Lenovo

Local Console Manager

LCM 8/LCM 16

Installer/User Guide

Second Edition, March 2016.

TABLE OF CONTENTS

Chapter 1. Product Overview

The Local Console Manager switch is an analog keyboard, video, and mouse (KVM) switch that provides flexible, centralized local access to data center servers. It can also provide centralized remote access to data center servers when used in conjunction with the optional digital activation key.

Features and Benefits

Reduce Cable Bulk

With device densities continually increasing, cable bulk remains a major concern for network administrators. The switch significantly reduces KVM cable volume in the rack by utilizing the innovative CO cable and single, industry-standard Unshielded Twisted Pair (UTP) cabling. This allows a higher device density while providing greater airflow and cooling capacity.

CO cables

The switch supports CO cables that are powered directly from the target device and provide Keep Alive functionality when the switch is not powered. The CO cables with CAT 5 design dramatically reduce cable clutter while providing optimal resolution and video settings. The built-in memory of CO cables simplifies configuration by assigning and retaining unique device names and Electronic ID (EID) numbers for each attached device.

PS/2 and USB CO cables are available allowing direct KVM connectivity to devices. VCO and VCO2 CO cables are also available. The switch is offered with 8 or 16 ARI ports that are used to connect CO cables to the switch. Then utilizing the CO cables, you can attach additional switches to expand your switch system. This flexibility allows you to add capacity as your data center grows.

User interfaces

The switch is equipped with two “point-and-click” interfaces to manage the switch locally. They are the local user interface (UI) and the on-board web interface (OBWI). Using the configuration options provided by these interfaces, you can tailor your switch to your specific application. The OBWI can also be used to access and control any attached devices, and handle all basic KVM needs remotely.

NOTE: Remote KVM sessions via the OBWI requires the installation of the digital activation key.

Local user interface

The local user interface, accessed using the local port, features intuitive menus and operation modes to configure your switch and devices. Devices can be identified by name, EID, or port number.

Security

The interface allows you to protect your system with a screen saver password. When the screen saver mode engages, access is prohibited until the appropriate password is entered to reactivate the system. By typing Help in the password dialog, you are directed to Avocent Technical Support.

Recommended usage for the switch is in a data center infrastructure protected by a firewall.

OBWI

You can also use the OBWI to manage your switch. The OBWI is launched directly from the switch and does not require a software server or any installation. With the addition of the optional digital activation key installed, you can also establish remote KVM and virtual media sessions to target devices.

Terminal console interface

The terminal console interface is accessed through the "SETUP" port. A terminal screen or a PC running terminal emulation software can be used to access these screens.

Virtual media and smart card support

The switch allows you to view, move, or copy data located on local media and smart cards. Smart cards are pocket-sized cards that store and process information including identification and authentication information to enable access to computers, networks, and secure rooms or buildings.

A virtual media or a smart card reader can be connected directly to the USB ports on the switch. In addition, virtual media or smart card readers may be connected to any remote workstation that is running the remote OBWI, switch software, or DSView management software, and is connected to the switch using an Ethernet connection.

NOTE: To open a virtual media or smart card session with a target device, you must first connect the target device to a switch using a VCO or VC02 CO cable.

IPv4 and IPv6 capabilities

The switch is compatible with systems using either of the currently used Internet Protocol Versions, IPv4 or IPv6. You can change the network settings and choose either IPv4 or IPv6 mode via the terminal console, local interface, or OBWI.

Access the switch using a standard TCP/IP network

The device is accessible for configuration via the standard TCP/IP Network. If the optional digital activation key is installed, you can access all attached systems via Ethernet.

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

NOTE: KVM over IP sessions are supported when the digital activation key is installed.

Upgradeable

Upgrade your switch at any time to ensure you are always running the most current firmware version available. For more information, see Tools - Rebooting and Upgrading on page 33.

Two-tier expansion

The switch allows you to tier one additional switch from each ARI port on the primary switch. Each tiered switch is attached in the same manner as any device. This additional tier of units allows you to attach up to 256 servers in one system. See CO Cable Connection on page 8.

Digital activation key

The optional digital activation key, installed in the USB port, supports the following features.

KVM remote access

A single KVM remote user is supported using the digital activation key. With the digital activation key, you can manage remote operating system installation, operating system recovery, hard drive recovery or duplication, BIOS updating, and server backup.

DSView™ management software plug-in

The DSView management software may be used with the switch to allow IT administrators to securely and remotely access and monitor target devices on multiple platforms through a single, web-based user interface. A session may be launched to a device from a single point of access.

Local video scaling

The switch digitizes a video signal with a maximum pixel resolution of up to 1600 x 1200 or 1920 x 1080 (widescreen), depending on the length of cable separating your switch and devices.

Encryption

The switch supports 128-bit SSL(ARCFOUR), AES, DES, and 3DES encryption of keyboard/mouse, video, and virtual media sessions.

Chapter 2. Installation

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

You may use the terminal software, local user interface, or the OBWI to manage your switch system. The OBWI manages a single switch and its connections. With the optional digital activation key, you can also perform KVM and serial switching tasks using the OBWI or DSView management software. For more information about DSView management software, visit http://www.emersonnetworkpower.com.

NOTE: Ensure that every switch has been upgraded to the most recent version of firmware. For information on upgrading the switch using the OBWI, see Tools - Rebooting and Upgrading on page 33.

Setting Up Your Network

The switch uses IP addresses to uniquely identify the switch and attached devices. The switch supports 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.

Keyboards

A USB keyboard and mouse can be connected to the analog ports of the switch.

NOTE: The switch also supports the use of multiple keyboards and multiple mice on the analog port. The use of more than one input device simultaneously, however, may produce unpredictable results.

Quick Setup

The following is a quick setup list. For detailed rack mounting and installation instructions, see the KVM Switch Rack Mount Quick Installation Guide.

1. Unpack the switch and verify that all components are present and in good condition.
2. Install the switch hardware and connect a CO cable to each target device or tiered switch. Connect each CO cable to the switch with CAT 5 cabling and connect the keyboard, monitor, and mouse connectors to the analog ports of the switch.
3. Connect the local port peripherals to the appropriate ports on the back panel of the switch and set up the network configuration. The IP address can be set here. Using a static IP address is recommended.

4. For the local port connection, input all device names using the local interface or the OBWI.
5. Adjust mouse acceleration on each device to *Slow* or *None*.

Connecting the LCM Switch Hardware

The following figure illustrates an example configuration for the LCM switch.

Figure 1. Basic Configuration

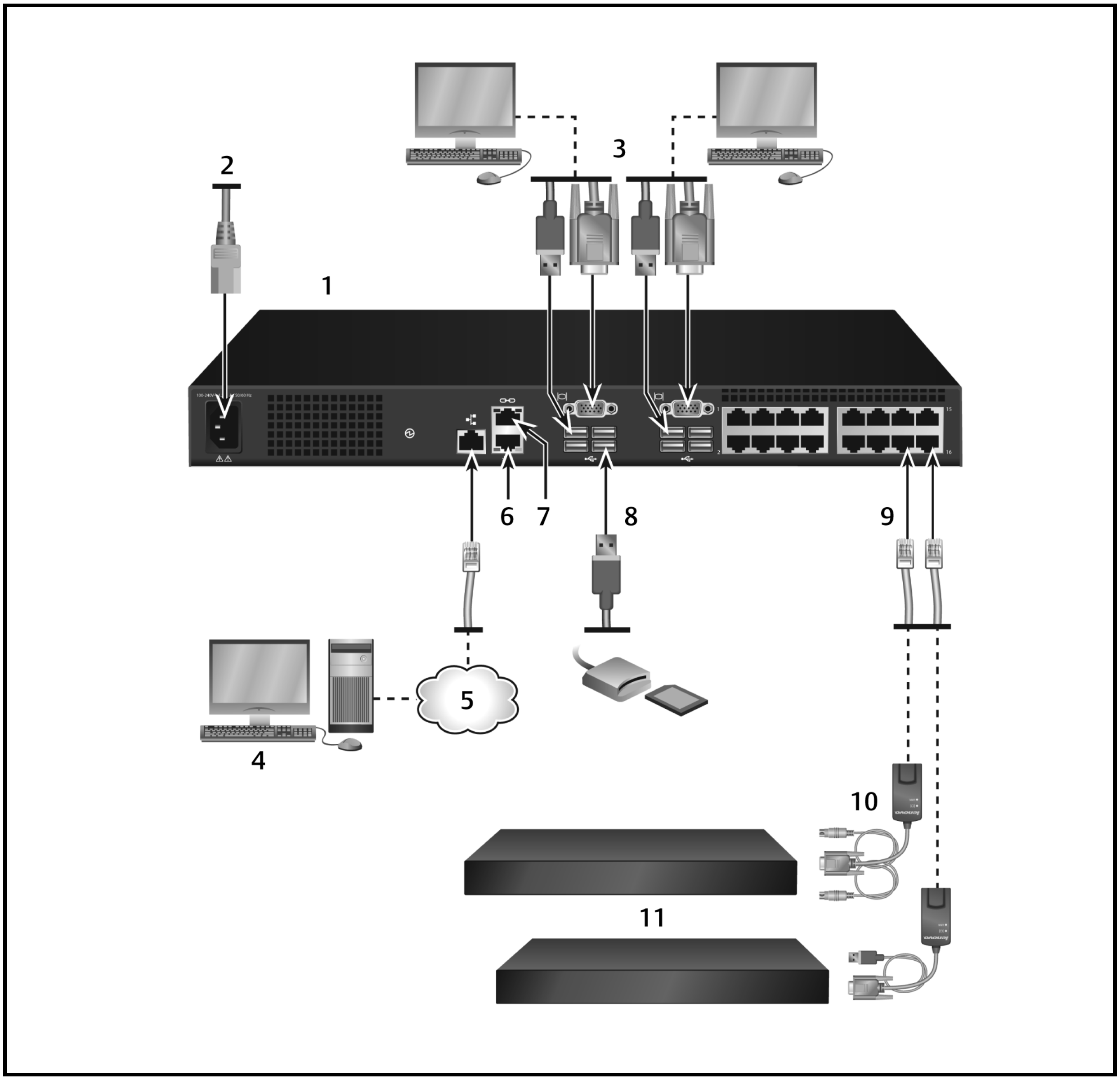


Table 1. Basic Configuration Descriptions

Number	Description	Number	Description
1	LCM switch (16-Port Model Shown)	7	ACI Connection
2	Power Cord	8	External Virtual Media - USB Connections

Number	Description	Number	Description
3	Analog Users (2)	9	Target Device Ports
4	Digital User (requires the digital activation key)	10	CO cables
5	LAN/Network	11	Servers/Target Devices
6	SETUP Console Setup Port		

NOTE: The switch supports connecting to another appliance via an ACI connection. This connection requires that the secondary appliance in the tier have an ACI connector on the user side.

To connect and turn on your switch:

CAUTION: To reduce the risk of electric shock or damage to your equipment, do not disable the jumper cord grounding plug. The grounding plug is an important safety feature. Plug the jumper cord into a grounded (earthed) outlet that is easily accessible at all times. Disconnect the power from the unit by unplugging the jumper cord from either the power source or the unit.

NOTE: If the building has 3-phase AV power, ensure that the computer and monitor are on the same phase to avoid potential phase-related video and/or keyboard problems.

NOTE: The maximum supported cable length from switch to server is 30 meters.

- Do not disable the power grounding plug. The grounding plug is an important safety feature.
- Connect the jumper cord into a grounded (earthed) outlet that is easily accessible at all times.
- Disconnect the power from the product by unplugging the jumper cord from either the power source or the product.
- This product has no user-serviceable parts inside the product enclosure. Do not open or remove product cover.

1. Connect your VGA monitor and USB keyboard and mouse cables to the appropriately labeled ports.
2. Connect one end of a UTP cable (4-pair, up to 98 ft/30 m) to an available numbered port. Connect the other end to an RJ-45 connector of a CO cable.
3. Connect a CO cable to the appropriate port on the back of a device. Repeat steps 2 and 3 for all devices you want to connect.

NOTE: When connecting to a Sun Microsystems server, 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 a user-supplied UTP cable from the Ethernet network to the LAN port on the back of the switch. Network users will access the switch through this port.
5. Turn on each device, then locate the jumper cord that came with the switch. Connect one end to the power socket on the rear of the switch. Connect the other end into an appropriate power source.
6. (Optional) Connect the virtual media or smart card readers to any of the USB ports on the switch.

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

CO Cable Connection

The following figure illustrates a typical CO cable connection between the switch and a device.

To connect a CO cable to each device:

1. Locate the CO cables for your switch.
2. If you are using a PS/2 CO cable connection, attach the color-coded ends of the CO cable cable to the appropriate keyboard, monitor, and mouse ports on the first device you will be connecting to this switch. If you are using a USB connection, attach the plug from the CO cable to the USB port on the first device you will be connecting to this switch.
3. To the RJ-45 connector on the CO cable, attach one end of the CAT 5 cabling that will run from your CO cable to the switch.
4. Connect the other end of the CAT 5 cable to the desired ARI port on the back of your switch.
5. Repeat steps 2-4 for all devices you wish to attach.

NOTE: Turn off the switch before servicing. Always disconnect the jumper cord from the power source.

Adding a tiered switch

You can tier up to two levels of switches, enabling users to connect to up to 256 devices. In a tiered system, each device port on the main switch will connect to the ACI port on each tiered switch. Each tiered switch can then be connected to a device with a CO cable.

To tier multiple switches:

1. Attach one end of a UTP cable (up to 30 meters in length) to a device port on the switch.
2. Connect the other end of the UTP cable to the ACI port on the back of your tiered switch.
3. Connect the devices to your tiered switch.
4. Repeat these steps for all the tiered switches you wish to attach to your system.

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

NOTE: The switch supports one tiered switch per device port of the main switch. You cannot attach a switch to the tiered switch.

Figure 2. Tiering the Switch with a UTP Cable

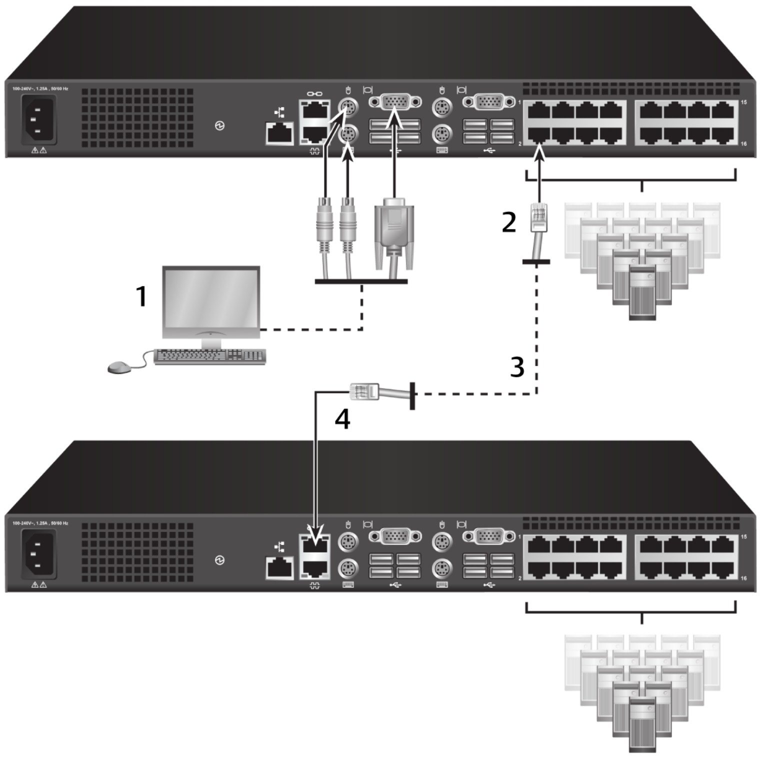


Table 2. Descriptions for Tiering the switch

Number	Description
1	Local User
2	ARI Connection
3	UTP Connection
4	ACI Connection (chain icon)

Adding a tiered legacy switch

The following figure illustrates a tiered legacy switch configuration.

To add a legacy switch (optional):

1. Mount the switch into your rack. Locate a UTP cable (up to 30 meters) to connect your switch to the legacy switch.

2. Attach one end of the UTP cabling to the ARI port on your switch.
3. Connect the other end of the UTP cable to a PS/2 CO cable.
4. Connect the CO cable to the legacy switch according to the switch manufacturer's recommendations.
5. Repeat steps 1-4 for all the legacy switches you wish to attach to your switch.

NOTE: The primary switch supports only one switch per ARI port or USB port. You cannot tier a switch to a tiered switch.

Figure 3. Tiering Legacy Switches

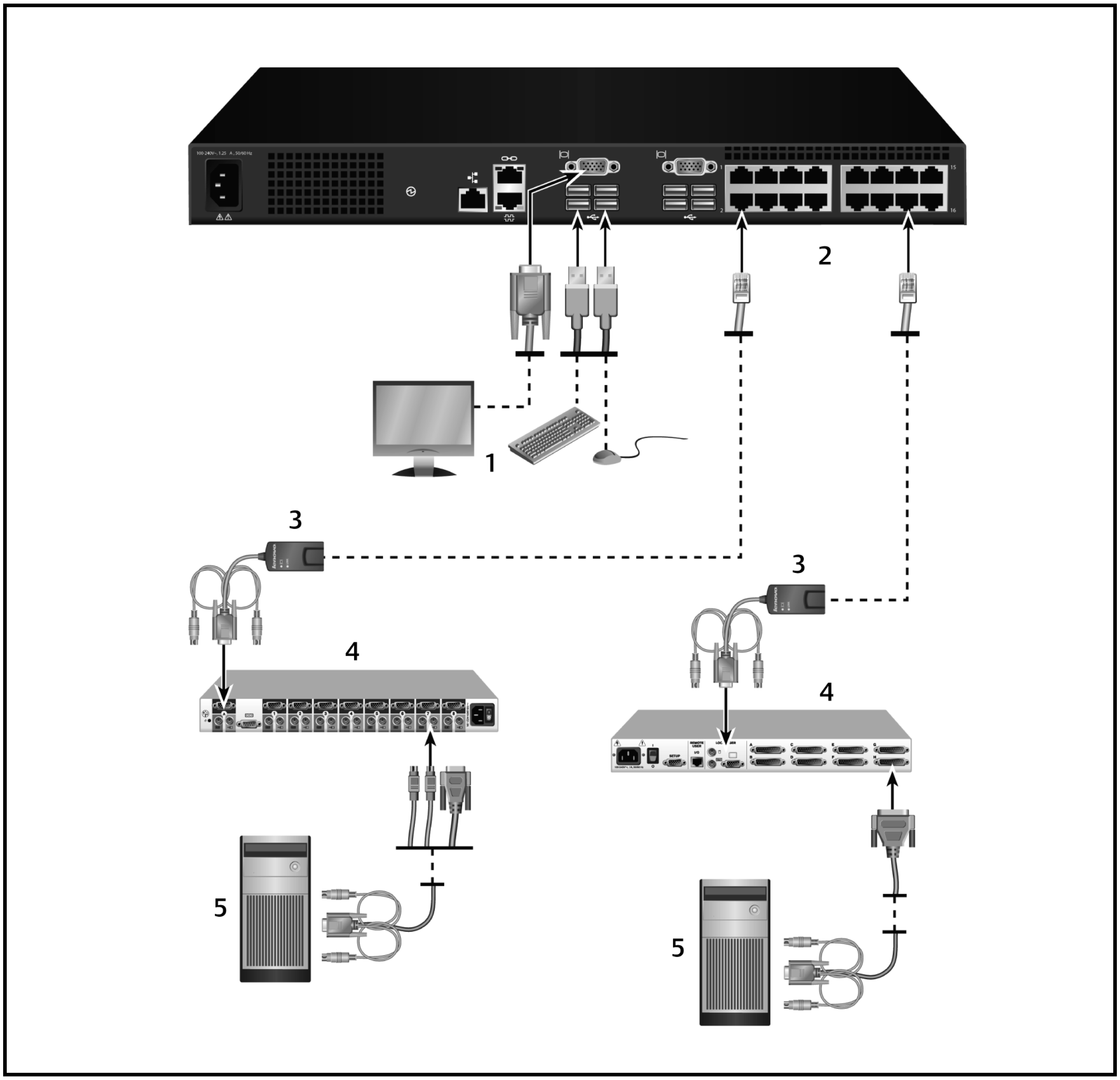


Table 3. Descriptions for Tiering Legacy Switches

Number	Description
1	Local User
2	ARI Connection
3	CO cable
4	PS2 Connection
5	Target Device Connection

Configuring Your Switch

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 using serial interface, OBWI, local UI, or the

DSView management software. When configuring the switch using the local UI, see Network Settings on page 36. When using DSView management software, the digital activation key is required. See the applicable Avocent Installer/User Guide for detailed instructions.

Setting Up the Built-in Web Server

Before using the OBWI to access the switch, the IP address must be specified using the setup port on the back panel of the switch, or through the local user interface. To use the switch UI, see Local User Interface (UI) on page 15.

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 4. OBWI Ports With a Firewall

Port Number	Function
TCP 80	Used for the initial downloading of the Video Viewer. The appliance Admin can change this value.
TCP 443	Used by the web browser interface for managing the switch and launching KVM sessions. The appliance Admin can change this value.
TCP 2068	Transmission of KVM session data (mouse and keyboard) or transmission of video on switches (requires the digital activation key).
TCP/UDP 3211	Discovery (requires the digital activation key).

The following figure and table provide a typical configuration where the user’s computer is located outside of the firewall and the switch resides inside the firewall.

Figure 4. Typical Firewall Configuration
Figure 5.

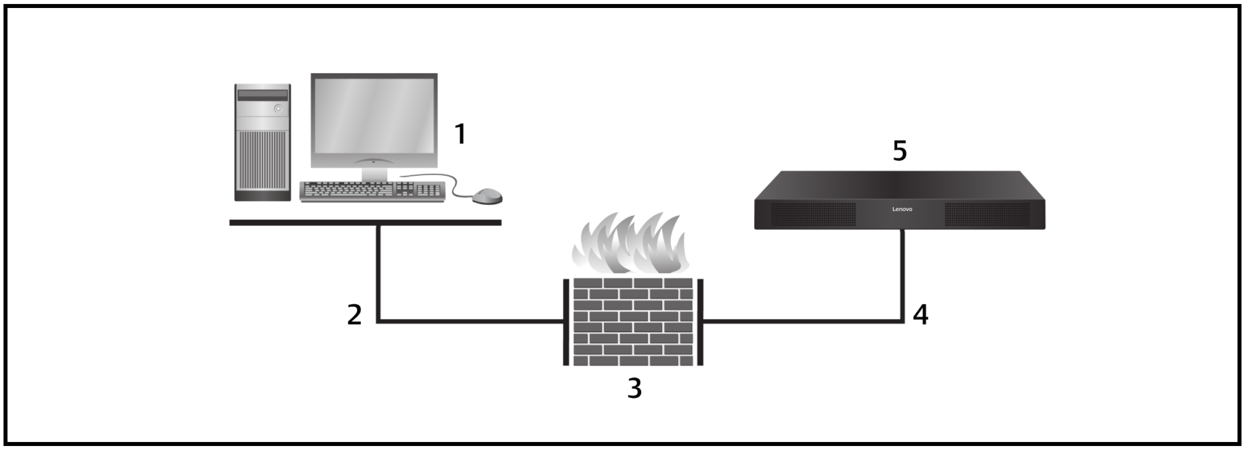


Table 5. Descriptions for Firewall Configuration

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

To configure the firewall:

To access the switch from outside a firewall, configure your firewall to forward ports 80 and 443 from its external interface to the KVM switch through the firewall’s internal interface. Consult your firewall manual for specific port forwarding instructions.

NOTE: Ports 80 and 443 can be reconfigured by an administrator. You must reboot for a port change to take effect.

For information on launching the OBWI, see OBWI Operation on page 29.

Verifying Power Status

The switch has one power supply. The LED illuminates when the switch is turned on and operating normally.

Adjusting Mouse Settings on Target Devices

You must set the target mouse speed and turn off acceleration. For machines running Microsoft® Windows® (Windows NT®, 2000, XP, or Server 2003), use the default USB 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 device system being viewed and the mouse pointer on the client computer.

Chapter 3. Local User Interface (UI)

The LCM switch features user-side keyboard and mouse ports that allow you to connect a USB keyboard and mouse for direct analog access. The switch uses the local UI to configure your system and devices. You can use the local UI to access devices that are attached to the switch.

Main Dialog Box Functions

To access the local UI Main dialog box:

Press **Print Screen** to launch the local UI. The Main dialog box will appear.

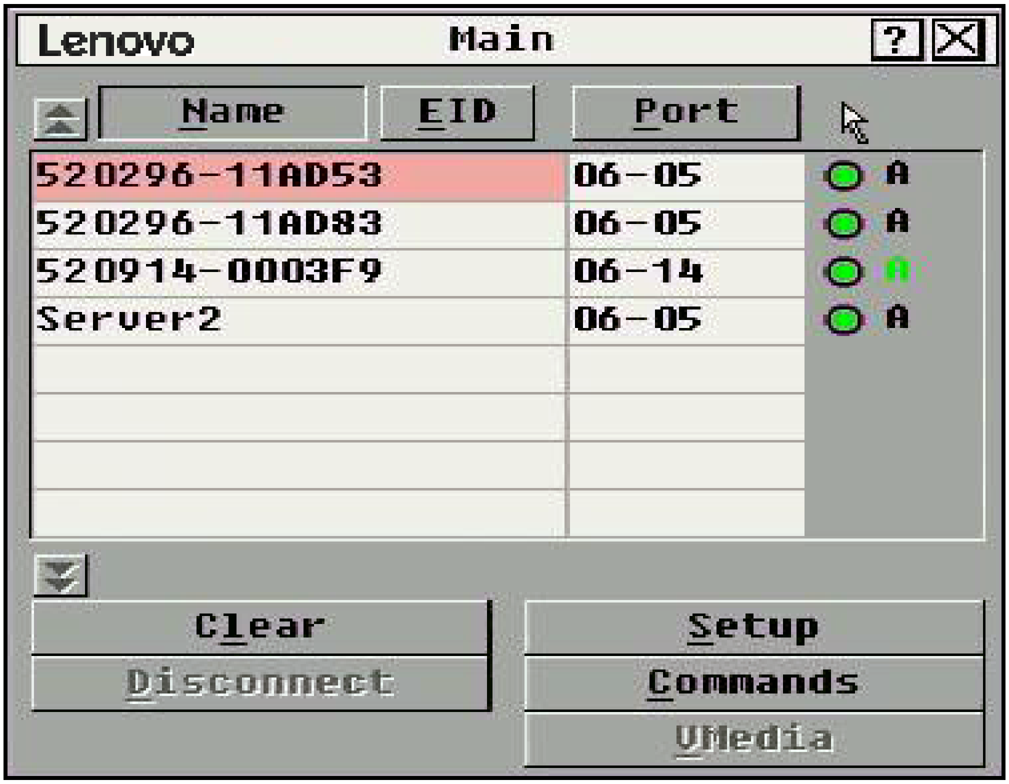
NOTE: If the local UI password has been enabled, you will be prompted to enter a password before you can launch the local UI.

Viewing and selecting ports and devices

Use the local UI *Main* dialog box to view, configure, and control devices in the switch system. View your devices by name, port, or by the unique EID number embedded in each CO cable.

In the following figure, the Port column indicates the ARI port to which a device is connected. If you tier a switch from the main switch, creating another tier, the ARI port on the switch is listed first, and is followed by the switch port to which the device is connected.

Figure 6. Local UI Main Dialog Box



Name	EID	Port	
520296-11AD53		06-05	● A
520296-11AD83		06-05	● A
520914-0003F9		06-14	● A
Server2		06-05	● A

NOTE: You can press the **Control** , **Alt** , or **Shift** keys twice within one second to launch the local UI. You can use this key sequence when you see **Print Screen** throughout this chapter.

Table 6. Main Dialog Box Functions

Button	Function
Name	Name of device.
EID	Unique EID in a module.
Port	The port to which a device is connected.
Clear	Clear all offline CO cables.
Disconnect	Disconnect the KVM session.
Setup	Access the Setup dialog box and configure the local UI.
Commands	Access the Commands dialog box.
VMedia	Control virtual media connection.

Viewing switch system status

The status of devices in your system is indicated in the right column of the *Main* dialog box. The following table describes the status symbols.

Table 7. Local UI Status Symbols

Symbol	Description
🟢	(green circle) device connected, turned on, and the IQ Module is online.
❌	Connected device is turned off or is not operating properly, and the IQ Module is offline.
∴	Connected switch is online.
✗ ○○	Connected switch is offline or not operating properly.
🟡	(yellow circle) The designated IQ Module is being upgraded. When this symbol displays, do not cycle power to the switch or connected devices and do not disconnect the IQ Module. Doing so may render the module permanently inoperable and require the IQ Module to be returned to the factory for repair.
A	(green letter) IQ Module is being accessed by the indicated user channel.
A	(black letter) IQ Module is blocked by the indicated user channel.
E	(red letter) Smart card support is available.

Selecting devices

Use the Main dialog box to select a device. When you select a device, the switch reconfigures the local keyboard and mouse to the settings for that device.

To select a device:

Double-click the device name, EID, or port number.

or-

If the display order of your list is by port (the *Port* button is depressed), type the port number and press **Enter** .

-or-

If the display order of your list is by name or EID (the Name or EID button is depressed), type the first few letters of the name of the device or the EID number to establish it as unique and press **Enter**.

To select the previous device:

Press **Print Screen** and then **Backspace**. This key combination toggles between the previous and current connections.

To disconnect from a device:

Press **Print Screen** and then **Alt+0** (zero). This leaves the user in a free state, with no device selected. The status flag on your desktop displays the word Free.

Soft switching

Soft switching is the ability to switch devices using a hotkey sequence. You can soft switch to a device by pressing **Print Screen**, and then depending on the method you've selected, typing the first few characters of its name or number. If you have set a Screen Delay Time for the local UI and you press the key sequences before that time has elapsed, the local UI will not be displayed.

To soft switch to a device:

Press **Print Screen**, type the port number and the first few letters of the name of the device, to establish it as unique and press **Enter**.

To switch back to the previous device, press **Print Screen** and then **Backspace**.

Navigating the local UI

The following table describes how to navigate the local UI using the keyboard and mouse.

Table 8. Local UI Navigation Basics

Keystroke	Function
Print Screen, Ctrl+Ctrl, Shift+Shift and/or Alt+Alt	Local UI activation sequence. By default, **Print Screen** and **Ctrl+Ctrl** are set as the local UI activation options. **Shift+Shift** and **Alt+Alt** must be set within the local UI before use.
F1	Opens the Help screen for the current dialog box.
Escape	Closes the current dialog box without saving changes and returns to the previous one. If the Main dialog box is displayed, pressing **Escape** closes the local UI and displays a status flag if status flags are enabled. See Commands Dialog Box Functions on page 24 for more information. In a message box, pressing **Escape** closes the pop-up box and returns to the current dialog box.
Alt	Opens dialog boxes, selects or checks options, and executes actions when used with underlined

Keystroke	Function
	or other designated letters.
Alt+X	Closes current dialog box and returns to previous one.
Alt+O	Selects the OK button, then returns to the previous dialog box.
Enter	Completes a switch operation in the Main dialog box and exits the local UI.
Single-click, **Enter**	In a text box, single-clicking an entry and pressing **Enter** selects the text for editing and enables the left and right arrow keys to move the cursor. Press **Enter** again to quit the Edit mode.
Print Screen, Backspace	Toggles back to previous selection.
Print Screen, Pause	Immediately turns on Screen Saver mode and prevents access to that specific console, if it is password protected.
Up/Down Arrows	Moves the cursor from line to line in lists.
Right/Left Arrows	Moves the cursor between columns. When editing a text box, these keys move the cursor within the column.
Page Up/Page Down	Pages up and down through Name and Port lists and Help pages.
Home/End	Moves the cursor to the top or bottom of a list.
Backspace	Erases characters in a text box.

Connecting local virtual media

You can connect virtual media directly to the switch using a USB port on the switch.

NOTE: All USB ports are assigned to a single virtual media session and cannot be independently mapped.

To start a local virtual media session, complete the following steps:

1. Press **Print Screen** to start the local UI and open the Main window.
2. Connect the user to the device with which you want to establish a virtual media session.
3. Use the arrow keys to highlight the device name, and then press **Enter**.
4. Press <Print Screen> to start the local UI again. The Virtual Media window is displayed.
5. Select one or more of the following checkboxes:
   - Locked - Select this checkbox to specify that when the user is disconnected from a device, the virtual media is also disconnected.
   - Reserve - Select this checkbox to specify that the virtual media connection can be accessed only by your user name and that no other user can connect to that device. If both Locked and Reserved are selected, the session will be reserved.

- CD ROM - Select this checkbox to establish a virtual media CD connection to a device. Clear this checkbox to end the connection.
- Mass Storage - Select this checkbox to establish a virtual media mass-storage connection to a device. Clear this checkbox to end the connection.
- Write Access - Select this checkbox to enable the connected device to write data to the virtual media during a virtual media session. Read access is always enabled during virtual media sessions.

6. Click *OK*.

Setup Dialog Box Functions

You can configure your switch system from the Setup dialog box within the local UI. Select the *Names* button when initially setting up your switch to identify devices by unique names. Select the other setup features to manage routine tasks for your devices from the local UI menu. The following table lists the functions accessed using each of the buttons in the Setup dialog box.

To access the local UI Setup dialog box, click *Setup* on the *Main* dialog box.

Table 9. Setup Dialog Box Features

Feature	Purpose
Menu	Change the Main dialog box list sorting option by toggling numerically between port number, EID number, or alphabetically by name. Change the Screen Delay Time before the local UI displays after pressing Print Screen. You can also change how the local UI activation sequence is invoked.
Security	Set passwords to protect or restrict access or enable the screen saver.
Devices	Identify the appropriate number of ports on an attached tiered switch.
Names	Identify devices by unique names.
Keyboard	Set the keyboard country code value for the USB devices.
Broadcast	Set up to simultaneously control multiple devices through keyboard and mouse actions.
Switch	Change how local port connections are managed by the switch. Control Local to Local Share Mode.
Network	Choose your network speed, transmission mode, and configuration.
Scan	Set up a custom Scan pattern for multiple devices.
VMedia	Set the behaviour of the switch during a virtual media session.

Changing the display behavior

Use the *Menu* dialog box to change the order of displayed devices, change how the local user interface is invoked, or set a *Screen Delay Time* for the local UI. This setting alters how devices are displayed in several dialog boxes, including the *Main*, *Devices*, and *Scan List* boxes.

To access the local UI *Menu* dialog box, activate the local interface and click *Setup - Menu* in the *Main* dialog box.

To choose the display order of devices:

1. Select *Name* to display devices alphabetically by name.

   -or-

   Select *EID* to display devices numerically by EID number.

   -or-

   Select *Port* to display devices numerically by port number.

2. Click *OK*.

Depending on the display method selected, the corresponding button will be depressed in the *Main* dialog box.

To change how the local UI is invoked:

1. Select the checkbox next to one of the listed methods.
2. Click *OK*.

To set a Screen Delay Time for the local UI:

1. Type in the number of seconds (0-9) to delay the local interface display after you press Print Screen. Enter **0** to launch the local user interface with no delay.
2. Click *OK*.

Setting a Screen Delay Time enables you to complete a soft switch without the local user interface. To perform a soft switch, see Soft switching on page 18.

Controlling the status flag

The status flag displays on your desktop and shows the name or EID number of the selected device or the status of the selected port. Use the *Flag* dialog box to configure the flag to display by device name or EID number, or to change the flag color, opacity, display time, and location on the desktop.

To access the local UI *Flag* dialog box:

Activate the local UI and click *Setup* > *Flag* to open the *Flag* dialog box.

To determine how the status flag is displayed:

1. Select *Name* or *EID* to determine what information will be displayed. The following interface *Status Flags* are available.
   - Flag Description
   - Flag type by name
   - Flag type by EID number
   - Flag indicating that the user has been disconnected from all systems

2. Select *Displayed* to activate the flag display. After a switch, the flag will remain on the screen until the user switches to another device. Selecting *Timed* will cause the flag to display for five seconds when a switch is made and then disappear.
3. Select a flag color under Display Color. The following flag colors are available:
    - Flag 1 - Gray flag with black text
    - Flag 2 - White flag with red text
    - Flag 3 - White flag with blue text
    - Flag 4 - White flag with violet text
4. In Display Mode, select *Opaque* for a solid color flag or *Transparent* to see the desktop through the flag.
5. To position the status flag on the desktop:
    a. Click *Set Position* to gain access to the position flag screen.
    b. Left-click on the title bar and drag it to the desired location.
    c. Right-click to return to the *Flag* dialog box.

NOTE: Changes made to the flag position are not saved until you click OK in the Flag dialog box.

6. Click *OK* to save settings.

   -or-

   Click *X* to exit without saving changes.

Setting the keyboard country code

NOTE: Using a keyboard code that supports a language different from that of your switch firmware will cause incorrect keyboard mapping.

By default, the switch sends the US keyboard country code to USB modules attached to devices, and the code is applied to the devices when they are turned on or rebooted. Codes are then stored in the IQ Module. Issues may arise when you use the US keyboard country code with a keyboard of another country.

For example, the Z key on a US keyboard is in the same location as the Y key on a German keyboard. The *Keyboard* dialog box enables you to send a different keyboard country code than the default US setting. The specified country code is sent to all devices attached to the switch when they are turned on or rebooted, and the new code is stored in the IQ Module.

NOTE: If an IQ Module is moved to a different device, the keyboard country code will need to be reset.

Assigning device types

To access the local UI *Devices* dialog box:

Activate the local user interface and click *Setup* > *Devices* to open the *Devices* dialog box.

NOTE: The Modify button is available only if a configurable switch is selected.

When the switch discovers a tiered switch, the numbering format changes from switch port to [switch port]-[switch port] to accommodate each device under that switch.

For example, if a switch is connected to console switch port 6, each device connected to it would be numbered sequentially. The device using console switch port 6, switch port 1, would be 06-01, the device using console switch port 6, switch port 2, would be 06-02, and so on.

To assign a device type:

1. In the *Devices* dialog box, select the desired port number.
2. Click *Modify* to open the *Device Modify* dialog box.
3. Choose the number of ports supported by your switch and click *OK*.
4. Repeat steps 1-3 for each port requiring a device type to be assigned.

Assigning device names

Use the *Names* dialog box to identify devices by name rather than by port number. The *Names* list is always sorted by port order. You can toggle between displaying the name or the EID number of each IQ Module, so even if you move the IQ Module/device to another port, the name and configuration will be recognized by the switch.

NOTE: When it is initially connected, a device will not appear in the Names list until it is turned on. Once an initial connection has been made, it will appear in the Names list even when turned off.

To access the local UI *Names* dialog box, activate the local UI and click *Setup - Names*.

NOTE: If new CO cables are discovered by the switch, the on-screen list will be automatically updated. The mouse cursor will change into an hourglass during the update. No mouse or keyboard input will be accepted until the list update is complete.

To assign names to devices:

1. In the *Names* dialog box, select a device name or port number and click *Modify* to open the *Name Modify* dialog box.
2. Type a name in the *New Name* box. Names of devices may contain all printable characters.
3. Click *OK* to assign the new name.
4. Repeat steps 1-3 for each device in the system.

5. Click *OK* in the *Names* dialog box to save your changes.

   -or-

   Click *X* or press *Escape* to exit the dialog box without saving changes.

Configuring network settings

Use the *Network* dialog box to set the Network Speed, Transmission Mode, and Network Configuration feature.

To change network settings:

1. If the local UI is not open, press **Print Screen** to open the *Main* dialog box.
2. Click *Setup* - *Network* to open the *Network* dialog box.
3. Make desired changes and click *OK* to confirm or click **X** to exit without saving.

NOTE: Changing the network settings will cause the switch to reboot.

4. Click *OK* in the *Devices* dialog box to save settings.

NOTE: Changes made in the Device Modify dialog box are not saved to the switch until you click OK in the Device Modify dialog box.

NOTE: Changes made in the Name Modify dialog box are not saved to the switch until you click OK in the Names dialog box.

NOTE: If an IQ Module has not been assigned a name, the EID is used as the default name.

Commands Dialog Box Functions

From the local UI *Commands* dialog box, you can manage your switch system and user connections, enable the Scan mode, and update your firmware.

Table 10. Commands to Manage Routine Tasks for Your Devices

Features	Purpose
Scan Enable	Begin scanning your devices. Set up a device list for scanning in the Setup dialog box. You must have at least two devices selected in the Setup - Scan List menu to enable device scanning.
User Status	View and disconnect users.
IQ Module Status	Display the currently available firmware for each type of IQ Module.
Display Versions	View version information for the switch as well as view and upgrade firmware for individual CO cables.
Display Config	View current configuration parameters.

Features	Purpose
Device Reset	Re-establish operation of keyboard and mouse on the local port.

To access the local UI *Commands* dialog box:

Activate the local UI and click *Commands* to open the dialog box.

Selecting devices for scan mode

The *Scan* dialog box allows the local user to define a custom list of devices to include while in Scan mode and the number of seconds to display each device. The creation of the Scan list does not start Scan mode. You must enable Scan mode using the *Scan Enable* checkbox on the *Commands* dialog box. The Scan list is displayed in the manner set from the *Menu* dialog box. It can be changed in the *Scan* dialog box to sort either by name, EID, or port by choosing one of the buttons. If a device on the list is *unavailable*, it is skipped. Watch mode views a device unless a conflicting network user blocks the path to that device. If a conflict is detected in Watch mode (or the device is unavailable), the device to be viewed is skipped.

To add devices to the Scan list:

1. Activate the local UI and click *Setup* - *Scan* to open the *Scan* dialog box.
2. The dialog box contains a listing of all devices attached to your switch. Click the checkbox to the right of the device, double-click on the desired entry, or highlight the device, and click the *Add/Remove* button to toggle the *Scan* checkbox setting. You can select up to 100 devices for inclusion in the Scan list.

NOTE: Click the *Clear* button to remove all devices from the Scan list.

3. In the Time field, type the number of seconds (from 3 - 255) to display each device while scanning. The default is 15 seconds per device.
4. Click *OK*.

NOTE: The order in which the devices appear in the *Scan* dialog box is based on the order in which they were selected. Scanning a single device multiple times during a loop is not supported. Scan time must be the same for all devices.

Enabling or disabling scan mode

To start the Scan mode:

1. Activate the local UI and click *Commands*. The *Commands* dialog box is displayed.
2. Select *Scan Enable* in the *Commands* dialog box. Scanning will begin.

3. Click *X* to close the *Commands* dialog box.

To cancel Scan mode:

Select a device if the local UI is open.

-or-

Move the mouse or press any key on the keyboard if the local UI is not open. Scanning will stop at the currently selected device.

-or-

From the *Commands* dialog box, clear the Scan Enable checkbox.

Viewing and disconnecting user connections

You can view and disconnect users through the *User Status* dialog box. The username (U) and server (S) will always be displayed when connected to a device (local or remote). You can display either the device name or EID number to which a user is connected. If there is no user currently connected to a channel, the username and device fields will be blank.

To view current user connections, activate the local UI and click *Commands* > *User Status* to open the *User Status* dialog box.

To disconnect a user:

1. On the *User Status* dialog box, click the letter corresponding to the user to disconnect. The *Disconnect* dialog box will appear.
2. Click *Disconnect* to disconnect the user and return to the *User Status* dialog box.

   -or-

   Click *X* or press *Escape* to exit the dialog box without disconnecting a user.

Displaying version information and upgrading firmware

For troubleshooting and support, the local UI enables you to display the version number of the switch firmware and any auxiliary devices connected to the switch, as well as upgrade your firmware for optimum performance.

To display version information and upgrade firmware:

1. Activate the local UI and click *Commands - Display Versions*. The top half of the box lists the subsystem version in the switch. The lower half displays the current IP address, Mask, MAC, and EID.
2. If you want to upgrade the firmware, click *Upgrade* and then click *OK* to open the download box. You will be prompted for an FTP or TFTP device IP address and the related information.
3. Click *Download*. After the firmware is downloaded, the *Upgrade* dialog box will appear.

4. Click the *Upgrade* button.

NOTE: The switch will reboot when the upgrade is complete.

To upgrade individual CO cables:

1. Click the *IQ* button to view individual CO cable version information.
2. Select the *IQ* button to view and click the *Version* button.
3. Click the *Load Firmware* button.
4. Click *OK* to initiate the upgrade and return to the *Status* dialog box.

NOTE: During an upgrade, the CO cable status indicator in the Main dialog box is yellow. The CO cables are *unavailable* when an upgrade is in progress. When an upgrade is initiated, any current connection to the device using the CO cable is terminated.

To simultaneously upgrade multiple CO cables:

1. Activate the local UI, click *Commands - IQ Status* and click one or more types of CO cables to upgrade.
2. Click *Upgrade*.

NOTE: When the Enable IQ Auto update option is enabled in the IQ Status dialog box, CO cable firmware is automatically upgraded when the switch firmware is upgraded or when a new CO cable is discovered by the switch after a firmware upgrade. CO cables that have already been discovered but which are not attached to the switch during the firmware upgrade must be upgraded manually.

3. The IQ *Upgrade* dialog box is displayed. Click *OK* to initiate the upgrade and return to the IQ *Status* dialog box.

To return a CO cable to factory default status:

1. Click *IQ* in the *Version* dialog box.
2. Select a CO cable, then click *Decommission*.
3. Click *OK* to restore factory defaults. You will see the CO cable go offline briefly and return.

   - or-

   Click *X* or press *Escape* to cancel the operation.
4. Click *X* to close the IQ *Select* dialog box.

Chapter 4. OBWI Operation

The OBWI for the LCM switch is a remote, web browser-based user interface. For details on setting up your system, see Connecting the LCM Switch Hardware on page 6. 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 11. 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.

NOTE: The switch will attempt to detect if Java is already installed on your PC. If it is not, in order to use the OBWI, you will need to install it. You may also need to associate the JNLP file with Java WebStart.

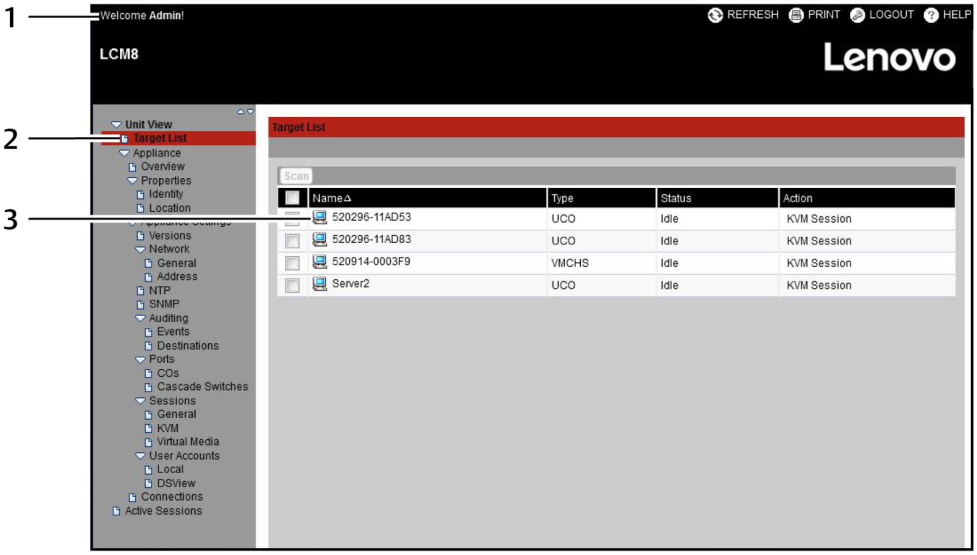
NOTE: Using the OBWI requires using Java Runtime Environment (JRE) version 1.6.0_11 or higher.

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

Using the OBWI

After you have been authenticated, the user interface appears. You may view, access, and manage your switch, as well as specify system settings and change profile settings. The following figure shows the user interface window areas. Screen descriptions are provided in the following table.

Figure 7. OBWI Window
Figure 8.



□	Name∆	Type	Status	Action
□	520296-11AD53	UCO	Idle	KVM Session
□	520296-11AD83	UCO	Idle	KVM Session
□	520914-0003F9	VMCHS	Idle	KVM Session
□	Server2	UCO	Idle	KVM Session

Table 12. Descriptions for the OBWI

Number	Description
1	Top option bar: Use the top option bar to contact Technical Support, view the software general information, log out of an OBWI session, or access the Help tool
2	Side navigation bar: Use the side navigation bar to select the information to be displayed. You can use the side navigation bar to display windows in which you can specify settings or perform operations.

Number	Description
3	Content area: Use the content area to display or make changes to the switch OBWI system.

Viewing System Information

You can view switch and target device information from the following screens in the user interface.

Table 13. System Information

Category	Select This:	To View This:
Target Devices	Unit View - Target Devices	List of connected devices, as well as the name, type, status, and action of each device. Click on a target device to view the following information: name, type, EID, available session option, and the connection path.
LCM switch	Unit View - Appliance - Tools	Name, type, and the switch tools (Maintenance-Overview/Reboot/Reset and Upgrade, Certificates, and Trap MIB).
	Unit View - Appliance - Files	Configuration and User Database for the switch.
	Unit View - Appliance - Properties - Identity	Part number, serial number, and status of the digital activation key (default setting is disabled).
	Unit View - Appliance - Properties - Location	Site, department, and location of each unit.
	Unit View - Appliance Settings - Versions	Current application, boot, build, hardware, UART, and video ASIC versions.
	Unit View - Appliance Settings - Network	Network address, LAN speed, and web server ports.
	Unit View - Appliance Settings - SNMP	System description, SNMP setting, contact, read/write and trap settings, and designations for allowed managers.
	Unit View - Appliance Settings - Auditing	Events list and status and SNMP trap destinations.
	Unit View - Appliance Settings - Ports	Status, EID, name, port, application and interface type for each CO cable; name, port, type, channels, and status for each tiered switch.
	Unit View - Appliance Settings	General session timeout and sharing details; KVM encryption levels and keyboard language; virtual media settings, drive mappings, encryption level, and CO cable access.

Category	Select This:	To View This:
	Sessions	
	Unit View - Appliance - User Accounts	Security and user lock-out for the local account; authentication server assignments for DSView management software, and override admin username and password in case of a failed operation.
	Unit View - Appliance - Connections	Connection path name and type.
	Active Sessions	Server, owner, remote host, duration, and type of each active session.

Generating a Certificate

A web certificate allows you to access the OBWI without having to acknowledge the switch as a trusted web device each time you access it. Using the Install Web Certificate window, you can generate a new self-signed openssl or upload a certificate. Uploaded certificates must be in OpenSSL PEM format with an unencrypted private key.

To install a web certificate:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Manage Appliance Web Certificate*.
3. Click *Update*.
4. Select the *Generate a new Self-Signed Certificate* radio button and enter the following fields:
   - Common Name: your name. (Since this is your root certificate, use an appropriate name such as, "Company_Name Certificate Authority.")
   - Organization: organization unit name (marketing, for example).
   - City or Locality: the city where your organization is located.
   - State or Province: the unabbreviated state or province where your organization is located.
   - Country: the two-letter ISO abbreviation for your country.
   - Email Address: the email address for the Certificate Authority (CA) to contact.
5. Click Generate to create the certificate.

To upload a new certificate:

1. Click the Upload a New Certificate radio button.
2. Select the method (Filesystem, TFTP, FTP, or HTTP).
3. Click Browse to search for the certificate or enter the certificate filename.
4. Select Install. Close the web browser, then launch the OBWI again for the same IP address.

NOTE: If importing a company certificate file, it may take up to 30 seconds for the OBWI to launch.

5. When prompted, click to view the certificate and follow the instructions to import the certificate into the Root Certificate Authority folder. After the certificate is stored, the user should not see the certificate warning.

Tools - Rebooting and Upgrading

From the Unit View - Appliance - Overview page, you can view the switch name and type. You can also perform the following tasks.

Rebooting the Switch

To reboot the switch:

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

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 switch to complete the reboot.

Upgrading switch firmware

You can update your switch with the latest firmware available.

After the 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 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, click *Unit View - Appliance - Overview* to open the Unit Maintenance screen.
2. Click *Upgrade Firmware*.

3. Select one of the following methods to load the firmware file: *Filesystem*, *TFTP*, *FTP*, or *HTTP*.

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

4. If you selected Filesystem, 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 the *Upgrade* button.

Saving and restoring configurations and user databases

You may save the switch configuration to a file. The configuration file will contain information about the managed switch. 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 switch configuration or user database of a managed switch:

1. From the side navigation bar, click *Unit View - Appliance - Overview*.
2. Click either the *Save Appliance Configuration* or *Save Appliance User Database*, then click the *Save* tab.
3. Select the file save method: *Filesystem*, *TFTP*, *FTP*, or *HTTP PUT*.
4. If you selected TFTP, enter the Server IP Address and Firmware Filename you wish to load.

   -or-

   If you selected FTP or HTTP, enter the Server IP Address, Username, User Password, and Firmware Filename you wish to load.

5. Click the *Download* button. The *Save As* dialog box will open.
6. Navigate to the desired location and enter a name for the file. Click the *Save* button.

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

1. From the side navigation bar, click the *Unit View - Appliance - Overview*.
2. Click either the *Restore Appliance Configuration or Restore Appliance User Database*, then click the *Restore* tab.
3. Select the file save method: *Filesystem*, *TFTP*, *FTP*, or *HTTP*.

4. If you selected Filesystem, click the *Browse* button to specify the location of the firmware upgrade file.

   -or-

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

   -or-

   If you selected FTP or HTTP, enter the Server IP Address, User Name, User Password, and Firmware Filename you wish to load.
5. Click the *Browse* button. Navigate to the desired location and select the file name. Click the *Upload* button.
6. After the success screen appears, reboot the managed switch to enable the restored configuration. See Tools - Rebooting and Upgrading on page 33.

Recovering From a Failed Flash Upgrade

NOTE: You may only recover from a failed Flash upgrade when using IPv4 mode. If the green power LED on the front and back panel of the Remote Console switch blinks continuously, the Remote Console switch is in recovery mode.

To recover from a failed Flash upgrade:

1. Download the latest Flash firmware.
2. Save the Flash upgrade file to the appropriate directory on the TFTP server.
3. Set up the TFTP server with the server IP address 10.0.0.20.
4. Rename the downloaded file “CMN-1095.fl” and place it into the TFTP root directory of the TFTP server.
5. If the Remote Console switch is not on, turn it on now. The recovery process should start automatically.

Property Identity and Location Settings

The switch can report most device properties directly through the switch web browser. Clicking Identity displays the Unit Identification Properties screen and provides the Part Number, Serial Number, and status of the digital activation key. The Unit Location Properties screen displays the Site, Department and Location.

Viewing Version Information

The Version screen displays version information of the Current Application, Boot, Build, Hardware, UART, and Video ASIC versions. This screen is a read-only screen.

Network Settings

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

From the side navigation bar, click *Network* to display the General, IPv4, and IPv6 tabs.

To configure general network settings:

1. Click the *Network* tab, then click the **General** tab to display the switch General Network Settings screen.
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*, or *100 Mbps 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. Verify or modify the HTTP or HTTPS ports. The settings will default to HTTP 80 and HTTPS 443.
5. Click *Save*.

To configure IPv4 network settings:

1. Click the *Network* tab, then click the *Address* tab to display the IPv4 Settings screen.
2. Click the *IPv4* button.
3. Click to fill or clear the **Enable IPv4** checkbox.
4. Enter the desired information in the Address, Subnet, and Gateway fields. IPv4 addresses are entered as the xxx.xxx.xxx.xxx dot notation.
5. Select either *Enabled* or *Disabled* from 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.

6. Click *Save*.

To configure IPv6 network settings:

1. Click the *IPv6* button.

2. Enter the desired information in the Address, Subnet, and Prefix Length fields. IPv6 addresses are entered as the FD00:172:12:0:0:0:0:33 or abbreviated FD00:172:12::33 hex notation.
3. Select either *Enabled* or *Disabled* from the DHCP drop-down menu.

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

4. 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. 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. Click *SNMP* to open the SNMP screen.
2. Click to enable the *Enable SNMP* checkbox 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 switch.
6. Click *Save*.

Auditing 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. Click *Auditing* to open the Events screen.
2. Specify the events that will generate notifications by clicking the appropriate checkboxes in the list.

   -or-

   Select or clear the checkbox 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 devices. The events enabled on the Events screen are sent to all the devices listed on the Event Destination screen.

To set event destinations:

1. Click *Auditing* and the **Destinations** tab 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 devices.
3. Click *Save*.

Ports Settings - Configuring a CO cable

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

You can also delete an offline CO cable and upgrade the CO cable firmware.

Deleting CO cables

To delete an offline CO cable:

1. From the side navigation bar, click *Ports - COs* to open the CO cable screen.
2. Click in the applicable CO cable checkbox.
3. Click *Delete Offline*.

Upgrading CO cables

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

To upgrade the CO cable firmware:

1. From the side navigation bar, click *Ports - COs* to open the CO cables screen.
2. Select the checkboxes next to the CO cables that you wish to modify.
3. Select *Choose an operation* and select *Upgrade*.
4. If the settings are correct, click *Upgrade*.

If the switch is configured to auto upgrade COs, the COs will automatically update when the switch updates. To update your switch firmware, see Tools - Rebooting and Upgrading on page 33 or the DSView management software Online Help. If issues occur during the normal upgrade process, CO cables may also be force-upgraded when needed.

To set the USB speed:

NOTE: This section only applies to the VCO CO cable.

1. From the side navigation bar, click *Ports - COs* to open the CO cables screen.
2. Select the checkboxes next to the CO cables that you wish to modify.
3. Select *Operations* and select either *Set USB 1.1 speed* or *Set USB 2.0 speed*.

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 Target Devices. A list of available devices will appear.
2. The applicable action, KVM Session, will be displayed in the Action column, and will depend on the target device that was selected to launch the session. If more than one action is available for a given target device, click the drop-down arrow and select the applicable action from the list.

If the target device is currently in use, you may be able to gain access by forcing a connection to the device if your 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 checkbox. The Video Viewer window will appear.

NOTE: The digital activation key is required for KVM remote access.

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

General sessions settings

To configure general session settings:

1. From the side navigation bar, select *Sessions - General*. The General Session Settings screen appears.
2. Select or deselect the *Enable Inactivity Timeout* checkbox.
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. Click *Save*.

Local user account settings

NOTE: User Account settings are supported when the digital activation key is installed.

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

Access levels

NOTE: Multiple access levels are supported when the digital activation key is installed.

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 14. Allowed Operations by 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	No

Operation	Appliance Administrator	User Administrator	Users
		only	
Change Your Own Password	Yes	Yes	Yes
Access Server	Yes, all Servers	Yes, all Servers	Yes, if allowed

To add a new user account (User Administrator or Appliance Administrator only):

1. From the side navigation bar, select *User Accounts - Local User Accounts* to open the 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 access level for the new user.
5. Select any of the available devices that you wish to assign to the user account and click *Add*.

NOTE: User Administrators and Appliance Administrators can access all devices.

6. Click *Save*.

To delete a user account (User Administrator or Appliance Administrator only):

1. From the side navigation bar, select *User Accounts - Local Accounts* to open the Local User Accounts screen.
2. Click the checkbox 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. From the side navigation bar, select *User Accounts - Local Accounts*. The 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*.

Virtual media session settings

To set virtual media options:

1. From the side navigation bar, select *Sessions - Virtual Media* to open the Virtual Media Session Settings screen.
2. Either enable or disable the *Virtual Media locked to KVM Sessions* checkbox.
3. Either enable or disable the *Allow Reserved Sessions* checkbox.

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. Click *Save*.
7. Select the checkbox next to each CO cable for which you want to enable virtual media and click *Enable VM*.

   -or-

   Select the checkbox next to each CO cable for which you want to disable virtual media and click *Disable VM*.

Virtual media options

You can determine the behavior of the switch during a virtual media session using the options provided in the Virtual Media Session Settings screen. The following table outlines the options that can be set for virtual media sessions.

Local users

Local users can 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 that are listed in the following table.

Table 15. 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 checkbox to establish a virtual media CD-ROM or DVD-ROM connection to a device. Disable to end a virtual media CD-ROM or DVD-ROM connection to a device.
Mass Storage	Allows virtual media sessions to the first detected mass storage drive. Enable this checkbox to establish a virtual media mass storage connection to a device. Disable to end a virtual media mass storage connection to a device.

DSView Software Settings

NOTE: DSView Software settings are supported when the digital activation key is installed.

You can contact and register an unmanaged switch with an DSView management software device by specifying the IP address of the management software device.

To configure the device IP address:

1. On the side navigation bar, select *User Accounts - Avocent*. The DSView management software Settings screen is displayed.
2. Enter the device IP addresses that you want to contact. Up to four addresses are allowed.
3. Use the scroll bar to select the desired retry interval.
4. To disassociate the switch that has been registered with the device, click the *Disassociate* button.
5. Click *Save*.

Active 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.

Closing a Session

To close a session:

1. From the side navigation bar, select *Active Sessions* to display the Appliance Active Sessions screen.
2. Click the checkbox 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* checkbox.

Chapter 5. 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 KVM 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

The Local Console Manager switch uses 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

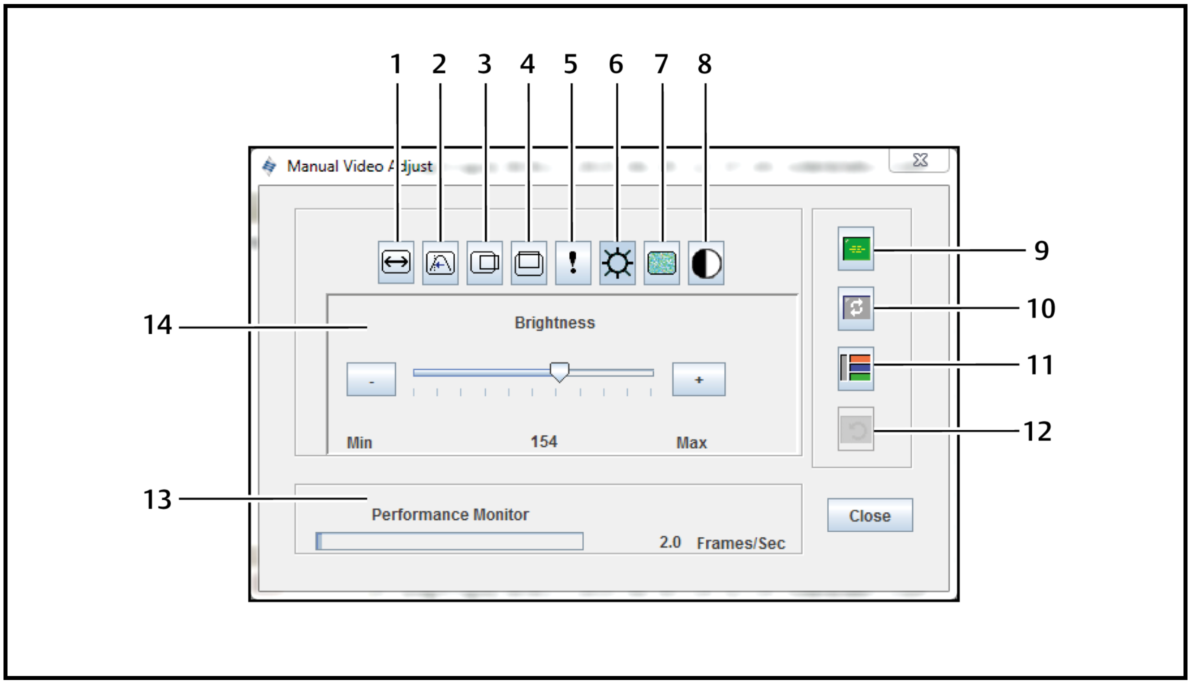


Table 16. Manual Video Adjust Window Descriptions

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. For details, see the Mouse and Pointer Settings Technical Bulletin, which is available on the Avocent web site.

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, 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.
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 17. 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 6. Appendices

Appendix 1: Terminal Operation

Each switch may be configured at the switch level through the Terminal Console menu interface, which is accessed through the setup port. All terminal commands are accessed through a terminal screen or a 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 a serial adaptor, a terminal or a PC that is running terminal emulation software, such as HyperTerminal software, 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 the switch and each target device. When the switch completes initialization, the Console menu will display the following message: *Press any key to continue.*

Network Configuration

To configure network settings using the Console menu:

1. When you turn on the switch, it initializes for approximately one minute. After it completes initialization, press any key on the terminal or on the computer running the terminal emulation software to access the Console menu interface.

   The terminal may be connected at any time, even when the switch is already turned on.
2. Once the Console Main Menu is displayed, type the number corresponding to Network Configuration and press **Enter** .
3. Type 1 and press **Enter** to set your network speed. For best performance, set the switch at the same speed as the Ethernet switch to which it is attached. Press **Enter** to return to the Console Network Configuration menu.
4. Type 2 and press **Enter** to specify whether you are using a static or DHCP address.

   A static IP configuration may be used to provide a user-defined IP address, netmask, or prefix length, and default gateway for the switch.

DHCP is a protocol that automates the configuration of TCP/IP-enabled computers. When DHCP is selected, the IP address, netmask or prefix length, and default gateway settings are automatically assigned to the switch and may not be modified by a switch user.

If you are using the DHCP option, configure your DHCP device to provide an IP address to the switch and then go to step 6.

5. Select the remaining options from the Network Configuration menu to finish the configuration of your switch with an IP address, netmask or prefix length, and default gateway.
6. Type **0** (zero) and press **Enter** to return to the Console Main menu.

Other Console Main Menu Options

Besides the Network Configuration option, the Console Main Menu of the switch features the following menu items: Firmware Management, Enable Debug Messages, Set/Change Password, Restore Factory Defaults, Reset Switch, Set Web Interface Ports, and Exit. Each menu item is discussed in this section.

Firmware management

This menu contains the Flash Download selection. For more information, see Tools - Rebooting and Upgrading on page 33.

Enable debug messages

This menu option turns on console status messages. Because this can significantly reduce performance, 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.

Set/Change password

This menu option allows enabling and disabling of serial port security, which locks the serial port with a user-defined password.

Restore factory defaults

This menu option will restore all switch options to the default settings.

Reset appliance

This menu option allows you to execute a soft reset of the appliance.

Set web interface ports

The switch uses ports 80 and 443 for HTTP and HTTPS port numbers, respectively. The user can modify or specify alternate ports.

NOTE: A reboot of the switch is required to use new port numbers.

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 Password login screen.

Appendix 2: Setup Port Pinouts

The switch setup port is an 8-pin modular jack. The setup port pinouts and descriptions are provided in the following figure and table.

Figure 10. Setup Port Pinouts

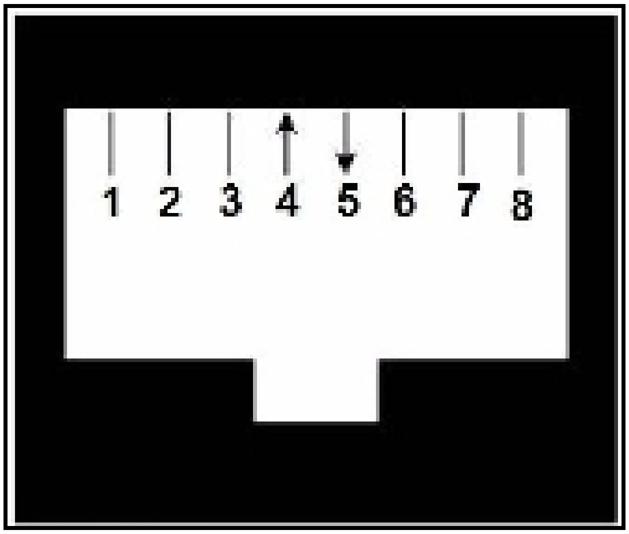


Table 18. Console/Setup Port Pinout Descriptions

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

Appendix 3: Using Serial IQ Modules

The serial CO cable is a serial-to-VGA converter that allows VT100-capable devices to be viewed from the switch local port, the OBWI, or by using the switch software. All serial data coming from the device is read-only. The data is displayed in a VT100 window, placed into a video buffer, and sent to the switch as though it came from a VGA device. Likewise, keystrokes entered on a keyboard are sent to the attached device as though they were typed on a VT100 terminal.

Serial CO cable modes

The following modes can be accessed from the serial CO cable:

- On-Line: This mode enables you to send and receive serial data.
- Configuration: This mode enables you to specify switch communication parameters, the appearance of the Terminal Applications menu, and key combinations for specific actions and macros.
- History: This mode enables you to review serial data.

Configuring the serial CO cable

NOTE: The serial CO cable is a DCE device and only supports VT100 terminal emulation.

Pressing **Ctrl-F8** will activate the Configuration screen of the CO cable's Terminal Applications menu, which enables you to configure your serial CO cable.

NOTE: When any Terminal Applications menu is active, pressing Enter saves changes and returns you to the previous screen. Pressing Escape returns you to the previous screen without saving changes.

Within the Terminal Applications menu's Configuration screen, you can modify the following options:

- Baud Rate: This option allows you to specify the serial port communications speed. Available options are 300, 1200, 2400, 9600, 19,200, 34,800, 57,600 or 115,200 bps. The default value is 9600.
- Parity: This option allows you to specify the communications parity for the serial port. Available options are EVEN, ODD or NONE. The default value is NONE.
- Flow Control: This option allows you to specify the type of serial flow control. Available options are NONE, XOn/XOff (software) and RTS/CTS (hardware). The default value is NONE. If you select a bps rate of 115,200, the only available flow control is RTS/CTS (hardware).
- Enter Sends: This option enables you to specify the keys that are transmitted when Enter is pressed. Available options are CR (Enter), which moves the cursor to the left side of the

screen, or CR LF (Enter-Linefeed), which moves the cursor to the left side of the screen and down one line.

- Received: This option enables you to specify how the module translates a received Enter character. Available options are CR (Enter) or CR LF (Enter-Linefeed).
- Background: This option changes the screen's background color. The currently selected color displays in the option line as it is changed. Available colors are Black, Light Grey, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon and Brown. The default color is Black. This value cannot be identical to the Normal Text or Bold Text value.
- Normal Text: This option changes the screen's normal text color. The currently selected color displays in the option line as it is changed. Available colors are Grey, Light Grey, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon and Brown. The default color is Grey. This value cannot be identical to the Bold Text or Background value.
- Bold Text: This option changes the screen's bold text color. The currently selected color displays in the option line as it is changed. Available colors are White, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon, Brown and Light Grey. The default color is White. This value cannot be identical to the Normal Text or Background value.
- Screen Size: This option allows you to specify the screen's text width size. Available values are widths of 80 columns or 132 columns. The length for both widths is 26 lines.

The following options for the Terminal Application menu's Configuration screen enable you to define the function keys that will perform a selected action. To specify a new function key, press and hold the Ctrl key, then press the function key that you want to associate with the action. For example, if you want to change the Configuration (Config) Key Sequences option from **Ctrl-F8** to **Ctrl-F7** , press and hold the **Ctrl** key and then press **F7** .

- Config Key Sequences: This option allows you to define the key combination that makes the Terminal Application menu's Configuration screen appear. The default key sequence is **Ctrl-F8** .
- On-Line Key Sequence: This option allows you to define the key sequence that displays the On-Line mode. The default key sequence is **Ctrl-F10** .
- Help Key Sequence: This option allows you to define the key combination that displays the Help System screen. The default key sequence is **Ctrl-F11**.
- History Key Sequence: This option allows you to define the key combination that enables History mode. The default key sequence is **Ctrl-F9**.
- Clear History Key Sequence: This option allows you to define the key combination that clears the history buffer while in History mode. The default key sequence is **Ctrl-F11**.

- Break Key Sequence: This option allows you to configure the key combination that generates a break condition. The default key sequence is **Alt-B**.

To configure a serial CO cable:

1. Press **Ctrl-F8** . The Configuration Screen will appear.
2. Select a parameter to change. You can navigate the Configuration Screen using the **Up Arrow** and **Down Arrow** keys.
3. Modify the selected value using the **Left Arrow** and **Right Arrow** keys.
4. Repeat steps 2 and 3 to modify additional values.
5. Press **Enter** to save your changes and exit the Configuration Screen.

   -or-

   Press **Escape** to exit the Configuration Screen without saving the changes.

Creating a Serial CO Module Macro

Pressing the **Page Down** key when the Terminal Applications menu's Configuration screen is displayed will provide access to the Macro Configuration screen. The serial CO cable can be configured with up to 10 macros. Each macro can be up to 128 characters in length.

To create a macro:

1. Select the serial CO cable you wish to configure and press **Ctrl-F8** to activate the Terminal Applications menu's Configuration screen.
2. When the Terminal Applications menu appears, press **Page Down** to view the Macro Configuration screen. The Macro Configuration screen shows the 10 available macros and the associated key sequences, if any, for each.
3. Using the **Up Arrow** and **Down Arrow** keys, scroll to an available macro number and highlight the listed keystroke sequence. Type the new macro keystroke sequence over the default. Any combination of **Ctrl** or **Alt** and a single key may be used. When you have finished entering the keystroke sequence that will activate the new macro, press the **Down Arrow** key.
4. On the line below the macro keystroke sequence you just entered, type the keystroke sequence that you wish the macro to perform.
5. Repeat steps 3 and 4 to configure additional macros.
6. When finished, press **Enter** to return to the previous screen.

Using history mode

History mode allows you to examine the contents of the history buffer, which contains the events that have occurred.

The serial CO cable maintains a buffer containing 240 lines minimum, or 10 screens, of output. When the history buffer is full, it will add new lines at the bottom of the buffer and delete the oldest lines at the top of the buffer.

NOTE: The Config Key Sequence, On-Line Key Sequence and Clear History Key Sequence used in the following procedure are the default values. These key combinations can be changed using the Terminal Applications menu.

To use History mode:

1. Press **Ctrl-F9** . The mode will display as History.
2. Press one of the following key combinations to perform the indicated action:
    - **Home**: Move to the top of the buffer.
    - **End**: Move to the bottom of the buffer.
    - **Page Up**: Move up one buffer page.
    - **Page Down**: Move down one buffer page.
    - **Up Arrow**: Move up one buffer line.
    - **Down Arrow**: Move down one buffer line.
    - **Ctrl-F8** : Enters Configuration mode. The Configuration screen will appear.
    - **Ctrl-F9** : While in Configuration mode, returns to the previous screen with History mode enabled.
    - **Ctrl-F10** : While in Configuration mode, returns to the previous screen with On-Line mode enabled.
    - **Ctrl-F11** : Clears the history buffer. If you choose this option, a warning screen will appear. Press **Enter** to delete the history buffer or Escape to cancel the action. The previous screen will reappear.
3. When finished, press **Ctrl-F10** to exit History mode and return to On-Line mode.

Serial CO cable pinouts

The following table lists the pinouts for the serial CO cable.

Table 19. Serial IQ Module Pinouts

DB9-F Pin	Host Signal Name Description	Signal Flow	SRL Signal Name Description
1	DCD - Data Carrier Detect	Out of SRL	DTR - Data Terminal Ready
2	RXD - Receive Data	Out of SRL	TXD - Transmit Data
3	TXD - Transmit Data	In to SRL	RXD - Receive Data
4	DTR - Data Terminal Ready	In to SRL	DSR - Data Set Ready
5	GND - Signal Ground	N/A	GND - Signal Ground
6	DSR - Data Set Ready	Out of SRL	DTR - Data Terminal Ready
7	RTS - Request to Send	In to SRL	CTS - Clear to Send
8	CTS - Clear to Send	Out of SRL	RTS - Request to Send
9	N/C - Not Connected	N/A	N/C - Not Connected

Appendix 4: 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 CO 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 20. 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.

(2) The Command key is the Sun Meta (diamond) key.

Appendix 5: UTP Cabling

This appendix discusses various aspects of connection media. The switch system utilizes UTP cabling. The performance of the 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 switch supports.

- CAT 5 (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. CAT 5 cable is generally used for networks running at 10 or 100 Mbps.
- CAT 5E (enhanced) cable has the same characteristics as CAT 5, but is manufactured to somewhat more stringent standards.
- CAT 6 cable is manufactured to tighter requirements than CAT 5E cable. CAT 6 has higher measured frequency ranges and significantly better performance requirements than CAT 5E 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 UTP cable specifications. The switch system supports either of these wiring standards. The following table describes the standards for each pin.

Table 21. 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.

Appendix 6: Technical Specifications

Table 22. LCM Switch Technical Specifications

Category	Value
Number of Ports	LCM8: 8 AHI/ARI LCM16: 16 AHI/ARI
Type	PS/2, USB and serial modules
Connectors	8-pin modular (RJ-45)
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, 30 meters maximum length
Dimensions	
Form Factor	1U or 0U rack mount
Dimensions	1.70 x 17.00 x 9.42 inches (Height x Width x Depth) (4.32 x 43.18 x 23.93 cm)
Weight (without cables)	LCM8: 5.98 lb (2.71 kg); LCM16: 6.16 lb (2.79 kg)
Setup Port	
Number	1
Protocol	RS-232 serial
Connector	8-pin modular (RJ-45)
Local Port	
Number/Type	8 Port 1 VGA - HDD15 4 USB 16 Port 2 VGA - HDD15 8 USB
Network Connection	
Number	2
Protocol	10/100 Ethernet
Connector	8-pin modular (RJ-45)
USB Port	

Category	Value
Number	4 or 8 depending on model
Protocol	USB 2.0
Power Specifications	
Connectors	LCM8: 1 IEC C14 LCM16: 2 IEC C14
Type	Internal
Power	18W
Heat Dissipation	47 BTU/hr
AC Input Range	100 - 240 VAC
AC Frequency	50/60 Hz auto-sensing
AC Input Current Rating	0.6A
AC Input Power (Maximum)	20 W
Ambient Atmospheric Condition Ratings	
Temperature	Operating: 32 to 122 degrees Fahrenheit (0 to 50 degrees Celsius) Non-operating: -4 to 158 degrees Fahrenheit (-20 to 70 degrees Celsius)
Humidity	Operating: 20% to 80 % relative humidity (non-condensing) Non-operating: 5% to 95% relative humidity, 38.7 degrees Celsius maximum wet bulb temperature
Safety and EMC Standard Approvals and Markings	UL / cUL, CE - EU, N (Nemko), GOST, C-Tick, NOM / NYCE, KCC, SASO, Nemko GS, IRAM, FCC, ICES, VCCI, SoNCAP, SABS, Bellis, Koncar, INSM, STZ, KUCAS 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.