



Avocent[®] AutoView[™] 2108/2216 Switch for Dell[®]

Installer/User Guide

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. Visit <https://www.VertivCo.com/en-us/support/> for additional assistance.

TABLE OF CONTENTS

1 Product Overview	1
1.1 Features and Benefits	1
1.1.1 Reduce cable bulk	1
1.1.2 IQ modules	1
1.1.3 Multiplatform support	1
1.1.4 User interfaces	1
1.1.5 Virtual media and smart card-capable switches	2
1.1.6 IPv4 and IPv6 capabilities	2
1.1.7 Access the AutoView switch for Dell using a standard TCP/IP network	2
1.1.8 Upgradeable	2
1.1.9 Two-tier expansion	3
1.1.10 Remote Access Key (RAK)	3
1.2 Safety Precautions	3
1.3 General	3
1.4 LAN Related Precautions	4
2 Installation	5
2.1 Setting Up Your Network	5
2.1.1 Keyboards	5
2.2 Quick Setup	5
2.3 Connecting the AutoView™ Switch for Dell® Hardware	5
2.4 Tiering Your Switch Using an IQ Module	8
2.4.1 Adding a tiered switch	9
2.4.2 Adding a tiered legacy switch	11
2.5 Configuring Your Switch	13
2.6 Setting Up the Built-in Web Server	13
2.7 Connecting to the OBWI Through a Firewall	13
2.8 Verifying Power Status	14
2.9 Adjusting Mouse Settings on Target Devices	14
3 Local OSCAR™ User Interface	17
3.1 Main Dialog Box Functions	17
3.1.1 Viewing and selecting ports and devices	17
3.1.2 Viewing switch system status	18
3.1.3 Selecting devices	19
3.1.4 Soft switching	20
3.1.5 Navigating the OSCAR interface	20
3.1.6 Connecting local virtual media	21
3.2 Setup Dialog Box Functions	22
3.2.1 Changing the display behavior	22

3.2.2	Controlling the status flag	23
3.2.3	Setting the keyboard country code	24
3.2.4	Assigning device types	24
3.2.5	Assigning device names	24
3.2.6	Configuring network settings	25
3.3	Commands Dialog Box Functions	25
3.3.1	Selecting devices for scan mode	26
3.3.2	Enabling or disabling scan mode	26
3.3.3	Viewing and disconnecting user connections	27
3.3.4	Displaying version information and upgrading firmware	27
4	OBWI Operation	29
4.1	Using the OBWI	30
4.2	Viewing System Information	30
4.3	Generating a Certificate	31
4.4	Tools - Rebooting and Upgrading	32
4.4.1	Rebooting the switch	32
4.4.2	Upgrading switch firmware	32
4.4.3	Saving and restoring configurations and user databases	33
4.5	Property Identity and Location Settings	34
4.6	Viewing Version Information	34
4.7	Network Settings	34
4.8	SNMP Settings	35
4.9	Auditing Event Settings	36
4.10	Setting Event Destinations	36
4.11	Ports Settings - Configuring an IQ Adaptor	36
4.11.1	Deleting IQ adaptors	36
4.11.2	Upgrading IQ adaptors	37
4.12	Launching a Session	37
4.12.1	General sessions settings	37
4.12.2	Local user account settings	38
4.12.3	Virtual media session settings	39
4.13	DSView™ Software Settings	40
4.14	Active Sessions	40
4.15	Closing a Session	40
5	KVM Video Viewer	41
5.1	Virtual Media Sessions	41
5.2	KVM Session	41
5.3	Performance Errors	41
5.4	Java Versions	41
5.5	Opening a KVM Session	42

5.6 Saving the View	42
5.7 Pasting Text	42
5.8 Closing a KVM Video Viewer Session	42
5.9 KVM Video Viewer Profile Settings	42
5.9.1 Refresh	42
5.9.2 Fit	43
5.9.3 Full Screen	43
5.9.4 Mini-Mode	43
5.9.5 Scaling	44
5.9.6 Color Modes	44
5.9.7 Session User List	44
5.9.8 Status Bar	44
5.10 Macros	45
5.10.1 Global Macros	45
5.11 Virtual Media	47
5.11.1 Requirements	47
5.11.2 Creating an image	49
5.12 Session Options	49
5.12.1 General	49
5.12.2 Mouse Synchronization	50
5.12.3 Certificate	50
5.12.4 Automatic Video Adjust	50
5.12.5 Manual Video Adjustment	50
5.12.6 Cursor Commands	52
5.12.7 Stats	52
5.13 Power Control	52
5.14 Smart Cards	52
5.14.1 Video Recording	53
6 Terminal Operation	55
6.1 Network Configuration	55
6.2 Other Console Main Menu Options	56
6.2.1 Firmware Management	56
6.2.2 Enable Debug Messages	56
6.2.3 Set/Change Password	56
6.2.4 Restore Factory Defaults	56
6.2.5 Reset Switch	56
6.2.6 Set Web Interface Ports	56
6.2.7 Exit	56
Appendices	57
Appendix A: MIB SNMP Traps	57

Appendix B: Setup Port Pinouts	60
Appendix C: Using Avocent Serial IQ Modules	62
Appendix D: Sun Advanced Key Emulation	66
Appendix E: UTP Cabling	68
Appendix F: Technical Specifications	70
Appendix G: KVM Session Optimization	74

1 PRODUCT OVERVIEW

The Avocent® AutoView™ 2108/2216 Switch for Dell® 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 Remote Access Key (RAK).

1.1 Features and Benefits

1.1.1 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 IQ module and single, industry-standard Unshielded Twisted Pair (UTP) cabling. This allows a higher device density while providing greater airflow and cooling capacity.

1.1.2 IQ modules

The switch supports IQ modules that are powered directly from the target device and provide Keep Alive functionality when the switch is not powered. The IQ modules with CAT5 design dramatically reduce cable clutter while providing optimal resolution and video settings. The built-in memory of IQ modules simplifies configuration by assigning and retaining unique device names and Electronic ID (EID) numbers for each attached device.

PS/2 and USB IQ modules are available allowing direct KVM connectivity to devices. The USB2+CAC IQ module is also available. The switch is offered with 8 or 16 ARI ports that are used to connect IQ modules to the switch. Then utilizing the IQ modules, you can attach additional switches to expand your switch system. This flexibility allows you to add capacity as your data center grows.

NOTE: A patch panel is not recommended as a connection point between the appliance and an IQ module because it can cause distance, power or video quality control feature issues. If the issues are still present when the patch panel is removed, contact Technical Support.

1.1.3 Multiplatform support

Dell IQ modules are available for use with the switch to support PS/2, USB, USB2 and USB2+CAC device environments.

Interoperability with Avocent® IQ Module Intelligent Cabling can also be used to connect local devices to the switch. PS/2, USB and Sun® module options are available. For more information, please refer to the appropriate Avocent installer/user guide for your product or visit VertivCo.com for more information.

1.1.4 User interfaces

The switch is equipped with two “point-and-click” interfaces to manage the switch locally. They are the local user interface (UI), referred to as the Avocent® OSCAR™ graphical user interface (GUI) 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 require the installation of the Dell RAK.

OSCAR™ interface

The OSCAR™ 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.

The OSCAR 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 Vertiv™ 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 Dell RAK installed, you can also establish remote KVM and virtual media sessions to target devices. For more information, see [Remote Access Key \(RAK\)](#) on page 3.

Terminal console interface

The terminal console interface is accessed through the "10101" setup port. A terminal screen or a PC running terminal emulation software can be used to access these screens.

1.1.5 Virtual media and smart card-capable switches

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 can 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 USB 2.0 or USB+CAC IQ module.

1.1.6 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, OSCAR interface or OBWI.

1.1.7 Access the AutoView switch for Dell using a standard TCP/IP network

The device is accessible for configuration via the standard TCP/IP network. If the optional Dell RAK is installed, you can access all attached systems via Ethernet. See [Remote Access Key \(RAK\)](#) on page 3.

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

NOTE: KVM over IP sessions are supported when the Dell RAK is installed.

1.1.8 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 32.

1.1.9 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 512 servers in one system. See [Tiering Your Switch Using an IQ Module](#) on page 8.

1.1.10 Remote Access Key (RAK)

The optional RAK, installed in the USB port, supports the following features.

KVM remote access

A single KVM remote user is supported using the RAK. With the RAK, 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 can 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 can be launched to a device from a single point of access. For more information, see the Technical Bulletin for the DSView management software plug-in.

Local video scaling

The switch digitizes a video signal with a maximum pixel resolution of up to 1600 x 1200 or 1680 x 1050 (widescreen), depending on the length of the 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.

1.2 Safety Precautions

This document pertains only to the Dell DAV2108/DAV2216 Server Console Switch. You should also refer to the following additional safety instructions:

- Dell Safety Sheet
- Dell RTF Regulatory Tech Bulletin

1.3 General

Use the following safety guidelines to help ensure your own personal safety and to help protect your system and working environment from potential damage:



CAUTION: The power supplies in your system can produce high voltages and energy hazards, which can cause bodily harm. Only trained service technicians are authorized to remove the covers and access any of the components inside the system. This warning applies to the Dell™ Server Console Switch, Dell™ PowerEdge™ server and Dell PowerVault™ storage system.

- Observe and follow service markings.
- Do not service any product except as explained in your system documentation.

- Opening or removing covers that are marked with the triangular symbol with a lightning bolt can expose you to electrical shock.
- Components inside these compartments should be serviced only by a trained service technician.
- This product contains no serviceable components. Do not attempt to open.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
 - The power cable, extension cable or plug is damaged.
 - An object has fallen into the product.
 - The product has been exposed to water.
 - The product has been dropped or damaged.
 - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.

NOTE: To help avoid damaging your system, be sure the voltage selection switch (if provided) on the power supply is set for the voltage that most closely matches the AC power available in your location. Also be sure that your monitor and attached devices are electrically rated to operate.

- Be sure that your monitor and attached devices are electrically rated to operate with the power available in your location.
- Use only power cables provided with this product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adaptor plugs or remove the grounding prong from a cable.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the power strip does not exceed 80 percent of the ampere ratings limit for the power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner or uninterruptible power supply (UPS).
- Position system cables and power cables carefully. Route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

1.4 LAN Related Precautions

- Do not connect or use during a lightning storm. There can be a risk of electrical shock from lightning.
- Never connect or use in a wet environment.

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 can use the terminal software, OSCAR™ interface or the OBWI to manage your switch system. The OBWI manages a single switch and its connections. With the optional Dell RAK, 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.VertivCo.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 32.

2.1 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.

2.1.1 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, can produce unpredictable results.

2.2 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 an IQ module to each target device or tiered switch. Connect each IQ module to the switch with CAT5 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 OSCAR interface or the OBWI.
5. Adjust mouse acceleration on each device to *Slow* or *None*.

2.3 Connecting the AutoView™ Switch for Dell® Hardware

The following figure illustrates an example configuration for the AutoView Switch for Dell.

Figure 2.1 Basic Configuration

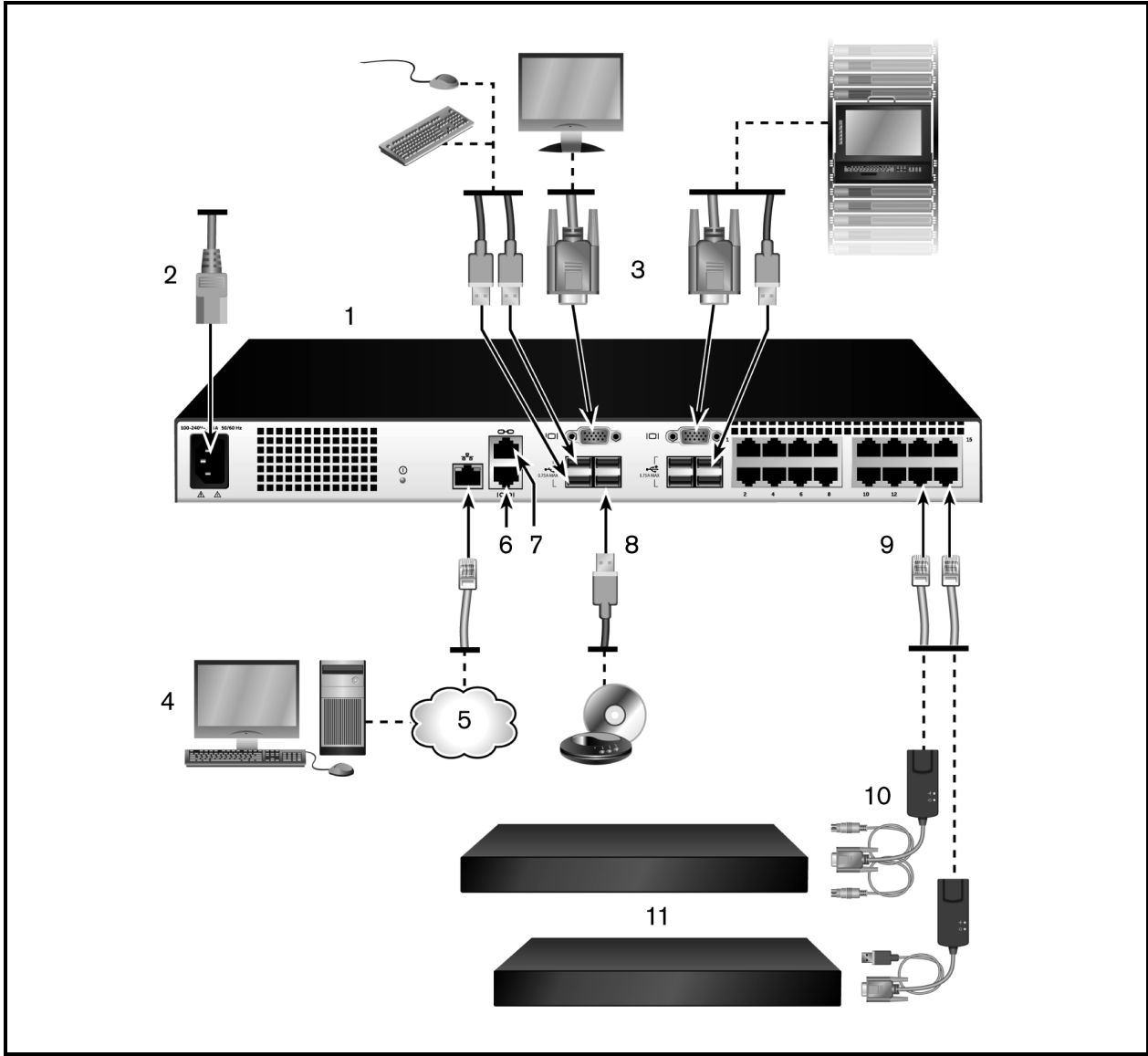


Table 2.1 Basic Configuration Descriptions

ITEM	DESCRIPTION	ITEM	DESCRIPTION
1	AutoView Switch for Dell (16-Port Model Shown)	7	ACI Connection
2	Power Cord	8	External Virtual Media - USB Connections
3	Analog Users (2)	9	Target Device Ports
4	Digital User (requires the RAK)	10	IQ modules
5	LAN/Network	11	Servers/Target Devices
6	10101 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 AC 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.

NOTE: This product has no user-serviceable parts inside the product enclosure. Do not open or remove the 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 RJ45 connector of a IQ module.
3. Connect an IQ module 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 USB2 or USB2+CAC IQ module.

2.4 Tiering Your Switch Using an IQ Module

The following figure illustrates a typical IQ module connection between the switch and a device.

NOTE: A patch panel is not recommended as a connection point between the appliance and an IQ module because it can cause distance, power or video quality control feature issues. If the issues are still present when the patch panel is removed, contact Technical Support.

To connect an IQ module to each device:

NOTE: When tiering devices, the switch closest to the actual user is the primary switch.

1. Locate the IQ modules for your switch.
2. If you are using a PS/2 IQ module connection, attach the color-coded ends of the IQ module cable to the appropriate keyboard, monitor and mouse ports on the first device you is connecting to this switch. If you are using a USB connection, attach the plug from the IQ module to the USB port on the first device you is connecting to this switch.
3. To the RJ45 connector on the IQ module, attach one end of the CAT5 cabling that will run from your IQ module to the switch.
4. Connect the other end of the CAT5 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.

Figure 2.2 IQ Module Connection

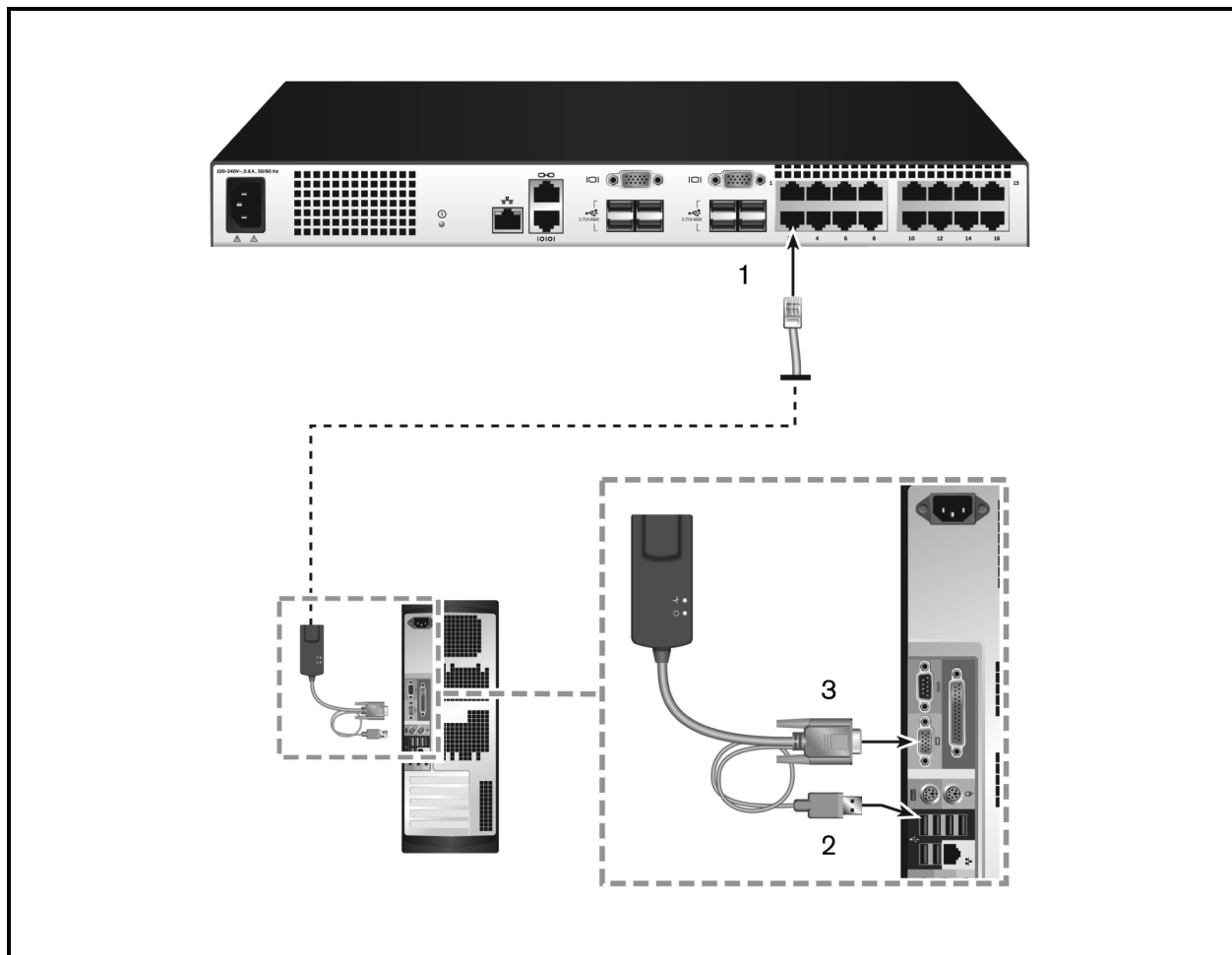


Table 2.2 IQ Module Connection Descriptions

ITEM	DESCRIPTION
1	CAT5
2	USB Connection
3	VGA Connection

2.4.1 Adding a tiered switch

NOTE: The switch does not support the Avocent® OutLook EL80-DT KVM switch.

You can tier up to two levels of switches, enabling users to connect to up to 512 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 an IQ module.

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 2.3 Tying the Switch With a UTP Analog Switch

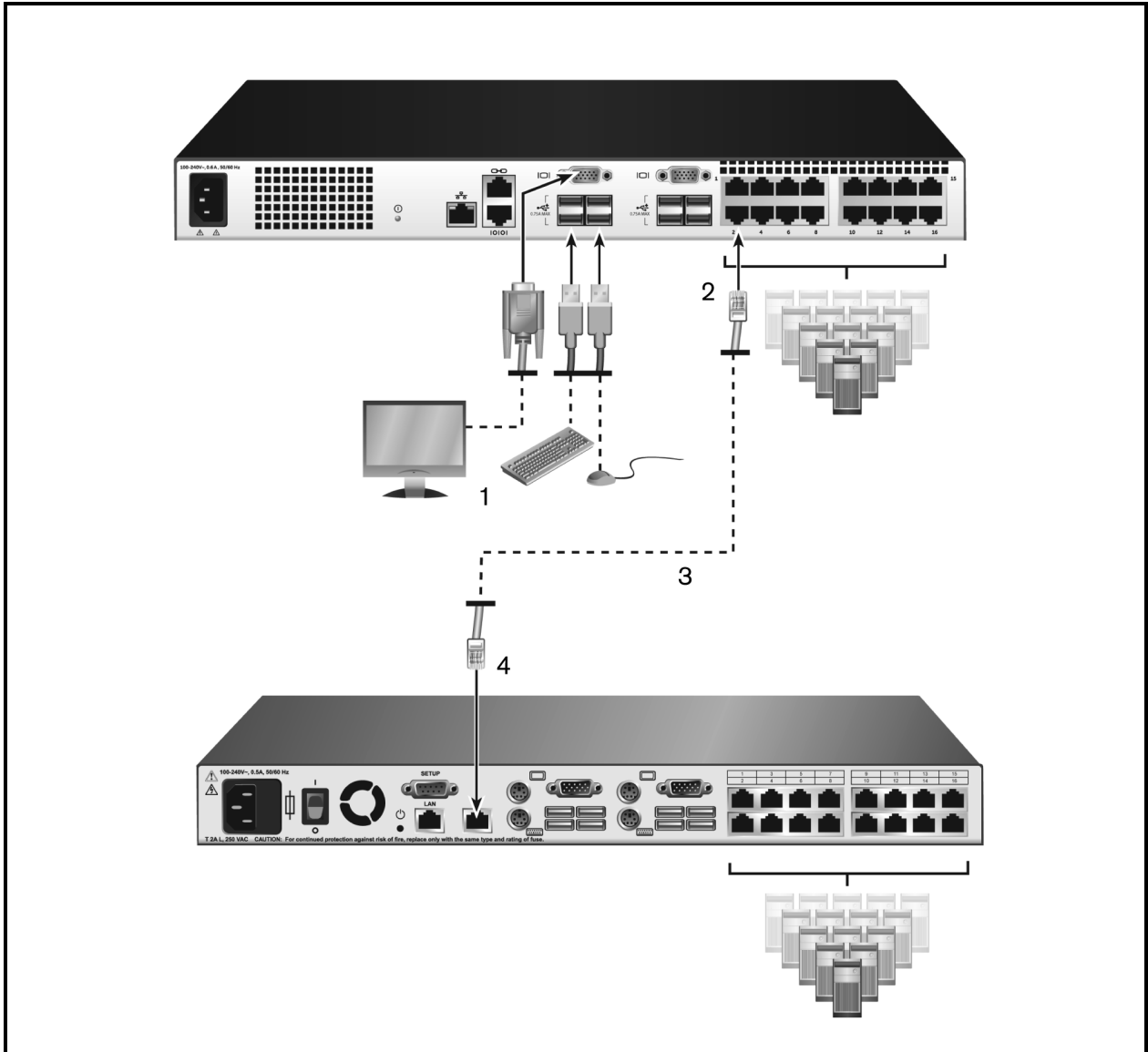


Table 2.3 Tiering the Switch With a UTP Analog Switch Descriptions

ITEM	DESCRIPTION
1	Local User
2	ARI Connection
3	UTP Connection
4	ACI Connection (chain icon)

2.4.2 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 IQ module.
4. Connect the IQ module 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 2.4 Tiers Legacy Switches

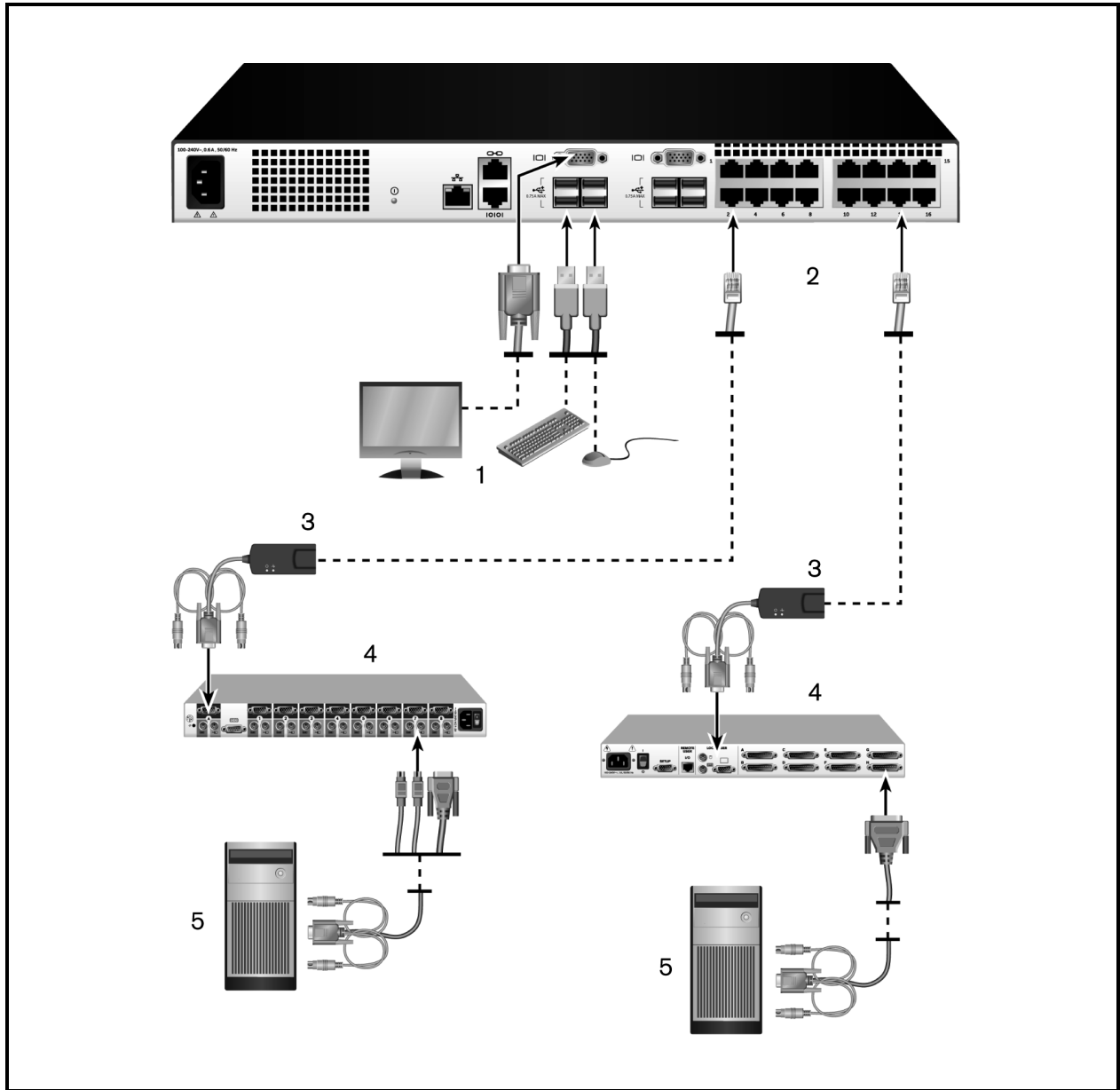


Table 2.4 Descriptions for Tiering Legacy Switches

ITEM	DESCRIPTION
1	Local User
2	ARI Connection
3	IQ module
4	PS2 Connection
5	Target Device Connection

2.5 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 the serial interface, OBWI, OSCAR™ or the DSView™ management software. When configuring the switch using OSCAR, see [Network Settings](#) on page 34. When using DSView management software, the RAK is required. See the applicable Installer/User Guide for detailed instructions.

2.6 Setting Up the Built-in Web Server

Before using the OBWI to access the switch, the IP address must be specified using the 10101 setup port (on the back panel of the switch), or through the local user interface (OSCAR). To use the switch UI, see [Local OSCAR™ User Interface](#) on page 17.

2.7 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 2.5 OBWI Ports With a Firewall

PORT	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 RAK).
TCP/UDP 3211	Discovery (requires the RAK).

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 2.5 Typical Firewall Configuration

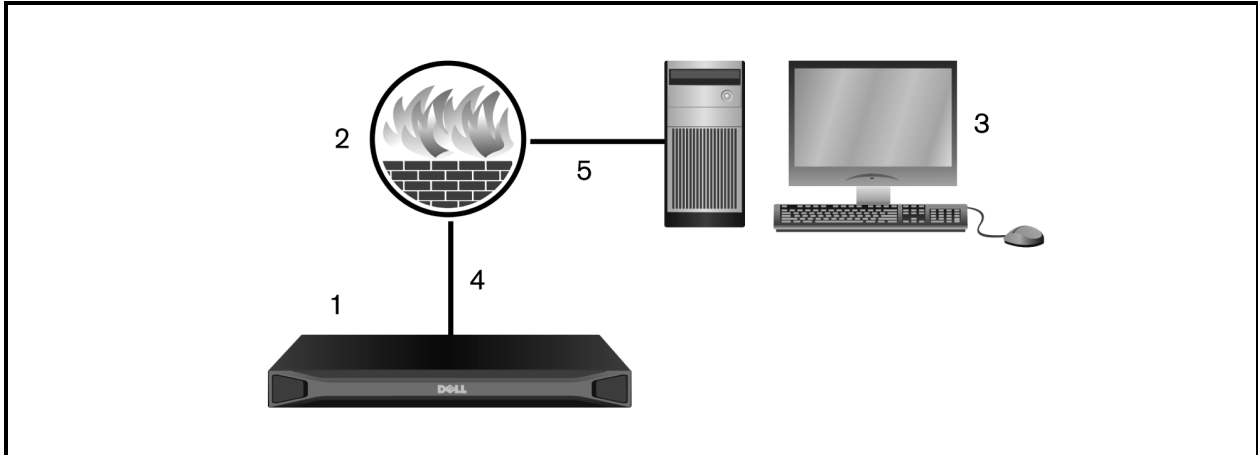


Table 2.6 Descriptions for Firewall Configuration

ITEM	DESCRIPTION
1	Avocent® AutoView™ 2108/2216 Switch for Dell®
2	Firewall
3	User's computer
4	Firewall forwards HTTP requests and KVM traffic to the switch
5	User browses to IP address outside the firewall

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.

2.8 Verifying Power Status

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

2.9 Adjusting Mouse Settings on Target Devices

Before a computer connected to the switch can be used for remote user control, you must set the 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 can 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.

This page intentionally left blank

3 LOCAL OSCAR™ USER INTERFACE

The AutoView™ switch for Dell® 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 OSCAR™ interface to configure your system and devices. You can also use the OSCAR interface to access devices that are attached to the AutoView switch for Dell.

3.1 Main Dialog Box Functions

To access the OSCAR interface Main dialog box:

Press **Print Screen** to launch the OSCAR interface. The Main dialog box appears.

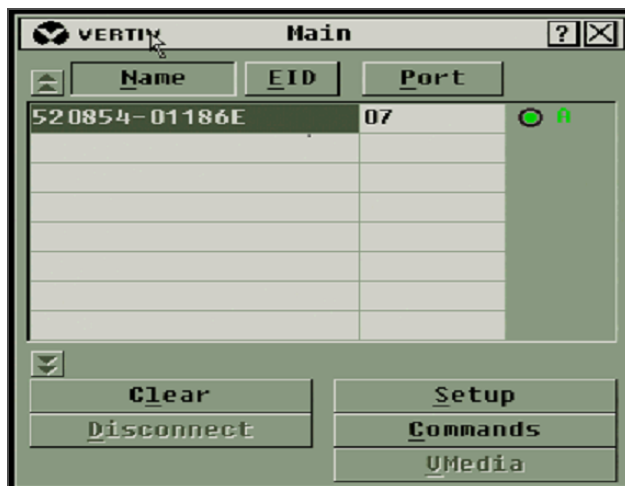
NOTE: If the OSCAR password has been enabled, you is prompted to enter a password before you can launch the OSCAR interface.

3.1.1 Viewing and selecting ports and devices

Use the OSCAR™ *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 IQ module.

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 3.1 OSCAR Interface Main Dialog Box



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









Table 3.1 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 IQ modules
Disconnect	Disconnect the KVM session
Setup	Access the Setup dialog box and configure the OSCAR interface
Commands	Access the Commands dialog box
VMedia	Control virtual media connection

3.1.2 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 3.2 OSCAR Interface 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 can render the module permanently inoperable and require the IQ module to be returned to the factory for repair.
	(green letter) IQ module is being accessed by the indicated user channel.
	(black letter) IQ module is blocked by the indicated user channel.
	(red letter) Smart card support is available.

3.1.3 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.

3.1.4 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 OSCAR™ interface and you press the key sequences before that time has elapsed, the OSCAR interface 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**.

3.1.5 Navigating the OSCAR interface

The following table describes how to navigate the OSCAR interface using the keyboard and mouse.

Table 3.3 OSCAR™ Interface Navigation Basics

KEYSTROKE COMBINATION	FUNCTION
Print Screen, Ctrl+Ctrl, Shift+Shift and/or Alt+Alt	OSCAR interface activation sequence. By default, Print Screen and Ctrl+Ctrl are set as the OSCAR interface activation options. Shift+Shift and Alt+Alt must be set within the OSCAR interface 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 OSCAR interface and displays a status flag if status flags are enabled. See Commands Dialog Box Functions on page 25 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 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 OSCAR interface.
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.

3.1.6 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 OSCAR interface 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 OSCAR interface 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 username and that no other user can connect to that device. If both Locked and Reserved are selected, the session is 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*.

3.2 Setup Dialog Box Functions

You can configure your switch system from the Setup dialog box within the OSCAR™ interface. 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 OSCAR interface menu. The following table lists the functions accessed using each of the buttons in the Setup dialog box.

To access the OSCAR interface Setup dialog box, click *Setup* on the *Main* dialog box.

Table 3.4 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 OSCAR interface displays after pressing Print Screen . You can also change how the OSCAR interface 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.
Network	Choose your network speed, transmission mode and configuration.
Scan	Set up a custom Scan pattern for multiple devices.
VMedia	Set the behavior of the switch during a virtual media session.

3.2.1 Changing the display behavior

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

To access the OSCAR interface *Menu* dialog box, activate the OSCAR 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 is depressed in the *Main* dialog box.

To change how the OSCAR™ interface is invoked:

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

To set a Screen Delay Time for the OSCAR interface:

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

Setting a Screen Delay Time enables you to complete a soft switch without the OSCAR interface. To perform a soft switch, see [Soft switching](#) on page 20.

3.2.2 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 OSCAR interface *Flag* dialog box:

Activate the OSCAR interface 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 is 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.

3.2.3 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 can 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.

3.2.4 Assigning device types

To access the OSCAR™ interface *Devices* dialog box:

Activate the OSCAR 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.

3.2.5 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 is 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 appears in the Names list even when turned off.

To access the OSCAR interface *Names* dialog box, activate the OSCAR interface and click *Setup - Names*.

NOTE: If new IQ modules are discovered by the switch, the on-screen list is automatically updated. The mouse cursor will change into an hourglass during the update. No mouse or keyboard input is 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 can 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.

3.2.6 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 OSCAR™ interface 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.

3.3 Commands Dialog Box Functions

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

Table 3.5 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 IQ modules.
Display Config	View current configuration parameters.
Device Reset	Re-establish operation of keyboard and mouse on the local port.

To access the OSCAR interface Commands dialog box, activate the OSCAR interface and click *Commands* to open the dialog box.

3.3.1 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 OSCAR™ interface 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.

3.3.2 Enabling or disabling scan mode

To start the Scan mode:

1. Activate the OSCAR interface and click *Commands*. The Commands dialog box is displayed.
2. Select *Scan Enable* in the Commands dialog box. Scanning begins.
3. Click *X* to close the Commands dialog box.

To cancel Scan mode:

Select a device if the OSCAR interface is open.

-or-

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

-or-

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

3.3.3 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 is blank.

To view current user connections, activate the OSCAR™ interface 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 appears.
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.

3.3.4 Displaying version information and upgrading firmware

For troubleshooting and support, the OSCAR interface 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 OSCAR interface 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 is 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 appears.
4. Click the *Upgrade* button.

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

To upgrade individual IQ modules:

1. Click the *IQ* button to view individual IQ module 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 IQ module status indicator in the Main dialog box is yellow. The IQ modules are unavailable when an upgrade is in progress. When an upgrade is initiated, any current connection to the device using the IQ module is terminated.

To simultaneously upgrade multiple IQ modules:

1. Activate the OSCAR interface, click *Commands - IQ Status* and click one or more types of IQ modules to upgrade.
2. Click *Upgrade*.

NOTE: When the Enable IQ Auto update option is enabled in the IQ Status dialog box, IQ module firmware is automatically upgraded when the switch firmware is upgraded or when a new IQ module is discovered by the switch after a firmware upgrade. IQ modules that have already been discovered but 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 an IQ module to factory default status:

1. Click *IQ* in the Version dialog box.
2. Select an IQ module, then click *Decommission*.
3. Click *OK* to restore factory defaults. You will see the IQ module 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.

4 OBWI OPERATION

The OBWI for the AutoView™ switch for Dell® is a remote, web browser-based user interface. For details on setting up your system, see [Connecting the AutoView™ Switch for Dell® Hardware](#) on page 5. 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 4.1 Operating Systems Supported by the OBWI

OPERATING SYSTEM	BROWSER		
	MICROSOFT® INTERNET EXPLORER® VERSION 9.0	FIREFOX VERSION 10 AND LATER	GOOGLE CHROME VERSION 19 AND LATER
Microsoft Windows Server® 2003 Standard, Enterprise or Web Edition	Yes	Yes	Yes
Microsoft Windows XP Home Edition or Professional	Yes	Yes	Yes
Microsoft Windows 7 or 8	Yes	Yes	Yes
Microsoft Windows Server® 2012	Yes	Yes	Yes
Microsoft Windows 2008	Yes	Yes	Yes
Red Hat Enterprise Linux® 5 and 6	No	Yes	No
Canonical Ubuntu 12.04	No	Yes	No
Sun Solaris® 10 and 11	No	Yes	No
Novell SUSE Linux Enterprise 10 and 11	No	Yes	No
Apple Mac OS X Tiger 10.4+	No	Yes	No

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 appears.

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 can 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.

4.1 Using the OBWI

After you have been authenticated, the user interface appears. You can 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 4.1 OBWI Window

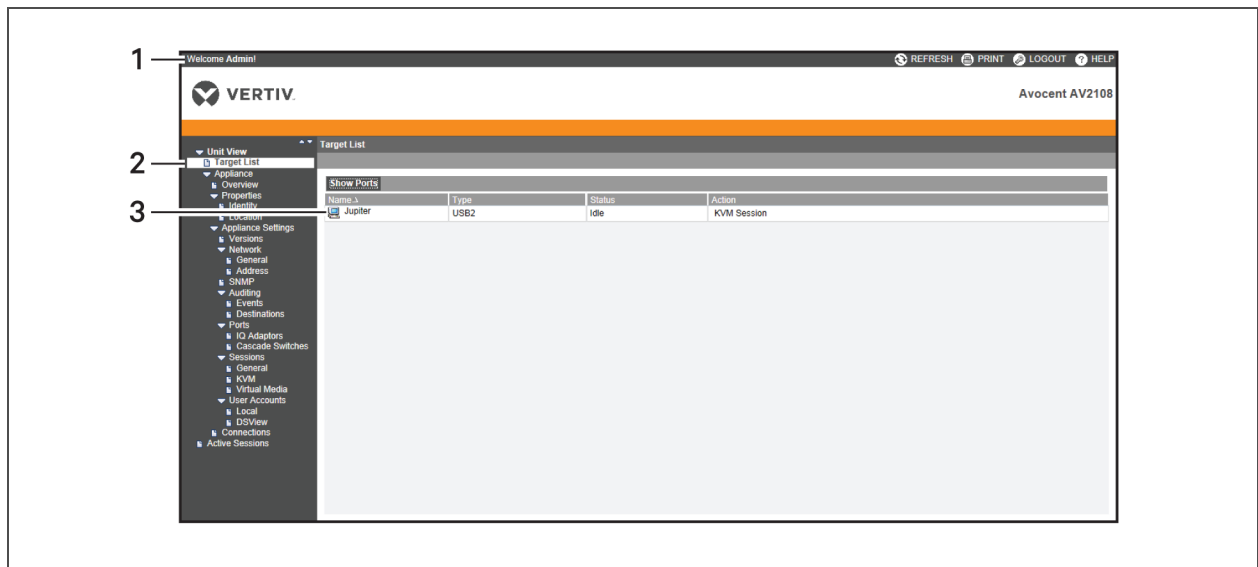


Table 4.2 OBWI Descriptions

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

4.2 Viewing System Information

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

Table 4.3 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.
AutoView Switch for Dell	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 Dell RAK (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 IQ adaptor; name, port, type, channels and status for each tiered switch.
	Unit View - Appliance Settings Sessions	General session timeout and sharing details; KVM encryption levels and keyboard language; virtual media settings, drive mappings, encryption level and IQ adaptor access.
	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.

NOTE: IQ adaptor and IQ module are used interchangeably. IQ module is the term used in the OSCAR™ interface. IQ adaptor is the term used in the OBWI.

4.3 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 can 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.

4.4 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.

4.4.1 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 is disconnected. Click the *OK* button.

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

4.4.2 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 IQ adaptor sessions. A target device experiencing an IQ adaptor firmware update can not display or can display as disconnected. The target device appears normally when the update is completed.



CAUTION: Disconnecting an IQ adaptor during a firmware update or cycling power to the target device will render the module inoperable and require the IQ adaptor 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 username and user password.

5. Click the *Upgrade* button.

4.4.3 Saving and restoring configurations and user databases

You can save the switch configuration to a file. The configuration file will contain information about the managed switch. You can also save the local user database on the switch. After saving either file, you can 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 *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, username, user password and firmware filename you wish to load.

5. Click the *Browse* button. Navigate to the desired location and select the filename. 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 32.

To recover from an Update failure:

If after an update, the switch does not boot into the new firmware version, you can use the following steps to revert to the previous firmware version.

1. Connect a serial cable to the 10101 port on the rear panel of the switch.
2. Run a terminal program on the PC connected to the 10101 port. The serial port settings should be: 9600 baud, 8 data bits, 1 stop bit, no parity and no flow control.
3. Turn on the switch.
4. In the terminal program, when the prompt "Hit any key to stop autoboot" appears, press any key. A menu is displayed.
5. Enter **1** (Boot Alternate) and press **Enter**. The switch will automatically reboot to the previous firmware version.
6. After the switch reboots, attempt the upgrade.

4.5 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 Dell Remote Access Key. The Unit Location Properties screen displays the site, department and location.

NOTE: After changing network settings, the switch must be rebooted.

4.6 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.

4.7 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 *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 is 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 *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 is ignored.

4. Click *Save*.

4.8 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 can 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 can 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 can leave these fields blank to allow any station to manage the switch.
6. Click *Save*.

4.9 Auditing Event Settings

An event is a notification sent by the switch to a management station indicating that something has occurred that can 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 Event Name checkbox to select or deselect the entire list.

3. Click *Save*.

4.10 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*.

4.11 Ports Settings - Configuring an IQ Adaptor

From the switch you can display a list of the attached IQ adaptors, as well as the following information about each IQ adaptor: EID, port, status, application version and interface type. You can click on one of the IQ adaptors 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 IQ adaptor and upgrade the IQ adaptor firmware.

4.11.1 Deleting IQ adaptors

To delete an offline IQ adaptor:

1. From the side navigation bar, click *Ports - IQ adaptors* to open the IQ adaptor screen.
2. Click in the applicable IQ adaptor checkbox.
3. Click *Delete Offline*.

4.11.2 Upgrading IQ adaptors

The IQ adaptors will automatically update when the switch is updated. To update your switch firmware, see [Tools - Rebooting and Upgrading](#) on page 32 or the DSView management software Online Help. If issues occur during the normal upgrade process, IQ adaptors can also be force-upgraded when needed.

NOTE: Check <http://www.VertivCo.com/en-us/support/> for firmware upgrade files.



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

To upgrade the IQ adaptor firmware:

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

To set the USB speed to USB 1.1 or USB 2.0:

NOTE: This section only applies to the USB2 IQ adaptor.

1. From the side navigation bar, click *Ports - IQ adaptors* to open the IQ adaptors screen.
2. Select the checkboxes next to the IQ adaptors that you wish to modify.

4.12 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 appears.
2. The applicable action, KVM Session, is 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 can 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 appears.

NOTE: The Dell RAK 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.

4.12.1 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.

4.12.2 Local user account settings

NOTE: User Account settings are supported when the Dell® RAK is installed.

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

Access levels

NOTE: Multiple access levels are supported when the Dell® RAK is installed.

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

Table 4.4 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 only	No
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.

NOTE: Multiple access levels are supported when the Dell® RAK is installed.

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 appears.
3. Fill out the user information on the screen, then click *Save*.

4.12.3 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 IQ adaptor for which you want to enable virtual media and click *Enable VM*.

-or-

Select the checkbox next to each IQ adaptor 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 4.5 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.

4.13 DSView™ Software Settings

NOTE: User account settings are supported when the Dell® RAK is installed.

You can contact and register an unmanaged switch with a 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 - DSView*. The DSView™ Authentication Servers 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*.

4.14 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.

4.15 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 is disconnected.

To close a session (local users only):

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

5 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 can 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 three-button mouse.

5.1 Virtual Media Sessions

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

5.2 KVM Session

KVM sessions can be launched to devices from any supported KVM switch. Each KVM session is 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.

5.3 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 can affect system performance and is not recommended.

When using a non-proxied connection, video performance over a slower network connection can be less than optimal. Since certain color settings use less network bandwidth than others, changing the color settings can 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.

5.4 Java Versions

The KVM Video Viewer client requires Java when launched from Mozilla® Firefox® browsers. 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 does not have a 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 can not be able to launch the KVM Video Viewer. In this case, you can configure Java to find the JRE. See the product release notes for supported Java versions.

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*.

5.5 Opening a KVM Session

To open a KVM session from the MergePoint Unity® switch:

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.

The KVM Video Viewer launches in a new window.

5.6 Saving the View

The display of a KVM Video Viewer window can 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 filename 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.

5.7 Pasting Text

Text from the client machine can 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.

5.8 Closing a KVM Video Viewer Session

To close a KVM Video Viewer session:

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

5.9 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.

5.9.1 Refresh

The Refresh setting enables background refresh.

To update the Video Viewer window:

Click *View - Refresh*.

5.9.2 Fit

To resize the KVM Video Viewer window for digitized video:

1. Click *View - Fit*.
2. 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 is scaled to fit in the client window. In this case, the client window occupies 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 is maximized to fit on the client workstation window and scroll bars appear to allow access to the target server's image.

5.9.3 Full Screen

To toggle the client between Full Screen mode and Windowed mode:

Click *View - Full Screen*.

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 takes 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 is re-enabled.
- Resume keyboard pass-through and do other tasks currently performed by the Viewer client when in Windowed mode.

5.9.4 Mini-Mode

To toggle the client between Mini-Mode and Windowed mode:

Click *View - Mini-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.

To exit Mini-Mode:

1. Double-click on the Mini-Mode window.

-or-

2. 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*.

5.9.5 Scaling

To change the KVM Video Viewer window resolution:

1. Click *View - Scaling*.
2. Click *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 is 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 is adjusted automatically.

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

To maintain the aspect ratio for video in Windowed or Full Screen mode:

1. Select *Tools - Session Options*.
2. Check the box next to *Windowed or Full Screen Mode* and click *Apply*.

5.9.6 Color Modes

To change the color depth the KVM Video Viewer uses:

Click *View - Color Modes*.

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.

5.9.7 Session User List

To view active users of this session:

Click *View - Session User List*.

5.9.8 Status Bar

To display or hide the status bar at the bottom of the Viewer window:

Click *View - Status Bar*.

5.10 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 can type the desired keystrokes or you can 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 can 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.

5.10.1 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 macro groups and their associated macros as part of the preferences saved on the server. One of the macro groups is used as the default macro group for the DSView software profile. The macros in the default group is 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:

1. Click on a group and then check the Display on Menu box.
2. Select the All radio button at the bottom of the screen to view all the macro groups

-or-

Select the Personal or Global radio button to view 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 Global or Personal radio button 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*.

5.11 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 can also add and map an ISO or floppy image file as a virtual drive on the target device.

You can have one CD drive and one mass storage device mapped concurrently as follows:

- 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.

5.11.1 Requirements

The following lists requirements for using virtual media:

- 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 can 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 *Virtual Media - Activate*.

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 appears 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 want to enable the Read Only checkbox if the session settings enabled read and write access, but you want 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 can 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. When prompted, 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. Click *Details* again to close the Details table.

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 appears. Click *USB Reset*.
3. A warning message appears, indicating the possible effects of the reset. Confirm or cancel the reset.
4. To close the Details box, click *Details* again.

5.11.2 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 *Virtual Media - Create Image* from the KVM Video Viewer menu.
2. 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*.

5.12 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.

5.12.1 General

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

Keystrokes that a user enters can be interpreted in one of the following 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 Pass all keystrokes to target box.
4. Click *OK*.

To enter Single Cursor mode:

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

To exit Single Cursor mode:

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

5.12.2 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 the 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 a USB-2 IQ module, but is not running a Windows® or Macintosh® operating system, the status is Not Available.

7. Click *Apply*.

5.12.3 Certificate

To view the current session's certificate:

Click *Tools - Session Options - Certificate*.

NOTE: You can also set where the certificate is stored on the local machine and empty certificates from that location.

5.12.4 Automatic Video Adjust

To automatically adjust the video:

In the KVM Video Viewer menu, click *Tools - Automatic Video Adjust*.

NOTE: A green screen with yellow lettering can appear during auto-adjustment.

5.12.5 Manual Video Adjustment

Generally, the Video Viewer window automatic adjustment feature optimizes the video for the best possible view. However, you can fine-tune the video with the help of Vertiv™ 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 5.1 Manual Video Adjust Window

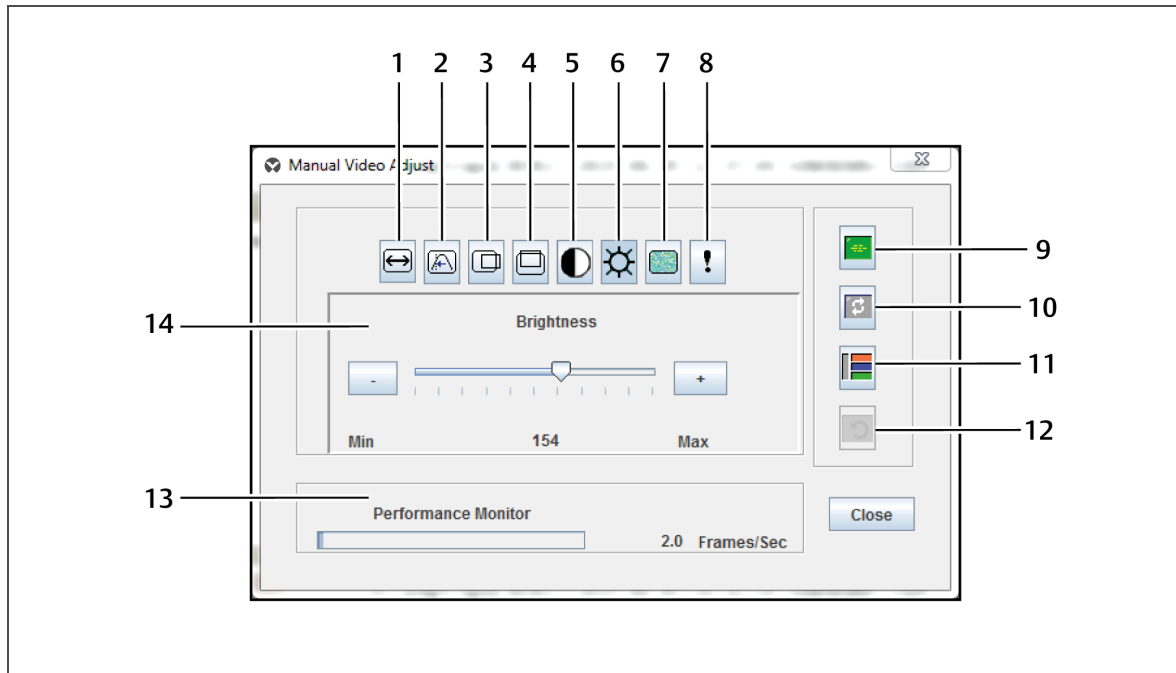


Table 5.1 Manual Video Adjust Window Descriptions

NUMBER	DESCRIPTION	NUMBER	DESCRIPTION
1	Image Capture Width	8	Contrast
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 Vertiv™ 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*.

5.12.6 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 becomes disabled and the device will have to be rebooted.

To prevent potential mouse conflicts, you can 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 Vertiv™ 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.

5.12.7 Stats

To view frame rate, bandwidth, compression, packet rate and virtual media information:

Click *Tools - Stats*.

5.13 Power Control

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

To manage power:

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

5.14 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 is 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 can also be displayed showing whether the smart card is mapped, not mapped or disabled.

5.14.1 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 deleted.

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 5.2 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 <i>Pause</i> button will pause the Live playback. Live mode will change to Continuous and the Play button is disabled.
	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 is again. 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 is 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 Video 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*.

6 TERMINAL OPERATION

Each switch can be configured at the switch level through the Terminal Console menu interface, which is accessed through the 10101 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 DB9 M/F serial adaptor, connect a terminal or a PC that is running terminal emulation software, such as HyperTerminal software, to the 10101 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.*

6.1 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 can 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 can 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 cannot 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.

6.2 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.

6.2.1 Firmware Management

This menu contains the Flash Download selection. For more information, see [Tools - Rebooting and Upgrading](#) on page 32.

6.2.2 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.

6.2.3 Set/Change Password

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

6.2.4 Restore Factory Defaults

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

6.2.5 Reset Switch

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

6.2.6 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.

6.2.7 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 is prompted with the Password login screen.

APPENDICES

Appendix A: MIB SNMP Traps

The switch has the ability to send audit events to an SNMP Manager. The SNMP traps are defined in an SNMP Trap MIB.

The Trap MIB file can be uploaded from the switch using the Save Trap MIB function. The uploaded Trap MIB file can then be loaded into an SNMP Trap Receiver application.

This appendix describes the trap events that can be generated by the switch. Although care has been taken to keep the information in this appendix up to date, the actual Trap MIB file will contain the most accurate trap information.

An SNMP manager can access MIB-II objects of the switch using the IPv4 or IPv6 protocols.

By design, the enterprise specific MIB objects within the switch cannot be accessed using SNMP.

The switch trap definitions use the structure described in the following Request For Comments (RFCs):

- RFC-1155-SMI
Describes the common structures and identification scheme for the definition of management information for use with TCP/IP-based Internet.
- RFC-1212
Describes the format for producing concise and descriptive MIB modules.
- RFC-1213-MIB
Describes the Internet standard MIB-II for use with network management protocols in TCP/IP-based inter-networks.
- RFC-1215
Describes the SNMP standardized traps and provides a means for defining enterprise-specific traps. The specific objects reported by each trap are defined in the Trap MIB file which is uploaded from the switch. The following table is a list of the generated trap events.

Table A.1 Generated Trap Events

TRAP EVENT	TRAP NUMBER
User Authentication Failure	1
User Login	2
User Logout	3
Target Session Started	4
Target Session Stopped	5
Target Session Terminated	6
Traps 7-8 are Unused	7-8
User Added	9
User Deleted	10
User Modified	11
Reboot Started	12
Image File Upgrade Started	13
Image File Upgrade Results	14
IQ module Added	15
IQ module Removed	16
Target Device Name Changed	17
Tiered Switch Added	18
Tiered Switch Removed	19
Tiered Switch Name Changed	20
Configuration File Loaded	21
User Database File Loaded	22
Traps 23-32 are Unused	23-32
User Locked	33
User Unlocked	34
IQ module Upgrade Started	35
IQ module Image Upgrade Result	36
IQ module Restarted	37
Virtual Media Session Started	38
Virtual Media Session Stopped	39
Virtual Media Session Terminated	40
Virtual Media Session Reserved	41
Virtual Media Session Unreserved	42
Virtual Media Session Mapped	43

Table A.1 Generated Trap Events (continued)

TRAP EVENT	TRAP NUMBER
Virtual Media Drive Unmapped	44
Traps 45-75 are Unused	45-75
Smart Card Inserted	76
Smart Card Removed	77
Traps 78-79 are Unused	78-79
Aggregated Target Device Status Changed	80

Appendix B: Setup Port Pinouts

The switch 10101 setup port is an 8-pin modular jack. The setup port pinouts and descriptions are provided in the following figure and table.

Setup Port Pinouts

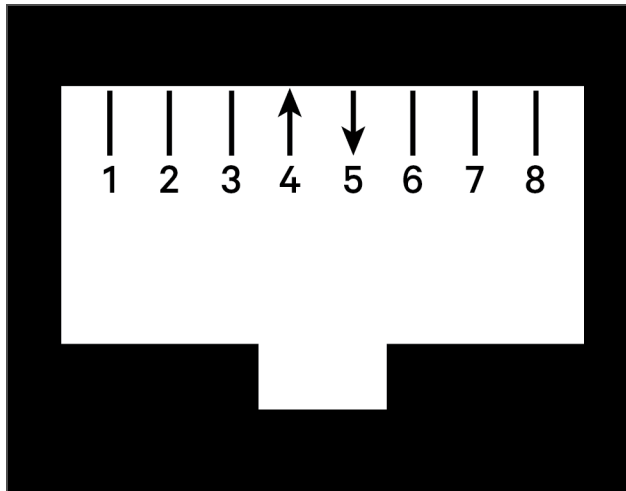


Table B.1 Console/Setup Port Pinout Descriptions

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

This page intentionally left blank

Appendix C: Using Avocent Serial IQ Modules

The serial IQ module 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.

C.1 Serial IQ module modes

The following modes can be accessed from the serial IQ module:

- 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.

C.2 Configuring the serial IQ module

NOTE: The serial IQ module is a DCE device and only supports VT100 terminal emulation.

Pressing **Ctrl-F8** activates the Configuration screen of the IQ module's Terminal Applications menu, which enables you to configure your serial IQ module.

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, 19200, 34800, 57600 or 115200 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 115200, 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 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 IQ module:

1. Press **Ctrl-F8**. The Configuration Screen appears.
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.

C.3 Creating a serial IQ 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 IQ module 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 IQ module 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 can 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.

C.4 Using History Mode

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

The serial IQ module 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 appears.
 - **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 appears. 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.

C.5 Serial IQ module pinouts

The following table lists the pinouts for the serial IQ module.

Table C.1 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 D: 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 Dell® USB, USB2 and USB2+CAC IQ modules and Avocent® USB, USB2 and VMC IQ modules. 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 D.1 Sun Key Emulation

ACTION	KEYBOARD SEQUENCE
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.	

This page intentionally left blank

Appendix E: 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.

E.1 UTP Copper Cabling

The following are basic definitions for the three types of UTP cabling that the switch supports:

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

E.2 Wiring Standards

There are two supported wiring standards for 8-conductor (4-pair) RJ45 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 E.1 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
7	white/brown	white/brown
8	brown	brown

E.3 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 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 location. Leave at least five feet at the work outlet side and 15 feet at the patch panel side.
- Choose the 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 F: Technical Specifications

Table F.1 AutoView™ Switch for Dell® Technical Specifications

TYPE	DESCRIPTION
Number of Ports	DAV2108: 8 AHI/ARI DAV2216: 16 AHI/ARI
Type	Dell PS/2, USB, USB2 and USB2+CAC IQ modules Avocent PS/2, PS2M, USB, Sun, USB2 and VMC modules
Connectors	8-pin modular (RJ45)
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
Target Resolutions	Standard 1024 x 768 @ 60 Hz (preferred) 1280 x 1024 @ 60 Hz (preferred) 1600 x 1200 @ 60 Hz (preferred) Widescreen 1280 x 800 @ 60 Hz (preferred) 1680 x 1050 @ 60 Hz (preferred)
Supported Cabling	4-pair UTP, 30 meters maximum length
Dimensions	
Form Factor	1U or 0U rack mount
Dimensions	17.00 x 9.42 x 1.70 inches (Width x Depth x Height) (43.18 x 23.93 x 4.32 cm)
Weight (without cables)	DAV2108: 5.98 lb (2.71 kg); DAV2216: 6.16 lb (2.79 kg)
10101 Setup Port	
Number	1
Protocol	RS232 serial
Connector	8-pin modular (RJ45)
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

Table F.1 AutoView™ Switch for Dell® Technical Specifications (continued)

TYPE	DESCRIPTION
Connector	8-pin modular (RJ45)
USB Port	
Number	4
Protocol	USB 2.0
Power Specifications	
Connectors	DAV2108: 1 IEC C14 DAV22 16: 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	0.6 A
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

This page intentionally left blank

Appendix G: KVM Session Optimization

To improve session performance:

In the KVM Video Viewer, click *Tools - Automatic Video Adjustment* to calibrate the A/D converter to the video signal coming from the server video card.

To identify a KVM session that is slow due to unclean video signals:

Click *Tools - Manual Video Adjustment*.

A clean video signal will create 0 pkt/sec on the performance monitor when there is not any activity on the target server.

NOTE: Adjusting the screen resolution and screen refresh rate can have a significant effect on the cleanliness of the video signal and the speed of the resulting KVM session. For best results, try different combinations of these two settings followed by an auto video adjustment to improve the session speed.

The amount of video input plays a big role in the speed of KVM sessions. Lower screen resolutions is faster than higher screen resolutions. Decreasing the color depth and the screen scaling will also decrease the amount of KVM session data being transported and will increase session speed.

If the above optimization options are ineffective at improving session speeds, the Video Noise Control setting can be enabled, which will increase session speed by ignoring small video changes. Other settings can also be configured for KVM targets globally or individually to improve performance.

NOTE: While this setting can increase speed, it can also cause an increase in video "blocks".

The following are possible target and network metrics; however, every environment is different.

Example appliance KVM sessions in a 100 mbps LAN environment:

The following metrics represent the KVM window resolution 1280x1024 @70 Hz on a Windows server:

- Zero screen movement = 0 pkts/sec (avg. 0.7 kbps download | 0.5 kbps upload)
- Continuous mouse circles movement on screen = 35 pkts/sec (avg. 216 kbps download | 247 kbps upload)
- Rapidly opening and closing full-screen windows = 35-100 pkts/sec (~ 2.9 mbps download | 257 kbps upload)

The following metrics represent the KVM window resolution 1024x768 @70 Hz on a Windows server:

- Zero screen movement = 0 pkts/sec (avg. 0.9 kbps download | 0.4 kbps upload)
- Continuous mouse circles movement on screen = 30 pkts/sec (avg. 212 kbps download | 246 kbps upload)
- Rapidly opening and closing full-screen windows = 30-70 pkts/sec (avg. 2.5 mbps download | 230 kbps upload)

The following metrics represent the KVM window resolution 1024x768 @60 Hz on a Ubuntu desktop:

- Zero screen movement = 0 pkts/sec (avg. 1.3 kbps download | 1.0 kbps upload)
- Continuous mouse circles movement on screen = 30 pkts/sec (avg. 470 kbps download | 245 kbps upload)

- Rapidly opening and closing full-screen windows = 40-50 pkts/sec (avg. 750 kbps download | 180 kbps upload)





VertivCo.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

© 2018 Vertiv Co. All rights reserved. Vertiv and the Vertiv logo are trademarks or registered trademarks of Vertiv Co. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness herein, Vertiv Co. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications are subject to change without notice.

590-1687-501B