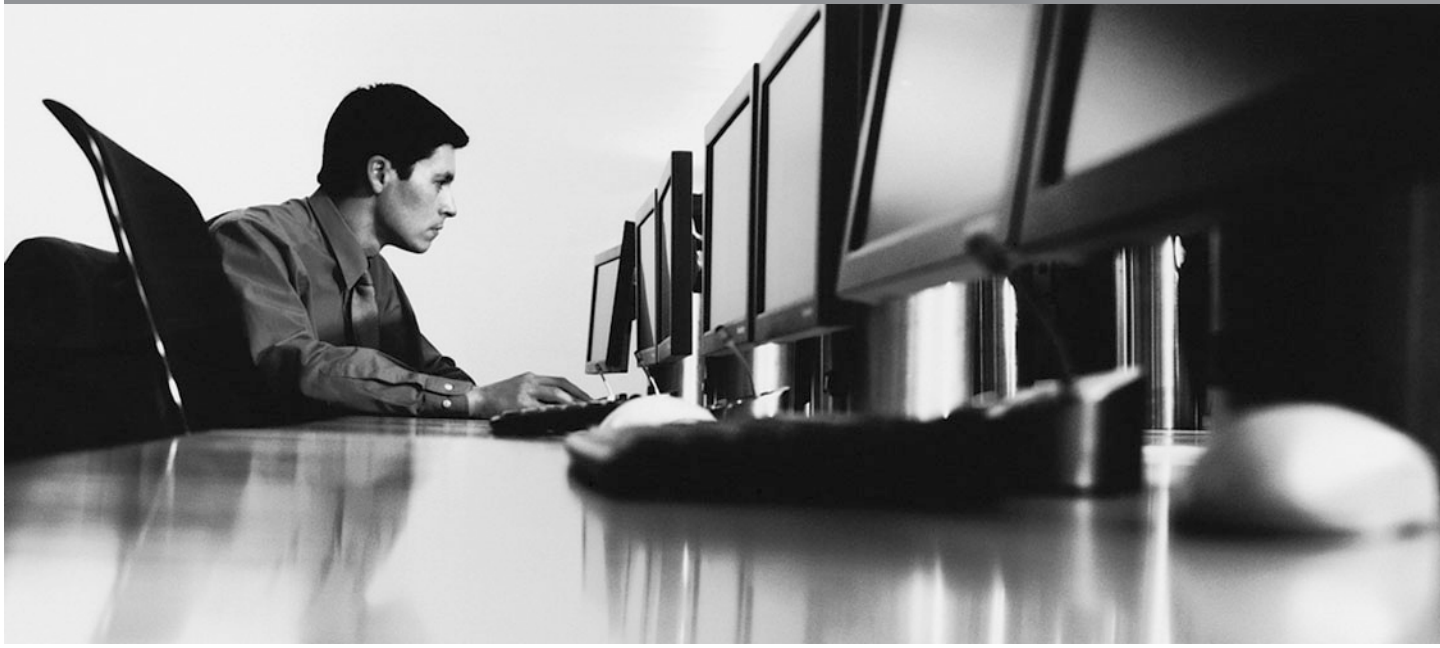




MERGEPOINT UNITY™ SWITCH

Installer/User Guide



European Union Notification

WARNING: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

USA Notification

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his/her own expense.

Canadian Notification

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

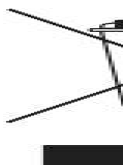
Japanese Notification

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Korean Notification

기종별	사용자 안내문
A급 기기 (업무용 정보통신기기)	이 기기는 업무용으로 전자파 적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 구매 구입 하였을 때에는 가정용으로 교환하시기 바랍니다.





MergePoint Unity™ Switch

Installer/User Guide

Avocent, the Avocent logo, The Power of Being There, MergePoint Unity, DSView and Dambrackas Video Compression are trademarks or registered trademarks of Avocent Corporation or its affiliates in the U.S. and other countries. All other marks are the property of their respective owners.

© 2011 Avocent Corporation. 590-883-501D

**Instructions**

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

**Dangerous Voltage**

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

**Power On**

This symbol indicates the principal on/off switch is in the on position.

**Power Off**

This symbol indicates the principal on/off switch is in the off position.

**Protective Grounding Terminal**

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

TABLE OF CONTENTS

Product Overview.....	1
<i>Features and Benefits.....</i>	<i>1</i>
<i>Reduce cable bulk.....</i>	<i>2</i>
<i>KVM switching capabilities.....</i>	<i>2</i>
<i>True serial capabilities.....</i>	<i>2</i>
<i>Local and remote user interfaces.....</i>	<i>2</i>
<i>Control of virtual media and smart card-capable appliances.....</i>	<i>2</i>
<i>Access the MergePoint Unity switch via a standard TCP/IP network.....</i>	<i>3</i>
<i>FIPS cryptographic module.....</i>	<i>3</i>
<i>DSView™ 3 management software plug-in.....</i>	<i>4</i>
<i>Sample Configuration.....</i>	<i>4</i>
Installation.....	7
<i>MergePoint Unity Switch Connectivity.....</i>	<i>7</i>
<i>Getting started.....</i>	<i>9</i>
<i>Setting up your network.....</i>	<i>10</i>
<i>Rack Mounting a MergePoint Unity Switch.....</i>	<i>10</i>
<i>Rack mounting safety considerations.....</i>	<i>10</i>
<i>Connecting the MergePoint Unity Switch Hardware.....</i>	<i>11</i>
<i>Cascading MergePoint Unity Switches.....</i>	<i>13</i>
<i>Configuring the MergePoint Unity Switch.....</i>	<i>14</i>
<i>Setting up the built-in web server.....</i>	<i>14</i>
<i>Connecting to the OBWI through a firewall.....</i>	<i>14</i>
<i>Verifying the Connections.....</i>	<i>16</i>
<i>Front and rear panel Ethernet connection LEDs.....</i>	<i>16</i>
<i>Front panel status LEDs.....</i>	<i>16</i>
<i>Rear panel power status LEDs.....</i>	<i>16</i>
<i>IQ and DSRIQ-SRL modules.....</i>	<i>17</i>
<i>Adjusting Mouse Settings on Target Devices.....</i>	<i>17</i>
Local and Remote Configuration.....	19
<i>The User Interfaces.....</i>	<i>19</i>

<i>Local UI</i>	19
<i>OBWL</i>	20
<i>Using the user interfaces</i>	21
<i>Viewing System Information</i>	24
<i>MergePoint Unity Switch Sessions</i>	25
<i>Launching a session</i>	25
<i>Configuring sessions</i>	25
<i>Closing a session</i>	26
<i>MergePoint Unity Switch Appliance Tools</i>	26
<i>Rebooting the MergePoint Unity switch</i>	27
<i>Upgrading the MergePoint Unity switch firmware</i>	27
<i>Saving and restoring appliance configurations and appliance user databases</i>	28
<i>Network Settings</i>	29
<i>DNS Settings</i>	30
<i>Local UI Settings</i>	30
<i>Local port user settings</i>	30
<i>Virtual Media</i>	31
<i>Local virtual media settings</i>	32
<i>Modem Settings</i>	33
<i>Scan Mode</i>	33
<i>DSView 3 Server IP Addresses</i>	34
<i>User Accounts</i>	34
<i>Managing local accounts</i>	34
<i>Access levels</i>	34
<i>SNMP Settings</i>	35
<i>Event Settings</i>	36
<i>Setting Event Destinations</i>	37
<i>Configuring IQ Modules</i>	37
<i>Upgrading IQ modules</i>	37
<i>Power Device Settings</i>	38

The Video Viewer.....	41
<i>The Video Viewer Window.....</i>	<i>41</i>
<i>Changing the toolbar.....</i>	<i>43</i>
<i>Launching a Session.....</i>	<i>44</i>
<i>Session time-out.....</i>	<i>44</i>
<i>Window Size.....</i>	<i>44</i>
<i>Adjusting the View.....</i>	<i>45</i>
<i>Refreshing the Image.....</i>	<i>46</i>
<i>Video Settings.....</i>	<i>46</i>
<i>Additional video adjustment.....</i>	<i>46</i>
<i>Target video settings.....</i>	<i>48</i>
<i>Automatic video adjustment.....</i>	<i>48</i>
<i>Video Test Pattern.....</i>	<i>48</i>
<i>Vendor-specific video settings.....</i>	<i>48</i>
<i>Color Settings.....</i>	<i>49</i>
<i>Adjusting Color Depth.....</i>	<i>49</i>
<i>Contrast and brightness.....</i>	<i>49</i>
<i>Noise Settings.....</i>	<i>49</i>
<i>Detection thresholds.....</i>	<i>49</i>
<i>Block Noise Threshold and Pixel Noise Threshold.....</i>	<i>49</i>
<i>Mouse Settings.....</i>	<i>50</i>
<i>Adjusting mouse options.....</i>	<i>50</i>
<i>Cursor type.....</i>	<i>50</i>
<i>Mouse scaling.....</i>	<i>52</i>
<i>Mouse alignment and synchronization.....</i>	<i>53</i>
<i>Avocent Mouse Sync.....</i>	<i>53</i>
<i>Virtual Media.....</i>	<i>54</i>
<i>Requirements.....</i>	<i>54</i>
<i>Sharing and preemption considerations.....</i>	<i>54</i>
<i>Virtual Media dialog box.....</i>	<i>55</i>

<i>Opening a virtual media session.....</i>	55
<i>Closing a virtual media session.....</i>	58
<i>Smart Cards.....</i>	58
<i>Keyboard Pass-through.....</i>	59
<i>Macros.....</i>	60
<i>Saving the View.....</i>	60
<i>Closing a Session.....</i>	60
LDAP.....	61
<i>Configuring LDAP in the User Interface.....</i>	61
<i>LDAP Overview parameters.....</i>	61
<i>LDAP Search parameters.....</i>	62
<i>LDAP Query parameters.....</i>	63
<i>Appliance and Target Device Query Modes.....</i>	64
<i>Setting up Active Directory for Performing Queries.....</i>	67
Appendix A: Terminal Operations.....	69
Appendix B: Using Serial IQ Modules.....	71
Appendix C: UTP Cabling.....	77
Appendix D: Cable Pinout Information.....	80
Appendix E: Technical Specifications.....	82
Appendix F: Sun Advanced Key Emulation.....	86
Appendix G: Technical Support.....	89

Product Overview

Features and Benefits

The Avocent MergePoint Unity™ KVM over IP and serial console switch combines analog and digital technology to provide flexible, centralized control of data center servers and virtual media, and to facilitate the OA&M (operations, activation and maintenance) of remote branch offices where trained operators may be unavailable. The IP-based MergePoint Unity switch gives you flexible target device management control and secure remote access from anywhere at anytime.

The MergePoint Unity switch provides enterprise customers with the following features and options:

- significant reduction of cable volume
- keyboard, video and mouse (KVM) capabilities, configurable for analog (local) or digital (remote) connectivity
- true serial capability through Secure Shell (SSH) and Telnet
- enhanced video resolution support, up to 1600 x 1200 or 1680 x 1050 (wide-screen) native from target to remote
- optional dual power models for redundancy
- optional support for managing intelligent power devices
- virtual media capability accessed through USB ports
- dual independent local port video paths (dedicated to ACI)
- dual stack IPv4 (DHCP) and IPv6 (DHCPv6 and auto configuration) for simultaneous access
- smart card capability
- accessibility to target devices across 10/100 or 1000BaseT (some models) LAN port(s)

- supports V.34, V.90 or V.92-compatible modems that may be used to access the switch when an Ethernet connection is not available
- supports embedded Federal Information Processing Standards (FIPS) cryptographic module

Reduce cable bulk

With server densities continually increasing, cable bulk remains a major concern for network administrators. The MergePoint Unity switches significantly reduce 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 server density while providing greater airflow and cooling capacity.

KVM switching capabilities

The MergePoint Unity switch supports IQ modules, which are powered directly from the target device and provides Keep Alive functionality when the switch is not powered. The following IQ modules are supported: DSRIQ-PS2, DSRIQ-USB, DSRIQ-VMC, DSRIQ-SUN, DSAVIQ-USB2, DSAVIQ-PS2M and MPUIQ-VMC modules. The DSAVIQ-USB2, DSAVIQ-PS2M, DSRIQ-VMC and MPUIQ-VMC modules are virtual media-capable. The DSRIQ-VMC and MPUIQ-VMC modules are also smart card-capable.

True serial capabilities

The MergePoint Unity switch supports the MPUIQ-SRL module, which provides true serial capabilities through Telnet. You can launch an SSH session or launch a serial viewer from the on-board web interface (OBWI) to connect the MergePoint Unity switch's attached target devices that have an MPUIQ-SRL module.

Local and remote user interfaces

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

Control of virtual media and smart card-capable appliances

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

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

Virtual media and smart card readers can be connected directly to the switch using USB ports located on the switch. In addition, virtual media and smart card readers may be connected to any remote workstation that is running the remote OBWI or DSView™ 3 management software and is connected to the MergePoint Unity switch using an Ethernet connection.

NOTE: To open a virtual media session with a target device, you must first connect the target device to a switch using a virtual media capable DSAVIQ-USB2, DSRIQ-PS/2M DSRIQ-VMC or MPUIQ-VMC module. For a smart card, you must first connect the target device to a switch using a smart card-capable DSRIQ-VMC or MPUIQ-VMC module.

Access the MergePoint Unity switch via a standard TCP/IP network

The MergePoint Unity switches provide agentless remote control and access. No special software or drivers are required on the attached servers or client.

NOTE: The client connects to the server hosting the DSView 3 management software using an Internet browser.

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

FIPS cryptographic module

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

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

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

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

The MergePoint Unity switch uses an embedded FIPS 140-2 validated cryptographic module (Certificate #1051) running on a Linux PPC platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.

DSView™ 3 management software plug-in

The DSView 3 software may be used with the MergePoint Unity switch to allow IT administrators to remotely access, monitor and control target devices on multiple platforms through a single, web-based user interface. For more information, see the DSView 3 Software Plug-In for MergePoint Unity Switches Technical Bulletin.

Sample Configuration

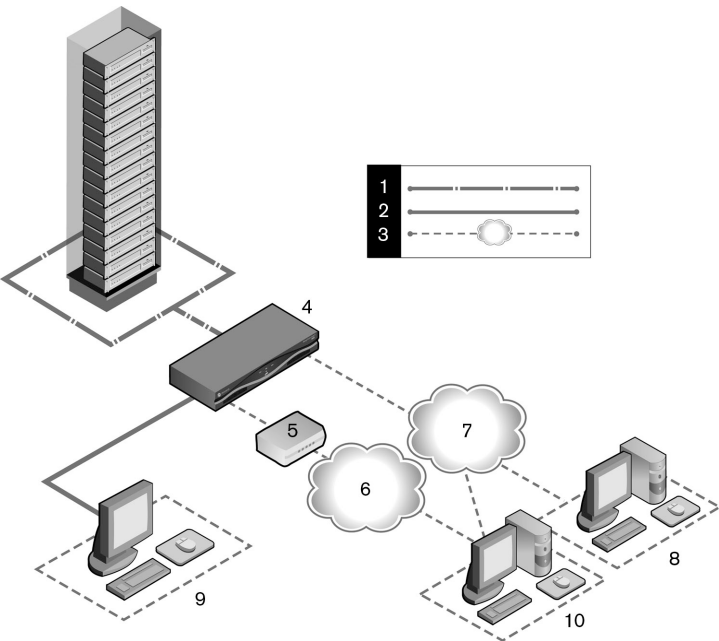


Figure 1.1: Example MergePoint Unity Switch Configuration

Table 1.1: Descriptions for Figure 1.1

Number	Description	Number	Description
1	CAT 5 Connection	6	Telephone Network
2	KVM Connection to the Switch	7	Ethernet
3	Remote IP Connection	8	DSView 3 Server
4	MergePoint Unity Switch	9	Analog User (local UI)

Number	Description	Number	Description
5	Modem	10	Digital User (computer with Internet browser, remote OBWI)

MergePoint Unity Switch Connectivity

A MergePoint Unity switching system transmits KVM and serial information between operators and target devices attached to the switch over a network using either an Ethernet or modem connection.

The MergePoint Unity switch uses TCP/IP for communication over Ethernet. Although 10BaseT Ethernet may be used, Avocent recommends a dedicated, switched 100BaseT or 1000BaseT network for switches that support it.

The MergePoint Unity switch uses the Point-to-Point Protocol (PPP) for communication over a V.34, V.90 or V.92 modem. You can perform KVM and serial switching tasks by using the OBWI or the DSView 3 software. For more information on the DSView 3 software, visit www.avocent.com or see the DSView 3 Installer/User Guide.

Figure 2.1 illustrates a basic configuration for the MergePoint Unity switch, using the MergePoint Unity 8032 switch model for the example. Descriptions follow in Table 2.1.

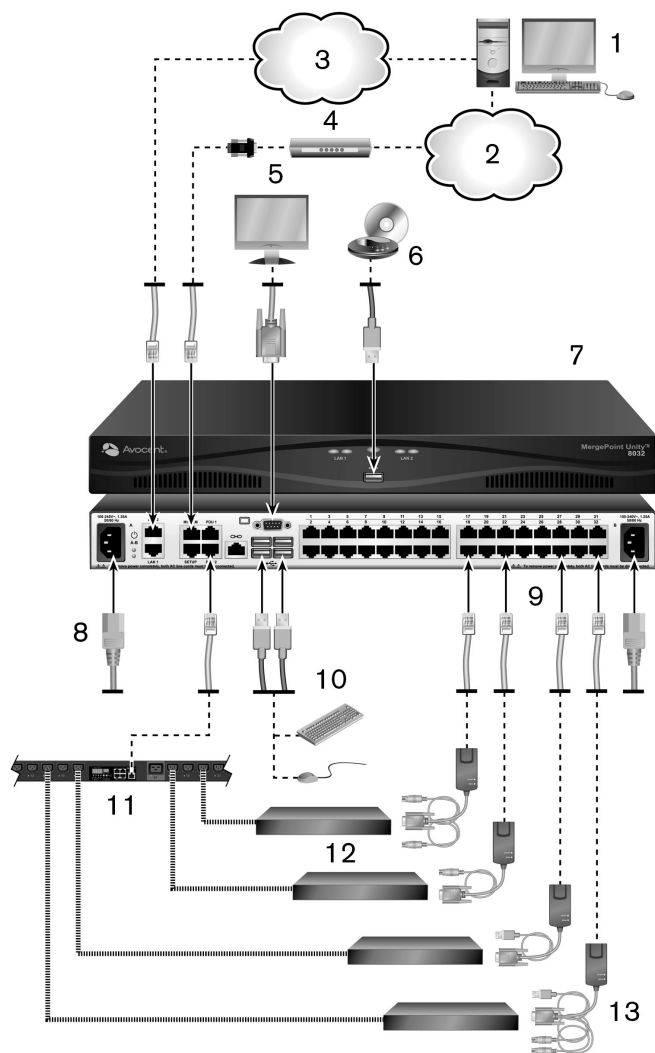


Figure 2.1: Basic MergePoint Unity Switch Configuration (MergePoint Unity 8032 Switch Shown)

Table 2.1: Descriptions for Figure 2.1

Number	Description	Number	Description
1	Digital User	8	Power Cord
2	Telephone Network	9	Ports 1-32

Number	Description	Number	Description
3	Network	10	Local USB Connections
4	Modem	11	Power Control Device
5	Analog User	12	Target Devices 1-32
6	External Virtual Media	13	IQ Modules (PS/2, USB, VMC, Sun and serial are available)
7	MergePoint Unity 8035 Switch		

Getting started

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

Supplied with the MergePoint Unity switch

- Rack mount bracket kit
- Rack Mounting Bracket Quick Installation Guide
- MergePoint Unity Switch Quick Installation Guide
- Safety and Regulatory Statements Guide
- Cables and adaptors for the MODEM and SETUP ports
- AC power cord(s)

Additional items needed

- One IQ module per target device
- One DSRIQ-SRL or MPUIQ-SRL module per serial device
- One UTP patch cable per IQ module (4-pair UTP, up to 45 meters)
- UTP patch cable(s) for network connectivity (4-pair UTP, up to 45 meters)
- One DSAVIQ-USB2, DSAVIQ-PS2M DSRIQ-VMC or MPUIQ-VMC module per target device for virtual media sessions
- One DSRIQ-VMC or MPUIQ-VMC module per target device for smart card control
- (Optional) DSView 3 software
- (Optional) V.34, V.90 or V.92-compatible modem and cables

- (Optional) Power control device(s)

Setting up your network

The MergePoint Unity switching system uses IP addresses to uniquely identify the switch and the target devices. The MergePoint Unity switch family supports both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. Avocent recommends that IP addresses be reserved for each switch and that they remain static while the switches are connected to the network.

For additional information on setting up the MergePoint Unity switch using the DSView 3 software, and for information on how the MergePoint Unity switch uses TCP/IP, see the DSView 3 Installer/User Guide.

Rack Mounting a MergePoint Unity Switch

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

Most MergePoint Unity switches may be rack mounted in a 1U configuration. The MergePoint Unity switch family does not support a 0U configuration.

Rack mounting safety considerations

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

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

Connecting the MergePoint Unity Switch Hardware

To connect and turn on your MergePoint Unity switch:

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

WARNING: To reduce the risk of electric shock or damage to your equipment:

- Do not disable the power grounding plug. The grounding plug is an important safety feature.
 - Plug the power cord into a grounded (earthed) outlet that is easily accessible at all times.
 - Disconnect the power from the product by unplugging the power cord from either the electrical outlet or the product.
 - The AC inlet is the main disconnect for removing power to this product. For products that have more than one AC inlet, to remove power completely, all AC line cords must be disconnected.
 - This product has no user serviceable parts inside the product enclosure. Do not open or remove product cover.
-

1. Plug your VGA monitor and USB keyboard and mouse cables into the appropriately labeled ports. You must install both a keyboard and mouse on the local ports or the keyboard will not initialize properly.
 2. Choose an available port on the MergePoint Unity switch. Plug one end of a CAT 5 cable (4-pair, up to 150 ft/45 m) into a numbered port. Plug the other end into an RJ-45 connector of an IQ module.
 3. Plug the IQ module into the appropriate ports on the back of a target device. Repeat this procedure for all target devices you want to connect.
-

NOTE: When connecting a DSRIQ-SUN module, 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. Plug a CAT 5 cable from the Ethernet network into a LAN port on the back of the MergePoint Unity switch. Network users will access the MergePoint Unity switch through this port.
 5. (Optional) The MergePoint Unity switch may also be accessed using an ITU V.92, V.90 or V.24-compatible modem. Plug one end of an RJ-45 cable into the MODEM port on the MergePoint Unity switch. Plug the other end into the RJ-45 to DB-9 (male) adaptor, which then plugs into the appropriate port on the back of the modem.
-

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

6. (Optional) Plug one end of the RJ-45 cable supplied with the Power Distribution Unit (PDU) into the PDU1 port on the MergePoint Unity switch. Using the supplied RJ-45 adaptor, plug the other end into the PDU. Plug the power cords from the target devices into the PDU. Plug the PDU into an appropriate AC wall outlet. Repeat this procedure for the PDU2 port to connect a second PDU, if desired.
7. Turn on each target device, then locate the power cord that came with the MergePoint Unity switch. Plug one end into the power socket on the rear of the MergePoint Unity switch. Plug the other end into an appropriate AC wall outlet. If using a model equipped with dual power, use your second power cord to connect to the second power socket on the rear of the MergePoint Unity switch and plug the other end into an appropriate AC wall outlet.

To connect local virtual media or a smart card reader:

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

NOTE: For all virtual media sessions, you must use a DSAVIQ-USB2, DSAVIQ-PS2M, DSRIQ-VMC or MPUIQ-VMC module. For all smart card readers, you must use a DSRIQ-VMC or MPUIQ-VMC module.

For information on connecting virtual media remotely, see *Virtual Media* on page 54. For information on connecting a smart card reader remotely, see *Smart Cards* on page 58.

To connect a DSRIQ-SRL module to a serial device:

1. Attach the DSRIQ-SRL module 9-pin serial connector to the serial port of the device to be connected to your MergePoint Unity switch.
2. Attach one end of the UTP patch cable to the RJ-45 connector on the DSRIQ-SRL module. Connect the other end of the UTP patch cable to the desired port on the back of your MergePoint Unity switch.

NOTE: The DSRIQ-SRL module is a DCE device and only supports VT100 terminal emulation.

3. Connect the power supply to the power connector on your DSRIQ-SRL module. The cable expander can be used to provide power for up to four DSRIQ-SRL modules from a single power supply.
4. Connect the DSRIQ-SRL module power supply to a grounded AC wall outlet. Turn on your serial device. See *Using DSRIQ-SRL Modules* on page 71.

To connect an MPUIQ-SRL module to a serial device:

1. Attach the MPUIQ-SRL module CAT 5 connector to the serial device.

2. (Optional) Attach the MPUIQ-SRL module to an RJ-45 to 9-pin female adaptor. Attach the adaptor to the serial port of the serial device.
3. Plug one end of a CAT 5 cable (4-pair, up to 150 ft/45 m) into an available numbered port on the rear of the MergePoint Unity switch. Plug the other end into the RJ-45 connector of the MPUIQ-SRL module.
4. Connect the power supply to the power connector on your MPUIQ-SRL module. The cable expander can be used to provide power for up to four MPUIQ-SRL modules from a single power supply.
5. (Optional) Attach a USB-to-barrel power cord to the power connector on your MPUIQ-SRL module. Plug the USB connector on the USB-to-barrel power cord into any available USB port on the serial target device.

NOTE: You can not use the cable expander with the USB-to-barrel power cord. Multiple MPUIQ modules can use power off of the power supply, but not off of the target device.

6. If using the power supply, connect the MPUIQ-SRL module power supply to an appropriate AC wall outlet. Turn on your serial device.

Cascading MergePoint Unity Switches

You can cascade up to two levels of MergePoint Unity switches, enabling users to connect to up to 1024 servers. In a cascaded system, each target port on the main MergePoint Unity switch will connect to the ACI port on each cascaded MergePoint Unity switch. Each cascaded switch can then be connected to a server with an IQ module.

To cascade multiple MergePoint Unity switches:

1. Attach one end of a CAT 5 cable to a target port on the MergePoint Unity switch.
2. Connect the other end of the CAT 5 cable to the ACI port on the back of your cascaded MergePoint Unity switch.
3. Connect the devices to your cascaded MergePoint Unity switch.
4. Repeat these steps for all the cascaded MergePoint Unity switches you wish to attach to your system.

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

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

NOTE: Local port cascading is not supported on the MergePoint Unity switch.

Configuring the MergePoint Unity Switch

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

To configure the MergePoint Unity switch using the DSView 3 software:

See the DSView 3 Installer/User Guide for detailed instructions.

To configure the MergePoint Unity switch using the local UI:

See *Network Settings* on page 29 for detailed instructions on using the local UI to configure initial network setup.

Setting up the built-in web server

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

Connecting to the OBWI through a firewall

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

Table 2.2: TCP Ports and Functions for the MergePoint Unity Switch OBWI

TCP Port Number	Function
22	Used for SSH for serial sessions to an MPUIQ-SRL module
23	Used for Telnet (when Telnet is enabled)
80	Used for the initial downloading of the Avocent Video Viewer (for downloading the Java applet)
443	Used by the web browser interface for managing the MergePoint Unity switch and launching KVM sessions
2068	Transmission of KVM session data (mouse & keyboard) or transmission of video on MergePoint Unity switches

In a typical configuration, as shown in Figure 2.2, the user's computer is located outside of the firewall, and the MergePoint Unity switch resides inside the firewall.

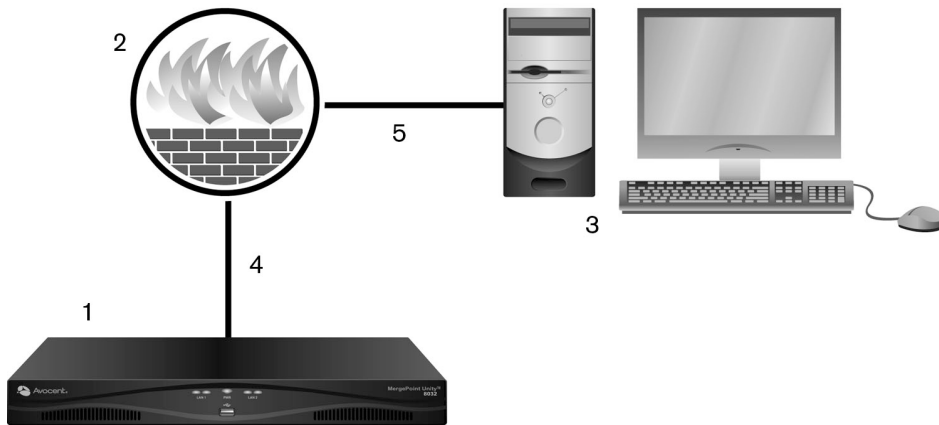


Figure 2.2: Typical MergePoint Unity Switch Firewall Configuration

Table 2.3: Descriptions for Figure 2.2

Number	Description
1	MergePoint Unity Switch
2	Firewall
3	User's Computer
4	Firewall Forwards HTTP Requests and KVM Traffic to the MergePoint Unity Switch
5	User Browses to Firewall's External IP Address

To configure the firewall:

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

For information on launching the OBWI, see *OBWI* on page 20.

Verifying the Connections

Front and rear panel Ethernet connection LEDs

On 16-port and 32-port models of the MergePoint Unity switch, the front and rear panels feature two LEDs indicating the Ethernet LAN1 connection status and two LEDs indicating the Ethernet LAN2 connection status. On the 4-port and 8-port switches, all LEDs are on the rear panel.

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

Front panel status LEDs

The front panel of MergePoint Unity switches (16-port and 32-port models only) have a bi-color general status LED that may illuminate green or amber.

- The LED illuminates green when the MergePoint Unity switch is turned on and operating normally.
- The LED blinks green when the MergePoint Unity switch is booting.
- The LED illuminates amber if a fault condition occurs, such as power supply failure (for MergePoint Unity switches equipped with dual power supplies), elevated ambient temperature or fan failure. The LED will continue to illuminate amber as long as the failure persists.
- The LED blinks between green and amber when the MergePoint Unity switch is Flash downloading.

Rear panel power status LEDs

The rear panel of 16-port and 32-port MergePoint Unity switches feature one power status LED for single power MergePoint Unity switches and two power status LEDs for dual power MergePoint Unity switches. On the 4-port and 8-port switches, all LED status indicators are on the rear panel. The LED(s) illuminate green when the MergePoint Unity switch is turned on and operating normally.

- The LED is off if the power supply does not have power or has failed.

- The LED illuminates when the unit is ready.
- The LED blinks when the MergePoint Unity switch is booting or an upgrade is in progress.
- The LED blinks "SOS" if a fault condition occurs, such as power supply failure (for MergePoint Unity switches equipped with dual power supplies), elevated ambient temperature or fan failure. The LED will continue to illuminate amber as long as the failure persists.

IQ and DSRIQ-SRL modules

Typically, IQ modules feature two green LEDs: a *POWER* LED and a *STATUS* LED.

- The *POWER* LED indicates that the attached module is powered.
- The *STATUS* LED indicates that a valid selection has been made to a MergePoint Unity switch.

The DSRIQ-SRL module prevents a serial break from the attached device if the module loses power. However, a user can generate a serial break with the attached device by pressing Alt+B after accessing the Terminal Applications menu.

Adjusting Mouse Settings on Target Devices

Before a computer connected to the MergePoint Unity switch can be used for remote user control, you must either enable Avocent Mouse Sync (see *Mouse Settings* on page 50) or set the target mouse speed and turn off acceleration. For machines running Microsoft® Windows® (Windows NT®, 2000, XP, Server 2003), use the default PS/2 mouse driver.

To ensure that the local mouse movement and remote cursor display remain in sync, mouse acceleration must be set to “none” for all user accounts accessing a remote system through a KVM switch. Mouse acceleration must also be set to “none” on every remote system. Special cursors should not be used and cursor visibility options, such as pointer trails, Ctrl key cursor location animations, cursor shadowing and cursor hiding, should also be turned off.

For more information about setting mouse movement and cursor features for use with Avocent hardware products and DSView 3 management software, please visit www.avocent.com and consult the Mouse and Pointer Settings guide.

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, newer versions of the DSView 3 software include the *Tools Single Cursor Mode* command available in the Video Viewer window. This command places the Video Viewer window into an “invisible mouse” mode which allows you to manually toggle control between the mouse pointer on the target system being viewed and the mouse pointer on the client server running DSView 3 software.

Local and Remote Configuration

The User Interfaces

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

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

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

- The Video Viewer window allows you to control the keyboard, monitor and mouse functions of individual target devices connected to the MergePoint Unity switch in real time. You may also use predefined global macros to perform actions within the Video Viewer window. For instructions on how to use the Video Viewer, see Chapter 4.
- The serial viewer window allows you to manage individual target devices either by using commands or scripts.

Local UI

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

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

To launch the local UI:

1. Connect your monitor, keyboard and mouse cables to the MergePoint Unity switch. For more information, see *Connecting the MergePoint Unity Switch Hardware* on page 11.
2. Press any of the enabled keystrokes to launch the local UI.

3. If local UI authentication has been enabled, enter your username and password.

NOTE: If the MergePoint Unity switch has been added to a DSView 3 server, then the DSView 3 server will be accessed to authenticate the user. If the MergePoint Unity switch has not been added to a DSView 3 server, or if the DSView 3 server cannot be reached, then the MergePoint Unity switch local user database will be accessed to authenticate the user. The default local username is Admin, and there is no password. Usernames in the local user database are case sensitive.

OBWI

The MergePoint Unity switch OBWI is a remote, web browser-based user interface. For details on setting up your system, see *Connecting the MergePoint Unity Switch Hardware* on page 11. shows which operating systems and browsers the OBWI supports. Avocent recommends that the browser be kept up-to-date with the latest version.

Table 3.1: OBWI Supported Operating Systems and Browsers

Operating System	Browser	
	Microsoft® Internet Explorer® version 6.0 SP1 and later	Firefox® version 2.0 and later
Windows 2000 Workstation or Server with Service Pack 2	Yes	Yes
Windows Server® 2003 Standard, Enterprise or Web Edition	Yes	Yes
Windows XP Home Edition or Professional	Yes	Yes
Windows Vista®	Yes	Yes
Red Hat® Enterprise Linux® 3, 4 and 5	No	Yes
Sun® Solaris™ 9 and 10	No	Yes
Novell® SUSE® Linux Enterprise 9 and 10	No	Yes
Fedora Core 6, 7 and 8	No	Yes
Mac OS® X Tiger (10.4+) (requires Firefox 1.5 or later)	No	Yes

To log in to the MergePoint Unity 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 MergePoint Unity 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 MergePoint Unity OBWI will appear.

NOTE: The default username is Admin with no password.

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

Using the user interfaces

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

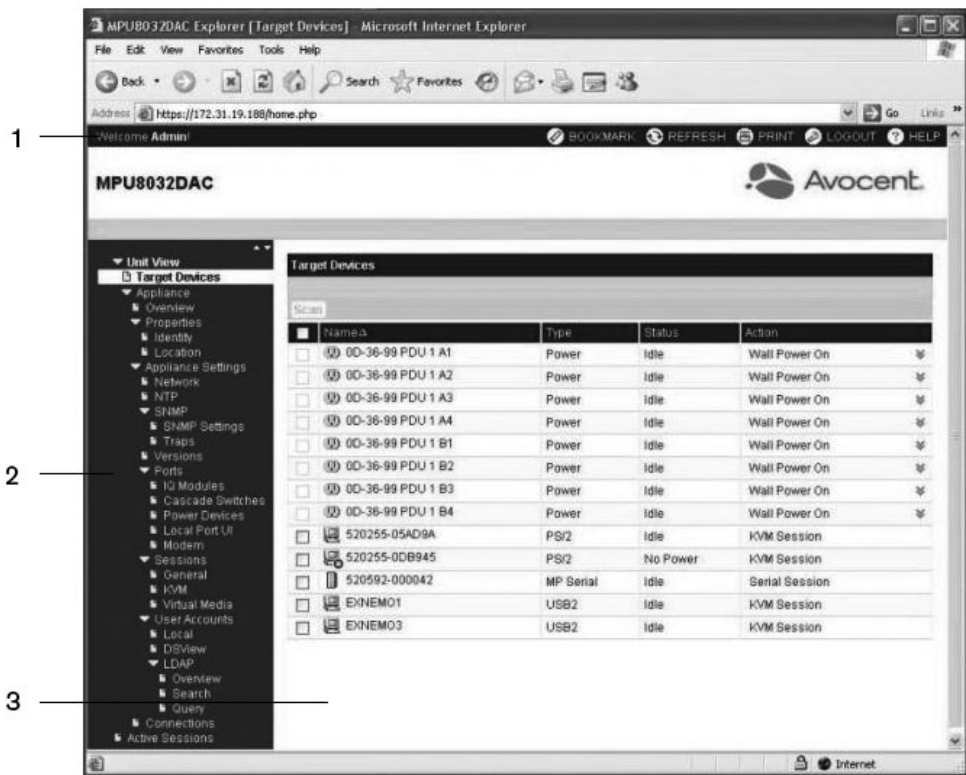


Figure 3.1: User Interface Window

Table 3.2: Descriptions for

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

Using the side navigation bar

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

Using the top option bar

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

Bookmarking a window (Microsoft Internet Explorer only)

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

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

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

To bookmark a window:

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

Printing a window

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

To print a MergePoint Unity switch OBWI window:

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

Refreshing a window

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

Logging out

A user may log out at any time by clicking the logout icon in the top option bar.

Viewing System Information

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

Table 3.3: System Information

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

You will also be alerted if any of the following fault conditions occur: power supply failure (for MergePoint Unity switches equipped with dual power supplies), elevated ambient

temperature or fan failure. A yellow triangle with an exclamation point and the name of the failure will appear in the header of each screen. This notification will appear or disappear only after you refresh the page. You can click on the notification to get more information.

MergePoint Unity Switch Sessions

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

Launching a session

NOTE: Java 1.5.0_11 or later is required to launch a session when using a Linux or Mac operating system.

To launch a session:

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

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

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

1. From the side navigation bar, select *Local Session*.
 2. Select the *Resume Active Session* checkbox. The Video Viewer window will appear.
- or-
- Press **Esc**.

Configuring sessions

To configure general session settings:

1. From the side navigation bar, select *Unit View - Appliance - Appliance Settings - Sessions - General*. The Appliance General Session Settings screen appears.
2. Select or deselect the *Enable Inactivity Timeout* 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. Select or deselect the *Enable Preemption Timeout* checkbox.
6. In the Preemption Timeout field, enter the amount of time you want to pass (from 1 to 120 seconds).
7. Click *Save*.

To configure KVM session settings:

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

To configure serial session settings:

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

Closing a session

To close a session:

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

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

To close a session (local users only):

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

MergePoint Unity Switch Appliance Tools

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

Rebooting the MergePoint Unity switch

To reboot the MergePoint Unity switch:

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

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

Upgrading the MergePoint Unity switch firmware

You can update your MergePoint Unity switch with the latest firmware available.

NOTE: The preferred method for updating the firmware is to use the DSView 3 software. See the DSView 3 Installer/User Guide for detailed instructions.

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

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

To upgrade the MergePoint Unity switch firmware:

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

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

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

-or-

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

-or-

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

5. Click *Upgrade*.

Saving and restoring appliance configurations and appliance user databases

NOTE: You may only save and restore appliance configurations and user databases when using the remote OBWL.

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

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

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

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

1. From the side navigation bar, select *Unit View - Appliance - Overview* to open the Unit Overview window.
2. Click *Restore Appliance Configuration* or *Restore Appliance User Database*. The Restore Appliance Configuration Window or Restore Appliance User Database Window will appear.
3. Click *Browse*. Navigate to the desired location and select the file name. Click *Upload*.
4. After the success screen appears, click *Close*. Reboot the managed appliance to enable the restored configuration. See *Rebooting the MergePoint Unity switch* on page 27.

Network Settings

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

To configure general network settings:

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

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

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

To configure IPv4 network settings:

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

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

5. Click *Save*.

To configure IPv6 network settings:

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

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

5. Click *Save*.

DNS Settings

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

To manually configure DNS settings:

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

Local UI Settings

To change how the local UI is invoked:

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

Local port user settings

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

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

To change the default preemption level (administrator only):

1. From the side navigation bar, select *Unit View - Appliance - Appliance Settings - Ports - Local Port UI* to open the Local Port UI Settings screen.
2. Select or deselect the *Disable Local Port User Authentication* checkbox.

3. Select one of the following options from the User Access Level drop-down menu: *User*, *User Administrator* or *Appliance Administrator*.
4. Select a number 1 - 4 from the User Preemption Level drop-down menu.
5. Click *Save*.

Virtual Media

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

For information about using virtual media in a KVM session, see *Virtual Media* on page 54.

Table 3.4: Virtual Media Session Settings

Setting	Description
Session Settings: Virtual Media locked to KVM session	The locking option specifies whether a virtual media session is locked to the KVM session on the target device. When locking is enabled (default) and the KVM session is closed, the virtual media session will also be closed. When locking is disabled and the KVM session is closed, the virtual media session will remain active.
Session Settings: Allow Reserved Sessions	Ensures that a virtual media connection can only be accessed with your username and that no other user can create a KVM connection to that target device. When the associated KVM session is disconnected, the virtual media session may be disconnected according to the Locked setting in the Virtual Media dialog box.
Drive Mappings: Virtual Media Access Mode	You may set the access mode for mapped drives to read-only or read-write. When the access mode is read-only, the user will not be able to write data to the mapped drive on the client server. When the access mode is read-write, the user will be able to read and write data from/to the mapped drive. If the mapped drive is read-only by design (for example, certain CD/DVD drives or ISO images), the configured read-write access mode will be ignored. Setting the read-only mode can be helpful when a read-write drive such as a mass storage device or a USB removable media is mapped, and you wish to prevent the user from writing data to it.
Encryption Level	You may configure encryption levels for virtual media sessions. The choices are: None (default), 128-bit SSL(ARCFOUR), DES, 3DES and AES.
Virtual Media Access per IQ Module: Enable VM/Disable VM	If the MergePoint Unity switch supports virtual media, the Virtual Media Access per IQ Module section lists all USB2 or PS2M IQ modules. The list includes details about each IQ module, including a virtual media status of Enabled or Disabled. You can either enable or disable virtual media for each IQ module. If the KVM switch does not support virtual media, this section and associated buttons and links are not displayed.

To set virtual media options:

1. From the side navigation bar, select *Unit Views - Appliance - Appliance Settings - Sessions - Virtual Media* to open the Appliance Virtual Media Session Settings screen.
2. Either enable or disable the *Virtual Media locked to KVM Sessions* 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. Select the checkbox next to each IQ module for which you want to enable virtual media and click *Enable VM*.

-or-

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

7. Click *Save*.

Local virtual media settings

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

Table 3.5: Local Virtual Media Session Settings

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

To configure local virtual media settings:

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

Modem Settings

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

For information on connecting your MergePoint Unity switch to a modem, see *Connecting the MergePoint Unity Switch Hardware* on page 11.

To configure modem settings:

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

Scan Mode

NOTE: Scan mode is only available when using the local UI.

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

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

To add target devices to the Scan list:

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

To configure Scan Time:

1. From the side navigation bar, select *Unit View - Appliance - Appliance Settings - Ports - Local Port UI* to open the Local Port UI Settings screen.
2. Under the Scan Mode heading, enter an amount of time in seconds (from 3-255) in the Scan Time field.

3. Click *Save*.

DSView 3 Server IP Addresses

You can contact and register an unmanaged MergePoint Unity switch with a DSView 3 server by specifying the IP addresses of up to four DSView 3 servers.

To configure the DSView 3 server IP address:

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

User Accounts

Managing local accounts

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

Access levels

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

Table 3.6: Allowed Operations by Access Level

Operation	Access Level		
	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

Operation	Access Level		
	Appliance Administrator	User Administrator	Users
Access target device	Yes, all target devices	Yes, all target devices	Yes, if allowed

To add a new user account (administrator only):

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

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

6. Click *Save*.

To delete a user account (administrator only):

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

SNMP Settings

SNMP is a protocol used to communicate management information between network management applications and MergePoint Unity switches. Other SNMP managers can communicate with your MergePoint Unity switches by accessing MIB-II and the public portion

of the enterprise MIB. When you open the SNMP screen, the OBWI will retrieve the SNMP parameters from the unit.

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

To configure general SNMP settings:

1. Select *Unit View - Appliance - Appliance Settings - SNMP - SNMP Settings* to open the SNMP screen.
2. Click to enable the *Enable SNMP* checkbox to allow the MergePoint Unity 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 MergePoint Unity switch. The values can be up to 64 characters in length. These fields may not be left blank.
5. Type the address of up to four management workstations that are allowed to manage this MergePoint Unity switch in the Allowable Managers fields. Alternatively, you may leave these fields blank to allow any station to manage the Remote Console Switch.
6. Click *Save*.

Event Settings

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

To enable individual events:

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

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

Setting Event Destinations

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

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

Configuring IQ Modules

From the Appliance IQ Modules screen, you can display a list of the attached IQ modules, as well as the following information about each IQ module: EID, Port, Status, Application, Interface Type and USB Speed. You can click on one of the IQ modules to view the following additional information: Switch Type, Boot Version, Hardware Version, FPGA Version, Version Available and Upgrade Status

You can also perform the following tasks: delete offline IQ modules, upgrade the IQ module firmware, set the USB speed or decommission the IQ module.

To delete offline IQ modules:

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

To set the IQ module USB Speed (for DSAVIQ-USB2 modules only):

1. From the side navigation bar, click *Unit View - Appliance - Appliance Settings - Ports - IQ Modules* to open the Appliance IQ Modules screen.
2. Select the checkbox(es) next to the IQ module(s) that you wish to modify.
3. Click either *Set USB 1.1 Speed* or *Set USB 2.0 Speed*.

Upgrading IQ modules

The IQ module Flash upgrade feature allows appliance administrators to update IQ modules with the latest firmware available. This update can be performed using the MergePoint Unity switch user interfaces or DSView 3 software.

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

IQ modules are automatically updated when the MergePoint Unity switch is updated. To update your MergePoint Unity switch firmware, see *MergePoint Unity Switch Appliance Tools* on page 26 or the DSView 3 Software Online Help. If issues occur during the normal upgrade process, IQ modules may also be force upgraded when needed.

NOTE: Check www.avocent.com for firmware upgrade files.

To upgrade the IQ module firmware:

1. From the side navigation bar, click *Unit View - Appliance - Appliance Settings - Ports - IQ Modules* to open the Appliance IQ Modules screen.
2. Select the checkbox(es) next to the IQ module(s) that you wish to upgrade and click *Upgrade*.

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

Power Device Settings

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

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

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

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

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

To delete offline power devices:

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

To change the minimum on time, off time or wake up state:

1. From the side navigation bar, select *Unit View - Appliance - Appliance Settings - Ports - Power Devices* to open the Appliance Power Devices screen.
2. Click the name of the unit you wish to configure, and select *Sockets*.
3. Click the socket name that you wish to modify.
4. Use the drop-down windows to alter the desired settings, and click *Save*.

CHAPTER

4

The Video Viewer

The Video Viewer Window

The Video Viewer is used to conduct a KVM session with the target devices attached to a MergePoint Unity switch using the OBWI. When you connect to a device using the Video Viewer, the target device desktop appears in a separate window containing both the local and the target device cursors.

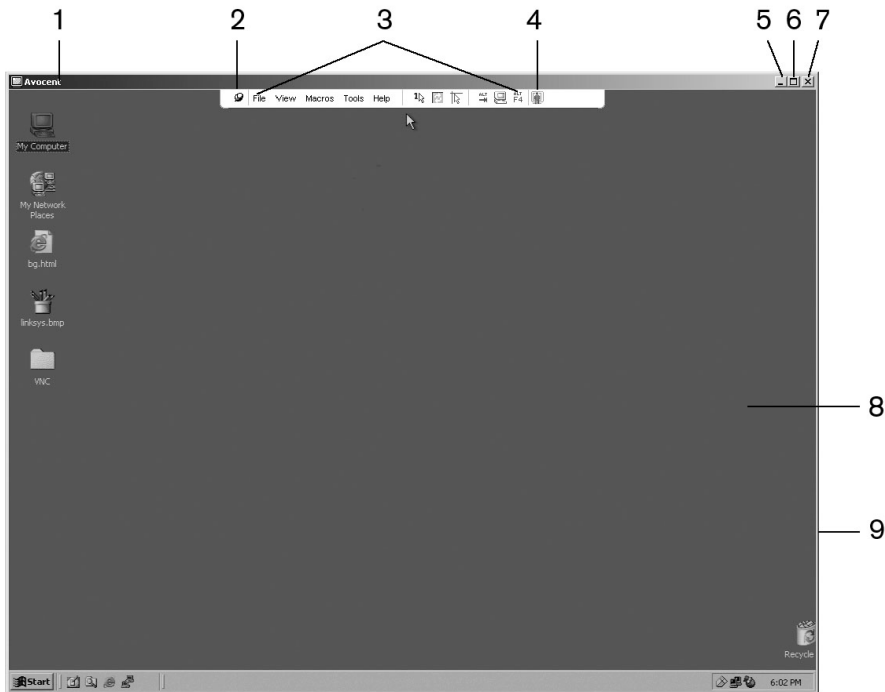
The MergePoint Unity switch OBWI software uses a Java-based program to display the Video Viewer window. The MergePoint Unity switch onboard web interface automatically downloads and installs the Video Viewer the first time it is opened.

NOTE: Java 1.5.0_11 or later is required to launch the Video Viewer when using a Linux or Mac operating system.

NOTE: The MergePoint Unity switch OBWI does not install the Java Resource Engine (JRE). The JRE is available as a free download from <http://www.sun.com> for PC users and from <http://www.apple.com> for Mac users.

NOTE: The MergePoint Unity switch OBWI uses system memory to store and display images within Video Viewer windows. Each opened Video Viewer window requires additional system memory: An 8-bit color setting on the client server requires 1.4 MB of memory per Video Viewer window. A 16-bit color setting requires 2.4 MB and a 32-bit color setting requires 6.8 MB. Opening more than four simultaneous Video Viewer windows may affect system performance and is not recommended. If you attempt to open more Video Viewer windows than your system memory allows, you will receive an out-of-memory error and the requested Video Viewer window will not open.

If the device you are attempting to access is currently being viewed by another user, you will be prompted to preempt the other user if your preemption level is equal to or greater than the other user's preemption level. An appliance administrator can also disconnect an active user via the Active Session page. For more information, see *MergePoint Unity Switch Sessions* on page 25.

**Figure 4.1: Video Viewer Window (Normal Window Mode)****Table 4.1: Descriptions for Figure 4.1**

Number	Description
1	Title Bar: Displays the name of the target device being viewed. When in Full Screen mode, the title bar disappears and the target device name appears between the menu and toolbar.
2	Thumbtack: Locks the display of the menu and toolbar so that it is visible at all times.
3	Menu and toolbar: Enables you to access many of the features in the Video Viewer window. The menu and toolbar is in a show/hide state if the thumbtack has not been used. Place your cursor over the toolbar to display the menu and toolbar. Up to ten commands and/or macro group buttons can be displayed on the toolbar. By default, the Single Cursor Mode, Refresh, Automatic Video Adjust and Align Local Cursor buttons appear on the toolbar. For more information, see <i>Changing the toolbar</i> on page 43 and <i>Macros</i> on page 60.

Number	Description
4	Macro buttons: Commonly used keyboard sequences that can be sent to the target device.
5	Minimize button: Minimizes the display of the Video Viewer window into the task bar at the bottom of the local computer.
6	<p>Maximize button: Changes the window to Full Screen mode, which expands the accessed device desktop to fill the entire screen. Expanding the window causes the following to occur:</p> <p>The title bar disappears.</p> <p>The target device name appears between the menu and toolbar.</p> <p>The Maximize button changes to a Normal Window Mode button and appears on the toolbar. Clicking the button toggles the Video Viewer window to Normal Window mode.</p> <p>The Close button appears on the toolbar.</p>
7	<p>Close button: Closes the Video Viewer window.</p> <p>NOTE: The Close button may not be present for all operating systems.</p>
8	Accessed device desktop: Interacts with your device through this window.
9	Frame: Resizes the Video Viewer window by clicking and holding on the frame.

Changing the toolbar

You can choose the amount of elapsed time before the toolbar hides in the Video Viewer window when it is in show/hide state (that is, not locked in place by the thumbtack).

To specify a toolbar hide time:

1. Select *Tools - Session Options* from the Video Viewer window menu.
-or-
Click the *Session Options* button.
The Session Options dialog box appears.
2. Click the *Toolbar* tab.
3. Use the arrow keys to specify the number of elapsed seconds prior to hiding the toolbar.
4. Click *OK* to save your changes and close the dialog box.

Launching a Session

NOTE: When using a non-proxied connection, video performance over a slower network connection may be less than optimal. Since certain color settings (such as Grayscale) use less network bandwidth than others (such as Best Color), changing the color settings can increase video performance. For optimal video performance over a slower network connection, Avocent recommends a color setting such as Grayscale/Best Compression or Low Color/High Compression. See *Adjusting the View* on page 45 for more information.

NOTE: If a user connects to a target device with a higher screen resolution than the local computer, the Video Viewer window will display a portion of the target device screen, with scroll bars for viewing the remainder of the screen. The user may view the entire screen by adjusting the resolution on the target device, the local computer or both.

To launch a KVM session from the MergePoint Unity Explorer window:

1. Click on a device listed on the Target Devices screen to open the unit overview window.
2. Click the *KVM Session* link to open the Video Viewer in a new window.

Session time-out

A remote session can time-out when no activity occurs in a Session window for a specified time. The session time-out value can be configured in the Appliance KVM Session Settings window. The specified time-out value will be used the next time the switch OBWI is accessed.

To enable, disable or configure the session time-out:

1. In the side menu, select *Unit View - Appliance - Appliance Settings - Sessions - General*.
2. Select the desired setting for the *Enable Activity Timeout* box.
3. If necessary, select the time limit for the inactivity time-out.
4. Click *Save*.

Window Size

NOTE: The View - Scaling command is not available if the Video Viewer window is in Full Screen mode or to non-primary users of a shared session.

When the MergePoint Unity switch OBWI is used for the first time, any open Video Viewer windows display at a resolution of 1024 x 768 until the user changes the value. Each Video Viewer window can be set to a different resolution.

The MergePoint Unity switch OBWI automatically adjusts the display if the window size changes during a session as long as autoscaling is enabled. If the target device resolution changes any time during a session, the display adjusts automatically.

To change the Video Viewer window resolution:

1. Select the *View - Scaling* command.
2. Select the desired resolution.

Adjusting the View

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

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable Full Screen mode. When Full Screen mode is enabled, the image adjusts to fit the desktop up to a size of 1600 x 1200 or 1680 x 1050 (wide-screen). If the desktop has a higher resolution, the following occurs:
 - The full-screen image is centered in the desktop, and the areas surrounding the Video Viewer window are black.
 - The menu and toolbar are locked so that they are visible at all times.
- Enable automatic, full or manual scaling of the session image:
 - With full scaling, the desktop window remains fixed and the device image scales to fit the window.
 - With automatic scaling, the desktop window is sized to match the resolution of the target device being viewed.
 - With manual scaling, a drop-down menu of supported image scaling resolutions is displayed.
- Change the color depth of the session image.

To align the mouse cursors:

Click the *Align Local Cursor* button in the Video Viewer window toolbar. The local cursor should align with the cursor on the remote device.

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

To refresh the screen, click the *Refresh Image* button in the Video Viewer window, or select *View - Refresh* from the Video Viewer window menu. The digitized video image is completely regenerated.

To enable Full Screen mode, click the *Maximize* button, or select *View - Full Screen* from the Video Viewer window menu. The desktop window disappears and only the accessed device

desktop is visible. The screen resizes up to a maximum of 1600 x 1200 or 1680 x 1050 (wide-screen). If the desktop has a higher resolution, then a black background surrounds the full screen image. The floating toolbar appears.

To disable Full Screen mode, click the *Full Screen Mode* button on the floating toolbar to return to the desktop window.

To enable full scaling, select *View - Scaling* from the Video Viewer window menu. The device image scales automatically to the resolution of the target device being viewed.

To enable manual scaling, select *View - Scaling* from the Video Viewer window menu. Choose the dimension to scale the window. The available manual scaling sizes will vary according to your system.

Refreshing the Image

Clicking the *Refresh Image* button in the Manual Video Adjust dialog box completely regenerates the digitized video image.

NOTE: You can also select *View - Refresh* from the Video Viewer window menu to refresh the image.

Video Settings

Additional video adjustment

Generally, the Video Viewer window automatic adjustment features optimize the video for the best possible view. However, users can fine-tune the video with the help of Avocent Technical Support by selecting the *Tools - Manual Video Adjust* command in the Video Viewer window menu or clicking the *Manual Video Adjust* button. This displays the Manual Video Adjust dialog box. Video adjustment is a per target setting.

Users 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.

To manually adjust the video quality of the window:

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

1. Select *Tools - Manual Video Adjust* from the Video Viewer window menu.

-or-

Click the *Manual Video Adjust* button.

The Manual Video Adjust dialog box appears.

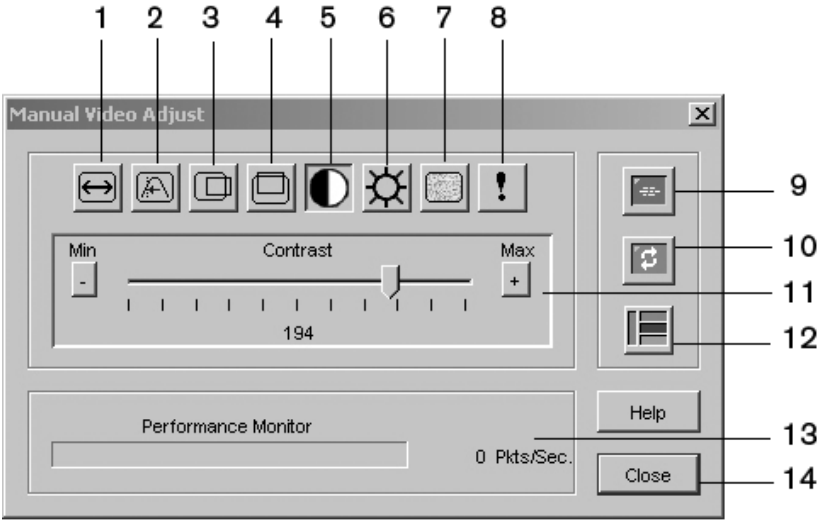


Figure 4.2: Manual Video Adjust Dialog Box

Table 4.2: Descriptions for Figure 4.2

Number	Description	Number	Description
1	Image Capture Width	8	Pixel Noise Threshold
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	Contrast	12	Video Test Pattern
6	Brightness	13	Performance Monitor
7	Block Noise Threshold	14	Close button

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* to exit the Manual Video Adjust dialog box.

Target video settings

The Image Capture Width, Pixel Sampling/Fine Adjust, Image Capture Horizontal Position and Image Capture Vertical Position adjustments affect how the target video is captured and digitized. They are seldom changed.

The image capture parameters are automatically changed by the Automatic Adjustment function. A special image is required on the target in order to make accurate adjustments independently.

Automatic video adjustment

In most cases, you do not need to alter the Video Settings from the default settings. The system automatically adjusts and uses the optimal video parameters. The MergePoint Unity switch OBWI performs best when the video parameters are set such that no (0) video packets are transmitted for a static screen.

You can easily adjust your video parameters to ideal settings by clicking on the *Auto Adjust Video* button in the Manual Video Adjust dialog box.

NOTE: You can also select *Tools - Automatic Video Adjust* from the Video Viewer window menu or click the *Automatic Video Adjust* toolbar icon to automatically adjust the video.

Video Test Pattern

Clicking the *Video Test Pattern* button in the Manual Video Adjust dialog box toggles a display of a video test pattern. Click the *Video Test Pattern* button again to toggle back to a normal video image.

Vendor-specific video settings

Video settings vary significantly among manufacturers. Avocent maintains an online database of optimized video settings for various video cards, particularly Sun-specific ones. This information can be obtained from Avocent's online knowledge base or by calling Avocent technical support.

Color Settings

Adjusting Color Depth

The Dambrackas Video Compression® (DVC) algorithm enables users to adjust the number of viewable colors in a remote session window. You can choose to display more colors for the best fidelity or fewer colors to reduce the volume of data transferred on the network.

Video Viewer windows can be viewed using the Best Color Available (slower updates), Best Compression (fastest updates), a combination of Best Color and Best Compression or in Grayscale.

You can specify the color depths of individual ports and channels by selecting the *View Color* command in a remote session window. These settings are saved individually per channel.

Contrast and brightness

If the image in the Video Viewer window is too dark or too light, select *Tools - Automatic Video Adjust* or click the *Automatic Video Adjust* button. This command is also available in the Video Adjustments dialog box. In most cases, this corrects video issues.

When clicking *Auto Adjust* several times does not set the contrast and brightness as desired, adjusting the contrast and brightness manually can help. Increase the brightness. Do not go more than 10 increments before moving the contrast. Generally, the contrast should be moved very little.

Noise Settings

Detection thresholds

In some cases, noise in the video transmission keeps the packets/sec count up, which is indicated by small dots changing in the area of the cursor when it is moved. Varying the threshold values may result in “quieter” screens and can improve cursor tracking.

You can modify Noise Threshold and Priority Threshold values if you are using standard video compression. You can also modify Block Noise Threshold and Pixel Noise Threshold values. You can restore default threshold values by clicking *Auto Adjust Video*.

Block Noise Threshold and Pixel Noise Threshold

The Block Noise Threshold and Pixel Noise Threshold values set the minimum color levels in terms of changed video blocks and pixels per thousand that are allowed.

- The Block Noise Threshold sets the minimum color change that occurs in a single video block. Increasing the value reduces the network bandwidth. Decreasing the value makes the size of these artifacts smaller.
- The Pixel Noise Threshold sets the minimum color change in a single pixel. Decreasing the value reduces the number of low-contrast artifacts, but increases network bandwidth.

See *Adjusting the View* on page 45 for information about changing the color depth.

Mouse Settings

Adjusting mouse options

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

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

Cursor type

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

In Single Cursor mode, the display of the local (second) cursor in the Video Viewer window turns off and only the target device mouse pointer is visible. The only mouse movements that appear are those of the target device remote cursor. Use Single Cursor mode when there is no need for a local cursor.

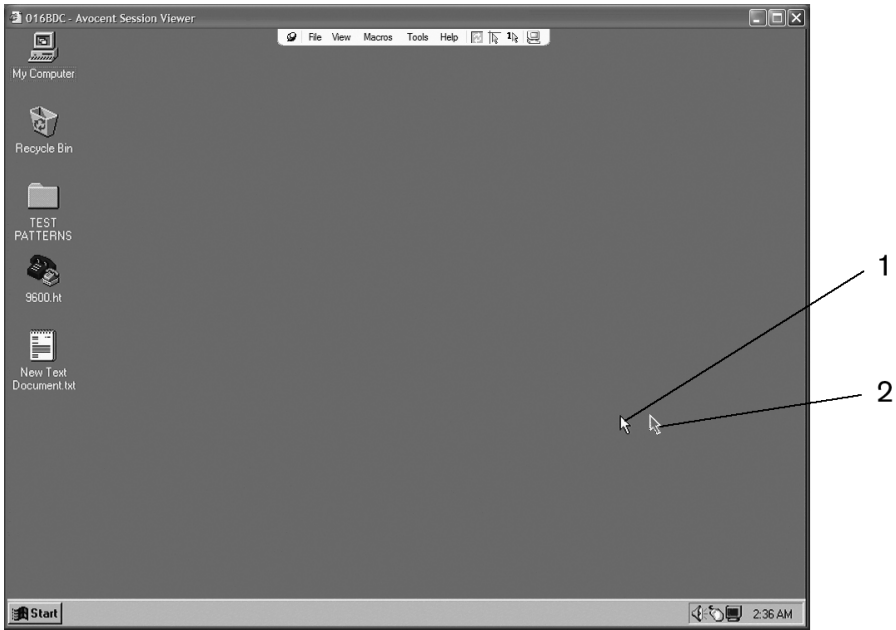


Figure 4.3: Video Viewer Window with Local and Remote Cursors Displayed

Table 4.3: Descriptions for Figure 4.3

Number	Description
1	Remote Cursor
2	Local Cursor

The Cursor mode status of the Video Viewer window displays in the title bar, including the keystroke that will exit Single Cursor mode. You can define the keystroke that will exit Single Cursor mode in the Session Options dialog box.

NOTE: When using a device that captures keystrokes before they reach the client server, you should avoid using those keys to restore the mouse pointer.

To enter Single Cursor mode, select *Tools - Single Cursor Mode* from the Video Viewer window menu, or click the *Single Cursor Mode* button. The local cursor does not appear and all movements are relative to the target device.

To select a key for exiting Single Cursor mode:

1. Select *Tools - Session Options* from the Video Viewer window menu.

-or-

Click the *Session Options* button.

The Session Options dialog box appears.

2. Click the *Mouse* tab.
3. Select a terminating keystroke from the drop-down menu in the Single Cursor mode area.
4. Click *OK* to save settings.

When you enable Single Cursor mode, you can press the specified key to return to Regular Desktop mode.

To exit Single Cursor mode, press the key on the keyboard that is identified in the title bar.

To change the mouse cursor setting:

1. Select *Tools - Session Options* from the Video Viewer window menu.

-or-

Click the *Session Options* button.

The Session Options dialog box appears.

2. Click the *Mouse* tab.
3. Select a mouse cursor type in the Local Cursor panel.
4. Click *OK* to save settings.

Mouse scaling

Some earlier versions of Linux did not support adjustable mouse accelerations. For installations that must support these earlier versions, you can choose among three preconfigured mouse scaling options or set your own custom scaling. The preconfigured settings are Default (1:1), High (2:1) or Low (1:2):

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

To set mouse scaling:

1. Select *Tools - Session Options* from the Video Viewer window menu.

-or-

Click the *Session Options* button.

The Session Options dialog box appears.

2. Click the *Mouse* tab.
3. To use one of the preconfigured settings, check the appropriate radio button.
-or-
To set custom scaling:
 - a. Click the *Custom* radio button to enable the X and Y fields.
 - b. Type a scaling value in the X and Y fields. For every mouse input, the mouse movements are multiplied by the respective X and Y scaling factors. Valid input range is 0.25-3.00.

Mouse alignment and synchronization

Because the MergePoint Unity switch OBWI cannot get constant feedback from the mouse, there are times when the mouse on the MergePoint Unity switch may lose sync with the mouse on the host system. If your mouse or keyboard no longer responds properly, you can align the mouse to reestablish proper tracking.

Alignment causes the local cursor to align with the remote target device's cursor. Resetting causes a simulation of a mouse and keyboard reconnect as if you had disconnected and reconnected them.

To realign the mouse, click the *Align Local Cursor* button in the Video Viewer window toolbar.

Avocent Mouse Sync

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

NOTE: You may only use Avocent Mouse Sync when you are using a DSAVIQ-USB2, DSRIQ-VMC or MPUIQ-VMC module and the target device is running on a Windows or Macintosh operating system.

To set Avocent Mouse Sync from the Video Viewer:

1. Select *Tools - Session Options* from the Video Viewer menu or click the *Session Options* button. The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. In the Avocent Mouse Sync section, the current status is shown. Select the *Enable Synchronization* checkbox to enable Avocent Mouse Sync.
-or-
Deselect the *Enable Synchronization* checkbox to disable Avocent Mouse Sync.

NOTE: On supported system configurations, the Avocent Mouse Sync status is Available. If you are using a DSAVIQ-USB2, DSRIQ-VMC or MPUIQ-VMC module but the target device cannot support the Avocent Mouse Sync protocol, the status is Unavailable. If you are not using a DSAVIQ-USB2, DSRIQ-VMC or MPUIQ-VMC module, the status is Not Supported.

4. Click *OK*.

Virtual Media

The virtual media feature allows the user on the client server to map a physical drive on that machine as a virtual drive on a target device. The client server may also add and map an ISO or floppy image file as a virtual drive on the target device. You may have one CD drive and one mass storage device mapped concurrently.

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

For information on configuring virtual media settings using the OBWI, see *Virtual Media* on page 31.

Requirements

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

The target device must be intrinsically able to use the types of USB2-compatible media that you virtually map. In other words, if the target device does not support a portable USB memory device, you cannot map that on the client server 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. See *Access levels* on page 48.

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

Sharing and preemption considerations

The KVM and virtual media sessions are separate; therefore, there are many options for sharing, reserving or preempting sessions. The DSView 3 software has the flexibility to accommodate the system needs.

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

active. This could be desirable if a user is performing a time-intensive task using the virtual media session (such as an operating system load), and wants to establish a KVM session with a different target device to perform other functions while the operating system load progresses.

Once a target device has an active virtual media session without an associated active KVM session, two situations can occur - the original user (User A) can reconnect or a different user (User B) can connect to that channel. You may set an option in the Virtual Media dialog box (Reserved) that allows only the User A to access that channel with a KVM session.

If User B is allowed to access that session (the Reserved option is not enabled), User B could control the media that is being used in the virtual media session. By using the Reserved option in a tiered environment, only User A could access the lower switch and the KVM channel between the upper switch and lower switch would be reserved for User A.

Virtual Media dialog box

The Virtual Media dialog box allows you to manage the mapping and unmapping of virtual media. The dialog box displays all the physical drives on the client server that can be mapped as virtual drives. You may also add ISO and floppy image files and then map them using the Virtual Media dialog box.

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

You may specify that the virtual media session is reserved. When a session is reserved, and the associated KVM session is closed, another user cannot launch a KVM session to that target device. If a session is not reserved, another KVM session may be launched.

You may also reset the USB2 IQ module from the Virtual Media dialog box. This action will reset every form of USB media on the target device, and should therefore be used with caution, and only when the target device is not responding.

Opening a virtual media session

To launch a virtual media session:

Select *Tools - Virtual Media* from the Video Viewer menu. The Virtual Media dialog box will appear. To make this a reserved session, click *Details*, then select the *Reserved* checkbox.

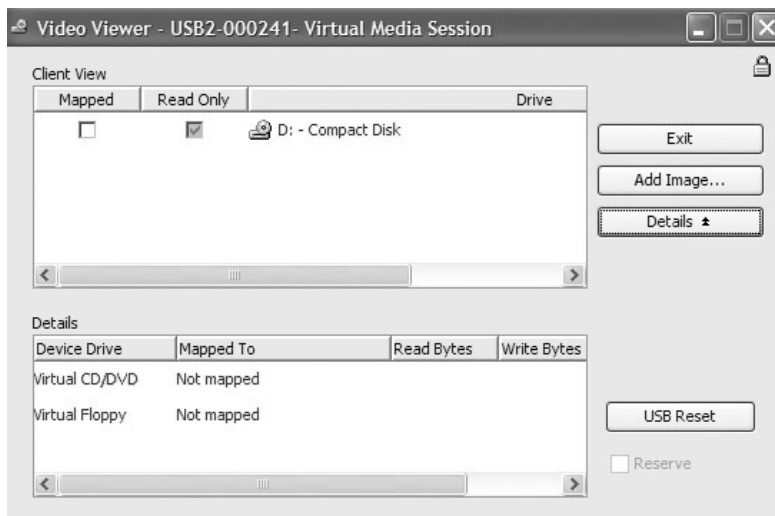


Figure 4.4: Video Viewer Virtual Media Dialog Box

To map a virtual media drive:

1. Open a virtual media session from the Video Viewer menu by selecting *Tools - Virtual Media*.
2. To map a physical drive as a virtual media drive:
 - a. In the Virtual Media dialog box, click the *Mapped* checkbox next to the drive(s) you wish to map.
 - b. If you wish to limit the mapped drive to read-only access, click the *Read Only* checkbox next to the drive. If the virtual media session settings were previously configured so that all mapped drives must be read only, this checkbox will already be enabled and cannot be changed.

You might wish to enable the *Read Only* checkbox if the session settings enabled read and write access, but you wished to limit a particular drive's access to read only.
3. To add and map an ISO or floppy image as a virtual media drive:
 - a. In the Virtual Media dialog box, click *Add Image*.
 - b. The common file dialog box will appear, with the directory containing disk image files (that is, those ending in .iso or .img) displayed. Select the desired ISO or floppy image file and click *Open*.

-or-

If the client server's operating system supports drag-and-drop, select the desired ISO or floppy image file from the common file dialog box and drag it onto the Virtual Media dialog box.

- c. The file's header is checked to ensure it is correct. If it is, the common file dialog box will close and the chosen image file will appear in the Virtual Media dialog box, where it can be mapped by clicking the *Mapped* checkbox.
- d. Repeat steps a through c for any additional ISO or floppy images you wish to add. You may add any number of image files (up to the limits imposed by memory), but you may only have one virtual CD or DVD or virtual mass storage mapped concurrently.

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

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

To unmap a virtual media drive:

1. In the Virtual Media dialog box, uncheck the *Mapped* checkbox next to the drive you wish to unmap.
2. You will be prompted to confirm. Confirm or cancel the unmapping.
3. Repeat for any additional virtual media drives you wish to unmap.

To display virtual media drive details:

In the Virtual Media dialog box, click *Details*. 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.

To close the Details view, click *Details* again.

To reset all USB devices on the target device:

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

1. In the Virtual Media dialog box, click *Details*.

2. The Details View will appear. Click *USB Reset*.
3. A warning message will appear, indicating the possible effects of the reset. Confirm or cancel the reset.
4. To close the Details view, click *Details* again.

Closing a virtual media session

To close the Virtual Media dialog box:

1. Click *Exit*.
2. If you have any mapped drives, a message is displayed, indicating that the drives will be unmapped. Confirm or cancel the operation.

If a user attempts to disconnect a virtual media session or an active KVM session that has an associated locked virtual media session, a confirmation message is displayed, indicating that any virtual media mappings will be lost.




Smart Cards

You can connect a smart card reader to an available USB port on the client server and access attached target devices on the MergePoint Unity switch system. You can then launch a KVM session to open the Video Viewer and map a smart card.

NOTE: For all smart card readers, you must use a DSRIQ-VMC or MPUIQ-VMC module.

The smart card status is indicated by the smart card icon at the far right of the Video Viewer toolbar. The following table describes the smart card status icons.

Table 4.4: Smart Card Icons

Icon	Description
	A smart card is not in the smart card reader, or a smart card reader is not attached.
	A smart card is in the smart card reader but has not been mapped yet.
	A smart card is mapped.

To map a smart card:

1. Open a KVM session to display the Video Viewer window menu.
2. Insert a smart card into the smart card reader attached to your client server.
3. Click *Tools - Map Smart Card* on the Video Viewer window menu.

4. If no smart card is mapped to the target device, the No Card Mapped option will have a dot beside it. Select your smart card, listed below this option, to map the smart card.

To unmap a smart card, close out the KVM session by clicking *X* in the Video Viewer window menu, selecting *Tools - No Card Mapped*, removing the smart card from the smart card reader or disconnecting the smart card reader from the client server.

Keyboard Pass-through

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

- If a Video Viewer window is in Full Screen mode, all keystrokes and keyboard combinations except Ctrl-Alt-Del are sent to the remote target device being viewed.
- If a Video Viewer window is in Regular Desktop mode, Keyboard Pass-through mode can be used to control whether the remote target device or local computer recognizes certain keystrokes or keystroke combinations.

Keyboard pass-through must be specified using the Session Options dialog box. When enabled, keyboard pass-through sends all keystrokes and keystroke combinations except Ctrl-Alt-Del to the remote target device being viewed when the Video Viewer window is active. When the local desktop is active, keystrokes and keystroke combinations entered by the user affect the local computer.

NOTE: The Ctrl-Alt-Del keyboard combination can be sent only to a remote target device by using a macro.

NOTE: The Japanese keyboard **ALT-Han/Zen** keystroke combination is always sent to a remote target device regardless of the Screen mode or keyboard pass-through setting.

To specify keyboard pass-through:

1. Select *Tools - Session Options* from the Video Viewer window menu.
-or-
Click the *Session Options* button.
The Session Options dialog box appears.
2. Click the *General* tab.
3. Select *Pass-through all keystrokes in regular window mode*.
4. Click *OK* to save setting.

Macros

The MergePoint Unity switch OBWI comes pre-configured with macros for the Windows and Sun platforms.

To send a macro, select *Macros - <desired macro>* from the Video Viewer window menu, or select the desired macro from the buttons available on the Video Viewer menu.

Saving the View

You can save the display of a Video Viewer either to a file or to the clipboard for pasting into a word processor or other program.

To capture the Video Viewer window to a file:

1. Select *File - Capture to File* from the Video Viewer window menu.

-or-

Click the *Capture to File* button.

The Save As dialog box appears.

2. Enter a filename and choose a location to save the file.
3. Click *Save* to save the display to a file.

To capture the Video Viewer window to your clipboard, select *File - Capture to Clipboard* from the Video Viewer window menu, or click the *Capture to Clipboard* button. The image data is saved to the clipboard.

Closing a Session

To close a Video Viewer window session:

Select *File - Exit* from the Video Viewer window.

CHAPTER

5

LDAP

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

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

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

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

Configuring LDAP in the User Interface

LDAP Overview parameters

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

LDAP authentication priority

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

To configure LDAP authentication priority parameters:

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

3. Click *Save*.

LDAP servers

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

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

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

To configure LDAP server parameters:

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

LDAP Search parameters

On the LDAP Search page, you can configure the parameters used when searching for LDAP directory service users.

Use the Search DN field to define an administrator-level user that the appliance uses to log into the directory service. Once the appliance is authenticated, the directory service grants it access to the directory to perform the user authentication queries specified on the LDAP Query page. The default values are `cn=Administrator`, `cn=Users`, `dc=yourDomainName` and `dc=com` and may be modified. For example, to define an administrator Distinguished Name (DN) for `test.view.com`, type **`cn=Administrator`**, **`cn=Users`**, **`dc=test`**, **`dc=view`**, and **`dc=com`**. Each Search DN value must be separated by a comma.

The Search Password field is used to authenticate the administrator or user specified in the Search DN field.

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

The UID Mask field specifies the search criteria for User ID searches of LDAP target devices. The format should be in the form <name>=<%1>. The default value is sAMAccountName=%1, which is correct for use with Active Directory. This field is required for LDAP searches.

To configure LDAP search parameters:

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

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

LDAP Query parameters

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

The appliance performs two different types of queries. Query Mode (Appliance) is used to authenticate administrators and users attempting to access the appliance itself. Query Mode (Target Device) is used to authenticate users that are attempting to access attached target devices. Additionally, each type of query has three modes that utilize certain types of information to determine whether or not an LDAP user has access to an appliance or connected target devices. See *Appliance and Target Device Query Modes* on page 64 detailed information on each mode.

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

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

level associated with a group is configured by setting the value of an attribute in the group object.

- For example, if the Notes property in the group objects list is used to implement the access control attribute, the Access Control Attribute field on the LDAP Query Page should be set to info. Setting the Notes property to KVM User Admin causes the members of that group to have user administration access to the appliances and target devices that are also members of that same group.
- The Notes property is used to implement the access control attribute. The value of the Notes property, available in group and user objects shown in Active Directory Users and Computers (ADUC), is stored internally in the directory, in the value of the info attribute. ADUC is a Microsoft Management Console snap-in for configuring Active Directory. It is started by selecting *Start - Programs - Administrative Tools - Active Directory Users and Computers*. This tool is used to create, configure and delete objects such as users, computers and groups. See *Appliance and Target Device Query Modes* on page 64 for more information.
- The Group Container Mask field defines the object type of the Group Container, which is normally an organizational unit. The default value is “ou=%1”.
- The Target Mask field defines a search filter for the target device. The default value is “cn=%1”.
- The Access Control Attribute field specifies the name of the attribute that is used when the query modes are set to User Attribute or Group Attribute. The default value is info.

To configure LDAP query parameters:

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

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

Appliance and Target Device Query Modes

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

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

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

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

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

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

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

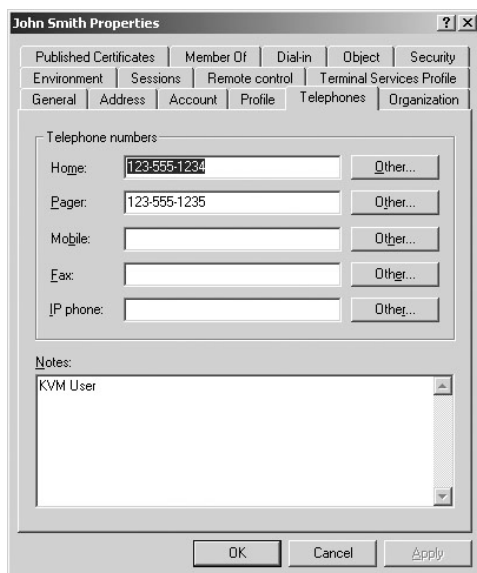


Figure 5.1: Active Directory - KVM User

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

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

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

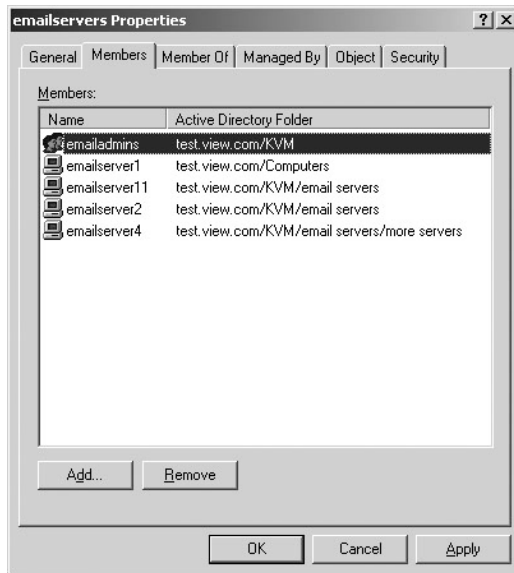


Figure 5.2: Active Directory - Define Groups

Setting up Active Directory for Performing Queries

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

To set up group queries:

1. Log into Windows with administrator privileges.
2. Open Active Directory software.
3. Create an organizational unit to be used as a group container.
4. Create a computer object in Active Directory with a name identical to the switching system name for querying appliances (specified in the Appliance Overview screen of the OBWI), or identical to the attached target devices for querying target devices. The name must match exactly, including case.
5. The appliance names and target device names used for group queries are stored in the appliance. The appliance name specified in the Appliance Overview screen of the OBWI and target device names must identically match the object names in Active Directory. Each appliance name and target device name may be comprised of any combination of upper-

case and lower-case letters (a-z, A-Z), digits (0-9) and hyphens (-). You cannot use spaces and periods (.) or create a name that consists entirely of digits. These are Active Directory constraints.

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

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

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

APPENDICES

Appendix A: Terminal Operations

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

NOTE: The preferred method is to make all configuration settings in the DSView 3 software. See the DSView 3 Installer/User Guide for more information.

To connect a terminal to the MergePoint Unity switch:

1. Using a null modem cable, connect a terminal or a PC that is running terminal emulation software (such as HyperTerminal®) to the SETUP port on the back panel of the MergePoint Unity switch. For MergePoint Unity switch models that support an RJ-45 port, an RJ-45 to DB9 (female) adaptor is provided.

The terminal settings are 9600 bits per second (bps), 8 bits, 1 stop bit, no parity and no flow control.

2. Turn on each target device and then turn on the MergePoint Unity switch. When the MergePoint Unity switch completes initialization, the Console menu will display the following message: *Press any key to continue.*

Console boot menu options

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

- Boot Normal
- Boot Alternate Firmware
- Reset Factory Defaults
- Full-Factory Reset

Console main menu options

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

- Debug messages: This menu option turns on console status messages. Because this can significantly reduce performance, you should only enable debug messages when instructed

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

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

Appendix B: Using Serial IQ Modules

Both DSRIQ-SRL and MPUIQ-SRL serial modules are supported and described in the following sections.

Using DSRIQ-SRL Modules

The DSRIQ-SRL module is a serial-to-VGA converter that allows VT100-capable devices to be viewed from the MergePoint Unity switch local port, the OBWI, or by using the DSView 3 software. The actual serial data is not accessed, but is merely displayed. All serial data coming from the target device is displayed in a VT100 window, placed into a video buffer and sent to the MergePoint Unity switch as though it came from a VGA target. Likewise, keystrokes entered on a keyboard are sent to the attached device as though they were typed on a VT100 terminal.

DSRIQ-SRL module modes

The following modes can be accessed from the DSRIQ-SRL module:

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

Configuring the DSRIQ-SRL module

NOTE: The DSRIQ-SRL module is a DCE device and only supports VT100 terminal emulation.

Pressing Ctrl-F8 will activate the Configuration screen of the DSRIQ-SRL module's Terminal Applications menu, which enables you to configure your DSRIQ-SRL 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, 19,200, 34,800, 57,600 or 115,200 bps. The default value is 9600.
- Parity: This option allows you to specify the serial port's communications parity. Available options are EVEN, ODD or NONE. The default value is NONE.

- **Flow Control:** This option allows you to specify the type of serial flow control. Available options are NONE, XOn/XOff (software) and RTS/CTS (hardware). The default value is NONE. If you select a bps rate of 115,200, the only available flow control is RTS/CTS (hardware).
- **DSR/CD Mode:** This option allows you to control how the MergePoint Unity switch and CD lines operate. Available options are Always on and Toggle. When in Toggle mode, DSR and CD lines are turned off for one-half second and then turned on each time a module is selected or deselected. The default value is Always on.
- **Enter Sends:** This option enables you to specify the keys that are transmitted when Enter is pressed. Available options are <CR> (Enter), which moves the cursor to the left side of the screen, or <CR><LF> (Enter-Linefeed), which moves the cursor to the left side of the screen and down one line.
- **Received:** This option enables you to specify how the module translates a received Enter character. Available options are <CR> (Enter) or <CR><LF> (Enter-Linefeed).
- **Background:** This option changes the screen's background color. The currently-selected color displays in the option line as it is changed. Available colors are Black, Light Grey, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon and Brown. The default color is Black. This value cannot be identical to the Normal Text or Bold Text value.
- **Normal Text:** This option changes the screen's normal text color. The currently-selected color displays in the option line as it is changed. Available colors are Grey, Light Grey, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon and Brown. The default color is Grey. This value cannot be identical to the Bold Text or Background value.
- **Bold Text:** This option changes the screen's bold text color. The currently-selected color displays in the option line as it is changed. Available colors are White, Yellow, Green, Teal, Cyan, Blue, Dark Blue, Purple, Pink, Orange, Red, Maroon, Brown and Light Grey. The default color is White. This value cannot be identical to the Normal Text or Background value.
- **Screen Size:** This option allows you to specify the screen's text width size. Available values are widths of 80 columns or 132 columns. The length for both widths is 26 lines.

The following options for the Terminal Application menu's Configuration screen enable you to define the function keys that will perform a selected action. To specify a new function key, press and hold the **Ctrl** key, then press the function key that you want to associate with the

action. For example, if you want to change the Configuration (Config) Key Sequences option from <CTRL-F8> to <CTRL-F7>, press and hold the **Ctrl** key and then press **F7**.

- **Config Key Sequences:** This option allows you to define the key combination that makes the Terminal Application menu's Configuration screen appear. The default key sequence is Ctrl-F8.
- **On-Line Key Sequence:** This option allows you to define the key sequence that displays the On-Line mode. The default key sequence is Ctrl-F10.
- **Help Key Sequence:** This option allows you to define the key combination that displays the Help System screen. The default key sequence is Ctrl-F1.
- **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 DSRIQ-SRL module:

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

-or-

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

Creating a DSRIQ-SRL 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 DSRIQ-SRL module can be configured with up to ten macros. Each macro can be up to 128 characters in length.

To create a macro:

1. Select the DSRIQ-SRL 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 ten available macros and the associated key sequences, if any, for each.
3. Use the Up Arrow and Down Arrow keys to scroll to an available macro number and highlight the listed keystroke sequence. Type the new macro keystroke sequence over the default. Any combination of Ctrl or Alt and a single key may be used. When you have finished entering the keystroke sequence that will activate the new macro, press the **Down Arrow** key.
4. On the line below the macro keystroke sequence you just entered, type the keystroke sequence that you wish the macro to perform.
5. Repeat steps 3 and 4 to configure additional macros.
6. When finished, press **Enter** to return to the previous screen.

Using History mode

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

The DSRIQ-SRL 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 will appear.

- Ctrl-F9: While in Configuration mode, returns to the previous screen with History mode enabled.
- Ctrl-F10: While in Configuration mode, returns to the previous screen with On-Line mode enabled.
- Ctrl-F11: Clears the history buffer. If you choose this option, a warning screen will appear. Press **Enter** to delete the history buffer or **Escape** to cancel the action. The previous screen will reappear.

3. When finished, press **Ctrl-F10** to exit History mode and return to On-Line mode.

DSRIQ-SRL module pinouts

Table B.1 lists the pinouts for the DSRIQ-SRL module.

Table B.1: DSRIQ-SRL 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

Using MPUIQ-SRL Modules

An administrator can choose between the ACS console server and Cisco® pinouts for each MPUIQ-SRL serial port via the local user interface or the remote OBWL. ACS is the default.

To change the pinout to Cisco mode:

1. Select *Unit View - Appliance - Appliance Settings - Ports - RIPs*.
2. Click on the desired RIP.
3. Select *Settings - Pinout*.

NOTE: If the DB9 adaptor is used, select the ACS console server pinouts.

ACS console server port pinouts

The following table lists the ACS console server serial port pinouts for the MPUIQ-SRL module.

Table B.2: ACS Console Server Serial Port Pinouts

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

Cisco port pinouts

The following table lists the Cisco serial port pinouts for the MPUIQ-SRL module.

Table B.3: Cisco Serial Port Pinouts

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

Appendix C: UTP Cabling

This appendix discusses various aspects of connection media. The performance of a MergePoint Unity switching system depends on high quality connections. Poor quality or poorly installed or maintained cabling can diminish MergePoint Unity switching system performance. MergePoint Unity switching systems utilize UTP cabling.

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

UTP copper cabling

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

- CAT 5 UTP (4-pair) high performance cable consists of twisted pair conductors, used primarily for data transmission. The twisting of the pairs gives this cable some immunity from the infiltration of unwanted interference. CAT 5 cable is generally used for networks running at 10 or 100 Mbps.
- CAT 5E (enhanced) cable has the same characteristics as CAT 5, but is manufactured to somewhat more stringent standards.
- CAT 6 cable is manufactured to tighter requirements than CAT 5E cable. CAT 6 has higher measured frequency ranges and significantly better performance requirements than CAT 5E cable at the same frequencies.

Wiring standards

There are two supported wiring standards for 8-conductor (4-pair) RJ-45 terminated UTP cable: EIA/TIA 568A and B. These standards apply to installations utilizing CAT 5, 5E and 6 cable specifications. The MergePoint Unity switching system supports either of these wiring standards. Table C.1 describes the standards for each pin.

Table C.1: UTP Wiring Standards

Pin	EIA/TIA 568A	EIA/TIA 568B
1	white/green	white/orange
2	green	orange
3	white/orange	white/green

Pin	EIA/TIA 568A	EIA/TIA 568B
4	blue	blue
5	white/blue	white/blue
6	orange	green
7	white/brown	white/brown
8	brown	brown

Cabling installation, maintenance and safety tips

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

- Keep all UTP runs to a maximum of 30 feet each.
- Maintain the twists of the pairs all the way to the point of termination, or no more than one-half inch untwisted. Do not skin off more than one inch of the jacket while terminating.
- If bending the cable is necessary, make it gradual with no bend sharper than a one inch radius. Allowing the cable to be sharply bent or kinked can permanently damage the cable's interior.
- Dress the cables neatly with cable ties, using low to moderate pressure. Do not over tighten the ties.
- Cross-connect cables where necessary, using rated punch blocks, patch panels and components. Do not splice or bridge the cable at any point.
- Keep the UTP cable as far away as possible from potential sources of EMI, such as electrical cables, transformers and light fixtures. Do not tie the cables to electrical conduits or lay the cables on electrical fixtures.
- Always test every installed segment with a cable tester. "Toning" alone is not an acceptable test.
- Always install jacks so as to prevent dust and other contaminants from settling on the contacts. The contacts of the jack should face up on the flush mounted plates, or left/right/down on surface mount boxes.

- Always leave extra slack on the cables, neatly coiled in the ceiling or nearest concealed location. Leave at least five feet at the work outlet side and 15 feet at the patch panel side.
- Choose either 568A or 568B wiring standard before beginning. Wire all jacks and patch panels for the same wiring scheme. Don't 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 D: Cable Pinout Information

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

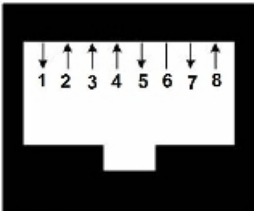


Figure D.1: Modem Jack

Table D.1: Descriptions for Figure D.1

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

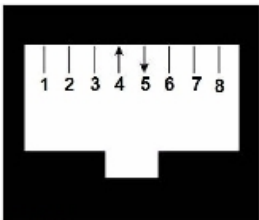


Figure D.2: Console/Setup Jack

Table D.2: Descriptions for Figure D.2

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

Appendix E: Technical Specifications

Table E.1: Technical Specifications

Server Ports	
Number	MPU8032DAC/8032/4032DAC/4032/2032DAC/2032: 32
	MPU2016DAC/2016/1016DAC/1016: 16
	MPU108EDAC/108E: 8
	MPU104E: 4
Type	PS/2, Sun, USB and Serial
Connectors	8-pin modular
Sync Types	Separate horizontal and vertical
Input Video Resolution	Standard
	640 x 480 @ 60 Hz
	800 x 600 @ 75 Hz
	960 x 700 @ 75 Hz
	1024 x 768 @ 75 Hz
	1280 x 1024 @ 75 Hz
	1600 x 1200 @ 60 Hz
	Wide-screen
	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
Supported Cabling	4-pair UTP CAT 5 or CAT 6, 45 meters maximum length
Dimensions	

Form Factor	1 U-rack, mountable
16 and 32 port models	1.72 x 17.00 x 13.38 (Height x Width x Depth)
4 and 8 port models	1.72 x 17.00 x 11.00 (Height x Width x Depth)
Weight (without cables)	MPU8032DAC: 8.6 lbs
SETUP Port	
Number	1
Type	RS-232 serial
Connector	8-pin modular
Local Port (4 and 8 port)	
Number/Type	1 VGA/4 USB
Local Port (16 and 32 port)	
Number/Type	1 VGA/1 USB
Network Connection	
Number	2
Type	10/100/1000 Ethernet
Connector	8-pin modular
USB Device Port	
Number	4 (4 port), 8 (8 port) or 5 (16 and 32 port)
Type	USB 2.0
MODEM Port	
Number	1
Type	RS-232 serial

Connectors	8-pin modular
PDU Port	
Number	2
Type	RS-232 serial
Connector	8-pin modular
Power Specifications	
Connectors	2 devices: MPU8032DAC/4032DAC/2032DAC/2016DAC/ 1016DAC/108EDAC 1 device: MPU8032/4032/2016/1016/108E/104E
Type	Internal
Power	MPU8032DAC/8032: 24W
	MPU4032DAC/4032: 18W
	MPU2032DAC/2032: 17W
	MPU2016DAC/2016: 15W
	MPU1016DAC/1016: 14W
	MPU108EDAC/108E: 13W
	MPU104E: 12W
Heat Dissipation	MPU8032DAC/8032: 82 BTU/hr
	MPU4032DAC/4032: 62 BTU/hr
	MPU2032DAC/2032: 57 BTU/hr
	MPU2016DAC/2016: 47 BTU/hr
	MPU1016DAC/1016: 45 BTU/hr
	MPU108EDAC/108E: 43 BTU/hr
	MPU104E: 39 BTU/hr

AC Input Range	100 - 240 VAC
AC Frequency	50 - 60 Hz auto-sensing
AC Input Current Rating	1.25 A
AC Input Power (maximum)	40 W
Ambient Atmospheric Condition Ratings	
Temperature	32 to 122 degrees Fahrenheit (0 to 50 degrees Celsius) operating; -4 to 158 degrees Fahrenheit (-20 to 70 degrees Celsius) non-operating
Humidity	Operating: 20% to 80 % relative humidity (non-condensing) Non-operating: 5% to 95% relative humidity, 38.7 degrees C maximum wet bulb temperature
Safety and EMC Standards Approvals and Markings	UL, FCC, cUL, ICES-003, CE, VCCI, KCC, C-Tick, GOST Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.

Appendix F: Sun Advanced Key Emulation

Certain keys on a standard Type 5 (US) Sun keyboard can be emulated by key press sequences on a PS/2 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 Table F.1 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 DSRIQ-SRL module (if your Sun system comes with a USB port) as well as the Sun VSN and WSN 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 F.1: Sun Key Emulation

Sun Key (US)	PS/2 Key to Enable Sun Key Emulation
Compose	Application ⁽¹⁾
Compose	keypad
Power	F11
Open	F7
Help	Num Lock
Props	F3
Front	F5
Stop	F1
Again	F2
Undo	F4
Cut	F10
Copy	F6
Paste	F8

Sun Key (US)	PS/2 Key to Enable Sun Key Emulation
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)

(1)Windows 95 104-key keyboard. (2)The Command key is the Sun Meta (diamond) key.

Special considerations for Japanese Sun USB and Korean Sun USB keyboards (USB IQ modules only)

Japanese Sun USB and Korean Sun USB keyboards assign usage IDs for certain keys that differ from standard USB usage IDs. If USB IQ modules are attached to your Sun servers, the Han/Zen and Katakana/Hiragana keys on Japanese Sun USB keyboards and Hangul and Hanja keys on Korean Sun USB keyboards must be accessed using alternate keystrokes.

Due to these keyboard-specific differences, keyboard mapping inconsistencies may be encountered when switching between target devices using Sun VSN and WSN IQ modules and target devices using USB IQ modules. These keys function normally if your Sun servers are attached to the MergePoint Unity switch using a VSN or WSN IQ module.

Table F. 2 lists the keyboard mapping that will take place when a USB IQ module is used in this setting.

Table F.2: PS/2-to-USB Keyboard Mappings

PS/2 Keyboard	USB Usage ID	Sun USB Keyboard	Korean Sun USB Keyboard	Japanese Sun USB Keyboard
Right-Alt	0xE6	AltGraph	Hangul	Katakana/Hiragana
Windows Application	0x65	Compose	Hanja	Compose
Hangul	0x90	N/A	N/A	N/A

PS/2 Keyboard	USB Usage ID	Sun USB Keyboard	Korean Sun USB Keyboard	Japanese Sun USB Keyboard
Hanja	0x91	N/A	N/A	N/A
Katakana/Hiragana	0x88	N/A	N/A	Han/Zen
Han/Zen	0x35			N/A

Appendix G: Technical Support

Our Technical Support staff is ready to assist you with any installation or operational issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Visit www.avocent.com/support and use one of the following resources:

Search the knowledge base or use the online service request

-or-

Select *Technical Support Contacts* to find the Avocent Technical Support location nearest you.



For Technical Support:

www.avocent.com/support