Virtual Console Software

Installation and User's Guide

Virtual Console Software Installation and User’s Guide

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Product overview

About IBM Virtual Console Software

With IBM® Virtual Console Software (VCS), a cross-platform management application, you can add and manage multiple switches and attached target devices. The cross-platform design offers compatibility with most commonly-used operating systems and hardware platforms. Each switch handles authentication and access control individually, placing system control at the point of need.

The software utilizes browser-like navigation with a split-screen interface, providing you with a single point of access for all switches. Use the software to manage existing switches, install a new target device, or open a session to a target device. Built-in groupings such as Devices, Sites, and Folders provide a way to select the units to view. Use the search and sort capabilities to find any unit.

Features and benefits

Easy to install and configure

Wizard-based installation and online help simplify initial system configuration. You can use the graphical interface to manage and update switches, target devices, and Conversion Option (CO) cables.

Powerful customization capabilities

You can tailor the software to fit specific system needs, using built-in groups or creating your own. You can customize unit names, field names, and icons for maximum flexibility and convenience. Use names that are meaningful to you to quickly find any target device.

Extensive switch management

The GCM16 and GCM32 firmware includes an integrated Web interface that can be used for configuring GCM16 and GCM32 switches and configuring and accessing connected target devices. You can add and manage multiple switches in one system with the software. After a new switch is added, you can configure operating parameters, control and preempt user sessions to target devices, and execute numerous control functions, such as rebooting and upgrading the switch. You can enable Simple Network Management Protocol (SNMP) traps, configure target devices, and manage user databases.

You can use the software to manage the following IBM switches:

- IBM Global 2x16 Console Manager (GCM16): The GCM16 switch includes two digital ports for KVM-over-IP access, 16 ARI ports for connecting CO cables and target devices, adds a second dedicated local path for the ACI port, smart card support, two power receptacles, and one VGA and four USB ports, virtual media capability for one local user and up to four remote users.
- IBM Global 2x32 Console Manager (GCM32): The GCM32 switch includes four digital ports for KVM-over-IP access, 32 ARI ports for connecting CO cables and target devices, adds a second dedicated local path for the ACI port, smart card support, two power receptacles, and one VGA and four USB ports, virtual media capability for one local user and up to four remote users.

Authentication and authorization

Administrators can configure each switch either to use local user databases on the switch or to use databases on an LDAP server for user authentication and authorizations checking. Local authentication is always used, either as the primary authentication method or as a fallback method when LDAP authentication is configured.

The switch can be configured to use LDAP for authentication only with the local databases used for authorizations checking.

After users log in to a switch, 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. From the Explorer, you can view the switches and target devices defined in the local database. Built-in groupings such as Appliances and Devices provide different ways 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 Explorer Devices list, you can select a device from the list of target devices and start a KVM session with the device. Starting a KVM session brings up a Video Viewer. From the Explorer Appliances list, you can select a switch to configure.

Video Viewer

Users access and manage target devices through 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 to connect to target devices on GCM16 and GCM32 switches. For more details, see "About the Video Viewer" on page 41.

The Video Viewer also provides access to the Virtual Media window. You can use the Virtual Media window to map a physical drive, such as a disk, CD-ROM, or DVD-ROM data drive, onto a target device so that the media device is available to the target device even though it is not directly connected. For more information on the Virtual Media window, see "Using virtual media" on page 61.

Glossary

The following words are used throughout this documentation:

- ACI port connection – a CAT 5 cable connection between the ARI port of a GCM16 or GCM32 switch 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 switches that allows target device management from a single KVM switch.

  For example, the tiering of an analog KVM switch under a digital KVM switch will allow keyboard and mouse input control to all target devices attached to that analog KVM switch using the VCS interface or the Web interface.

  cascade switch – an earlier-model analog KVM switch that is connected to a KCO cable attached to the ARI port of a GCM16 or GCM32 switch, allowing for integration of an existing earlier-model switch configuration with the VCS.
- **CO cable** - a Conversion Option cable that, when attached to the switch and a target device, provides additional functionality.
- **SCO cable** - a Serial Conversion Option cable that, when attached to the switch and a serial device, provides true direct serial access.
- **VCO2 cable** - Virtual Media Conversion Option G2 cable that, when attached to the switch and a server, provides additional Smart Card/CAC and high resolution support up to 1600 x 1200.
- **switching system** - a set of switches and attached target devices and CO cables.
- **target device** - equipment such as a server or router that is attached to a switch.
- **unit** - includes switches 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 switch. Also refers to any user of the switch system that has an account configured either in the user database on the switch or in the LDAP directory service on an LDAP server.
- If LDAP is used for authentication while the switch database is used for authorization, each user account must be configured in the switch database with or without administrator rights and with access to specified devices, but without a password; the same user must be configured on the LDAP server with a password.

virtual media - shared use of a USB media device that is either attached to a switch or to a remote computer that is using the Web interface to access a target device through a Web interface-enabled switch. The media device can be made available to any target device that is connected to the switch using a VCO or VCO2 cable.

Operating features

"Keyboard and mouse shortcuts" on page 70 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 switch 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 a switch is added, the target device names retrieved from the switch 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 switch.

Since the software is a decentralized management system, you can change the name assigned to a target device on the switch 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 switch 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 switch to obtain target device information.
- The Resync Wizard overwrites locally-defined target device names only if the switch target device name has been changed from the default value. Non-default target device names that are read from the switch 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.

IPv4 and IPv6 network address capabilities

The VCS application is compatible with systems using either of the currently supported Internet Protocol Versions, IPv4 (default) or IPv6. For GCM16 and GCM32 switches, you can change the network settings and select IPv4 and IPv6 mode simultaneously.

The IPv4 mode connection can be either a stateful (configuration and IP addresses are provided by the server) or a stateless (the switch normally receives the IP address and router address dynamically from the router) auto-configuration. Switch firmware upgrades and emergency boot firmware upgrades are supported for both TFTP and FTP servers while in IPv4 mode.

The IPv6 mode is a stateless, auto-configuration connection. While in IPv6 mode, switch firmware upgrades are only facilitated in FTP mode and emergency boot firmware flash downloads cannot be performed. To perform a flash download, you must temporarily connect to an IPv4 network with a TFTP server. VCS 4.0.0.0 or higher is required for IPv6 function.

CHAPTER 2

Installation and startup

Getting started

Before you install the software on a client computer, make sure that you have all the required items and that the target devices and VCS client computers are running the supported operating systems, browsers, and Java Runtime Environment.

Supplied with VCS

The VCS is shipped with switches on a Virtual Console Installation Software CD. The user documentation is available as an option on the Help menu from the VCS Explorer window.

NOTE: Make sure you have the most recent version of the VCS. Compare the version at http://www.ibm.com/support/ to the version on the VCS CD. If a newer firmware version is available, download the newer version to the client computer and install it.

Supported operating systems

Client computers running the VCS must be running one of the following operating system versions:

- Microsoft® Windows® 2003 Server with Service Pack 3 Web, Standard, and Enterprise
- Microsoft Windows 2008 Server Web, Standard, and Enterprise
- Microsoft Windows XP Professional with Service Pack 3
- Microsoft Windows Vista™ Business with Service Pack 1
- Microsoft Windows 2000 Professional with Service Pack 4
- Microsoft Windows 7 Home Premium and Professional
- Red Hat Enterprise Linux® 4.0 and 5.0 WS, ES, and AS
- SUSE Linux Enterprise Server 10 and Server 11
- Ubuntu 8 Server and Workstation

Target devices must be running one of the following operating systems:

- Microsoft Windows 2000 Server (32-bit) and Advanced Server
- Microsoft Windows XP Professional and Standard with Service Pack 3
- Microsoft Windows Server 2003 Web, Standard, and Enterprise

- Microsoft Windows Server 2008 Web, Standard, and Enterprise
- Microsoft Windows Vista Standard, Business with Service Pack 1, and Enterprise
- Microsoft Windows 7 Home Premium and Professional
- Netware 6.5 (32-bit)
- Red Hat Enterprise Linux 4.0 and 5.0 with WS, ES, and AS
- Solaris Sparc 10 (64-bit)
- SUSE Linux Enterprise Server 10 and Server 11
- Ubuntu 8 Server and Workstation
- VMWare ESX 3 and ESX 4 (32-bit)

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

Computers used to access the Web interface and client computers running the VCS must have one of the following browsers installed:

- Microsoft® Internet Explorer version 6.x SP1 or later
- Firefox 2.0 or later

JRE requirements

Computers used to access target devices using the Web interface and client computers running the VCS must have Java Runtime Environment (JRE) 1.6.0_11 or higher installed. The switch will attempt to detect if Java is installed on your PC. If Java is not installed, download it from http://www.java.com, then associate the JNLP file with Java WebStart.

Installing the software

During installation, you are prompted to select the destination location for the VCS application. You can select an existing path or type a directory path. The default path for Windows operating systems is C:\Program Files. The default path for Linux operating systems is /usr/lib.

If you enter a pathname 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.

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

1. Make sure you have the most recent version of the VCS by comparing the version at http://www.ibm.com/support/ to the version on the VCS CD.
2. If a more recent version is available, download the newest VCS and complete the following steps.
    a. Navigate to the directory where you downloaded the VCS.
    b. Double-click the setup.exe program name or icon and go to step 4.
3. If you are installing the software from the CD, insert the VCS CD into the CD drive, and complete one of the following steps:
    a. If the setup program starts automatically, go to go to step 4.

       If AutoPlay is supported and enabled, the setup program starts automatically.

    b. If AutoPlay does not start the setup program, locate the CD drive icon on the desktop, double-click the icon to open the CD folder, and double-click the **setup.exe** program file.

       -or-

       Select **Run** on the **start** menu, and enter the following command to start the install program (replace “drive” with the letter of the CD drive):

       ```
       drive:\VCS\win32\setup.exe
       ```
4. Follow the on-screen instructions.

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

1. Make sure you have the most recent version of the VCS by comparing the version at http://www.ibm.com/support/ to the version on the VCS CD.
2. If a more recent version is available at www.ibm.com, download the newer VCS and complete the following steps.
    a. Open a command window and navigate the download directory, for example:

       ```
       % cd /home/username/temp
       ```

    b. Enter the following command to start the install program:

       ```
       % sh .setup.bin
       ```
3. If you are installing the software from the CD, insert the VCS CD into the CD drive and perform one of the following steps:
    a. Continue to step 4 if the CD mounts automatically.

       With the Red Hat and SUSE Linux distributions, the CD is usually mounted automatically.

    b. If the CD does not mount automatically, 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 filename and *mount_point* is the directory on which to mount the CD. Typical default values include "/mnt/cdrom" and "/media/cdrom."

See the Linux operating system documentation for the specific mount command syntax to use.

4. Open a command window and navigate to the CD mount point. For example:

```
% cd /mnt/cdrom
```

5. Enter the following command to start the install program:

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

6. Follow the on-screen instructions.

Uninstalling the software

To uninstall the VCS 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 VCS 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 Windows 32-bit operating 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 VCS 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 /usr/lib.
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.

Starting the software

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

- If the /usr/lib directory is in the PATH, enter the command:

  ```
  % ./IBM_Virtual_Console_Software
  ```
- Change directories to /usr/lib and enter the following command:

  ```
  % ./IBM_Virtual_Console_Software
  ```
- If a desktop shortcut was created on installation, double-click the shortcut.

Configuring switches and user access to target devices

This section provides an overview of configuration steps. Details are provided in other chapters.

For switch-specific information, see the *Installation and User’s Guide* for the switch.

To add switches, complete the following steps:

1. Install the VCS on one or more client computers.
2. Open the VCS on a client computer.
3. Use the Explorer to set unit properties, options, and other customization as needed.
4. Configure the names of all target devices using the local GUI interface.
5. Repeat steps 3 through 6 for each switch you want to manage.
6. After one VCS environment is set up, select **File > Database > Save** to save a copy of the local database with all the settings.
7. From the VCS on a second computer, select **File > Database > Load** and browse to find the saved file. Select the file and then click **Load**. Repeat this step for each client computer that you want to setup.
8. To access a target device attached to an switch, 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).

You can configure user accounts either through the VCS or through the GCM16 or GCM32 switch integrated Web interface.

For how to use the Web interface to create user accounts, see the *Global Console Manager GCM16 and GCM32 Installation and User’s Guide*.

To configure a GCM16 or GCM32 switch, complete the following steps:

1. Connect a terminal or PC running the terminal emulation software to the configuration port on the back panel of the switch using the supplied serial cable. The terminal should be set to 9600 baud, 8 bits, 1 stop bit, no parity, and no flow control.
2. Plug the supplied power cord into the back of the switch and then into an appropriate power source.
3. When the power is switched on, the Power indicator on the rear of the unit will blink for 30 seconds while performing a self-test. Press the <Enter> key to access the main menu.

To configure the Remote Console Switch hardware:

1. You will see the **Main** menu with eleven options. Select option 1, **Network Configuration**.
2. Select option 1 to set your network speed. Once you enter your selection, you will be returned to the **Network Configuration** menu.
3. Select option 2 to open the **IP Configuration** menu.
4. Type the appropriate number to select one of the following types of IP addresses: 1: **None**, 2: **IPv4 Static**, 3: **IPv4 Dynamic**, 4: **IPv6 Static**, or 5: **IPv6 Dynamic**.
5. Select options 3-5 from the **Terminal Applications** menu, in turn, to finish configuring your Remote Console Switch for IP address, Netmask, and Default Gateway.
6. Once this is completed, type Ø to return to the main menu.

To configure the HTTP and HTTPS ports:

1. You will see the **Main** menu with eleven options. Select option 10, **Set Web Interface Ports** to open the **Web Interface Port Configuration Menu**.
2. Select option 1 to set the port numbers. Type the port numbers you wish to use for the HTTP port and the HTTPS port.
3. If the values are correct for your network, type <Y> and press the <Enter> key.
4. At the local user station, input the target device names.

Mouse Acceleration

If you are experiencing slow mouse response during a remote video session, deactivate mouse acceleration in the operating system of the target device and adjust mouse acceleration on each target device to **Slow** or **None**.

Web Interface Installation and Setup

Once you have installed a new switch, you can use the web interface to configure unit parameters and launch video sessions.

Supported Browsers

The web interface supports the following browsers:

- Microsoft Internet Explorer® version 6.x SP1 or later

- Firefox version 2.0 or later

Launching the On-board Web Interface

To launch the web interface:

1. Open a web browser and type the IP address of the switch using the local Web interface.

NOTE: If you changed the default HTTP/HTTPS ports in the serial console and are using an IPv4 address, use IP address format: https://<ipaddress>:<port#>, where “port#” is the number you specified in the serial console. If you are using an IPv6 address, use format: https://[<ipaddress>]:<port#>, where “port#” is the number you specified in the serial console. If you are using an IPv6 address, you must enclose the address in square brackets.

2. The log in window opens. Type your username and password and click **OK**.
3. The web interface opens and displays the **Connections** tab.

NOTE: To use the Web interface, Java Runtime Environment (JRE) version 1.6.0_11 or higher must be installed on your computer. The KVM Switch will attempt to detect Java on your PC. If Java is not installed, download it from http://www.java.com, then associate the JNLP file with Java WebStart.

NOTE: Once you have logged in to the web interface, you will not have to log in again when launching new sessions unless you have logged out or your session has exceed the inactivity timeout specified by the administrator.

CHAPTER 3

VCS Explorer

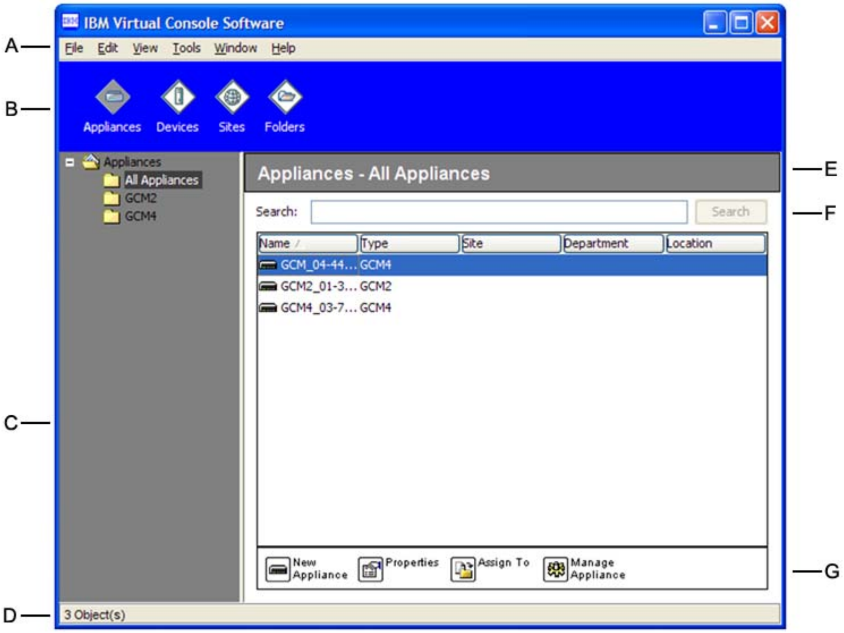
About the VCS Explorer

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.

Window features

When you start the software, the main Explorer window opens. 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 a switch is selected or what task is to be completed. Figure 3.1 on page 16 shows the window areas; descriptions follow in Table 3.1 on page 16.

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 17.



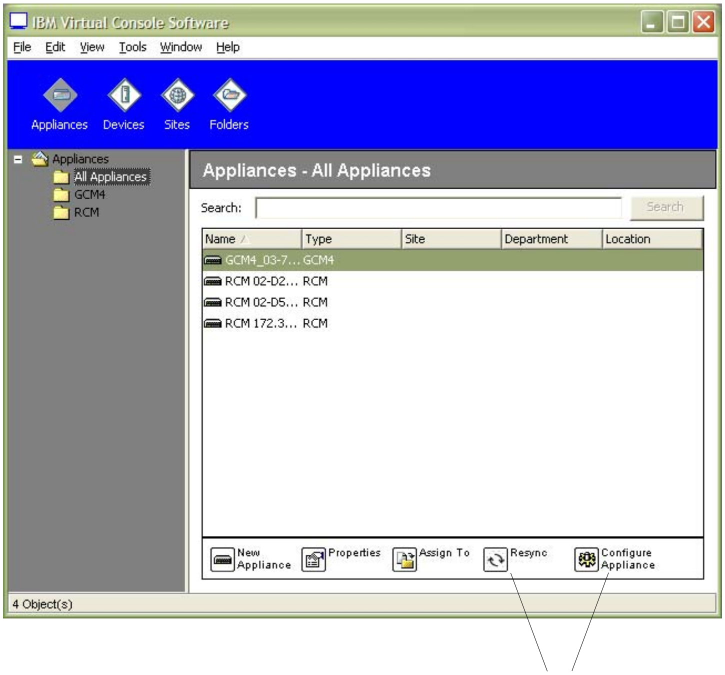
Name	Type	Site	Department	Location
GCM_04-44...	GCM4			
GCM2_01-3...	GCM2			
GCM4_03-7...	GCM4			

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, switches, 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.

If a selected switch is enabled for the Web interface, two additional buttons appear at the bottom of the Explorer window: Resync and Configure Appliance.



Name	Type	Site	Department	Location
GCM4_03-7...	GCM4			
RCM 02-D2...	RCM			
RCM 02-D5...	RCM			
RCM 172.3...	RCM			

Additional buttons

Figure 3.2: Additional Explorer buttons when a switch is enabled for the Web interface

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 70 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 31.

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 a switch

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

To manually add a switch 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**.

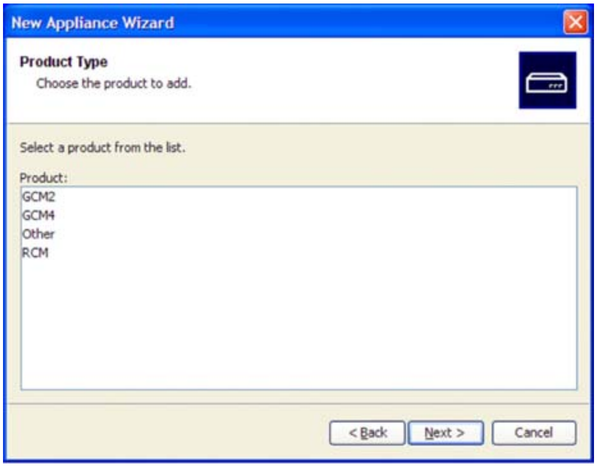


Figure 3.3: New Appliance Wizard

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

   The software searches for the indicated unit as well as all the powered CO cables and target device names you associated with it in the local interface, if any.

   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 switch and the tiered switch types to which they are connected, if any. When this window first opens, all switches are set to **None**. Detected switches 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.

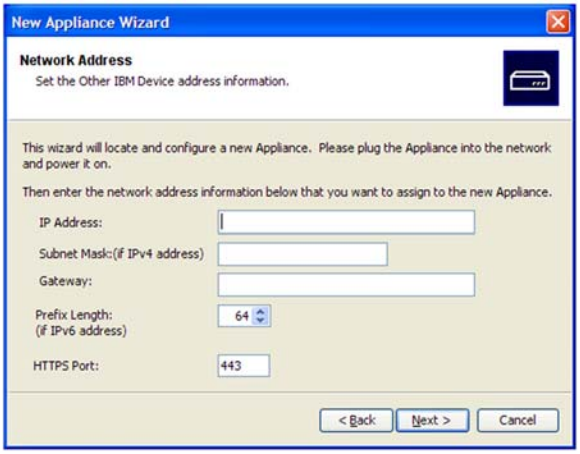
b. Associate the applicable cascade switch types from the pull-down menus for each CO cable that has a cascade switch attached.

6. When you reach the final page of the Wizard, click **Finish** to exit the Wizard and return to the main window. The switch is now included in the Unit list.

To manually add a new switch 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 switch does not have an assigned IP address, then click **Next**.
3. The Network Address window opens. Type the IP address, subnet mask (if using IPv4 mode) or prefix length (if using IPv6 mode), and gateway you wish to assign to the unit and click **Next**.



New Appliance Wizard

Network Address

Set the Other IBM Device address information.

This wizard will locate and configure a new Appliance. Please plug the Appliance into the network and power it on.

Then enter the network address information below that you want to assign to the new Appliance.

IP Address:

Subnet Mask:(if IPv4 address)

Gateway:

Prefix Length: (if IPv6 address) 64

HTTPS Port: 443

Figure 3.4: Network Address window

4. The software searches for any switches that do not have assigned IP addresses. Select the unit to add from the list of new switches 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 switch. Click **Next**.

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

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 switch 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 switch is now included in the Unit list.

To discover and add a switch 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. Complete one of the following steps:
   - If using IPv4 mode, select Use IPv4 address range. Type the range of IP addresses you wish to search on the network in the To Address and From Address boxes. Use IP address dot notation: xxx.xxx.xxx.xxx.

     -or-
   - If using IPv6 mode, select Use IPv6 subnet, and specify the IPv6 address and network prefix. Use the IPv6 "address/prefix" format.
3. You may also change the default HTTP and HTTPS port numbers, if the switch has changed from the default on the serial console, by typing the new port numbers in the **HTTP Port** and **HTTPS Port** fields. Click **Next** to continue.
4. 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 switches found (for example, 21 of 100 addresses probed: 3 switches found). If one or more new switches are discovered, the Wizard shows the Select Appliances to Add page. From this page, you can select the switches to add to the local database.

     -or-
   - If no new switches 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 switches manually.
5. Select one or more switches 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 switches you want to add, click **Next**.
6. The Adding Appliances progress bar window opens. Once all of the switches 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 switch is now visible in the Unit list.

If one or more switches 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 switches that you selected and the status for each. The status indicates if a switch was added to the local database and if not, why the process failed. Click **Done** when you are finished reviewing the list.

If a switch 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 switch.

Accessing switches

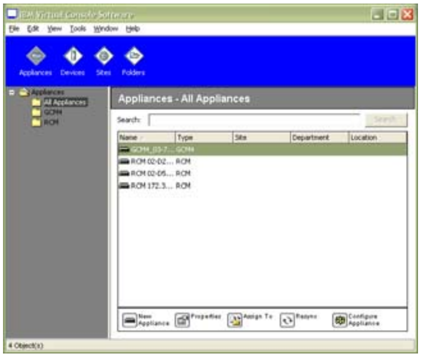
Clicking the **Appliances** button opens a list of the switches currently defined in the local database. The Group Selector pane is visible if two or more switch types are defined. Click **All Appliances** or click on a folder to view all switches of a particular type.

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**.

To log in to a switch, complete the following steps:

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



Name	Type	Site	Department	Location
GCM4_03-7...	GCM4			
RCM 02-D2...	RCM			
RCM 02-D5...	RCM			
RCM 172.3...	RCM			

Figure 3.5: Appliances window in the Explorer

2. Complete one of the following steps:
   - Double-click on a switch in the Unit list.
   - Highlight the name of a switch. On the Web interface, click the **Configure Appliance** button.

- Right-click on a switch. A pull-down menu opens. Select either **Manage Appliance** or **Configure Appliance** from the pop-up menu.
- Select a switch in the list and press Enter.

3. If a user name and password prompt opens, type the user name and password. [If this is the first switch 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 switch.
   - Click **Cancel** to exit without logging in.

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

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

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.

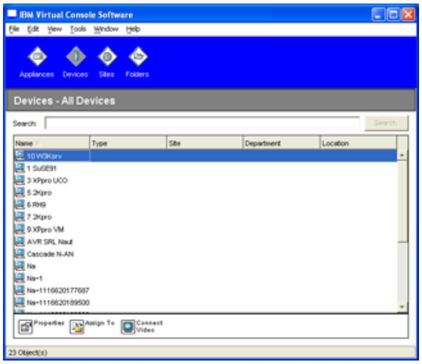
When you select a device and click the **Connect Video** button, the Video Viewer launches. The Video Viewer allows you full keyboard, video and mouse control over a device. If a URL has been defined for a given device, then the **Browse** button will also be available. The **Browse** button will launch the configured Web browser, if any, or default browser to the defined URL for that device.

For more information, see "Customizing properties" on page 24 and "Customizing options" on page 30.

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 50.

To access a target device, complete the following steps:

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



Name	Type	Site	Department	Location
10 W3Ksrv				
1 SuSE91				
3 XPpro UCO				
5 2Kpro				
6 RH9				
7 2Kpro				
9 XPpro VM				
AVR SRL Naut				
Cascade N-AN				
Na				
Na-1				
Na-1116620177687				
Na-1116620189500				

Figure 3.6: Devices in the Explorer

2. Complete one of the following steps:
   - Double-click on a target device in the list.
   - Select a target device, and then click the connection button: **Connect Video** if connected to a switch 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 switch 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 Devices list, complete the following steps:

1. Click the **Devices** button, then click on any item in the 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, and if you have greater privileges than the primary user and preemption has been configured by an administrator, you can preempt the user so you can have access to that target device, or request a shared session with that user. For more information, see "Using preemption" on page 45 and **"Using digital share mode**" on page 48.

Launching the VNC or RDP viewer

The Explorer supports user-defined Virtual Network Computing (VNC) and Remote Desktop Protocol (RDP) viewers. To launch either the VNC or RDP viewer, select the Server tab from the Explorer. Select a server from the units list, then click on either the VNC or RDP button at the bottom right of the screen.

Customizing properties

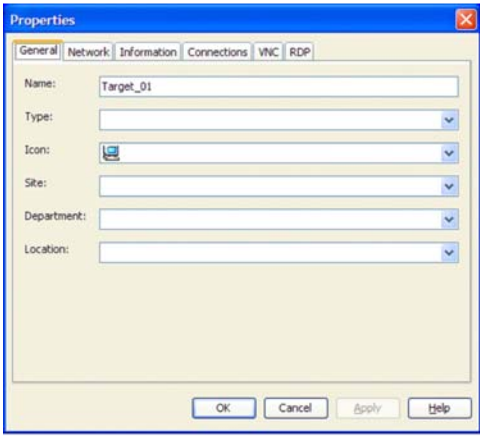
The Properties window in the Explorer contains the following tabs: **General**, **Network**, **Information**, if the selected unit is a device, **Connections**, and for viewer applications, **VNC** and **RDP**. Use these tabs to view and change properties for the selected unit.

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 30.)

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.



Name: Target_01

Figure 3.7: 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 switch database might contain a different name for this unit.)
4. The **Type** field is read-only for switches. 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.

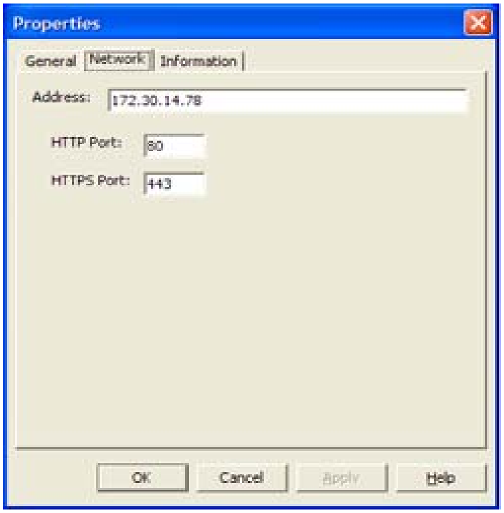
Network properties

For a switch, network properties include the address of the switch.

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.



Address: 172.30.14.78

HTTP Port: 80

HTTPS Port: 443

Figure 3.8: Network properties tab window

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 (switches only), enter the switch address in IP dot notation or 1 to 128 character host name. You may use either an IPv4 or an IPv6 address. The address cannot be blank, a loopback address, all zeros or a duplicate address.
5. In the **Browser URL** field (devices only), enter a 1 to 256 character URL for establishing a browser connection.
6. Type the HTTP and HTTPS port numbers in the **HTTP Port** and **HTTPS Port** fields, respectively, if the port numbers were changed for the Remote Console Switch in the serial console.
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.

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.

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.

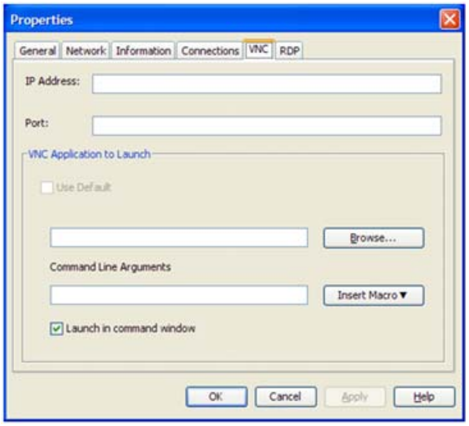
To view connections properties, complete the following steps:

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 to view the connections of the server. Connections properties are available only for servers and are read-only. The display indicates the physical connection path that is used to access this device and the connection type, such as video.
4. When finished, click **OK** or **Cancel** to close the window.

VNC Properties

When you indicate a user-specified VNC application, you may include its command line arguments. A selection of macros is available for placement in the command line; this may be useful for automatic replacement of variables such as IP address, port number, user name and password. For VNC commands that do not provide their own GUI, such as those for computers running Windows, Linux and Unix® operating systems, you can launch the VNC application from within an OS command window.



□ Use Default

☑ Launch in command window

Figure 3.9: VNC Properties tab

To change VNC properties:

1. Select a switch or server in the unit list.
2. Select **View — Properties** from the Explorer.

   — or —

   Click the **Properties** task button.

   — or —

   Right-click on the unit. Select **Properties** from the pop-up menu.

   The Properties dialog box appears.
3. Click the **VNC** tab.
4. For servers only, in the IP Address field, enter an IP address in dot notation or a 1-128 character domain name. You may use either an IPv4 or IPv6 IP address. Duplicate addresses are allowed. Spaces are not allowed.
5. In the Port field, enter a port number in the range 23-65535. If blank, port 23 is used.
6. Enable or disable the **Use Default** check box. When this setting is enabled, the default global setting specified in Options will be used and all other portions of the VNC Application to Launch area are disabled.

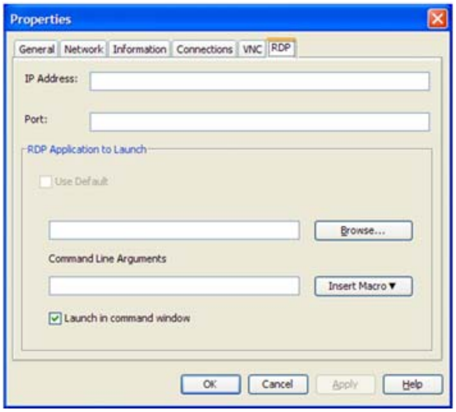
7. Enter the directory path and name or click the **Browse** button to locate the path and name.
8. Enter command line arguments in the box below the path and name.

   — or —

   To insert a predefined macro at the cursor location in the command line, click the **Insert Macro** list box and select a macro from the drop-down menu. The Explorer will automatically replace these variables when the application runs.
9. Enable or disable the **Launch in command window** check box. When enabled, the user-specified VNC application will be launched from within an OS command window.
10. 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.

RDP Properties

When you indicate a user-specified RDP application, you may include its command line arguments. A selection of macros is available for placement in the command line; this may be useful for automatic replacement of variables such as IP address, port number, user name and password. For RDP commands that do not provide their own GUI, such as those for computers running Windows, Linux and Unix operating systems, you can launch the RDP application from within an OS command window.



□ Use Default

☑ Launch in command window

Figure 3.10:RDP properties tab

To change RDP properties:

1. Select a switch or server in the unit list.
2. Select **View — Properties** from the Explorer.

   — or —

Click the **Properties** task button.

— or —

Right-click on the unit. Select **Properties** from the pop-up menu.

The Properties dialog box appears.

3. Click the **RDP** tab.
4. For servers only, in the IP Address field, enter an IP address in dot notation or enter a 1-128 character domain name. You may use either an IPv4 or IPv6 IP address. Duplicate addresses are allowed. Spaces are not allowed.
5. In the Port field, enter a port number in the range 23-65535. If blank, port 23 is used.
6. Enable or disable the **Use Default** check box. When enabled, the default global setting specified in Options will be used and all other portions of the RDP Application to Launch area are disabled.
7. Enter the directory path and name or click the **Browse** button to locate the path and name.
8. Enter command line arguments in the box below the path and name.

   — or —

   To insert a predefined macro at the cursor location in the command line, click the **Insert Macro** list box and select a macro from the drop-down menu. The Explorer will automatically replace these variables when the application runs.
9. Enable or disable the **Launch in command window** check box. When enabled, the user-specified RDP application will be launched from within an OS command window.
10. 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.

Customizing options

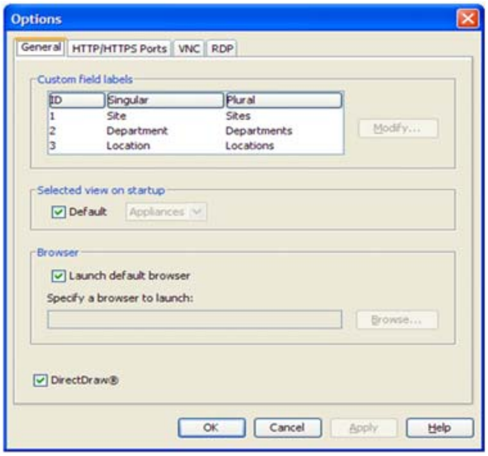
Set general options for the Explorer in the Options window. General options include custom field names, selected view on startup, browser application, and DirectDraw support. You can customize options for the Explorer, including custom name fields, default view, and default browser.

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.



Custom field labels

ID	Singular	Plural
1	Site	Sites
2	Department	Departments
3	Location	Locations

Selected view on startup

☑ Default Appliances

Browser

☑ Launch default browser

Specify a browser to launch:

☑ DirectDraw®

Figure 3.11: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. Click **OK** to save the settings or **Cancel** to exit without saving the assignment.

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:
   - 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.

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:
   - 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.

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:
   - Click another tab to change additional properties.
   - If finished, click **OK** to save the new settings.

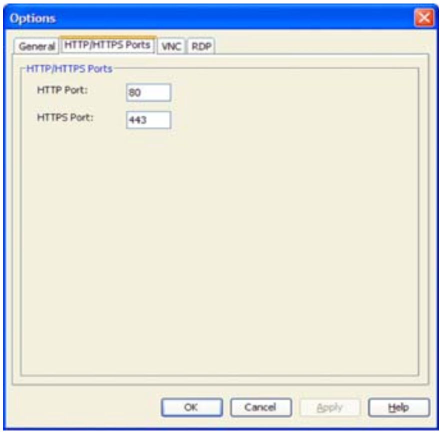
- Click **Cancel** to exit without saving the new settings.

HTTP/HTTPS options

The switch and the Explorer use port 80 as the default HTTP port and port 443 as the default HTTPS port. You can change the default port numbers used in the **HTTP/HTTPS Ports** tab of the Options dialog box.

To change HTTP/HTTPS options:

1. Select **Tools - Options** from the Explorer menu. The Options dialog box appears.
2. Click the **HTTP/HTTPS Ports** tab.
3. Enter the appropriate ports in the HTTP Port and HTTPS Port fields.
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.



HTTP Port: 80

HTTPS Port: 443

Figure 3.12: HTTP/HTTPS port window

VNC options

The Explorer supports a user-defined VNC viewer through the properties page. In the **VNC** tab you can search for a user-specific VNC application and include its command line arguments. A selection of macros is available for placement in the command line; this may be useful for automatic replacement of variables such as IP address, port number, user name and password. For VNC commands that do not provide their own GUI, such as those for computers running standard Windows, Linux and Unix operating systems, you may have the VNC application launch from within an OS command window.

NOTE: The switch will attempt to detect if Java is already installed on your PC. If it is not, in order to use the web interface, download the latest version of Java Runtime Environment from http://www.java.com and associate the JNLP file with Java WebStart.

To change VNC options:

1. Select **Tools - Options** from the Explorer. The Options dialog box appears.

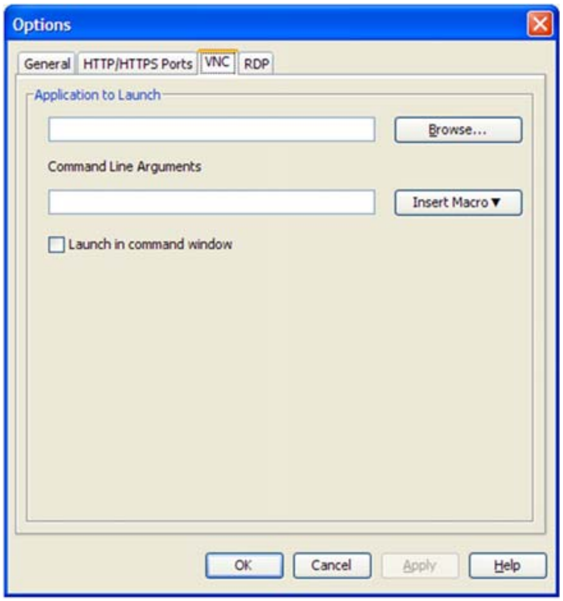


Figure 3.13:Options VNC window

2. Click the **VNC** tab.
3. In the VNC Application to Launch field, enter the directory path and name or click the **Browse** button to locate the path and name.
4. Enter command line arguments in the box below the path and name.

   — or —

   To insert a predefined macro at the cursor location in the command line, click the **Insert Macro** list box and select a macro from the drop-down menu. The Explorer will automatically replace these variables when the application runs.
5. Enable or disable the **Launch in command window** by marking or clearing the check box. When enabled, the user-specified VNC application will be launched from within an OS command window.
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.

RDP options

The Explorer supports a user-defined RDP viewer through the properties page. In the **RDP** tab you can search for a user-specific RDP application and you may include its command line arguments. A selection of macros is available for placement in the command line; this may be useful for automatic replacement of variables such as IP address, port number, user name and password. For RDP commands that do not provide their own GUI, such as those for computers running Windows, Linux and Unix operating systems, you can launch the RDP application from within an OS command window.

NOTE: The switch will attempt to detect if Java is already installed on your PC. If it is not, in order to use the web interface, download the latest version of Java Runtime Environment from http://www.java.com and associate the JNLP file with Java WebStart.

To change RDP options:

1. Select **Tools - Options** from the Explorer. The Options dialog box appears.

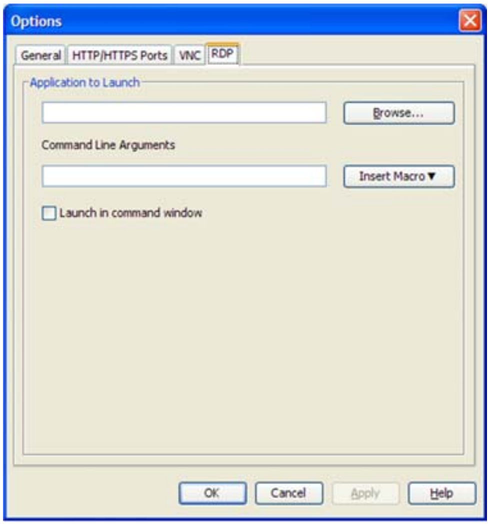


Figure 3.14:Options RDP window

2. Click the **RDP** tab.
3. In the RDP Application to Launch field, enter the directory path and name or click the **Browse** button to locate the path and name.
4. Enter command line arguments in the box below the path and name.

   — or —

To insert a predefined macro at the cursor location in the command line, click the **Insert Macro** list box and select a macro from the drop-down menu. The Explorer will automatically replace these variables when the application runs.

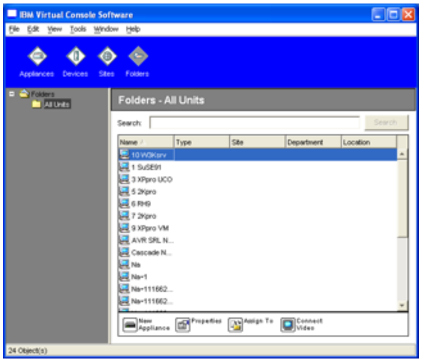
5. Enable or disable the **Launch in command window** by marking or clearing the check box. When enabled, the user-specified RDP application will be launched from within an OS command window.
6. Complete one of the following steps:
   - Click another tab to change additional properties.
   - If finished, click **OK** to save the new settings.
   - Click **Cancel** to exit without saving the new settings.

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.



Name	Type	Site	Department	Location
10 W3Ksrv				
1 SuSE91				
3 XPpro UCO				
5 2Kpro				
6 RH9				
7 2Kpro				
9 XPpro VM				
AVR SRL N...				
Cascade N...				
Na				
Na-1				
Na-111662...				
Na-111662...				

Figure 3.15: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 37. To rename or delete a folder, see "Renaming" on page 39 and "Deleting" on page 38.

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 a switch, 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 a switch 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 switch 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. 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.

CHAPTER

4

Video Viewer

About the Video Viewer

The Video Viewer is used for connecting to target devices on GCM16 or GCM32 switches.

When you connect to a target device using the VCS, 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. You can select the Toolbar Align local cursor button to enable a single cursor mode, so that only the target device cursor is visible.

From the viewer window, you can access all the normal functions of the 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.

If the target device you are attempting to access is currently being viewed by another user, you can be presented with session sharing options depending on how the administrator has configured KVM sessions and depending on your access rights.

Session sharing options

Session sharing can be configured by Admin and other users with Appliance Administrator or User Administrator rights. The first user with a KVM session with a target device is called the primary user. If another (secondary) user attempts to start a KVM session with the same target device, options for the secondary user depend on the following two conditions:

- The access rights of the two users
- Whether an administrator has configured global connection sharing

  Automatic Sharing, Exclusive Connections, and Stealth Connections all are configurable options that require connection sharing to be enabled.

Table 4.1:Session sharing definitions

Term	Definition
Automatic Sharing	Secondary users can share a KVM session without first requesting permission from primary users.
Exclusive Connection	Primary users can designate a KVM session as an exclusive connection that cannot be shared.

Table 4.1:Session sharing definitions (Continued)

Term	Definition
Stealth Connection	A stealth connection allows undetected viewing of KVM sessions. A secondary user with Appliance Administrator rights can create a stealth connection to any KVM session. A secondary user with User Administrator rights can create a stealth connection when the access rights of the secondary user are the same as or higher than the rights of the primary user. Stealth permissions follow preemption permissions.
Preempt mode	A secondary user with Appliance Administrator rights can preempt a session. a secondary user with User Administrator rights can preempt a session only when the access rights of the secondary user are the same as or higher than the rights of the primary user.

If you are an administrator, you can share a KVM session and preempt the session. If session sharing and stealth connections are enabled, an administrator can observe the session in stealth mode. For more information about access rights and session types, see "Video session indicators in the toolbar" on page 45.

Video Viewer window

The following figure shows a Video Viewer window and the default arrangement of buttons on the toolbar. (The arrangement and the types of buttons are user configurable.)

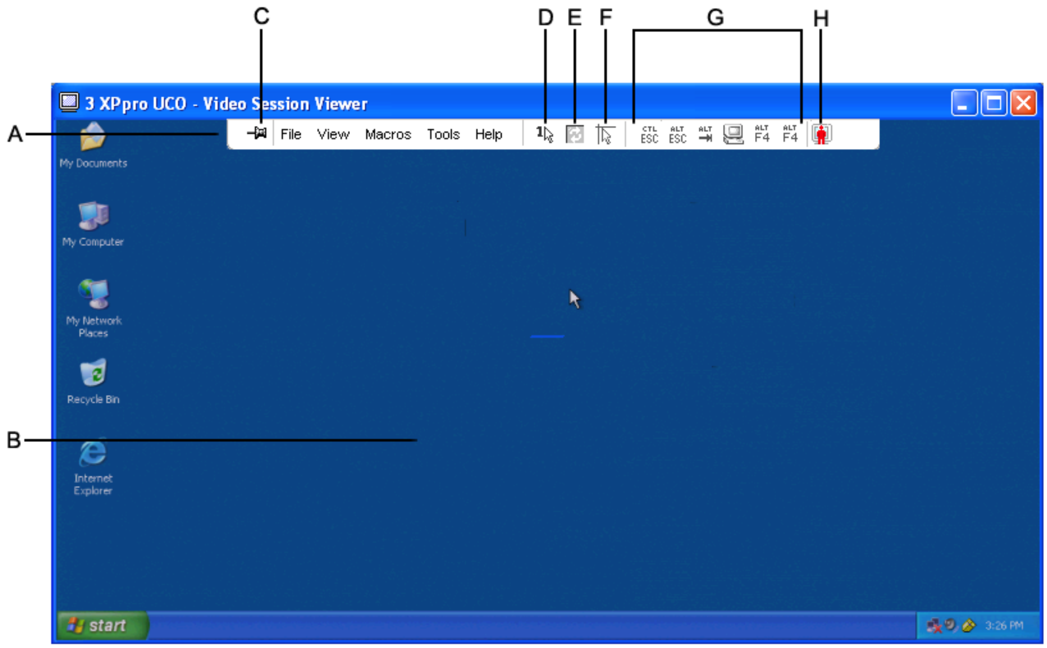


Figure 4.1: Video Viewer window

Table 4.2:Video Viewer window areas

Callout	Description
A	**Menu and toolbar.**
B	**Target device desktop**.
C	**Thumbtack icon**: When the thumbtack is locked, the toolbar is visible. When the thumbtack is unlocked, the toolbar is visible only when the mouse hovers over it.
D	**Single Cursor Mode button:** Hides the local cursor and displays only the target device cursor. Useful when administrators do not to reset mouse acceleration on each target device.
E	**Refresh Video button**.
F	**Align Local Cursor button:** Re-establishes tracking of the local cursor to the target device cursor.
G	User-selected buttons and macro commands.
H	**Connection Status indicator.**

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 can have the option to preempt the session, share the session, or observe the session in stealth mode, depending on session sharing configuration and your access rights.

   If you are not currently logged into the target device, a login prompt appears.
3. Log in if needed.

Important: A user name and password is not required for any subsequent access attempts if you do not log out, unless the system times you out.

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 indicators in the toolbar

The current type of session is indicated by an icon on the right side of the Video Viewer toolbar.

Table 4.3:Video session type icons

Session types	Icons	Description
Active (normal)	👤	A normal KVM session that is not exclusive and is not being shared.
Locked (normal)	👤	A normal KVM session and a VM session locked together.The administrator has configured locking of KVM and Virtual Media (VM) sessions. The KVM session cannot be shared or preempted, and it is not subject to inactivity timeout. It can be terminated by an administrator. For more information, see "Using virtual media" on page 61.
Exclusive	🔒	An exclusive KVM session that cannot be shared. It can be preempted or observed in stealth mode by an administrator.
Active sharing: (primary)	👥	A shared KVM session whose user is the first (primary) user to connect to the target device. The session is being shared with a secondary user or users.
Active sharing: (secondary)	👥	A shared KVM session whose user is a secondary user.
Passive sharing	👥	A shared KVM session whose secondary user can view the video ouput, but who is not allowed keyboard and mouse control over the target device.
Stealth	🕵	A KVM session in which the secondary user is able to view the video output of the target device without the permission or knowledge of the primary user. The user cannot have keyboard and mouse control over the target device. Available for administrators only.
Scanning		A session during which the current user is able to monitor up to 16 target devices in thumbnail view. No status indicator icon is visible when in scan mode.

Using preemption

Secondary users with administrator access rights that are equal to or greater than those of the primary user rights can preempt a KVM session, if an administrator has enabled session preemption.

All users sharing the session that is being preempted are warned, unless the target device is connected to an RCM switch. A primary user with administrator access rights that are equal to those of the secondary user can reject the preemption.

Table 4.4 outlines the preemption scenarios and detailed scenarios in which preemption requests can be rejected.

Table 4.4: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
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. The time period given before disconnection is defined by the Video session preemption timeout setting in the **Global - Sessions** category.

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 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.

When another user is viewing this target device, a message indicates that the target device is already involved in a KVM session.

If the switch has connection sharing enabled, you are given the option to share the session. For information about connection sharing, see "Using preemption" on page 45. 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.

3. 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.

Using exclusive mode

If session sharing and exclusive connections are enabled, you can create an exclusive KVM session. When operating a 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.

To enable exclusive KVM sessions on a switch, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on a GCM16 or GCM32 switch in the Unit list.
   - Select a GCM16 or GCM32 switch from the Unit list, then click the **Manage Appliance** button.
   - Right-click on a GCM16 or GCM32 switch in the Unit list. Select **Manage Appliance** from the pop-up menu.
   - Select a GCM16 or GCM32 switch in the Unit list and press Enter.
3. Select the **Global - Sessions** subcategory.
4. Select the **Enable Shared** Sessions check box in the **Connection Sharing** area.
5. 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.

To configure a switch 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 GCM16 or GCM32 switch in the Unit list.
   - Select a GCM16 or GCM32 switch from the Unit list, then click the **Manage Appliance** button.
   - Right-click on a GCM16 or GCM32 switch in the Unit list. Select **Manage Appliance** from the pop-up menu.
   - Select a GCM16 or GCM32 switch in the Unit list and press Enter.
3. Select the **Global - Sessions** subcategory.
4. Select **Enable Share Mode** in the **Connection Sharing** area.
5. 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.

   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 switch 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.

3. 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.

If you are not prompted to connect in share mode, either the switch to which the target device is connected is not configured to allow digital share mode sessions or it is not a GCM16 or GCM32 switch.

Using stealth mode

Administrators can connect to a target device in stealth mode to view 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.

To enable stealth KVM sessions on a switch, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on a GCM16 or GCM32 switch in the Unit list.
   - Select a GCM16 or GCM32 switch from the Unit list, then click the **Manage Appliance** button.
   - Right-click on a GCM16 or GCM32 switch in the Unit list. Select **Manage Appliance** from the pop-up menu.
   - Select a GCM16 or GCM32 switch in the Unit list and press Enter.
3. Select the **Global - Sessions** subcategory.
4. 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 switch 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 switch 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 switch the target device is connected to is not a GCM16 or GCM32 switch

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 switch 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.

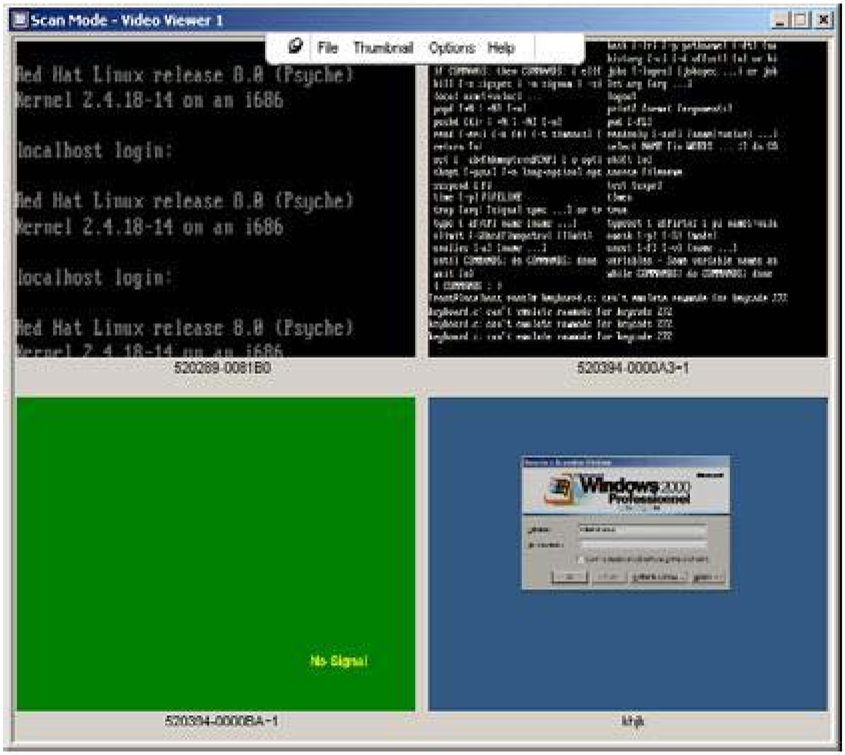
Scan mode has a lower priority than an active connection. If a user is connected to a target device, that target device is skipped in the scan sequence, and scan mode proceeds to the next target device. No login error messages are visible. After the interactive session is closed, the thumbnail is included 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.



```
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.18-14 on an i686

localhost login:

Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.18-14 on an i686

localhost login:

Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.18-14 on an i686
```

```
[illegible]
```

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.

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 1600 x 1200 (standard) or 1680 x 1050 (widescreen). 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.

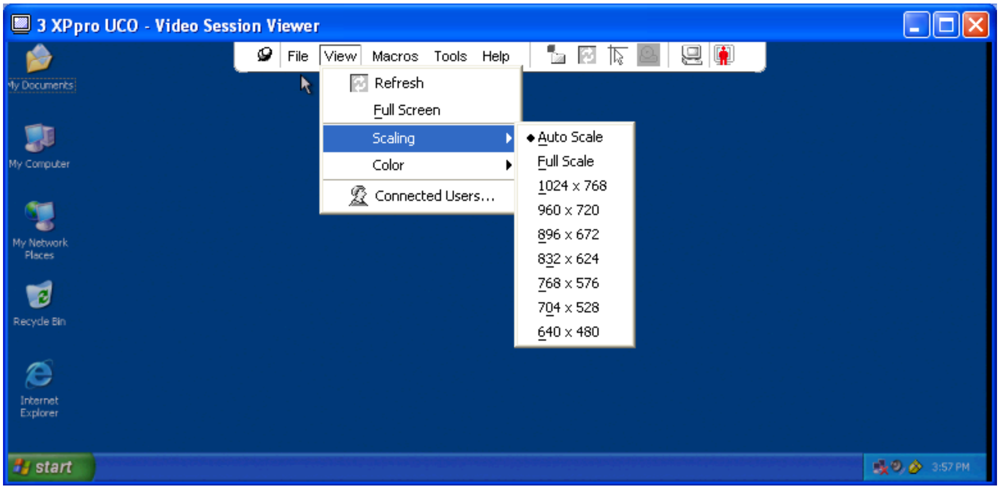


Figure 4.3: Viewer manual scale

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 your technical-support representative 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 your technical-support representative.

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 4.4; descriptions follow the figure in Table 4.5.
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.

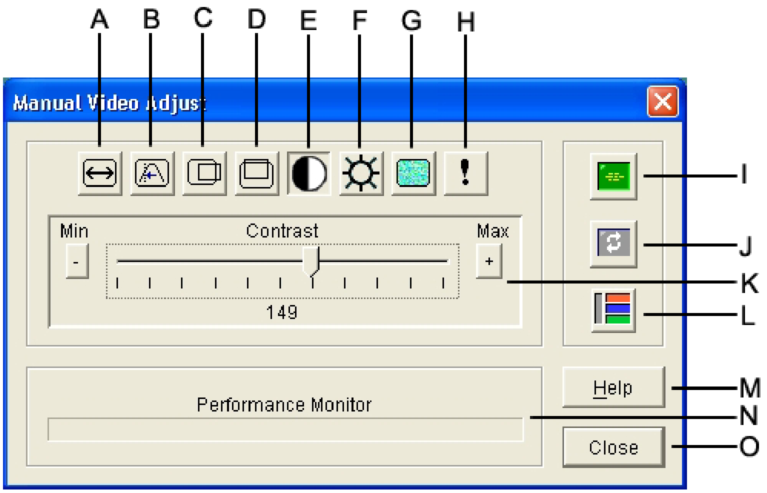


Figure 4.4: Manual Video Adjust window

Table 4.5:Manual Video Adjust window areas

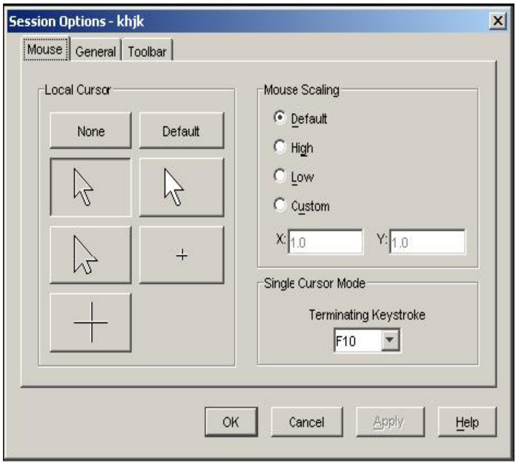
Area	Description	Area	Description
A	Image capture width	**I**	Automatic video adjustment
B	Pixel sampling fine adjust	**J**	Refresh image

Table 4.5:Manual Video Adjust window areas (Continued)

Area	Description	Area	Description
C	Image capture horizontal position	K	Adjustment bar
D	Image capture vertical position	L	Video test pattern
E	Contrast	M	Help button
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.



Session Options - khjk

Mouse | General | Toolbar

Local Cursor

Mouse Scaling
● Default
○ High
○ Low
○ Custom
X: 1.0 Y: 1.0

Single Cursor Mode
Terminating Keystroke: F10

Figure 4.5: 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:

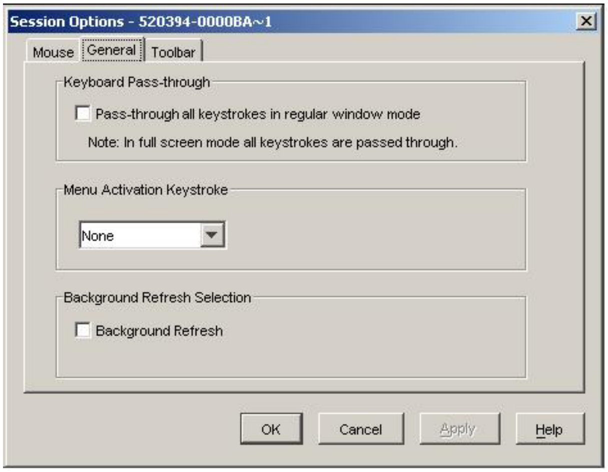
1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.
2. Click the **Mouse** tab.
3. Select the desired terminating keystroke from the drop down list in the **Single Cursor Mode** area.
4. Click **OK**.

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.


Session Options - 520394-0000BA~1

Keyboard Pass-through

□ Pass-through all keystrokes in regular window mode

Note: In full screen mode all keystrokes are passed through.

Menu Activation Keystroke

None

Background Refresh Selection

□ Background Refresh

Figure 4.6: Session Options - General tab

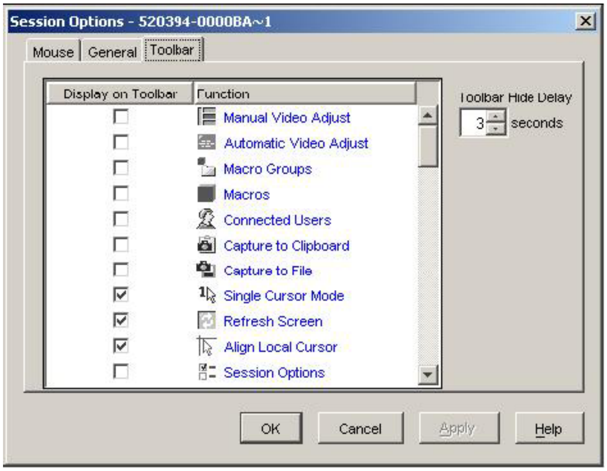
Adjusting the Video Viewer toolbar

You can add up to ten 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.



Display on Toolbar	Function
□	Manual Video Adjust
□	Automatic Video Adjust
□	Macro Groups
□	Macros
□	Connected Users
□	Capture to Clipboard
□	Capture to File
☑	Single Cursor Mode
☑	Refresh Screen
☑	Align Local Cursor
□	Session Options

Toolbar Hide Delay
3 seconds

Figure 4.7: 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, Linux 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.

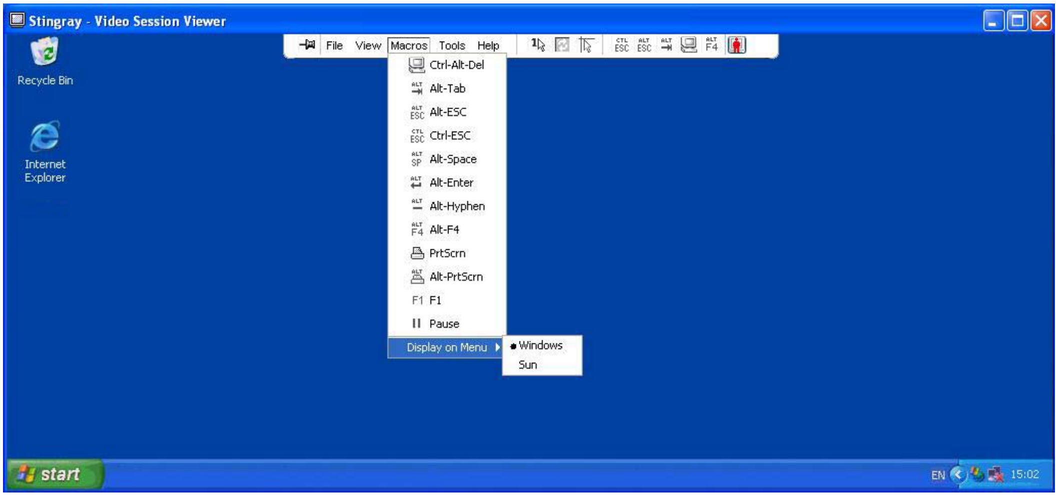


Figure 4.8: Video Viewer Macros menu expanded

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 DVD-ROM drive and one mass storage device mapped concurrently.

- A CD/DVD-ROM drive, or ISO disk image file is mapped as a virtual DVD 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 GCM16 or GCM32 switches.

The target device must be connected to the GCM16 or GCM32 switch with a VCO or VCO2 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 GCM16 will support up to two concurrent virtual media sessions (including local and remote). A GCM32 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 switch and the KVM channel between the upper switch and lower switch is reserved for User A.

Preemption levels offer additional flexibility of combinations.

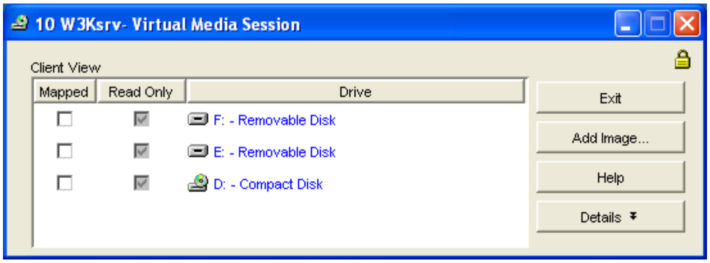
Virtual Media window

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 timeouts on the KVM session.

You can also reset the VCO or VCO2 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.



10 W3Ksrv- Virtual Media Session

Client View

Mapped	Read Only	Drive
☐	☑	F: - Removable Disk
☐	☑	E: - Removable Disk
☐	☑	D: - Compact Disk

Figure 4.9: Virtual Media window

Virtual media session settings

Virtual media session settings include locking, mapped drives access mode, and encryption level settings for the supported GCM16 or GCM32 switches.

Table 4.6 lists and describes the virtual media session settings.

Table 4.6: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 4.6: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 GCM16 or GCM32 switches that are connected with VCO or VCO2 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 DVD-ROM or virtual mass storage mapped concurrently.

   If you attempt to map too many drives (one DVD and one mass storage device) or too many drives of a particular type (more than one DVD 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 DVD 1 or Virtual DVD 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 61 for information about other factors that can affect virtual media session closings.

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/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 GCM16 and GCM32 switches enables you to connect to the USB port of an attached computer. With this feature, a user located at the switch or using the remote software can access a local USB storage device, such as a USB CD/DVD-ROM drive, diskette drive, or flash drive, from an attached computer.

The VCO and VCO2 cables are composite devices that address four functions: keyboard, mouse, DVD drive, and mass storage device. The CD/DVD 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 VCO2 cable presents the keyboard and mouse as a composite USB 2.0 device. Therefore, the BIOS must support a 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 switch. 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 GCM16 and GCM32 switches.

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/DVD 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/DVD-ROM drive to the GCM16 or GCM32 switch with an operating system installation CD/DVD that is bootable, and map it to the target device. Reboot the target device to determine if it will boot from this attached CD/DVD 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/DVD drive to a USB port on the target device and reboot the target device. If the target device successfully boots from the CD/DVD 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 VCO2 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 GCM16 and GCM32 switches only support connection of USB 2.0 diskette drives, flash drives, and CD/DVD-ROM 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 switches. This information can be used to configure firewalls to let VCS operate in the networks.

Table D.1:Ports Used by VCS

Port Number	Switch	Type	Purpose
3211	GCM16, GCM32	TCP	Proprietary management protocol
3211	GCM16, GCM32	UDP	Proprietary install and discovery protocol
2068	GCM16, GCM32	TCP	Encrypted keyboard and mouse data
2068	GCM16 or GCM32	TCP	Digitized video data
2068	GCM16 or GCM32	TCP	Virtual media

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 system, 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 *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your system.
- Go to the IBM support Web site at http://www.ibm.com/systems/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 IBM systems also describes the diagnostic tests that you can perform. Most 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 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/systems/support/ and follow the instructions. Also, some documents are available through the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

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 systems, optional devices, services, and support. The address for IBM System x™ and xSeries® information is http://www.ibm.com/systems/x/. The address for IBM BladeCenter information is http://www.ibm.com/systems/bladecenter/. The address for IBM IntelliStation® information is http://www.ibm.com/intellistation/.

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

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and xSeries servers, BladeCenter products, IntelliStation workstations, and switches. 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 your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/partnerworld/ and click **Find a Business Partner** on the right side of the page. For IBM support telephone numbers, see http:/www.ibm.com/planetwide/. 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.

IBM Taiwan product service

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation

3F, No 7, Song Ren Rd.

Taipei, Taiwan

Telephone: 0800-016-888

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Linux is a registered trademark of Linus Torvalds 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.

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 might differ from its retail version (if available) and might not include user manuals or all program functionality.

INDEX