



Virtual Console Software

Installation and User's Guide





Virtual Console Software Installation and User's Guide

TABLE OF CONTENTS

List of Figures	vii
List of Tables	ix
<i>Features and benefits.....</i>	<i>1</i>
<i>System components</i>	<i>2</i>
<i>Glossary.....</i>	<i>3</i>
<i>Operating features</i>	<i>4</i>
<i>Target device naming</i>	<i>4</i>
<i>Installing the software</i>	<i>8</i>
<i>Uninstalling the software.....</i>	<i>9</i>
<i>Opening the software.....</i>	<i>10</i>
<i>Setting up the software.....</i>	<i>10</i>
<i>Window features</i>	<i>13</i>
<i>Customizing the window display</i>	<i>15</i>
<i>Adding an appliance.....</i>	<i>15</i>
<i>Accessing appliances</i>	<i>18</i>
<i>Accessing target devices</i>	<i>19</i>
<i>Customizing properties</i>	<i>21</i>
<i>Viewing and changing general properties.....</i>	<i>21</i>
<i>Viewing and changing network properties.....</i>	<i>22</i>
<i>Viewing and changing information properties.....</i>	<i>22</i>
<i>Viewing connections properties.....</i>	<i>23</i>
<i>Customizing options.....</i>	<i>23</i>
<i>Viewing and changing general options</i>	<i>24</i>
<i>Managing folders.....</i>	<i>26</i>
<i>Assigning units</i>	<i>27</i>
<i>Deleting.....</i>	<i>28</i>
<i>Renaming</i>	<i>29</i>
<i>Managing the software database.....</i>	<i>29</i>
<i>Saving and loading a database.....</i>	<i>30</i>
<i>Exporting a database.....</i>	<i>30</i>
<i>Video session types</i>	<i>32</i>

<i>Using preemption</i>	33
<i>Preemption of a user by an administrator</i>	34
<i>Preemption of a local user/administrator by an administrator</i>	34
<i>Using exclusive mode</i>	35
<i>Using digital share mode</i>	36
<i>Using stealth mode</i>	37
<i>Using scan mode</i>	38
<i>Accessing scan mode</i>	39
<i>Setting scan options</i>	39
<i>Managing the scan sequence</i>	40
<i>Using the Thumbnail Viewer</i>	40
<i>Window features</i>	41
<i>Adjusting the view</i>	42
<i>Additional video adjustment</i>	43
<i>Adjusting mouse options</i>	45
<i>Cursor type</i>	45
<i>Scaling</i>	46
<i>Single cursor mode</i>	46
<i>Adjusting general options</i>	46
<i>Adjusting the Video Viewer toolbar</i>	47
<i>Setting the Toolbar Hide Delay time</i>	48
<i>Using macros</i>	48
<i>Sending macros</i>	49
<i>Selecting the macro group to display</i>	49
<i>Using virtual media</i>	49
<i>Virtual Media window</i>	50
<i>Virtual media session settings</i>	51
<i>Opening a virtual media session</i>	52
<i>Mapping virtual media drives</i>	52
<i>Displaying virtual media drive details</i>	53
<i>Resetting USB media devices</i>	53
<i>Closing a virtual media session</i>	54
<i>Managing Global settings</i>	56
<i>Configuring Global Network settings</i>	56
<i>Configuring Global Session settings</i>	58

<i>Configuring Global Virtual Media settings</i>	60
<i>Configuring Global Authentication settings</i>	62
<i>Configuring LDAP</i>	63
<i>LDAP authentication configuration parameters</i>	63
<i>LDAP server parameters</i>	64
<i>LDAP search parameters</i>	65
<i>LDAP Query Parameters</i>	66
<i>Appliance and target device query modes</i>	68
<i>Setting up Active Directory for performing queries</i>	70
<i>Managing local user accounts</i>	71
<i>Access levels</i>	71
<i>Locking and unlocking user accounts</i>	74
<i>Managing user sessions</i>	75
<i>Viewing and changing Conversion Option settings</i>	76
<i>Using SNMP</i>	78
<i>Managing SNMP traps</i>	80
<i>Viewing target device connection information</i>	82
<i>Modifying target device names</i>	82
<i>Resynchronizing the target device list</i>	84
<i>Configuring cascade switch connections</i>	84
<i>Viewing appliance and CO cable version information</i>	86
<i>Licensing appliance options</i>	86
<i>Upgrading firmware</i>	86
<i>Automatic firmware upgrades</i>	86
<i>Upgrading GCM4, GCM2, or RCM appliance firmware</i>	87
<i>Upgrading CO cable firmware</i>	88
<i>Rebooting the appliance</i>	89
<i>Managing the appliance configuration database</i>	90
<i>Saving an appliance configuration database</i>	90
<i>Restoring an appliance configuration database</i>	91
<i>Managing the appliance user database</i>	91
<i>Saving an appliance user database</i>	92
<i>Restoring an appliance user database</i>	92
Appendixes	93

<i>Appendix A: Updating VCS</i>	93
<i>Appendix B: Virtual media</i>	94
<i>Appendix C: Keyboard and mouse shortcuts</i>	96
<i>Appendix D: Ports used by the software</i>	98
<i>Appendix E: Getting help and technical assistance</i>	99
<i>Appendix F: Notices</i>	101
Index	103

LIST OF FIGURES

<i>Figure 3.1: Explorer window areas</i>	14
<i>Figure 3.2: New Appliance Wizard</i>	15
<i>Figure 3.3: Appliances in the Explorer</i>	18
<i>Figure 3.4: Devices in the Explorer</i>	19
<i>Figure 3.5: Device General Properties window</i>	21
<i>Figure 3.6: General Options window</i>	24
<i>Figure 3.7: Folders in the Explorer</i>	26
<i>Figure 4.1: Video Viewer window</i>	31
<i>Figure 4.2: Video Viewer - Thumbnail Viewer</i>	39
<i>Figure 4.3: Video Viewer window</i>	41
<i>Figure 4.4: Viewer manual scale</i>	43
<i>Figure 4.5: Manual Video Adjust window</i>	44
<i>Figure 4.6: Viewer Mouse Session Options window</i>	45
<i>Figure 4.7: Session Options - General tab</i>	47
<i>Figure 4.8: Session Options Window - Toolbar tab</i>	48
<i>Figure 4.9: Video Viewer Macros menu expanded</i>	49
<i>Figure 4.10: Virtual Media window</i>	51
<i>Figure 5.1: AMP Global Network settings</i>	57
<i>Figure 5.2: AMP Global Sessions settings</i>	59
<i>Figure 5.3: AMP Global Virtual Media settings</i>	61
<i>Figure 5.4: AMP Global Authentication settings</i>	62
<i>Figure 5.5: Server Parameters tab</i>	64
<i>Figure 5.6: Search Parameters tab</i>	65
<i>Figure 5.7: Query Parameters tab</i>	67
<i>Figure 5.8: Active Directory - KVM user</i>	69
<i>Figure 5.9: Active Directory - KVM appliance admin</i>	69
<i>Figure 5.10: Active Directory - Define groups</i>	70
<i>Figure 5.11: AMP User settings</i>	72
<i>Figure 5.12: AMP Status tab</i>	76
<i>Figure 5.13: AMP Conversion Option settings</i>	77
<i>Figure 5.14: AMP SNMP category</i>	79

Figure 5.15: AMP SNMP - Traps subcategory 81

Figure 5.16: AMP Settings - Devices 83

Figure 5.17: AMP Settings - Cascaded Switches 85

Figure 5.18: Conversion Options upgrade..... 87

Figure 5.19: AMP tools tab..... 90

LIST OF TABLES

Table 3.1: Explorer window areas 14

Table 4.1: Video session types..... 32

Table 4.2: Preemption scenarios..... 33

Table 4.3: Video Viewer window areas..... 42

Table 4.4: Manual Video Adjust window areas..... 44

Table 4.5: Virtual media session settings 51

Table 5.1: GCM4, GCM2, or RCM appliance access levels..... 71

Table C.1: Divider pane keyboard and mouse shortcuts..... 96

Table C.2: Tree view control keyboard and mouse shortcuts 96

Table C.3: Unit list keyboard and mouse operations 97

Table D.1: Ports Used by VCS 98

ation, you can
firm design offers
ns. Each
control at the

ing you with a
iances, install a
Devices, Sites,
ibilities to find

ou can use the
on Option

reating your own.
d convenience.

y appliance is

- IBM Global 2x16 Console Manager (GCM2)
- IBM Global 4x16 Console Manager (GCM4)
- IBM Remote Console Manager (RCM)

The GCM2 appliance includes two digital port sets for KVM-over-IP access, 1 analog port set for KVM access, 16 analog rack interface (ARI) ports for connecting CO cables and target devices, and virtual media capability for one local user and up to two remote users. The GCM4 appliance includes four digital ports for KVM-over-IP access, 1 analog port set for KVM access, 16 ARI ports for connecting CO cables and target devices, and virtual media capability for one local user and up to four remote users. The RCM appliance includes one digital port set for KVM-over-IP access, 1 analog port set for KVM access, 16 ARI ports for connecting CO cables and target devices. For a complete list of features supported by each appliance, refer to the corresponding *Installation and User's Guide*.

Authentication and authorization

Depending on how each appliance is configured, you can authenticate and authorize users by using either the appliance database or the Lightweight Directory Assistance Protocol (LDAP). LDAP is a vendor-independent protocol standard used for accessing, querying, and updating a directory using TCP/IP. Based on the X.500 directory services model, LDAP is a global directory structure that supports strong security features including authentication, privacy, and integrity. For more information on using LDAP authentication see "Configuring Global Authentication settings" on page 62.

After users log in to an appliance, the software caches their credentials (user name and password) for the duration of the VCS session.

System components

The software contains the following major components.

VCS Explorer

The VCS Explorer is the primary point of control for accessing the software features and functionality. It is the main Graphic User Interface (GUI) that displays on screen when the software is opened. From the Explorer, you can easily view the appliances and target devices defined in the local database. Built-in groupings such as Appliances and Devices provide a way to list units. You can create custom groups of units by adding and naming folders. Other groupings are also available, based on custom fields that you can assign to units.

From the VCS Explorer, you can select a target device from a Unit list, then click an icon to open a session to it. You can also select an appliance, then click an icon to start management and control functions.

Video Viewer

Control the keyboard, monitor, and mouse functions of individual target devices with the Video Viewer. You can use predefined macros and choose which macro group is displayed on the Video

Viewer Macros menu. You can open the Video Viewer for target devices on GCM4, GCM2, or RCM appliances.

The Video Viewer also provides access to the Virtual Media window. You can use the Virtual Media window to map drives from a target device to physical drives, such as a disk, CD, or DVD drive, on the client computer. For more information on the Virtual Media window, see "Using virtual media" on page 49.

Appliance Management Panels (AMPs)

Each AMP is implemented as a network management module that supports a target device type, such as keyboard, video, and mouse (KVM). An AMP contains a tabbed pane; each tab represents a top-level function category for the appliance. For example, the AMP tabs can be **Settings**, **Status**, and **Tools**. The number and content of tabbed panes differs for each appliance.

Glossary

The following words are used throughout this documentation:

- **ACI port connection** – a Cat5 cable connection between the ARI port of the GCM2 or GCM4 to an ACI-enabled KVM switch, allowing for integration of that KVM switch with the VCS
- **appliance** or **switch** (these terms are used interchangeably) - equipment that provides KVM-over-IP connectivity to attached target devices
- **cascade** or **tier** (these terms are used interchangeably) – connection between multiple KVM appliances that allows full keyboard and mouse input control and target device management from a single KVM appliance

For example, the tiering of an analog KVM appliance under a digital KVM appliance will allow keyboard and mouse input control to all target devices attached to that analog KVM appliance via the VCS interface. This can either be connected through a cascade switch or an ACI port connection.

- **cascade switch** – an earlier-model analog KVM appliance that is connected to a KCO cable attached to the ARI port of an RCM, GCM2, or GCM4 appliance, allowing for integration of an existing earlier-model switch configuration with the VCS
- **CO cable** - a Conversion Option cable that, when attached to the appliance and a target device, provides additional functionality such as virtual media sessions
- **switching system** - a set of appliances and attached target devices and CO cables
- **target device** - equipment such as a server or router that is attached to an appliance
- **unit** - includes appliances and target devices; this term is used when the procedure is referring to either or both
- **user** - a KVM connection from an analog port on the appliance
- **virtual media** - a USB media device that can be attached to the appliance and made available to any target device that is connected to the appliance

Operating features

"Keyboard and mouse shortcuts" on page 96 lists the Explorer navigation shortcuts. Other components also support full keyboard navigation in addition to mouse operations.

Target device naming

The software requires that each appliance and target device have a unique name. To minimize the need for operator intervention, the software uses the following procedure to generate a unique name for a target device whose current name conflicts with another name in the database.

During background operations (such as an automated operation that adds or modifies a name or connection), if a name conflict occurs, the conflicting name is automatically made unique. This is done by appending a tilde (~) followed by an optional set of digits. The digits are added in cases where adding the tilde alone does not make the name unique. The digits start with a value of one and are incremented until a unique name is created.

During operations, if you or another user specifies a non-unique name, a message informs the corresponding user that a unique name is required.

Target device name displays

When an appliance is added, the target device names retrieved from the appliance are stored in the software database. The operator can then rename a target device in the Explorer. The new name is stored in the database and used in various component screens. This new target device name is not communicated to the appliance.

You can change target device names on both the appliance and the database by using the Modify Device Name window in the AMP. For more information see "Modifying target device names" on page 82.

Since the software is a decentralized management system, you can change the name assigned to a target device on the appliance at any time without updating the software database. Each operator can customize a particular view of the list of target devices being managed.

Since you can associate more than one name with a single target device - one on the appliance and one in the software - the software uses the following rules to determine which name is used:

- The Explorer only shows the target devices listed in its database, with the name specified in the database. In other words, the Explorer does not talk to the appliance to obtain target device information.
- The AMP displays information retrieved from the appliance, except where noted.
- The Resync Wizard (which is used to resynchronize target device lists in the AMP) overwrites locally-defined target device names only if the appliance target device name has been changed from the default value. Non-default target device names that are read from the appliance during a resynchronization override the locally-defined names.

Sorting

In certain displays, the software component displays a list of items with columns of information about each item. If a column header contains an arrow, you can sort the list by that column in ascending or descending order.

To sort a display by a column header, click the arrow in a column header. The items in the list are sorted according to that column. An upward-pointing arrow indicates the list is sorted by that column header in ascending order. A downward-pointing arrow indicates the list is sorted by that column header in descending order.

Getting started

Before you install the software, make sure that you have all the required items.

Supplied with VCS

The following items come with the VCS:

- Documentation CD
- Virtual Console Software CD
- Download instructions

Supported operating systems

The following operating systems are supported by the VCS:

- Microsoft® Windows® 2000 Workstation Service Pack 4
- Microsoft Windows 2000 Server Service Pack 4
- Microsoft Windows XP (Home and Professional) Service Pack 2
- Microsoft Windows Server 2003 Service Pack 1
- Red Hat Enterprise Linux 3.0 WS
- Red Hat Enterprise Linux 4.0 WS
- SuSE Linux Enterprise Server 8
- SuSE Linux Enterprise Server 9
- SuSE Linux 9.2
- SuSE Linux 9.3

Hardware configuration requirements

The software is supported on the following minimum computer hardware configurations:

- 500 MHz Pentium III
- 256 MB RAM
- 10BASE-T or 100BASE-T NIC

- XGA video with graphics accelerator
- Desktop size must be a minimum of 800 x 600
- Color palette must be a minimum of 65,536 (16-bit) colors

Browser requirements

You will need one of the following browsers installed on the computer to run the VCS:

- Internet Explorer 5.0 or later (Windows only)
- Netscape 6.0 or later
- Mozilla™ 1.4 or later
- Firefox 1.0 or later

Installing the software

To install on Microsoft Windows operating systems, complete the following steps:

1. Insert the VCS CD into the CD drive. Complete one of the following steps:
 - If AutoPlay is supported and enabled, the setup program starts automatically.
 - If the computer does not support AutoPlay, set the default drive to the CD drive letter and execute the following command to start the install program (replace “drive” with the CD drive letter on the system):
`drive:\VCS\win32\setup.exe`
2. Follow the on-screen instructions.

To install on Linux operating systems, complete the following steps:

1. Insert the VCS CD into the CD drive. Complete one of the following steps:
 - When using Red Hat and SUSE Linux distributions, the CD will usually be mounted automatically.
Continue with step 2 if the CD mounts automatically.
 - If the CD does not mount automatically, you might need to issue the mount command manually. The following is an example of a typical mount command:
`mount -t iso9660 device_file mount_point`
where *device_file* is the system-dependent device file associated with the CD and *mount_point* is the directory that will be used to access the contents of the CD after it is mounted. Typical default values include `"/mnt/cdrom"` and `"/media/cdrom"`.
See the Linux operating system documentation for the specific mount command syntax to use.
2. Open a command window and navigate to the CD mount point. For example:
`cd /mnt/cdrom`
3. Enter the following command to start the install program:

```
sh ./VCS/linux/setup.bin
```

4. Follow the on-screen instructions.

During installation

You are prompted to select the destination location where the application will be installed. You can select an existing path or type a directory path. The default path for Windows 2000, NT, and XP systems is the program files directory. The default path for Linux systems is the `usr/lib` directory.

If you enter a path that does not exist, the installation program automatically creates it during installation.

You can also indicate if you want a VCS icon installed on the desktop.

Uninstalling the software

To uninstall the software on Microsoft Windows operating systems, starting at the Control Panel, complete the following steps:

1. Open the Control Panel and select **Add/Remove Programs**. A sorted list of currently installed programs opens.
2. Select the VCS entry.
3. Click the **Change/Remove** button. The uninstall wizard starts.
4. Click the **Uninstall** button and follow the on-screen instructions.

To uninstall the software on Microsoft Windows operating systems, using a command window, complete the following steps:

1. Open a command window and change to the VCS install directory used during installation. The default path for win32 systems is the program files directory.
2. Change to the `UninstallerData` subdirectory and enter the following command (the quotation marks are required):

```
"Uninstall IBM Virtual Console Software.exe"
```

The uninstall wizard starts. Follow the on-screen instructions.

To uninstall the software on Linux operating systems, complete the following steps:

1. Open a command window and change to the VCS install directory used during installation. The default path for Linux systems is the `usr/lib` directory.
2. Change to the `UninstallerData` subdirectory and enter the following command:

```
sh ./Uninstall_IBM_Virtual_Console_Software
```

The uninstall wizard starts. Follow the on-screen instructions.

Opening the software

To open the software on Microsoft Windows operating systems, complete one of the following steps:

- Select **Start > Programs > IBM Virtual Console Software**.
- Double-click the **IBM VCS** icon.

To open the software on Linux from the application folder (the default location is `/usr/lib/IBM_Virtual_Console_Software/`), complete one of the following steps:

- Enter the command: `./IBM_Virtual_Console_Software`
- From `(/user/bin)`, enter the following link: `./IBM_Virtual_Console_Software`
- If a desktop shortcut was created on installation, double-click the shortcut.

Setting up the software

This section provides an overview of setup and configuration steps. Details are provided in other chapters. For appliance-specific information, see the *Installation and User's Guide* for the appliance.

To set up the software, complete the following steps:

1. Install the software on each computer.
2. From one computer, open the software.
3. Complete one of the following steps:
 - Click the **New Appliance** button to add an appliance to the software database. The New Appliance Wizard opens.
 - Select **Tools > Discover** from the software menu to search for all IBM GCM2, GCM4, and RCM appliances.
4. Use the Explorer to set unit properties, options, and other customization as needed.
5. Select an appliance and click the **Manage Appliance** button to create local user accounts through the appliance AMP.
6. From the AMP **Devices** category, set the names of all target devices.
7. Repeat steps 3 through 6 for each GCM4, GCM2, and RCM appliance you want to manage.
8. After one VCS environment is set up, select **File > Database > Save** to save a copy of the local database with all the settings.
9. From the software on a second computer, select **File > Database > Load** and browse the file you have saved. Select the file and then click **Load**. Repeat this step for each client computer that you want to setup.

10. To access a target device attached to an appliance, select the target device in the Explorer and click the **Connect Video** or **Browse** button to open a session (only the corresponding button for the selected target device is visible).

For information about creating user accounts on an LDAP directory service, see "Configuring LDAP" on page 63.

To set up a GCM4, GCM2, or RCM appliance, complete the following steps:

1. Adjust mouse acceleration on each target device to **Slow** or **None**.
2. Install the appliance hardware, connect the CO cables and connect the keyboard, monitor, and mouse to the analog port.
3. Connect a terminal to the serial configuration port on the rear panel of the appliance and set up the network configuration (network speed and address type).
4. At the local analog computer, input all target device names using the OSCAR interface. You can also input target device names using the VCS.

VCS Explorer

About the VCS Explorer

The VCS Explorer (which is called Explorer from here on) is the main GUI interface for the software. You can view, access, manage, and create custom groupings for all supported units.

When you start the software, the main Explorer window opens.

Window features

The Explorer window is divided into several areas: the View Selector buttons, the Group Selector pane, and the Unit Selector pane. The content of these areas changes, based on whether a target device or an appliance is selected or what task is to be completed. Figure 3.1 on page 14 shows the window areas; descriptions follow in Table 3.1 on page 14.

Click one of the **View Selector** buttons to view the switching system organized by categories: **Appliances**, **Devices**, **Sites**, or **Folders**. The Explorer's default display is user-configurable. For more information, see "Customizing the window display" on page 15.

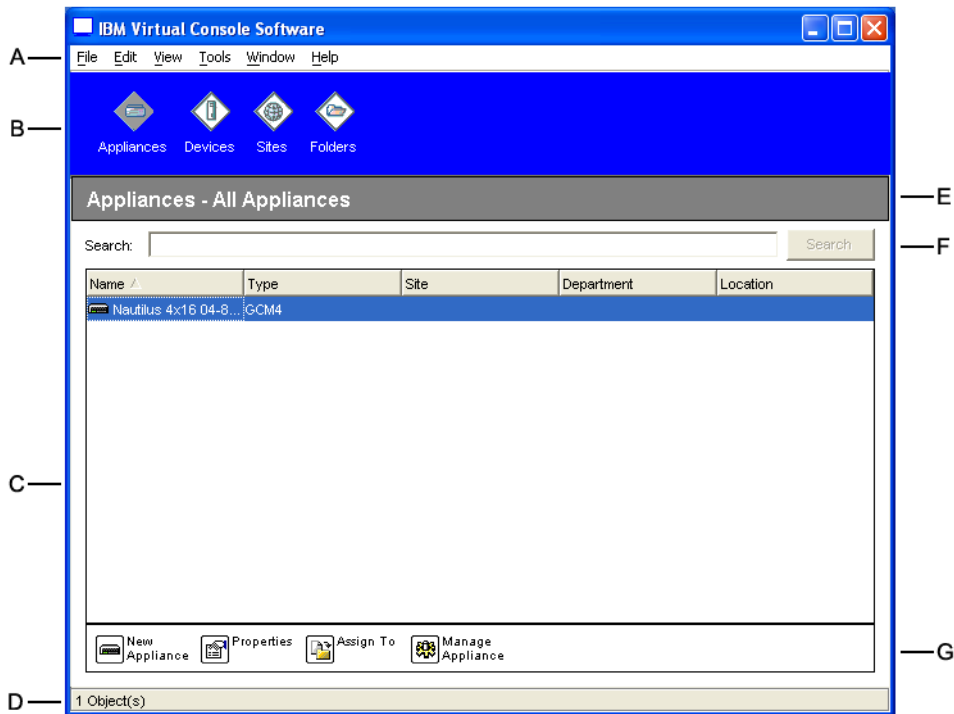


Figure 3.1: Explorer window areas

Table 3.1: Explorer window areas

Area	Description
A	Menu bar: Provides access to many of the features in the software.
B	View Selector pane: Contains View Selector buttons for choosing the Explorer view. Clicking a button shows the switching system organized by the button category: Appliances , Devices , Sites , or Folders . You can configure which button is visible by default.
C	Unit list: Displays a list of target devices, appliances, and other selectable units contained in the currently selected group, or the results of the search executed from the Search bar.
D	Status bar: Displays the number of units shown in the Unit list.
E	Unit Selector pane: Contains the Search bar, Unit list, and Task buttons that correspond to the selected view or group.
F	Search bar: Gives you the ability to search the database for the text entered in the Search field.
G	Task buttons: Represent tasks that can be executed. Some buttons are dynamic, based on the unit selected in the Unit list, while other buttons are fixed and always present.

Customizing the window display

You can resize the Explorer window at any time. Each time you start the application, the Explorer window opens to its default size and location.

A split-pane divider that runs from top to bottom separates the Group Selector pane and the Unit Selector pane. You can move the divider left and right to change the viewing area of these two panes. Each time the Explorer is opened, the divider returns to its default location. See "Keyboard and mouse shortcuts" on page 96 for divider pane and tree view control shortcuts.

You can specify which view (Appliances, Devices, Sites, or Folders) is visible on startup or you can let the Explorer determine it. For more information, see "Selected view on startup" on page 25.

You can change the order and sorting of the Unit list by clicking the sort bar above the column. An upward-pointing arrow in a column header indicates that the list is sorted by that field name in ascending order. A downward-pointing arrow indicates the list is sorted by that field name in descending order.

Adding an appliance

Before you can access the appliance through the software, you must add it to the software database. After an appliance is added, it is visible in the Unit list. You can either manually add or discover an appliance.

To manually add an appliance with an assigned IP address, complete the following steps:

1. Complete one of the following steps:
 - Select **File > New > Appliance** from the Explorer menu.
 - Click the **New Appliance** button.

The New Appliance Wizard opens. Click **Next**.

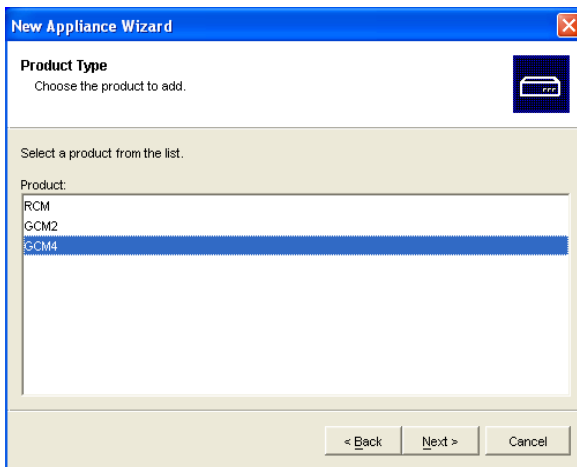


Figure 3.2: New Appliance Wizard

2. Select the type of appliance you are adding. Click **Next**.
3. Click **Yes** to indicate that the appliance has an assigned IP address, then click **Next**.
4. Type the IP address and click **Next**.
5. The software searches for the appliance.

The software searches for the indicated unit as well as all the powered CO cables and target device names you associated with it in OSCAR, if any. To search for unpowered CO cables, you can access the resync feature in the **Devices** category of the AMP and select the **Include Offline Conversion Options** check box.

The Enter Cascade Switch Information window opens if the software detects an attached cascade switch. This window contains a list of all ports and CO cable eIDs (Electronic Identification Numbers) retrieved from the appliance and the tiered switch types to which they are connected, if any. When this window first opens, all appliances are set to **None**. Detected appliances have an icon next to the pull-down menu.

- a. The **Existing Cascaded Switches** field contains all the current cascade switch types defined in the database. Click **Add**, **Delete**, or **Modify** to alter the list.
 - b. Associate the applicable cascade switch types from the pull-down menus for each CO cable that has a cascade switch attached.
6. When you reach the final page of the Wizard, click **Finish** to exit the Wizard and return to the main window. The appliance is now included in the Unit list.

To manually install a new appliance with no assigned IP address, complete the following steps:

1. Complete one of the following steps:
 - Select **File > New > Appliance** from the Explorer menu
 - Click the **New Appliance** button.

The New Appliance Wizard opens. Click **Next**.

2. Click **No** to indicate that the appliance does not have an assigned IP address, then click **Next**.
3. The Network Address window opens. Type the IP address, subnet mask, and gateway you want to assign to the appliance and then click **Next**.
4. The software searches for any GCM4, GCM2, or RCM appliances that do not have assigned IP addresses. Select the unit to add from the list of new appliances that were found and then click **Next**.
5. The Configuring Appliance window indicates whether the IP information was configured. If the configuration is complete, the software searches for the new appliance. Click **Next**.

The software also searches for all CO cables and target device names associated with the appliance.

The Enter Cascade Switch Information window opens if the software detects an attached cascade switch. This window contains a list of all ports and CO cable eIDs retrieved from the appliance and the cascade switch types to which they are connected, if any.

- a. The Existing Cascaded Switches field contains all the current cascade switch types defined in the database. Click **Add**, **Delete**, or **Modify** to alter the list.
 - b. Associate the applicable cascade switch type from the pull-down menus for each CO cable that has a cascade switch attached.
6. When complete, click **Finish** to exit the Wizard and return to the main window. The appliance is now included in the Unit list.

To discover an appliance by IP address, complete the following steps:

1. Select **Tools > Discover** from the Explorer menu. The Discover Wizard opens. Click **Next**.
2. The Address Range page opens. Type the range of IP addresses to search on the network in the To and From boxes. Use IP address dot notation. Click **Next**.
3. Complete one of the following steps:
 - The Searching Network progress window opens. Progress text indicates how many addresses have been probed from the total number specified by the range, and the number of appliances found (for example, 21 of 100 addresses probed: 3 appliances found). If one or more new appliances are discovered, the Wizard shows the Select Appliances to Add page. From this page, you can select the appliances to add to the local database.
 - If no new appliances were found (or if you clicked **Stop**), the Wizard shows the No New Appliances Found page. You can try entering a different range to search or add the appliances manually.
4. Select one or more appliances to add and click the **Add (>)** icon to move the selection or selections to the Appliances to Add list. When the Appliances to Add list contains all the appliances you want to add, click **Next**.
5. The Adding Appliances progress bar window opens. Once all of the appliances have been added to the local database, the Discover Wizard Completed page opens. Click **Finish** to exit the Wizard and return to the main window. The new appliance is now visible in the Unit list. If one or more appliances cannot be added to the local database for any reason, the Discover Wizard Not All Appliances Added page opens. This page lists all of the appliances that you selected and the status for each. The status indicates if an appliance was added to the local database and if not, why the process failed. Click **Done** when you are finished reviewing the list.

If an appliance already exists in the database with the same IP address as a discovered unit, then the discovered unit is ignored and is not listed on the next Wizard page.

The Discover Wizard does not automatically find target devices attached to the appliance. After running the Discover Wizard, access the applicable AMP and click the **Resync** button on the **Devices** category to find target devices attached to the appliance.

Accessing appliances

Clicking the **Appliances** button opens a list of the appliances currently defined in the local database. The Group Selector pane is visible if two or more appliance types are defined. Click **All Appliances** or click on a folder to view all appliances of a particular type.

A user name and password prompt opens if this is the first unit access attempt during the VCS session. After a unit is accessed, subsequent access attempts for any unit that uses the same user name and password credentials during this VCS session do not require a user name and password. The software provides credential caching that captures credentials upon first use and automates the authentication of subsequent unit connections.

To clear login credentials, open the Explorer and go to **Tools > Clear Login Credentials**.

Accessing the appliance opens the AMP for that appliance. For more information, see the "Appliance Management Panel" chapter beginning on page 55.

To log in to an appliance, complete the following steps:

1. Click the **Appliances** button in the Explorer.

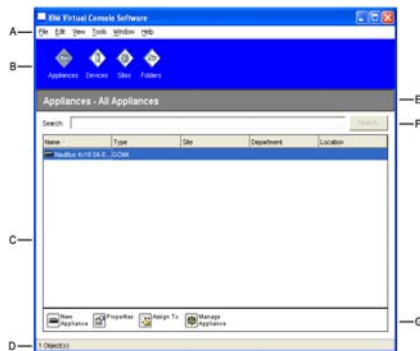


Figure 3.3: Appliances in the Explorer

2. Complete one of the following steps:
 - Double-click on an appliance in the Unit list.
 - Select an appliance, and then click the **Manage Appliance** button.
 - Right-click on an appliance. A pop-up menu opens. Select **Manage Appliance** from the pop-up menu.
 - Select an appliance in the Unit list and press Enter.
3. If a user name and password prompt opens, type the user name and password. [If this is the first appliance access since initialization or reinitialization, the default user name is Admin (case sensitive) with no password.]
4. Complete one of the following steps:

- Click **OK** to access the appliance. This opens the AMP for the appliance. For more information about the AMP, see "Appliance Management Panel" chapter beginning on page 55.
- Click **Cancel** to exit without logging in.

Accessing target devices

Clicking the **Devices** button opens a list of target devices such as servers, routers, and other managed equipment that is defined in the local database. The Group Selector pane is visible if two or more device types are defined. Click **All Devices** or click on a folder to view all target devices of a particular type.

A user name and password prompt opens if this is the first unit access attempt during the VCS session. After a unit is accessed, subsequent access attempts for any unit that uses the same user name and password credentials during this VCS session do not require a user name and password. The software provides credential caching that captures credentials upon first use and automates the authentication of subsequent unit connections.

To clear login credentials, in the Explorer go to **Tools > Clear Login Credentials**.

When you select a device and click the **Connect Video** button, the Video Viewer launches. The Video Viewer allows you full keyboard, video and mouse control over a device. If a URL has been defined for a given device, then the **Browse** button will also be available. The **Browse** button will launch the configured Web browser, if any, or default browser to the defined URL for that device. For more information, see "Customizing properties" on page 21 and "Customizing options" on page 23.

You can also scan through a customized list of devices using the **Thumbnail Viewer**. This view contains a series of thumbnail frames, each containing a small, scaled, non-interactive version of a device screen image. For more information, see "Using scan mode" on page 38.

To access a target device, complete the following steps:

1. Click the **Devices** button in the Explorer.

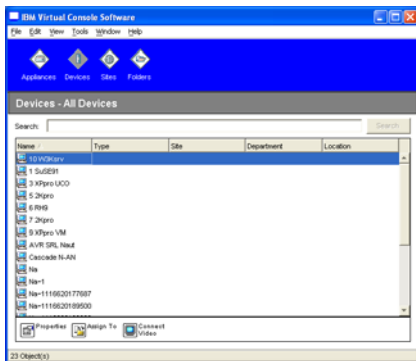


Figure 3.4: Devices in the Explorer

2. Complete one of the following steps:
 - Double-click on a target device in the Unit list.
 - Select a target device, and then click the connection button: **Connect Video** if connected to a GCM4, GCM2, or RCM appliance or **Browse** if a URL is configured. Only the applicable button or buttons for the selected target device are visible.
 - Right-click on the target device. Select the connection entry from the pop-up menu: **Connect Video** for a GCM4, GCM2, or RCM appliance or **Browse** if a URL is configured. Only the applicable entry for the selected target device is visible.
 - Select a target device in the Unit list and press Enter.
3. If a browser is used for access, no user name and password prompt opens.

If the Video Viewer is used for access, a user name and password prompt opens if this is the first access attempt during the VCS session.

After a unit is accessed, subsequent access attempts for any unit that uses the same user name and password credentials during this VCS session do not require a user name and password.

The configured access method for that target device opens in a new window.

To search for a target device in the local database, complete the following steps:

1. Click the **Devices** button and insert the cursor in the **Search** field.
2. Type the search information. This could be a target device name or a property such as type or location.
3. Click the **Search** button. The results are included in the Unit list.
4. Complete one of the following steps:
 - Review the results of the search.
 - Click the **Clear Results** button to open the entire list again.

To auto search by typing in the Unit list, complete the following steps:

1. Click the **Devices** button, then click on any item in the Unit list.
2. Begin typing the first few characters of a target device name. The highlight moves to the first target device name beginning with those characters. To reset the search so you can find another target device, pause for a few seconds and then type the first few characters of the next target device.

If the target device you are attempting to access is currently being viewed by another user, you can preempt the user so you can have access to that target device, or request a shared session with that user (KVM sharing is only available on GCM4 and GCM2 appliances). For more information, see "Using preemption" on page 33 and "Using digital share mode" on page 36.

Customizing properties

The Properties window in the Explorer contains the following tabs: **General**, **Network**, **Information**, and, if the selected unit is a device, **Connections**. Use these tabs to view and change properties for the selected unit.

Viewing and changing general properties

In general properties, you can specify a unit Name, Type (target device only), Icon, Site, Department, and Location. (To customize the Site, Department, and Location field labels, see "Custom field names" on page 24.)

To view or change general properties, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
 - Select **View > Properties** from the Explorer menu.
 - Click the **Properties** button.
 - Right-click on the unit. Select **Properties** from the pop-up menu.

The General Properties window opens.

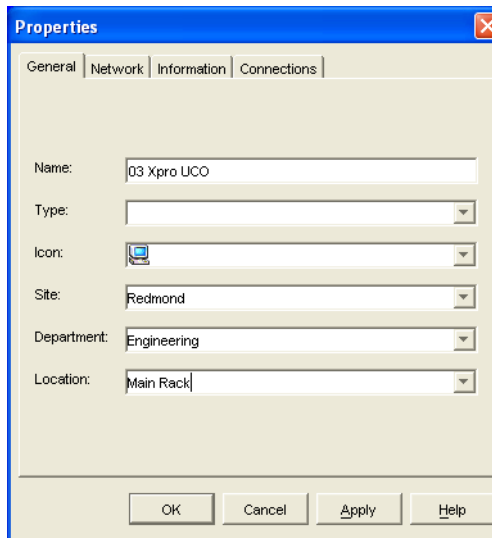


Figure 3.5: Device General Properties window

3. In the **Name** field, type a 1 to 32 character unique name. (This name is local to the software database; the appliance database might contain a different name for this unit.)

4. The **Type** field is read-only for appliances. For a target device, select a type from the pull-down menu or enter a 1 to 32 character type in the text field.
5. In the **Icon** field, select an icon from the pull-down menu.
6. In the **Site**, **Department**, and **Location** fields, select an entry from the pull-down menu or enter a 1 to 32 character Site, Department, or Location in the corresponding text field.
7. Complete one of the following steps:
 - Click another tab to change additional properties.
 - If finished, click **OK** to save the new settings.
 - Click **Cancel** to exit without saving the new settings.

Viewing and changing network properties

For an appliance, network properties include the address of the appliance.

For a target device, network properties specify the URL to use when establishing a browser connection to the target device. When this field contains a value, the **Browse** button is visible in the Explorer task bar.

To view or change network properties, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
 - Select **View > Properties** from the Explorer menu.
 - Click the **Properties** button.
 - Right-click on the unit. Select **Properties** from the pop-up menu.

The Properties window opens.

3. Click the **Network** tab.
4. In the Address field (appliances only), enter the appliance address in IP dot notation or 1 to 128 character host name. The address cannot be blank, a loopback address, or all zeros. You cannot enter duplicate addresses.
5. In the **Browser URL** field (devices only), enter a 1 to 256 character URL for establishing a browser connection.
6. Complete one of the following steps:
 - Click another tab to change additional properties.
 - If finished, click **OK** to save the new settings.
 - Click **Cancel** to exit without saving the new settings.

Viewing and changing information properties

Information properties include description, contact phone number, and comment information; you can use these fields to store any information you require.

To view or change information properties, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
 - Select **View > Properties** from the Explorer menu.
 - Click the **Properties** button.
 - Right-click on the unit. Select **Properties** from the pop-up menu.The Properties window opens.
3. Click the **Information** tab. You can enter any information in the following fields.
 - a. In the **Description** field, enter 0 to 128 characters.
 - b. In the **Contact** field, enter 0 to 128 characters.
 - c. In the **Contact Phone Number** field, enter 0 to 64 characters.
 - d. In the **Comment** field, enter 0 to 256 characters.
4. Complete one of the following steps:
 - Click another tab to change additional properties.
 - If finished, click **OK** to save the new settings.
 - Click **Cancel** to exit without saving the new settings.

Viewing connections properties

Connections properties are available only for target devices and are read-only. The display indicates the physical connection path that is used to access this target device and the connection type, such as video.

To view connections properties, complete the following steps:

1. Select a target device in the Unit list.
2. Complete one of the following steps:
 - Select **View > Properties** from the Explorer menu.
 - Click the **Properties** button.
 - Right-click on the unit. Select **Properties** from the pop-up menu.The Properties window opens.
3. Click the **Connections** tab.

Customizing options

Set general options for the Explorer in the Options window. General options include custom field names, selected view on startup, browser application, and DirectDraw support.

Viewing and changing general options

You can customize options for the Explorer, including custom name fields, default view, and default browser.

Custom field names

In the Custom field labels area, you can change the Site, Department, and Location headings that are visible in the Group and Unit Selector panes. You can group units in ways that are meaningful to you. The **Department** field is a subset of Site.

To change custom field names, complete the following steps:

1. Select **Tools > Options** from the Explorer menu. The General Options window opens.

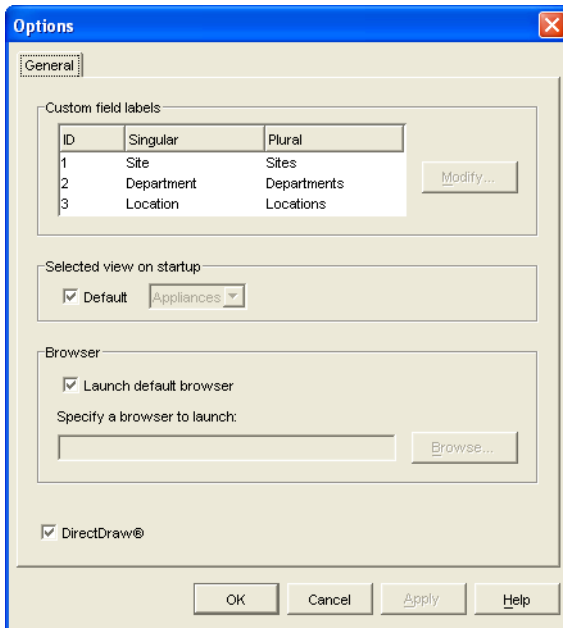


Figure 3.6: General Options window

2. In the Custom field labels area, select a field label to modify and click the **Modify** button. The Modify Custom Field Label window opens. Remember that the **Department** field is a subset of the **Site** field, even if it is renamed. Type the 1 to 32 character singular and plural versions of the new field label. You can use embedded spaces but not leading or trailing spaces. You cannot use blank field labels.
3. Complete one of the following steps:
 - If finished, click **OK** to save the new settings.
 - Click **Cancel** to exit without saving the new settings.

Selected view on startup

The “Selected view on startup option” specifies the view that is visible when the software opens, either Appliances, Devices, Sites, or Folders. You can select a view or let the Explorer determine the view. When you let the Explorer determine the view, the Devices view is visible if you have one or more target devices defined. If you do not, the Appliances view is visible.

To view or change the selected view on startup, complete the following steps:

1. Select **Tools > Options** from the Explorer menu. The General Options window opens.
2. Complete one of the following steps:
 - If you want the Explorer to determine the best view on startup, select the **Default** check box.
 - If you want to specify which view opens on startup, clear the **Default** check box and select **Appliances, Devices, Sites, or Folders** from the pull-down menu.
3. Complete one of the following steps:
 - If finished, click **OK** to save the new settings.
 - Click **Cancel** to exit without saving the new settings.

Default browser

The Browser option specifies the browser application that opens when you click the **Browse** button for a target device that has URL defined, or when the VCS online help is opened. You can either enable the default browser application of the current computer or select among other available browsers.

To view or change the default browser, complete the following steps:

1. Select **Tools > Options** from the Explorer menu. The General Options window opens.
2. Complete one of the following steps:
 - In the **Browser** field, select the **Launch Default Browser** check box to specify the default browser.
 - Clear the **Launch Default Browser** check box. Click the **Browse** button and select a browser executable on the computer. You can also enter the full path name of the browser executable.
3. Complete one of the following steps:
 - If finished, click **OK** to save the new settings.
 - Click **Cancel** to exit without saving the new settings.

DirectDraw support (Windows only)

The DirectDraw option affects operation of the Video Viewer when running on Windows operating systems. The software supports DirectDraw, a standard that you can use to directly manipulate video display memory, hardware blitting, hardware overlays, and page flipping without the

intervention of the Graphical Device Interface (GDI). This can result in smoother animation and improvement in the performance of display-intensive software.

However, if the machine has a software cursor or pointer shadow enabled, or if the video driver does not support DirectDraw, you can experience a flicker in the mouse cursor when over the title bar of the Video Viewer. You can either disable the software cursor or pointer shadow, load a new target device driver for the video card, or disable DirectDraw.

To view or change DirectDraw support, complete the following steps:

1. Select **Tools > Options** from the Explorer menu. The General Options window opens.
2. In the DirectDraw field, select or clear the **DirectDraw** check box.
3. Complete one of the following steps:
 - If finished, click **OK** to save the new settings.
 - Click **Cancel** to exit without saving the new settings.

Managing folders

Use folders to create a customized organizational system for groups of units. For example, you might create a folder for critical target devices or for remote target devices. Folders are listed under the **Folders** button in the Explorer. You can name and structure folders in any way you choose.

To create a folder, complete the following steps:

1. Select the **Folders** button.

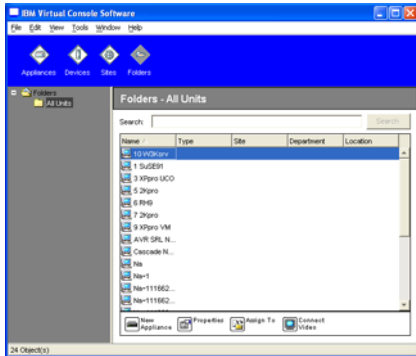


Figure 3.7: Folders in the Explorer

2. Complete one of the following steps:
 - Click on the top-level **Folders** node and select **File > New > Folder**.
 - To create a nested folder, click on an existing folder and select **File > New > Folder** in the Explorer menu. The New Folder window opens.

3. Type a 1 to 32 character name. Folder names are not case sensitive. You can use embedded spaces but not leading or trailing spaces. You cannot use duplicate folder names at the same level, but you can use duplicate folder names on different levels.
4. Click **OK**. The new folder is listed in the Group Selector pane.

To assign a unit to a folder, see "Assigning units" on page 27. To rename or delete a folder, see "Renaming" on page 29 and "Deleting" on page 28.

Assigning units

After you have created a new Site, Location, or Folder, you can assign a unit to that organization. The **Assign** menu item is only enabled when a single unit is selected in the Unit list (the custom assignment targets are defined in the General Properties window).

There are three ways to assign a unit to a Site, Location, or Folder: editing the unit Properties window, using the Assign function, or dragging and dropping.

To assign a unit to a Site, Location, or Folder using the Properties window, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
 - Select **View > Properties** from the Explorer menu.
 - Click the **Properties** button. The Properties window opens.
3. Click the **General** tab. Select the Site, Department, or Location to which you want to assign the unit.
4. Complete one of the following steps:
 - Click **OK** to save the assignment.
 - Click **Cancel** to exit without saving the assignment.

To assign a unit to a Site, Location, or Folder using the Assign function, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
 - Select **Edit > Assign** from the Explorer menu.
 - Click the **Assign To** button.
 - Right-click on a unit and select **Assign To** from the pop-up menu.

The Assign To window opens.

3. In the Category pull-down menu, select **Site, Location, or Folder**.
4. In the Target list, select the assignment you want to designate. The target list is empty if no Site, Location, or Folder has been defined in the local database.
5. Complete one of the following steps:

- Click **OK** to save the assignment.
- Click **Cancel** to exit without saving the assignment.

To assign a unit to a Site, Location, or Folder using drag and drop, complete the following steps:

1. To use drag and drop, click and hold on a unit in the Unit list.
2. Drag the item on top of a folder icon (node) in the tree view of the Group Selector pane. Release the mouse button.
3. The item is now visible in the Unit list when you click that node.

A unit cannot be moved to All Departments, All Units, or the root Sites node. Units can only be moved one at a time.

Deleting

The delete function works according to what is currently selected in the Group and Unit Selector panes. When you select and delete a unit in the Unit list, it is removed from the local database. When you select and delete an item in the tree view of the Group Selector pane, you can delete Server Types, Sites, Departments, or Folders; however, none of the actions result in units being deleted from the local database.

To delete a unit, complete the following steps:

1. Select the unit or units to delete from the Unit list.
2. Complete one of the following steps:
 - Select **Edit > Delete** from the Explorer menu.
 - Right-click on a unit and select **Delete** from the pop-up menu.
 - Press the Delete key on the keyboard.
3. A window prompts you to confirm the number of units you want to delete. If you are deleting an appliance, the window includes a **Delete Associated Devices** check box. Select or clear the check box as needed. If you do not delete the associated target devices, they are still visible in the target devices list but you cannot connect to them unless they have a URL assigned, in which case you can connect to the target device using a browser.
4. Complete one of the following steps:
 - Click **Yes** to confirm the deletion. You might receive additional message prompts, depending on the configuration. Respond as needed. The units are deleted.
 - Click **No** to cancel the deletion.

To delete a target device Type, Site, Department, or Folder, complete the following steps:

1. Select the target device Type, Site, Department, or Folder to delete from the Group Selector pane.
2. Complete one of the following steps:
 - Select **Edit > Delete** from the Explorer menu.

- Press the Delete key on the keyboard.
3. You are prompted to confirm the number of units that are affected by this deletion. Complete one of the following steps:
 - Click **Yes** to confirm the deletion. You might receive additional message prompts, depending on the configuration. Respond as needed. The element is deleted.
 - Click **No** to cancel the deletion.

Renaming

The rename function works according to what is currently selected. You might select and rename an appliance or a target device from the Unit list. You can select and rename unit Types, Sites, Departments, and Folder names in the tree view of the Group Selector pane.

To rename a unit Type, Site, Department, or Folder, complete the following steps:

1. Complete one of the following steps:
 - Select a unit from the Unit list.
 - In the Group Selector pane, select the unit Type, Site, Department, or Folder to rename.
2. Complete one of the following steps:
 - Select **Edit > Rename** from the Explorer menu.
 - Right-click on the unit Type, Site, Department, or Folder in the Unit list and select **Rename** from the pop-up menu. The Rename window opens.
3. Type a 1 to 32 character name. You can use embedded spaces but not leading or trailing spaces. (This name is local to the software database; the appliance database might contain a different name for this unit.)
4. Complete one of the following steps:
 - Click **OK** to save the new name.
 - Click **Cancel** to exit without saving changes.

For a unit Type, Site, Department, or Folder, you cannot use duplicate names, including the same name with different cases, with two exceptions: department names can be duplicated on different sites and folder names can be duplicated on different levels.

Managing the software database

Each computer running the software contains a local database that records the information that you enter about the units. If you have multiple computers, you can configure one computer and then save a copy of this database and load it into the other computers to avoid unnecessarily reconfiguring each computer. You can also export the database for use in another application.

Saving and loading a database

You can save a copy of the local database and then load it back to the same computer where it was created, or onto another computer running the software. The saved database is compressed into a single Zip file.

While the database is being saved or loaded, you cannot use or modify the database. You must close all other windows, including target device session windows and AMP windows. If other windows are open, a message prompts you to either continue and close all open windows or quit and cancel the database save process.

To save a database, complete the following steps:

1. Select **File > Database > Save** from the Explorer menu. The Database Save window opens.
2. Enter a file name and select a location to save the file.
3. Click **Save**. A progress bar is visible during the save. When finished, a message indicates that the save is complete and you are returned to the main window.

To load a database, complete the following steps:

1. Select **File > Database > Load** from the Explorer menu. The Database Load window opens.
2. Browse to select a database to load.
3. Click **Load**. A progress bar is visible during the load. When finished, a message indicates that the load is complete, and you are returned to the main window.

Exporting a database

You can export fields from the local database to a Comma Separated Value (CSV) file or Tab Separated Value (TSV) file. The following database fields are exported:

Appliance flag	Type	Name
Address	Custom Field 1	Custom Field 2
Custom Field 3	Description	Contact Name
Contact Phone	Comments	Browser URL

The first line of the exported file contains the column names for the field data. Each additional line contains the field data for a unit. The file contains a line for each unit defined in the local database.

To export a database, complete the following steps:

1. Select **File > Database > Export** from the Explorer menu. The Database Export window opens.
2. Type a file name and browse to the location to save the exported file.
3. Click **Export**. A progress bar is visible during the export. When finished, a message indicates that the export is complete, and you are returned to the main window.

Video Viewer

About the Video Viewer

When you connect to a target device using the Video Viewer, the desktop of the device is visible in a separate Video Viewer window. You can see both the local cursor and the target device cursor.

From this window, you can access all the normal functions of this target device as if you were sitting in front of it. You can also perform viewer-specific tasks such as sending macro commands to the target device.

You can open the Video Viewer for target devices on GCM4, GCM2, or RCM appliances.

If the target device you are attempting to access is currently being viewed by another user, you have several options depending on your access rights. If you are an administrator, you can share the session, preempt the session, or observe the session in stealth mode. For more information about access rights and session types, see "Video session types" on page 32 and "Managing local user accounts" on page 71.

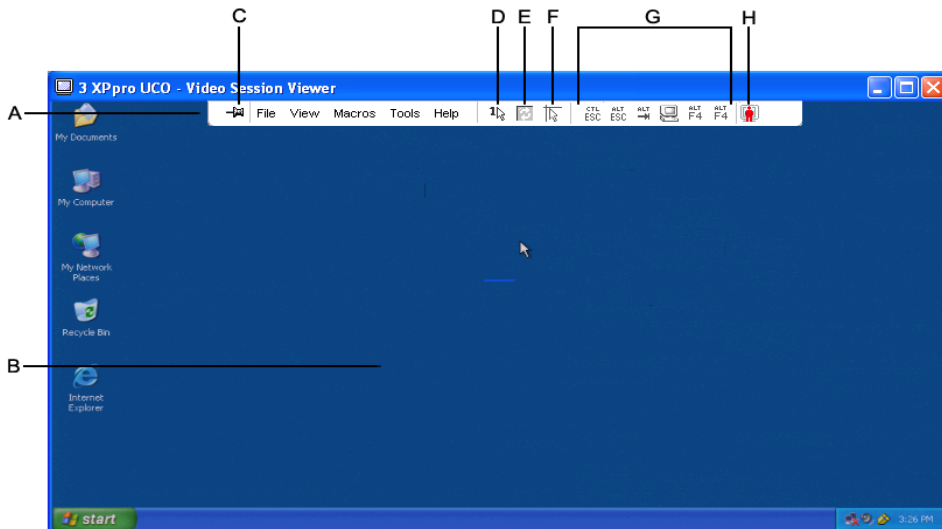


Figure 4.1: Video Viewer window

To access the Video Viewer, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
 - Double-click on the target device in the Unit list.
 - Select the target device, then click the **Connect Video** button.
 - Right-click on the target device. Select **Connect Video** from the pop-up menu.
 - Select the target device and press Enter.

If the target device is not being viewed by another user, the Video Viewer opens in a new window. If the target device is being accessed by another user, you might have the option to preempt the session, share the session, or observe the session in stealth mode, depending on your access rights. If this is the first unit access of the VCS session, a user name and password is required.

Important: A user name and password is not required for any subsequent access attempts during the same VCS session unless you clear the current cached credentials.

To close a Video Viewer session, complete one of the following steps:

- Select **File > Exit** from the Video Viewer menu.
- Click **X** to close the Video Viewer session.

Video session types

When using the Video Viewer with GCM2 and GCM4 appliances, you can choose which type of session you want to operate. In addition to operating a normal KVM session, administrators and users with certain access rights can also operate a session in an exclusive mode, share the session with one or more users, observe a session in stealth mode, or scan multiple target devices. The current type of session is indicated by an icon on the right side of the Video Viewer toolbar. Video session types are outlined in the table below.

Table 4.1: Video session types








Session types	Icons	Description
Active (normal)		You are conducting a normal KVM session that is not exclusive, but is not currently shared. An active session icon is visible.
Locked (normal)		Your administrator has configured the appliance to lock KVM and Virtual Media (VM) sessions together. You have a normal KVM session and have opened a VM session. Your KVM session cannot be shared or preempted, and it is not subject to inactivity time-out. It can be terminated by an administrator. For more information, see "Using virtual media" on page 49.
Exclusive		You have exclusive control over the target device. During this KVM session the connection to the target device cannot be shared, but it can be preempted or observed in stealth mode by an administrator.

Table 4.1: Video session types (Continued)

Session types	Icons	Description
Active sharing: (primary)		You are the first user to connect to the target device, and you have allowed other users to share the KVM session.
Active sharing: (secondary)		You can view and interact with the target device while sharing the KVM session with a primary user and, possibly, other secondary users.
Passive sharing		You can view the video output of the target device, but you are not allowed to have keyboard and mouse control over the target device.
Stealth		You can view the video output of the target device without the permission or knowledge of the primary user. You cannot have keyboard and mouse control over the target device. This session type is available for administrators only.
Scanning		You can monitor up to 16 target devices in thumbnail view. No status indicator icon is visible when in scan mode.

Using preemption

Preemption provides a means for users with sufficient privilege to take control of a target device from another user with lesser or equal privilege.

All users sharing the connection that is being preempted are warned, unless the target device is connected to an RCM appliance. If the primary user has the corresponding access rights, they can reject the preemption.

Table 4.2 outlines the preemption scenarios and detailed scenarios in which preemption requests can be rejected.

Table 4.2: Preemption scenarios

Current user	Preempted by	Preemption can be rejected
User	Local user	No
User	User administrator	No
User	Appliance administrator	No
Appliance administrator	Local user	Yes
Appliance administrator	Appliance administrator	Yes
User administrator	Local user	No
User administrator	User administrator	Yes
User administrator	Appliance administrator	No
Local user	User administrator	Yes

Table 4.2: Preemption scenarios

Current user	Preempted by	Preemption can be rejected
Local user	Appliance administrator	Yes

Preemption of a user by an administrator

If an administrator attempts to access a target device that is being accessed by a user, a message requests that the administrator wait while the user is informed that their session will be preempted. The user cannot reject the preemption request and will be disconnected. If the target device is attached to an RCM appliance, the user will not be warned. The time period given before disconnection is defined by the Video session preemption timeout setting in the **Global - Sessions** category. For information, see "Configuring Global Network settings" on page 56 and "Configuring Global Session settings" on page 58.

Preemption of a local user/administrator by an administrator

If an administrator attempts to access a target device that is being accessed by the local user or by another administrator with equal privileges, the currently connected user can accept or reject the preemption request. A message asks the connected local user or administrator whether they want to accept the preemption request. If the target device is attached to an RCM appliance, the user will not be given the option to accept or reject preemption. If the preemption request is rejected, a message is displayed informing the administrator that their request has been rejected and that they cannot access the target device.

In scenarios where a preemption request can be rejected, the Session Preemption Request window opens. Use this window to accept the preemption request by clicking the **Accept** button, or reject the preemption request by clicking the **Reject** button or by closing the window.

To preempt the current user, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
 - Double-click on the target device in the Unit list.
 - Select the target device, then click the **Connect Video** button.
 - Right-click on the target device. Select **Connect Video** from the pop-up menu.
 - Select the target device and press Enter.
3. When another user is viewing this target device, a message indicates that the target device is already involved in a KVM session.

If the appliance has connection sharing enabled, you are given the option to share the session. For information about connection sharing, see "Using digital share mode" on page 36. If your access rights (as compared with those of the primary user) allow it, you are prompted to either share or preempt the existing session. If the option is available, select **Preempt**.
4. Complete one of the following steps:

- Click **OK** or **Yes**. A preemption notification is sent to the primary user. Depending on your access rights, the primary user might be able to reject the preemption.
 - Click **No** to let the primary user retain the connection.
5. If the preemption completes, the Video Viewer of the target device session opens.

For more information about access levels, see "Managing local user accounts" on page 71.

You cannot preempt a local user who is in broadcast mode. See the corresponding *Installation and User's Guide* for the GCM4, GCM2, or RCM appliance for additional information.

Using exclusive mode

When operating a video session in exclusive mode, you cannot receive any share requests from other users. However, administrators can choose to preempt (or terminate) the session or monitor the session in stealth mode.

You cannot use exclusive mode when connecting to a target device on an RCM appliance.

To enable exclusive KVM sessions on an appliance, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
 - Double-click on a GCM2 or GCM4 appliance in the Unit list.
 - Select a GCM2 or GCM4 appliance from the Unit list, then click the **Manage Appliance** button.
 - Right-click on a GCM2 or GCM4 appliance in the Unit list. Select **Manage Appliance** from the pop-up menu.
 - Select a GCM2 or GCM4 appliance in the Unit list and press Enter.
3. Click the **Settings** tab in the AMP.
4. Select the **Global - Sessions** subcategory.
5. Select the **Enable Shared** Sessions check box in the **Connection Sharing** area.
6. Select **Exclusive Connections** in the **Connection Sharing** area.

Only the primary user of a shared connection or the only user of a non-shared session can access the Video Viewer in exclusive mode. To access the Video Viewer in exclusive mode, complete the following steps:

1. Open a KVM session to a target device.
2. Select **Tools > Exclusive Mode** from the Video Viewer toolbar.
3. If the KVM session is currently shared, only the primary user can designate the session as exclusive. A message warns the primary user that secondary sessions will be terminated if an exclusive session is invoked.

Complete one of the following steps:

- Select **Yes** to terminate the sessions of the secondary users.

- Select **No** to cancel the exclusive mode action.

Secondary users cannot share the exclusive KVM session. However, administrators or users with certain access rights can still terminate the session.

Using digital share mode

Multiple users can view and interact with a target device using digital share mode. When a session is shared, the secondary user can be an active user with keyboard and mouse control or a passive user that does not have keyboard and mouse control.

You cannot use digital share mode when connecting to a target device on an RCM appliance.

To configure an appliance to share KVM sessions, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
 - Double-click on a GCM2 or GCM4 appliance in the Unit list.
 - Select a GCM2 or GCM4 appliance from the Unit list, then click the **Manage Appliance** button.
 - Right-click on a GCM2 or GCM4 appliance in the Unit list. Select **Manage Appliance** from the pop-up menu.
 - Select a GCM2 or GCM4 appliance in the Unit list and press Enter.
3. Click the **Settings** tab in the AMP.
4. Select the **Global - Sessions** subcategory.
5. Select **Enable Share Mode** in the **Connection Sharing** area.
6. You can choose to select **Automatic Sharing**. This enables secondary users to automatically share a KVM session without first requesting permission from the primary user.

To share a digital connection, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
 - Double-click on the target device in the Unit list.
 - Select the target device, then click the **Connect Video** button.
 - Right-click on the target device. Select **Connect Video** from the pop-up menu.
 - Select the target device and press Enter.
3. When another user is viewing this target device, a message indicates that the target device is already involved in a KVM session.
If connection sharing is enabled on the appliance and your access rights (as compared with those of the primary user) allow it, you are prompted to either share or preempt the existing session. If the option is available, select **Share**.
4. Complete one of the following steps:

- Click **OK** or **Yes**. If Automatic Sharing is not enabled, a share request is sent to the primary user, who can accept the share request as either an active or passive (read-only) session, or reject the share request entirely.
- Click **No** to cancel the share request.

If the primary user accepts the share request, or if Automatic Sharing is enabled, a KVM session to the target device session opens, and the session type icon within the new Video Viewer window indicates if the session status is active or passive. If the request is rejected, a message indicates that the request was denied. Administrators have several options at this point. They can either try to connect again and preempt the session or connect in stealth mode, or they can terminate the session entirely from the AMP **Active Sessions** category; see "Managing user sessions" on page 75.

If you are not prompted to connect in share mode, either the appliance to which the target device is connected is not configured to allow digital share mode sessions or it is not a GCM2 or GCM4 appliance.

Using stealth mode

Administrators can connect to a target device in stealth mode, viewing the video output of a remote user undetected. When in stealth mode, the administrator does not have keyboard or mouse control over the target device.

You cannot use stealth mode when connecting to a target device on an RCM appliance.

To enable stealth KVM sessions on an appliance, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
 - Double-click on a GCM2 or GCM4 appliance in the Unit list.
 - Select a GCM2 or GCM4 appliance from the Unit list, then click the **Manage Appliance** button.
 - Right-click on a GCM2 or GCM4 appliance in the Unit list. Select **Manage Appliance** from the pop-up menu.
 - Select a GCM2 or GCM4 appliance in the Unit list and press Enter.
3. Click the **Settings** tab in the AMP.
4. Select the **Global - Sessions** subcategory.
5. Select **Stealth Connections** in the **Connection Sharing** area.

To monitor a target device in stealth mode, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
 - Double-click on the target device in the Unit list.
 - Select the target device, then click the **Connect Video** button.

- Right-click on the target device. Select **Connect Video** from the pop-up menu.
 - Select the target device and press Enter.
3. If another user is already viewing this target device, a message indicates that the target device is already involved in a KVM session.
If connection sharing and stealth connections are enabled on the appliance and your access rights (as compared with those of the primary user) allow it, you are prompted to either share or preempt the existing session. If the option is available, select **Stealth**.
 4. Complete one of the following steps:
 - Click **OK** or **Yes**.
 - Click **No** to cancel the stealth request.

A KVM session to the target device opens, and the administrator can view all video output of the target device while remaining undetected.

If **Stealth** is not listed as an option, one of the following conditions exist:

- the appliance to which the target device is connected is not configured to allow **Stealth Connections**
- you do not have the necessary access rights (**Stealth** permissions follow **Preemption** permissions)
- the appliance the target device is connected to is not a GCM2 or GCM4 appliance

Using scan mode

You can view multiple target devices using the scan mode Thumbnail Viewer. This view contains a series of thumbnail frames, each containing a small, scaled, non-interactive version of a target device screen image. The target device name and status indicator are visible below each thumbnail as follows:

- A green circle icon indicates that a target device is currently being scanned.
- A red X icon indicates that the last scan of the target device failed. The scan can have failed due to a credential or path failure (for example, the target device path on the appliance was not available). The tool tip for the icon indicates the reason for the failure.

You can set up a scan sequence of up to 16 target devices to monitor. The scan mode moves from one thumbnail image to the next, logging into a target device and displaying an updated target device image for a specified length of time (**View Time Per Server**), before logging out of that target device and moving on to the next thumbnail image. You can also specify a scan delay between thumbnails (**Time Between Servers**). During the delay, you can see the last thumbnail image for all target devices in the scan sequence, but you won't be logged into any target devices.

When you first open the Thumbnail Viewer, each frame is filled with a black background until a target device image is visible. An indicator icon at the bottom of each frame displays the target device status. The default thumbnail size is based on the number of target devices in the scan list.

Scan mode has a lower priority than an active connection. If a user is connected to a target device, that target device is skipped in the scan sequence, and scan mode proceeds to the next target device.

No login error messages are visible. After the interactive session is closed, the thumbnail is included in the scan sequence again.

You can disable a target device thumbnail from the scan sequence. The thumbnail image remains, but it is not updated until it is once again enabled.

Accessing scan mode

To access scan mode, complete the following steps:

1. Select the **Appliance, Devices, Sites,** or **Folders** button in the Explorer window.
2. Select two or more target devices in the Unit list by pressing the Shift or Control key. The **Scan Mode** button is visible.
3. Click the **Scan Mode** button. The Thumbnail Viewer window opens.

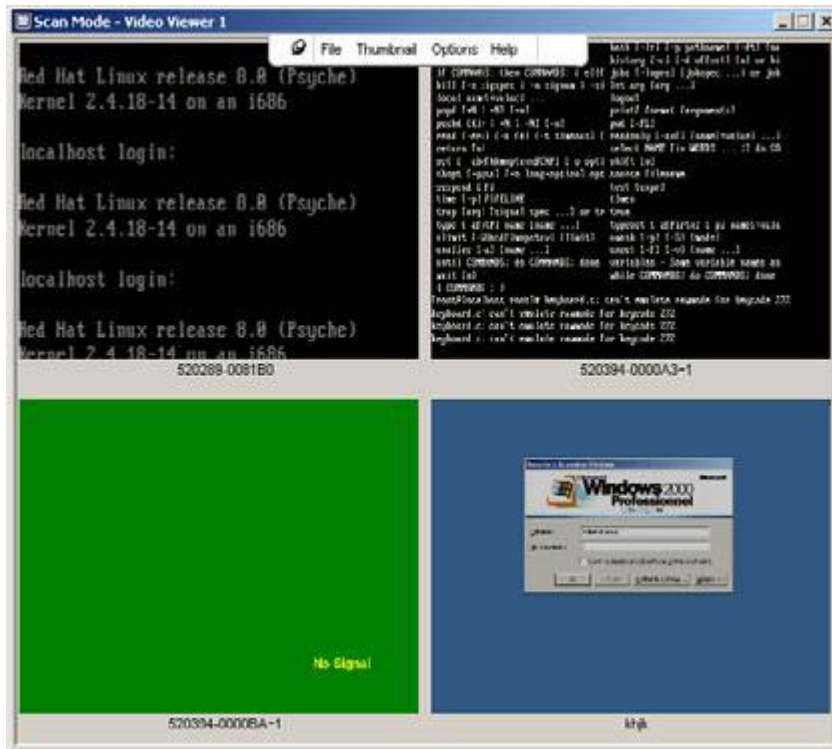


Figure 4.2: Video Viewer - Thumbnail Viewer

Setting scan options

To set scan preferences, complete the following steps:

1. Select **Options > Preferences** from the Thumbnail Viewer menu. The Preferences window opens.
2. In the **View Time Per Server** field, enter the time each thumbnail is active during the scan, in the range of 10 to 60 seconds.
3. In the **Time Between Servers** field, enter the time the scan stops between each target device, in the range of 5 to 60 seconds.
4. Click **OK**.

To change the thumbnail size, complete the following steps:

1. Select **Options > Thumbnail Size** from the Thumbnail Viewer menu.
2. Select a thumbnail size from the cascaded menu.

Managing the scan sequence

To pause or restart a scan sequence, complete the following steps:

1. Select **Options > Pause Scan** from the Thumbnail Viewer menu.
2. The scan sequence pauses at the current thumbnail if the Thumbnail Viewer has a scan in progress or restarts the scan if currently paused.

To disable a target device thumbnail in the scan sequence, complete one of the following steps:

- Select a target device thumbnail. Select **Thumbnail > “target device name” > Enable** from the Thumbnail Viewer menu. (The Enable menu item state can be toggled from checked (enabled) to unchecked (disabled) each time it is selected).
- Right-click on a target device thumbnail and select **Disable** from the pop-up menu. Updating of that thumbnail image stops until it is enabled again.

To enable a target device thumbnail in the scan sequence, complete one of the following steps:

- Select a target device thumbnail. Select **Thumbnail > “target device name” > Enable** from the Thumbnail Viewer menu. (The Enable menu item state can be toggled from checked (enabled) to unchecked (disabled) each time it is selected).
- Right-click on a target device thumbnail and select **Enable** from the pop-up menu. Updating of that thumbnail image resumes.

If a target device is currently being accessed by a user, the Enable Scan menu is disabled for that target device thumbnail.

Using the Thumbnail Viewer

To open a session to a target device from the Thumbnail Viewer, complete one of the following steps:

- Select a target device thumbnail. Select **Thumbnail > “target device name” > View Interactive Session** from the Thumbnail Viewer menu.

- Right-click on a target device thumbnail and select **View Interactive Session** from the Thumbnail Viewer menu.
- Double-click on a target device thumbnail.

That target device desktop opens in a Video Viewer window.

To set target device credentials from the Thumbnail Viewer, complete the following steps:

1. Complete one of the following steps:
 - Select a target device thumbnail. Select **Thumbnail > “target device name” > Credentials** from the Thumbnail Viewer menu.
 - Right-click on a target device thumbnail and select **Credentials** from the pop-up menu. The Login window opens.
 - Double-click the thumbnail window.
2. Enter a user name and password for the target device.

Window features

Figure 4.3 shows the Video Viewer window areas; descriptions follow in Table 4.3. The following figure shows one way of arranging buttons on the toolbar. You can customize the buttons and display position.

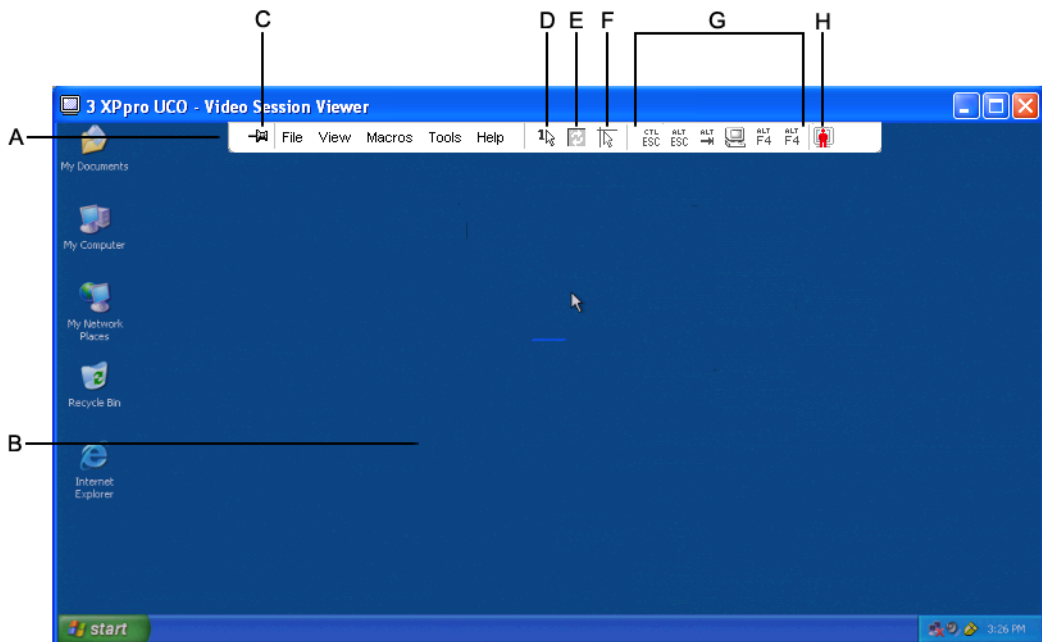


Figure 4.3: Video Viewer window

Table 4.3: Video Viewer window areas

Area	Description
A	Menu and toolbar: Provides access to many of the features in the Video Viewer.
B	Accessed target device desktop: Interact with the target device through this window.
C	Thumbtack button: Determines toolbar position. When locked, the toolbar remains fixed on screen. When unlocked, the toolbar is visible only when the mouse hovers over the top of the window.
D	Single Cursor Mode button: Hides the local cursor and displays only the target device cursor.
E	Refresh Video button: Regenerates the digitized video image of the target device desktop.
F	Align Local Cursor button: Re-establishes true tracking of the local cursor to the target device cursor.
G	User-selected buttons: You can choose to display additional buttons and macro commands on the toolbar.
H	Connection Status indicator: Icons indicate the status of the KVM session. See Table 4.1 for more information.

Adjusting the view

Using menus or buttons in the Video Viewer window, you can:

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable full screen mode.
- Enable automatic or manual scaling of the session image. With automatic scaling, the desktop window remains fixed and the target device image is scaled to fit the window. With manual scaling, a drop-down menu of supported image scaling resolutions is visible.

To align the mouse cursors, click the **Align Local Cursor** button in the Video Viewer toolbar. The local cursor aligns with the cursor on the target device.

If cursors drift out of alignment, turn off mouse acceleration on the target device.

To refresh the screen, complete one of the following steps:

- Click the **Refresh Image** button in the Video Viewer toolbar.
- Select **View > Refresh** from the Video Viewer menu. The digitized video image is regenerated.

To enable or disable full screen mode, complete the following steps:

1. Complete one of the following steps:

- If you are using Windows, click the **Maximize** button in the upper right corner of the window.
- Select **View > Full Screen** from the Video Viewer menu.

The desktop window is hidden and only the accessed target device desktop is visible. The screen is resized up to a maximum of 1024 x 768. If the desktop has a higher resolution, then a black background surrounds the full screen image. The floating toolbar is visible.

2. Complete one of the following steps:

- To disable full screen mode, click the **Full Screen Mode** button on the floating toolbar to return to the desktop window.
- Select **View > Full Screen** from the Video Viewer menu.

To enable automatic or manual scaling, complete one of the following steps:

- To enable automatic scaling, select **View > Scaling > Auto Scale** from the Video Viewer menu. The target device image is scaled automatically.
- To enable manual scaling, select **View > Scaling** from the Video Viewer menu, then select the dimension to scale the window.

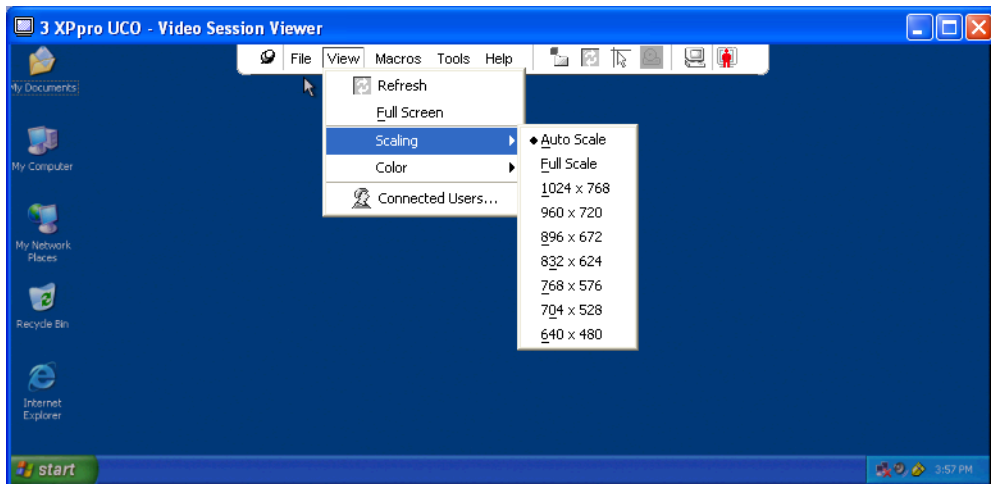


Figure 4.4: Viewer manual scale

Additional video adjustment

Generally, the Video Viewer automatic adjustment features optimizes the video for the best possible view. However, you can fine tune the video with the help of technical support. Video adjustment is a global setting and applies to each target device you access.

NOTE: The following video adjustments should be made only on the advice and with the help of technical support.

To manually adjust the video quality of the window, complete the following steps:

1. Select **Tools > Manual Video Adjust** from the Video Viewer menu. The Manual Video Adjust window opens. See Figure 4.5; descriptions follow the figure in Table 4.4.
2. Click the icon corresponding to the feature you want to adjust.
3. Move the slider bar and then fine tune the setting by clicking the **Min (-)** or **Max (+)** buttons to adjust the parameter for each icon pressed. The adjustments take effect immediately in the Video Viewer window.
4. When finished, click **Close** to exit the Manual Video Adjust window.

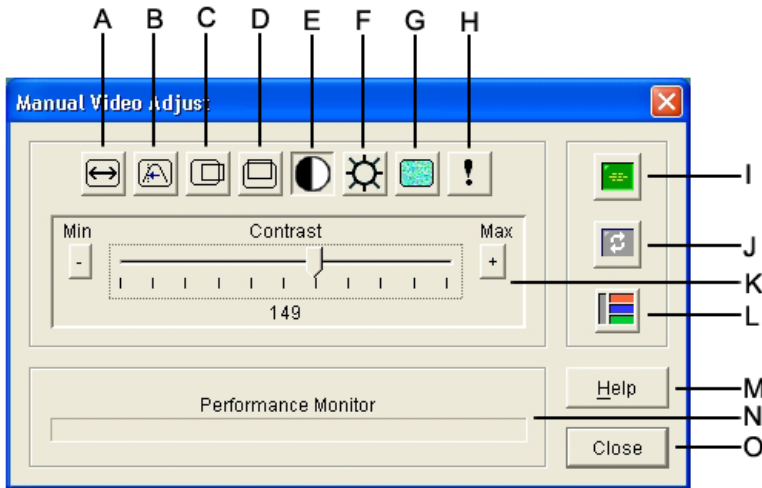


Figure 4.5: Manual Video Adjust window

Table 4.4: Manual Video Adjust window areas

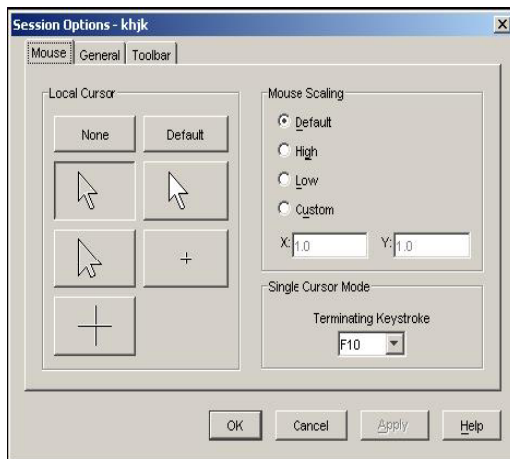
Area	Description	Area	Description
A	Image capture width	I	Automatic video adjustment
B	Pixel sampling fine adjust	J	Refresh image
C	Image capture horizontal position	K	Adjustment bar
D	Image capture vertical position	L	Video test pattern
E	Contrast	M	Help button

Table 4.4: Manual Video Adjust window areas (Continued)

Area	Description	Area	Description
F	Brightness	N	Performance monitor
G	Noise threshold	O	Close button
H	Priority threshold		

Adjusting mouse options

The Video Viewer mouse options affect cursor type, scaling, alignment, and resetting. Mouse settings are device-specific; that is, they can be set differently for each target device.

**Figure 4.6: Viewer Mouse Session Options window**

Cursor type

The Video Viewer offers five display choices for the local mouse cursor. You can also select no cursor or the default cursor.

To change the mouse cursor setting, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.
2. Click the **Mouse** tab.
3. Select a mouse cursor type in the **Local Cursor** area.
4. Click **OK**.

Scaling

You can select any of three preconfigured mouse scaling options or set custom scaling. The preconfigured settings are: Default (1:1), High (2:1) or Low (1:2), as follows:

- In a 1:1 scaling ratio, every mouse movement on the desktop window sends an equivalent mouse movement to the target device.
- In a 2:1 scaling ratio, the same mouse movement sends a 2X mouse movement.
- In a 1:2 scaling ratio, the value is 1/2X.

To set mouse scaling, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.
2. Click the **Mouse** tab.
3. To use one of the preconfigured settings, check the corresponding radio button in the **Mouse Scaling** area.
4. To set custom scaling, click the **Custom** radio button. The **X** and **Y** fields become enabled. Type a mouse scaling value in the **X** and **Y** fields. For every mouse input, the mouse movements are multiplied by the corresponding X and Y scaling factors. Valid input ranges are 0.25 to 3.00.

Single cursor mode

When using single cursor mode, the Video Viewer title bar will show the keystroke that should be pressed to exit this mode.

To change the terminating keystroke for single cursor mode, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.
2. Click the **Mouse** tab.
3. Select the desired terminating keystroke from the drop down list in the **Single Cursor Mode** area.
4. Click **OK**.

Adjusting general options

The General tab in the Session Options window allows you to control Keyboard Pass-through in non-full screen mode, Menu Activation Keystroke, and Background Refresh.

To adjust general options, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.
2. Click the **General** tab.

3. Select the **Keyboard Pass-through** check box to enable Keyboard Pass-through, or clear the check box to disable Keyboard Pass-through. The **Keyboard Pass-through** check box is not selected by default. When **Keyboard Pass-through** is selected, all keystrokes except for Control-Alt-Delete are sent directly to the target device instead of the client computer.
4. Select a keystroke to use to activate the Video Viewer toolbar from the list in the **Menu Activation Keystroke** area.
5. If you want the Video Viewer to receive a constant stream of video data from the target device, select the **Background Refresh** check box. If you want the Video Viewer to receive data only when a change has occurred on the target device, clear the **Background Refresh** check box.

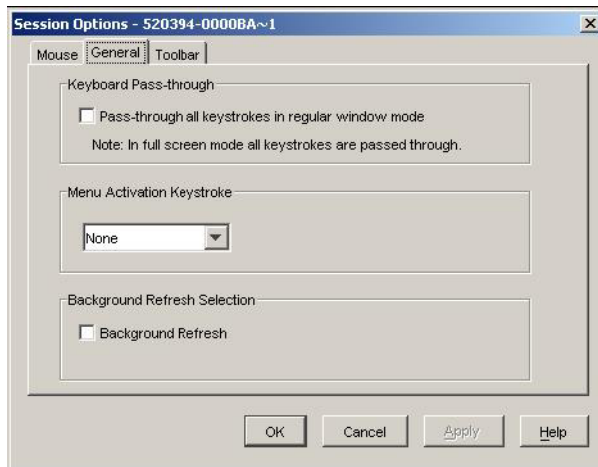


Figure 4.7: Session Options - General tab

Adjusting the Video Viewer toolbar

You may add up to 10 buttons to the toolbar. Use these buttons to provide easy access to defined function and keyboard macros. By default, the **Align Local Cursor**, **Refresh Image**, and **Single Cursor Mode** buttons are visible on the toolbar.

To add buttons to the toolbar, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer toolbar. The Session Options window opens.
2. Click the **Toolbar** tab.
3. Select the items you want to add to the Video Viewer toolbar.
4. Complete one of the following steps:
 - Click **OK** to accept the changes and return to the Video Viewer main window.
 - Click **X** or **Cancel** to return to Video Viewer main window without making changes.

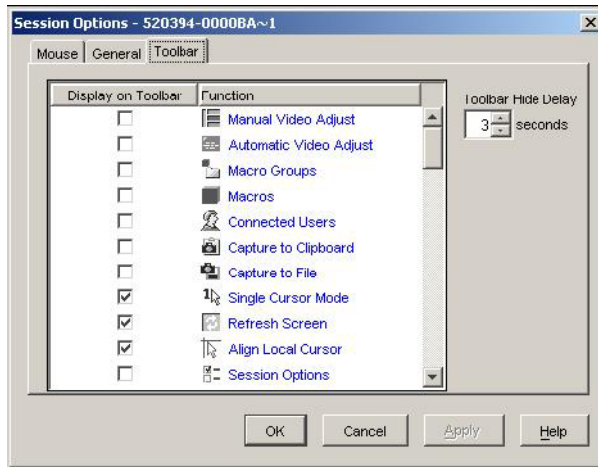


Figure 4.8: Session Options Window - Toolbar tab

Setting the Toolbar Hide Delay time

The toolbar disappears when you remove the mouse cursor unless the **Thumbtack** button has been clicked. You can change the interval between the removal of the mouse cursor and the disappearance of the toolbar by adjusting the Toolbar Hide Delay time.

To change the Toolbar Hide Delay time, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer toolbar. The Session Options window opens.
2. Click the **Toolbar** tab.
3. Complete one of the following steps:
 - In the **Toolbar Hide Delay** field, type the number of seconds you want the toolbar to be visible after the mouse cursor is removed.
 - Using the **Up** and **Down** buttons, click to increase or decrease the number of seconds you want the toolbar to be visible after the mouse cursor is removed.
4. Complete one of the following steps:
 - Click **OK** to accept the changes and return to the Video Viewer.
 - Click **X** or **Cancel** to return to Video Viewer without making changes.

Using macros

Use the Video Viewer macro function to:

- Send a macro from a predefined macro group. Macro groups for Windows and Sun are already defined. Selecting from the available categories and keystrokes saves time and eliminates the risk of typographical errors.
- Change the macro group that is listed by default. This causes the macros in the specified group to be available in the Video Viewer Macros menu.

Macro group selection are device-specific; that is, it can be set differently for each target device.

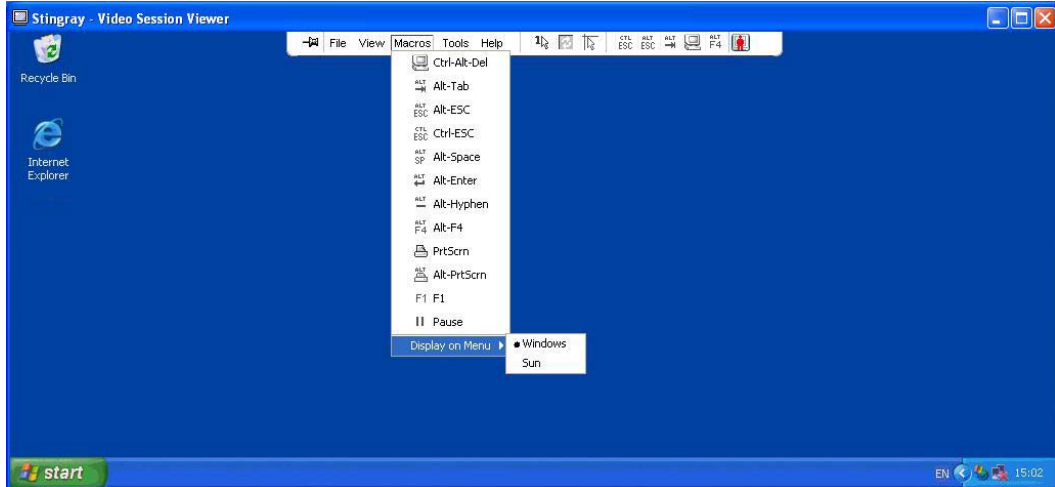


Figure 4.9: Video Viewer Macros menu expanded

Sending macros

To send a macro, select **Macros** from the Video Viewer menu and choose a macro from the list.

Selecting the macro group to display

You can select the macro group applicable to the operating system of the target device.

To display macro groups in the Macros menu, complete the following steps:

1. Select **Macros > Display on Menu** from the Video Viewer menu.
2. Select the macro group you want to list on the Video Viewer Macro menu.
3. The macro group you select will be displayed in the Video Viewer Macros menu the next time you open the Macros menu.

Using virtual media

With virtual media you can map a physical drive on the local client machine as a virtual drive on a target device. You can also add and map an ISO or diskette image file on the local client as a virtual drive on the target device.

You can have one CD drive and one mass storage device mapped concurrently.

- A CD drive, DVD drive, or ISO disk image file is mapped as a virtual CD drive.
- A diskette drive, diskette image file, USB memory device, or other media type is mapped as a virtual mass storage device.

Requirements

Virtual media is supported on GCM2 and GCM4 appliances.

The target device must be connected to the GCM2 or GCM4 appliance with a VCO cable.

The target device must support the types of USB2-compatible media that you virtually map. In other words, if the target device does not support a portable USB memory device, you cannot map the local device as a virtual media drive on the target device.

You (or the user group to which you belong) must have permission to establish virtual media sessions or reserved virtual media sessions to the target device.

A GCM2 will support up to three concurrent virtual media sessions (one local and two remote). A GCM4 will support up to four concurrent virtual media sessions (including local and remote). Only one virtual media session can be active to a target device at one time.

Sharing and preemption considerations

The KVM and virtual media sessions are separate; therefore, there are many options for sharing, reserving or preempting sessions.

For example, the KVM and virtual media sessions can be locked together. In this mode, when a KVM session is disconnected, so is the associated virtual media session. If the sessions are not locked together, the KVM session can be closed but the virtual media session remains active.

After a target device has an active virtual media session without an associated active KVM session, either the original user (User A) can reconnect or a different user (User B) can connect to that channel. You can set an option in the Virtual Media window (Reserved) that lets only User A access the associated target device with a KVM session.

If User B has access to that KVM session (the Reserved option is not enabled), User B could control the media that is being used in the virtual media session. In some environments, this might not be desirable.

By using the Reserved option in a tiered environment, only User A can access the lower appliance and the KVM channel between the upper appliance and lower appliance is reserved for User A.

Preemption levels offer additional flexibility of combinations.

Virtual Media window

Use the Virtual Media window to manage the mapping and unmapping of virtual media. The window displays all the physical drives on the client computer that can be mapped as virtual drives (non-USB hard drives are not available for mapping). You can also add ISO and diskette image files and then map them using the Virtual Media window.

After a target device is mapped, the Details View of the Virtual Media window displays information about the amount of data transferred and the time elapsed since the target device was mapped.

You can specify that the virtual media session is reserved. When a session is reserved, and the associated KVM session is closed, another user cannot open a KVM session to that target device. If a session is not reserved, another KVM session can be opened. Reserving the session can also be used to make sure that a critical update is not interrupted by another user attempting to preempt the KVM session or by inactivity time-outs on the KVM session.

You can also reset the VCO cable from the Virtual Media window. This action resets every form of USB media on the target device, and should therefore be used with caution, and only when the target device is not responding.



Figure 4.10: Virtual Media window

Virtual media session settings

Virtual media session settings include locking, mapped drives access mode, and encryption level. See "Configuring Global Virtual Media settings" on page 60 to specify these settings for the supported GCM2 or GCM4 appliances.

Table 4.5 lists and describes the virtual media session settings.

Table 4.5: Virtual media session settings

Setting	Description
Locked	The Locked setting specifies whether a virtual media session is locked to the KVM session on the target device. When locking is enabled (which is the default) and the KVM session is closed, the virtual media session also closes. When locking is disabled and the KVM session is closed, the virtual media session remains active.

Table 4.5: Virtual media session settings

Setting	Description
Mapped drives access mode	You can set the access mode for mapped drives to read-only. When the access mode is read-only, you cannot write data to the mapped drive on the client computer. When the access mode is not set as read-only, you can read and write data from or to the mapped drive. If the mapped drive is read-only by design (for example, certain CD drives, DVD drives, or ISO images), the configured read-write access mode is ignored. Setting the read-only mode can be helpful when a read-write drive such as a mass storage device or a USB removable media is mapped, and you want to prevent the user from writing data to it.
Encryption level	You can configure up to three encryption levels for virtual media sessions. Any combination is valid. The choices are: DES, 3DES and 128-bit SSL. The highest level selected is used. The default is no encryption (no encryption levels selected).

Opening a virtual media session

The following procedures are valid only on GCM2 or GCM4 appliances that are connected with VCO cables.

To open a virtual media session, complete the following steps:

1. Open a Video Viewer session to the target device.
2. From the Video Viewer toolbar, select **Tools > Virtual Media**. The Virtual Media window opens.
3. If you want to make this a reserved session, on the Virtual Media window click **Details**, then select the **Reserved** check box.

Mapping virtual media drives

To map a virtual media drives, complete the following steps:

1. Open a virtual media session from the Video Viewer toolbar by selecting **Tools > Virtual Media**.
2. To map a physical drive as a virtual media drive, complete the following steps:
 - a. In the Virtual Media window, select the **Mapped** check box next to the drive or drives you want to map.
 - b. If you want to limit the mapped drive to read-only access, select the **Read Only** check box next to the drive prior to mapping the drive. If the virtual media session settings were previously configured so that all mapped drives must be read-only, this check box is already enabled and cannot be changed.

You might want to select the **Read Only** check box if the session settings enabled read and write access, but you want to limit the access of a particular drive to read-only.

3. To add and map an ISO or diskette image as a virtual media drive, complete the following steps:
 - a. In the Virtual Media window, click **Add Image**.
 - b. The Common File Chooser window opens, with the directory containing disk image files (ending in .iso or .img) visible. Select an ISO or diskette image file and click **Open**.
 - c. The file header is checked to make sure it is correct. If it is, the Common File Chooser window closes and the chosen image file opens in the Virtual Media window, where it can be mapped by selecting the **Mapped** check box.
 - d. Repeat steps a through c for any additional ISO or diskette images you want to add. You can add any number of image files (up to the limits imposed by memory), but you can only have one virtual CD or virtual mass storage mapped concurrently.

If you attempt to map too many drives (one CD and one mass storage device) or too many drives of a particular type (more than one CD or mass storage device), a message is displayed. If you still want to map a new drive, you must first unmap an existing mapped drive, then map the new drive.

After a physical drive or image is mapped, it can be used on the target device.

To unmap a virtual media drive, eject the mapped drive from the target device. Clear the **Mapped** check box.

Displaying virtual media drive details

To display virtual media drive details, complete the following steps:

1. In the Virtual Media window, click **Details**. The window expands to display the Details table. Each row indicates:
 - **Target Drive** - Name used for the mapped drive, such as Virtual CD 1 or Virtual CD 2.
 - **Mapped to** - Identical to Drive information that is listed in the Client View Drive column.
 - **Read Bytes and Write Bytes** - Amount of data transferred since the mapping.
 - **Duration** - Elapsed time since the drive was mapped.
2. To close the Details view, click **Details** again.

Resetting USB media devices

To reset all USB media devices on the target device, complete the following steps:

Important: The USB reset feature resets every USB device on the target device, including the mouse and keyboard. It should only be used when the target device is not responding.

1. In the Virtual Media window, click **Details**.
2. The Details View is visible. Click **USB Reset**.
3. A warning message indicates the possible effects of the reset. Click **Yes** to confirm the reset or **No** to cancel the reset.
4. To close the Details view, click **Details** again.

Closing a virtual media session

To close the Virtual Media window, complete the following steps:

1. Click **Exit** or **X** to close the window.
2. If you have any mapped drives, a message indicates that the drives will be unmapped. Click **Yes** to confirm and close the window or click **No** to cancel the close.

If you attempt to disconnect an active KVM session that has an associated locked virtual media session, a confirmation message indicates that any virtual media mappings will be lost.

See "Sharing and preemption considerations" on page 50 for information about other factors that can affect virtual media session closings.

Appliance Management Panel

About the Appliance Management Panel

After you add an appliance in the software, you can view and configure unit parameters, view and control active video sessions, and execute a variety of control functions. These operations are accomplished through the Appliance Management Panel (AMP).

The AMP has three tabs: **Settings**, **Status**, and **Tools**, as follows:

- The **Settings** tab contains categories in the left portion of the tab. Categories with a preceding plus sign (+) have subcategories. The content of the remaining area of the panel changes according to the category or subcategory that is selected.

Settings categories include general appliance information, user accounts, SNMP, and other unit configuration information.

- The **Status** tab displays information about currently active Video Viewer and virtual media sessions. As an administrator, you can disconnect sessions from this tab.
- The **Tools** tab can be used to execute control functions on the appliance such as rebooting, saving and restoring databases, and upgrading firmware.

Some operations that you perform through the AMP trigger a message indicating that a reboot is required in order for the change to take effect. In such cases, you can choose to reboot immediately or wait to reboot later.

You can use the AMP to manage GCM4, GCM2, or RCM appliances. Some features are only available for GCM4 and GCM2 appliances.

NOTE: References to the local user refer to an OSCAR user connected to the appliance at the local user port.

For more information about the appliance and its operations, see the corresponding *Installation and User's Guide*.

To access the AMP, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps
 - Double-click on an appliance in the Unit list.
 - Select an appliance from the Unit list, then click the **Manage Appliance** button.

- Right-click on a GCM4, GCM2, or RCM appliance in the Unit list. Select **Manage Appliance** from the pop-up menu.
 - Select an appliance in the Unit list and press Enter.
3. If this is the first time a unit has been accessed since the VCS was started, a user name and password prompt opens.
 - a. Type in your user name and password. [If this is the first appliance access since initialization or reinitialization, the default user name is Admin (case sensitive) with no password.]
 - b. Click **OK** to log in, or click **Cancel** to exit without logging in.

The AMP opens.

To exit the AMP, complete one of the following steps:

- Click **OK** to save any changes and exit the AMP.
- Click **Cancel** to exit the AMP without saving any changes.

Managing Global settings

The Global category lists the appliance product type, its serial number, and the language the appliance is currently using. Use the Global category to control many of the options for target devices running the software.

Configuring Global Network settings

The **Global - Network** subcategory specifies the IP address, subnet mask and gateway (all read-only if DHCP is enabled), MAC address (read-only), LAN interface speed, and DHCP state (enabled or disabled) of the appliance. The appliance name is also listed. The name is read-only in this sub-category; you can change the appliance name in the SNMP category.

To change global network values, complete the following steps:

1. Click the **Settings** tab in the AMP.

2. Select the **Global - Network** subcategory.

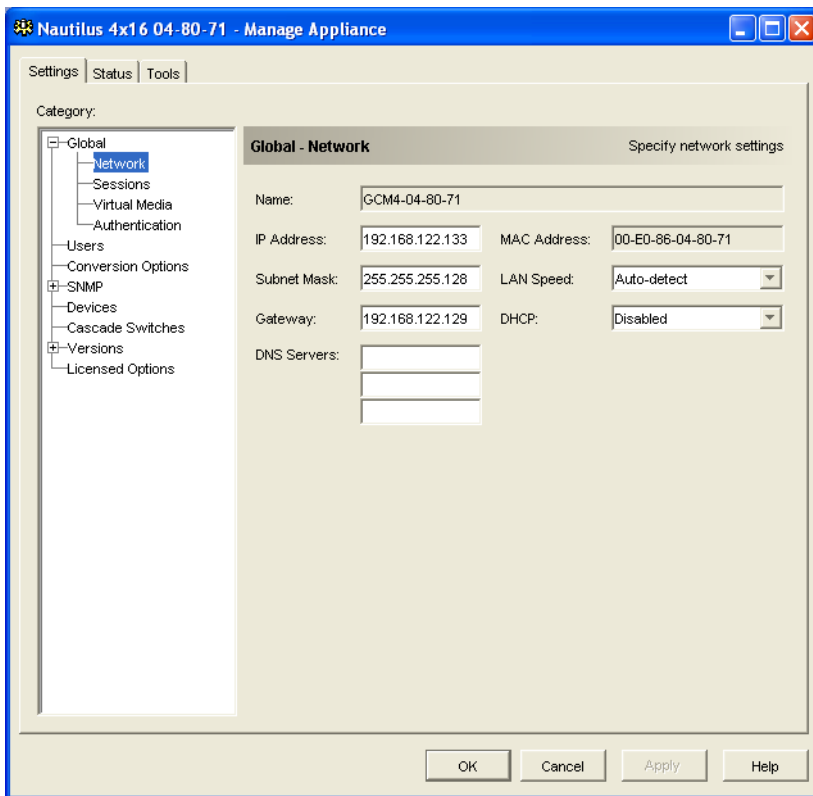


Figure 5.1: AMP Global Network settings

3. In the **IP Address** field, enter the appliance address in IP dot notation. The value cannot be a loopback address or all zeros. This field can be modified only if DHCP is disabled.
4. In the **Subnet Mask** field, enter the appliance subnet mask in IP address dot notation. The value cannot be a loopback address or all zeros. This field can be modified only if DHCP is disabled.
5. In the **Gateway** field, enter the appliance gateway address in IP address dot notation. The value cannot be a loopback address. If there is no gateway address, enter 0.0.0.0. This field can only be modified if DHCP is disabled.
6. In the **LAN Speed** field, select a value from the pull-down menu.
7. Complete one of the following steps:
 - In the **DHCP** field, select **Disabled** or **Enabled** from the pull-down menu. When enabled, the appliance gets its IP address dynamically at boot time from a DHCP server so the **IP Address**, **Subnet Mask**, and **Gateway** fields are disabled.

- If BootP is supported (as for the RCM appliances), it is visible instead of DHCP. Select **Disabled** or **Enabled** from the pull-down menu.
8. If LDAP is licensed for the appliance, you can enter the IP address for up to three DNS target devices. If you are using an RCM appliance, you can only enable DNS target devices through the serial interface of the appliance. See the corresponding GCM4, GCM2, or RCM *Installation and User's Guide* for more information.
 9. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

Configuring Global Session settings

Use the **Global - Sessions** subcategory to designate video session settings for the appliance, including Inactivity Time-out, Preemption Time-out, Encryption Levels, and Connection Sharing settings.

To change global session values, complete the following steps:

1. Click the **Settings** tab in the AMP.

2. Select the **Global - Sessions** subcategory.

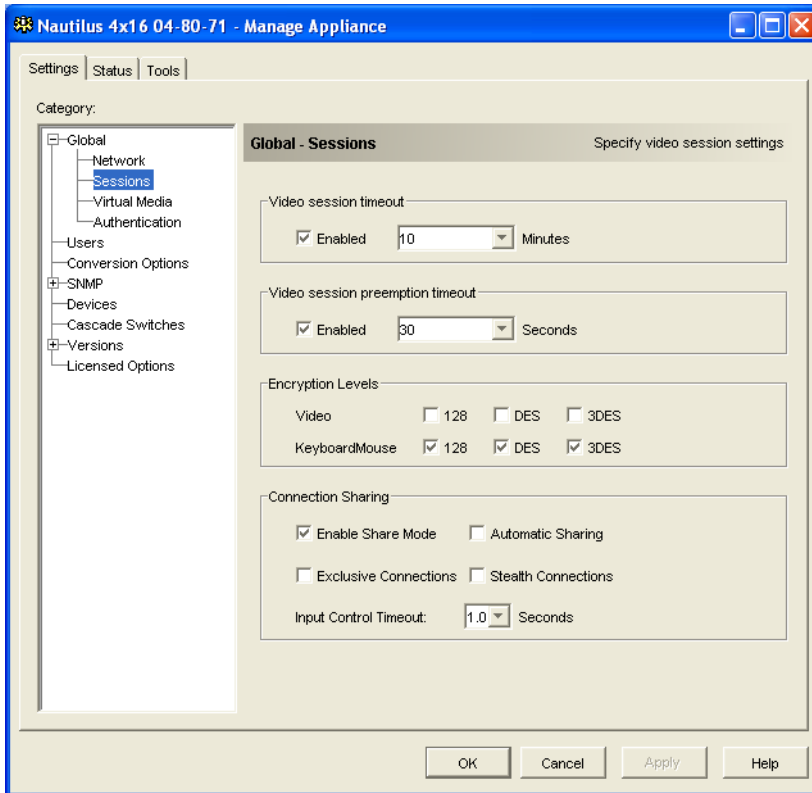


Figure 5.2: AMP Global Sessions settings

3. In the **Video Session Timeout** area, select or clear the **Enabled** check box. If you enable the video session time-out, specify the time-out value in the **Minutes** list. This value indicates the number of minutes the appliance will wait to close an inactive video session. You can select a value from the list or enter a value in the range of 1 to 60 minutes.
4. In the **Video session preemption timeout** area, select or clear the **Enabled** check box. If you enable the preemption warning, specify the time-out value in the **Seconds** list. This value indicates the number of seconds the appliance will wait for a user to respond to a preemption warning. You can select a value from the list or enter a value in the range of 5 to 120 seconds.
5. In the **Encryption Levels** area, select one or more levels of encryption to encode keyboard and mouse data sent over a video session to the appliance. The highest level enabled is used. Repeat this step for the Video encryption level.
Video encryption is optional, but at least one Keyboard/Mouse encryption level must be selected.

6. In the **Connection Sharing** area, select sharing options as needed. If you select **Enable Share Mode**, users can share KVM sessions for the same target device. If you select **Automatic Sharing**, secondary users can share KVM sessions without first requesting permission from the primary user. If you select **Exclusive Connections**, primary users can designate a KVM session as exclusive (exclusive sessions cannot be shared). Selecting **Stealth Connections** enables administrators to monitor a target device undetected. You can also specify in the **Input Control Timeout** field the number of seconds the appliance will wait for activity before transferring keyboard and mouse control from the primary user to the secondary user.
7. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

Configuring Global Virtual Media settings

Use the **Global - Virtual Media** subcategory to specify the settings for Virtual Media sessions.

To change global session values, complete the following steps:

1. Click the **Settings** tab in the AMP.

2. Select the **Global - Virtual Media** subcategory.

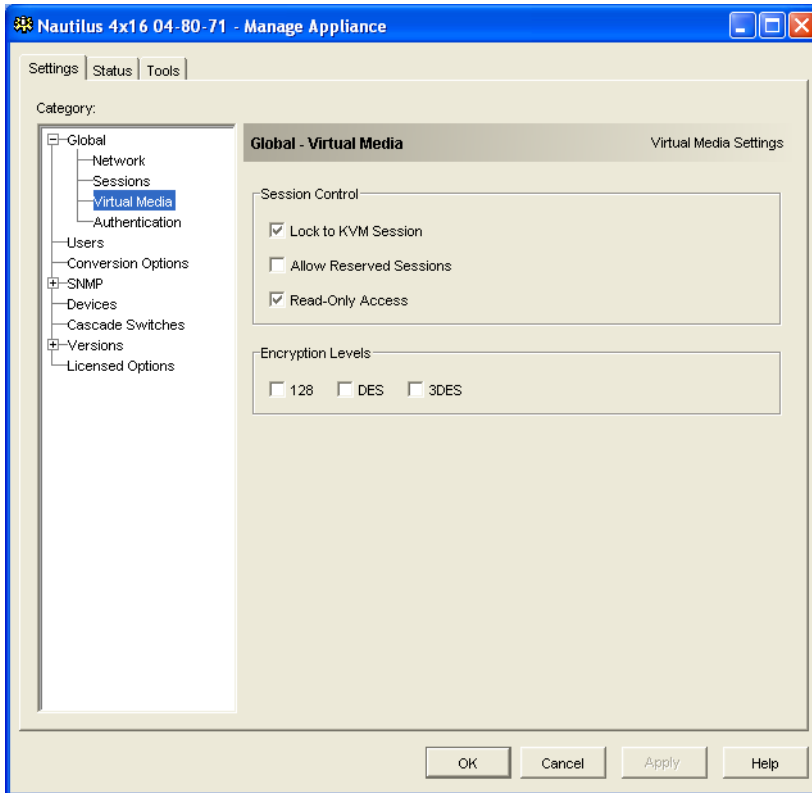


Figure 5.3: AMP Global Virtual Media settings

3. In the **Session Control** area, select or clear the check boxes as needed. If you clear **Lock to KVM Session**, virtual media sessions can remain after the Video Session that starts it closes. If you select **Allow Reserved Sessions**, then the owner of the virtual media session can choose to prevent other users from establishing a KVM session to the same target device. Also when the virtual media session is reserved, the corresponding KVM session is not subject to inactivity time-outs and cannot be preempted. If you select **Read-Only Access**, write access to Virtual Media sessions is prevented.
4. In the **Encryption Levels** area, select zero or more levels of encryption to encode Virtual Media data sent over a video session to the appliance. The highest level enabled is used.
5. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

Configuring Global Authentication settings

There are two types of user accounts: internal and external. Internal (local) user accounts reside within the appliance itself, while external user accounts are stored on an external authentication server. The **Users** category provides methods for managing internal user accounts.

The **Global - Authentication** category specifies the type and order of any authentication methods used. If a method fails or is unavailable, the software uses the next enabled authentication method.

Local authentication is always available as the primary or backup authentication method, and cannot be disabled.

See "Licensing appliance options" on page 86 for information on enabling LDAP.

To change authentication settings, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Global - Authentication** subcategory.

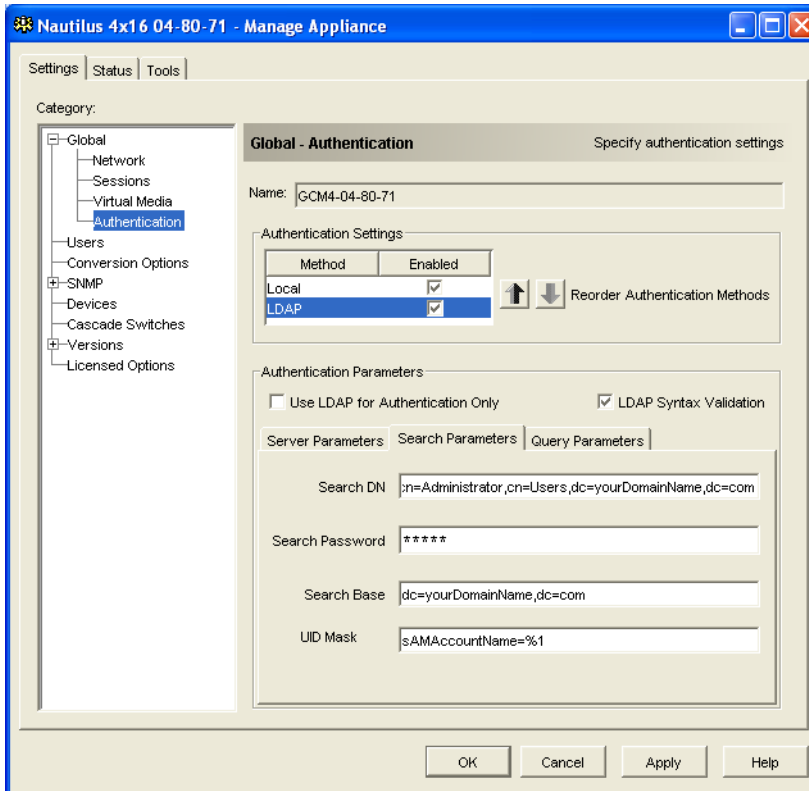


Figure 5.4: AMP Global Authentication settings

3. To specify an authentication method, select the check box next to the method in the **Authentication Settings** area.
4. When you specify more than one authentication method, you can control the order in which they are tried by changing the order in the list. Select a method and then click one of the **Reorder Authentication Methods** buttons. Click the **up** button to shift the selected method up; click the **down** button to shift the selected method down.
5. You can choose to use LDAP for authentication only, not for authorization, when using the local user database for authorization. Select or clear the check box next to **Use LDAP for Authentication Only** as needed.
6. You can choose to validate the values entered by the user for LDAP-related fields in either the **Search Parameters** or **Query Parameters** tab. Select or clear the check box next to **LDAP Syntax Validation** as needed.
7. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

For example, if LDAP is enabled as the first authentication method, followed by Local, the following process occurs:

- The appliance attempts LDAP authentication by querying its Management Information Base (MIB) to obtain the LDAP parameters specified in the **LDAP Parameters** field, which are then sent to and verified on the LDAP directory service.
- If LDAP authentication fails, the appliance attempts local authentication.
- If local authentication also fails, an error code is returned for the highest priority authentication method attempted, which in this case is LDAP.

Configuring LDAP

LDAP is a vendor-independent protocol standard used for accessing, querying, and updating a directory using TCP/IP. Based on the X.500 Directory Services model, LDAP is a global directory structure that supports strong security features including authentication, privacy, and integrity.

LDAP authentication configuration parameters

If individual user accounts are stored on an LDAP-enabled directory service, such as Active Directory, you can use the directory service to authenticate users.

The default values given for the LDAP search and query parameters are defined for use with Active Directory.

The settings made in the **Global - Authentication** subcategory of the AMP **Settings** tab let you configure your authentication configuration parameters. The software sends the VCS user name, password, and other information to the appliance, which then determines whether the VCS user has permission to view or change configuration parameters for the appliance in the AMP.

Important: Unless otherwise specified, the LDAP default values should be used unless Active Directory has been reconfigured. Modifying the default values may cause LDAP authentication server communication errors.

LDAP server parameters

Clicking the **Server Parameters** tab displays the parameters that define LDAP server connection information.

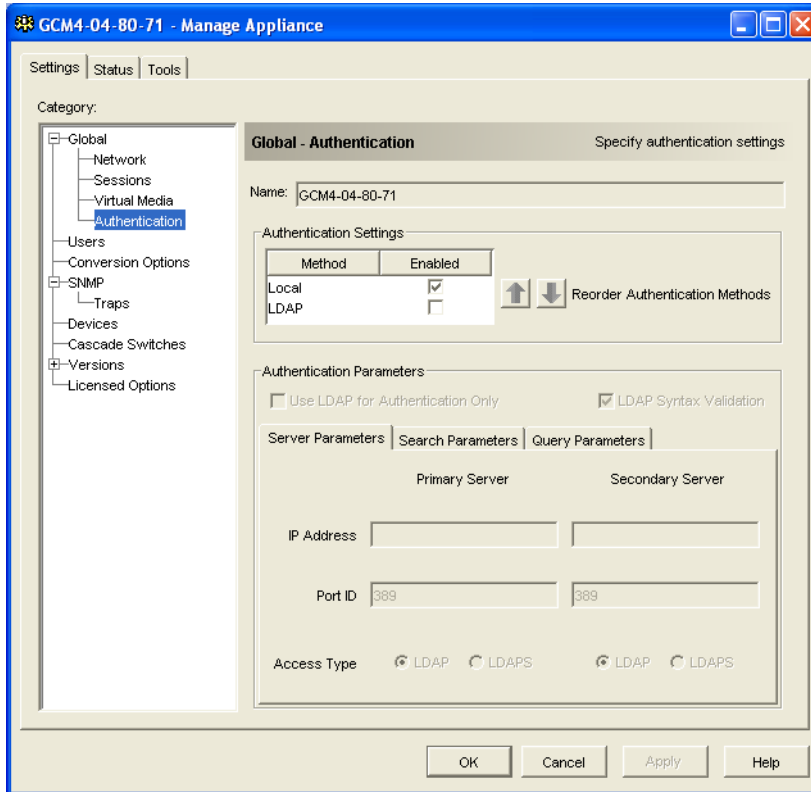


Figure 5.5: Server Parameters tab

The **IP Address** fields specify the host names or IP addresses of the primary and secondary LDAP servers. These values cannot be loopback addresses or all zeros.

The second LDAP server is optional.

The **Port ID** fields specify the User Datagram Protocol (UDP) port numbers that are used to communicate with the LDAP servers. The default value is 389 for non-secure LDAP and 636 for secure LDAP. The default Port ID is automatically entered by the software when an access type is specified.

The **Access Type** radio buttons specify how a query is sent to each LDAP target device. Click **LDAP** to send a query as clear text (non-secure LDAP) or **LDAPS** to send a query using a Secure Socket Layer (SSL) (secure LDAP).

NOTE: When using **LDAP**, all user names, passwords, etc. sent between an appliance and LDAP server are sent as non-secure, clear text. Use **LDAPS** for secure, encrypted communication between an appliance and LDAP server.

LDAP search parameters

Clicking the **Search Parameters** tab displays the parameters used when searching for LDAP directory service users.

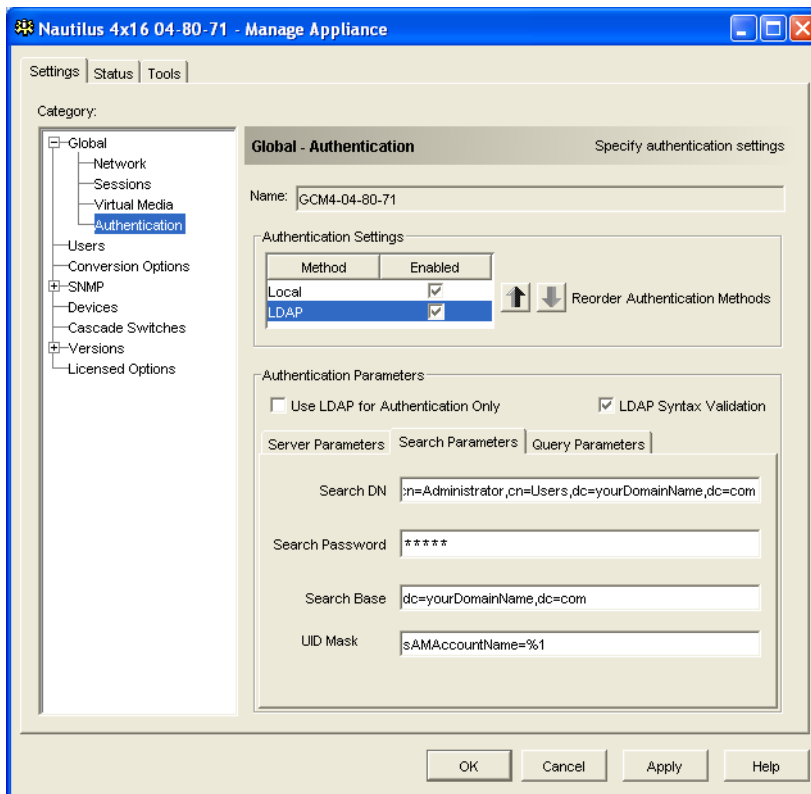


Figure 5.6: Search Parameters tab

Use the **Search DN** field to define an administrator-level user that the GCM4, GCM2, or RCM uses to log into the directory service. Once the appliance is authenticated, the directory service grants it access to the directory to perform the user authentication queries specified on the **Query Parameters** tab. The default values are *cn=Administrator, cn=Users, dc=yourDomainName, and dc=com* and may be modified. For example, to define an administrator Distinguished Name (DN)

for test.view.com, type *cn=Administrator, cn=Users, dc=test, dc=view, and dc=com*. This is a required field unless the directory service has been configured to enable anonymous search, which is not the default.

Each **Search DN** value must be separated by a comma. The **Search Password** field is used to authenticate the administrator or user specified in the **Search DN** field.

Use the **Search Base** field to define a starting point from which LDAP searches begin. The default values are *dc=yourDomainName, dc=com*, and may be modified. For example, to define a search base for test.com, type *dc=test, dc=com*. Each **Search Base** value must be separated by a comma.

The **UID Mask** field specifies the search criteria for User ID searches of LDAP target devices. The format should be in the form *<name>=<%I>*. The default value is *sAMAccountName=%I*, which is correct for use with Active Directory. This field is required for LDAP searches.

LDAP Query Parameters

Clicking the **Query Parameters** tab displays the parameters used when performing user authentication queries.

The appliance performs two different types of queries. Query mode (appliance) is used to authenticate administrators attempting to access the appliance itself. Query mode (device) is used to authenticate users that are attempting to access attached target devices.

Additionally, each type of query has three modes that utilize certain types of information to determine whether or not a VCS user has access to an appliance or connected target devices.

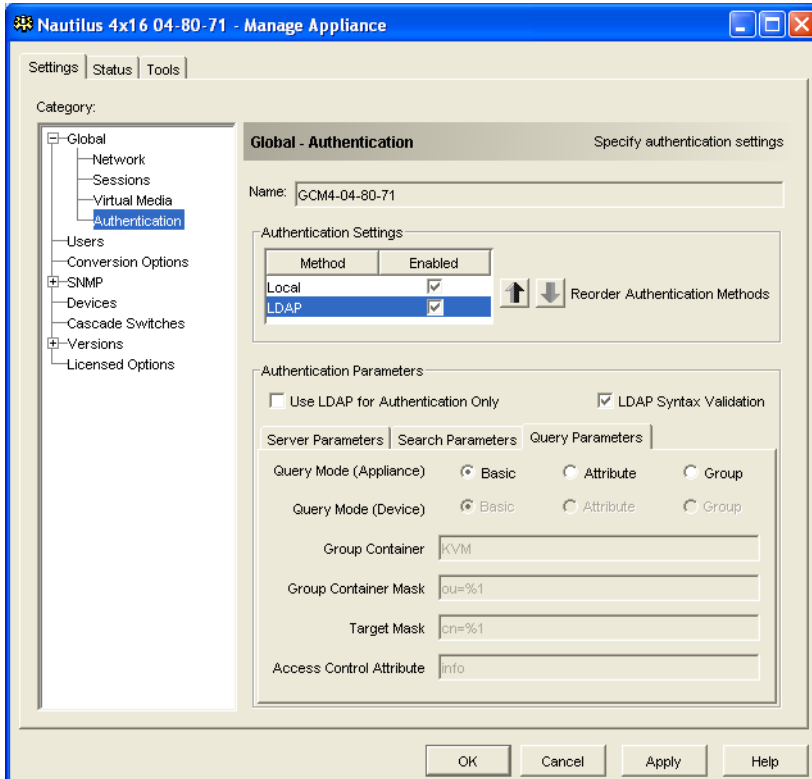


Figure 5.7: Query Parameters tab

You can configure the following settings in the **Query Parameters** tab:

- The **Query Mode (Appliance)** parameters determine whether or not a VCS user has access to the appliance.
- The **Query Mode (Device)** parameters determine whether or not a VCS user has user access to target devices connected to an appliance. The user does not have access to the appliance.
- The **Group Container**, **Group Container Mask**, and **Target Mask** fields are only used for group query modes and are required when performing an appliance or device query.
- The **Group Container** field specifies the organizational unit (ou) created in Active Directory by the administrator as the location for group objects. Group objects are Active Directory objects that can contain users, computers, contacts, and other groups. **Group Container** is used when **Query Mode** is set to Group. Each group object, in turn, is assigned members to associate with a particular access level for member objects (people, appliances, and target devices). The access level associated with a group is configured by setting the value of an

attribute in the group object. For example, if the **Notes** property in the group object is used to implement the access control attribute, the **Access Control Attribute** field in the **Query Parameters** tab should be set to *info*. Setting the **Notes** property to **KVM User Admin** causes the members of that group to have user administration access to the appliances and target devices that are also members of that same group.

The **Notes** property is used to implement the access control attribute. The value of the **Notes** property, available in group and user objects shown in Active Directory Users and Computers (ADUC), is stored internally in the directory, in the value of the *info* attribute. ADUC is a Microsoft Management Console snap-in for configuring Active Directory. It is started by selecting **Start > Programs > Administrative Tools > Active Directory Users and Computers**. This tool is used to create, configure and delete objects such as users, computers and groups. See Figure 5.8 on page 69 and Figure 5.9 on page 69 for more information.

- The **Group Container Mask** field defines the object type of the **Group Container**, which is normally an organizational unit. The default value is “ou=%1”.
- The **Target Mask** field defines a search filter for the target device. The default value is “cn=%1”.
- The **Access Control Attribute** field specifies the name of the attribute that are used when the query modes are set to Attribute. The default value is *info*.

Appliance and target device query modes

One of three different modes can each be used for **Query Mode (Appliance)** and **Query Mode (Device)**:

- **Basic** – A user name and password query for the VCS user is made to the directory service. If they are verified, the VCS user is given administrator access to the appliance and any attached target devices for **Query Mode (Appliance)**, or to any selected target device for **Query Mode (Device)**.
- **Attribute** – A user name, password, and **Access Control Attribute** query for the appliance user is made to the directory service. The **Access Control Attribute** is read from the user object (the user account) in Active Directory.

If the value “KVM Appliance Admin” is found, the VCS user is given appliance administrator access to the appliance and any attached target devices for **Query Mode (Appliance)**, or to any selected target device for **Query Mode (Device)**. If the value “KVM User Admin” is found, the VCS user is given User administrator access to the appliance and attached target devices for **Query Mode (Appliance)**, or to any selected target device for **Query Mode (Device)**.

The following are examples showing how the **KVM Appliance Admin** and **KVM User Admin** attribute modes are defined in Active Directory for a user named John Smith, stored in the ADUC. You can access the ADUC by selecting **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

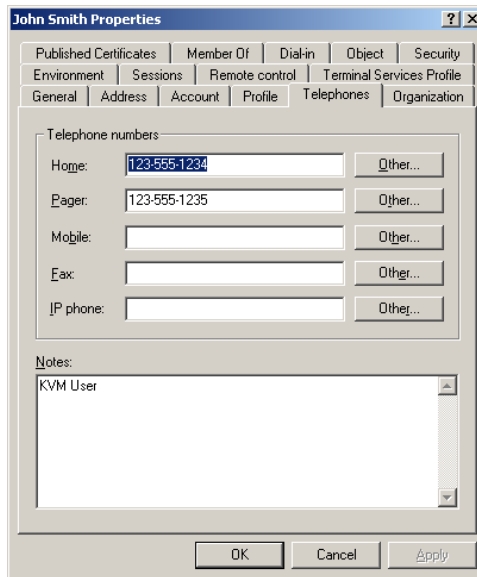


Figure 5.8: Active Directory - KVM user

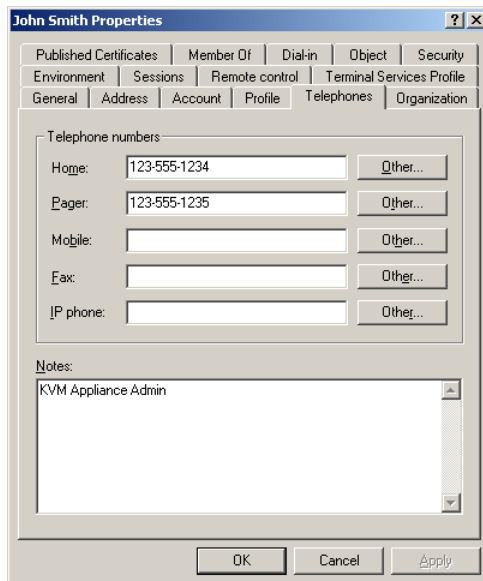


Figure 5.9: Active Directory - KVM appliance admin

- **Group** – A user name, password, and group query is made to the directory service for an appliance and attached target devices when using **Query Mode (Appliance)**, or for a selected target

device when using **Query Mode (Device)**. If a group is found containing the user and the appliance name, the VCS user is given access to the appliance or attached target devices, depending on the group contents, when using **Query Mode (Appliance)**. If a group is found containing the user and target device IDs, the VCS user is given access to the selected target device connected to the appliance when using **Query Mode (Device)**.

Groups can be nested to a maximum of 16 levels in depth. Use nesting to create groups within other groups. For example, you may have a top-level group named Computers that contains a member named R&D, which is a group. The R&D group may contain a member named Domestic, which is a group, and so on.

The following is an example of groups defined in Active Directory.

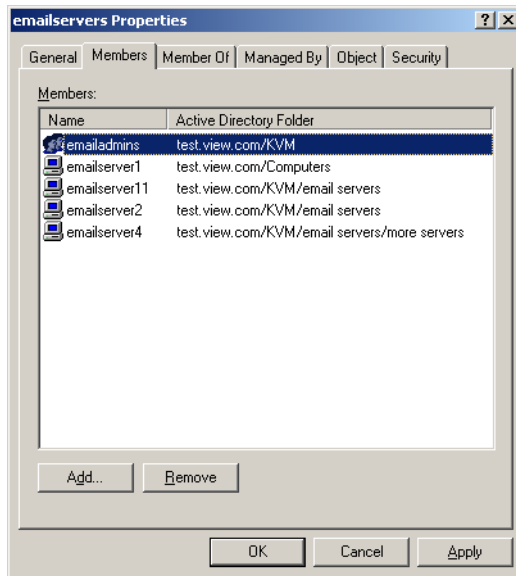


Figure 5.10: Active Directory - Define groups

Setting up Active Directory for performing queries

Before you can use any of the querying modes for units, you must first make changes to Active Directory so that the selected querying mode can assign the applicable authorization level for the VCS user.

To set up group queries, complete the following steps:

1. Log into Windows with administrator privileges.
2. Open Active Directory software.
3. Create an organizational unit to be used as a group container.

4. Create an object in Active Directory with a name identical to the switching system name for querying appliances (specified in the **Name** field in the **SNMP** category of the AMP), or identical to the attached target devices for querying target devices (specified in the **Devices** category of the AMP). The name must match exactly, including case.

The appliance names and target device names used for group queries are stored in the appliance. The appliance name and target device names specified in the **SNMP** and **Devices** categories of the AMP must identically match the object names in Active Directory. Each appliance name and target device name may be comprised of any combination of upper-case and lower-case letters (a-z, A-Z), digits (0-9) and hyphens (-). You cannot use spaces and periods (.) or create a name that consists entirely of digits. These are Active Directory constraints. The factory default RCM name in earlier versions contains a space that must be removed by editing the switching system name in the **SNMP** category of the AMP.

5. Create one or more groups under the group container organizational unit.
6. Add the user names and target device and appliance objects to the groups you created in step 5.
7. Specify the value of any attribute being used to implement the access control attribute. For example, if you are using *info* as the attribute in the **Access Control Attribute** field and using the **Notes** property in the group object to implement the access control attribute, the value of the **Notes** attribute in Active Directory may be set to one of the three available access levels (**KVM User**, **KVM User Admin**, or **KVM Appliance Admin**) for the group object. The members of the group may then access the appliances and target devices at the specified access level.

Managing local user accounts

The **Users** category lists user names in the appliance user database and their access levels. You can add, modify, or delete a user account from this category. The security lock-out feature is also controlled from this category.

The fields in this category are disabled if LDAP is being used for both Authentication and Authorization. If LDAP is being used only for Authentication, then users can be added and modified in this category, but only to set the access control lists for the users (the password fields are disabled in this mode).

Access levels

You can assign users one of three access levels: user, user administrator, or appliance administrator. Use the user access level to assign individual target device access rights to a user.

Table 5.1 indicates the types of appliance operations that can be performed in the three access levels.

Table 5.1: GCM4, GCM2, or RCM appliance access levels

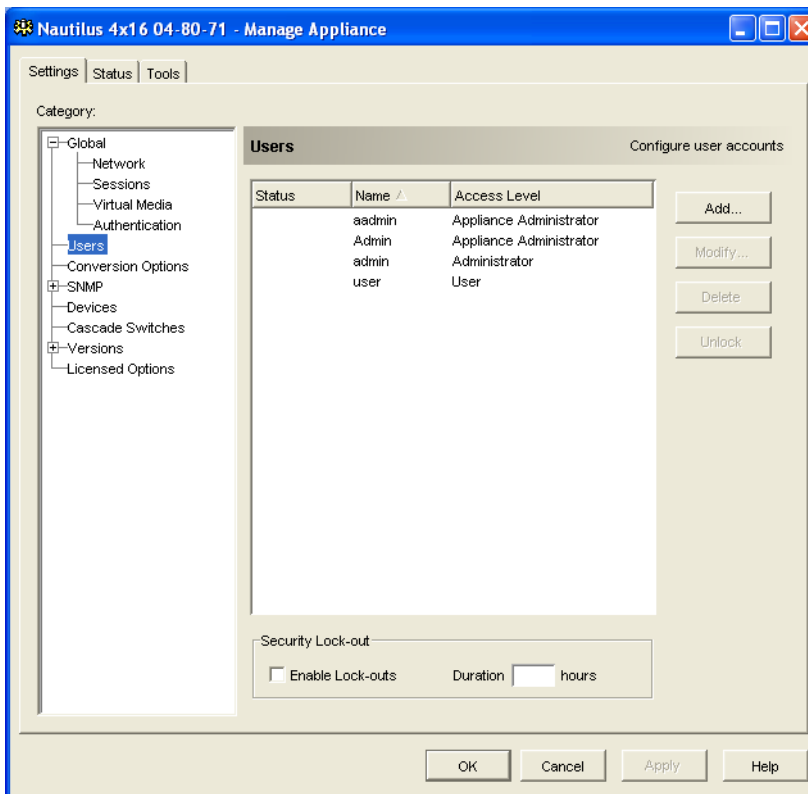
Operations	Appliance administrator	User administrator	User
Preempt other users	All	Equal and lesser	No

Table 5.1: GCM4, GCM2, or RCM appliance access levels (Continued)

Operations	Appliance administrator	User administrator	User
Set network and global values	Yes	No	No
Reboot and upgrade firmware	Yes	No	No
Manage user accounts	Yes	Yes	No
Monitor target device status	Yes	Yes	No
Access target devices	Yes	Yes	Assigned by Admin

To add or modify a user, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Users** category.

**Figure 5.11: AMP User settings**

3. Complete one of the following steps:
 - To add a new user, click the **Add** button. The Add User window opens.
 - To modify a user, select a user name and click the **Modify** button. The Modify User window opens.
4. Complete one of the following steps:
 - When adding a user, enter the user name and password to assign to the user and then verify the password by typing it in the **Verify Password** field.
 - When modifying a user, change the password, if needed.

When **Use LDAP for Authentication only** is selected in the **Global - Authentication** category, the password field is disabled and only the access rights of the user are used.
5. Select the needed access level for this user from the pull-down menu. If you select the **User** option, the **Access Rights** button is visible.
 - a. To select individual target device access for the user, click the **Access Rights** button. The User Access Rights window opens.
 - b. To add access to target devices, select one or more target devices in the left (No access to) column. Click the **Add** button.
 - c. To remove access to target devices, select one or more target devices in the right (Allow access to) column. Click the **Remove** button.
 - d. Repeat steps b and c until the right (Allow access to) column represents the applicable target device access for this user, and then click **OK**.
6. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

To delete a user, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Users** category.
3. Select the user or users to delete.
4. Click the **Delete** button. You are prompted to confirm the deletion.
5. Click **Yes** to confirm the deletion.
6. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

NOTE: Add, Modify and Delete user operations may be combined and saved at the same time by pressing the **Apply** or **OK** buttons on the AMP when done with the changes.

Locking and unlocking user accounts

When the security lock-out feature is enabled, and a user enters an invalid password five consecutive times, that user account is disabled for a specified number of hours, or until it is unlocked or the appliance is rebooted. If a locked-out user tries to log in during the lock-out period, an error message is displayed. A closed-lock icon is visible next to the names of locked-out users on the AMP **Users** category. Security lock-out, when enabled, applies to all local user accounts on the appliance, but not to LDAP users.

An appliance administrator can specify the lock-out period. A user administrator can unlock only user accounts; an appliance administrator can unlock any type of account.

When the security lock-out feature is disabled, no users are locked-out. Disabling security lock-out has no effect on users who are already locked-out.

To enable or disable security lock-out, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Users** category.
3. Complete one of the following steps:
 - Select the **Enable Lock-outs** check box. Enter the number of hours (1 to 99) in the lock-out period in the **Duration** field.
 - Clear the **Enable Lock-outs** check box.
4. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

To unlock an account, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Users** category.
3. Select the user to unlock.
4. Click the **Unlock** button.
5. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

A locked-out user is unlocked if the appliance is rebooted or when the configured lock-out duration expires.

Managing user sessions

The **Status** tab displays information about currently active Video Viewer and virtual media sessions. Each line of session information includes:

- The status of the session. A Locked icon is shown for KVM sessions that are locked to virtual media sessions, and a Reserved icon is shown for reserved virtual media sessions.
- The name of the user who is logged in to the session.
- The length of time this session has been active, in the form hours:minutes:seconds. If the session has been active for more than 24 hours, the number of days precedes the other time information. For example, a session that has been active for two days, three hours, seven minutes, and 52 seconds shows 2d 3:07:52.
- The type of session, including both virtual media sessions and KVM sessions. The session status also displays the video session type, such as KVM (Stealth). For more information on session types see Table 4.1.
- The name of the target device to which this session is connected. If the session is connected to a CO cable with no target device name specified in the database, the CO cable eID is listed. If the session is connected to a cascade switch, the CO cable eID, appliance name, and channel number are listed.
- The IP address of the remote client connected to this session.

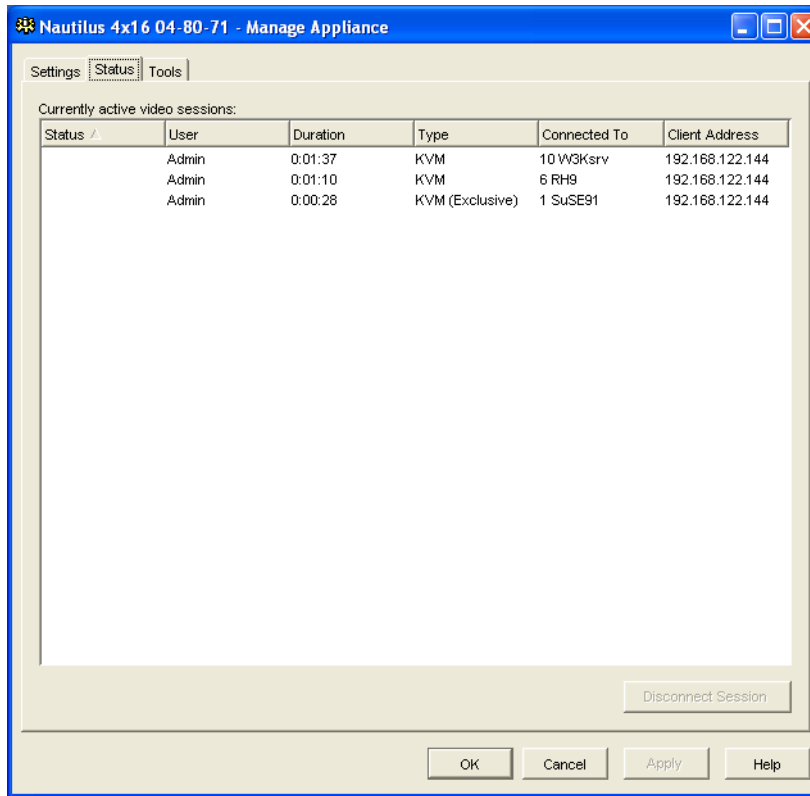


Figure 5.12: AMP Status tab

To disconnect a user session, complete the following steps:

1. Click the **Status** tab in the AMP.
2. Select one or more users sessions to disconnect. Use the Shift or Ctrl key to select multiple user sessions.
3. Click the **Disconnect Session** button. A message prompts you to confirm the disconnect request.
4. Complete one of the following steps:
 - Click **Yes** to disconnect the user sessions.
 - Click **No** to cancel the disconnect.

Viewing and changing Conversion Option settings

The **Conversion Options** category displays information about each CO cable, including its input port number, ID, type, language, and status. The possible status values are:

- Green circle = the CO cable is online
- Yellow circle = the CO cable is upgrading
- Red X = the CO cable is offline

To display CO cable information, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Conversion Options** category.

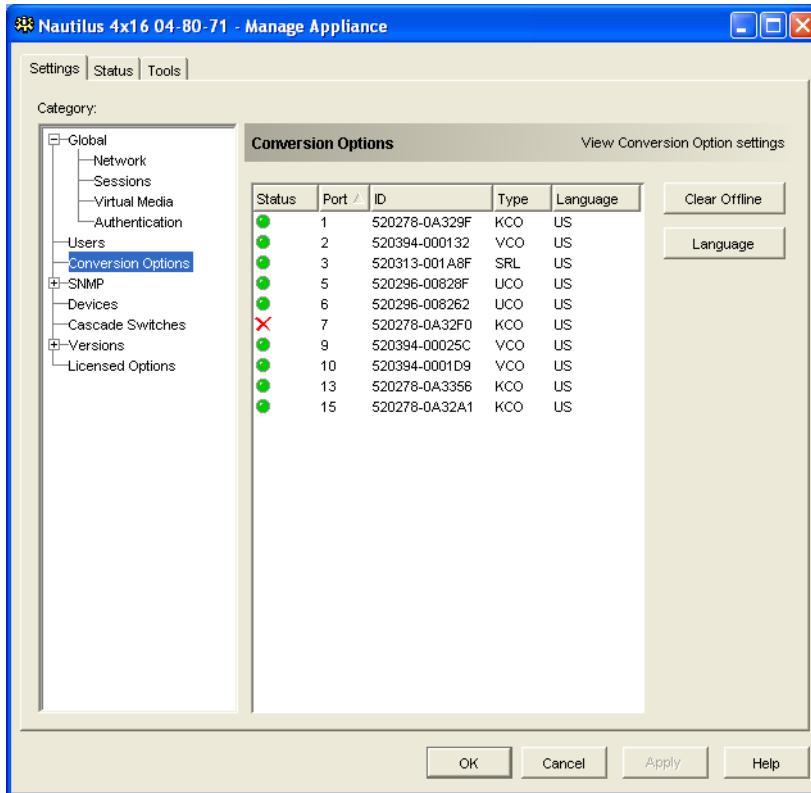


Figure 5.13: AMP Conversion Option settings

To remove offline conversion options from the list, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Conversion Options** category.
3. Click **Clear Offline**.

To change the language reported by USB CO cables, complete the following steps:

1. Click the **Settings** tab in the AMP.

2. Select the **Conversion Options** category.
3. Click **Language**.
4. Select the keyboard layout from the list.
5. Complete one of the following steps:
 - Click **OK** to select the keyboard layout.
 - Click **Cancel** to return to the AMP without changing the language.
6. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

All Conversion Options report in the new language.

Using SNMP

The **SNMP** category specifies general SNMP configuration information. The **SNMP - Traps** subcategory indicates which traps are enabled and disabled.

SNMP (Simple Network Management Protocol) is a protocol used to communicate management information between network management applications and appliances. SNMP managers (such as Tivoli and HP OpenView) can communicate with the appliance by accessing MIB-II (Management Information Base) and the public portion of the enterprise MIB. MIB-II is a standard MIB that many SNMP managers support. You can:

- Enable or disable SNMP operations.
- Enter switching system information and community strings.
- Indicate which computers can manage the appliance. If you enter one or more allowable managers, only those IP addresses can monitor the appliance using SNMP. If you do not enter any allowable managers, then the appliance can be monitored using SNMP from any IP address.
- Indicate which computers receive SNMP traps from the appliance. If you do not specify any trap destinations, no traps are sent.

When you enable SNMP, the unit responds to SNMP requests over UDP port 161. Port 161 is the standard UDP port used to send and receive SNMP messages.

The AMP uses SNMP within a secure tunnel to manage appliances. For this reason, UDP port 161 does not need to be exposed on firewalls. You must expose UDP port 161 to monitor appliances using third party SNMP-based management software.

To configure general SNMP settings, complete the following steps:

1. Click the **Settings** tab in the AMP.

2. Select the **SNMP** category.

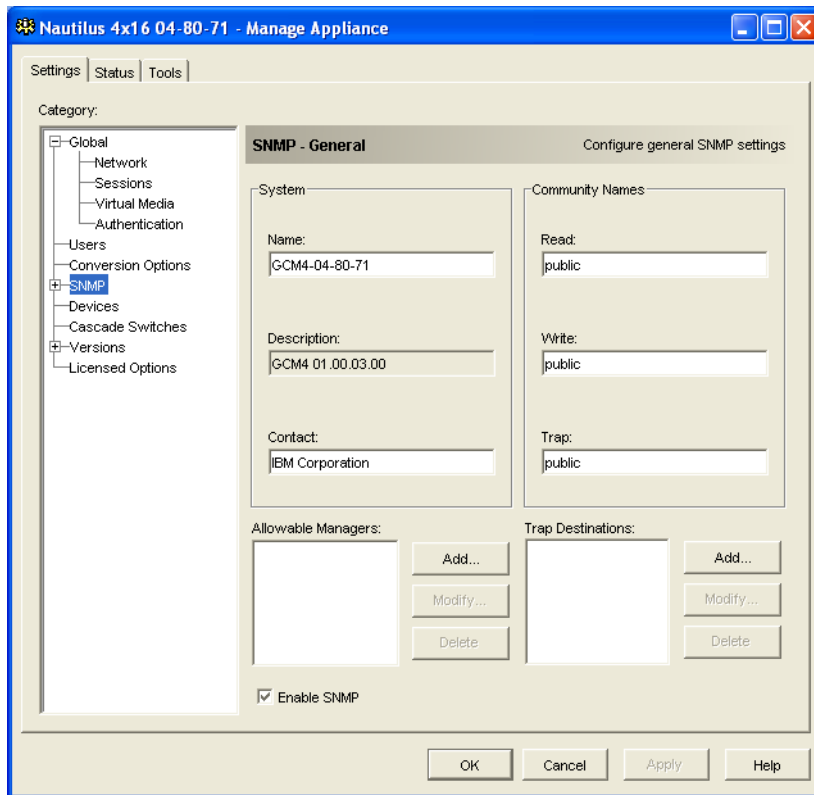


Figure 5.14: AMP SNMP category

3. Select or clear the **Enable SNMP** check box.
4. In the **Name** field, enter the 0 to 255 character fully qualified domain name of the appliance. In the **Contact** field, enter 0 to 255 characters of contact information.
5. In the **Community Names** area, enter the 1 to 64 character **Read**, **Write**, and **Trap** community names. These specify the community strings that must be used in SNMP actions. The **Read** and **Write** strings apply only to SNMP over UDP port 161 and act as passwords that protect access to the appliance.
6. In the **Allowable Managers** area, specify up to four SNMP management entities to monitor the appliance, or leave this area blank to let any computer to monitor the appliance.

To add an allowable manager, complete the following steps:

 - a. Click the **Add** button. The Allowable Manager window opens.
 - b. Enter the IP address of the management computer.
 - c. Click **OK** to add the management computer.

To modify an allowable manager, complete the following steps:

- a. Select an entry in the **Allowable Managers** list, then click the **Modify** button. The Allowable Manager window opens.
- b. Modify the entry as needed.
- c. Click **OK** to save the change.

To delete an allowable manager, complete the following steps:

- a. Select one or more entries in the **Allowable Managers** list, then click the **Delete** button. You are prompted to confirm the deletion.
- b. Click **Yes** to confirm the deletion.

7. In the **Trap Destinations** area, specify up to four destinations to which this appliance sends traps.

To add a trap destination, complete the following steps:

- a. Click the **Add** button. The Trap Destination window opens.
- b. Enter the IP address of the trap destination.
- c. Click **OK** to add the trap destination.

To modify a trap destination, complete the following steps:

- a. Select one or more entries in the **Trap Destinations** list, then click the **Modify** button. The Trap Destination window opens.
- b. Modify the entry as needed.
- c. Click **OK** to save the change.

To delete a trap destination, complete the following steps:

- a. Select an entry in the **Trap Destinations** list, then click the **Delete** button. You are prompted to confirm the deletion.
- b. Click **Yes** to confirm the deletion.

8. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.
9. If you clicked **Apply** or **OK**, you are prompted to confirm a reboot. The new settings are not used until the appliance reboots. Complete one of the following steps:
 - Click **Yes** to reboot the appliance. The AMP displays the status and indicates when the reboot is complete.
 - Click **No** to reboot at a later time.

Managing SNMP traps

An SNMP trap is a notification sent by the appliance to a management computer, indicating that an event has occurred in the appliance that can require further attention. You can specify which

individual SNMP traps are sent to the management computers by selecting the corresponding check boxes, or you can enable or disable all traps. The GCM4, GCM2, and RCM appliance have enterprise traps. To interpret these traps correctly, download the corresponding trap MIB from the IBM Web site.

To enable or disable SNMP traps, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **SNMP - Traps** subcategory. A list of traps is displayed. Traps that are currently enabled are selected; disabled traps are not selected.

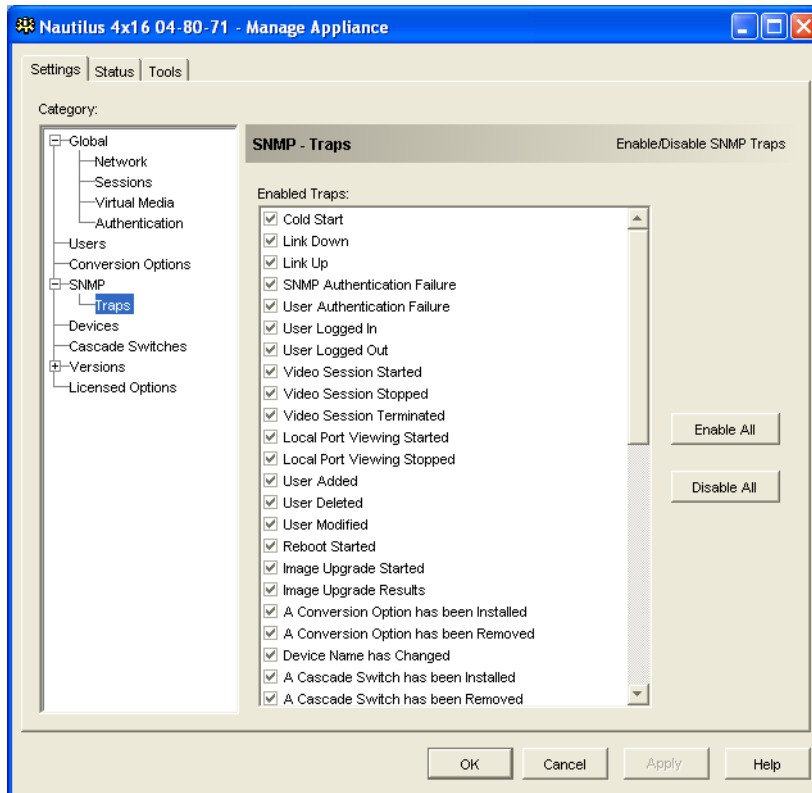


Figure 5.15: AMP SNMP - Traps subcategory

3. Complete one of the following steps:
 - Select or clear the individual trap check boxes.
 - To enable all traps, click the **Enable All** button.
 - To disable all traps, click the **Disable All** button.
4. Complete one of the following steps:

- Click **Apply** to save any changes without exiting the AMP.
- Click **OK** to save any changes and exit the AMP.
- Click **Cancel** to exit the AMP without saving any changes.

Viewing target device connection information

The **Devices** category displays connection information for each target device, as follows:

- **CO** - The display shows the eID of the CO cable.
- **Cascaded switch** - The display shows the appliance and all of its channels.
- **No device connection** - The display indicates “None”.

When you select the **Devices** category for the first time, the AMP retrieves the target devices that exist in the software database as well as information on how the target devices are connected to the selected appliance. The Connections column lists the current target device connection. This can be to either a CO cable or a cascade switch. If connected to a CO cable, the CO cable eID is visible in the Connections column. If connected to a cascade switch, the cascade switch and all of its channels are visible. If no unit is currently connected to the path, then this field displays “None”.

Clicking on a hyperlink of a target device entry opens the Video Viewer.

You can resynchronize the database on the computer with the database on the appliance from this category. See Figure 5.16 on page 83.

Modifying target device names

The **Devices** category can be used to modify the target device name on both the appliance and in the client database.

To modify the name of a target device, complete the following steps:

1. Click the **Settings** tab in the AMP.

2. Select the **Devices** category.

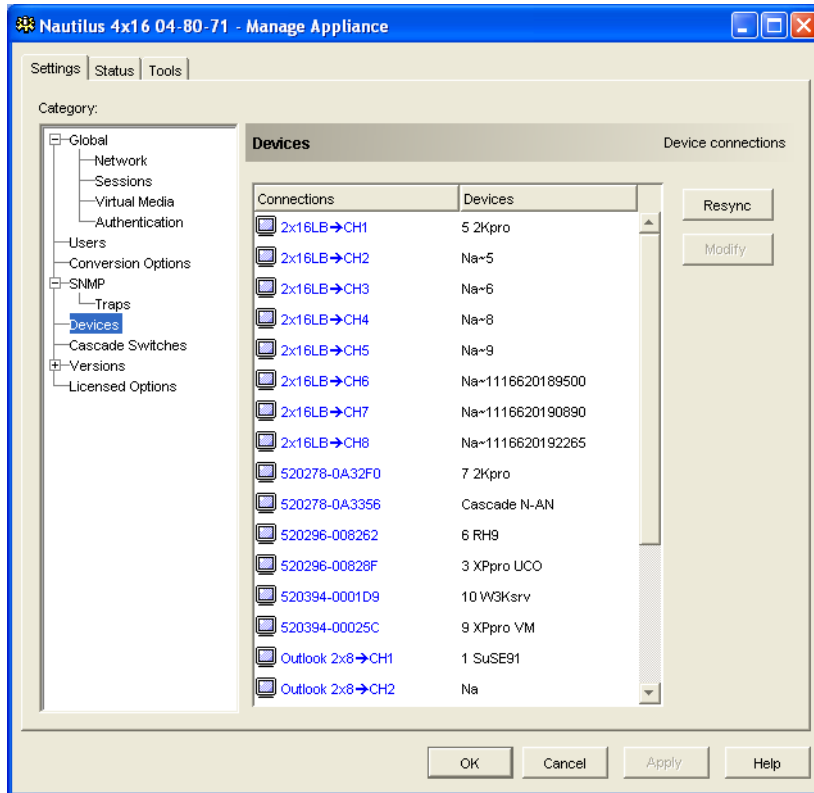


Figure 5.16: AMP Settings - Devices

3. Select the target device from the list that you want to modify. You can only modify one target device at a time.
4. Click **Modify**.
5. The pop-up window lists the current name of the target device as stored in both the appliance and the client database (not necessarily the same).
6. Type the new name of the target device in the **New Name** field.
7. Complete one of the following steps:
 - Click **OK** to change the target device name.
 - Click **Cancel** to keep the target device name as is.
8. Repeat the steps 3 through 7 for each target device name that you want to change.
9. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.

- Click **OK** to save any changes and exit the AMP.
- Click **Cancel** to exit the AMP without saving any changes.

Resynchronizing the target device list

You might need to resynchronize the target device list if the local user has changed target device names on the appliance using the OSCAR interface or if CO cables have been added or moved. For more information about names, see "Target device naming" on page 4.

Prior to starting the resynchronization process, a warning message indicates that the database will be updated to match the current configuration in the appliance. This warning contains a check box that indicates whether offline CO cables will be included. When enabled, target devices associated with CO cables that are offline are included. When disabled, offline CO cables are not included and any existing target devices associated with them in the database are removed.

This procedure only resynchronizes your own VCS client. To keep databases consistent when you have multiple computers using the software, save your resynchronized local database and restore it to the other computers.

To resynchronize the target device list, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Devices** category.
3. Click the **Resync** button. The Resync Wizard opens. Click **Next**.
4. A warning message indicates that the database will be updated to match the current configuration in the appliance. Select or clear the **Include Offline Conversion Options** check box. Click **Next**.
5. A Polling Appliance message is displayed with a progress bar indicating that appliance information is being retrieved.
6. Complete one of the following steps:
 - If no changes were detected in the appliance, a completion window opens with this information. Click **OK**.
 - If target device changes were detected, the Detected Changes window opens. Click **Next** to update the database.
 - If a cascade switch was detected, the Enter Cascaded Switch Information window opens. Select the type of cascade switch connected to the appliance from the pull-down menu. If the type you are looking for is not available, you can add it using the **Add** button. For more information, see "Configuring cascade switch connections" on page 84. Click **Next**.
7. The completion window opens. Click **Finish** to exit.

Configuring cascade switch connections

The **Cascade Switches** category displays tiered cascade switch information, including the CO cable eIDs, cascade switch type, and the port to which each is connected.

To configure a cascade switch connection, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Cascaded Switches** category.

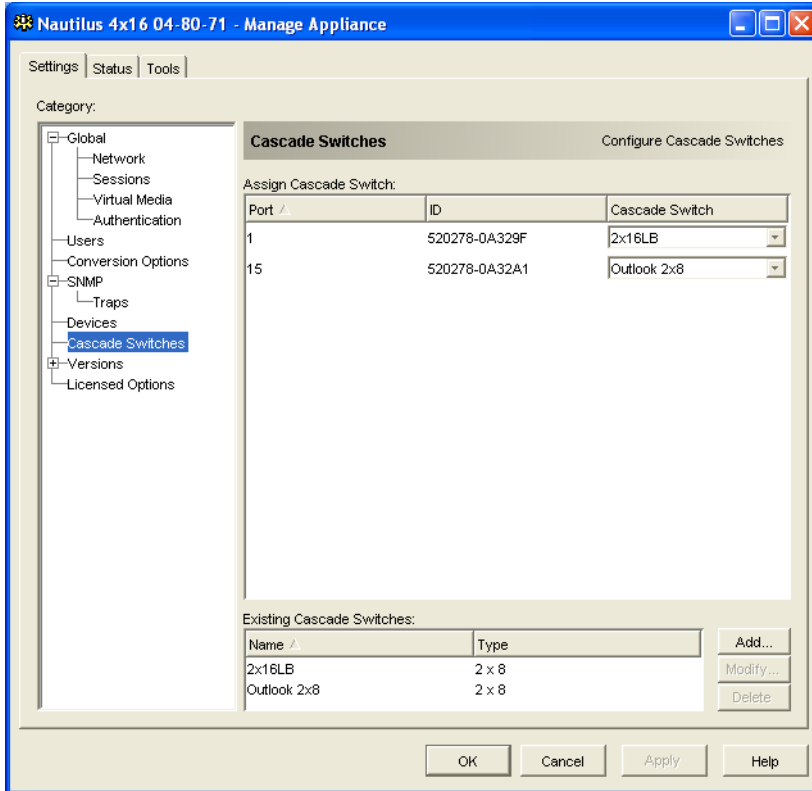


Figure 5.17: AMP Settings - Cascaded Switches

3. Complete one of the following steps:
 - Click the pull-down list next to the cascade switch and select the cascade switch type to assign.
 - If the cascade switch type is not in the pull-down list, add a cascade switch to the **Existing Cascaded Switches** list by clicking the **Add** button. The Add Cascaded Switch window opens.
Type the name of the cascade switch and select the cascade switch type from the list.
Click **OK** to add the cascade switch. The cascade switch is now in the **Existing Cascaded Switches** list and in the Cascade Switch pull-down list.
4. Repeat step 3 for each cascade switch to be configured.

5. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

Viewing appliance and CO cable version information

The **Versions** category displays firmware version numbers.

The **Versions - Hardware** subcategory displays the hardware component version numbers of the unit.

The **Versions - COs** subcategory displays CO cable version information. You can individually view and upgrade CO cables from this category.

Licensing appliance options

When you click the **Licensed Options** category in the AMP, the Licensed Options window opens. Use this window to configure options for use that are available on the GCM4, GCM2, or RCM firmware. The Licensed Options window lists each option available on the GCM4, GCM2, or RCM and if the option has been enabled by a license key.

To license a GCM4, GCM2, or RCM option, complete the following steps:

1. Click the **Licensed Options** category in the left column in the AMP.
2. Click the **Add** button on the right side of the window to add a GCM4, GCM2, or RCM option. The Enter Key window opens.
3. Type a license key. The license key is comprised of 20 case-sensitive characters.
4. Click **OK**. If the key for the option you are licensing is valid, the license type is listed in the Option Name column and Yes is listed in the Options Enabled column for the licensed option.

NOTE: Currently, the only available option is **LDAP Authentication**.

Upgrading firmware

You can upgrade the firmware for either the GCM4, GCM2, or RCM appliance or the CO cables.

Automatic firmware upgrades

You can set the AMP to upgrade the CO cable firmware automatically.

To enable automatic CO cable firmware upgrades, complete the following steps:

1. Click the **Settings** tab in the AMP.

2. Select the **Versions - Conversion Options** subcategory.

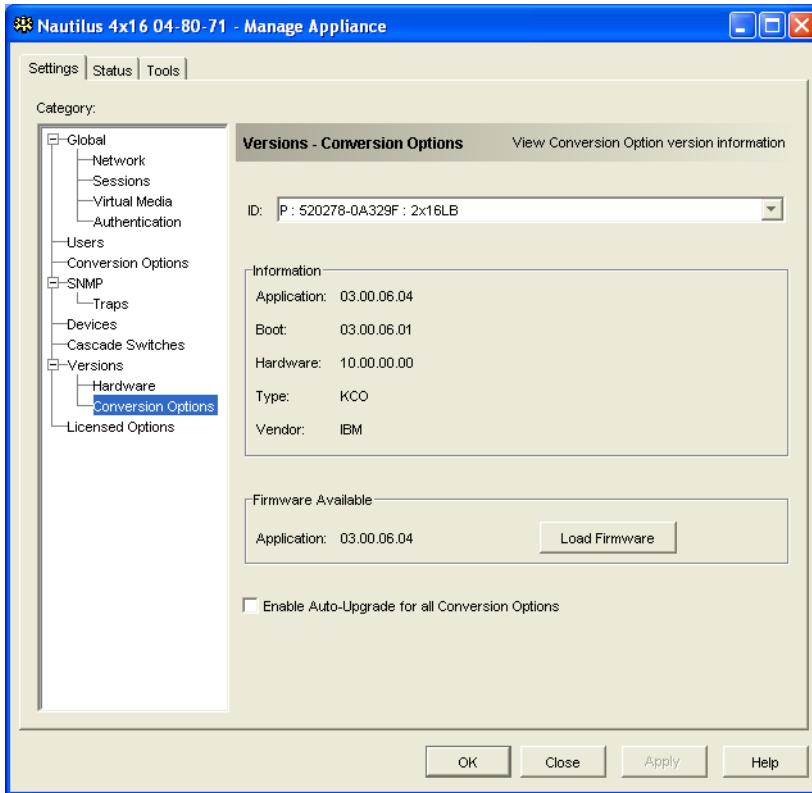


Figure 5.18: Conversion Options upgrade

3. Enable the check box next to **Enable Auto-Upgrade for all Conversion Options**.
4. Complete one of the following steps:
 - Click **Apply** to save any changes without exiting the AMP.
 - Click **OK** to save any changes and exit the AMP.
 - Click **Cancel** to exit the AMP without saving any changes.

Upgrading GCM4, GCM2, or RCM appliance firmware

To upgrade appliance firmware, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Upgrade Appliance Firmware** button.

If you have made changes in the Settings tab of the AMP but have not yet applied them, a warning message prompts you to confirm the upgrade. The firmware upgrade requires an appliance reboot and pending changes will be discarded.

To apply changes to the Settings tab before the upgrade, complete the following steps:

- a. Click **No** to cancel the appliance firmware upgrade.
 - b. Click **Apply**.
 - c. Continue with step 2 of this procedure, or click **Yes** to discard pending (unapplied) changes.
3. The Firmware Upgrade window opens. You can choose to use TFTP or ASMP file transfer. When upgrading an RCM appliance, only the TFTP option is available. To use TFTP, complete the following steps:
- a. Select the **TFTP Server** radio button.
 - b. In the **TFTP Server IP Address** field, type in the IP address of the TFTP target device where the firmware is installed.
 - c. In the **Firmware Filename** field, enter the name of the firmware file.
 - d. Click the **Upgrade** button. The AMP tracks and displays status.
4. To use ASMP, complete the following steps:
- a. Select the **File System** radio button.
 - b. Click **Browse** to select the firmware file to be transferred.
 - c. Click the **Upgrade** button. The AMP tracks and displays status.
5. When the upgrade is complete, a message prompts you to confirm a reboot. Complete one of the following steps:
- Click **Yes** to reboot the appliance. After rebooting, the AMP re-establishes a secure management connection with the appliance.
 - Click **No** to reboot at a later time. You must reboot to use the new firmware.
6. Click **Close** to exit the Firmware Upgrade window.

Important: Do not turn off the GCM2 or GCM4 appliance while it is upgrading.

Upgrading CO cable firmware

CO cables can be upgraded individually or simultaneously as a group by CO cable type. When an upgrade is started, the current status is listed.

When you request an upgrade for all CO cables of a particular type, that upgrade must finish before you can start another upgrade for any CO cable of that type. However, multiple individual CO cable firmware upgrades can be done in parallel.

To simultaneously upgrade the firmware of multiple CO cables, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Upgrade CO Firmware** button. The Upgrade CO Firmware window opens.

3. Select the check box in front of each type of CO cable to upgrade. (A check box for a CO cable type can only be selected if there is a later version available of the firmware. This is indicated by the Need Upgrade column. If one or more CO cables of a given type need upgrades, you can select this type for the upgrade. If there is no later firmware for a CO cable type, you cannot select the corresponding check box.)
4. Click **Upgrade**. The Status column displays either In Progress, Succeeded, or Failed (with reason included) depending on the status of each CO cable upgrade. A Firmware upgrade currently in progress message is visible until all of the selected CO cable types are upgraded.
5. When complete, a message prompts you to confirm the upgrade completion. When confirmed, the **Upgrade** button is again enabled.
6. Click **Close** to exit the Upgrade CO Firmware window.

To upgrade CO cable firmware individually, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Click the **Versions - Conversion Options** subcategory.
3. To view firmware information, select the CO cable from the eID pull-down menu list. Each entry is a combination of the port number, the eID, and either the target device name or cascade switch name, depending on what is attached to the CO cable. If the CO cable is not attached to anything, the menu displays **None**. When a CO cable is selected, its firmware information is listed in the **Information** field.
4. Compare the current information to the **Firmware Available** field to see the firmware upgrade available for the CO cable. (You can load firmware even if the current and available versions are the same. In some cases, you can downgrade the CO cable to an earlier, compatible version.) Click the **Load Firmware** button.
5. The firmware upgrade begins. During the upgrade, progress messages are visible below the **Firmware Available** field. When the upgrade is finished, a message indicates either that the upgrade is complete or the reason for failure.
6. Repeat steps 3 through 5 for each CO cable to upgrade.
7. When finished, click **OK**.

Rebooting the appliance

The Reboot Appliance tool instructs the appliance to reboot. The appliance broadcasts a disconnect message to all client connections before rebooting.

To reboot the appliance, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Reboot Appliance** button. A message prompts you to confirm the reboot. Click **Yes** to confirm the request. The appliance notifies each attached client, then reboots.
3. The AMP closes.

Managing the appliance configuration database

All appliance settings are stored in an appliance configuration database. (User account information is stored in a user database; see "Managing the appliance user database" on page 91 for more information.)

Saving an appliance configuration database

The Save Appliance Configuration tool saves the configuration database from the appliance to a file on the computer running the software.

The file is encrypted during the save process, and you are prompted to create a password when you save the database. You must enter this password when you restore the file.

To save a configuration from an appliance to a file, complete the following steps:

1. Click the **Tools** tab in the AMP.

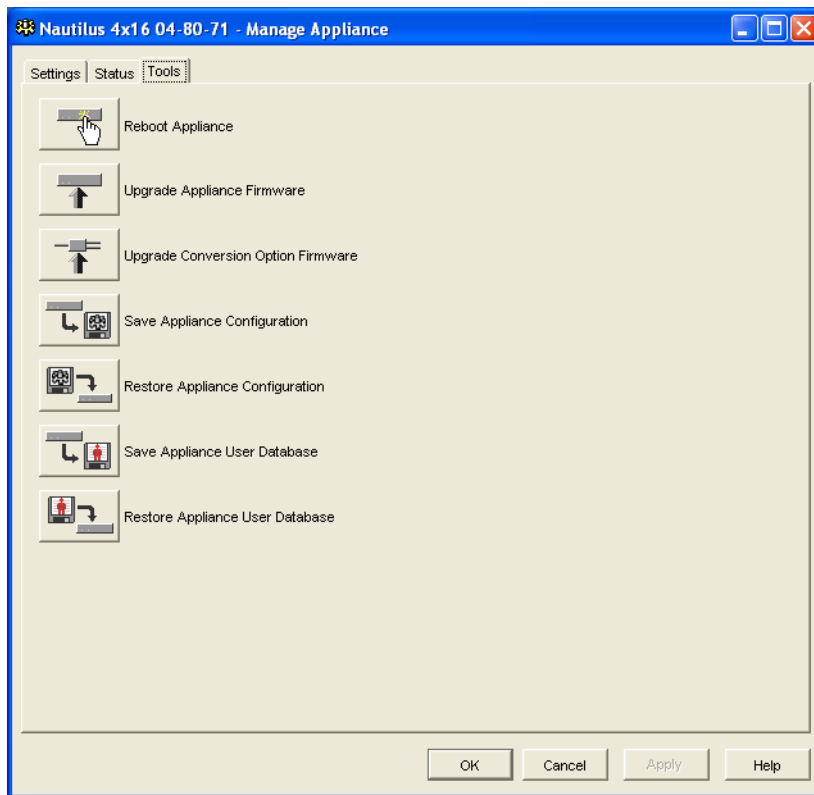


Figure 5.19: AMP tools tab

2. Click the **Save Appliance Configuration** button. The Save Appliance Configuration window opens.
3. Click **Browse** and navigate to a location to save the configuration file. The location is listed in the **Save To** field.
4. Click **Save**. The Enter Password window opens.
5. Enter a password in the **Password** field, then repeat the password in the **Verify Password** field. This password is requested when you restore this database to an appliance. Click **OK**.
6. The appliance configuration database file is read from the appliance and saved to the selected location. Progress messages are visible. When the save is complete, you are prompted to confirm the completion. Click **OK** to return to the Tools tab.

Restoring an appliance configuration database

The Restore Appliance Configuration tool restores a previously-saved configuration database from the computer running the software to the appliance. The database file can be restored to either the appliance from which it was saved or to another appliance of the same type. This eliminates the need to manually configure a new appliance.

To restore a configuration file to an appliance, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Restore Appliance Configuration** button. The Restore Appliance Configuration File window opens.
3. Click **Browse** and navigate to the location where you stored the saved configuration file. The filename and location are listed in the **File Name** field.
4. Click **Restore**. The Enter Password window opens.
5. Enter the password you created when the configuration database was saved. Click **OK**.
6. The configuration file is written to the appliance. Progress messages open. You are prompted to confirm a reboot. The restored configuration file is not used until the appliance reboots. Complete one of the following steps:
 - Click **Yes** to reboot the appliance. The AMP displays the status and indicate when the reboot is complete.
 - Click **No** to reboot at a later time.

Managing the appliance user database

All user accounts and access rights assignments are stored in a database.

The file is encrypted during the save process, and you are prompted to create a password when you save the database. You must enter this password when you restore the file.

Saving an appliance user database

The Save Appliance User Database tool saves this user database from the appliance to a file on the computer running the software.

To save a user database from an appliance to a file, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Save Appliance User Database** button. The Save Appliance User Database window opens.
3. Click **Browse** and navigate to a location to save the user database file. The location is listed in the **Save To** field.
4. Click **Save**. The Enter Password window opens.
5. Enter a password in the **Password** field, then repeat the password in the **Verify Password** field. This password is requested when you restore this database to an appliance. Click **OK**.
6. The user database file is read from the appliance and saved to a location. Progress messages open. When the save is complete, you are prompted to confirm the completion. Click **OK** to return to the Tools tab.

Restoring an appliance user database

The Restore Appliance User Database tool restores a previously-saved user configuration database from the computer running the software to the appliance. The database file can be restored to either the appliance from which it was saved or to another appliance of the same type. This eliminates the need to manually configure users on a new appliance.

To restore a user database file to an appliance, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Restore Appliance User Database** button. The Restore Appliance User Database window opens.
3. Click **Browse** and navigate to the location where you stored the saved user database file. The filename and location is listed in the **File Name** field.
4. Click **Restore**. The Enter Password window opens.
5. Enter the password you created when the user database was saved. Click **OK**.
6. The user database file is written to the appliance. Progress messages open. When complete, the new user database is used immediately; no reboot is required.

Appendix A: Updating VCS

For optimal operation of the switching system, make sure that you have the latest version of VCS available from the IBM Web site.

To update VCS, complete the following steps:

1. Go to <http://www.ibm.com/pc/support/> and download the update file.
2. Double-click on the installer. The installer determines if a previous version of the software resides on the computer.
3. Complete one of the following steps:
 - If no previous version has been detected and a window opens to confirm the upgrade, click **Continue**.
 - If a previous version is detected and a window opens alerting you to another version of the product, click **Overwrite** to confirm the upgrade.
 - Click **Cancel** to exit without upgrading the software.
4. Installation starts. The Program Files, Shortcuts, Environment Variables, and the Registry Entries (for Windows operating systems), are installed or overwritten with the new files and settings of the current version.

Appendix B: Virtual media

Virtual media and USB 2.0 constraints

The virtual media feature of GCM2, GCM4, and LCM2 appliances enables you to connect to the USB port of an attached computer. With this feature, a user located at the appliance or using the remote software can access a local USB storage device, such as a USB CD drive, diskette drive, or flash drive, from an attached computer.

The Virtual Media Conversion Option (VCO) cable is a composite device that addresses four functions: keyboard, mouse, CD drive, and mass storage device. The CD drive and mass storage device will be present on the target device whether or not a virtual media session is mapped. If a media device is not mapped, it is shown without media present. When a virtual media device is mapped to the target device, the target device will be notified that media has been inserted. When the media device is unmapped, the target device will be notified that the media was removed. Therefore, the USB virtual device is not disconnected from the target device.

The VCO cable presents the keyboard and mouse as a composite USB 2.0 device. Therefore the BIOS must support composite USB 2.0 human interface device (HID). If the BIOS of the connected computer does not support this type of device, the keyboard and mouse might not work until the operating system loads USB 2.0 device drivers. If this occurs, there might be a BIOS update provided by the computer manufacturer that will provide BIOS support for a USB 2.0 connected keyboard and mouse.

Booting a computer using virtual memory

In many cases the virtual media feature can boot an attached computer from a device attached to the USB port on the appliance. Most computers with a USB port can use virtual media; however, limitations in some USB media devices and the BIOS of some computers might prevent the computer from booting from a USB device attached to the GCM2, GCM4, or LCM2 appliance.

Booting from a virtual USB device is dependant on the target device supporting booting from an external composite USB device. It also requires a CD of the operating system that supports external USB 2.0 booting. The following is a partial list of operating systems that support booting from an external USB 2.0 device:

- Windows Server 2003
- Windows XP
- Windows 2000 Server with Service Pack 4 (SP4) or later

To determine if your computer can be booted from virtual media, complete the following steps:

1. Connect a USB CD drive to the GCM2, GCM4, or LCM2 appliance with an operating system installation CD that is bootable and map it to the target device. Reboot the target device to determine if it will boot from this attached CD drive. The BIOS might need to be set to boot from an external USB device.

2. If the target device will not boot, connect the USB CD drive to a USB port on the target device and reboot the target device. If the target device successfully boots from the CD drive, the BIOS is not supporting booting from a composite USB 2.0 device. Check the support Web site from the target device manufacturer to determine if a later BIOS is available that might support booting from a composite USB 2.0 device. If so, update the BIOS and retry.
3. If the target device is not capable of booting from an external USB 2.0 device, try the following methods to remotely boot this target device:
 - Some BIOS versions provide an option to limit USB speeds. If this option is available to you, change the USB port setting to “USB 1.1” or “Full Speed” mode and try booting again.
 - Insert a USB 1.1 card and try booting again.
 - Insert a USB 1.1 Hub between the VCO cable and the target device and try booting again.
 - Contact the manufacturer of the target device for information on availability or plans of a BIOS revision that will support booting from a composite USB 2.0 device.

Virtual media restrictions

The following list specifies restrictions for using virtual media:

- The GCM2, GCM4, or LCM2 virtual media appliances only support connection of USB 2.0 diskette drives, flash drives, and CD drives.
- The VCS only supports mapping of USB 2.0 and USB 1.1 diskette drives and flash drives connected to the client computer.

Appendix C: Keyboard and mouse shortcuts

This appendix lists the keyboard and mouse shortcuts that can be used in Explorer.

Table C.1: Divider pane keyboard and mouse shortcuts

Operation	Description
F6	Navigates between the split-screens and gives focus to the last element that had focus.
F8	Gives focus to the divider.
Left or Up Arrow	Moves the divider left if the divider has the focus.
Right or Down Arrow	Moves the divider right if the divider has the focus.
Home	Gives the right pane of the split-screen all of the area (left pane is hidden) if the divider has the focus.
End	Gives the left pane of the split-screen all of the area (right pane is hidden) if the divider has the focus.
Click + Mouse Drag	Moves the divider left or right.

Table C.2: Tree view control keyboard and mouse shortcuts

Operation	Description
Mouse Single-click	Deselects the existing selection and selects the node the mouse pointer is over.
Mouse Double-click	Toggles the expand and collapse state of an expandable node (a node with sublevels). Does nothing on a leaf node (a node with no sublevels).
Up Arrow	Deselects the existing selection and selects the next node above the current focus point.
Down Arrow	Deselects the existing selection and selects the next node below the current focus point.
Spacebar	Alternately selects and deselects the node that currently has the focus.
Enter	Alternately collapses and expands the node that has focus. Only applies to nodes that have sublevels. Does nothing if a node has no sublevels.
Home	Deselects the existing selection and selects the root node.
End	Deselects the existing selection and selects the last node visible in the tree.

Table C.3: Unit list keyboard and mouse operations

Operation	Description
Enter or Return	Starts the default action for the selected unit.
Up Arrow	Deselects current selection and moves selection up one row.
Down Arrow	Deselects current selection and moves selection down one row.
Page Up	Deselects current selection and scrolls up one page, then selects the first item on the page.
Page Down	Deselects current selection and scrolls down one page, then selects the last item on the page.
Delete	Performs the Delete function. Works the same as the Edit > Delete menu function.
Ctrl + Home	Moves the focus and the selection to the first row in the table.
Ctrl + End	Moves the focus and the selection to the last row in the table.
Shift + Up Arrow	Extends selection up one row.
Shift + Down Arrow	Extends selection down one row.
Shift + Page Up	Extends selection up one page.
Shift + Page Down	Extends selection down one page.
Shift + Mouse Click	Deselects any existing selection and selects the range of rows between the current focus point and the row the mouse pointer is over when the mouse is clicked.
Ctrl + Mouse Click	Toggles the selection state of the row the mouse pointer is over without affecting the selection state of any other row.
Mouse Double-click	Starts the default action for the selected unit.

Appendix D: Ports used by the software

Table D.1 lists the port numbers that the software uses to communicate with certain appliances. This information can be used to configure firewalls to let VCS operate in the networks.

Table D.1: Ports Used by VCS

Port Number	Appliance	Type	Purpose
3211	GCM4, GCM2, or RCM	TCP	Proprietary management protocol
3211	GCM4, GCM2, or RCM	UDP	Proprietary install and discovery protocol
2068	GCM4, GCM2, or RCM	TCP	Encrypted keyboard and mouse data
2068	GCM4 or GCM2	TCP	Digitized video data
2068	GCM4 or GCM2	TCP	Virtual media
8192	RCM	TCP	Digitized video data

Appendix E: Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your eServer™ or IntelliStation® system or optional device, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the Hardware Maintenance Manual and Troubleshooting Guide or Problem Determination and Service Guide on the IBM Documentation CD that comes with your system.

NOTE: For some IntelliStation models, the Hardware Maintenance Manual and Troubleshooting Guide is available only from the IBM support Web site.

- Go to the IBM support Web site at <http://www.ibm.com/pc/support/> to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with eServer and IntelliStation systems also describes the diagnostic tests that you can perform. Most eServer and IntelliStation systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your IBM eServer or IntelliStation system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/pc/support/> and follow the instructions. Also, some documents are available through the IBM Publications Ordering System at <http://www.elink.ibm.com/public/applications/publications/cgibin/pbi.cgi>.

Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM eServer and IntelliStation systems, optional devices, services, and support. The address for IBM xSeries and BladeCenter information is <http://www.ibm.com/eserver/xseries/>. The address for IBM IntelliStation information is <http://www.ibm.com/pc/us/intellistation/>.

You can find service information for IBM systems and optional devices at <http://www.ibm.com/pc/support/>.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with xSeries servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see <http://www.ibm.com/services/sl/products/>.

For more information about Support Line and other IBM services, see <http://www.ibm.com/services/>, or see <http://www.ibm.com/planetwide/> for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through IBM Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. See <http://www.ibm.com/planetwide/> for support telephone numbers, or in the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

Appendix F: Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Edition notice

© Copyright International Business Machines Corporation 2005. All rights reserved.

U.S. Government Users Restricted Rights — Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	NetBAY
IBM (logo)	PS/2
ServerProven	eServer
IntelliStation	

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adaptec and HostRAID are trademarks of Adaptec, Inc., in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

INDEX

A

Access levels

GCM2 and GCM4 appliances **71**

AMP

about **55**

accessing **18, 55**

changing global network values **56**

changing global session values **60**

exiting **56**

managing user sessions **75**

rebooting the appliances **89**

resynchronizing the device list **82**

upgrading firmware **86**

user accounts **71**

viewing CO cable information **76**

viewing device connection information **82**

See also *Databases*, *Firmware*, *SNMP*, and *User accounts*

Appliances

accessing **18**

adding **15**

assigning **27**

deleting **28**

renaming **29**

Assignment **27**

Authentication (CCM appliances) **62**

B

Browser

configuring application to launch **25**

configuring generic appliance URL **22**

requirements **8**

C

CO cables

adding **16, 84**

upgrading firmware individually **89**

upgrading firmware simultaneously **88**

viewing information **76, 82**

Components of VCS **2**

Connection

multiple connections **4**

Credentials

setting for device from Thumbnail Viewer **41**

credentials **18, 19**

cached **18, 19**

Custom label fields in Explorer **24**

D

Databases

exporting the local VCS database **30**

loading the local VCS database **30**

restoring a GCM2 and GCM4 appliances
configuration database **91**

restoring GCM2 and GCM4 appliances user
database **92**

saving a GCM2 and GCM4 appliances
configuration database **90**

saving a GCM2 and GCM4 appliances user
database **92**

saving the local VCS database **30**

VCS local database **29**

DCHP (GCM2 and GCM4 appliances) **56**

Department

- deleting **28**
- renaming **29**
- specifying in properties **21**

Devices

- accessing **19**
- assigning **27**
- auto searching in Unit list **20**
- changing network properties **22**
- deleting **28**
- name displays **4**
- naming **4**
- renaming **29**
- resynchronizing the list (GCM2 and GCM4 appliances) **82**
- searching in local database **20**
- viewing connection information (GCM2 and GCM4 appliances) **82**
- viewing connection properties **23**

DirectDraw **25**

E

Encryption

- keyboard/mouse for GCM2 and GCM4 appliances **60**
- specifying for virtual media sessions **52**
- when saving/restoring configuration databases (GCM2 and GCM4 appliances) **90**

Explorer

- accessing appliances **18**
- accessing devices **19**
- adding appliances **15**
- changing custom field labels **24**
- changing properties **21**
- changing the view on startup **25**
- keyboard and mouse shortcuts **96**
- window features **13**

F

Features and benefits **1**

Firmware

- displaying GCM2 and GCM4 appliances and CO cable version numbers **86**
- upgrading CO cables individually **89**
- upgrading CO cables simultaneously **88**
- upgrading GCM2 and GCM4 appliances **87**

Folders

- assigning a unit to **27, 28**
- creating **26**
- deleting **28**
- renaming **29**

Full screen mode (Video Viewer) **43**

G

Gateway

- changing for GCM2 and GCM4 appliances **56**

GCM2 and GCM4 appliances

- accessing **18**
- adding **15**
- quick setup **11**
- See also *AMP*

GCM2 and GCM4 database **90, 91**

Glossary **3**

H

Hardware requirements **7**

I

Installation **8**

IP address

- changing for GCM2 and GCM4 appliances **56**

K

Keyboard

configuring encryption level for GCM2 and GCM4 appliances **60**
shortcuts in Explorer **96**

L

LAN speed (GCM2 and GCM4 appliances) **56**

LDAP

Active Directory **63, 70**
authentication **63**
query modes **68**
query parameters **66**
search parameters **65**
server parameters **64**

Licensed options **86**

Location

assigning a unit to **27, 28**
specifying in properties **21**

Lock-out. See *Security lock-out*

M

Macros (Video Viewer)

displaying a macro group **49**
sending **49**
using **48**

Microsoft Windows

installing on **8**
launching on **10**
supported operating systems **7**
uninstalling on **9**

Mouse (Video Viewer)

adjusting options **45**
aligning cursor **42**
changing cursor setting **45**
realigning **46**
setting encryption level **60**

setting scaling **46**

Mouse shortcuts in Explorer **96**

Multiple connections **4**

N

Network settings

GCM2 and GCM4 appliances **56**

O

Operating systems **7**

P

Ports used by VC software **98**

Preemption

considerations in virtual media sessions **50**

Preemption of local user on Video Viewer **36**

Properties

about changing in Explorer **21**
changing general properties in Explorer **21**
changing information properties in Explorer **22**
changing network properties in Explorer **22**

Q

Quick setup

GCM2 and GCM4 appliances **11**
VCS **10**

R

Reboot

GCM2 and GCM4 appliances **89**

Red Hat Linux

installation on **8**
launching on **10**
supported operating systems **7**
uninstalling on **9**

Requirements

virtual media **50**

Resynchronization **82**

S

Scaling (Video Viewer)

enabling automatic or manual **43**

setting for mouse **46**

Scan mode (Video Viewer)

accessing **39**

changing the thumbnail size **40**

disabling a device thumbnail in the scan sequence **40**

enabling a device thumbnail in the scan sequence **40**

launching a session to a device **40**

setting device credentials **41**

Security lock-out

GCM2 and GCM4 appliances **74**

Sessions

closing a virtual media session **54**

Site

assigning a unit to **27, 28**

deleting **28**

renaming **29**

specifying in properties **21**

SNMP (GCM2 and GCM4 appliances)

configuring general settings **78**

enabling/disabling traps **80**

using **78**

Subnet mask

changing for GCM2 and GCM4 appliances **56**

T

Time-out values

Video Viewer sessions **60**

Type

deleting **28**

renaming **29**

specifying in properties for devices **21**

U

User accounts (GCM2 and GCM4 appliances)

about locking/unlocking **74**

access levels **71**

adding **72**

deleting **73**

enabling/disabling security lock-out **74**

modifying **72**

unlocking **74**

User sessions

GCM2 and GCM4 appliances **75**

V

VCO cables

required for virtual media **50**

VCS

about **1**

installing **8**

ports used **98**

quick setup **10**

system components **2**

Video Viewer

about **31**

accessing **31**

adjusting the view **36, 43**

changing session time-out value **60**

closing a session **32**

enabling automatic/manual scaling **43**

enabling/disabling DirectDraw **25**

enabling/disabling full screen mode **43**

macros **48**

preempting local user **36**
refreshing the screen **42**
See also *Macros*, *Mouse* and *Scan mode*
window features **32**

Virtual media

closing a session **54**
displaying drive details **53**
encryption level **52**
locking to KVM session **51**
mapped drive access mode **52**
mapping drives **52**

requirements **50**
reserved sessions **50**
resetting USB devices on the target device **53**
session settings **51**
sharing and preemption considerations **50**
unmapping drives **53**
window **50**

W

Window features

Explorer **13**
Video Viewer **32**

