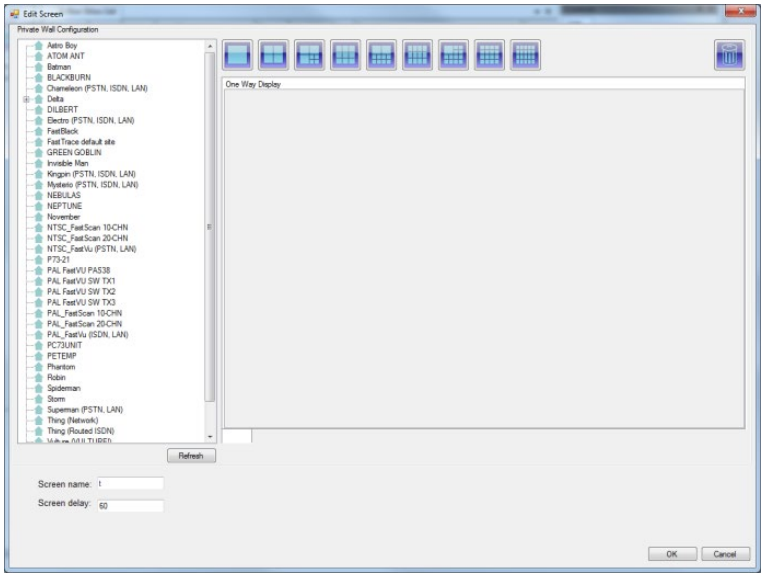


For a Guard Tour containing more than one screen, when the Edit Screens window opens it will display a tree view of the screens in this Guard Tour.



Click on a **screen title** and then **Open** to display the detail for that screen in the Edit Screen window.

When the Edit Screen window opens it displays the available Sites on its left side, the screen split on the right side and both the Screen name and Screen delay at the bottom left of the screen.



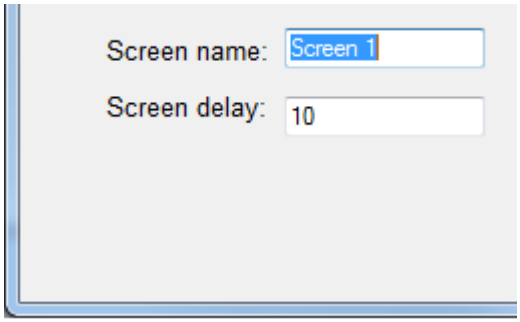
2.20.2.2 Set the Screen Split

Click on one of the icons above the view of the screen split to alter the number of cameos the screen will display.



2.20.2.3 Set the Screen Delay

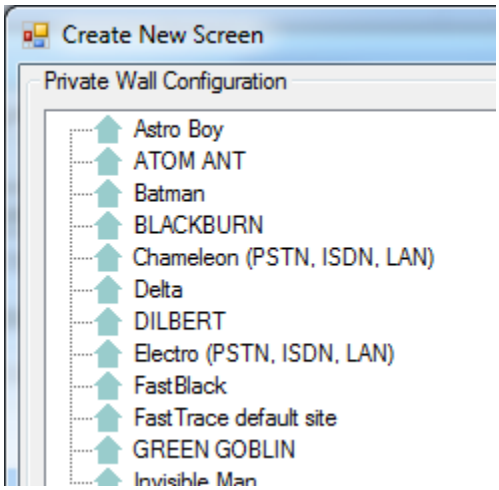
Edit the Screen delay as required. The Screen delay is its display time in seconds. After this period Private Wall will display the next screen in the Guard Tour.



The next screen will be displayed at the end of the screen delay.

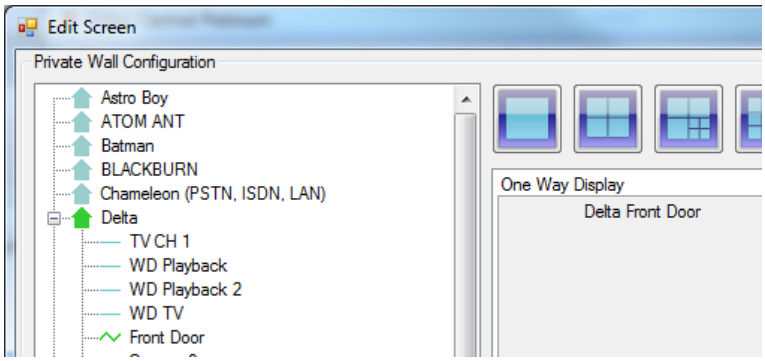
2.20.2.4 Set the Camera for Each Screen Cameo

Double-click on a Site from the tree view of available sites to connect to it, making its cameras available to be shown on the Guard Tour screen cameos.



When the icon changes from plain blue to blue with a '+' to its left the site cameras are available. Click on the '+' to view the site's available cameras.

Select a camera for each cameo, or simply drag the site to the first available cameo and the cameras will populate the screen cameos sequentially.
When the connection is made the site icon will change colour from blue to green; the connected cameras will display as branches in the site tree with green 'connected' icons and the unconnected cameras will continue to display as site tree branches with blue 'available' icons .

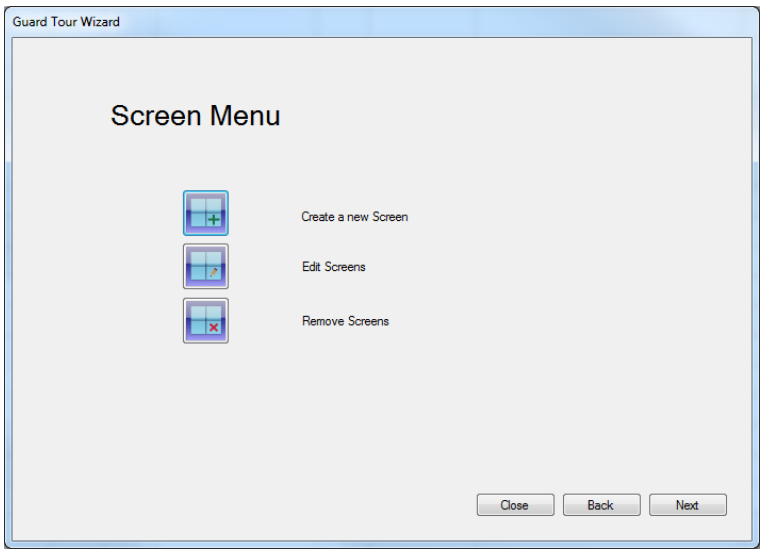


2.20.2.5 Complete Editing the Guard Tour Screen

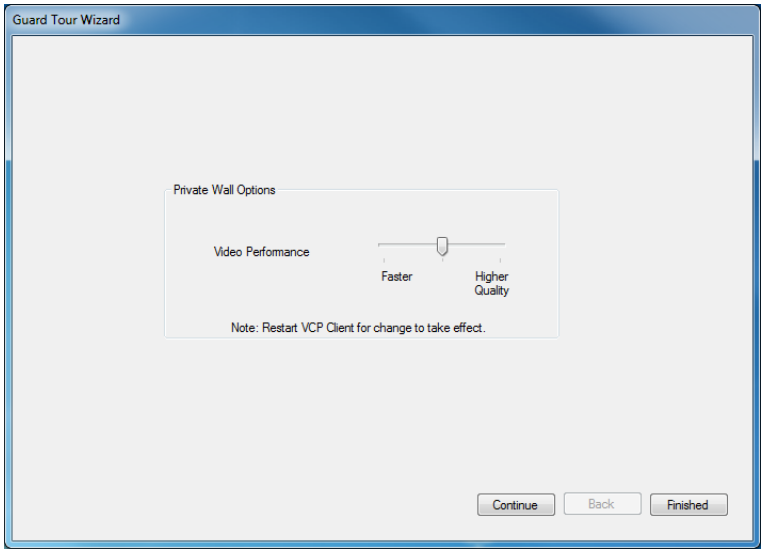
Click **OK**. The Edit Screens window opens, displaying the Edit Screen tree view. If you click **Cancel** instead the changes you made to the screen will be lost.

If more screens need to be configured select the screen to be edited and click **Open**.

Apply the desired settings in the Edit Screen until all screens have been configured and then, from the Edit Screen menu click **Close**. The Guard Tour Wizard will display the Screen Menu.

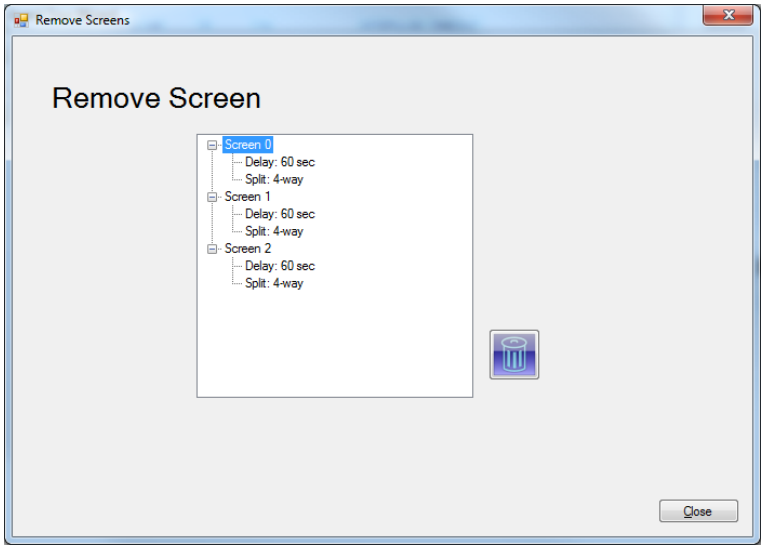


Click **Next** and then click **Finished**.



2.20.2.6 Remove Screens

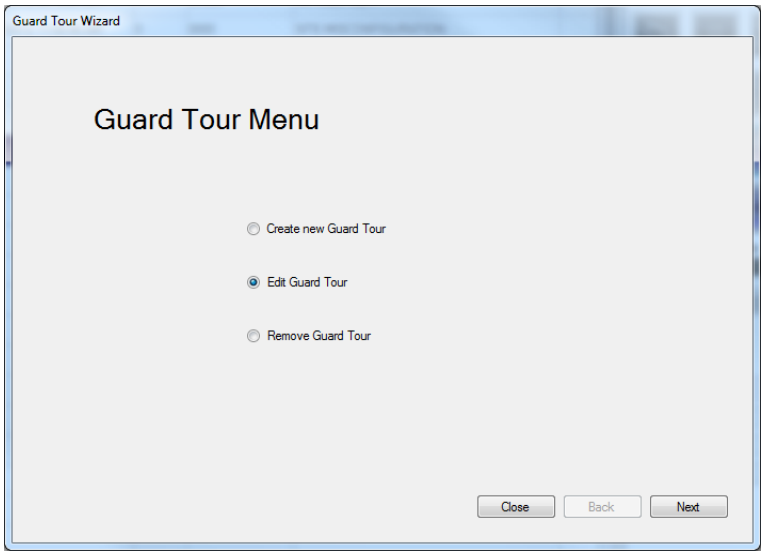
From the Guard Tour Wizard Screen Menu click **Remove Screens** to open the Remove Screen window. If the Guard Tour contains more than one screen select the screen to remove from the list before clicking the **Delete** button. The selected screen will be deleted from the Guard Tour.



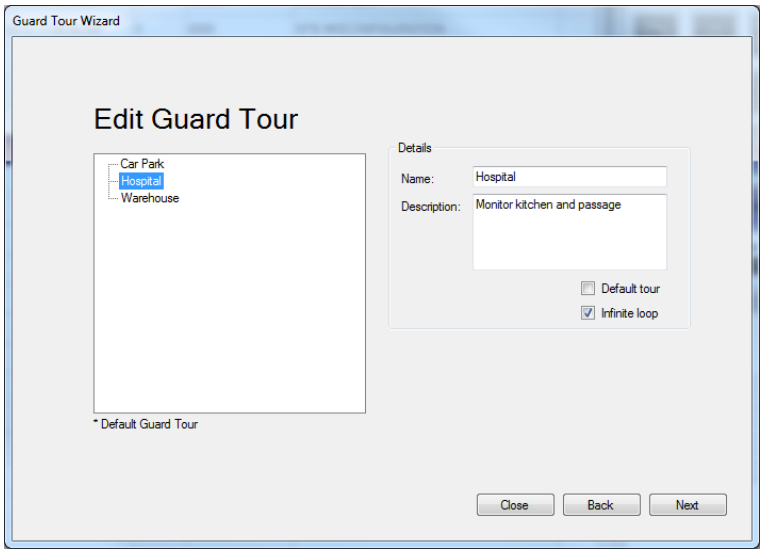
2.20.3 Edit an Existing Guard Tour

Launch the Guard Tour Wizard to edit an existing Guard Tour for Private Wall to display. While in the Active Sites List, select Tools > Administration > Guard Tour Wizard from the main menu. The Guard Tour Wizard will display the Guard Tour Menu screen.

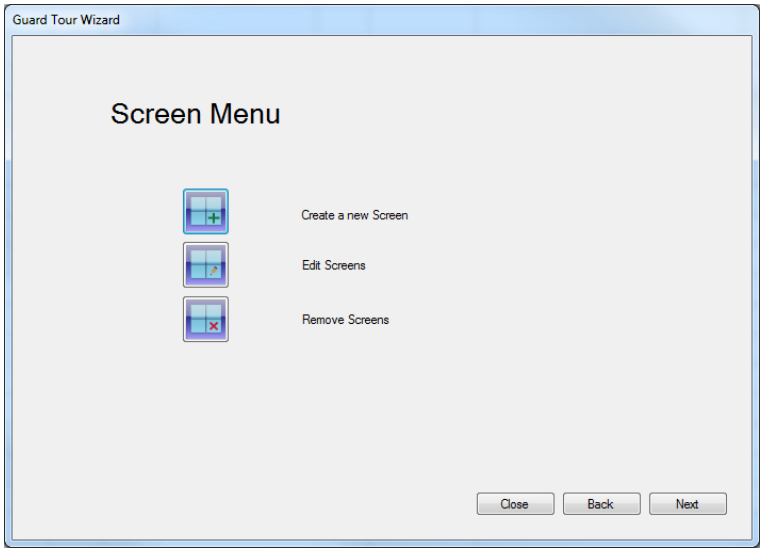
From the Guard Tour Menu screen select the Edit Guard Tour option and click on the Next button.



The Edit Guard Tour screen will display a list of current Guard Tours. Select a Guard Tour from the list and its settings populate the Details fields, where they can be edited.



Click **Next**. The Guard Tour Wizard displays the Screen Menu, from which you can create a new screen, edit existing screens or remove screens for this Guard Tour.



2.20.3.1 Create a New Screen

The procedure for creating a new screen in an existing Guard Tour has been described in Section 2.20.1.1.

2.20.3.2 Edit Screens

The procedure for editing a screen in an existing Guard Tour has been described in Section 2.20.2.1

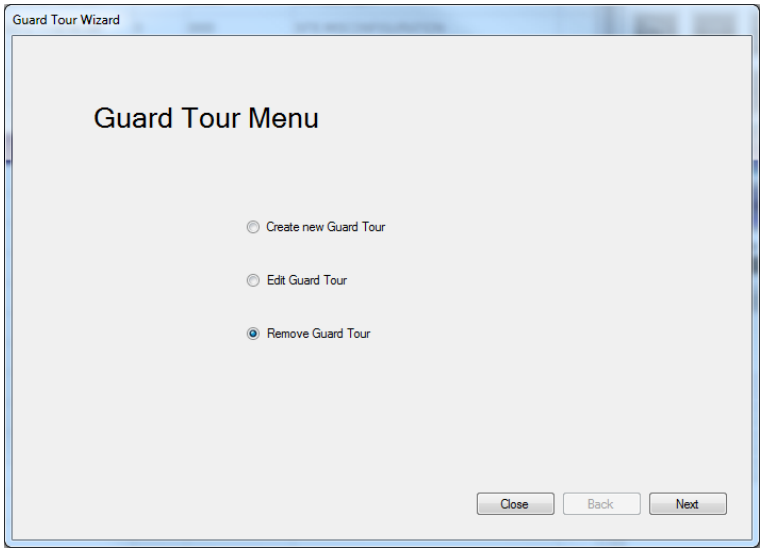
2.20.3.3 Remove Screens

The procedure for removing screens from an existing Guard Tour has been described in Section 2.20.2.6.

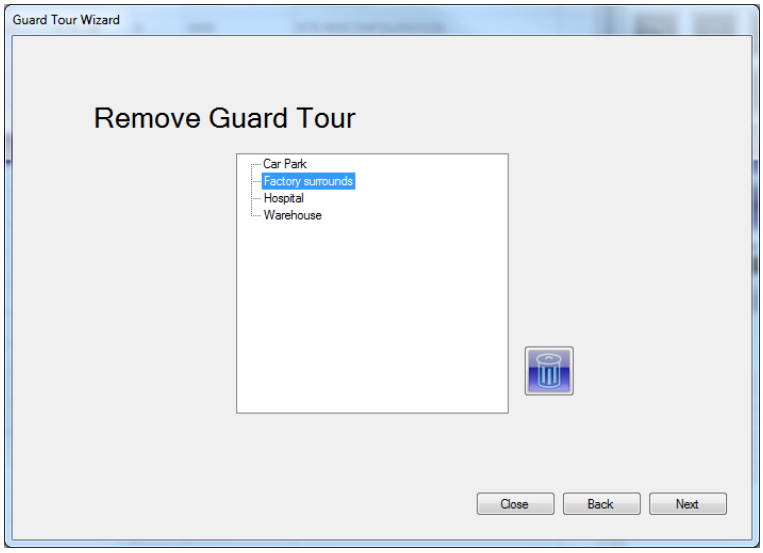
2.20.4 Remove a Guard Tour

Launch the Guard Tour Wizard to remove a Guard Tour from Private Wall. While in the Active Sites List, select Tools > Administration > Guard Tour Wizard from the main menu.

The Guard Tour Wizard will open the Guard Tour Menu screen. Select Remove Guard Tour and click **Next**.



The Guard Tour Wizard will display the Remove Guard Tour screen with a list of current Guard Tours. Select a Guard Tour and click on the **Delete** button.



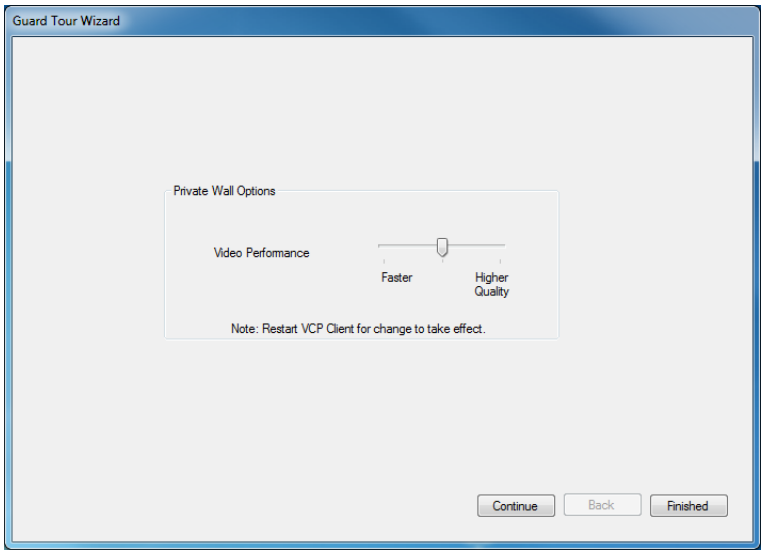
The Guard Tour list will show that the selected Guard Tour has been removed from the Guard Tour list.

Click **Next** to complete the deletion. The Guard Tour Wizard will display the screen displaying the options to continue to work on a new Guard Tour, create/edit or remove more screens from the current Guard Tour, or finish working with the Guard Tour Wizard.

If you click **Close** you will be asked if you are sure you want to abort the current operation because your Guard Tour Wizard changes will be lost. Complete a full Guard Tour Wizard Loop to Save Changes. Click **Yes** if you are sure you do not want to delete the Guard Tour.

2.20.5 Complete a full Guard Tour Wizard Loop to Save Changes

Whenever you create or edit Guard Tours and their screens, the wizard saves these changes when you arrive at the screen shown below. The screen displays the options to continue to work on a Guard Tour or finish working with the Guard Tour Wizard. If you click **Close** or **Cancel** on any screen before arriving at this screen you have not completed the full loop for the current process and changes made to Guard Tours and screens during the current process have not been saved. For a detailed explanation on the Video Performance option, refer to Section 2.20.6 Video Performance.



2.20.6 Video Performance

The Video Performance option sets the maximum video quality for Private Wall cameos appropriate to the available network bandwidth.

Private Wall can display a range of video resolutions in each cameo, depending on the quality level set for the camera a cameo is displaying and the result of several rules that are applied to manage the video quality for each cameo.

The available video resolutions are: QCIF (176 x 144 pixels), CIF (352 x 288 pixels), 2CIF (704 x 288 pixels) and 4CIF (704 x 576 pixels).

Video Performance is set with the Video Performance slider just before an operation is finished in the Guard Tour Wizard. The Video Performance slider has three settings: 'Faster', a middle setting and 'Higher Quality'.

Faster: This setting requires the least network bandwidth to display the video in its cameo. The maximum video resolution at this setting will be QCIF (176 x 144 pixels). This setting is advised for installations where a slower connection to the VCP Server via the network is available (slower ADSL).

Middle setting: This setting requires more network bandwidth to display the video in its cameo than the 'Faster' setting, but displays better quality video than the 'Faster' setting does. The maximum video resolution at this setting will be CIF (352 x 288 pixels). This setting is advised for installations where the connection to the VCP Server via the network uses ADSL.

Higher Quality: The highest quality setting requires the most network bandwidth to display video on its cameo but allows cameos to display up to 4CIF (704 x 576 pixels). This setting is advised for installations where the connection to the VCP Server is via a network LAN (Local Area Network).

While moving the slider towards **Faster** will update video more quickly by reducing its resolution and quality, there are alternative methods you can use to display video more quickly without reducing the video quality:

- Reduce the number of cameos (camera images) shown on one monitor to increase the responsiveness of the display.
- Display one cameo only on a monitor to display the feed from a high quality camera, optimising the image quality and responsiveness for that camera.
- Fit a faster video card, or a video card with more dedicated video memory, to increase the camera image responsiveness, while maintaining its image quality and displaying a higher number of cameos per monitor.

2.20.7 Protection Mode

Protection Mode protects Private Wall from overloading the system by displaying video at too high a resolution.

Video Central Platinum uses a series of rules to manage the video quality for each cameo displaying video from a camera, regardless of the site the camera is associated with.

Rule 1 protects the CPU from being overloaded. The quality of the images displayed in Private Wall cameos are determined by an algorithm that calculates whether an image resolution, for example 4CIF, can actually fit within the cameo, based upon the video card resolution settings and the dimensions of the cameo in play. If it can fit then the respective resolution will be displayed. If the image resolution does not fit then the algorithm will display the largest available image resolution that can fit.

Rule 2 protects the Network connection from being overloaded. The slider in the VW setup determines the max quality that can be displayed to be either 4CIF, CIF or QCIF. This is required for cases where insufficient communications bandwidth is available.

Rule 3 uses a feature of Fast Trace 2 (FT2) to protect the CPU from being overloaded. When a user connects to the FT2 and takes control of the FT2 video stream, by connecting to the camera from the VCP User Interface as an example, they may set a higher quality that can fit into the Private Wall cameo. In this case protection mode is entered. In Protection Mode the resolution the user requested is maintained, however the picture update rate drops to I-Frame mode where it updates the video once every 4 seconds and a shield icon is displayed in the top right-hand side of the cameo. Once the user drops control of the camera, by disconnecting from the camera in the VCP User Interface for this example, Private Wall will take control again and drop out of protection mode.

Note: Protection mode maybe entered permanently for IP Cameras if the lowest resolution the camera can be provided is higher than the maximum private wall quality set during setup.

2.20.8 Guard Tour Guidelines

For using a Guard Tour with a single screen and the Infinite loop setting it is recommended to set the Screen delay to 86400. This number is the number of seconds in a 24 hour period. This prevents the screen from refreshing periodically throughout the day.

The available image resolutions are: 4CIF(704 x 576 pixels), 2CIF(702 x 288 pixels), CIF(352 x 288 pixels) and QCIF(176 x 144 pixels).

2.21 Diagrams

Diagrams enable Operators to control Video Central Platinum from a map based graphical interface.

Typically, whilst viewing the Active Sites List, the Operator will start with the Top Level map, selecting buttons or hot spots and their associated macros to connect to sites. Once a site has been connected and Site View mode is entered, Video Central Platinum will automatically load the associated site map, which is used to control site functions.

When the site is acknowledged or disconnected the Top-Level map is automatically loaded.

Diagrams can include the following control types:

- connecting and disconnecting remote sites
- selecting cameras, image qualities, multi-screen views
- performing PTZ operations (preset functions only)
- activating remote outputs
- controlling audio operations
- viewing current status of alarm inputs and acknowledge alarms.

Diagrams are created using the Interactive Diagram Editor (IDEditor) which is accessed via Tools > Diagram Editor. The IDEditor tab will be displayed within the Active Sites List.

Note: Video Central Platinum Site Level maps must be created using the Video Central Platinum Diagram Editor.

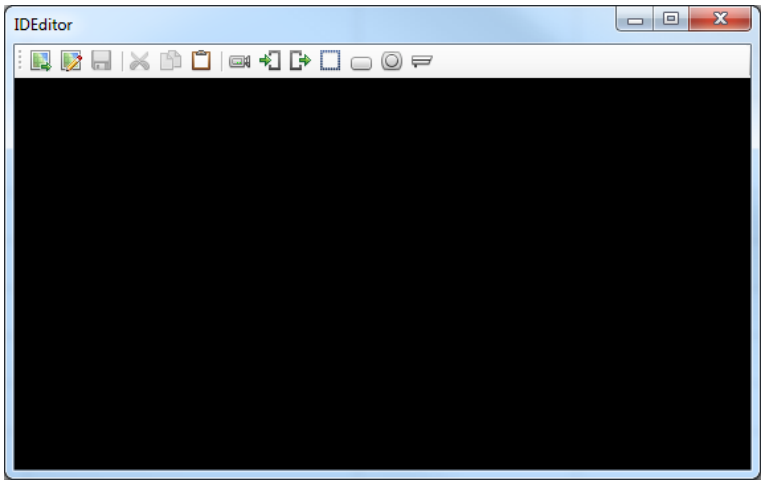
Special buttons and hot spots can be overlaid on the diagram and used to initiate certain actions.

Interactive elements may have different colours or appearance to represent their current state. For example, states may be represented as active, inactive or not available.

When an Interactive Element is clicked during operational mode, Video Central executes a macro, which is created, edited and assigned via IDEditor.

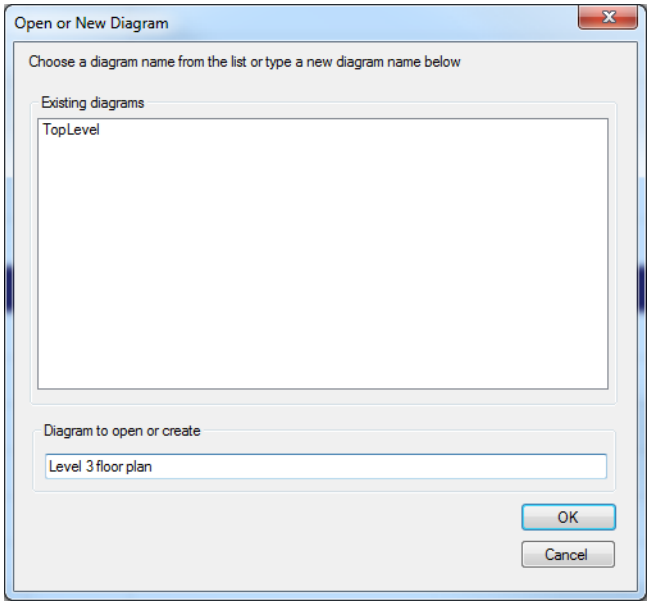
2.21.1 Creating and Editing Diagrams

To create a new Diagram click the **Open** icon  and the Open or New Diagram dialog will be displayed.



To open an existing diagram for editing select the name from the Existing Diagrams list then click **OK**.

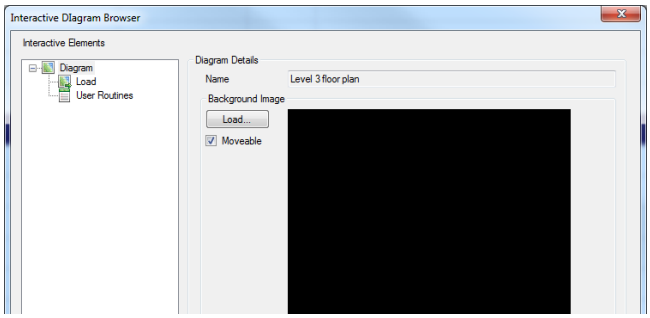
To create a new diagram, enter a name in the Diagram to Open or Create box then click **OK**. Click the **Save** icon and the name of the new diagram will appear in the Existing Diagrams list. The following example shows Level 3 Floor Plan being entered as a new name before being saved and listed.



2.21.1.1 Background Element

This is the image on which the various Interactive Elements are laid.

Select the Background Element by double-clicking anywhere on the open Diagram and the Interactive Diagram Browser will be displayed.



To load a background, under Background Image click **Load** and navigate to the image required. The image will be displayed in the Preview box. The following formats are supported; BMP, GIF, JPG, PNG, TIF, WMF.

Tick the Moveable Editor box if the background must be moved or re-sized from the main display. This will allow the image to be manipulated to fit within the display window.

Note: Some image distortion can occur if the aspect ratio of the original image is changed.



Diagrams may be deleted, renamed, or copied by clicking the **Manage Diagrams** icon then selecting the diagram and choosing the required action.

Backgrounds or Interactive Elements may be cut, copied, saved, or pasted by selecting the component then clicking the appropriate icon.

2.21.1.2 Interactive Elements

Interactive Elements form the basic building blocks of the diagram. Types of elements are:

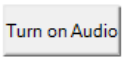
Camera may be monochrome or colour and be fixed, dome or have pan/tilt/zoom mechanisms. Camera icons on the diagram are associated with physical cameras connected to the ADPRO XO or HeiTel device. The icon is shown green for a camera that is currently selected or blue for a camera that is not selected.

Input is a detecting device providing warning, information, or feedback. Examples are a switch contact, glass breakage switch, pressure mat, or movement detector. Input icons are associated with the site, and their colours indicate the input state: green when selected and yellow in alarm.

Output is a device used to control or alert such as a bell, siren, electric latch, or light. Output icons are associated with the site, and display the output state.

Cameras, inputs, and output elements usually have an associated macro so when the element is selected the appropriate control can be executed.

Hot Spot is a transparent area that perform a programmable operation when the mouse is clicked anywhere within the hot spot. A hot spot might be used to turn on a light and switch to an associated camera output.

Button 

is an element that performs a programmable operation when clicked. An example of a button action might be a 'guard tour' that would sequence through all cameras using a 4-way screen split for 10 minutes.

To add an Interactive Element to the Diagram, click on the appropriate toolbar icon. Elements can be moved or resized by via the mouse and may be deleted or copied.

To copy an existing element, click on the element and select Edit-Copy then Edit-Paste. The duplicated element will appear on top of the existing element.

If the Interactive element has its 'Movable in Editor' property checked in the Interactive Diagram browser (by default it has), it can be moved within the main viewing area by clicking on the element and dragging to the required location.

Fire  is a smoke and/or fire-detecting device providing warning, information, and feedback on the fire threat level.

PIR  is a Passive Infrared detector that is associated with physical PIR detectors connected to the ADPRO XO device.

2.21.2 Interactive Diagram Browser

The Interactive Diagram Browser is a software package used to view or manipulate Interactive Elements.

To display the browser, double click on any element in the IDEditor.

The Interactive Diagram Browser has two panels. The left-hand panel lists all the Interactive Elements of a diagram and the events belonging to each element. Events are used to invoke (start) macro commands.

The right hand panel shows the properties of the element selected on the left-hand side and a number of frames containing various parameters for the element.

All Elements that have been assigned to a Diagram are listed in the Interactive Elements panel on the left of the main display.

Associated with each element is an Event, which can to run a macro command.

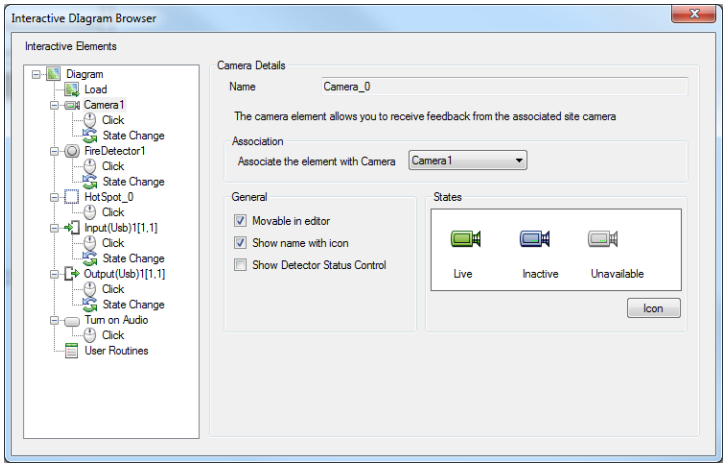
A macro can be started if the User clicks on the element or the field device changes state - such as an input element being switched on or off.

The available Event types are shown on the browser display next to each Interactive Element as either a Click or a State Change event type.

The properties of each Interactive Element can be viewed or modified by selecting the element with a double-click. An edit dialog containing the elements parameter frames will be displayed in the Main Viewing Area. The editing options differ according to element type.

2.21.2.1 Camera

When a Camera element is selected for editing, the Camera Details dialog is displayed.



Name The name of the element as shown on the main Interactive Diagram.

The name cannot be edited via this box but only from the Association details.

Association This parameter specifies an association for the element by selecting a device number. Device numbers are in the range of **1 to 16** inclusive.

The initial value of a blank field indicates that the element has not yet been associated with a device. One or more interactive elements may be associated with the same real world device.

General The General frame contains the following parameters:

Movable in Editor specifies if the element can be moved and resized.

Show Camera Name with Icon specifies if the Camera name from Video Central Platinum should be shown next to the icon on the Interactive Diagram. The default state is for the name to be visible.

Show Detector Status Control Specifies if the element should show an indication of the isolation and states  above the icon. The following describes this icon:

	Function
	No Video Detection
	Isolation Status of Detector Green when UNISOLATED Red when ISOLATED
	State of Detector Input. This icon changes colour due to level of threat: Green when INACTIVE Yellow when ACTIVE
	Motion Detection Icon
	Isolation Status of Detector Green when UNISOLATED Red when ISOLATED
	State of Detector Input. This icon changes colour due to level of threat: Green when INACTIVE Yellow when ACTIVE
	Contrast Detection
	Isolation Status of Detector Green when UNISOLATED Red when ISOLATED
	State of Detector Input. This icon changes colour due to level of threat: Green when INACTIVE Yellow when ACTIVE

States The States frame shows a non-editable graphic for each of the possible states for the element. A Camera graphic can show the following states: Active, Inactive, or Unavailable. These states are also indicated by the camera icon colour.

2.21.2.2 Fire Detector

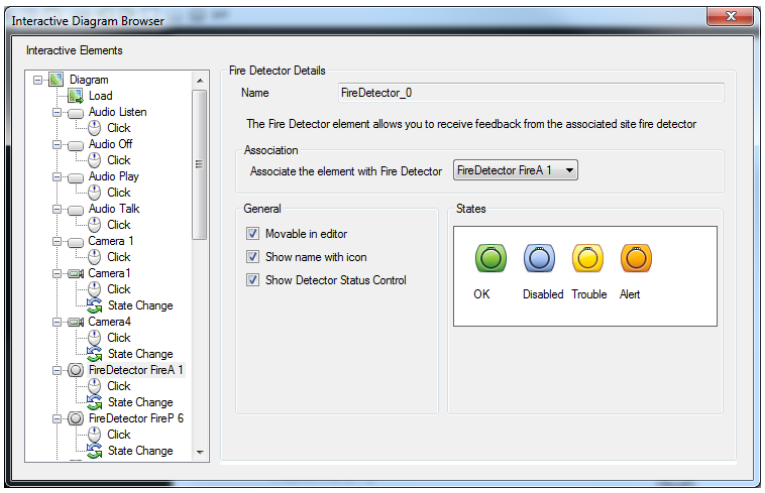
When a Fire Detector element is selected for editing, the Fire Detector Details dialog is displayed.

A fire detector element is associated with only one fire profile. If for example a fire detector has multiple outputs they can be wired into different USB Inputs on the ADPRO XO device. Different USB Inputs can be set to the same detector number and different fire profiles. In the example below two fire elements would be present on the diagram to represent the fire detectors Fire-P and/or Fire-T State.

Example:

USB Input 01 – Associated with detector number 1 and fire profile Fire-P

USB Input 02 – Associated with detector number 1 and fire profile Fire-T



Name The name of the element as used by the Interactive Diagram.

The name of the element is automatically populated from the ADPRO XO programming in operational mode.

Association This parameter specifies an association for the element by selecting a detector number and fire profile. The fire profiles are; Fire Primary (Fire-P), Fire Advisory (Fire-A) and Fire Trouble (Fire-T) and the detector numbers from 1 to 20.

The initial value of a blank field indicates that the element has not yet been associated with a device.

General The General frame contains the following parameters:

Movable in Editor specifies if the element can be moved and resized.

Show Name with Icon specifies if the Fire Detector name from the ADPRO XO device should be shown next to the icon on the Interactive Diagram. The default state is for the name to be visible.

Show Detector Status Control Specifies if the element should show an indication of the isolation and states  above to the icon.

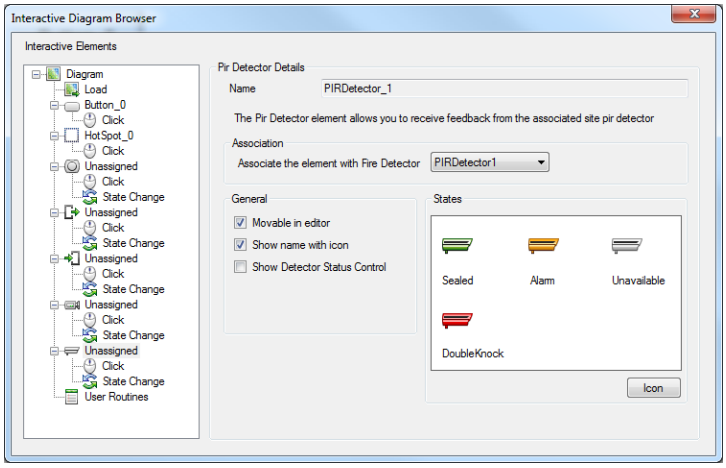
The following describes the IO Status icon:

	Function
	Detector Status Icon.
	Isolation Status of Detector Green when UNISOLATED Red when ISOLATED (When either fire or fire tamper are isolated detector status and tamper are both shown as isolated)
	State of Detector Input. This icon changes colour to indicate if the detector is active: Fire P – Orange Fire A - Orange Fire T - Yellow OK - Green Disabled - Grey
	Detector Tamper Status Icon
	Isolation Status of Detector Tamper Green when UNISOLATED Red when ISOLATED (When either fire or fire tamper are isolated detector status and tamper are both shown as isolated)
	State of Detector Tamper Green when not in Tamper Yellow when in Tamper

States The States frame shows a non-editable graphic for each of the possible states for the element. A Camera graphic can show the following states: Active, Inactive, or Unavailable. These states are also indicated by the camera icon colour.

2.21.2.3 PIR Detector

When a PIR Detector element is selected for editing, the PIR Detector Details dialog is displayed.



Name The name of the element as shown on the main Interactive Diagram.

The name cannot be edited via this box but only from the Association details.

Association This parameter specifies an association for the element by selecting a device number. Device numbers are in the range of **1 to 32** inclusive.

The initial value of a blank field indicates that the element has not yet been associated with a device. One or more interactive elements may be associated with the same real world device.

General The General frame contains the following parameters:

Movable in Editor specifies if the element can be moved and resized.

Show Name with Icon specifies if the PIR Detector name from the ADPRO XO device should be shown next to the icon on the Interactive Diagram. The default state is for the name to be visible.

Show Detector Status Control Specifies if the element should show an indication of the isolation and states  above to the icon.

Note: If multiple threat levels are active at the same time only the highest level is displayed.

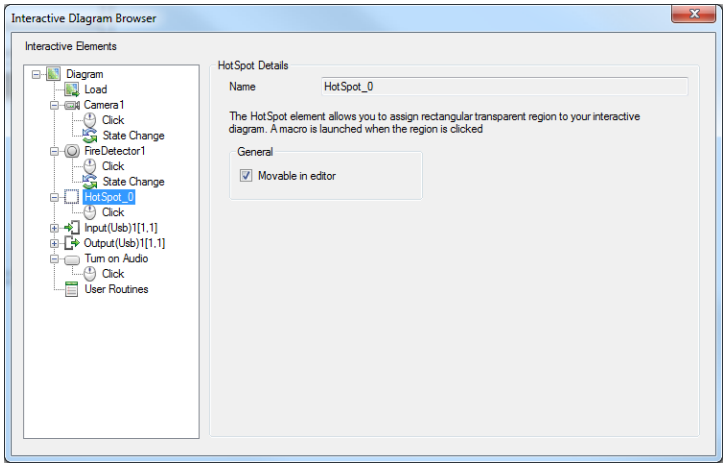
The following describes the IO Status icon:

	Function
	Detector Status Icon.
	Isolation Status of Detector Green when UNISOLATED Red when ISOLATED (When either PIR or PIR tamper are isolated detector status and tamper are both shown as isolated)
	State of Detector Input. This icon changes colour due to level of threat: OK – Green Alarm – Orange Double Knock - Red
	Detector Tamper Status Icon
	Isolation Status of Detector Tamper Green when UNISOLATED Red when ISOLATED (When either PIR or PIR tamper are isolated detector status and tamper are both shown as isolated)
	State of Detector Tamper Green when not in Tamper Yellow when in Tamper

States The States frame shows a non-editable graphic for each of the possible states for the element. A Camera graphic can show the following states: Active, Inactive, or Unavailable. These states are also indicated by the camera icon colour.

2.21.2.4 HotSpot

When a HotSpot element is selected for editing, the HotSpot Details dialog is displayed.



Name The name of the element as shown on the main Interactive Diagram.

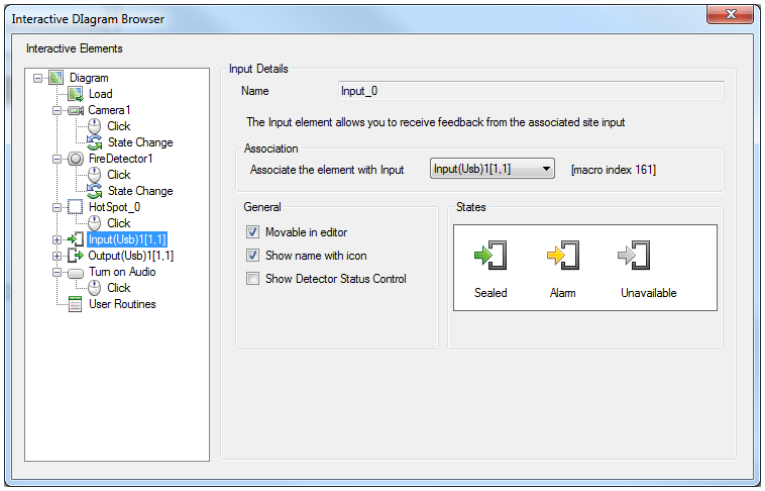
The name is automatically assigned and cannot be changed.

General The General frame contains the following parameters:

Movable in Editor Specifies if the element can be moved and resized.

2.21.2.5 Input

When an Input element is selected for editing, the Input Details dialog is displayed.



Name The name of the element as shown on the main Interactive Diagram. The name cannot be edited via this box but only from the Association details.

Association This parameter specifies an association for the element by selecting a device number. Device numbers are in the range of **1 to 160 for NETIO, 1 to 80 for USBIO, and 1 to 256 for Workbits** inclusive.

The initial value of a blank field indicates that the element has not yet been associated with a device. One or more interactive elements may be associated with the field device.

General The General frame contains the following parameters:

Movable in Editor Specifies if the element can be moved and resized.

Show Name with Icon specifies if the Input name from the site should be shown next to the icon on the Interactive Diagram. The default state is for the name to be visible.

Show Isolated State with Icon The state of the Input is visible by default.

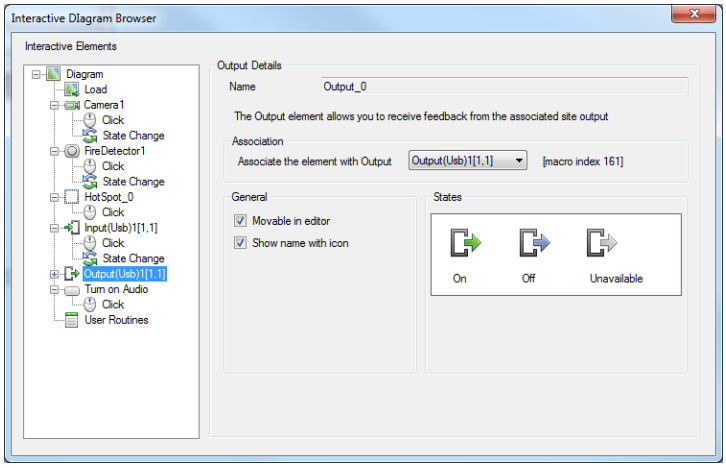
Show Detector Status Control Specifies if the element should show an indication of the isolation and states  above to the icon. The following describes the IO Status icon:

	Function
	Detector Status Icon.
	Isolation Status of Detector Green when UNISOLATED Red when ISOLATED
	State of Detector Input. This icon changes colour due to level of threat: Green when INACTIVE Yellow when ACTIVE
	Detector Tamper Status Icon
	Isolation Status of Detector Tamper Green when UNISOLATED Red when ISOLATED
	State of Detector Tamper Green when not in Tamper Yellow when in Tamper

States The States frame shows a graphic for each of the possible states for the element. These graphics are non-editable. An Input graphic can show the following states: Sealed, Alarm, Tamper Fault, or Not Available.

2.21.2.6 Output

When an Output element is selected for editing, the Output Details dialog is displayed.



Name The name of the element as shown on the main Interactive Diagram.

The name cannot be edited via this box but only from the Association details.

Association This parameter specifies an association for the element by selecting a device number. Device numbers are in the range of **1 to 160 for NETIO, 1 to 16 for USBIO, and 1 to 256 for Workbits** inclusive.

The initial value of a blank field indicates that the element has not yet been associated with a device. One or more interactive elements may be associated with the field device.

General The General frame contains the following parameters:

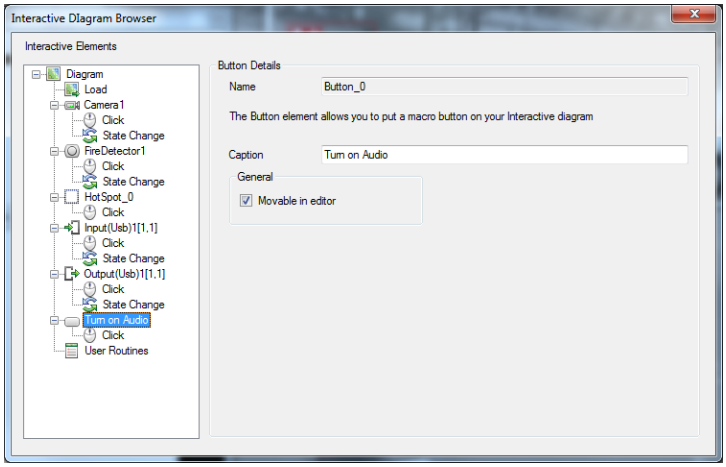
Movable in Editor Specifies if the element can be moved and resized.

Show Name with Icon specifies if the Output name from the site should be shown next to the icon on the Interactive Diagram. The default state is for the name to be visible.

States The States frame shows a graphic for each of the possible states for the element. These graphics are non-editable. An Output graphic can show the following states: **On**, **Off** or **Not Available**. Colour differences highlight state of the device.

2.21.2.7 Button

When a Button element is selected for editing, the Button Details dialog is displayed.



Name The name of the button element as shown on the Interactive Diagram.

The name is automatically assigned and cannot be changed.

Caption This is the text displayed on the button. The Caption should be of sufficient length to show the purpose of the Button on a single line. The size of the button will change to fit the Caption length. Captions may contain alphanumeric, spaces and symbols but not control characters.

2.21.3 Creating and Editing User Routines

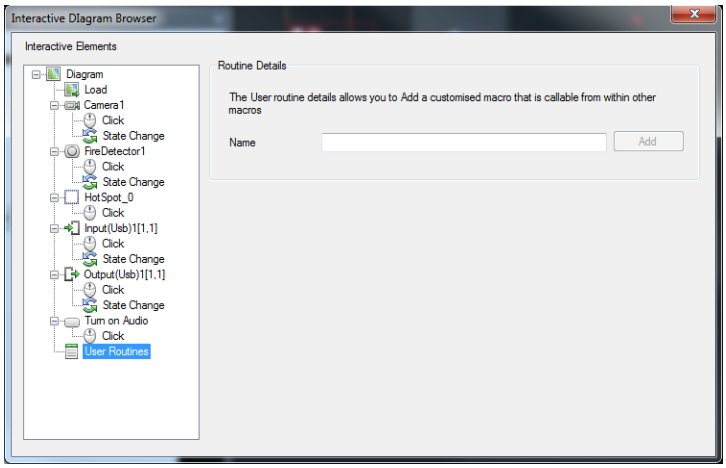
User Routines are macro commands that contain a script with a series of User Interface Control Commands. Each script can be customised to perform a specific action and is given a unique Macro name that can be associated to an Interactive Element event, such as a Click or a State_Change.

To create a new macro click **User Routines** at the bottom of the Diagrams tree and the right and side of the dialog will display Routine Details.

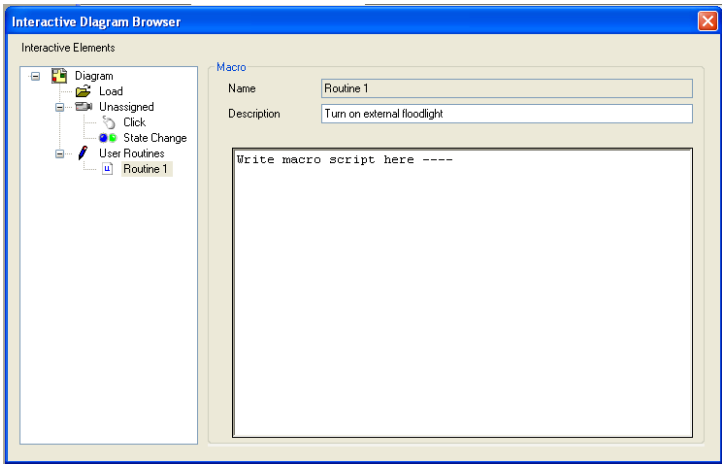
Enter a Name for the new User Routine then click **Add**. The Name will be displayed at the top with a Description box and Macro Edit box below.

Any name that already exists will have an underscore '_' added to make it unique.

Enter a brief description of the macro's action then write a custom macro script for the given interactive element event using specific User Interface Control Commands.



The left-hand side of the display will synchronise and display the new User Routine name once it has been entered.



2.21.4 User Interface Control Commands

Control commands set the series of steps that occur when an Interactive Element (IE) is requested to perform its defined task from within an Interactive Diagram. Each series of steps is known as a macro.

Macro scripts are written for either an IE ‘click’ or an IE ‘state_change’ activity. These activities are invoked when a User clicks on an element with the mouse pointer or the ‘real’ device (that the IE represents), changes it operational status.



In the figure above, the two available macros for Camera_1 are shown.

Control commands are also used in a ‘User Interface’ macro, which can be called from within a ‘click’ or ‘state_change’ activity script. A macro can range from a simple script to a large program with nested sub-routines.

The following is an example of a simple macro script. When the Interactive Element for “Camera 1” is clicked with the left button, this “Camera_1, State_Change” macro, is used to display video on screen for 10 seconds.

video (1)

diagram (HIDE)

wait (10)

diagram (REVEAL)

return

The following actions would occur for each control command:

- the video output from camera #1 is displayed [video (1)]
- the diagram window would be minimised to leave the video as the main window [diagram HIDE]
- the video would stay on screen for ten seconds [wait (10)]
- the diagram window would be maximised again [diagram REVEAL)]
- control would be returned to the Interactive Diagram program [return].

All macro commands that communicate with the Video Central User Interface program may generate the following run-time-errors if a response is not received within 15 seconds:

ERR_RESPONSE_TIMEOUT.

The one exception to this is the site dialling command, site(<site id>), which has a 95 second timeout.

When a Video Central User Interface program is unable to process the macro, the following error is generated:

ERR_CMD_NOT_POSSIBLE.

If the User Interface aborts a macro, then an ERR_ABORTED is generated.

2.21.4.1 Command Syntax

Control commands require the correct syntax for operation. The following syntax is used:

- Command with a variable - Command (var)
- Command with a variable and modifier - Command (var1,mod).

The following tables define the different commands and variables available. When a variable or a modifier is shown within a single chevron (< >), the text or value entered is selected from the range given in the command description.

2.21.4.1.1 Live Video Control

Video (<camera channel number 1..100>)	Request low quality video on selected channel
Video (<camera channel number 1..100>, <quality 1..7>)	Request video of specified quality on selected channel
Video (PAUSE)	Pause of live video
Video (MULTI, <1, 4, 7, 9, 10, 13, 16 or 20 way split screen>)	Request multi-screen display in 1, 4, 7, 9, 10, 13, 16 or 20 way splits RTE: ERR_OUT_OF_RANGE (other than 1, 4, 7, 9, 10, 13, 16 or 20)
Video (MULTI,NEXTSEQUENCE)	Requests next multi-screen sequence.
Video (MULTI,PREVIOUSSEQUENCE)	Requests previous multi-screen sequence.
Video (PROFILE, <profile_name>)	Requests specified multiscreen profile display

2.21.4.1.2 Audio Control

Audio (TALK)	Request high quality audio transmission
Audio (LISTEN)	Request high quality audio reception
Audio (OFF)	Switch off audio reception and transmission
SendLocalAudioFile	Plays an audio file to the remote site. **Site diagram;** Click_Event SendLocalAudioFile("filename.pcm") return Note file must first be associated with the site under Tools > Administration > Local Audio Setup.

2.21.4.1.3 User Interface Display Mode Control

Display_Mode (SINGLE)	Enlarge the video / event cycle image to full screen
Display_Mode (QUAD)	Restore the four images windows to equal quads
Display_Mode (EVENT_REPLAY)	Restore the four images windows to equal quads and display the cycling event image

2.21.4.1.4 Output Control

Output (ON, <output number 1..176>) NETIO 1 = 1 to NETIO 160 = 160 USBIO 1 = 161 to USBIO 16 = 176	Request transmitter output to switch on
Output (OFF, <output number 1..176>) NETIO 1 = 1 to NETIO 160 = 160 USBIO 1 = 161 to USBIO 16 = 176	Request transmitter output to switch off

2.21.4.1.5 PTZ Control

PTZ (HOME)	Request the pre-programmed home position
PTZ (PREPOSITION, <preposition number 0..255>)	Request the specified pre-programmed position

2.21.4.1.6 Site Control

Site (“<site name>”) Note: Site Name is equivalent to Site ID in VCP diagrams.	Request the User Interface to connect to the selected site’s transmitter
Site (“<site name>”, NO_DIAGRAM)	Request the User Interface to connect to the selected site and enter NO_DIAGRAM mode, so that the current macro can continue running without being interrupted by the loading of the new site's diagram
Site (AUTO_SELECT)	Request the User Interface to automatically obtain the site of highest priority from the all-sites table
Site (HANGUP)	Request the User Interface to disconnect from the remote site's transmitter **Note:** Mandatory Site Acknowledgement must not be enabled in Video Central Platinum if this command is to be used
Site (FINISH)	Request the User Interface to return to the active sites list
Site (ACKNOWLEDGE)	Request the User Interface to display the site acknowledge dialog box

Each Site Control command may have the optional parameter of DONT_UNLOAD. This stops the map being unloaded, allowing the macro to continue. This lets the system connect to another site, instead of the diagram browser loading the top level map. For example:

- Site (HANGUP, DONT_UNLOAD)
- Site (“ABCD”, DONT_UNLOAD)

This example enables the current site to be disconnected and the map for site ABCD to be loaded, without the top level map being displayed.

Note: Entering DONT_UNLOAD in the second line of this example prevents the top level map being flashed on the screen before the site map for ABCD is loaded.

2.21.4.1.7 Detector Control

Isolate(<detector_type>, <detector_number>, ON)	Changes the isolation status of the detector type specified to on.
Isolate(<detector_type>, <detector_number>, OFF)	Changes the isolation status of the detector type specified to off.

2.21.4.2 Basic Commands

2.21.4.2.1 Diagram Control

Diagram (“<diagram name>”)	Load the specified diagram and run its ‘diagram_load’ macro
Diagram (TOP_LEVEL)	Load the diagram called ‘Top_Level’ and run its ‘diagram_load’ macro
Diagram (SITE_DEFAULT)	Load the default diagram for the current site and run its ‘diagram_load’ macro
Diagram (HIDE)	Minimise the diagram window and bring the User Interface window to the foreground
Diagram (REVEAL)	Restore the diagram window and bring it to the foreground

2.21.4.2.2 Message Boxes

Message_Box (“<message text string>”)	Displays a dialog box containing the message text and an OK button

2.21.4.2.3 Playing Wave Sound Files

Play_Sound (“<wave file name>”)	Plays the specified wave file, if it exists, or the system asterisk sound if the wave file fails

2.21.4.2.4 Delays

Wait (<number of seconds>)	Causes a delay of 0 seconds or greater (maximum value is INT_MAX, defined as a system constant)

2.21.4.2.5 Record

Record ({ON | OFF})	Causes manual live video recording to start or stop on. Record (ON) or Record (OFF) respectively

2.21.4.2.6 FireReset

FireReset()	Sends a global fire rest to the remote site to reset any latched fire detectors

2.21.4.2.7 Show Procedure

ShowProcedure(SECURITY)	Causes the security procedure to be displayed
ShowProcedure(FIRE)	Causes the fire procedure to be displayed
ShowProcedure(EVENT)	Causes the event procedure to be displayed. Note either the security or fire procedure must be activated first so the procedures window is present. Typical macro use is; ShowProcedure(SECURITY) ShowProcedure(EVENT) return

2.21.4.2.8 Private Wall

Wall_Clear(PRIVATE,1)	Clears the Private Wall.
Wall_Split(PRIVATE, 1, <1_4_7_9_10_13_16_or_20_way_split_screen>)	Defines how many cameo (or camera) positions the Private Wall will have.
Wall_SetCameo(PRIVATE, 1, <CAMEO_BLANK, CAMEO_ADPRO_LEGACY or CAMEO_ADPRO_FT2>, <Cameo_number_1-20>,<site>, <camera_channel_number>)	Assigns a camera from a specific site into a Private Wall cameo.
Wall_SetCameo(PRIVATE, 1, <CAMEO_BLANK, CAMEO_ADPRO_LEGACY or CAMEO_ADPRO_FT2>, <Cameo_number_1-20>,<site>, <camera_channel_number>,<MinQuality_1-7>,<MaxQuality_1-7>)	Assigns a camera from a specific site into a Private Wall cameo also specifying the image quality.

2.21.4.2.9 Exiting a Macro

Return	Causes the current macro routine to end. If the call() command has been used (see the Advanced Commands section), execution shall return to the line immediately following the call() command

2.21.4.3 Advanced Commands

2.21.4.3.1 Calling User Routines

Call (“<user routine name>”)	Execution of the current routine is suspended, the specified user routine is performed and then execution of the original routine continues RTE: ERR_RECURSION_ERROR (11th call() made) ERR_SUB_NOT_FOUND
Goto (“<user routine name>”)	Execution of current routine terminated and the specified user routine is performed. Execution of original routine does not continue RTE: ERR_SUB_NOT_FOUND

2.21.4.3.2 Trace to File

Trace (“<message text string>”)	Writes the message text to the file ‘c:\swlog.txt’

2.21.4.4 Variables

Integer variables can be used wherever a literal number would otherwise be used.

String variables can be used wherever a literal string would otherwise be used.

VC-Script supports variables primarily for use with:

- conveying system information to the VC-Script macros
- implementing conditional blocks and error handling
- parameters to the _statechange macros.

2.21.4.4.1 Standard Variables

Dim <variable> As Integer	Reserves memory for an integer variable that can store negative and positive whole numbers. The variable will only exist within the routine in which it is declared. Its numeric range is INT_MIN to INT_MAX. RTE: ERR_SYMBOL_INVALID (illegal name)
Global Dim <variable> As Integer	Same as the normal integer declaration, except the variable can be accessed from all routines. These are best declared in the diagram_load routine to ensure they are declared before use. RTE: ERR_SYMBOL_INVALID (illegal name)
Dim <variable> As String	Reserves memory for a text string variable that can store text. The variable will only exist within the routine in which it is declared. It can store up to 1024 characters. RTE: ERR_SYMBOL_INVALID (illegal name)
Global Dim <variable> As String	Same as the normal string declaration, except the variable can be accessed from all routines. These are best declared in the diagram_load routine to ensure that they are declared before use. RTE: ERR_SYMBOL_INVALID (illegal name)
<variable> = <expression>	Assigns a value to a variable. Expressions are explained in Section 2.21.4.6 Expressions. RTE: ERR_SYMBOL_UNDEFINED, ERR_CONSTANT_ASSIGNMENT (system constant used on the left of the =)

2.21.4.5 Parameter Variables

The _statechange macros have the following local variables automatically declared as parameters to the macros:

2.21.4.5.1 Camera State Change

nIsChannelActive	The state of the video at the time of the state change. (TRUE or FALSE.)

2.21.4.5.2 Input State Change

nInputChanged	If equal to TRUE, the nInputState variable is valid
nInputState	The state of the input at the time of the state change. (INPUT_UNAVAILABLE, INPUT_SEALED, INPUT_ALARM, or INPUT_TAMPER)
nIsolatedChanged	If equal to TRUE, the nIsIsolated variable is valid.
nDetectorType	Type of Detector. Can be one of the Detector Type System Constant values
nIsDetectorActive	The state of the Detector at the time of the state change
nDetectorActiveChanged	If equal to TRUE, the nIsDetectorActive variable is valid
nIsDetectorIsolated	The isolation status of the detector at the time of the status change
nDetectorIsolatedChanged	If equal to TRUE, the nIsDetectorIsolated variable is valid

2.21.4.5.3 Output State Change

nIsOutputOn	The state of the output at the time of the state change. (TRUE or FALSE.)

2.21.4.6 Expressions

Integer expressions can be used anywhere a number literal would be used. The following operators are available

+	Addition
_	Subtraction
*	Multiplication
/	Division RTE: ERR_DIVIDE_BY_ZERO

Round brackets can be used to apply standard mathematical rules of operator precedence.

Examples:

Dim ValueA as integer, Dim ValueB as integer Dim Result as integer, ValueA = 2, ValueB = 4	
Result = ValueA + ValueB	Result = 6
Result = (ValueA + ValueB)	Result = 6
Result = (ValueA + ValueB) / 2	Result = (2 + 4) / 2 = 6 / 2 = 3
Result = ValueA + ValueB / 2	Result = 2 + 4/2 = 4
Result = (ValueA + ValueB) * (ValueA - ValueB)	Result = (2 + 4) * (2 - 4) = 6 * (-2) = -12

The following errors can be generated when integer expressions are evaluated:

RTE:, ERR_INVALID_TYPE, ERR_SYMBOL_UNDEFINED, ERR_DIVIDE_BY_ZERO

2.21.4.6.1 String (Text) Expressions

String expressions can be used anywhere a literal string would be used. The following operator is available

&	Concatenation

Round brackets *cannot* be used within string expressions.

Integer expressions can be concatenated to the end of a string and between strings but not to the beginning.

String expressions must use double-quotes (“ “)

Examples:

Dim ValueA as string, Dim ValueB as string Dim IntValue as integer, Dim Result as string ValueA = “hello”, ValueB = “world”, IntValue = 6	
Result = ValueA & ValueB	Result = helloworld
Result = ValueA & “ “ & ValueB	Result = hello world
Result = ValueA & “ “ & ValueA	Result = hello hello
Message_Box(IntValue = " & IntValue)	Displays a message box with the text, “IntValue = 6“

The following errors can be generated when string expressions are evaluated:

RTE: ERR_INVALID_TYPE, ERR_SYMBOL_UNDEFINED.

2.21.4.6.2 Boolean (Logic) Expressions

Boolean expressions are to be used with the IF(), ELSEIF() and WHILE() macro commands.

The following comparison operators are available for comparing integer expressions to integer expressions and string expressions to string expressions:

=	Equal to
< >	Not equal to
<	Less than
>	Greater than
<=	Less than or equal to
>=	Greater than or equal to

The following operators are available for extending Boolean sub-expressions:

<sub-expression A> AND < sub-expression B>	Evaluating this expression results in TRUE only if both sub-expressions evaluate to TRUE
<sub-expression A> OR < sub-expression B>	Evaluating this expression results in TRUE if either subexpression evaluates to TRUE

Round brackets cannot be used around Boolean expressions.

Examples:

Dim IntValueA as integer	
Dim IntValueB as integer	
Dim StrValueA as integer	
Dim StrValueB as integer	
IntValueA = 2	
IntValueB = 4	
StrValueA = “hello”	
StrValueB = “world”	
If (IntValueA < IntValueB) then	Condition is TRUE
If (IntValueA >= IntValueB) then	Condition is FALSE
If (IntValueA >= 10 OR StrValueA = ‘hello’) then	Condition is TRUE (2nd sub-expression is TRUE)
If (IntValueA >= 10 AND StrValueA = “hello”) then	Condition is FALSE (1st sub-expression is FALSE)
If (IsOutputOn[1] = TRUE) then	Condition is TRUE if transmitter Output #1 is ON
If (IntValueA <> IntValueB) then	Condition is TRUE
While (TRUE)	Condition is TRUE. (While/Wend will loop until aborted.)`

The following errors can be generated when Boolean expressions are evaluated:

RTE:, ERR_INVALID_TYPE, ERR_SYMBOL_UNDEFINED, ERR_DIVIDE_BY_ZERO.

2.21.4.7 Conditional Blocks

2.21.4.7.1 If / Endif Blocks

If (<condition1>) then	If <condition1> is TRUE, the block of commands immediately following this command shall be executed
ElseIf (<condition2>) then	If <condition1> of the preceding If/Then command was FALSE, and <condition2> to TRUE, the block of commands immediately after this command shall be executed. RTE: ERR_MIXED_BLOCK_TYPES
Else	If <conditionX> of the preceding If/Then or ElseIf/Then command was FALSE, the block of commands immediately following this command shall be executed. RTE: ERR_MIXED_BLOCK_TYPES
EndIf	Ends the conditional block. RTE: ERR_MIXED_BLOCK_TYPES

2.21.4.7.2 For / Next Blocks

For <integer variable> = <a> To <b>	Starts the for-loop block. The specified variable will take on the values of <a> through to <b>, incrementing by 1 each time through the loop. RTE: ERR_SYMBOL_UNDEFINED, ERR_CONSTANT_ASSIGNMENT, ERR_INVALID_TYPE

For <integer variable> = <a> To <b> Step <c>	Starts the for-loop block. The specified variable will take on the values of <a> through to <b>, incrementing by <c> each time through the loop. Note that <c> can be negative if <a> is greater than <b>
Next <integer variable>	Marks the end of the loop block. The variable is required to identify the matching For command. RTE: ERR_MIXED_BLOCK_TYPES (no matching For), ERR_SYMBOL_UNDEFINED, ERR_SYMBOL_INVALID (var doesn't match For)

2.21.4.7.3 While / Wend Blocks

While (<Boolean expression>)	Start the while block. The commands between the While and the Wend commands are repeated as long as the <Boolean expression> evaluates to TRUE. Note that the block shall loop until manually aborted if the expression never evaluates to FALSE.
Wend	Marks the end of the loop block. RTE: ERR_MIXED_BLOCK_TYPES

2.21.4.8 Modes of Operation

2.21.4.8.1 Handling New Events at the User Interface

On new_event abort	When a new event arrives at the interface, any macro running in the interactive diagram viewer shall be aborted. (This is the default behaviour.)
On new_event resume	When a new event arrives at the interface, any macro running shall not be aborted

2.21.4.8.2 Handling Run-time Errors

Refer to Section 2.21.4.9 Error Handling

On new_event abort	When a new event arrives at the interface, any macro running in the interactive diagram viewer shall be aborted. (This is the default behaviour.)
On new_event resume	When a new event arrives at the interface, any macro running shall not be aborted

2.21.4.9 Error Handling

2.21.4.9.1 Syntax and Runtime Errors

Syntax errors are typographic errors or badly constructed macro commands.

Runtime errors are detected only when a macro is tested, hence the name ‘runtime’.

2.21.4.9.2 Runtime Error Constants

The following is the complete set of VC-Script runtime errors:

ERR_NONE	Signifies that no error has occurred
ERR_OUT_OF_RANGE	This error occurs when an index into an array does not fit within the array's range
ERR_INVALID_TYPE	This indicates that a text string was used in place of an integer, or an integer was used in place of a text string
ERR_CONSTANT_ASSIGNMENT	This indicates that an attempt was made to assign a value to a constant symbol, instead of a variable

ERR_SYMBOL_UNDEFINED	This indicates that an attempt was made to access a variable or constant that has not been declared using the DIM keyword
ERR_SYMBOL_INVALID	This indicates that the declaration or use of a variable or constant is invalid
ERR_DIVIDE_BY_ZERO	This indicates that the division calculation attempted an illegal divide by zero
ERR_ABORTED	This indicates that the macro was aborted
ERR_RECURSION_ERROR	This indicates that the CALL command has called a routine, which called a routine, and so on until the call limit was reached
ERR_MIXED_BLOCK_TYPES	This indicates that there is a cross-matched use of WHILE/WEND, FOR/NEXT or IF/ENDIF blocks
ERR_SUB_NOT_FOUND	This indicates that the CALL command cannot locate the specified routine
ERR_NO_DIAGRAM_MODE	This indicates that the operation cannot be performed because NO_DIAGRAM keyword was used in a SITE() command. Only by re-loading the TOP_LEVEL diagram will the NO_DIAGRAM mode switch off
ERR_CMD_NOT_POSSIBLE	This indicates that the User Interface is unable to perform the command
ERR_RESPONSE_TIMEOUT	This indicates that the User Interface has not responded to the command within a allowed time frame

2.21.4.9.3 Runtime Error Handling

The following macro commands can be used to switch between error handling modes:

On error abort	Causes the macro to abort, and display the Runtime error dialog box
On error resume	The error is ignored, and execution resumes at the next command. (This is the default mode of operation.) Error status can be explicitly tested in this mode.

The abort mode of operation is useful for testing a new macro. The resume mode is a better choice for normal operation of interactive diagrams, and is the default mode of operation.

The best location for these macro commands is in the diagram_load macro.

2.21.4.9.4 Error Reporting Dialog Boxes

When the Runtime error dialog box is displayed, the operator can select one of two buttons:

Ignore	The Ignore button will cause the error to be ignored and the execution will resume at the next macro command
Abort	The macro shall be aborted

2.21.4.9.5 Explicit Checking For Errors

When using this mode of operation, runtime errors are ignored and the execution will resume at the next macro command. Errors can be detected by examining the following variables:

nLastErrorNumber	Stores the error constant corresponding to the last error
sLastErrorString	Stores the error message corresponding to the last error
sLastErrorMacro	Stores the macro in which the last error occurred.
nLastErrorMacroLine	Stores the line number at which the last error occurred

The simplest way to check for errors is to reset the nLastErrorNumber system variable to ERR_NONE, perform the macro command to be tested, and then check nLastErrorNumber to see if it is still ERR_NONE.

The following example checks that a site connection is made before calling a user routine:

```
nLastErrorNumber = ERR_NONE
Site (sSiteIds[nSiteIx], NO_DIAGRAM)
If (nLastErrorNumber = ERR_NONE) Then
Call ("TourConnectedSite")
Site (HANGUP)
Endif
```

2.21.4.10 System Symbols

2.21.4.10.1 System Constants

VC_SCRIPT_MAJOR_VERSION	Major version of the VC-Script parser
VC_SCRIPT_MINOR_VERSION	Minor version of the VC-Script parser
TRUE	Boolean TRUE value, to be used in Boolean expressions
FALSE	Boolean FALSE value, to be used in Boolean expressions
INT_MAX	Largest possible positive integer value
INT_MIN	Largest possible negative integer value
INPUT_UNAVAILABLE	Input state
INPUT_SEALED	Input state
INPUT_ALARM	Input state
INPUT_TAMPER	Input state
DETECTOR_UNDEFINED	Detector State
DETECTOR_PRESIDIUM_DETECTION	Detector State
DETECTOR_NO_VIDEO	Detector State
DETECTOR_VMD	Detector State
DETECTOR_CONTRAST_ALARM	Detector State
DETECTOR_CAMERA_ALL	Detector State
DETECTOR_ALARM_INPUT	Detector State
DETECTOR_ALARM_INPUT_TAMPER	Detector State
DETECTOR_ALARM_INPUT_ALL	Detector State
DETECTOR_ALL	Detector State
DETECTOR_PIR	Detector State
DETECTOR_PIR_TAMPER	Detector State
PIR_DETECTOR_UNAVAILABLE	Detector State
PIR_DETECTOR_INACTIVE	Detector State
PIR_DETECTOR_ALARM	Detector State
PIR_DETECTOR_DOUBLEKNOCK	Detector State

2.21.4.10.2 System Variables

nLastErrorNumber	Stores the error constant corresponding to the last error
sLastErrorString	Stores the error message corresponding to the last error
sLastErrorMacro	Stores the macro in which the last error occurred
nLastErrorMacroLine	Stores the line number at which the last error occurred
nActiveChannel	Stores the currently active live video channel
nAvailableChannels	Stores the number of available video channels
nMaxChannel	Stores the highest available video channel
IsChannelAvailable[<channel>]	Stores TRUE or FALSE for each channel 1 to 16
nInputStatus[<input number>]	Stores the status of the inputs 1 to 16. Values are INPUT_UNAVAILABLE, INPUT_SEALED, INPUT_ALARM, or INPUT_TAMPER
IsInputIsolated[<input number>]	Stores TRUE or FALSE for each input 1 to 16
IsOutputOn[<output number>]	Stores TRUE or FALSE for each output 1 to 10
IsDetectorIsolated[<nDetectorType >, <index>]	Stores TRUE or FALSE for Isolation Status of each Detector. nDetectorType can be one of the Detector Type System Constant values (excluding DETECTOR_UNDEFINED)

	Index is the Detector number.
IsDetectorActive[<nDetectorType >,<index>]	Stores TRUE or FALSE for Detector State of each Detector. Parameters are the same as above
PirDetectorStatus[<pir_detector_number>]	Stores the status of the PIR detectors 1 to 32. Values are; PIR_DETECTOR_UNAVAILABLE PIR_DETECTOR_INACTIVE PIR_DETECTOR_ALARM PIR_DETECTOR_DOUBLEKNOCK
IsPirDetectorIsolated[<pir_detector_number>]	Stores TRUE or FALSE for each input 1 to 32

CurrentSiteConnected	Stores the site name of the current connected site.
	
	Top level diagram;
	
	Click_Event
	
	Message_Box ("Site is " & CurrentConnectedSite)
	return
	
	Site diagram;
	
	Click_Event
	
	Message_Box ("Site is " & CurrentConnectedSite)
	return
	
	Click_Event
	
	If (CurrentConnectedSite = "MySite") then
	Message_Box("connected")
	else
	Message_Box("not connected")
	endif
	return

2.21.4.11 Macro Example

2.21.4.11.1 Change Channel and Pause Live Video based on Input or Output State Change

Diagram_load
GLOBAL DIM changeToChannel AS INTEGER return

Input(Usb)1[1,1] (State Change)
--Input (USB) 1 [1,1] Macro 161 IF (nInputStatus[161] = True) THEN ' show cam 4 on output on

```
changeToChannel = 4

Else

' show cam 5 on output off

changeToChannel = 5

EndIf

Call("ChangeChannel")

return
```

Output(Usb)1[1,1] (State Change)

```
----Output (USB) 1 [1,1] Macro 161

IF (IsOutputOn [161] = True) THEN

changeToChannel = 1

EndIf

Call("ChangeChannel")

return
```

User Routine: ChangeChannel

```
--User Routine called "ChangeChannel"

' Only try to change the channel if it is available.

if (IsChannelAvailable[changeToChannel] = true) then

' Only request live stream if necessary.

if (nActiveChannel <> changeToChannel) then

Video(changeToChannel)

' Wait for the live stream images.

While (nActiveChannel <> changeToChannel)

Wait(1)
```

```
WEnd

endif

' Pause the video

Video(Pause)

endif

return
```

2.21.4.11.2 Run a Private Wall macro based upon the state of a fire detector

Fire Detector 1 State Change

```
'IF (IsFireDetectorIsolated[1] = TRUE)THEN

IF (FireDetectorStatus[1] = FIRE_DETECTOR_FIRE_1)THEN

Wall_Clear(PRIVATE,1)

Wall_Split(PRIVATE, 1, 1)

Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 1,"November", 6)

Else

Wall_Clear(PRIVATE,1)

Wall_Split(PRIVATE, 1, 1)

Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 1,"November", 7)

ENDIF
return
```

2.21.4.11.3 Run a Private Wall macro

Button

```
Wall_Clear(PRIVATE,1)
Wall_Split(PRIVATE, 1, 16)
Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 1,"November", 6, 2, 7)
Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 3,"Lima", 3, 2, 7)
Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 5,"Lima", 4, 1, 7)
Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 16,"Lima", 5)
Wait (10)
```

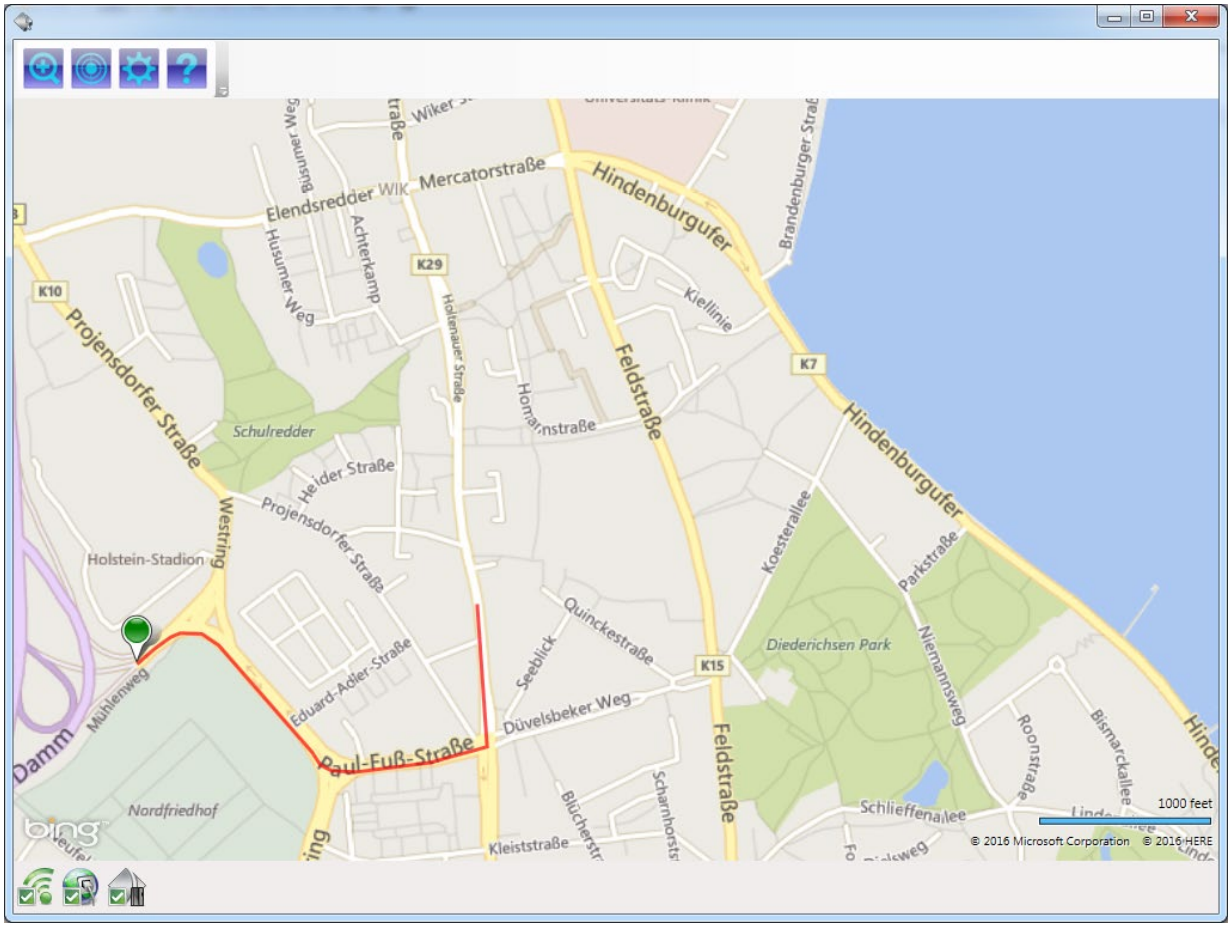
```
Wall_Clear(PRIVATE,1)
Wall_Split(PRIVATE, 1, 4)
Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 1,"November", 7, 2, 7)
Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 2,"Lima", 3, 2, 7)
Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 3,"Echo", 4, 1, 7)
Wall_SetCameo(PRIVATE, 1, CAMEO_ADPRO_FT2, 4,"India", 2)
return
```

2.22 Global Maps

Global Maps is an application that allows to track HeiTel units that have GPS tracking enabled.

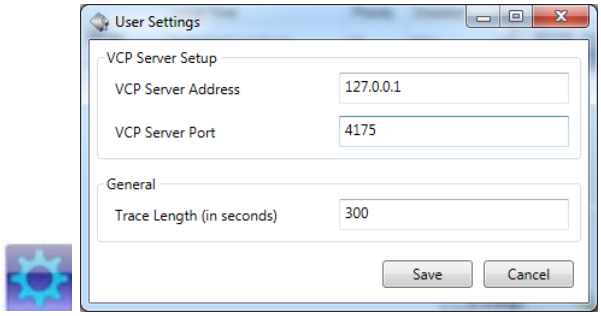
The Global Maps application is installed during setup of the VCP User Interface. Through the VCP setup wizard the Global Maps application is also available as a separate setup.

The VCP User Interface has an option to automatically launch the Global Maps application when the VCP User Interface application starts. This option is located under Tools > User Interface Options > Global Maps Auto Start.



Note: for the Global Maps application to work properly, a Microsoft Bing Maps key is required. For more information on acquiring and setting up the key, see section 2.11.7.

2.22.1 Settings



VCP Server Address allows to set the IP address where the VCP Server can be reached.

The Global Maps application retrieves information from the VCP Server on where to connect to the HeiTel HTConnect Server. Once the Global Maps application is connected with the HTConnect Server, the HTConnect Server can send GPS updates about GPS-enabled HeiTel units to the Global Maps application. If the Global Maps application fails to connect to VCP Server for retrieving the HTConnect Server details, the Global Maps application will use default HTConnect Server connection settings.

Default HTConnect Server settings are:

- HTConnect Server IP Address = VCP Server Address
- HTConnect Server Port = 4444

VCP Server retrieves the HTConnect Server settings it sends to the Global Maps application, from the VCPServerConfig.xml file. The VCPServerConfig.xml file is located in the VCP\VCPDataRoot folder. In the VCPServerConfig.xml file there is a section that looks like this:

```
<HTConnectServer>
      <Address>10.0.1.17</Address>
      <Port>4444</Port>
</HTConnectServer>
```

The <Address> element defines the HTConnect Server IP address that the VCP Server will use.

The <Port> element defines the HTConnect Server port.

Note: these elements are configurable, but they must match the actual HTConnectServer address and port.

If the Address setting is not present under the <HTConnectServer> element, 127.0.0.1 will be used as default.

If the Port setting is not present, 4444 will be used as default.

The IP address and port that will actually be used by the HTConnect Server is configured in the CAMCTRL.INI file, which is located at the path VCP\Server\CCServer\CAMCTRL.INI.

The CAMCTRL.INI file has a section that starts with [HTCONNECTCTRL]. Amongst other settings, this section has the HTCONNECTSERVER_ADDRESS and STATUSSERVERPORT settings.

For example:

[HTCONNECTCTRL]
HTCONNECTSERVER_ADDRESS=127.0.0.1
STATUSSERVERPORT=4444

VCP Server Port is the port at which the Global Maps application will try to connect to the VCP Server for retrieving the HTConnect Server connection details.

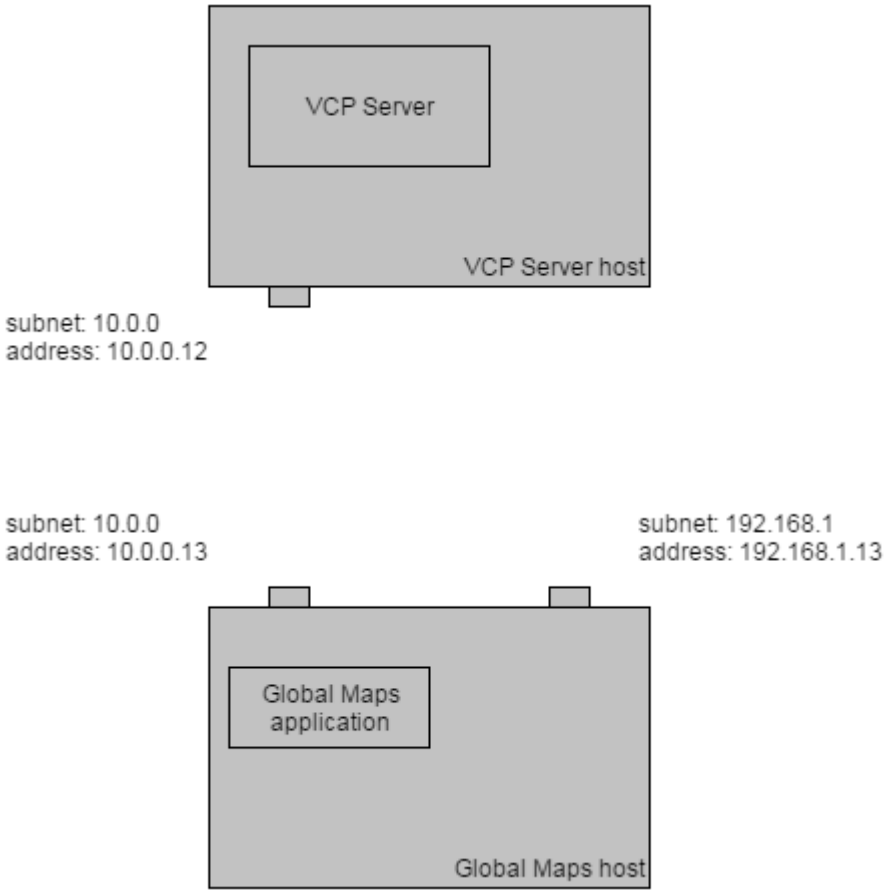
Trace Length (in seconds) indicates how long the Global Maps application needs to keep the GPS trace information for a GPS-enabled HeiTel device. For example: if this field is set to 300, the application will keep the trace information for the last 300 seconds. All trace information older than 300 seconds will be discarded. Thus, in this example, the trace line will show where the HeiTel unit has been during the last 300 seconds.

2.22.2 Advanced Settings

The settings for the Global Maps application are stored in %programdata%\ADPRO VCP\GPSMapsSettings.xml.

The only setting that you may want to change here is **BindToAddress**. This setting allows you to choose the IP address that will be used by the Global Maps application for receiving information from the VCP Server. If the BindToAddress setting is not specified, which is the default, then the Global Maps application will listen on all IP addresses that are configured on the machine where the application runs. However, listening on all IP addresses can cause a problem under certain conditions.

Consider the following situation.



The VCP Server host machine has configured a single IP address 10.0.0.12 on subnet 10.0.0.

The Global Maps host has configured 2 IP addresses, one on subnet 10.0.0 and another on subnet 192.168.1.

It is a general rule that two computers on a local network that have IP addresses on a separate subnet will not be able to communicate with each other using these addresses. Therefore, the VCP Server host and Global Maps host will not be able to communicate using subnet 192.168.1, because the Server host does not have a 192.168.1 subnet configured.

If in this situation, the Global Maps application is configured to listen on all IP addresses that are configured on the Global Maps host machine, then it will also listen on the 192.168.1.13 address. This can lead to a situation where an attempt is made for VCP Server to connect to the Global Maps application on address 192.168.1.13. In that case the connection attempt will fail. To avoid this situation, the **BindToAddress** setting provides a means to configure the Global Maps application to listen to a specific address. In the example case, the address to configure has to be 10.0.0.13, because this address is on the same subnet as the address that is configured at the Server side.

Note: as an alternative to solve the issue in this example, you could also configure an extra IP address at the Server, that is, an IP address in the 192.168.1 subnet.

2.23 Scenarios

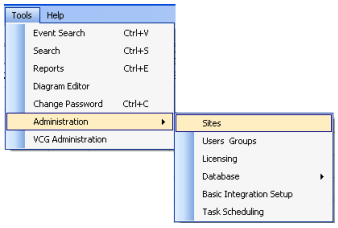
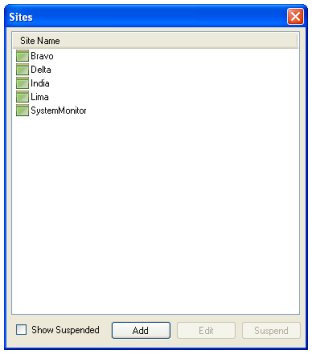
2.23.1 Add a Site to the VCP Database

This process adds a new Site to the VCP Database. VCP UIs connected to the VCP Database can then monitor the new site.

Prerequisite

The VCP UI is not connected to a site.

Process

Step	Action	Reference Section
Open the Sites dialogue	Select the Tools > Administration > Sites menu 	2.6.1 Adding New Sites
Add the site	Click **Add** 	
Enter the Site detail	Enter the required fields in the Tx tab: **Unit ID**: This is a unique identifier for receiving alarms from the ADPRO XO or HeiTel device. **Name:** Enter a unique and easily identifiable site name. **IP Address:** Enter the IP of the ADPRO XO or HeiTel device. Click **OK**.	

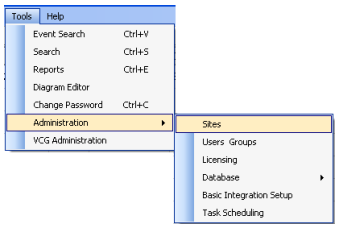
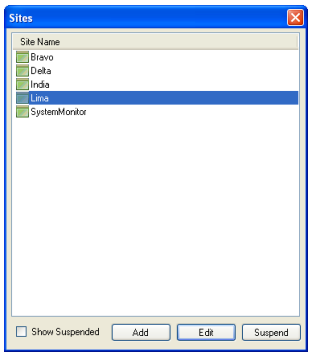
2.23.2 Suspend a Site

This process suspends a Site from the VCP Database. It is not monitored while it is suspended.

Prerequisite

The VCP UI is not connected to a site.

Process

Step	Action	Reference Section
Open the Sites dialogue	Select the Tools > Administration > Sites menu 	2.7.1 Suspending a Site
Suspend the site	Select the Site from the list.  Click **Suspend** The Site will not be visible in the Sites List until it is restored.	

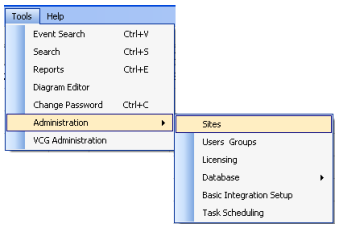
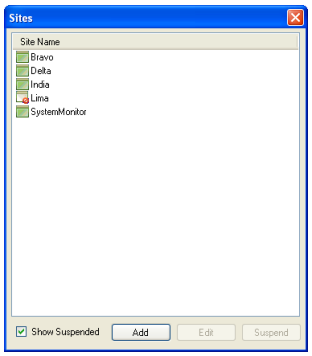
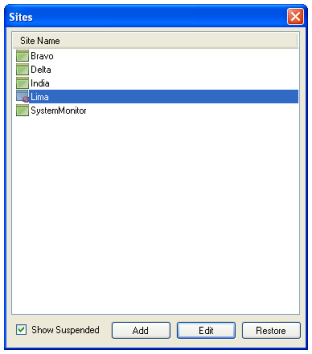
2.23.3 Restore a Site

This process restores a Site from the VCP Database.

Prerequisite

The VCP UI is not connected to a site.

Process

Step	Action	Reference Section
Open the Sites dialogue	Select the Tools > Administration > Sites menu 	2.7.2, Restoring a Site
Show the Suspended sites	Click the **'Show Suspended'** option.  Select the suspended Site  from the list.	
Restore the site	Click **Restore**.  The Site will now be visible in the Sites List.	

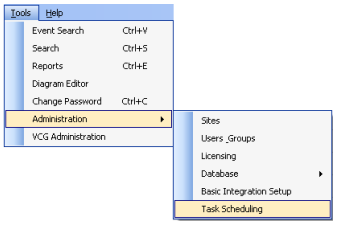
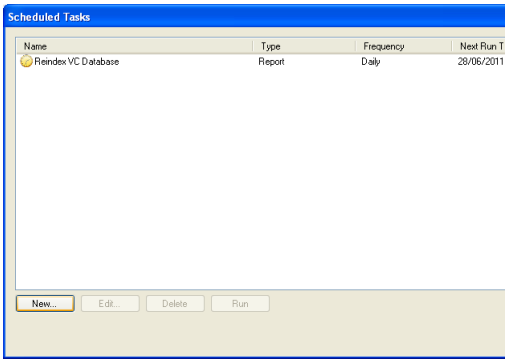
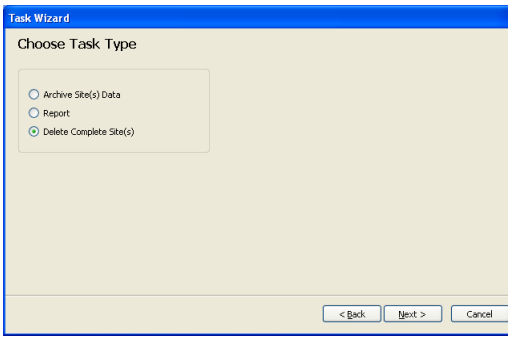
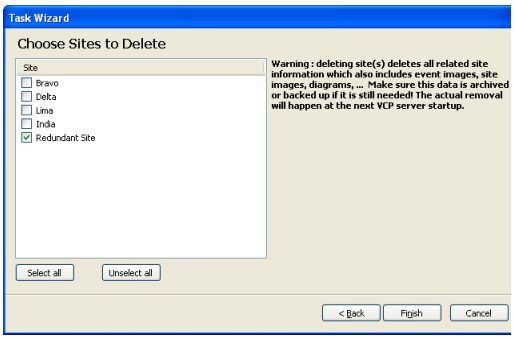
2.23.4 Delete a Site and its Events

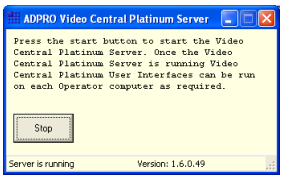
This process deletes a Site and all its events from the VCP Database permanently.

Prerequisite

The VCP UI is not connected to a site.

Process

Step	Action	Reference Section
Open the Task Schedule Wizard	Select the Tools > Administration > Task Scheduling menu 	2.7.3 Deleting a Site
Select the Delete Complete Site task	Click **New**  The Task Wizard is displayed. Click **Next** Select 'Delete Complete Site(s)'  Click **Next**	
Select the site to delete	Select the site(s), click **Finish** 	
Close the Task Scheduler	Click **OK** to close the Scheduled Tasks.	

Step	Action	Reference Section
Re-start the VCP Server to start the deletion process	**Note:** When Video Central Platinum Server is closed down the CMS is not in operation. You should stop the VCP Server at a time when its sites do not need to be monitored. Stop the VCP Server.  It is advised that you also exit the VCP UI. The deletion will occur next time the VCP Server starts up. Start the VCP Server.	

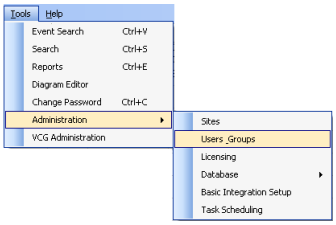
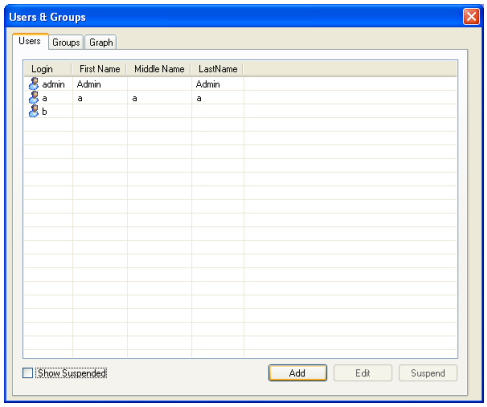
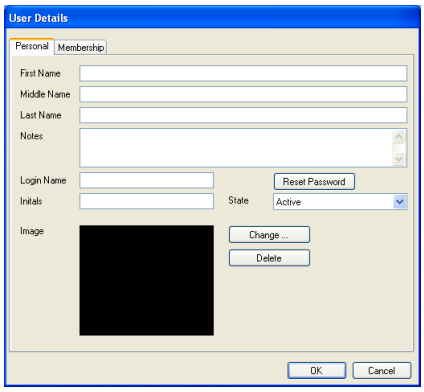
2.23.5 Add User

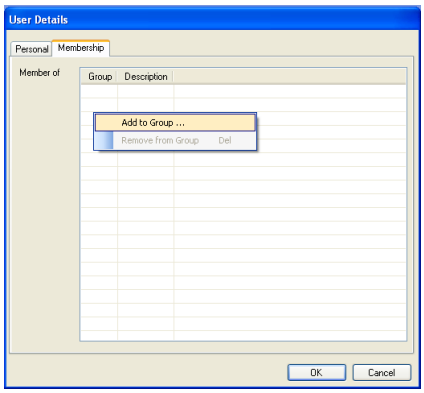
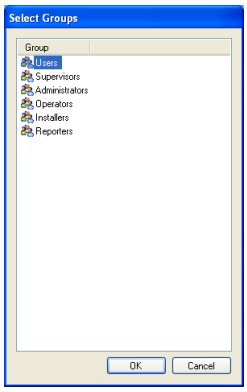
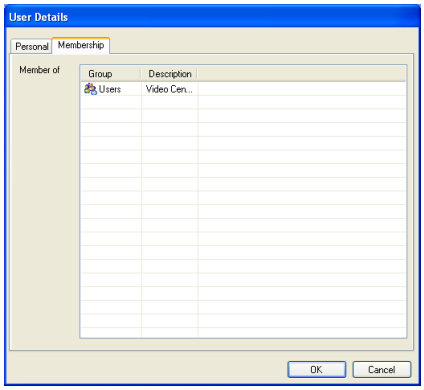
This process adds a User to the VCP Database.

Prerequisite

The VCP UI is not connected to a site.

Process

Step	Action	Reference Section
Open the Users & Groups dialogue	Select the Tools > Administration > Users & Groups menu 	2.8.1.1 Adding Users
Add the user	Click **Add** in the **Users** tab.  Enter a unique Login name and other detail identifying the user. 	

Step	Action	Reference Section
Add the user to User Groups according to their task permissions	Select the Membership tab and right-click within the Group list.  Select **Add to Group**  Select a group and click **OK**.  Repeat these steps to add the user to more groups.	

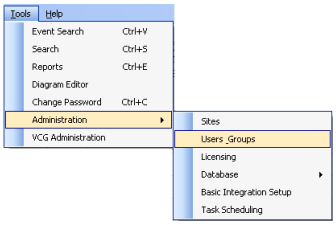
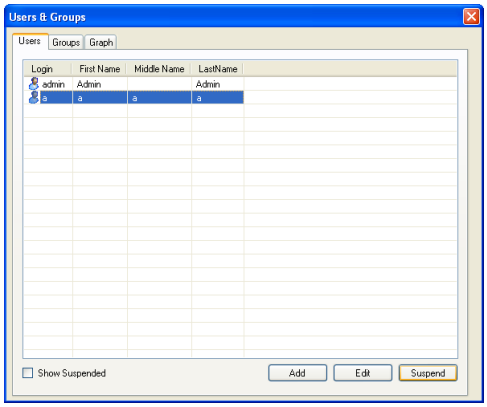
2.23.6 Suspend User

Suspending Users removes their login from the Users and Groups list and from the Graph.

Prerequisite

The VCP UI is not connected to a site.

Process

Step	Action	Reference Section
Open the Users & Groups dialogue	Select the Tools > Administration > Users & Groups menu 	2.8.1.3 Suspending Users
Suspend the user	Select a User and click the **Suspend** button.  Click **OK** 	

https://www.security.honeywell.com

A *Disclaimer* about this document, statements about *Intellectual Property, Copyrights*, and *Liability*, as well as a *General Warning* are available in an earlier section of this document.

Doc. 19116_22

Honeywell