Lenovo

Global Console Manager Switch

Installer/User Guide

Second Edition, March 2016.

TABLE OF CONTENTS

Chapter 1. Product overview

Features and benefits

The Lenovo® Global Console Manager Switch KVM over IP and serial console switches combine analog and digital technology to provide flexible, centralized control of data center servers, and virtual media, and to facilitate the operations, activation, and maintenance of remote branch offices where trained operators may be unavailable. IP-based GCM switches give you flexible target device management control and secure remote access from anywhere at anytime.

The GCM switches provide enterprise customers with the following features and options:

- significant reduction of cable volume
- keyboard, video, and mouse (KVM) capabilites, configurable for analog (local) or digital (remote) connectivity
- true serial capability through Secure Shell (SSH) and Telnet
- enhanced video resolution support, up to 1600 x 1200 or 1680 x 1050 (widescreen) native from target to remote
- optional dual power models for redundancy
- optional support for managing intelligent power devices
- virtual media capability accessed through USB ports
- dual independent local port video paths (dedicated to ACI)
- dual stack IPv4 (DHCP) and IPv6 (DHCPv6 and stateless auto-configuration) for simultaneous access
- smart card capability
- accessibility to target devices across 10/100 or 1000BaseT (some models) LAN port(s)
- a MODEM port that supports V.34, V.90 or V.92-compatible modems that may be used to access the switch when an Ethernet connection is not available
- embedded Federal Information Processing Standards (FIPS) cryptographic module

Reduce cable bulk

With server densities continually increasing, cable bulk remains a major concern for network administrators. The GCM switches significantly reduce KVM cable volume in the rack by utilizing the innovative virtual media conversion option cables and single, industry-standard Unshielded

Twisted Pair (UTP) cabling. This allows a higher server density while providing greater airflow and cooling capacity.

KVM switching capabilities

The GCM switches support conversion option (CO) cables that are powered directly from the target device and provide Keep Alive functionality when the switch is not powered. The following CO cables are supported: KCO, UCO, VCO, VCO2, and SCO cables. The VCO and VCO2 cables are virtual media-capable. The VCO2 cable is also smart card-capable.

True serial capabilities

The GCM switches support SCO cables that provide true serial capabilities through Telnet. You can launch an SSH session or launch a serial viewer from the on-board web interface (OBWI) to connect the targets that are connected to the GCM switches with an SCO cable.

Local and remote user interfaces

You can use the local user interface (local UI) by connecting directly to the local port to manage the GCM switches. You can also use the remote OBWI to manage your switch. The OBWI is web browser based and is launched directly from the switch, and any devices connected to the GCM switches are automatically detected. The two user interfaces share a similar look and feel for an optimal user experience.

Control of virtual media and smart card-capable switches

The GCM switches allow you to view, move, or copy data located on virtual media to and from any target device. You can manage remote systems more efficiently by allowing operating system installation, operating system recovery, hard drive recovery or duplication, BIOS updating, and target device backup.

The GCM switches allow you to use smart cards in conjunction with your switch system. Smart cards are pocket-sized cards that store and process information. Smart cards such as the Common Access Card (CAC) can be used to store identification and authentication to enable access to computers, networks, and secure rooms or buildings.

Virtual media and smart card readers can be connected directly to the switch using USB ports located on the switch. In addition, virtual media and smart card readers may be connected to any remote workstation that is running the remote OBWI or Avocent® DSView™ Management Software and is connected to the switch using an Ethernet connection.

NOTE: References to DSView Management Software in this document apply to DSView 3 Management Software and later.

NOTE: To open a virtual media session with a target device, you must first connect the target device to a switch using the VCO or VCO2 cable. For a smart card, you must first connect the target device to a switch using the smart card-capable VCO2 cable.

Access the switch via a standard TCP/IP network

The switch provides agentless remote control and access. No special software or drivers are required on the attached servers or client.

NOTE: The client connects to the switch using an Internet browser.

You can access the switch and all attached systems via Ethernet or using a V.34, V.90, or V.92 modem from a client. The clients can be located anywhere a valid network connection exists.

FIPS cryptographic module

The GCM switches support FIPS 140-2 Level 1 cryptographic security requirements. The FIPS mode of operation can be enabled or disabled via the OBWI, local port, or DSView plug-in and is executed after a reboot. When the FIPS module is enabled, a reboot of the switch requires approximately two additional minutes to complete a FIPS mode integrity check. Also, when the FIPS module is enabled, if the keyboard, mouse, or video encryption is set to 128-bit SSL (ARCFOUR) or DES, the encryption level is automatically changed to the encryption level AES.

NOTE: The FIPS mode of operation is initially disabled and must be enabled to operate.

NOTE: The SETUP port factory default setting will automatically disable the FIPS module.

NOTE: The FIPS mode cannot be changed via the DSView software plug-in.

Lenovo® GCM switches use an embedded FIPS 140-2 validated cryptographic module (Certificate #1747) running on a Linux PPC platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.

When the FIPS module is disabled, the User Database and Appliance Configuration files saved from or restored to the appliance as external files are encrypted (or decrypted) using DES. This is true even when the user does not fill in the Password parameter in the Save (or Load) dialog on the OBWI, in which case a default OEM password is used for encryption or decryption.

One result of enabling the FIPS module is to render previously saved User Database and Appliance Configuration files incompatible. In this case, you may temporarily disable the FIPS module, reboot the appliance, restore the previously saved database or configuration file, re-enable the FIPS module, reboot, and then save the file externally again while the FIPS module is

enabled. The new, saved external file will be compatible with the appliance as long as the appliance is running with FIPS mode enabled.

The opposite situation is also true, in that database and configuration files saved with the FIPS module enabled are not compatible for restoring to an appliance without the FIPS module enabled or an appliance with older firmware not supporting the FIPS module.

DSView™ Management Software plug-in

The DSView software may be used with the switch to allow IT administrators to remotely access, monitor, and control target devices on multiple platforms through a single, web based user interface.

Sample configuration

Figure 1. Example switch configuration

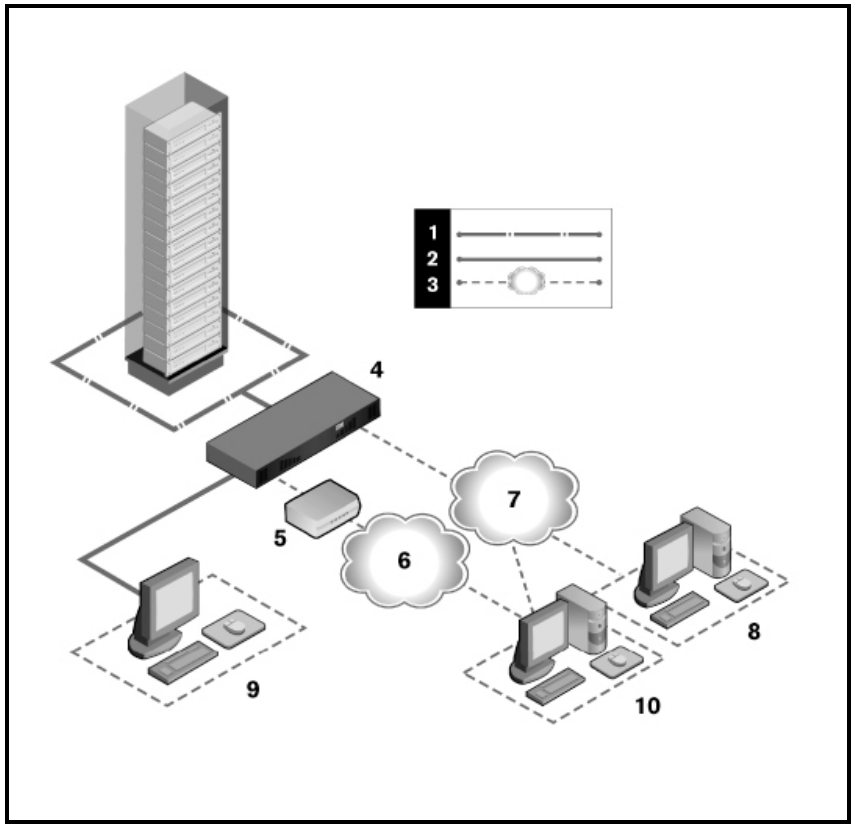


Table 1. Descriptions for Example switch configuration on page 4

Number	Description	Number	Description
1	UTP connection	6	Telephone network
2	KVM connection to the GCM switches	7	Ethernet
3	Remote IP connection	8	DSView software server

Number	Description	Number	Description
4	GCM switches	9	Analog user (local UI)
5	Modem	10	Digital user (computer with Internet browser, remote OBWI)

Chapter 2. Installation

GCM switch connectivity

The GCM switches transmit KVM and serial information between operators and target devices attached to the switch over a network using either an Ethernet or modem connection.

The GCM switches use TCP/IP for communication over Ethernet. For the best system performance, use a dedicated, switched 100BaseT or 1000BaseT network. You can also use 10BaseT Ethernet.

The GCM switches use the Point-to-Point Protocol (PPP) for communication over a V.34, V.90, or V.92 modem. You can perform KVM and serial switching tasks by using the OBWI or the DSView software. For more information on the DSView software, visit http://www.avocent.com. Basic switch configuration using the GCM switch on page 8 illustrates an example basic configuration for the switch.

Basic switch configuration using the GCM32 switch on page 8 illustrates an example basic configuration for the switch. Descriptions follow in Descriptions for Basic switch configuration using the GCM32 switch on page 8 on page 8.

Figure 2. Basic switch configuration using the GCM32 switch

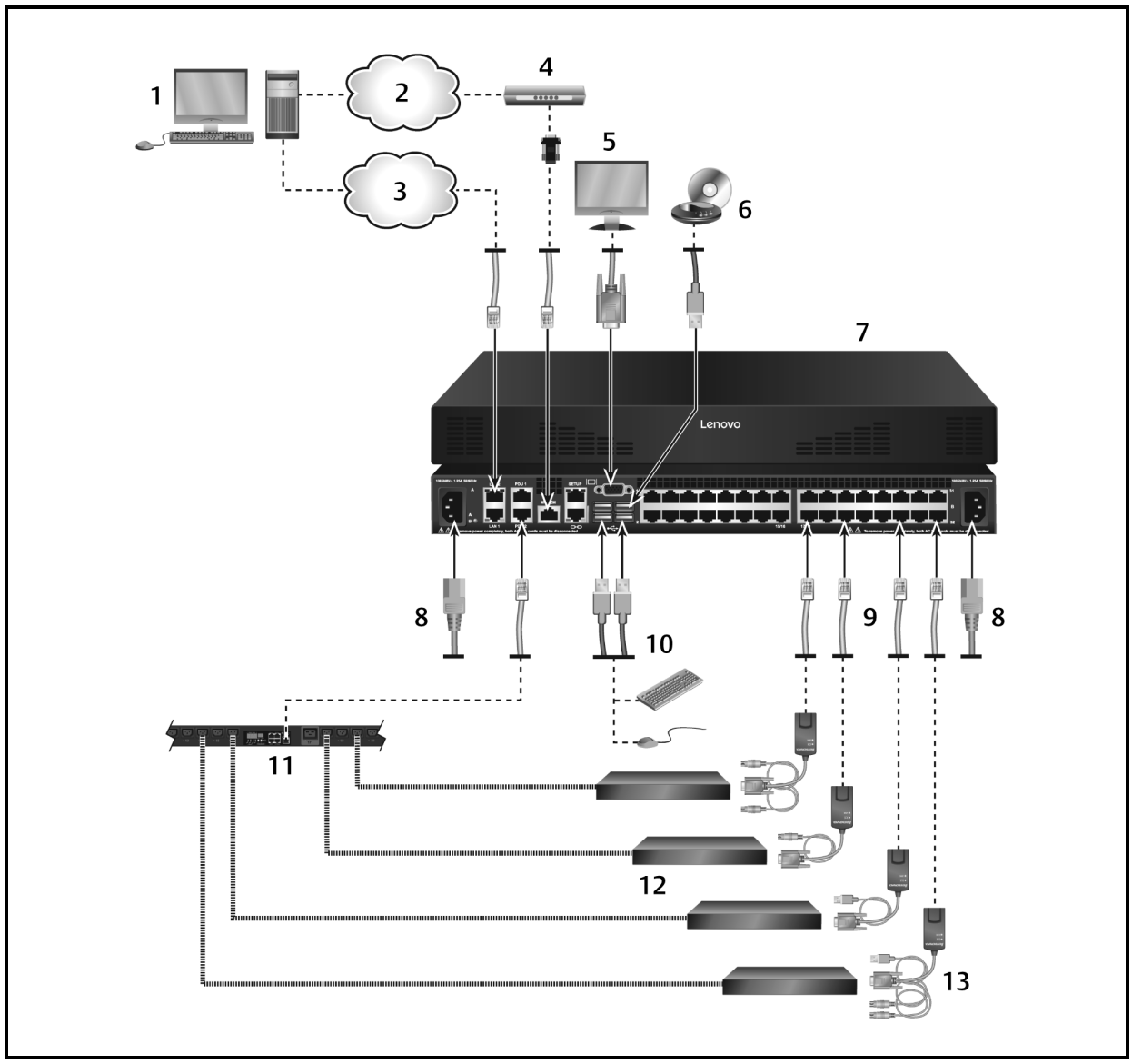


Table 2. Descriptions for Basic switch configuration using the GCM32 switch on page 8

Number	Description	Number	Description
1	Digital user	8	Power cord
2	Telephone network	9	Ports 1-32
3	Network	10	Local USB connections
4	Modem	11	Power control device
5	Analog user	12	Target devices 1-32
6	External virtual media	13	CO cables (KCO, UCO, VCO, VCO2, and SCO are available)
7	GCM32 switch		

Getting started

Before installing your switch, refer to the following lists to ensure you have all items that shipped with the switch, as well as other items necessary for proper installation.

Supplied with the switch

- Rack mount bracket kit
- Rack Mounting Bracket Quick Installation Guide
- Global Console Manager GCM16 and GCM32 Quick Installation Guide
- Safety and Regulatory Statements Guide
- Cables and adapters for the MODEM and SETUP ports
- AC power cord(s)

Additional items needed

- One conversion option (CO) cable per target device
- One serial conversion option (SCO) cable per serial device
- One UTP patch cable per CO cable (4-pair UTP, up to 45 meters)
- UTP patch cable(s) for network connectivity (4-pair UTP, up to 45 meters)
- One virtual media-capable VCO or VCO2 cable per target device for virtual media sessions
- One smart card-capable VCO2 cable per target device for smart card control
- (Optional) DSView software
- (Optional) V.34, V.90, or V.92-compatible modem and cables
- (Optional) Power control device(s)

Setting up your network

The switch uses IP addresses to uniquely identify the switch and the target devices. The GCM switches support both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. Make sure that an IP address is reserved for each switch and that each IP address remains static while the switch is connected to the network.

Rack mounting GCM switches

A rack mounting kit is supplied with each switch. You may either place the switch on the rack shelf or mount the switch directly into an Electronic Industries Alliance (EIA) standard rack.

The switch may be rack-mounted in a 1U or 0U configuration.

Rack mounting safety considerations

- Rack Loading: Overloading or uneven loading of racks may result in shelf or rack failure, causing damage to equipment and possible personal injury. Stabilize racks in a permanent location before loading begins. Mount components beginning at the bottom of the rack, then work to the top. Do not exceed your rack load rating.
- Power considerations: Connect only to the power source specified on the unit. When multiple electrical components are installed in a rack, ensure that the total component power ratings do not exceed circuit capabilities. Overloaded power sources and extension cords present fire and shock hazards.
- Elevated ambient temperature: If installed in a closed rack assembly, the operating temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the switch.
- Reduced air flow: Install the equipment in the rack so that the amount of airflow required for safe operation of the equipment is not compromised.
- Reliable earthing: Maintain reliable earthing of rack-mounted equipment. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).
- Product should not be mounted with the rear panel facing in the downward position.

For complete instructions on installing the rack mounting bracket, please refer to your Rack Mounting Bracket Quick Installation Guide.

Connecting the switch hardware

To connect and turn on your switch:

NOTE: To avoid potential video and/or keyboard problems when using the products: If the building has 3-phase AC power, ensure that the computer and monitor are on the same phase. For best results, they should be on the same circuit.

Statement 1:

DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- Connect all power cords to a properly wired and grounded electrical outlet.
- Connect to properly wired outlets any equipment that will be attached to this product.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.

To Connect:	To Disconnect:
1. Turn everything OFF. 2. First, attach all cables to devices. 3. Attach signal cables to connectors. 4. Attach power cords to outlet. 5. Turn device ON.	1. Turn everything OFF. 2. First, remove power cords from outlet. 3. Remove signal cables from connectors. 4. Remove all cables from devices.

1. Connect your VGA monitor and USB keyboard and mouse cables into the appropriately labeled ports.
2. Choose an available port on the switch. Connect one end of a UTP cable (4-pair, up to 150 ft/45 m) into a numbered port. Connect the other end into an RJ-45 connector of a CO cable.
3. Connect the CO cable into the appropriate ports on the back of a target device. Repeat this procedure for all target devices you want to connect.

NOTE: When connecting to a Sun Microsystems target device, you must use a multi-sync monitor in the local port to accommodate Sun computers that support both VGA and sync-on-green or composite sync.

4. Connect both LAN ports to independent Ethernet switches to provide redundancy.
5. (Optional) The switch may also be accessed using an ITU V.92, V.90, or V.24-compatible modem. Connect one end of an RJ-45 cable into the MODEM port on the switch. Connect the

other end into the supplied RJ-45 to DB-9 (male) adapter, which then plugs into the appropriate port on the back of the modem.

NOTE: Using a modem connection instead of a LAN connection will limit the performance capability of your switch.

6. (Optional) Connect one end of the RJ-45 cable into the PDU1 port on the switch. Connect the other end into the Power Distribution Unit (PDU). Connect the power cords from the target devices into the PDU. Connect the PDU into an appropriate AC wall outlet. Repeat this procedure for the PDU2 port to connect a second PDU, if desired.
7. Turn on each target device, then locate the power cord(s) that came with the switch. Connect one end into the power socket on the rear of the switch. Connect the other end into an appropriate AC wall outlet. Use your second power cord to connect to the second power socket on the rear of the switch. Connect the other end into an appropriate wall outlet.

NOTE: Plug the redundant power supplies into separate branch circuits to provide additional redundancy in the event one external AC power source should go away.

To connect local virtual media or a smart card reader:

Connect the virtual media or smart card reader to an available USB port on the switch.

NOTE: For all virtual media sessions, you must use a VCO or VCO2 cable. For all smart card readers, you must use a VCO2 cable.

For information on connecting virtual media remotely, see *Virtual Media*. For information on connecting a smart card reader remotely, see *Smart Cards*.

To connect the SCO cable to a serial device using a UTP connector:

1. Attach the SCO cable UTP connector to the serial device.

   -or-

   Attach the SCO cable to an RJ-45 to 9-pin female adapter. Attach the adapter to the serial port of the serial device.
2. Connect one end of a UTP cable (4-pair, up to 150 ft/45 m) into an available numbered port on the rear of the switch. Connect the other end into the RJ-45 connector of the SCO cable.
3. Attach a USB-to-barrel power cord to the power connector on your SCO cable. Connect the USB connector on the USB-to-barrel power cord into any available USB port on the serial target device.

Cascading GCMswitches

You can cascade up to two levels of switches, enabling users to connect to up to 1024 servers. In a cascaded system, each target port on the main switch will connect to the ACI port on each cascaded switch. Each cascaded switch can then be connected to a device with a CO cable.

To cascade multiple switches:

1. Attach one end of a UTP cable to a target port on the switch.
2. Connect the other end of the UTP cable to the ACI port on the back of your cascaded switch.
3. Connect the devices to your cascaded switch.
4. Repeat these steps for all the cascaded switch you wish to attach to your system.

NOTE: The system will automatically “merge” the two switches. All devices connected to the cascaded switches will display on the main switch device list in the local UI.

NOTE: The switch supports one cascaded switch per target port of the main switch. You cannot attach more switches to the cascaded switch.

NOTE: Local port cascading is not supported on GCM switches.

Configuring GCM switches

Once all physical connections have been made, you will need to configure the switch for use in the overall switch system. This can be accomplished in two ways.

To configure the switch using DSView software:

See the DSView Installer/User Guide for detailed instructions.

To configure the switch using the local UI:

See Network settings on page 26 for detailed instructions on using the local UI to configure initial network setup.

Setting up the built-in web server

You can access the switch via an embedded web server that handles most day-to-day switch tasks. Before using the web server to access the switch, first specify an IP address through the local port on the back panel of the switch or local UI. See Chapter 3 for detailed instructions on using the switch user interface.

Connecting to the OBWI through a firewall

For switch installations that use the OBWI for access, the following ports must be opened in a firewall if outside access is desired.

Table 3. TCP ports and functions for the switch OBWI

TCP Port Number	Function
22	Used for SSH for serial sessions to a serial conversion option cable
23	Used for Telnet (when Telnet is enabled)
80	Used for the initial downloading of the Video Viewer
443	Used by the web browser interface for managing the switch and launching KVM sessions
2068	Transmission of KVM session data (mouse & keyboard) or transmission of video on switches

In a typical configuration, as shown in Typical switch firewall configuration on page 14, the user's computer is located outside of the firewall, and the switch resides inside the firewall.

Figure 3. Typical switch firewall configuration

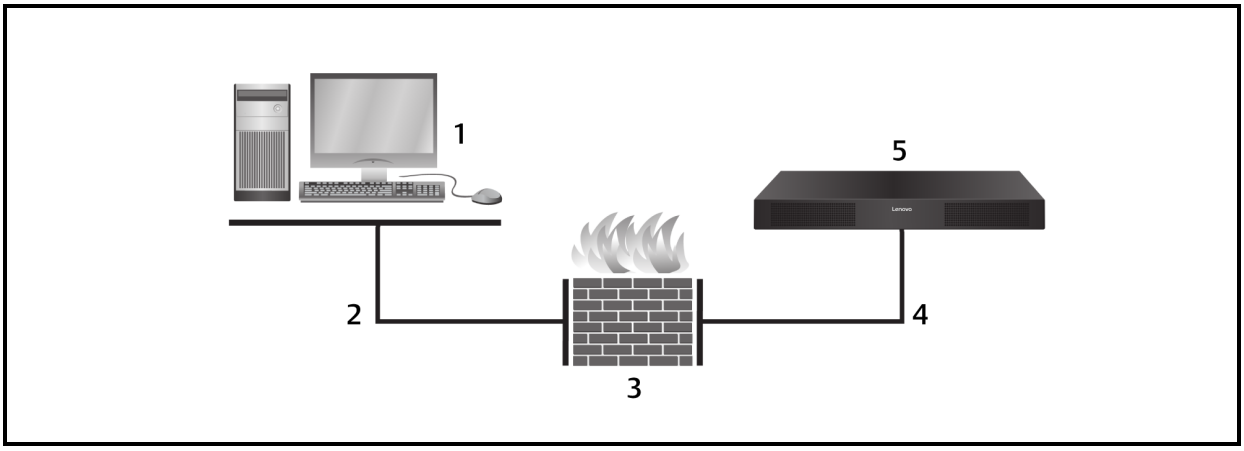


Table 4. Descriptions for Typical switch firewall configuration on page 14

Number	Description
1	User's computer
2	User browses to firewall's external IP address
3	Firewall
4	Firewall forwards HTTP requests and KVM traffic to the switch
5	GCM switches

To configure the firewall:

To access the switch from outside a firewall, configure your firewall to forward ports 22, 23 (if Telnet is enabled), 80, 443 and 2068 from its external interface to the KVM switch through the firewall's internal interface. Consult the manual for your firewall for specific port forwarding instructions.

For information on launching the OBWI, see OBWI on page 18.

Verifying the connections

Rear panel Ethernet connection LEDs

On GCM switches, the rear panel features two LEDs indicating the Ethernet LAN1 connection status and two LEDs indicating the Ethernet LAN2 connection status.

- The green LEDs illuminate when a valid connection to the network is established and blink when there is activity on the port.
- The bi-color LEDs may illuminate either green or amber.
  - They illuminate green when the communication speed is 1000M.
  - They illuminate amber when the communication speed is 100M.
  - They are not illuminated when the communication speed is 10M.

Rear panel power status LEDs

The rear panel of each appliance has two power status LEDs, one for each power supply. The LED (s) illuminate green when the switch is turned on and operating normally.

- The LED is off if the power supply does not have power or has failed.
- The LED illuminates when the unit is ready.
- The LED blinks when the switch is booting or an upgrade is in progress.
- The LED blinks "SOS" if a fault condition occurs, such as power supply failure, elevated ambient temperature, or fan failure. The LED will continue to blink "SOS" as long as the failure persists.

The switch prevents a serial break from the attached device if the module loses power. However, a user can generate a serial break with the attached device by pressing **Serial Break** on the serial session viewer.

NOTE: The break command is not transmitted to the serial target in an OBWI serial session.

Adjusting mouse settings on target devices

Before a computer connected to the switch can be used for remote user control, you must set the target mouse speed and turn off acceleration. For machines running Microsoft® Windows® (Windows NT®, 2000, XP, Server 2003), use the default PS/2 mouse driver.

To ensure that the local mouse movement and remote cursor display remain in sync, mouse acceleration must be set to “none” for all user accounts accessing a remote system through a KVM switch. Mouse acceleration must also be set to “none” on every remote system. Special cursors

should not be used and cursor visibility options, such as pointer trails, **Ctrl** key cursor location animations, cursor shadowing, and cursor hiding, should also be turned off.

NOTE: If you are not able to disable mouse acceleration from within a Windows operating system, or if you do not wish to adjust the settings of all your target devices, you may use the *Tools > Single Cursor Mode* command available in the Video Viewer window. This command places the Video Viewer window into an "invisible mouse" mode, which allows you to manually toggle control between the mouse pointer on the target system being viewed and the mouse pointer on the client computer.

Chapter 3. Local and remote configuration

User interfaces

The GCM switches come equipped with two “point-and-click” interfaces: a local user interface (local UI) and a remote on-board web interface (OBWI). Using the configuration options provided by these interfaces, you can tailor the switch to your specific application, control any attached devices, and handle all basic KVM or serial switch needs.

NOTE: The local UI and remote OBWI are almost identical. Unless specified, all information in this chapter applies to both interfaces.

From either interface, you can launch two different kinds of sessions:

- The Video Viewer window allows you to control the keyboard, monitor, and mouse functions of individual target devices connected to the switch in real time. You may also use predefined global macros to perform actions within the Video Viewer window. For instructions on how to use the Video Viewer, see Chapter 1.
- The serial viewer window allows you to manage individual target devices either by using commands or scripts.

Local UI

The switch includes a local port on the back. This port enables you to connect a keyboard, monitor and mouse directly to the switch and use the local UI.

You can choose any of the following keystrokes to be configured to open the local UI or to switch between the local UI and an active session: **Print Screen, Ctrl + Ctrl, Shift + Shift**, and **Alt + Alt**.

To launch the local UI:

1. Connect your monitor, keyboard and mouse cables to the switch. For more information, see Connecting the switch hardware on page 10.
2. Press any of the enabled keystrokes to launch the local UI.
3. If local UI authentication has been enabled, enter your username and password.

NOTE: If the switch has been added to a DSView server, then the DSView server will be accessed to authenticate the user. If the switch has not been added to a DSView server, or if the DSView server cannot

be reached, then the switch local user database will be accessed to authenticate the user. The default local username is Admin, and there is no password. Usernames in the local user database are case-sensitive.

OBWI

The switch OBWI is a remote, web browser based user interface. For details on setting up your system, see Connecting the switch hardware on page 10. The following table lists the operating systems and browsers that are supported by the OBWI. Make sure that you are using the latest version of your Web browser.

Table 5. Operating Systems Supported by the OBWI

Operating System	Browser					
	Microsoft® Internet Explorer® Version 9.0	Microsoft Internet Explorer Version 10.0	Apple® Safari® 6.1	Apple Safari 7	Mozilla® Firefox® Version 10 and Later	Google Chrome™ browser version 19 and Later
Microsoft Windows 2008_ R2	Yes	No	No	No	Yes	Yes
Microsoft Windows 7	No	Yes	No	No	Yes	Yes
Red Hat Enterprise Linux® 5 and 6	No	No	No	No	Yes	Yes
Apple Mac OS X® 8	No	No	Yes	No	Yes	Yes
Apple Mac OS X 9	No	No	No	Yes	Yes	Yes

To log in to the switch OBWI:

1. Launch a web browser.
2. In the address field of the browser, enter the IP address or host name assigned to the switch you wish to access. Use https://xxx.xx.xx.xx or https://hostname as the format.

NOTE: If using IPv6 mode, you must include square brackets around the IP address. Use https://[<ipaddress>] as the format.

3. When the browser makes contact with the switch, enter your username and password, then click *Login*. The switch OBWI will appear.

NOTE: The default username is Admin with no password.

To log in to the switch OBWI from outside a firewall, repeat the above procedure, entering the external IP address of the firewall instead.

Using the user interfaces

After you have been authenticated, the user interface appears for you to view, access, and manage your switch, as well as specify system settings and change profile settings.

Attached target devices in the local UI can be viewed and managed from two individual screens that are selected from the side navigation bar. For less than 20 targets, the Target List-Basic screen is recommended for navigation. For more than 20 attached target devices, the Target List-Full screen provides additional navigation tools. At the Target List-Full screen you can navigate by entering the page number, using the page navigation buttons, or using the filter. Either the Basic or Full screens can be set as the default screen for selecting target devices.

Filtering

You may filter the list of target devices by providing a text string that will be used to retrieve matching items. Filtering can provide a shorter, more exact list of items. When filtering is performed, the Name column is searched for the specified text string. The search is not case sensitive. When filtering, you may use an asterisk (*) before or after text strings as a wildcard. For example, typing emailserver* and clicking Filter will display items with emailserver at the beginning (such as emailserver, emailserverbackup).

NOTE: To set up the scanned target list, see the Local Sessions screen section.

User interface window on page 20 shows the user interface for the switch. Descriptions are provided in the following table.

Figure 4. User interface window

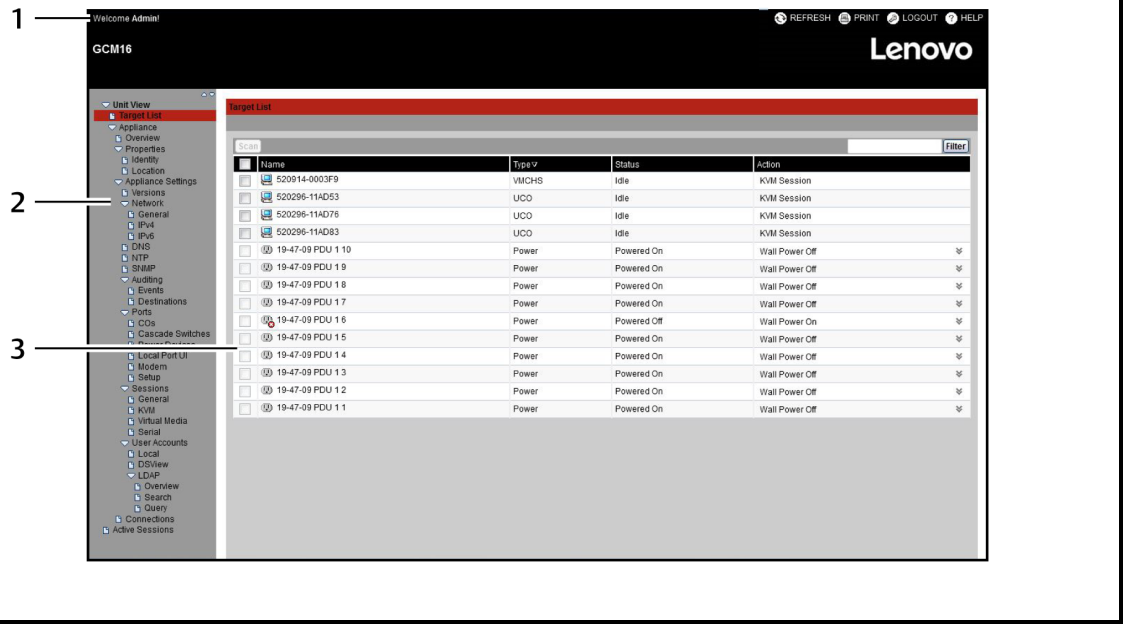


Table 6. User interface descriptions

Number	Description
1	Top option bar: Use the top option bar to bookmark an interface window, refresh the display of an interface window, print a web page, log out of an OBWI session, or access the online help page. The name of the logged in user appears on the left side of the top option bar.
2	Side navigation bar: Use the side navigation bar to select and display the system information in the content area. The side navigation bar also contains icons in the top left corner that, when clicked, expand or collapse all nodes.
3	Content area: Use the content area to display or make changes to the switch OBWI system.

Using the side navigation bar

You can use the side navigation bar to display windows in which you can specify settings or perform operations. Clicking on a link that does not contain an arrow will display its corresponding window.

Using the top option bar

NOTE: If authentication is disabled, only the Refresh button will appear in the local UI. If authentication is enabled, only the Refresh and Log Out buttons will appear in the local UI. All of the buttons will appear in the remote OBWI.

Bookmarking a window (Microsoft Internet Explorer only)

The user interface contains a bookmark icon and text in the top option bar. You can bookmark a window to add a link to the window in the Favorites drop-down menu. You may select the link at any

time to quickly access the bookmarked window.

If you bookmark a window and information related to the window changes, this new information will appear in the window when you next display the bookmarked window.

If you click *BOOKMARK* or the bookmark icon after the switch OBWI session has timed out, the User Login window will open and you must log in again.

To bookmark a window:

1. In the top option bar, click *BOOKMARK* or the bookmark icon. The Add Favorite dialog box will appear.
2. If you wish, type a name for the window. You may also click the *Create in* button to create or specify a folder in which to place the window.
3. Click *OK* to close the Add Favorite dialog box.

Printing a window

All switch OBWI windows contain a print icon in the top option bar.

To print the switch OBWI window:

1. In the top option bar, click *PRINT* or the print icon. The Print dialog box will appear.
2. Specify the options you wish to use for printing the switch OBWI window.
3. Click **Print** to print the switch OBWI window and close the Print dialog box.

Refreshing a window

The switch user interface may be refreshed at any time by clicking *REFRESH* or the refresh icon in the top option bar.

Logging out

To log out at any time, click the logout icon in the top option bar.

Viewing system information

You can view various appliance and target device information from several different screens in the user interface.

Table 7. System information

Category	Select This:	To View This:
Switch	*Unit View > Appliance > Overview*	Switch name and type and appliance tools

Category	Select This:	To View This:
	Unit View > Appliance > Properties > Identity	Current firmware revision for application and boot
	Unit View > Appliance > Properties > Location	Site, department, or location
	Unit View > Appliance > Appliance Settings > Versions	Current firmware revision for application, boot, and Video FPGA
	Unit View > Connections	List of the attached devices
Target Device	*Unit View > Target Devices*	List of connected target devices, as well as the following information about each device: Name, Type, Status, and Action Click on one of the target devices to view the following additional information: Name, Type, eID, available session option, and the connection path

You will also be alerted if any of the following fault conditions occur: power supply failure, elevated ambient temperature, or fan failure. A yellow triangle with an exclamation point and the name of the failure will appear in the header of each screen. This notification will appear or disappear only after you refresh the page. You can click on the notification to get more information.

GCM switch sessions

From the Active Sessions screen, you can view a list of active sessions and the following information about each session: Target Device, Owner, Remote Host, Duration, and Type.

Launching a session

NOTE: Java 1.6.0_11 or later is required to launch a session.

To launch a session:

1. From the side navigation bar, select *Unit View* > *Target Devices*. A list of available devices will appear.
2. Click the *KVM Session* or *Serial Session* link to the right of the desired target device to launch the session.

If the target device is currently in use, users attempting to gain access will be given an opportunity to force a connection to the device if their preemption level is equal to or higher than the current user's.

To switch to the active session from the local UI (local users only):

1. From the side navigation bar, select *Local Session*.

2. Select the *Resume Active Session* check box. The Video Viewer window will appear.

   -or-

   Press **Esc**.

Configuring sessions

To configure general session settings:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Sessions* > *General*. The Appliance General Session Settings screen appears.
2. Select or deselect the *Enable Inactivity Timeout* check box.
3. In the Inactivity Timeout field, enter the amount of inactive time you want to pass before the session closes (from 1 to 90 minutes).
4. In the Login Timeout field, enter the amount of inactive time you want to pass before you must log in again (from 21 to 120 seconds).
5. Select or deselect the *Enable Preemption Timeout* check box.
6. In the Preemption Timeout field, enter the amount of time (from 1 to 120 seconds) that a prompt will be displayed to inform you that your session is going to be preempted.
7. Under Sharing, select one or more session options (*Enabled*, *Automatic*, *Exclusive* and *Stealth*) and enter the amount of time that the input control will timeout (1-10 seconds).
8. Under Security, select *Enabled* or *Disabled*.
9. Click **Save**.

To configure KVM session settings:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Sessions* > *KVM*. The Appliance KVM Session Settings screen appears.
2. Select an encryption level for keyboard and mouse signals (*128-bit SSL*, *DES*, *3DES,* or *AES*) and for video signals (*128-bit SSL*, *DES*, *3DES*, *AES,* or *None*).
3. Select a language from the Keyboard drop-down menu.
4. Click **Save**.

To configure serial session settings:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Settings* > *Serial*. The Appliance Serial Session Settings screen appears.
2. Either enable or disable the *Telnet Access Enabled* check box.
3. Click **Save**.

Closing a session

To close a session:

1. From the side navigation bar, select *Active Sessions* to display the Appliance Sessions screen.
2. Click the check box next to the desired target device(s).
3. Click *Disconnect*.

NOTE: If there is an associated locked virtual media session, it will be disconnected.

To close a session (local users only):

1. From the side navigation bar, select *Local Session*.
2. Select the *Disconnect Active Session* check box.

GCM switch tools

From the Unit Overview screen, you can view the appliance name and type. You can also perform basic appliance tasks.

Rebooting the GCM switch

To reboot the GCM switch:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Overview* to open the Unit Overview screen.
2. Click *Reboot*.
3. A dialog box appears, warning you that all active sessions will be disconnected. Click *OK*.

NOTE: If you are using the local UI, the screen will be blank while the switch reboots. If you are using the remote OBWI, a message will appear to let you know that the interface is waiting on the appliance to complete the reboot.

Upgrading the GCM switch firmware

You can update your GCM switch with the latest firmware available.

After the Flash memory is reprogrammed with the upgrade, the switch performs a soft reset, which terminates all CO cable sessions. A target device experiencing a CO cable firmware update may not display, or may display as disconnected. The target device will appear normally when the Flash update is completed.

Attention: Disconnecting a CO cable during a firmware update or cycling power to the target device will render the module inoperable and require the CO cable to be returned to the factory for repair.

To upgrade the switch firmware:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Overview* to open the Unit Overview window.
2. Click *Upgrade Firmware* to open the Upgrade Appliance Firmware.
3. Select one of the following options from which to load the firmware file: *File System*, *TFTP*, *FTP*, or *HTTP*.

NOTE: The File System option is only available on the remote OBWI.

4. If you selected File System, select *Browse* to specify the location of the firmware upgrade file.

   -or-

   If you selected TFTP, enter the Server IP Address and Firmware File you wish to load.

   -or-

   If you selected FTP or HTTP, enter the Server IP Address and Firmware File you wish to load, as well as the User Name and User Password.
5. Click *Upgrade.*

Saving and restoring switch configurations and user databases

You may save the switch configuration to a file. The configuration file will contain information about the managed appliance. You may also save the local user database on the switch. After saving either file, you may also restore a previously saved configuration file or local user database file to the switch.

To save a managed appliance configuration or user database of a managed appliance:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Overview* to open the Unit Overview window.
2. Click *Save Appliance Configuration* or *Save Appliance User Database*. The File Download dialog box will open.
3. Click *Save*. The Save As dialog box will open.
4. Navigate to the desired location and enter a name for the file. Click *Save*.
5. Click *Close*.

To restore a managed appliance configuration or user database of a managed appliance:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Overview* to open the Unit Overview window.
2. Click *Restore Appliance Configuration* or *Restore Appliance User Database*. The Restore Appliance Configuration Window or Restore Appliance User Database Window will appear.
3. Click *Browse*. Navigate to the desired location and select the file name. Click *Upload*.
4. After the success screen appears, click *Close*. Reboot the managed appliance to enable the restored configuration.

Network settings

NOTE: Only switch administrators can make changes to the network dialog box settings. Other users will have view only access.

To configure general network settings:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Network* > *General*. The Appliance General Network Settings screen appears.
2. Select one of the following options from the LAN Speed drop-down menu: *Auto-Detect*, *10 Mbps Half Duplex*, *10 Mbps Full Duplex*, *100 Mbps Half Duplex*, *100 Mbps Full Duplex,* or *1 Gbps Full Duplex*.

NOTE: You must reboot if you change the Ethernet mode.

3. Select either *Enabled* or *Disabled* in the ICMP Ping Reply drop-down menu.
4. Click *Save*.

To configure IPv4 network settings:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Network* > *IPv4*. The switch IPv4 Settings screen appears.
2. Select or deselect the *Enable IPv4* check box to enable or disable IPv4 mode.
3. Enter the desired information in the Address, Subnet, and Gateway fields.
4. Select either *Enabled* or *Disabled* in the DHCP drop-down menu.

NOTE: If you enable DHCP, any information that you enter in the Address, Subnet, and Gateway fields will be ignored.

5. Click *Save*.

To configure IPv6 network settings:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Network* > *IPv6*. The switch IPv6 Settings screen appears.
2. Select or deselect the *Enable IPv6 Stateful Configuration* check box to enable or disable.
3. Enter the desired information in the Address, Gateway, and Prefix Length fields.
4. Select either *Enabled* or *Disabled* in the DHCPv6 drop-down menu.

NOTE: If you enable DHCPv6, any information that you enter in the Address, Gateway, and Prefix length fields will be ignored.

5. Click *Save*.

DNS settings

You can choose to either manually assign the DNS server or to use the addresses obtained using DHCP or DHCPv6.

To manually configure DNS settings:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *DNS*. The Appliance DNS Settings screen appears.
2. Select *Manual*, *DHCP* (if IPv4 is enabled) or *DHCPv6* (if IPv6 is enabled).
3. If you selected *Manual*, enter the DNS Server numbers in the Primary, Secondary and Tertiary fields.
4. Click *Save*.

Local UI settings

To change how the local UI is invoked:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *Local Port UI* to open the Local Port UI Settings screen.
2. Under the Invoke Local Port UI heading, select the check box next to one or more of the listed methods.
3. Click *OK*.

Local port user settings

You can turn on or turn off local port user interface authentication and choose a user access level. If you turn on local port user interface authentication, you will be required to log in to use the interface.

You can also select the keyboard language for the local port, scan mode time, enable/disable the setup port password and select a user preemption level. The preemption level of users determines whether they may disconnect another user's serial or KVM session with a target device. Preemption levels range from 1 - 4, with 4 being the highest level. For example, a user with a preemption level of 4 may preempt other level 4 users, as well as those with a level 1, 2, or 3 setting.

To change the default preemption level (administrator only):

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *Local Port UI* to open the Local Port UI Settings screen.
2. Select or deselect the *Disable Local Port User Authentication* check box.
3. Select one of the following options from the User Access Level drop-down menu: *User*, *User Administrator*, or *Appliance Administrator*.
4. Select a number 1 - 4 from the User Preemption Level drop-down menu.
5. Click *Save*.

Virtual media

You can determine the behavior of the switch during a virtual media session using the options provided in the Appliance Virtual Media Session Settings screen. Virtual media session settings on page 28 outlines the options that can be set for virtual media sessions. For information about using virtual media in a KVM session, see "Virtual media" on page 1.

Table 8. Virtual media session settings

Setting	Description
Session Settings: Virtual Media locked to KVM session	The locking option specifies whether a virtual media session is locked to the KVM session on the target device. When locking is enabled (default) and the KVM session is closed, the virtual media session will also be closed. When locking is disabled and the KVM session is closed, the virtual media session will remain active.
Session Settings: Allow Reserved Sessions	Ensures that a virtual media connection can only be accessed with your username and that no other user can create a KVM connection to that target device. When the associated KVM session is disconnected, the virtual media session may be disconnected according to the Locked setting in the Virtual Media dialog box.
Drive Mappings: Virtual Media Access Mode	You may set the access mode for mapped drives to read-only or read-write. When the access mode is read-only, the user will not be able to write data to the mapped drive on the client server. When the access mode is read-write, the user will be able to read and write data from/to the mapped drive. If the mapped drive is read-only by design (for example, a CD-ROM drive, DVD-ROM drive or ISO images), the configured read-write access mode will be 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 wish to prevent the user from writing data to it. You can have one DVD drive and one mass storage device mapped concurrently. A CD drive, DVD drive, or ISO disk image file is mapped as a virtual CD/DVD drive. NOTE: Virtual mapping of ISO images is supported on Windows 2008 targets.

Setting	Description
Encryption Level	You may configure encryption levels for virtual media sessions. The choices are: None (default), 128-bit SSL (ARCFOUR), DES, 3DES, and AES.
Virtual Media Access per CO cable: Enable VM/Disable VM	The Virtual Media Access per the CO cable section lists all VCO and VCO2 cables. The list includes details about each cable, including the option to enable or disable virtual media for each cable.

To set virtual media options:

1. From the side navigation bar, select *Unit Views* > *Appliance* > *Appliance Settings* > *Sessions* > *Virtual Media* to open the Appliance Virtual Media Session Settings screen.
2. Either enable or disable the *Virtual Media locked to KVM Sessions* check box.
3. Either enable or disable the *Allow Reserved Sessions* check box.
4. Select one of the following options from the Virtual Media Access Mode from the drop-down menu: *Read-Only* or *Read-Write*.
5. Select one of the Encryption Levels that you wish to be supported.
6. Select the check box next to each CO cable for which you want to enable virtual media and click *Enable VM*.

   -or-

   Select the check box next to each CO cable for which you want to disable virtual media and click *Disable VM*.
7. Click *Save*.

Local virtual media settings

Local users can also determine the behavior of virtual media from the Local Session screen. In addition to connecting and disconnecting a virtual media session, you can configure the settings in the following table.

Table 9. Local Virtual Media Session Settings

Setting	Description
CD ROM/ DVD ROM	Allows virtual media sessions to the first detected CD-ROM or DVD-ROM (read-only) drives. Enable this check box to establish a virtual media CD-ROM or DVD-ROM connection to a target device. Disable to end a virtual media CD-ROM or DVD-ROM connection to a target device.
Mass Storage	Allows virtual media sessions to the first detected mass storage drive. Enable this check box to establish a virtual media mass storage connection to a target device. Disable to end a virtual media mass storage connection to a target device.
Reserved	Ensures that a virtual media connection can only be accessed with your username and that no other user can create a KVM connection to that target device.

To configure local virtual media settings:

1. From the side navigation bar, select *Local Session*.
2. Select to enable or deselect to disable any of the Virtual Media Session options.

Modem settings

From the Appliance Modem Settings screen, you can configure several modem settings, as well as view the following modem settings: Local Address, Remote Address, Subnet Mask, and Gateway.

For information on connecting your switch to a modem, see Connecting the switch hardware on page 10.

To configure modem settings:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *Modem* to open the Appliance Modem Settings screen.
2. Either enable or disable the *Modem sessions can preempt digital sessions* check box.
3. Select an Authentication Timeout time from 30 to 300 seconds, and an Inactivity Timeout time from 1 to 60 minutes.
4. Select *Save*.

Scan mode

In Scan mode, the switch automatically scans from port to port (target device to target device). You can scan multiple target devices, specifying which devices to scan. The scanning order is determined by placement of the target device in the list. You can also configure the amount of time before the scan moves to the next target device in the sequence.

NOTE: The Scan button is disabled if you are connected via modem.

To add target devices to the Scan list:

1. From the side navigation bar, select *Unit View* > *Target Devices* to open the Target Devices screen.
2. Select the check boxes next to the names of the target devices you wish to scan.
3. Click *Scan*.

To configure Scan Time:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *Local Port UI* to open the Local Port UI Settings screen.

2. Under the Scan Mode heading, enter an amount of time in seconds (from 3-255) in the Scan Time field.
3. Click *Save*.

DSView device IP addresses

You can contact and register an unmanaged switch with a DSView server by specifying the IP addresses of up to four DSView servers.

To configure the DSView server IP address:

1. On the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *User Accounts* > *DSView*. The DSView Settings screen is displayed.
2. Enter up to four DSView software server IP addresses that you want to contact in the Server 1 - 4 fields.
3. Click *Save*.

User Accounts

Managing local accounts

The switch OBWI provides local and login security through administrator-defined user accounts. By selecting *Local Accounts* on the side navigation bar, administrators may add and delete users, define user preemption, and access levels and change passwords.

Access levels

When a user account is added, the user may be assigned to any of the following access levels: Appliance administrators, User administrators, and Users.

Table 10. Allowed Operations by Access Level

	Access Level		
Operation	**Appliance Administrator**	**User Administrator**	**Users**
Configure interface system-level settings	Yes	No	No
Configure access rights	Yes	Yes	No
Add, change and delete user accounts	Yes, for all access levels	Yes, for users and user administrators only	No
Change your own password	Yes	Yes	Yes
Access target device	Yes, all target devices	Yes, all target devices	Yes, if allowed

To add a new user account (administrator only):

1. On the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *User Accounts* > *Local Accounts* to open the Appliance Local User Accounts screen.
2. Click the *Add* button.
3. Enter the name and password of the new user in the blanks provided.
4. Select the preemption and access levels for the new user.
5. Select any of the available target devices that you wish to assign to the user account and click *Add*.

NOTE: User administrators and appliance administrators can access all target devices.

6. Click *Save*.

To delete a user account (administrator only):

1. On the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *User Accounts* > *Local Accounts* to open the Appliance Local User Accounts screen.
2. Click the check box to the left of each account that you wish to delete, then click *Delete*.

To edit a user account (administrator or active user only):

1. On the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *User Accounts* > *Local Accounts*. The Appliance Local User Accounts screen is displayed.
2. Click the name of the user you wish to edit. The user profile will appear.
3. Fill out the user information on the screen, then click *Save*.

SNMP settings

SNMP is a protocol used to communicate management information between network management applications and the switch. Other SNMP managers can communicate with your switch by accessing MIB-II and the public portion of the enterprise MIB. When you open the SNMP screen, the OBWI will retrieve the SNMP parameters from the unit.

From the SNMP screen, you can enter system information and community strings. You may also designate which stations can manage the switch as well as receive SNMP traps from the switch. If you select *Enable SNMP*, the unit will respond to SNMP requests over UDP port 161.

To configure general SNMP settings:

1. Select *Unit View* > *Appliance* > *Appliance Settings* > *SNMP* > *SNMP Settings* to open the SNMP screen.

2. Click to enable the *Enable SNMP* check box to allow the switch to respond to SNMP requests over UDP port 161.
3. Enter the system's fully qualified domain name in the Name field, as well as a node contact person in the Contact field.
4. Enter the Read, Write, and Trap community names. These specify the community strings that must be used in SNMP actions. The Read and Write strings only apply to SNMP over UDP port 161 and act as passwords that protect access to the switch. The values can be up to 64 characters in length. These fields may not be left blank.
5. Type the address of up to four management workstations that are allowed to manage this switch in the Allowable Managers fields. Alternatively, you may leave these fields blank to allow any station to manage the Remote Console Switch.
6. Click *Save*.

Event settings

An event is a notification sent by the switch to a management station indicating that something has occurred that may require further attention.

To enable individual events:

1. Select *Unit View* > *Appliance* > *Appliance Settings* > *Auditing* > *Events* to open the Events screen.
2. Specify the events that will generate notifications by clicking the appropriate check boxes in the list.

   -or-

   Select or clear the check box next to Event Name to select or deselect the entire list.
3. Click *Save*.

Setting event destinations

You can configure audit events to be sent to SNMP trap destinations and Syslog servers. The events enabled on the Events screen are sent to all the servers listed on the Event Destination screen.

1. Select *Unit View* > *Appliance* > *Appliance Settings* > *Auditing* > *Destinations* to open the Event Destinations screen.
2. Type the address of up to four management workstations to which this switch will send events in the SNMP Trap Destination fields, as well as up to four Syslog servers.
3. Click *Save*.

Configuring CO cables

From the switch, you can display a list of the attached CO cables, as well as the following information about each cable: eID (electronic ID), Port, Status, Application, Interface Type, and USB Speed. You can click on one of the cables to view the following additional information: Switch Type, Boot Version, Hardware Version, FPGA Version, Version Available, and Upgrade Status.

You can also perform the following tasks: delete offline CO cables, upgrade the cable firmware, set the USB speed, or decommission the cables.

To delete offline CO cables:

1. From the side navigation bar, click *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *CO* to open the Appliance CO screen.
2. Click *Delete Offline*.

To set the USB Speed (for VCO cables only):

1. From the side navigation bar, click *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *COs* to open the Appliance COs screen.
2. Select the check box(es) next to the CO(s) that you wish to modify.
3. Click either *Set USB 1.1 Speed* or *Set USB 2.0 Speed*.

Upgrading CO cables

The CO cable Flash upgrade feature allows appliance administrators to update the CO cable with the latest firmware available. This update can be performed using the switch user interface or DSView software.

After the Flash memory is reprogrammed with the upgrade, the switch performs a soft reset, which terminates all CO cable sessions. A target device experiencing a CO cable firmware update may or may not display as disconnected. The target device will appear normally when the Flash update is completed.

If the appliance is configured to Auto-Upgrade CO cables, the CO cables will automatically update when the switch is updated. To update your switch firmware, see GCM switch tools on page 24 or the DSView 3 Software Online Help. If issues occur during the normal upgrade process, CO cables may also be force-upgraded when needed.

To upgrade the CO firmware:

1. From the side navigation bar, click *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *COs* to open the Appliance COs screen.
2. Select the check box(es) next to the CO cable(s) that you wish to upgrade and click *Upgrade*.

Attention: Disconnecting a CO cable during a firmware update or cycling power to the target device will render the module inoperable and require the CO cable to be returned to the factory for repair.

Power device settings

NOTE: You must have administrator privileges to change power control device settings.

From the Appliance Power Devices screen, you can view a list of connected power devices, as well as the following information about each power device: Name, Port, Status, Version, Model, Buzzer, Alarm, and Temperature. You can also select a power device, then select *Settings* to view the following details about that power device: Name, Description, Status, Version, Sockets, Vendor Name, Model, and Input Feeds.

If a target device is connected to a power control device outlet, you can turn on, turn off or cycle (turn off, then turn on) the target device.

To turn on, turn off or power cycle a target device:

1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *Power Devices* to open the Appliance Power Devices screen.
2. Click the name of the unit you wish to configure and select *Sockets*.
3. Select the check box to the left of the socket(s) that you wish to configure.
4. Click *On*, *Off*, or *Cycle*, as desired.

To delete offline power devices:

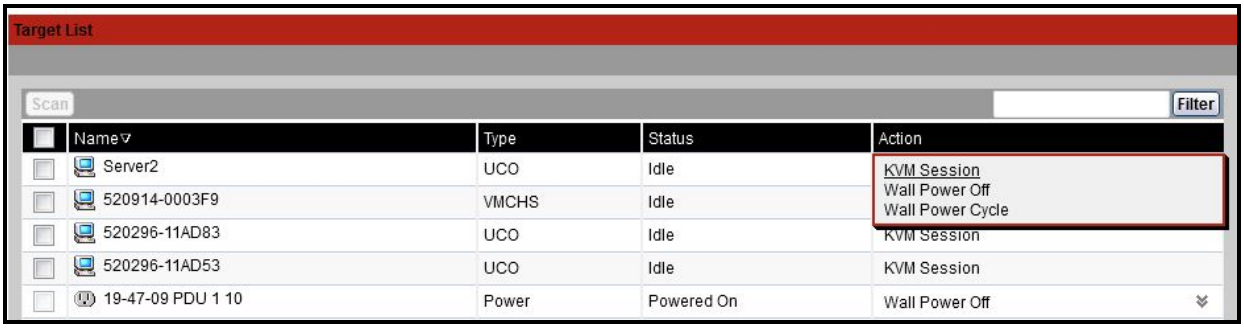
1. From the side navigation bar, select *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *Power Devices* to open the Appliance Power Devices screen.
2. Click *Delete Offline*.

Associated target servers and power outlets

By naming one or more power outlets with the same name as a target server, the outlets are linked or associated with the target server for easier control. In the OBWI Target Devices page, power control actions are selectable for a target with linked outlets. On the Target Overview page, a Wall Outlet Power table shows the outlets linked with a target device.

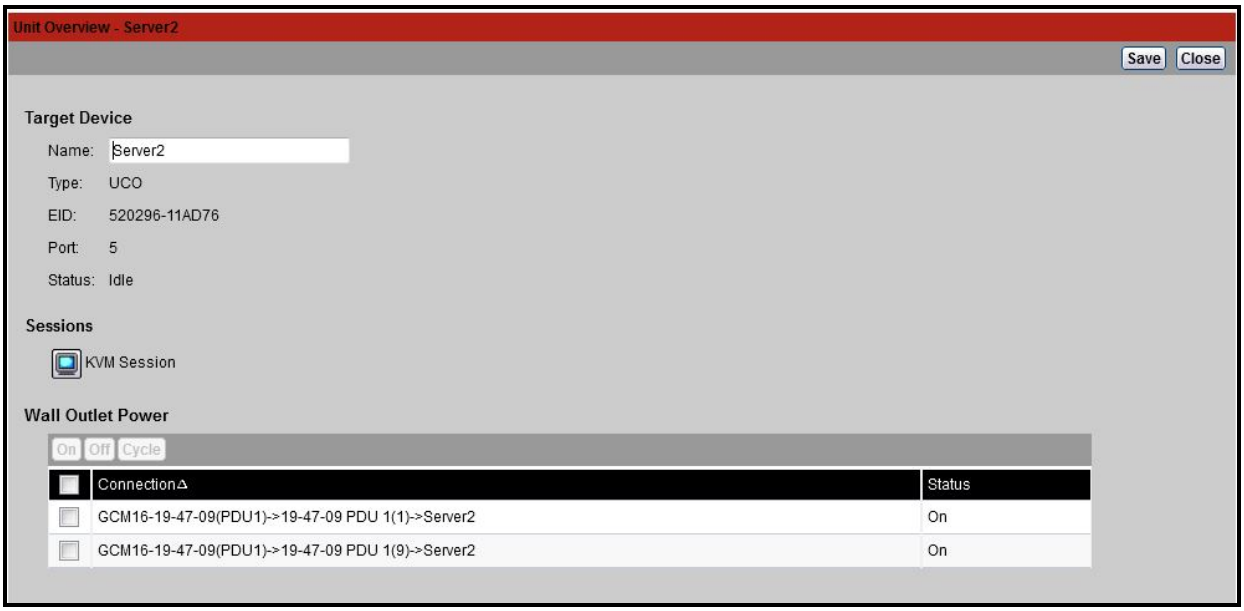
In the following figure, the target device named Server2 has linked power outlets. Clicking on the drop-down menu arrow in the Action column shows the additional power actions available.

Figure 5. Target devices



In the following figure, the target Unit Overview page for Server2 shows the Wall Outlet Power, where outlet 1 and outlet 9 from PDU 1 are linked to Server2.

Figure 6. Target overview Server2



Grouping power outlets

Multiple power outlets may be given the same name to link them into one group, which is listed as one target device. Power actions performed on the Target Devices page are applied to all applicable outlets. Power control actions for specific power outlets of a target may be performed on the Unit Overview page.

Default outlet names

On the Power Devices page, the check box “Assign Default Names to Outlets” controls whether or not power outlets are given default names for a power device, as shown in the following figure. Only power outlets with names are listed on the Target page. Default assigned power outlet names may be removed by clearing the "Assign Default Names to Outlets" check box and saving. Power outlets

without names are assigned default names by turning on “Assign Default Names to Outlets” and saving.

Assigning an outlet name

On the Power Device Outlet Settings page, three options are available for assigning the name of a outlet as shown in the following figure. The options are Manual Name assignment, Link to Target Device and Do Not Display as Target Device.

Figure 7. Power device outlet settings page

- The Manual Name assignment gives a unique name to a outlet. The name must be unique for all the COs and power outlet names. An attempt to specify a manual name which is not unique will result in an error and the name will not be saved.
- The Link to Target Device assignment links the outlet to another target name (either an outlet or CO) for power control of the named target. When an outlet is linked to a CO target name, typically the outlet physically provides power to the server attached to the CO.
- The Do Not Display as Target Device option gives the outlet a blank name, which prevents it from being displayed on the Target Devices page. This option may be used for spare outlets to remove them from the Target Devices page.

Access control inheritance

When a power outlet name is changed by linking it to a target, the outlet inherits the access control already configured for that target name. When a CO is added, if the name retrieved from the CO matches the name of an existing target, the new CO inherits the access control from that target. When a target device is renamed, all the COs and outlets of that target are renamed, and they carry forward the access control previously configured for the old target name.

Renaming of a target device

On the Target Overview page, the name for that target may be changed to any unique target name. The name must be unique for the set of all targets, including COs and power outlets. When a target is renamed, all outlets linked to that target are also given the new target name.

Prioritized status of target devices

On the Target Devices page, a target with linked power outlets controls multiple devices. The Status value displayed for a target is chosen as the highest priority of all the status values of the devices. The following table shows the possible status values in priority order (highest to lowest) and the applicable target device types.

Table 11. Target Status Values

Status Value	Applicable for:		Status Description
	CO	Power Outlet	
In Use	x	N/A	A session is active
Path Blocked	x	N/A	Path to Target is in use by another session
Upgrading	x	N/A	CO is being upgraded
Powering On	N/A	x	One or more outlets are powering on
Powering Off	N/A	x	One or more outlets are powering off
No Power	x	N/A	No power detected on CO
Partial Power	N/A	x	Target has outlets in both on and off states
Locked-Off	N/A	x	One or more outlets are locked on
Powered Off	N/A	x	One or more outlets are powered off
Locked-On	N/A	x	One or more outlets are locked off
Idle	x	N/A	No session active; CO has power
Powered On	N/A	x	Outlets are powered on

When a target device has multiple power outlets linked by name and they do not have a common power state, the appliance may consider the Locked-Off outlet status as Off, and the Locked-On outlet status as On. The following table lists the resulting Status values for combinations of two outlet status values.

Table 12. Multiple outlet status values and displayed status

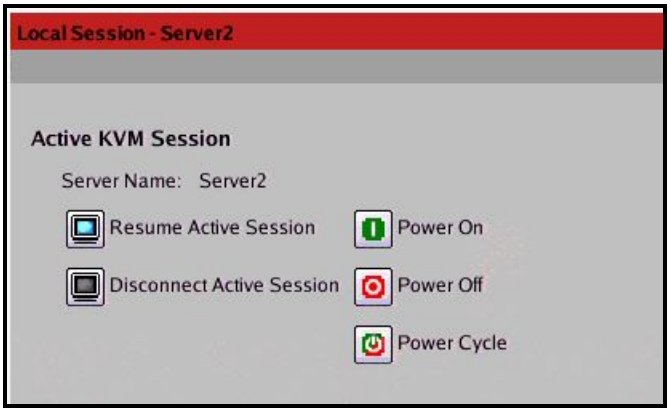
Outlet 1 Status	Outlet 2 Status	Resulting Status
Off	Off	Off
Off	On	Partial Power
On	On	Powered On
Locked-On	On	Powered On
Locked-On	Locked-On	Locked-On
Locked-On	Off	Partial Power

Outlet 1 Status	Outlet 2 Status	Resulting Status
Locked-Off	On	Partial Power
Locked-Off	Locked-Off	Locked-Off
Locked-Off	Off	Powered Off
Locked-On	Locked-Off	Partial Power

Local Session page on the local port

On the local port's Local Session page, when the target of the active session has power outlets linked, three power controls are displayed on the page under the Active session. The following figure illustrates the power controls displayed for an active local port session for a target named Server2.

Figure 8. Local Session page with power controls



Chapter 4. About the KVM Video Viewer

The KVM Video Viewer is used to conduct a KVM session with one or more target devices attached to one or more GCM switches. You may optionally use KVM session profiles to control session behavior on target devices. When you connect to a device using the KVM Video Viewer, the target device desktop appears in a separate window. The KVM Video Viewer window supports a 3-button mouse.

Virtual Media Sessions

Virtual media sessions, which are supported on certain KVM switches, are opened from the KVM Video Viewer.

KVM Session

GCM switches use either a Java-based program or an ActiveX applet to display the KVM Video Viewer window. The Java-based KVM Video Viewer is launched from a Mozilla® Firefox® or Google® Chrome® based client when a KVM session is requested. The ActiveX KVM Video Viewer is launched from a Microsoft® Internet Explorer® browser.

KVM sessions may be launched to devices from any supported KVM switch. Each KVM session will be established using the configured encryption level. To launch a KVM session, a user must have been assigned rights or belong to a user group which has been assigned rights to establish a KVM session.

Performance Errors

Each opened KVM Video Viewer window requires additional system memory. If you attempt to open more KVM Video Viewer windows than your system memory allows, you will receive an out of memory error and the requested KVM Video Viewer window will not open.

NOTE: Opening more than four simultaneous KVM Video Viewer windows may affect system performance and is not recommended.

When using a non-proxied connection, video performance over a slower network connection may be less than optimal. Since certain color settings use less network bandwidth than others, changing the color settings may increase video performance. For optimal video performance over a slower network connection, a color setting such as Grayscale/Best Compression or Low Color/High Compression is recommended.

Java Versions

The KVM Video Viewer client requires Java when launched from Mozilla Firefox browsers. The supported Java versions are 1.6 update 45 and 1.7 update 51. The software client automatically downloads and installs the JRE (Java Runtime Environment) the first time the KVM Video Viewer or Telnet Viewer is launched if the client machine did not have any supported JRE installed.

On a Windows client, it is recommended that the JRE (Java Runtime Environment) be installed in the C:\Program Files\ location. If your system automatically installs programs in another location, you may not be able to launch the KVM Video Viewer. In this case, you can configure Java to find the JRE.

To configure Java to find the JRE:

1. Access the Java Control Panel on your client workstation.
2. Select the *Java* tab.
3. In the Java Application Runtime Settings panel, click *View*.
4. Change the path to the installed JRE.
5. Click *OK*.

Opening a KVM Session

To open a KVM session:

1. From the side navigation bar of the switch web UI, click *Unit View - Target Devices*.
2. Click the KVM Session link for the target device you wish to view.
3. The KVM Video Viewer launches in a new window.

Opening an exclusive KVM session

An exclusive KVM connection is used when you need to access a port while excluding all other users. When a port is selected with the Exclusive KVM connection setting enabled, no other user in the system may switch to that port. Once you've launched a KVM session, click *Tools - Exclusive Mode* to enable an exclusive session.

Saving the View

The display of a KVM Video Viewer window may be saved to a file or to the clipboard for pasting into another program.

To capture the KVM Video Viewer window to a file:

1. Select *File - Capture to File* from the KVM Video Viewer menu. The Save As dialog box appears.
2. Enter a file name and choose a location to save the file.
3. Click *Save*.

To capture the KVM Video Viewer window to your clipboard:

Select *File - Capture to Clipboard* from the KVM Video Viewer menu. The image data is saved to the clipboard.

Pasting Text

Text from the client machine may be pasted to an appropriate program, for example Notepad, on the host either via a file or the clipboard.

To paste text from a file from the client machine to the host:

1. Select *File - Send Text File Contents* from the KVM Video Viewer menu. The Open dialog box appears.
2. Browse to the location on the client machine where the file is saved, click the file, then click *Open*.

To paste text from your clipboard to the host:

Select *File - Paste Text* from the KVM Video Viewer menu.

Closing a KVM Video Viewer Session

To close a KVM Video Viewer session:

Select *File - Exit* from the KVM Video Viewer menu.

KVM Video Viewer Profile Settings

The profile settings for the KVM Video Viewer are Refresh, Fit, Full Screen, Mini-Mode, Scaling, Color Modes, Session User List and Status.

NOTE: Each of the settings in this section can be accessed from the View tab of the KVM Video Viewer menu.

Refresh

The Refresh setting enables background refresh.

Clicking *View - Refresh* updates the Video Viewer window.

Fit

Click *View - Fit* to resize the KVM Video Viewer window to fit the size needed to completely display the resolution of the digitized video.

Select the *Fit* menu item from the View menu to resize the Viewer window to the size needed to completely display the resolution of the digitized video. If the target server's resolution is higher than the client workstation's resolution, and auto-scaling is in effect, the target image will be scaled to fit in the client window. In this case, the client window will occupy as much of the client workstation's desktop as necessary to scale both horizontally and vertically. If auto-scaling is not in effect, then the client window will be maximized to fit on the client workstation window and scroll bars will appear to allow access to the target server's image.

Full Screen

Click *View - Full Screen* to toggle the client between Full Screen mode and Windowed mode. When the Viewer is in Full Screen mode, the display occupies the entire user workstation's display.

When the Full Screen mode is enabled, the client will take the following actions:

- Resize the Viewer window to completely fill the user's desktop.
- Enable auto-scaling.
- Disable the entire Scaling menu, thereby not allowing the user to change the resolution while in Full Screen mode.
- Perform other tasks when Full Screen mode is enabled, such as turn on Keyboard Pass-through and display the floating menu bar.

When the Full Screen mode is exited, Windowed mode resumes and the following actions take place:

- Resize the Viewer window to its former size.
- Revert to the previous scaling mode.
- Temporarily disable all menu items in the Scaling menu. Once the resumed resolution has been confirmed, the Scaling menu items will be re-enabled.
- Resume keyboard pass-through and do other tasks currently performed by the Viewer client when in Windowed mode.

Mini-Mode

Click *View - Mini-Mode* to toggle the client between Mini-Mode and Windowed mode. In Mini-Mode, the KVM Video Viewer client will display a thumbnail view of the host server display and provide no

input for keyboard or mouse. The dimensions of the digitized video will not be changed while in Mini-Mode.

NOTE: To exit Mini-Mode, double-click on the Mini-Mode window or right-click on the Mini-Mode window and de-select the Mini-Mode menu item.

To select the window size for Mini-Mode:

1. Click *Tools - Session Options*.
2. From the Mini-Mode tab, use the drop-down menu to select the window size.
3. Click *OK*.

Scaling

Click *View - Scaling* to change the KVM Video Viewer window resolution. You may choose *Auto Scale, Server Resolution* or select a fixed resolution.

When auto scaling is enabled, the KVM Video Viewer will automatically adjust the display if the window size changes during a session. When a user accesses a channel using sharing, the display will be adjusted to match the input resolution selected by the primary user of that channel. The Viewer prevents a secondary user from changing the resolution and affecting the primary user. If the target device resolution changes any time during a session, the display will be adjusted automatically.

When enabled, the display window is sized to match the resolution of the server being viewed.

You can choose to maintain the aspect ratio for video in Windowed or Full Screen mode. Select *Tools - Session Options* then check the box next to Windowed or Full Screen Mode, then click *Apply*.

Color Modes

Click *View - Color Modes* to change the color depth the KVM Video Viewer will use.

The Dambrackas Video Compression™ (DVC) algorithm allows you to display more colors for the best fidelity, or fewer colors to reduce the volume of data transferred on the network.

The choices are (in descending color quantity): Best Color, Medium Color/Medium Compression, Low Color/High Compression or Gray Scale/Best Compression.

Session User List

Click *View - Connected Users* to view active users of this session.

Status Bar

Click *View - Status Bar* to display or hide the status bar at the bottom of the Viewer window.

Macros

The KVM Video Viewer window macro function allows you to:

- Send multiple keystrokes to a device, including keystrokes that you cannot generate without affecting your local system, such as **Ctrl-Alt-Delete.**
- Send a macro from a predefined macro group. Macro groups for Windows, Linux and Sun are already defined.
- Create, edit and delete your own macros. When you create or edit a macro, you may type the desired keystrokes or you may select from among several available categories of keystrokes. Each category contains a set of keystroke combinations. Selecting from the available categories and keystrokes saves time and eliminates the risk of typographical errors.

NOTE: Macro group settings are device-specific; they may be set differently for each device.

To send a macro:

Select *Macros - <desired macro>* from the KVM Video Viewer menu.

To create a macro:

1. Select *Macros - User Defined Macros- Manage* from the KVM Video Viewer menu.
2. Click *New*.
3. Type the keys for the macro in the dialog box.
4. Click *Create.*

To delete a macro:

1. Select *Macros - User Defined Macros - Manage* from the KVM Video Viewer menu.
2. Select the desired macro from the Defined Macros list and then click *Delete*.
3. Click *Yes* to confirm the deletion.

Global Macros

The KVM Video Viewer supports global macros from the DSView software. An administrator can create and designate a macro as Global or Personal. Global macros are created and used by the KVM viewer client but are stored on the DSView servers. Personal macros are associated with the name of the user.

The DSView server will send the macros groups and their associated macros as part of the preferences saved on the server. One of the macro groups will be used as the default macro group for the DSView software profile. The macros in the default group will be added to the Macros menu in the KVM Video Viewer.

The Macros menu of a viewer connected to a DSView server also contains Macros and Macro Groups menu items. From these menus, an administrator can create and manage custom macros and macros groups.

Macro Groups

From the DSView software, launch a KVM Video Viewer session and click *Macros-Configure-Macro Groups* to view and manage the macro groups on the DSView server. By default, three groups are already defined - Linux, Sun and Windows. You can create custom groups or edit existing groups.

To select a macro group to use as the default on the Macros menus of the KVM Video Viewer window, click on a group and then check the Display on Menu box. You can use the radio button at the bottom of the screen to view all the macro groups or just the personal or global groups.

NOTE: Only users with sufficient privileges can create, edit or delete a global macro group.

To create a new macro group:

1. Click *Create*.
2. Enter the name in the Macro Group Name field and select the radio button for Global or Personal as the group type.
3. From the Macros Available field, select the macros you want to add to the group and click *Add*.

NOTE: Once the macros are in the Macros In Group field, you can click *Move Up* or *Move Down* to re-order the macros.

4. Click *OK*.

To edit a macro group:

1. Click on the name of the group you want to edit and click *Edit*.
2. Make changes as desired and click *OK*.

To delete a macro group:

1. Click on the name of the group you want to delete and click *Delete*.
2. Click *OK* at the confirmation screen.

To copy a macro group:

1. Click on the name of the group you want to copy and click *Copy*.
2. Enter a new name for the copied group and select the group type.
3. Click *OK*.

Macros configuration

From the DSView software, launch a KVM Video Viewer session and click *Macros-Configure-Macros* to view and manage individual macros on the DSView server.

NOTE: You can use the radio button at the bottom right of the screen to view all the macro groups or just the personal or global groups.

To immediately send a macro to the target server:

Click on the macro and click *Execute*.

To create a new macro:

1. Click *Create*.
2. Enter a name for the macro in the Macro Name field and use the radio button to select Personal or Global as the macro type.
3. Use the drop-down menus to select the keyboard type and icon.
4. Use the virtual keyboard to enter the keystrokes for the macro in the Keystrokes field.

NOTE: Click *Remove* to remove the highlighted keystroke or click *Reset* to reset the macro. You can also re-arrange the order of the keystrokes by clicking *Move Up* or *Move Down*.

5. When finished, click OK.

To edit a macro:

1. Click on the name of the macro you want to edit and click *Edit*.
2. Make changes as desired and click *OK*.

To delete a macro:

1. Click on the name of the macro you want to delete and click *Delete*.
2. Click *OK* at the confirmation screen.

To copy a macro:

1. Click on the name of the macro you want to copy and click *Copy*.
2. Enter a new name for the copied macro and select its type.
3. Click *OK*.

Virtual Media

Use the virtual media feature on the client workstation to map a physical drive on that machine as a virtual drive on a target device. The client may also add and map an ISO or floppy image file as a virtual drive on the target device.

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

- A CD/DVD drive, disk image file (such as an ISO or a mass storage device) is mapped as a virtual CD drive.
- A floppy drive, USB memory device, a floppy image file or other media type is mapped as a virtual mass storage device.

Requirements

The target device must be connected to the KVM switch that supports virtual media with an IQ module that supports virtual media.

The target device must be intrinsically able to use the types of USB2-compatible media that you virtually map. If the target device does not support a portable USB memory device, you cannot map that on the client machine as a virtual media drive on the target device.

The user (or user group to which the user belongs) must have permission to establish virtual media sessions and/or reserved virtual media sessions to the target device.

Only one virtual media session may be active to a target device at one time.

NOTE: All steps in this section can be done by accessing the Virtual Media tab from the KVM Video Viewer menu.

To launch a virtual media session:

Select *Tools - Virtual Media*.

To map a virtual media drive:

1. Launch a virtual media session.
2. Map a physical drive as a virtual media drive:
    a. In the Virtual Media menu, select the drive you wish to map. The Mapping Dialog box will appear that allows you to select a disk image file or a physical device to map.
    b. If you wish to limit the mapped drive to read-only access, click the Read Only checkbox in the Mapping Dialog box. If the virtual media session settings were previously configured so that all mapped drives must be read only, this checkbox will already be enabled and cannot be changed.

    You might wish to enable the Read Only checkbox if the session settings enabled read and write access, but you wished to limit a particular drive's access to read only.
3. Add and map an ISO or floppy image as a virtual media drive. In the Mapping dialog box, from the drop-down menu, select the desired image file and click *Map Device*.

NOTE: Disk image files ending in either .iso or .img will display.

-or-

In the Mapping dialog box, from the drop-down menu, select the drive with the image file and click browse. Browse to the location of the file and click *Open*.

-or-

If the client workstation's operating system supports drag-and-drop, select the desired ISO or floppy image file from a program such as Windows Explorer or Mac Finder and drag it onto the Mapping dialog box.

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

To unmap a virtual media drive:

1. From the Virtual Media menu, select the menu item of the mapped device next to the drive you wish to unmap.
2. You will be prompted to confirm. Confirm or cancel the unmapping.
3. Repeat for any additional virtual media drives you wish to unmap.

To display virtual media drive details:

1. Display the Stats dialog box from the *Tools-Stats* tab of the KVM Video Viewer menu. The dialog box expands to display the Details table. Each row indicates:
   - Target Drive - Name used for the mapped drive, such as Virtual CD 1 or Virtual CD 2.
   - Mapped to - Identical to Drive information that appears 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 table, click *Details* again.

To reset all USB devices on the target device:

NOTE: 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 Stats dialog box, click *Details*.
2. The Details box will appear. Click *USB Reset*.
3. A warning message will appear, indicating the possible effects of the reset. Confirm or cancel the reset.
4. To close the Details box, click *Details* again.
5. Exporting

Creating an image

You can create an image file from a source file folder. The created image can then be mapped. You can also add an image file.

To create or add an image:

1. Select *Tools - Virtual Media* from the KVM Video Viewer menu.
2. Click *Create Image* and browse to the location where you want to create the image.
3. After the image has been created, check the Mapped checkbox to map the image.
4. Click *Exit*.

Session Options

The tabs located within session options are General, Mouse and Toolbar.

NOTE: Each of the settings in this section can be accessed from the *Tools - Session Options* tab of the KVM Video Viewer menu.

General

The Keyboard Pass Through mode setting enables or disables keyboard pass through.

Keystrokes that a user enters may be interpreted in two ways, depending on the screen mode of the KVM Video Viewer window.

- If a KVM Video Viewer window is in Full Screen mode, keystrokes and keyboard combinations are sent to the remote server being viewed.
- If a KVM Video Viewer window is in regular Desktop mode, Keyboard Pass Through mode allows you to control whether the remote server or local computer will recognize certain keystrokes or keystroke combinations.

When Keyboard Pass Through mode is enabled, keystrokes and keystroke combinations are sent to the remote server being viewed when the KVM Video Viewer window is active.

To enable Keyboard Pass Through mode:

1. Select *Tools - Session Options.*
2. Click the *General* tab.
3. Check the box next to Pass-through all keystrokes to target.
4. Click *OK*.

To enter Single Cursor mode:

Select *Tools - Single Cursor Mode*. The local cursor will not appear and all movements will be relative to the target device.

To exit Single Cursor mode:

Press they specified key to exit Single Cursor mode. You can specify which key is used under *Tools - Session Options*.

Mouse Synchronization

Enabling Mouse Synchronization in the KVM session profile provides improved mouse tracking on the target device. If Mouse Synchronization is enabled, it is not necessary to disable mouse acceleration on the target device.

The Video Viewer window offers five appearance choices for the local mouse cursor. You can also choose no cursor or the default cursor.

NOTE: Mouse Synchronization is supported on Windows, Macintosh and Linux (RHEL 6.x or later and SLES 11) target devices connected with a USB-2 IQ module.

To set Mouse Synchronization

1. Select *Tools - Session Options.*
2. Click the *Mouse* tab.
3. Under the Local Cursor heading, select cursor type you want to use.
4. Under the Mouse Scaling heading, use the radio button to select the desired speed. High sets a faster tracking speed while Low sets a slower tracking speed.
5. Under the Single Cursor heading, use the drop-down menu to specify a key for exiting Single Cursor mode.
6. Under the Mouse Synchronization heading, the current status is shown. Enable or disable the Enable Synchronization checkbox.

NOTE: On supported system configurations, the Mouse Synchronization status is Available. If the target device is running a supported operating system but is not connected with a USB-2 IQ module, the status is Not Supported. If the target device is connected with USB-2 IQ module but is not running a Windows or Macintosh operating system, the status is Not Available.

7. Click *Apply*.

Certificate

From the *Tools - Session Options - Certificate* menu, you can view the current session's certificate. You can also set where the certificate is stored on the local machine and empty certificates from that location.

Automatic Video Adjust

From the *Tools* tab of the KVM Video Viewer menu, click *Automatic Video Adjust* to automatically adjust the video. A green screen with yellow lettering may appear during auto-adjustment.

Manual Video Adjustment

Generally, the Video Viewer window automatic adjustment features optimize the video for the best possible view. However, you can fine-tune the video, with the help of Avocent Technical Support, by clicking *Manual Video Adjust* from the Tools tab of the Video Viewer window. You can also verify the level of packets per second required to support a static screen by observing the packet rate located in the lower left-hand corner of the dialog box.

NOTE: Video adjustment is a per target setting.

Figure 9. Manual Video Adjust Window

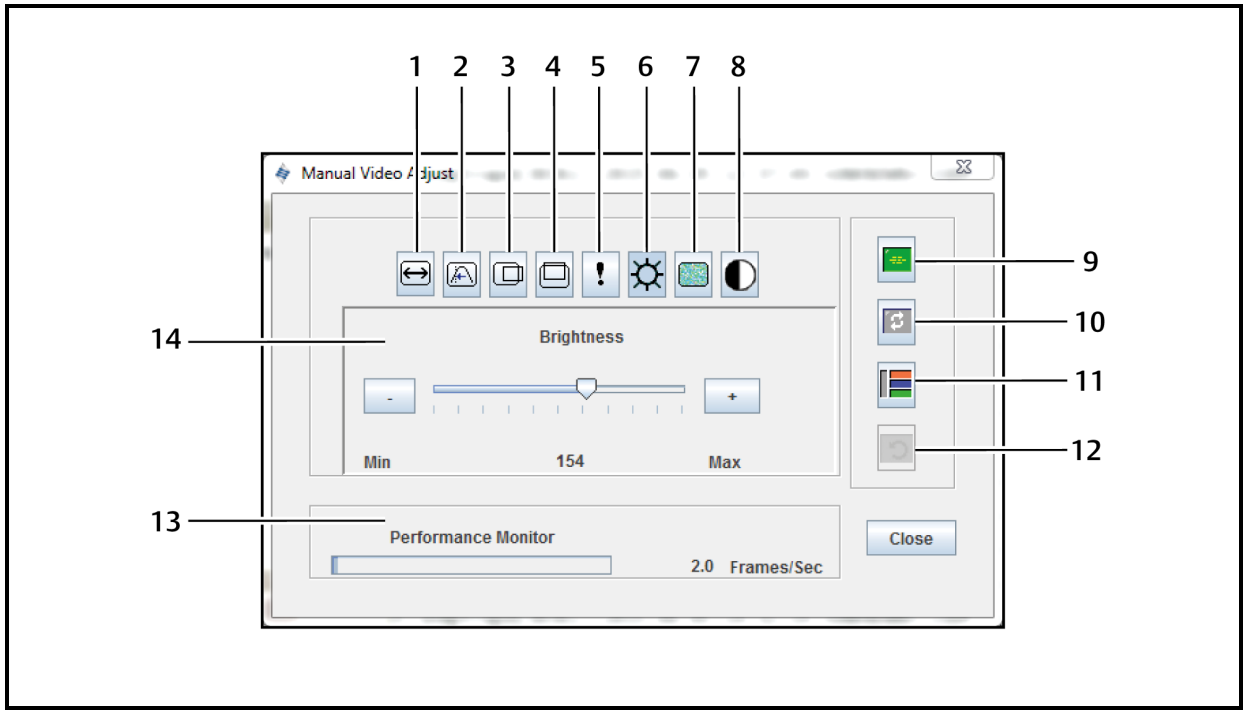


Table 13. Manual Video Adjust Window Descriptions

Number	Description	Number	Description
1	Image Capture Width	8	Contrast

Number	Description	Number	Description
2	Pixel Sampling/Fine Adjust	9	Automatic Video Adjustment
3	Image Capture Horizontal Position	10	Refresh Image
4	Image Capture Vertical Position	11	Adjustment Bar
5	Pixel Noise Threshold	12	Revert Video to Initial Settings
6	Brightness	13	Performance Monitor
7	Block Noise Threshold		

To manually adjust the video quality of the window:

NOTE: The following video adjustments should be made only with the help of Avocent Technical Support.

1. Click *Tools - Manual Video Adjust* from the Video Viewer window menu.
2. Click the icon corresponding to the feature you wish to adjust.
3. Move the Contrast 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 display immediately in the Video Viewer window.
4. When finished, click *Close.*

Cursor Commands

The commands to enter and exit Single Cursor mode and the command to align the mouse cursors cannot be set in a KVM session profile.

NOTE: If the target device does not support the ability to disconnect and reconnect the mouse (almost all newer PCs do), then the mouse will become disabled and the device will have to be rebooted.

To prevent potential mouse conflicts, you may configure certain settings on each server connected to a managed appliance.

To align the mouse cursors:

Click *Tools - Align Local Cursor*. The local cursor will align with the cursor on the remote device.

NOTE: If cursors drift out of alignment, turn off mouse acceleration in the device.

Stats

To view frame rate, bandwidth, compression, packet rate and virtual media information, click *Tools - Stats*.

Power Control

If opening a session from the DSView software or some Avocent® Universal Management Gateway appliances, you can turn the host device on or off or power cycle it.

To manage power:

1. Open a KVM session from the DSView software or a supported appliance.
2. Select *Tools - Power Control* from the KVM Video Viewer menu.
3. Click the appropriate button to turn on, turn off or power cycle the device.
4. Click *Close* when finished.

Smart Cards

A smart card is a plastic card with an embedded chip that can be loaded with data. The KVM Video Viewer supports smart cards attached to the client workstation. You can insert a smart card into a reader and map it to the host server as though it were mounted directly to the host server.

To map a smart card:

1. From the *Tools* tab of the KVM Video Viewer menu, click *Map Smart Card*.
2. The Map Smart Card screen will open and display all available card readers along with their current state. Use the drop-down menu to select a reader and card to map.
3. Click *Map Card* to send a request to the target server to map the smart card to the remote device.

NOTE: If the selected reader does not have a smart card, a message will display requesting you to insert a card into the reader. If a reader is not detected, a message will display until a reader is detected.

Once a smart card has been mapped, the card will be displayed at the bottom of the Tools tab along with a checkmark indicating it has been mapped. If supported by the target server, an icon may also be displayed showing whether the smart card is mapped, not mapped or disabled.

Video Recording

The KVM Video Viewer contains a built-in video recorder and player. The recorder is essentially two recorders as it can record continuously and persistently.

Continuous recording

The continuous recorder can operate at all times a KVM session is in progress. It stores KVM video in periods of 30 seconds up to a maximum of either 30 minutes or the configured maximum disk space. If the maximum time or space is exceeded, the oldest periods are released.

Persistent recording

The KVM Video Viewer can also record KVM video for persistent storage. You can select where to save the video file and recording will continue until one of the following occurs:

- You click the *Stop Record* button.
- The KVM session is ended.
- The maximum file size of the video recording is reached.
- The disk storage space on the client workstation is depleted.

To configure the recording capacity:

1. Select *Tools - Session Options* from the KVM Video Viewer menu.
2. Click the *Video Recording* tab.
3. Under the Persistent Recording heading, enter the maximum file size for persistent recording.
4. Check the box to record continuously and enter the maximum file size for continuous recording.
5. Click *OK*.

To control or view persistent video:

1. Select *Tools - Recorder/Playback Controls* from the KVM Video Viewer menu.
2. Use the controls as described in the following table.

Table 14. DVR Player Controls

Icon	Control	Description
	Open	Opens the File dialog box to browse for and open a DVC file either created by the Record function on the KVM Video Viewer or downloaded from an appliance or service processor.
	Return To Start	When a persistent file is being played, clicking this button will cause the playback to move back to the start of the file. When a session is being recorded, clicking this button will cause the continuous recording buffer to go to its oldest data and start playing back from that point.
	Skip Back	When a file or continuous recording is being played, clicking this button will cause the play position to go back one 30-second period at a time. Each time it is clicked, the play position will move back to the start of the previous period. If the playback mode was Play or Fast Forward when this button was clicked, the playback will proceed at a speed of 1X. If the playback mode was Paused when this button was clicked, the playback will display the first frame of the previous period. If the continuous recording buffer reaches the play position, then playback will proceed at a speed of 1X.
	Play	Click this button to play the recording.
	Pause	While a file is being played, the Play button becomes the Pause button. Click it to pause the playback. During a Live session, clicking the *Pause* button will pause the Live playback. Live mode will change to Continuous and the Play button will be disabled.

Icon	Control	Description
	Recording Stop/Start	Click this button to open the Save dialog box. Use the drop-down menu to choose a location to save the recording. Once you've entered a filename and clicked *Save*, the recording will begin. While recording, click the button again to stop the recording.
	Fast Forward	During playback, click this button to fast forward one 30-second period at a time. Each time this button is clicked, the playback rate will increment by 10:1 until the fifth time it is clicked. The fifth time it is clicked will return the playback rate back to 10X.
	Go To End	When this button is clicked, the file or continuous recording that is being played back will go to the end of the recording. When a file is not being played but a KVM session is in progress, clicking this button will display the live video from the connected KVM session.
	Live	When this button is clicked, it will terminate the playback of a file or a continuous recording and display the video from the connected KVM session. If there is no connected KVM session (such as a file was being played back without a connected KVM session, or the KVM session has terminated), then this button will be disabled and grayed out.
	Slider	The slider at the bottom of the screen displays the progress of the playback in the context of the overall length of the file or continuous recording. It will act like a scrollbar in that the thumb will move from left to right as the recording is played back. If the video is paused and you click or drag the slider, it will move to that position and remain paused. If video is playing and you click or drag the slider, it will move to that position and continue playing.

Exporting video

You can create a video from a source file on the host and then export it to the client machine.

To export video:

1. Select *Tools - Export Video* from the KVM Videw Viewer menu.
2. Browse for the source file.
3. Browse for the exported file.
4. Use the drop-down menu to select the resolution.
5. Click *Export*.

Chapter 5. LDAP

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

If individual user accounts are stored on an LDAP-enabled directory service such as Active Directory, you can use the directory service to authenticate users. The default values given for the LDAP search and query parameters are defined for use with Active Directory.

The settings made in the OBWI let you configure your authentication configuration parameters. The software sends the username, password and other information to the appliance, which then determines whether the user has permission to view or change configuration parameters for the appliance in the OBWI.

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

Configuring LDAP in the user interface

On the LDAP Overview page in the OBWI, you can configure the LDAP authentication priority and the parameters that define LDAP server connection information.

LDAP overview parameters

LDAP authentication priority

In the LDAP Priority section of the OBWI, you can disable LDAP, or you can set the authentication priority by choosing whether local authentication or LDAP authentication should happen first.

To configure LDAP authentication priority parameters:

1. Select *Appliance* > *Appliance Settings* > *User Accounts* > *LDAP Accounts* > *Overview*.
2. Select either *LDAP Disabled*, *LDAP before Local* or *LDAP after Local* for the LDAP Priority.
3. Click *Save*.

LDAP servers

The Address fields specify the host names or IP addresses of the primary and secondary LDAP servers. The secondary LDAP server is optional.

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

The Access Type radio buttons specify how a query is sent to each LDAP target device. When using LDAP, all usernames, passwords and other information sent between an appliance and LDAP server are sent as non-secure clear text. Use LDAPS for secure encrypted communication between an appliance and LDAP server.

To configure LDAP server parameters:

1. Select *Appliance* > *Appliance Settings* > *User Accounts* > *LDAP Accounts* > *Overview*.
2. Identify the primary and secondary server address, port and access type in the appropriate fields or radio buttons.
3. Click *Save*.

LDAP Search parameters

On the LDAP Search page, you can configure the parameters used when searching for LDAP directory service users. Use the Search DN field to define an administrator-level user that the appliance uses to log into the directory service. Once the appliance is authenticated, the directory service grants it access to the directory to perform the user authentication queries specified on the LDAP Query page. The default values are cn=Administrator, cn=Users, dc=yourDomainName and dc=com and may be modified. For example, to define an administrator Distinguished Name (DN) for test.view.com, type ***cn=Administrator, cn=Users, dc=test, dc=view***, and ***dc=com***. Each Search DN value must be separated by a comma. The Search Password field is used to authenticate the administrator or user specified in the Search DN field. Use the Search Base field to define a starting point from which LDAP searches begin. The modifiable default values are dc=yourDomainName and dc=com. For example, to define a search base for test.com, type ***dc=test, dc=com***. Each Search Base value must be separated by a comma. The UID Mask field specifies the search criteria for User ID searches of LDAP target devices. The format should be in the form <name>=<%1>. The default value is sAMAccountName=%1, which is correct for use with Active Directory. This field is required for LDAP searches.

To configure LDAP search parameters:

1. Select *Appliance* > *Appliance Settings* > *User Accounts* > *LDAP Accounts* > *Search*.
2. Enter the appropriate information in the Search DN, Search Password, Search Base and UID Mask fields.
3. Click *Save*.

NOTE: These options cannot be changed if the LDAP Priority is set to *LDAP Disabled* on the Overview screen.

LDAP Query parameters

On the LDAP Query page, you can configure the parameters used when performing user authentication queries.

The appliance performs two different types of queries. Query Mode (Appliance) is used to authenticate administrators and users attempting to access the appliance itself. Query Mode (Target Device) is used to authenticate users that are attempting to access attached target devices. Additionally, each type of query has three modes that utilize certain types of information to determine whether or not an LDAP user has access to an appliance or connected target devices. See Appliance and target device query modes on page 60 detailed information on each mode.

You can configure the following settings on the LDAP Query Page:

- The Query Mode (Appliance) parameters determine whether or not a user has access to the appliance.
- The Query Mode (Target Device) parameters determine whether or not a user has user access to target devices connected to an appliance. The user does not have access to the appliance, unless granted by Query Mode (Appliance).
- The Group Container, Group Container Mask, and Target Mask fields are only used for group query modes and are required when performing an appliance or device query.
- The Group Container field specifies the organizational unit (ou) created in Active Directory by the administrator as the location for group objects.
    - Group objects are Active Directory objects that can contain users, computers, contacts and other groups. Group Container is used when Query Mode is set to Group Attribute. Each group object, in turn, is assigned members to associate with a particular access level for member objects (people, appliances, and target devices). The access level associated with a group is configured by setting the value of an attribute in the group object.
    - For example, if the Notes property in the group objects list is used to implement the access control attribute, the Access Control Attribute field on the LDAP Query Page should be set to info. Setting the Notes property to KVM User Admin causes the members of that group to have user administration access to the appliances and target devices that are also members of that same group.

- The Notes property is used to implement the access control attribute. The value of the Notes property, available in group and user objects shown in Active Directory Users and Computers (ADUC), is stored internally in the directory, in the value of the info attribute. ADUC is a Microsoft Management Console snap-in for configuring Active Directory. It is started by selecting *Start* > *Programs* > *Administrative Tools* > *Active Directory Users and Computers*. This tool is used to create, configure and delete objects such as users, computers and groups. See Appliance and target device query modes on page 60 for more information.
- The Group Container Mask field defines the object type of the Group Container, which is normally an organizational unit. The default value is “ou=%1”.
- The Target Mask field defines a search filter for the target device. The default value is “cn=%1”.
- The Access Control Attribute field specifies the name of the attribute that is used when the query modes are set to User Attribute or Group Attribute. The default value is info.

To configure LDAP query parameters:

1. Select *Appliance* > *Appliance Settings* > *User Accounts* > *LDAP Accounts* > *Query*.
2. Select either *Basic*, *User Attribute* or *Group Attribute* for the Appliance Query Mode and the Target Device Query Mode.
3. Enter the appropriate information in the Group Container, Group Container Mask, Target Mask, and Access Control Attribute fields.
4. Click *Save*.

NOTE: These options cannot be changed if the LDAP Priority is set to *LDAP Disabled* on the Overview screen.

Appliance and target device query modes

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

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

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

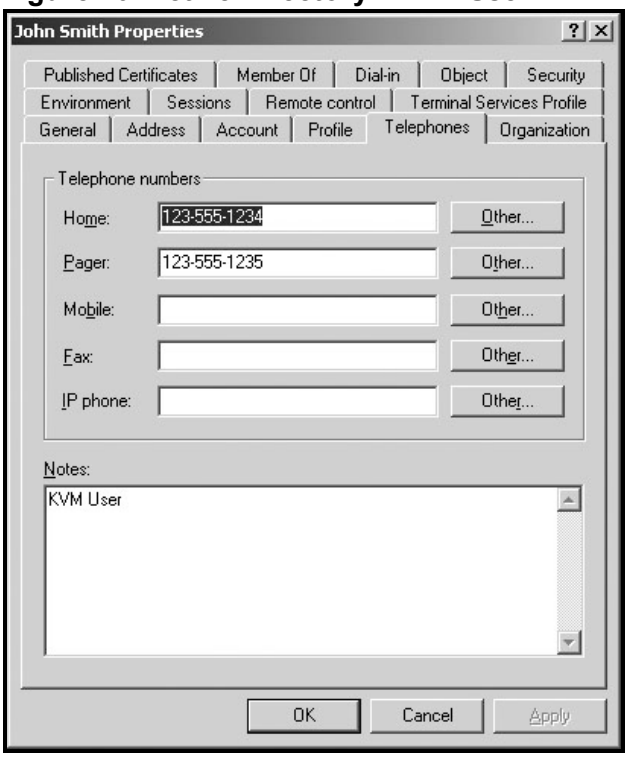
If the KVM User Admin value is found, the user is given user administrator access to the appliance and attached target devices for Query Mode (Appliance), or to any selected target device for Query Mode (Target Device).

If the KVM User value is found, the user is given user access to the appliance for Query Mode (Appliance), or to any selected target device for Query Mode (Target Device).

NOTE: If none of the three values are found, the user is given no access to the appliance and target devices for Query Mode (Appliance) or to any selected target device for Query Mode (Target Device), unless the user has User Admin or Appliance Admin privileges to the appliance.

You can access the ADUC by selecting *Start* > *Programs* > *Administrative Tools* > *Active Directory Users and Computers*.

Figure 10. Active Directory - KVM User



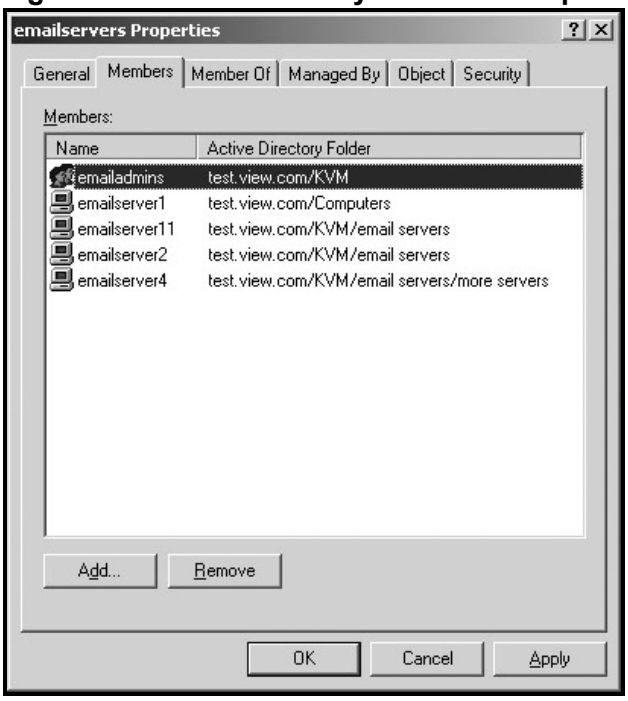
- Group Attribute – A username, password and group query is made to the directory service for an appliance and attached target devices when using Query Mode (Appliance), or for a selected target device when using Query Mode (Target Device). If a group is found containing the user and the appliance name, the user is given access to the appliance or attached target devices, depending on the group contents, when using Query Mode (Appliance). If a group is

found containing the user and target device IDs, the user is given access to the selected target device connected to the appliance when using Query Mode (Target Device).

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

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

Figure 11. Active Directory - Define Groups



Setting up Active Directory for performing queries

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

To set up group queries:

1. Log into Windows with administrator privileges.
2. Open Active Directory software.
3. Create an organizational unit to be used as a group container.
4. Create a computer object in Active Directory with a name identical to the switching system name for querying appliances (specified in the Appliance Overview screen of the OBWI), or

identical to the attached target devices for querying target devices. The name must match exactly, including case.

5. The appliance names and target device names used for group queries are stored in the appliance. The appliance name specified in the Appliance Overview screen of the OBWI and target device names must identically match the object names in Active Directory. Each appliance name and target device name may be comprised of any combination of upper-case and lower-case letters (a-z, A-Z), digits (0-9), and hyphens (-). You cannot use spaces and periods (.) or create a name that consists entirely of digits. These are Active Directory constraints.

NOTE: The factory default name in earlier versions contains a space that must be removed by editing the switching system name in the Appliance Overview screen of the OBWI.

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

NOTE: If none of the three values are found, the user is granted user level access to any appliance or target device listed in a group with the username.

Chapter 6. Appendices

Terminal Operations

Each switch may be configured at the appliance level through the Console menu interface accessed through the SETUP port. All terminal commands are accessed through a terminal or PC running terminal emulation software.

NOTE: The preferred method is to make all configuration settings in the local UI.

To connect a terminal to the switch:

1. Using the supplied RJ-45 to DB-9 (female) adapter and UTP cable, connect a terminal or a PC that is running terminal emulation software (such as HyperTerminal) to the SETUP port on the back panel of the switch. The terminal settings are 9600 bits per second (bps), 8 bits, 1 stop bit, no parity and no flow control.
2. Turn on each target device and then turn on the switch. When the switch completes initialization, the Console menu will display the following message: *Press any key to continue.*

Console boot menu options

While the switch is turning on, you can press a key to view the boot menu. From this menu, you can choose one of four options.

- Boot
- Boot Alternate
- Configuration Reset
- Full-Factory Reset

Console main menu options

Once turned on, the main menu displays the product name and version. From this menu, you can choose one of four options.

- Network configuration: This menu option allows you to configure the network settings of the appliance, including speed and IP configuration for remote connections made via the OBWI.
- Debug messages: This menu option turns on console status messages. Because this can significantly reduce performance, you should only enable debug messages when instructed to

do so by Technical Support. When you are finished viewing the messages, press any key to exit this mode.

- Reset Appliance: This menu option allows you to execute a soft reset of the switch.
- Exit: This menu selection will return you to the ready prompt. If the Console menu interface password is enabled, you must exit the Console main menu so that the next user will be prompted with the Username and Password login screen.

Using SCO cables

An administrator can choose between the ACS console server and Cisco pinouts for each SCO cable port via the local user interface or the remote OBWI. ACS is the default.

To change the pinout to Cisco mode:

1. Select *Unit View* > *Appliance* > *Appliance Settings* > *Ports* > *COs*.
2. Click on the desired *COs*.
3. Select *Settings* > *Pinout*.

NOTE: If the DB-9 adapter is used, select the ACS console server pinouts.

ACS console server port pinouts

The following table lists the ACS console server serial port pinouts for the SCO cable.

Table 15. ACS Console Server Serial Port Pinouts

Pin No.	Signal Name	Input/Output
1	RTS - Request to Send	OUT
2	DTR - Data Terminal Ready	OUT
3	TXD - Transmit Data	OUT
4	GND - Signal Ground	N/A
5	CTS - Clear to Send	IN
6	RXD - Receive Data	IN
7	DCD/DSR - Data Set Ready	IN
8	N/C - Not Connected	N/A

Cisco port pinouts

The following table lists the Cisco serial port pinouts for the SCO cable.

Table 16. Cisco Serial Port Pinouts

Pin No.	Signal Name	Input/Output
1	CTS - Clear to Send	IN
2	DCD/DSR - Data Set Ready	IN
3	RXD - Receive Data	IN
4	GND - Signal Ground	N/A
5	N/C - Not Connected	N/A
6	TXD - Transmit Data	OUT
7	DTR - Data Terminal Ready	OUT
8	RTS - Request to Send	OUT

UTP cabling

This appendix discusses various aspects of connection media. The switch system utilizes UTP cabling. The performance of a switch system depends on high quality connections. Poor quality or poorly installed or maintained cabling can diminish switch system performance.

NOTE: This appendix is for information purposes only. Please consult with your local code officials and/or cabling consultants prior to any installation.

UTP copper cabling

The following are basic definitions for the three types of UTP cabling that the GCM switches support:

- CAT5 (4-pair) high performance cable consists of twisted pair conductors, used primarily for data transmission. The twisting of the pairs gives this cable some immunity from the infiltration of unwanted interference. CAT5 cable is generally used for networks running at 10 or 100 Mbps.
- CAT5E (enhanced) cable has the same characteristics as CAT5, but is manufactured to somewhat more stringent standards.
- CAT6 cable is manufactured to tighter requirements than CAT5E cable. CAT6 has higher measured frequency ranges and significantly better performance requirements than CAT5E cable at the same frequencies.

Wiring standards

There are two supported wiring standards for 8-conductor (4-pair) RJ-45 terminated UTP cable: EIA/TIA 568A and B. These standards apply to installations utilizing CAT5, CAT5E, and CAT6 cable specifications. The GCM switch system supports either of these wiring standards. The following table describes the standards for each pin.

Table 17. UTP wiring standards

Pin	EIA/TIA 568A	EIA/TIA 568B
1	white/green	white/orange
2	green	orange
3	white/orange	white/green
4	blue	blue
5	white/blue	white/blue
6	orange	green

Pin	EIA/TIA 568A	EIA/TIA 568B
7	white/brown	white/brown
8	brown	brown

Cabling installation, maintenance, and safety tips

The following is a list of important safety considerations that should be reviewed prior to installing or maintaining your cables:

- Keep all UTP runs to KVM IQ modules to a maximum of 50 meters each.
- Keep all UTP runs to Serial IQ modules to a maximum of 30 meters each.
- Maintain the twists of the pairs all the way to the point of termination, or no more than one-half inch untwisted. Do not skin off more than one inch of the jacket while terminating.
- If bending the cable is necessary, make it gradual with no bend sharper than a one inch radius. Allowing the cable to be sharply bent or kinked can permanently damage the cable's interior.
- Dress the cables neatly with cable ties, using low to moderate pressure. Do not over tighten the ties.
- Cross-connect cables where necessary, using rated punch blocks, patch panels, and components. Do not splice or bridge the cable at any point.
- Keep the UTP cable as far away as possible from potential sources of EMI, such as electrical cables, transformers, and light fixtures. Do not tie the cables to electrical conduits or lay the cables on electrical fixtures.
- Always test every installed segment with a cable tester. "Toning" alone is not an acceptable test.
- Always install jacks so as to prevent dust and other contaminants from settling on the contacts. The contacts of the jack should face up on the flush mounted plates, or left/right/down on surface mount boxes.
- Always leave extra slack on the cables, neatly coiled in the ceiling or nearest concealed location. Leave at least five feet at the work outlet side and 15 feet at the patch panel side.
- Choose either 568A or 568B wiring standard before beginning. Wire all jacks and patch panels for the same wiring scheme. Do not mix 568A and 568B wiring in the same installation.
- Always obey all local and national fire and building codes. Be sure to firestop all the cables that penetrate a firewall. Use plenum-rated cable where it is required.

Cable pinout information

NOTE: All switches have the 8-pin modular jack for the modem and console/setup ports.

Figure 12. Modem jack

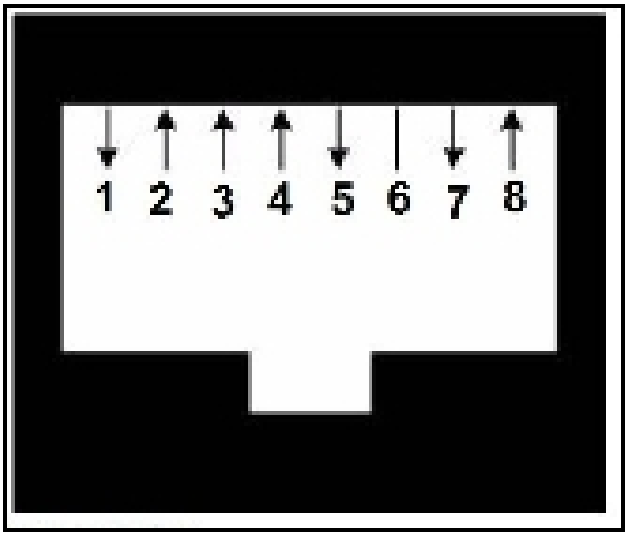


Table 18. Descriptions for Modem jack on page 71

Pin	Description	Pin	Description
1	Request to Send (RTS)	5	Transmit Data (TXD)
2	Data Set Ready (DSR)	6	Signal Ground (SG)
3	Data Carrier Detect (DCD)	7	Data Terminal Ready (DTR)
4	Receive Data (RXD)	8	Clear to Send (CTS)

Figure 13. Console/setup jack

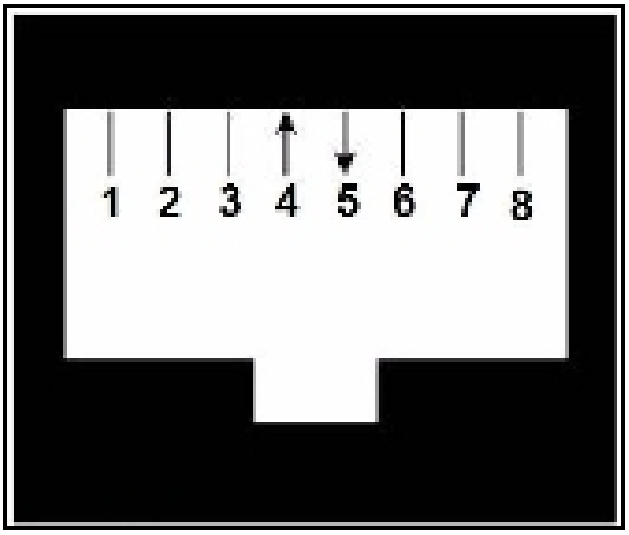


Table 19. Descriptions for Console/setup jack on page 71

Pin	Description	Pin	Description
1	No Connection (N/C)	5	Transmit Data (TXD)
2	No Connection (N/C)	6	Signal Ground (SG)
3	No Connection (N/C)	7	No Connection (N/C)
4	Receive Data (RXD)	8	No Connection (N/C)

Technical specifications

Table 20. Technical specifications

Server ports	
Number	GCM16: 16 GCM32: 32
Type	PS/2, USB, and Serial
Connectors	8-pin modular
Sync types	Separate horizontal and vertical
Input video resolution	Standard 640 x 480 @ 60 Hz 800 x 600 @ 75 Hz 960 x 700 @ 75 Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz 1600 x 1200 @ 60 Hz Widescreen 800 x 500 @ 60 Hz 1024 x 640 @ 60 Hz 1280 x 800 @ 60 Hz 1440 x 900 @ 60 Hz 1680 x 1050 @ 60 Hz 1920 x 1080 @ 60 Hz
Supported cabling	4-pair UTP or CAT 6, 45 meters maximum length
Dimensions	
Form factor	1 U-rack, mountable
Dimensions	1.72 x 17.00 x 9.20 (Height x Width x Depth)
Weight (without cables)	GCM16: 7.0 lb (3.2 kg) GCM32: 7.6 lb (3.4 kg)
SETUP port	
Number	1
Type	RS-232 serial
Connector	8-pin modular
Local port	
Number/Type	1 VGA/4 USB
Network connection	
Number	2
Type	10/100/1000 Ethernet
Connector	8-pin modular
USB device port	
Number	4
Type	USB 2.0

Server ports	
MODEM port	
Number	1
Type	RS-232 serial
Connectors	8-pin modular
PDU port	
Number	2
Type	RS-232 serial
Connector	8-pin modular
Power specifications	
Connectors	2
Type	Internal
Power	GCM16: 18W GCM32: 24W
Heat dissipation	GCM16: 45 BTU/hr GCM32: 47 BTU/hr
AC input range	100 - 240 VAC
AC frequency	50/60 Hz auto-sensing
AC input current rating	1.25 A
AC input power (maximum)	40 W
Ambient atmospheric condition ratings	
Temperature	32 to 122 degrees Fahrenheit (0 to 50 degrees Celsius) operating; -4 to 158 degrees Fahrenheit (-20 to 70 degrees Celsius) non-operating
Humidity	Operating: 20% to 80 % relative humidity (non-condensing) Non-operating: 5% to 95% relative humidity, 38.7 degrees C maximum wet bulb temperature
Safety and EMC Standards approvals and markings	UL, FCC, cUL, ICES-003, CE, VCCI, KCC, C-Tick, GOST Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number), or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.

Sun advanced key emulation

Certain keys on a standard Type 5 (US) Sun keyboard can be emulated by key press sequences on the local port USB keyboard. To enable Sun Advanced Key Emulation mode and use these keys, press and hold **Ctrl+Shift+Alt** and then press the **Scroll Lock**key. The **Scroll Lock** LED blinks. Use the indicated keys in the following table as you would use the advanced keys on a Sun keyboard. For example: For **Stop + A**, press and hold **Ctrl+Shift+Alt** and press **Scroll Lock**, then **F1 + A**.

These key combinations will work with the UCO, VCO and VCO2 conversion option cables. With the exception of **F12**, these key combinations are not recognized by Microsoft Windows. Using **F12** performs a Windows key press.

When finished, press and hold **Ctrl+Shift+Alt** and then press the **Scroll Lock** key to toggle Sun Advanced Key Emulation mode off.

Table 21. Sun key emulation

Sun key (US)	Key to enable Sun key emulation
Compose	Application(1)
Compose	keypad
Power	F11
Open	F7
Help	Num Lock
Props	F3
Front	F5
Stop	F1
Again	F2
Undo	F4
Cut	F10
Copy	F6
Paste	F8
Find	F9
Mute	keypad /
Vol.+	keypad +
Vol.-	keypad -
Command (left)(2)	F12
Command (left)(2)	Win (GUI) left(1)
Command (right)(2)	Win (GUI) right (1)
ENDNOTES: (1)Windows 95 104-key keyboard.	

Sun key (US)	Key to enable Sun key emulation
(2)The Command key is the Sun Meta (diamond) key.	