Avocent® MergePoint Unity™ KVM over IP and Serial Console Switch

Installer/User Guide

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

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

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

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit https://www.vertiv.com/en-us/support/ for additional assistance.

Proprietary and Confidential ©2026 Vertiv Group Corp.

TABLE OF CONTENTS

1 Getting Started **1**
1.1 Product Overview 1
1.2 Features and Benefits 1
1.2.1 Reduce cable bulk 1
1.2.2 KVM switching capabilities 1
1.2.3 True serial capabilities 2
1.2.4 Local and remote user interfaces 2
1.2.5 Control of virtual media and smart card-capable appliances 2
1.2.6 Access the switch via a standard TCP/IP network 3
1.2.7 FIPS cryptographic module 3
1.2.8 Vertiv™ Avocent® DSView™ 4.5 management software plug-in 3
1.3 Materials and Supplies 4
1.4 Switch Connectivity 4
1.5 Product Security 7
2 Installation and Initial Setup **9**
2.1 Setting Up the Network 9
2.2 Rack Mounting the Switch 9
2.2.1 Safety considerations 9
2.3 Connecting the Switch Hardware 10
2.3.1 Connecting and turning on the switch 10
2.3.2 Connecting virtual media and a smart card reader 11
2.3.3 Connecting IQ modules 11
2.4 Cascading Switches 12
2.5 Configuring the Switch 12
2.5.1 Setting up the built-in web server 12
2.5.2 Connecting to the OBWI through a firewall 12
2.6 Verifying the Connections 14
2.6.1 Checking the status of the switch 14
2.6.2 Checking the status of IQ and DSRIQ-SRL modules 14
2.7 Adjusting Mouse Settings on Target Devices 15
3 Local and Remote Configurations **17**
3.1 General Settings 19
3.2 Target List 20
3.2.1 Viewing and managing target devices 20
3.2.2 Filtering the target list 20
3.3 System Information 21
3.4 Appliance Tools 21
3.4.1 Rebooting the switch 22

3.4.2 Running diagnostics ... 22
3.4.3 Saving/restoring the appliance configuration ... 22
3.4.4 Saving/restoring the appliance user database ... 23
3.4.5 Exporting/importing target device configurations ... 24
3.4.6 Resetting the appliance configuration to factory defaults ... 24
3.4.7 Managing the appliance web certificate ... 24
3.4.8 Upgrading the firmware ... 25
3.4.9 Pinging the network ... 26
3.4.10 Saving the trap MIB ... 26
3.5 Network Settings ... 26
3.6 DNS Settings ... 27
3.7 SNMP Settings ... 27
3.8 Auditing ... 28
3.8.1 Enabling events ... 28
3.8.2 Configuring event destinations ... 28
3.9 Ports ... 28
3.9.1 Configuring IQ modules ... 28
3.9.2 Configuring power devices ... 29
3.9.3 Configuring local UI settings ... 30
3.9.4 Configuring modem settings ... 32
3.10 Sessions ... 32
3.10.1 Launching a session ... 32
3.10.2 Configuring a session ... 32
3.10.3 Closing a session ... 34
3.11 User Accounts ... 34
3.11.1 Managing local user accounts ... 34
3.11.2 Managing Vertiv™ Avocent® DSView™ 4.5 software user accounts ... 35
3.11.3 Configuring the LDAP settings ... 36
4 KVM Video Viewer ... 43
4.1 Supported Session Types ... 43
4.2 Performance Errors ... 43
4.3 Java Versions ... 44
4.4 KVM Session Configurations ... 44
4.5 Profile Settings ... 44
4.6 Macros ... 46
4.6.1 Global macros ... 47
4.6.2 Macro groups ... 47
4.6.3 Macros configuration ... 48
4.7 Virtual Media ... 49
4.7.1 Requirements ... 49

Proprietary and Confidential ©2026 Vertiv Group Corp.

4.7.2 Image creation 50
4.8 Session Options 50
4.8.1 General 50
4.8.2 Mouse synchronization 51
4.8.3 Certificate 52
4.8.4 Automatic video adjust 52
4.8.5 Manual video adjustment 52
4.8.6 Cursor commands 53
4.8.7 Stats 53
4.9 Power Control 53
4.10 Smart Cards 54
4.11 Video Recording 54
4.11.1 Continuous recording 54
4.11.2 Persistent recording 54
4.11.3 Exporting video 55
4.12 KVM Session Optimization 56
Appendices 57
Appendix A: Technical Specifications 57
Appendix B: Terminal Operations 61
Appendix C: Using Serial IQ Modules 63
Appendix D: UTP Cabling 69
Appendix E: Cable Pinout Information 71
Appendix F: Sun Advanced Key Emulation 73
Appendix G: Local UI Keyboard Shortcuts 75

This page intentionally left blank

Proprietary and Confidential ©2026 Vertiv Group Corp.

1 Getting Started

1.1 Product Overview

The Vertiv Avocent MergePoint Unity switch combines analog and digital technology to provide flexible, centralized control of data center servers and virtual media, and to facilitate the operations, activation and maintenance of remote branch offices where trained operators may be unavailable. The IP-based switch provides flexible target device management control and secure remote access from anywhere at anytime. This document supports versions up to and including release 1.30.

1.2 Features and Benefits

The Vertiv Avocent MergePoint Unity switch offers the following features and benefits for enterprise customers:

- 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 accessible 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

1.2.1 Reduce cable bulk

With server densities continually increasing, cable bulk remains a major concern for network administrators. The Vertiv Avocent 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.

1.2.2 KVM switching capabilities

The Vertiv Avocent 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 tables displays the IQ modules supported by the switch and highlights which modules support virtual media and smart card capabilities.

Proprietary and Confidential ©2026 Vertiv Group Corp.

Table 1.1 Supported IQ Modules

Module	Virtual-Media Capable?	Smart-Card Capable?
DSRIQ-PS2	No	No
DSRIQ-USB	No	No
DSRIQ-VMC	Yes	Yes
DSRIQ-SUN	No	No
DSAVIQ-USB2	Yes	No
DSVAIQ-PS2M	Yes	No
MPUIQ-VMC	Yes	Yes
MPUIQ-VMCHS	Yes	Yes
MPUIQ-VMCHD	Yes	Yes
MPUIQ-VMCDP	Yes	Yes
MPUIQ-VMCDV	Yes	Yes

1.2.3 True serial capabilities

The Vertiv Avocent 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 switch's attached target devices that have an MPUIQ-SRL module.

1.2.4 Local and remote user interfaces

For local access to the switch, you can connect directly to the 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. For remote access, you can launch the remote, web-based OBWI directly from the switch; any servers connected to the switch are automatically detected. Refer to the latest product release notes on the Vertiv™ Avocent® MergePoint Unity™ Software Downloads page to ensure your operating system and/or browser is supported by the OBWI. While different in accessibility, the two user interfaces share a similar look and feel for an optimal user experience. For information about configuring the interfaces, refer to Local and Remote Configurations on page 17.

From the interfaces, you can launch two different kinds of sessions:

- KVM Video Viewer: Allows you to control the keyboard, monitor and mouse functions of individual target devices connected to the Vertiv Avocent 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 KVM Video Viewer on page 43.
- Serial Viewer: Allows you to manage individual target devices by using either commands or scripts.

1.2.5 Control of virtual media and smart card-capable appliances

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

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

Virtual media and smart card readers can be connected directly to the switch via the USB ports located on the switch. Alternatively, virtual media and smart card readers may be connected to any remote workstation that is running the remote OBWI or Vertiv™ Avocent® DSView™ 4.5 management software and is connected to the Vertiv Avocent MergePoint Unity switch using an Ethernet connection.

NOTE: The Vertiv Avocent MergePoint Unity switch supports versions prior to and including Vertiv™ Avocent® DSView™ 4.5 management software.

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.

1.2.6 Access the switch via a standard TCP/IP network

The Vertiv Avocent 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 uses an Internet browser to connect to the server hosting the Vertiv™ Avocent® DSView™ 4.5 management software.

Users access the Vertiv Avocent 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.

1.2.7 FIPS cryptographic module

The Vertiv Avocent MergePoint Unity switch follows the guidelines set forth by the FIPS 140-2 program. 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. The Setup port factory default setting will automatically disable the FIPS module. The FIPS mode cannot be changed via the Vertiv™ Avocent® DSView™ 4.5 management software plug-in.

The Vertiv Avocent MergePoint Unity switch uses an embedded cryptographic module that is based on the FIPS 140-2 validated cryptographic module (certificate number 1747) running on a Linux PPC platform.

1.2.8 Vertiv™ Avocent® DSView™ 4.5 management software plug-in

The management software may be used with the Vertiv Avocent 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 Vertiv™ Avocent® DSView™ 4.5 Management Software Plug-In for Vertiv™ Avocent® MergePoint Unity™ Switches Technical Bulletin.

Proprietary and Confidential ©2026 Vertiv Group Corp.

1.3 Materials and Supplies

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

Supplied with the Vertiv Avocent MergePoint Unity switch:

- Rack mount bracket kit
- Vertiv™ Avocent® KVM Switch Rack Mount Kit Quick Installation Guide
- Vertiv™ Avocent® MergePoint Unity™ Switch Quick Installation Guide
- Safety and Regulatory Statements Guide
- Cables and adapters for the MODEM and SETUP ports
- AC power cord(s)

Additional items needed:

- One 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) Vertiv™ Avocent® DSView™ 4.5 Management Software
- (Optional) V.34, V.90 or V.92-compatible modem and cables
- (Optional) Power control device(s)

1.4 Switch Connectivity

A Vertiv Avocent 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. For instructions on configuring switch connectivity, refer to Setting Up the Network on page 9.

Ethernet Connections

The switch utilizes the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication over Ethernet. Although 10BaseT Ethernet may be used, Vertiv recommends a dedicated, switched 100BaseT or 1000BaseT network for switches that support it.

Modem Connections

The switch utilizes 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 On-Board User Interface (OBUI) or the Vertiv™ Avocent® DSView™ 4.5 management software. For more information about the management software, visit http://www.Vertiv.com or see the Vertiv™ Avocent® DSView™ 4.5 Management Software Installer/User Guide.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

Figure 1.1 Basic Configuration of the Vertiv™ Avocent® MergePoint Unity™ Switch

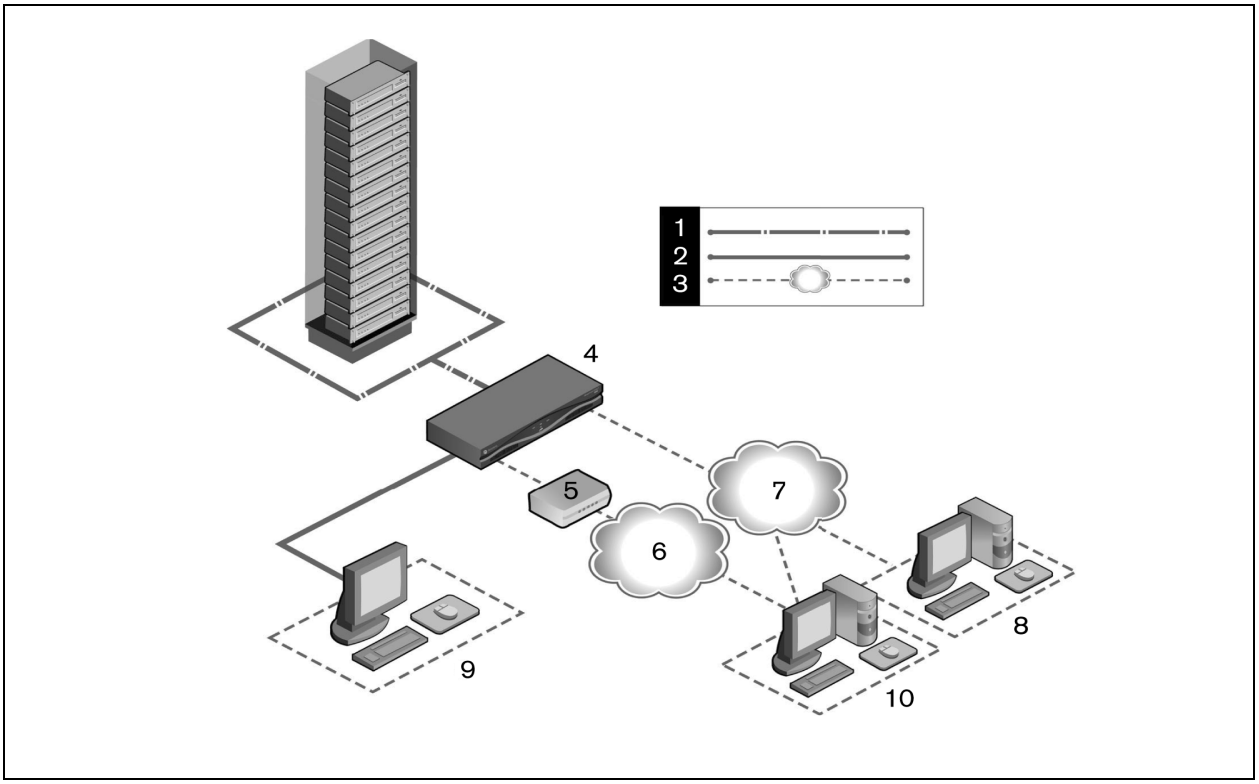


Table 1.2 Basic Configuration of the Vertiv™ Avocent® MergePoint Unity™ Switch Descriptions

Item	Description	Item	Description
1	CAT5 connection	6	Telephone network
2	KVM connection to the switch	7	Ethernet
3	Remote IP connection	8	Vertiv™ Avocent® DSView™ 4.5 management software server
4	Vertiv Avocent MergePoint Unity switch	9	Analog user (local UI)
5	Modem	10	Digital user (computer with Internet browser, remote OBWI)

Proprietary and Confidential ©2026 Vertiv Group Corp.

The following illustrates basic connections for the switch, using the Vertiv Avocent MergePoint Unity switch 8032 model for the example.

Figure 1.2 Example Configuration of the Vertiv™ Avocent® MergePoint Unity™ Switch 8032 Model

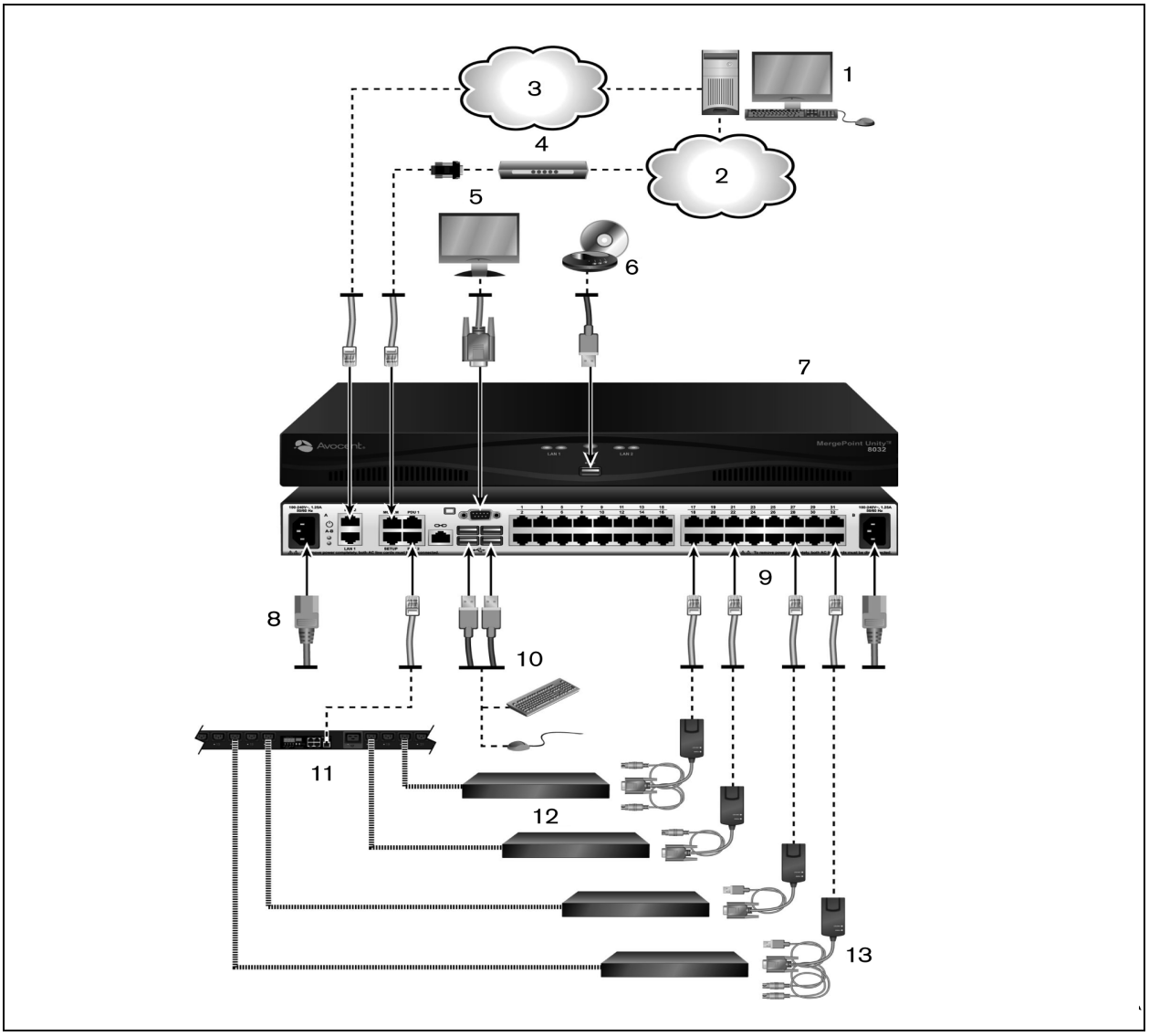


Table 1.3 Example Configuration of the Vertiv™ Avocent® MergePoint Unity™ Switch 8032 Model Descriptions

Item	Description	Item	Description
1	Digital user	8	Power cord
2	Telephone network	9	Ports 1-32
3	Network	10	Local USB connections
4	Modem	11	Power control device
5	Analog user	12	Target devices 1-32
6	External virtual media	13	IQ modules (PS/2, USB, VMC, Sun and serial are available)
7	Vertiv Avocent MergePoint Unity switch 8032 model		

1.5 Product Security

This product is designed and intended to be deployed and operated in a physically secure and network firewall-protected location. To ensure the highest security standards, the Vertiv Avocent MergePoint Unity switch must be deployed exclusively within firewall-protected data center infrastructure. Under no circumstances should the switch be connected to unsecured or public networks, as this could pose significant security risks.

For optimal security:

- Deploy the device only within firewall-protected data center infrastructure.
- Enable Local Port User Authentication
- Ensure the device always remains within physically secured areas.
- Maintain strict access control protocols to limit who can interact with the device.

A noteworthy feature of the system is its local user interface (UI). Local Port User Authentication may be enabled to require users to log in with valid credentials at the local UI. If you need assistance, you can easily contact Technical Support by clicking the *Forgot Password?* link that appears when user credentials are rejected at the local port.

IMPORTANT! Connecting this device to unsecured networks may expose critical infrastructure to security risks and is not supported.

Proprietary and Confidential ©2026 Vertiv Group Corp.

This page intentionally left blank

Proprietary and Confidential ©2026 Vertiv Group Corp.

2 Installation and Initial Setup

2.1 Setting Up the Network

The Vertiv Avocent MergePoint Unity switching system uses IP addresses to uniquely identify the switch and the target devices. The switch family supports both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. It is recommended 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 switch using the Vertiv™ Avocent® DSView™ 4.5 management software, and for information on how the switch uses TCP/IP, see the Vertiv™ Avocent® DSView™ 4.5 Management Software Installer/User Guide located on http://www.Vertiv.com.

2.2 Rack Mounting the Switch

A rack mounting kit is supplied with each Vertiv Avocent MergePoint Unity switch. The switch may either be placed on the rack shelf or mounted directly into an Electronic Industries Alliance (EIA) standard rack. Most Vertiv Avocent MergePoint Unity switches can be rack mounted in a 1U configuration.

NOTE: 0U configurations are not supported by the Vertiv Avocent MergePoint Unity switch family.

2.2.1 Safety considerations

Before installing the KVM switch rack mount, review the following safety considerations:

WARNING! 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.

CAUTION: 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.

CAUTION: If installed in a closed rack assembly, the operating temperature of the rack environment may be greater than room ambient temperature. Use care not to exceed the rated maximum ambient temperature of the switch.

CAUTION: Install the equipment in the rack so that the amount of airflow required for safe operation of the equipment is not compromised.

CAUTION: 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).

 Proprietary and Confidential ©2026 Vertiv Group Corp.

For complete instructions on installing the rack mounting bracket, please refer to the Vertiv™ KVM Switch Rack Mount Kit Quick Installation Guide shipped with your product. It can also be found on the product page on http://www.Vertiv.com.

2.3 Connecting the Switch Hardware

Before connecting the Vertiv Avocent MergePoint Unity switch hardware, review the following considerations:

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

NOTE: To avoid potential video and/or keyboard problems when using Vertiv™ 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. To remove power completely for products that have more than one AC inlet, all AC line cords must be disconnected.**
- **This product has no user serviceable parts inside the product enclosure. Do not open or remove the product cover.**

2.3.1 Connecting and turning on the switch

To connect and turn on your Vertiv Avocent MergePoint Unity switch:

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. Otherwise, the keyboard will not initialize properly.
2. Choose an available port on the switch. Plug one end of a CAT5 cable (4-pair, up to 150 ft/45 m) into a numbered port. Plug the other end into an RJ45 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 CAT5 cable from the Ethernet network into a LAN port on the back of the switch. Network users will access the switch through this port.
5. (Optional) The switch may also be accessed using an ITU V.92, V.90 or V.24-compatible modem. Plug one end of an RJ45 cable into the MODEM port on the switch. Plug the other end into the RJ45 to DB9 (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 Vertiv Avocent MergePoint Unity switch.

6. (Optional) Plug one end of the RJ45 cable supplied with the Power Distribution Unit (PDU) into the PDU1 port on the switch. Using the supplied RJ45 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 provided with the switch. Plug one end of the power cord into the power socket on the rear of the 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 switch and plug the other end into an appropriate AC wall outlet.

2.3.2 Connecting virtual media and a smart card reader

To connect local virtual media or a smart card reader:

For local connections, the virtual media or smart card reader should be connected to an available USB port of the Vertiv Avocent MergePoint Unity switch. All virtual media sessions require the use of a DSAVIQ-USB2, DSAVIQ-PS2M, DSRIQ-VMC or MPUIQ-VMC module. All smart card readers require a DSRIQ-VMC or MPUIQ-VMC module.

For information on connecting virtual media remotely, see Virtual Media on page 49. For information on connecting a smart card reader remotely, see Smart Cards on page 54.

2.3.3 Connecting IQ modules

NOTE: Attaching the MPUIQ-VMC or DSRIQ-VMC module to a Windows target may require the USB CCID driver to be installed. If you are prompted by the Windows New Hardware Wizard, select the Next button.

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 switch.
2. Attach one end of the UTP patch cable to the RJ45 connector on the DSRIQ-SRL module. Connect the other end of the UTP patch cable to the desired port on the back of your 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 63.

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

1. Attach the MPUIQ-SRL module CAT5 connector to the serial device.
2. (Optional) Attach the MPUIQ-SRL module to an RJ45 to 9-pin female adaptor. Attach the adapter to the serial port of the serial device.
3. Plug one end of a CAT5 cable (4-pair, up to 150 ft/45 m) into an available numbered port on the rear of the switch. Plug the other end into the RJ45 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.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

NOTE: The cable expander cannot be used with the USB-to-barrel power cord. Multiple MPUIQ modules can use power from the power supply but not from 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.

2.4 Cascading Switches

You can cascade up to two levels of Vertiv Avocent MergePoint Unity switches, enabling users to connect to a maximum of 1,024 servers. In a cascaded system, each target port on the main switch will connect to the ACI port on each cascaded switch. Each cascaded switch can then be connected to a server with an IQ module. Once connected, the system will automatically "merge" the two switches. All servers connected to the cascaded switch will display on the main switch server list in the local UI.

NOTE: The Vertiv Avocent 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 Vertiv Avocent MergePoint Unity switch.

To cascade multiple Vertiv Avocent MergePoint Unity switches:

1. Attach one end of a CAT5 cable to a target port on the switch.
2. Connect the other end of the CAT5 cable to the ACI port on the back of your cascaded switch.
3. Connect the devices to your cascaded switch.
4. Repeat these steps for all the cascaded switches you wish to attach to your system.

2.5 Configuring the Switch

Once all physical connections have been made, you must configure the switch to be used in the overall switching system. This can be accomplished via the Vertiv™ Avocent® DSView™ 4.5 management software or the local UI.

To configure the switch using the management software:

Refer to the Vertiv™ Avocent® DSView™ 4.5 Management Software Installer/User Guide on http://www.Vertiv.com for detailed instructions.

To configure the switch using the local UI:

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

2.5.1 Setting up the built-in web server

You can access the Vertiv Avocent 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, specify an IP address through the SETUP port on the back panel of the switch or local UI. For detailed instructions on navigating the user interface for switching, refer to Local and Remote Configurations on page 17.

2.5.2 Connecting to the OBWI through a firewall

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

Table 2.1 TCP Ports and Functions for the Vertiv™ Avocent® 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 Vertiv™ Video Viewer (for downloading the Java applet)
443	Used by the web browser interface for managing the switch and launching KVM and HTML5 serial sessions
2068	Transmission of KVM session data (mouse and keyboard) or transmission of video on Vertiv Avocent MergePoint Unity switches
4206	Used by the web browser interface for managing the switch and launching HTML5 KVM sessions

In a typical configuration, as shown in Figure 2.1 below, the user's computer is located outside of the firewall, and the switch resides inside the firewall.

Figure 2.1 Typical Firewall Configuration for the Vertiv™ Avocent® MergePoint Unity™ Switch Firewall Configuration

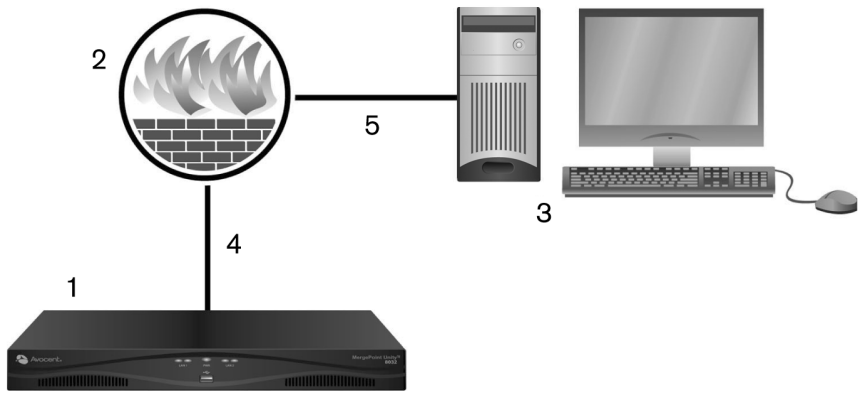


Table 2.2 Typical Firewall Configuration for the Vertiv™ Avocent® MergePoint Unity™ Switch Firewall Configuration Descriptions

Item	Description
1	Vertiv Avocent MergePoint Unity switch
2	Firewall
3	User's computer
4	Firewall forwards HTTP requests and KVM traffic to the switch
5	User browses to firewall's external IP address

 Proprietary and Confidential ©2026 Vertiv Group Corp.

To configure the firewall:

To access the Vertiv Avocent 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 Local and Remote Configurations on page 17.

2.6 Verifying the Connections

2.6.1 Checking the status of the switch

The Vertiv Avocent MergePoint Unity switch includes several LED indicators on the front and rear panel to indicate the Ethernet and power status of the switch.

Table 2.3 LED Status Descriptions

LED	Status	Description
Front and Rear Panel Ethernet (LAN) Connection Status		
LED 1	Green, Solid	Indicates a valid network connection has been established.
	Green, Blinking	Indicates there is activity on the port.
LED 2	Green, Solid	Indicates the communication speed is 1000M.
	Amber, Solid	Indicates the communication speed is 100M.
	Off	Indicates the communication speed is 10M.
Front Panel Power Status		
LED 1	Green, Solid	Indicates the switch is turned on and operating normally, with a single power supply.
	Green, Blinking	Indicates the switch is booting or an upgrade is in progress.
	Amber, Solid	Indicates a fault condition has occurred, such as power supply failure (for switches equipped with dual power supplies), elevated ambient temperature or fan failure. The LED continues blinking until the issue is resolved.
Rear Panel Power Status		
LED 1	Green, Solid	Indicates the switch is turned on and operating normally, with a single power supply.
	Green, Blinking	Indicates the switch is booting or an upgrade is in progress.
LED 2*	Green, Solid	Indicates the switch is turned on and operating normally, with dual power supplies.
	Amber, Solid	Indicates a fault condition has occurred, such as power supply failure (for switches equipped with dual power supplies), elevated ambient temperature or fan failure. The LED continues blinking until the issue is resolved.
* Only switches equipped with dual power supplies have two power LEDs on the rear panel.		

2.6.2 Checking the status of IQ and DSRIQ-SRL modules

Typically, IQ modules feature two green LEDs: a Power LED and a Status LED.

- Power LED - Indicates the attached module is turned on.
- Status LED - Indicates a valid selection has been made to a Vertiv Avocent 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.

2.7 Adjusting Mouse Settings on Target Devices

Before a computer connected to the Vertiv Avocent MergePoint Unity switch can be used for remote user control, review the following information:

- You must either enable Vertiv™ Mouse Sync 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.
- Mouse acceleration set to "none" for all user accounts accessing a remote system through a KVM switch to ensure the local mouse movement and remote cursor display remain synchronized.
- Mouse acceleration must also be set to "none" on every remote system.
- Special cursors should not be used.
- Cursor visibility options, such as pointer trails, Ctrl key cursor location animations, cursor shadowing and cursor hiding, should be turned off.

For more information about setting mouse movement and cursor features for use with Vertiv™ hardware products and Vertiv™ Avocent® DSView™ 4.5 management software, please visit http://www.Vertiv.com and consult the Mouse and Pointer Settings Technical Bulletin.

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 management 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 Vertiv™ Avocent® DSView™ 4.5 management software.

Proprietary and Confidential ©2026 Vertiv Group Corp.

This page intentionally left blank

3 Local and Remote Configurations

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

NOTE: Unless specified, all information in this chapter applies to both interfaces.

NOTE: If the switch has been added to a Vertiv™ Avocent® DSView™ management software server, then the server will be accessed to authenticate the user. If the switch has not been added to a management software server, or if the server cannot be reached, then the switch's local user database will be accessed to authenticate the user. Usernames in the local UI are case sensitive.

Launching the local UI for the first time

1. Connect your monitor, keyboard and mouse cables to the switch. For more information, see Connecting the Switch Hardware on page 10.
2. Press any of these keystrokes to open the local UI:
   - Print Screen
   - Ctrl + Ctrl
   - Shift + Shift
   - Alt + Alt

   For more information about the keystrokes enabled for the local UI, refer to Local UI Keyboard Shortcuts on page 75.
3. By default, the local UI does not require a username or password to log in. To enable local UI authentication, you must first access the remote OBWI and activate this setting. If local UI authentication has been enabled, then enter your username and password.

Launching the OBWI for the first time

For a list of supported operating systems and browsers, refer to the latest product release notes on the Vertiv™ Avocent® MergePoint Unity™ Software Downloads page.

1. Open a web browser and enter the IP address or host name assigned to the switch you wish to access. Use one of the following formats: https://xxx.xx.xx.xx or https://hostname

NOTE: If using IPv6 mode, add square brackets around the IP address. For example, https://[<ipaddress>]

NOTE: If logging into the OBWI from outside a firewall, enter the external IP address of the firewall instead.

2. When the browser makes contact with the switch, enter the default username Admin.
3. When prompted, create and confirm a password.
4. Click *Login*. The OBWI opens.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

Navigating the user interface

After logging into the switch, the user interface opens. Through the user interface, you may view, access and manage your Vertiv Avocent MergePoint Unity switch, as well as specify system settings and change profile settings. The following figure and table indicate the key areas of the user interface for the switch.

Figure 3.1 User Interface Window

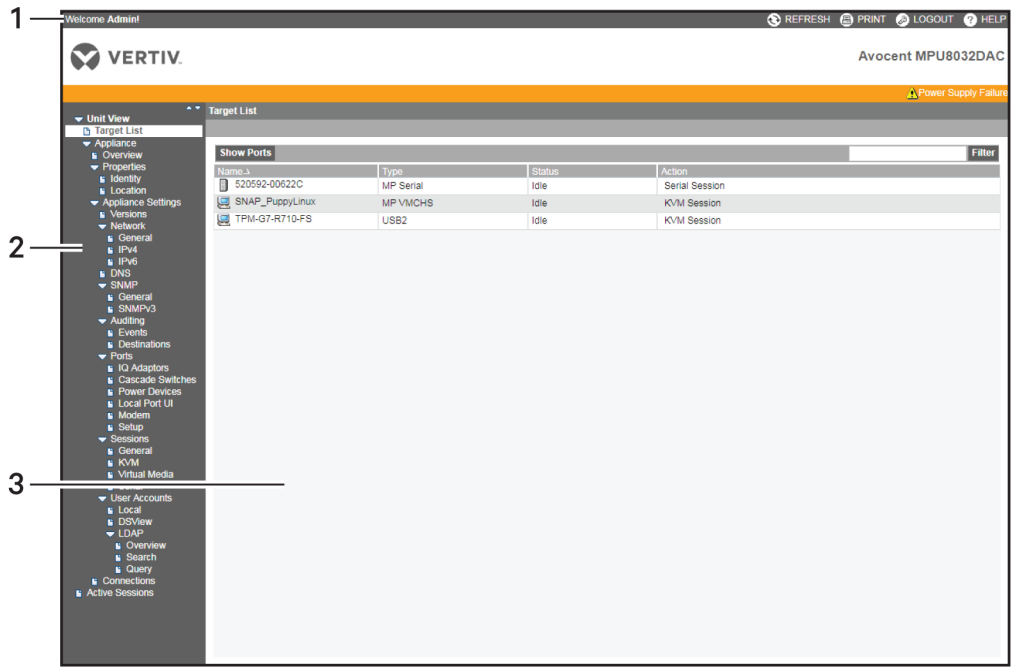


Table 3.1 User Interface Window Descriptions

Number	Description	Function
1	Top Option Bar (General Settings)	Use the top option bar to perform the following functions: • Bookmark an interface window • Refresh the display of an interface window • Print a web page • Log out of a software session • Access the Vertiv™ Technical Support help page. The name of the logged-in user appears on the left side of the top option bar. For more information, refer to General Settings on the facing page.
2	Side Navigation Bar	Use the side navigation bar to display the system information you wish to view or edit in the content area. The two main menu items are Unit View and Active Sessions. • Unit View: Contains several sub-menu items, in which you can specify settings or perform operations. • Active Sessions: Displays a list of the active sessions for the switch.
3	Content Area	Use the content area to display or make changes to the switch OBWI system.

3.1 General Settings

The general settings described in this section can be accessed from the top option bar of the user interface. The top option bar allows you to choose from Refresh, Print, Logout and Help.

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

Refresh

Click the *Refresh* button to refresh the user interface screen.

Print

Click the *Print* option to print any OBWI window.

Logout

Click the *Logout* button to log out of the switch system.

Help

Click the *Help* button to view a digital copy of the Vertiv™ Avocent® MergePoint Unity™ KVM over IP and Serial Console Switch Installer/User Guide.

Bookmark

NOTE: This feature is available only for Microsoft Internet Explorer browsers.

Click the *Bookmark* button or the bookmark icon to add a link to the window in the Favorites drop-down menu of your browser. This action provides quick access to the bookmarked window. If you bookmark a window and information related to the window changes, this new information will appear in the window when you next display the bookmarked window. If you click *Bookmark* or the bookmark icon after the switch OBWI session has timed out, the User Login window will open and you must log in again.

To bookmark a window:

1. From the top option bar, click *Bookmark* or the bookmark icon. The Add Favorite dialog box appears.
2. If desired, 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.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

3.2 Target List

From the Target List screen, you can access, manage, and filter the list of target devices.

3.2.1 Viewing and managing target devices

From the side navigation bar of the local UI, you can view and manage attached target devices from either of the following screens:

- Target List - Basic: Recommended for less than 20 targets.
- Target List - Full: Recommended for more than 20 targets as it allows you to sort through targets using various navigation tools.

Either the Basic or Full screens can be set as the default screen for selecting target devices.

From the side navigation bar of the OBWI, you can view and manage attached target devices from the Target List screen.

3.2.2 Filtering the target list

You can filter the list of target devices by providing a text string that will be used to retrieve matching items. Filtering can provide a shorter, more exact list of items. When filtering is performed, the Name column is searched for the specified text string. The search is not case sensitive.

To filter the list of target devices:

1. From the side navigation bar, click *Unit View - Target List*.
2. In the text bar in the right corner, enter your text string. If desired, you may use an asterisk (*) before or after the text string as a wildcard. For example. typing **emailserver*** and clicking *Filter* will display items with emailserver at the beginning (such as emailserver, emailserverbackup).
3. Click the *Filter* button. The target list is updated based on your filtered search.

3.3 System Information

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

Table 3.2 System Information

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

Additionally, you will be alerted if any of the following fault conditions occur:

- Power supply failure (for Vertiv Avocent MergePoint Unity switches equipped with dual power supplies)
- Elevated ambient temperature
- 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. Click on the notification to get more information.

3.4 Appliance Tools

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

- Rebooting the switch
- Running diagnostics
- Saving/restoring the appliance configuration
- Saving/restoring the appliance user database
- Exporting/importing target device configurations
- Managing the appliance web certificate
- Upgrading the firmware
- Pinging the network
- Saving the trap MIB

 Proprietary and Confidential ©2026 Vertiv Group Corp.

3.4.1 Rebooting the switch

To reboot the Vertiv Avocent MergePoint Unity switch:

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

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

3.4.2 Running diagnostics

You can run a diagnostics test on your switch. When you run the diagnostics, the LAN connections are tested, online and offline IQ modules are identified and suspect devices are detected. Suspect devices are devices attached to the switch that are the wrong brand for the appliance.

3.4.3 Saving/restoring the appliance configuration

NOTE: You can only save and restore appliance configurations when using the remote OBWI.

You can save the configuration of a Vertiv Avocent MergePoint Unity switch to a file. The configuration file will contain information about the managed appliance.

To save the configuration of a managed appliance:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Save Appliance Configuration*.
3. Select the radio button to use one of the following methods to download the configuration file: Filesystem, TFTP, FTP or HTTP PUT.
   a. If you selected TFTP, enter the Server and Filename information.

      -or-

   b. If you selected FTP or HTTP PUT, enter the Server, Username, Password and Filename information.
4. Enter an encryption password in the Encryption Password field.
5. Click *Download* in the top right corner. The configuration of the managed appliance downloads to the specified location.

After saving a file for the configuration of a managed appliance, you may also restore a previously-saved configuration file to a Vertiv Avocent MergePoint Unity switch.

To restore a previous configuration of a managed appliance:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Restore Appliance Configuration*.
3. Select the radio button to use one of the following methods to upload the configuration file: Filesystem, TFTP, FTP or HTTP PUT.
   a. If you selected Filesystem, click Choose File and browse to the configuration file.

      -or-

   b. If you selected TFTP, enter the Server and Filename information.

-or-

c. If you selected FTP or HTTP, enter the Server, Username, Password and Filename information.

4. Enter the decryption password in the Decryption Password field.
5. Click the *Upload* button in the top right corner.
6. After the success screen appears, click *Close*. Reboot the managed appliance to enable the restored configuration. See Rebooting the switch on the previous page.

3.4.4 Saving/restoring the appliance user database

NOTE: You can only save and restore appliance user databases when using the remote OBWI.

You can also save the local user database on a Vertiv Avocent MergePoint Unity switch.

To save the local user database of a managed appliance:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Save Appliance User Database*.
3. Select the radio button to use one of the following methods to download the configuration file: Filesystem, TFTP, FTP or HTTP PUT.
   a. If you selected TFTP, enter the Server and Filename information.

   -or-

   b. If you selected FTP or HTTP PUT, enter the Server, Username, Password and Filename information.
4. Enter an encryption password in the Encryption Password field.
5. Click *Download* in the top right corner. The local user database of the managed appliance downloads to the specified location.

After saving a file for the local user database of a managed appliance, you may also restore a previously-saved user database file to a Vertiv Avocent MergePoint Unity switch.

To restore a previous user database of a managed appliance:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Restore Appliance User Database*.
3. Select the radio button to use one of the following methods to upload the configuration file: Filesystem, TFTP, FTP or HTTP PUT.
   a. If you selected Filesystem, click Choose File and browse to the configuration file.

   -or-

   b. If you selected TFTP, enter the Server and Filename information.

   -or-

   c. If you selected FTP or HTTP, enter the Server, Username, Password and Filename information.
4. Enter the decryption password in the Decryption Password field.
5. Click the *Upload* button in the top right corner.
6. After the success screen appears, click *Close*. Reboot the managed appliance to enable the restored configuration. See Rebooting the switch on the previous page.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

3.4.5 Exporting/importing target device configurations

To export the configuration of the target device:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Export Target Device Configuration*.
3. Select the radio button to use one of the following methods to download the configuration file: Filesystem, TFTP, FTP or HTTP PUT.
   a. If you selected TFTP, enter the Server and Filename information.

      -or-

   b. If you selected FTP or HTTP PUT, enter the Server, Username, Password and Filename information.
4. Click *Download* in the top right corner. The configuration of the target device downloads to the specified location.

To import the configuration of the target device:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Import Target Device Configuration*.
3. Select the radio button to use one of the following methods to upload the configuration file: Filesystem, TFTP, FTP or HTTP PUT.
   a. If you selected TFTP, enter the Server and Filename information.

      -or-

   b. If you selected FTP or HTTP PUT, enter the Server, Username, Password and Filename information.
4. Click *Upload* in the top right corner. The configuration of the target device uploads from the specified location.

3.4.6 Resetting the appliance configuration to factory defaults

To reset the switch's configuration to factory defaults:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Reset Appliance Configuration to Factory Defaults*. A warning message appears: *Resetting the appliance will cause any active sessions to be disconnected, and ALL settings to be reset on the appliance. Do you want to continue with this operation?*
3. Click *OK*. The switch reverts back to its factory default settings.

3.4.7 Managing the appliance web certificate

To update the switch's web certificate:

NOTE: Uploaded certificates must be in OpenSSL PEM format with an unencrypted private key.

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Manage Appliance Web Certificate*.
3. Click the *Update* button in the top right corner.
4. To generate a new self-signed certificate, click the corresponding radio button, and then enter the information in the provided fields.

   -or-

To upload a new certificate, click the corresponding radio button, and then select the radio button to use one of the following methods to upload the file: Filesystem, TFTP, FTP or HTTP PUT.

a. If you selected Filesystem, click *Choose File* and browse to the new certificate.

   -or-

b. If you selected TFTP, enter the Server and Filename information.

   -or-

c. If you selected FTP or HTTP PUT, enter the Server, Username, Password and Filename information.

5. If you generated a new self-signed certificate, click the *Generate* button in the top right corner.

   -or-

   If you are uploading a new certificate, click the *Upload* button in the top right corner.

3.4.8 Upgrading the firmware

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

NOTE: The preferred method for updating the firmware is to use the Vertiv™ Avocent® DSView™ 4.5 management software. See the Vertiv™ Avocent® DSView™ 4.5 Management Software Installer/User Guide for detailed instructions.

After the Flash memory is reprogrammed with the upgrade, the 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 switch firmware:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Upgrade Firmware*.
3. Select the radio button to use one of the following options to upload the firmware file: *Filesystem*, *TFTP*, *FTP* or *HTTP*.

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

a. If you selected Filesystem, click *Choose File* and browse to the location of the firmware upgrade file.

   -or-

b. If you selected TFTP, enter the Server and Filename information of the firmware upgrade file.

   -or-

c. If you selected FTP or HTTP, enter the Server, Username, Password and Filename information of the firmware upgrade file.

4. Click the *Upgrade* button in the top right corner.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

3.4.9 Pinging the network

To send a network ping from the switch:

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Ping*.
3. Enter the desired network address in the Address field.
4. Enter the appropriate payload size for the ping in the Payload Size field.
5. Enter the number of pings you wish to send in the Count field.
6. Click the *Ping* button in the top right corner to ping the network.

3.4.10 Saving the trap MIB

To save the switch's trap management information base (MIB):

1. From the side navigation bar, select *Unit View - Appliance - Overview*.
2. Click *Save Appliance Trap MIB*.
3. Select the desired radio button to use one of the following methods to download the trap MIB file: Filesystem,, TFTP, FTP or HTTP PUT.
   a. If you selected TFTP, enter the Server and Filename information.

      -or-

   b. If you selected FTP or HTTP PUT, enter the Server, Username, Password and Filename information.
4. Click the *Download* button in the top right corner. The trap MIB file downloads to the specified location.

3.5 Network Settings

From the Network screen, you can configure general network settings, as well as IPV4 and IPv6 settings.

NOTE: Only Appliance Administrators can make changes to the Network dialog box settings. All other users are limited to read-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*.

3.6 DNS Settings

From the DNS screen, 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*.

3.7 SNMP Settings

Simple Network Management Protocol (SNMP) is a protocol used to communicate management information between network management applications and Vertiv Avocent MergePoint Unity switches. Other SNMP managers can communicate with your 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 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. From the side navigation bar, 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 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 Vertiv Avocent MergePoint Unity switch. The values can be up to 64 characters in length. These fields may not be left blank.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

5. Type the address of up to four management workstations that are allowed to manage this switch in the Allowable Managers fields. Alternatively, you may leave these fields blank to allow any station to manage the Remote Console Switch.
6. Click *Save*.

3.8 Auditing

From the Auditing screen, you can configure the events for which notifications will be sent. You can also specify the SNMP trap destinations and Syslog servers to which you wish the event to be sent.

3.8.1 Enabling events

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

To enable individual events:

1. From the side navigation bar, 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*.

3.8.2 Configuring 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.

To set event destinations:

1. From the side navigation bar, 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 Vertiv Avocent MergePoint Unity switch will send events in the SNMP Trap Destination fields, as well as up to four Syslog servers.
3. Click *Save*.

3.9 Ports

3.9.1 Configuring IQ modules

From the IQ Adaptors 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
- Set the USB speed

- Upgrade the IQ module firmware
- Decommission the IQ module

To delete offline IQ modules:

1. From the side navigation bar, click *Unit View - Appliance - Appliance Settings - Ports - IQ Adaptors* 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 Adaptors* 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 newest firmware available. This update can be performed using the Vertiv Avocent MergePoint Unity switch user interfaces or Vertiv™ Avocent® DSView™ 4.5 management software.

After the Flash memory is reprogrammed with the upgrade, the 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 switch is updated. To update your switch firmware, see Appliance Tools on page 21 or the Vertiv™ Avocent® DSView™ 4.5 Management Software Online Help. If issues occur during the normal upgrade process, IQ modules may also be force upgraded when needed.

NOTE: Check http://www.Vertiv.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 Adaptors* 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 *Operations - 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.

3.9.2 Configuring power devices

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

From the 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.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

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*.

3.9.3 Configuring local UI settings

From the Local Port UI screen, you can change how the local UI is invoked and configure local port user settings including user authentication, access and preemption levels, the default language and the default home page. You can also configure the local port virtual media session settings, scan mode, and keyboard language.

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

Local users 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*.

Local virtual media settings

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

Table 3.3 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, click *Unit View - Appliance - Appliance Settings - Ports - Local Port UI*.
2. Click the box to enable or deselect to disable any of the Virtual Media Session options.
3. Click *Save*.

Scan mode

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

In Scan mode, the Vertiv Avocent 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*.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

3.9.4 Configuring modem settings

From the Modem 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 Vertiv Avocent MergePoint Unity switch to a modem, see Connecting the Switch Hardware on page 10.

To configure modem settings:

1. From the side navigation bar, select *Unit View - Appliance - Appliance Settings - Ports - Modem* to open the Appliance Modem Settings screen.
2. Either enable or disable the Modem sessions can preempt digital sessions 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*.

3.10 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.

3.10.1 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, click *Unit View - Target List*. A list of available devices appears.
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 appears.

   -or-

   Press **Esc**.

3.10.2 Configuring a session

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*.

   For more information about KVM sessions, refer to KVM Video Viewer on page 43.

To configure virtual media session settings:

1. From the side navigation bar, select *Unit Views - Appliance - Appliance Settings - Sessions - Virtual Media* to open the Appliance Virtual Media Session Settings screen.

   Table 3.4 below outlines the options that can be set for virtual media sessions.

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 is also closed. When locking is disabled and the KVM session is closed, the virtual media session remaind 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. Read-only access mode: The user cannot write data to the mapped drive on the client server. 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. Read-write access mode: The user cannot read and write data from/to the mapped drive.
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 Vertiv Avocent 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.

2. Either enable or disable the Virtual Media locked to KVM Sessions checkbox.
3. Either enable or disable the Allow Reserved Session checkbox.
4. Select one of the following options from the Virtual Media Access Mode from the drop-down menu: *Read-Only* or *Read-Write*.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

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*.

   For information about using virtual media in a KVM session, see Virtual Media on page 49. For information about configuring the local virtual media settings, see Local virtual media settings on page 31.

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*.

3.10.3 Closing a session

To close a session:

1. From the side navigation bar, select *Active Sessions* to display the 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 also 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.

3.11 User Accounts

From the User Accounts screen, you can manage different kinds of user accounts including local users, Vertiv™ Avocent® DSView™ 4.5 management software users, and LDAP users.

3.11.1 Managing local user accounts

The Vertiv Avocent MergePoint Unity switch OBWI provides local and login security through administrator-defined user accounts. From the Local screen, administrators may add and delete users, define user preemption and access levels and change passwords.

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 3.5 Allowed Operations by Access Level

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

To add a new local user account (administrator only):

1. From the side navigation bar, select *Unit View - Appliance - Appliance Settings - User Accounts - Local* to open the Local User Accounts screen.
2. Click the *Add* button.
3. Enter the name and password of the new user in the provided fields.
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 local user account (administrator only):

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

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

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

3.11.2 Managing Vertiv™ Avocent® DSView™ 4.5 software user accounts

From the DSView screen, you can contact and register an unmanaged Vertiv Avocent MergePoint Unity switch with a Vertiv™ Avocent® DSView™ management software server by specifying the IP addresses of up to four Vertiv™ Avocent® DSView™ management software servers.

To configure the server IP address:

1. From the side navigation bar, click *Unit View - Appliance - Appliance Settings - User Accounts - DSView*. The Appliance DSView Settings screen appears.
2. Enter up to four Vertiv™ Avocent® DSView™ server IP addresses that you want to contact in the Server 1 - 4 fields.
3. Click *Save*.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

3.11.3 Configuring the LDAP settings

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.

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. For detailed information on each mode, see .

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.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

    - 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 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

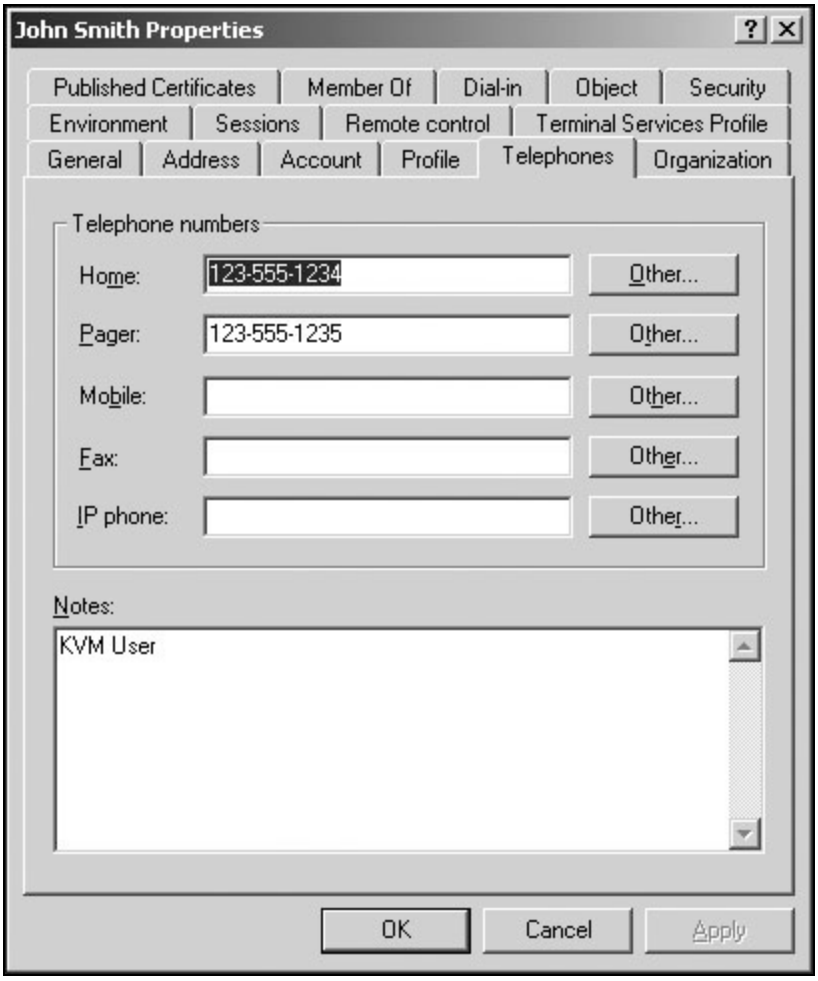
One of three different modes can each be used for Query Mode (Appliance) and Query Mode (Target Device):

- 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 the 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 3.2 Active Directory - KVM User

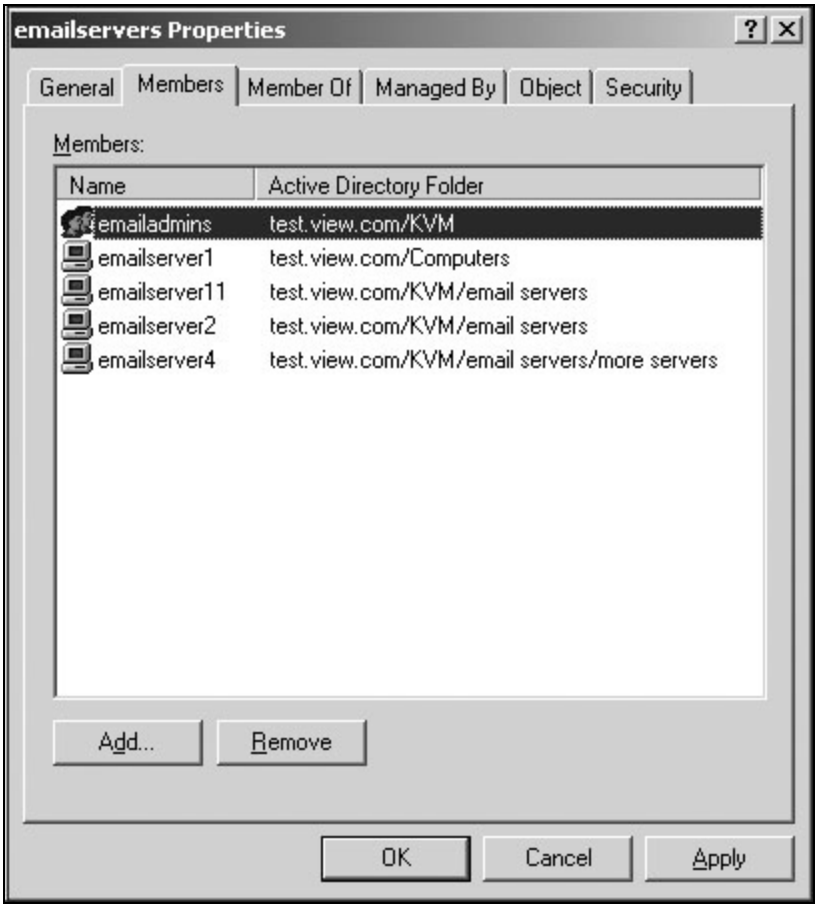


- Group Attribute – A username, password and group query is made to the directory service for an appliance and attached target devices when using Query Mode (Appliance), or for a selected target device when using Query Mode (Target Device). If a group is found containing the user and the appliance name, 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 3.3 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.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

This page intentionally left blank

4 KVM Video Viewer

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

4.1 Supported Session Types

The following table describes the types of sessions supported by the Vertiv Avocent MergePoint Unity switch.

Table 4.1 Session Types

Session Type	Description
Virtual media	Virtual media sessions, which are supported on certain KVM switches, are opened from the KVM Video Viewer.
KVM	KVM sessions can be launched to target devices from any supported KVM switch. Each session is established using the configured encryption level. The following devices use either a Java-based program or an ActiveX applet to display the KVM Video Viewer window: Vertiv™ Avocent® DSView™ 4.5 management software, Vertiv™ Avocent® Universal Management Gateway appliance and Vertiv Avocent MergePoint Unity switch. • Java-based program - Launched from a Mozilla Firefox or Google Chrome based client browser. • ActiveX program - Launched from a Microsoft Internet Explorer browser. **NOTE: To launch a KVM session, a user must have been assigned rights or belong to a user group which has been assigned rights to establish a KVM session.** **NOTE: You can also launch an HTML5 session. Google Chrome is the preferred browser for HTML5 video viewer sessions. For more information on the HTML5 viewer, see the Vertiv™ HTML5 Video Viewer Technical Bulletin.**

4.2 Performance Errors

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

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

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

Proprietary and Confidential ©2026 Vertiv Group Corp.

4.3 Java Versions

When launched from Mozilla Firefox browsers, the KVM Video Viewer client requires Java. If the client machine does not already have any supported Java Runtime Environment (JRE) installed, then the software client automatically downloads and installs the JRE the first time the KVM Video Viewer or Telnet Viewer is launched.

On a Windows client, it is recommended that the JRE be installed in the C:\Program Files\ location. If your system automatically installs programs in another location, you may not be able to launch the KVM Video Viewer. In this case, you can configure Java to find the JRE. For more information on supported Java versions, see the product release notes located on http://www.Vertiv.com.

To configure Java to find the JRE:

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

4.4 KVM Session Configurations

The following table describes the procedures for configuring KVM sessions. These configurations can be performed from the KVM Video Viewer. To access the KVM Video Viewer session configuration options, open a KVM Video Viewer session and click the *File* tab. For instructions on launching a session, refer to Launching a session on page 32.

Table 4.2 KVM Session Configuration Options

Setting	Description
Capture File	Click *File - Capture File*to save the display of a KVM Video Viewer window to a file. Enter a filename and choose a location to save the file, then click *Save*.
Capture to Clipboard	Click *File - Capture to Clipboard*to save the display of a KVM Video Viewer window to your clipboard. You can paste text from the client machine to another appropriate program, such as Notepad, on the host either via a file or the clipboard.
Sent Text File Contents	Click *File - Sent Text File Contents*to paste text from a file from the client machine to the host. Browse to the location on the client machine where the file is saved, click the file, then click *Open*.
Paste Text	Click *File - Paste Text*to paste text from your clipboard to the host..
Exit	Click *File - Exit*to close a KVM session. For more information, refer to Closing a session on page 34.

4.5 Profile Settings

The profile settings for the KVM Video Viewer are Refresh, Fit, Full Screen, Mini-Mode, Scaling, Color Modes, Session User List and Status. These settings are described in the following table. To access the profile settings, open a KVM Video Viewer session and click the *View* tab.

Table 4.3 Profile Settings

Setting	Description
Refresh	Click *View - Refresh* to update the KVM Video Viewer window.
Fit	Click *View - Fit* to resize the KVM Video Viewer window to adjust the window size to completely display the resolution of the digitized video. If the target server's resolution is higher than the client workstation's resolution, and auto-scaling is in effect, the target image will be scaled to fit in the client window. In this case, the client window will occupy as much of the client workstation's desktop as necessary to scale both horizontally and vertically. If auto-scaling is not in effect, then the client window will be maximized to fit on the client workstation window and scroll bars will appear to allow access to the target server's image.
Full Screen	Click *View - Full Screen* to toggle the client between Full Screen mode and Windowed mode. When the Full Screen mode is enabled, the following actions take place: • Resize the Viewer window to completely fill the user's desktop. • Enable auto-scaling. • Disable the entire Scaling menu, thereby not allowing the user to change the resolution while in Full Screen mode. • Perform other tasks when Full Screen mode is enabled, such as turn on Keyboard Pass-Through and display the floating menu bar. When the Full Screen mode is exited, Windowed mode resumes and the following actions take place: • Resize the Viewer window to its former size. • Revert to the previous scaling mode. • Temporarily disable all menu items in the Scaling menu. Once the resumed resolution has been confirmed, the Scaling menu items will be re-enabled. • Resume keyboard pass-through and do other tasks currently performed by the Viewer client when in Windowed mode.
Mini-Mode	Click *View - Mini-Mode* to toggle the client between Mini-Mode and Windowed mode. In Mini-Mode, the KVM Video Viewer client will display a thumbnail view of the host server display and provide no input for keyboard or mouse. The dimensions of the digitized video will not be changed while in Mini-Mode. **To select the window size for Mini-Mode:** 1. Click *Tools - Session Options*. 2. From the Mini-Mode tab, use the drop-down menu to select the window size. 3. Click *OK*. **NOTE: To exit Mini-Mode, double-click on the Mini-Mode window or right-click on the Mini-Mode window and de-select the Mini-Mode menu item.**
Scaling	Click *View - Scaling* to change the KVM Video Viewer window resolution. You can choose *Auto Scale, Server Resolution* or select a fixed resolution.

Proprietary and Confidential ©2026 Vertiv Group Corp.

Table 4.3 Profile Settings (continued)

Setting	Description
	If Auto Scale is selected, the KVM Video Viewer will automatically adjust the display if the window size changes during a session. When a user accesses a channel using sharing, the display will be adjusted to match the input resolution selected by the primary user of that channel. The Viewer prevents a secondary user from changing the resolution and affecting the primary user. If the target device resolution changes any time during a session, the display will be adjusted automatically. If Server Resolution is selected, the display window is sized to match the resolution of the server being viewed. **To maintain the aspect ratio for video in Windowed or Full Screen mode:** 1. Click *Tools - Session Options*. 2. Check the box next to Windowed or Full Screen mode. 3. Click *Apply*.
Color Modes	Click *View - Color Modes* to change the color depth used by the KVM Video Viewer. The Dambrackas Video Compression™ (DVC) algorithm allows you to display more colors for the best fidelity, or fewer colors to reduce the volume of data transferred on the network. The choices are (in descending color quantity): • Best Color • Medium Color/Medium Compression • Low Color/High Compression • Gray Scale/Best Compression
Session User List	Click *View - Session User List* to view active users of this session.
Status Bar	Click *View - Status Bar* to display or hide the status bar at the bottom of the Viewer window.

4.6 Macros

The KVM Video Viewer window macro function allows you to:

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

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

To send a macro:

From the KVM Video Viewer menu, select *Macros - <desired macro>*.

To create a macro:

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

To delete a macro:

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

4.6.1 Global macros

The KVM Video Viewer supports global macros from the Vertiv™ Avocent® DSView™ 4.5 management software. An administrator can create and designate a macro as Global or Personal. Global macros are created and used by the KVM viewer client but are stored on the Vertiv™ Avocent® DSView™ 4.5 management software servers. Personal macros are associated with the name of the user.

The Vertiv™ Avocent® DSView™ 4.5 management software server will send the macros groups and their associated macros as part of the preferences saved on the server. One of the macro groups will be used as the default macro group for the management software profile. The macros in the default group will be added to the Macros menu in the KVM Video Viewer. For more information, refer to Macros on the previous page.

The Macros menu of a viewer connected to a Vertiv™ Avocent® DSView™ 4.5 management software server also contains Macros and Macro Groups menu items. From these menus, an administrator can create and manage custom macros and macros groups.

4.6.2 Macro groups

From the Vertiv™ Avocent® DSView™ 4.5 management software, launch a KVM Video Viewer session and click *Macros - Configure - Macro Groups* to view and manage the macro groups on the management software. By default, three groups are already defined - Linux, Sun and Windows. You can create custom groups or edit existing groups.

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

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

To create a new macro group:

1. Click *Create*.
2. Enter the name in the Macro Group Name field and select the radio button for Global or Personal as the group type.
3. From the Macros Available field, select the macros you want to add to the group and click *Add*.
4. (Optional) Once the macros are in the Macros In Group field, click *Move Up* or *Move Down* to re-order the macros.
5. Click *OK*.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

To edit a macro group:

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

To delete a macro group:

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

To copy a macro group:

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

4.6.3 Macros configuration

From the Vertiv™ Avocent® DSView™ 4.5 management software, launch a KVM Video Viewer session and click *Macros - Configure - Macros* to view and manage individual macros on the management software server. You can use the radio button at the bottom right of the screen to view all the macro groups or just the personal or global groups.

To immediately send a macro to the target server:

Click on the macro and click *Execute*.

To create a new macro:

1. Click *Create*.
2. Enter a name for the macro in the Macro Name field and use the radio button to select Personal or Global as the macro type.
3. Use the drop-down menus to select the keyboard type and icon.
4. Use the virtual keyboard to enter the keystrokes for the macro in the Keystrokes field.
5. (Optional) Click *Remove* to remove the highlighted keystroke or click *Reset* to reset the macro. You can also re-arrange the order of the keystrokes by clicking *Move Up* or *Move Down*.
6. When finished, click *OK*.

To edit a macro:

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

To delete a macro:

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

To copy a macro:

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

4.7 Virtual Media

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

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

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

4.7.1 Requirements

Ensure these virtual media requirements are met:

- The target device must be connected to the KVM switch that supports virtual media with an IQ module that supports virtual media.
- The target device must be intrinsically able to use the types of USB2-compatible media that you virtually map. If the target device does not support a portable USB memory device, you cannot map that on the client machine as a virtual media drive on the target device.
- The user (or user group to which the user belongs) must have permission to establish virtual media sessions and/or reserved virtual media sessions to the target device.
- Only one virtual media session may be active to a target device at one time.

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

To launch a virtual media session:

Select *Virtual Media - Activate*.

To map a virtual media drive:

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

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

   -or-

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

   -or-

Proprietary and Confidential ©2026 Vertiv Group Corp.

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

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

To unmap a virtual media drive:

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

To display and close virtual media drive details:

1. Display the Stats dialog box from the *Tools-Stats* tab of the KVM Video Viewer menu. The dialog box expands to display the Details table. Each row indicates:
   - Target Drive - Name used for the mapped drive, such as Virtual CD 1 or Virtual CD 2.
   - Mapped to - Identical to Drive information that appears in the Client View Drive column.
   - Read Bytes and Write Bytes - Amount of data transferred since the mapping.
   - Duration - Elapsed time since the drive was mapped.
2. Click *Details* again to close the Details table.

To reset all USB devices on the target device:

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

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

4.7.2 Image creation

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

To create or add an image:

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

4.8 Session Options

Each of the settings in this section can be accessed from the *Tools - Session Options* tab of the KVM Video Viewer menu. The tabs located within session options are General, Mouse and Toolbar.

4.8.1 General

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

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

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

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

To enable Keyboard Pass-Through mode:

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

To enter Single Cursor mode:

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

To exit Single Cursor mode:

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

4.8.2 Mouse synchronization

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

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

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

To set Mouse Synchronization:

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

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

7. Click *Apply*.

 Proprietary and Confidential ©2026 Vertiv Group Corp.

4.8.3 Certificate

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

4.8.4 Automatic video adjust

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

4.8.5 Manual video adjustment

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

NOTE: Video adjustment is a per target setting.

Figure 4.1 Manual Video Adjust Window

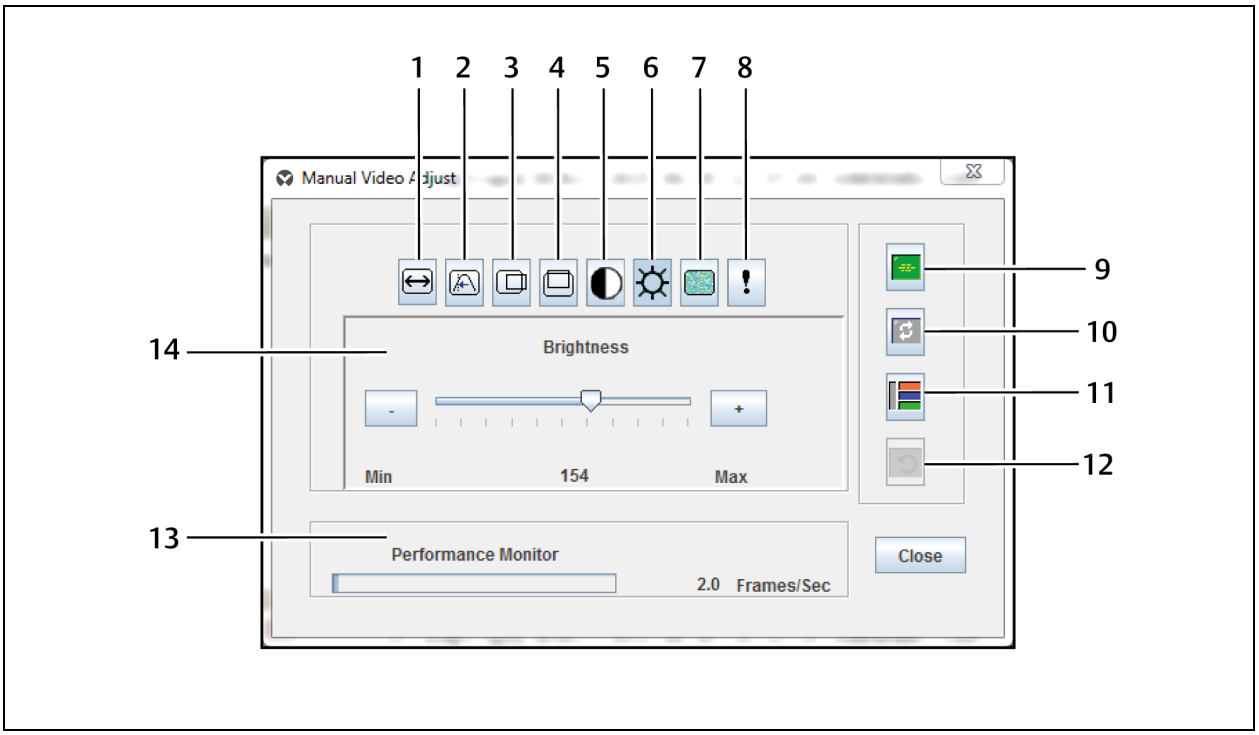


Table 4.4 Manual Video Adjust Window Descriptions

Item	Description	Item	Description
1	Image Capture Width	8	Contrast
2	Pixel Sampling/Fine Adjust	9	Automatic Video Adjustment
3	Image Capture Horizontal Position	10	Refresh Image

Table 4.4 Manual Video Adjust Window Descriptions (continued)

Item	Description	Item	Description
4	Image Capture Vertical Position	11	Adjustment Bar
5	Pixel Noise Threshold	12	Revert Video to Initial Settings
6	Brightness	13	Performance Monitor
7	Block Noise Threshold		

To manually adjust the video quality of the window:

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

1. Click *Tools - Manual Video Adjust* from the Video Viewer window menu.
2. Click the icon corresponding to the feature you wish to adjust.
3. Move the Contrast slider bar and then fine-tune the setting by clicking the Min *(-)* or Max *(+)* buttons to adjust the parameter for each icon pressed. The adjustments display immediately in the Video Viewer window.
4. When finished, click *Close*.

4.8.6 Cursor commands

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

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

To prevent potential mouse conflicts, you may configure certain settings on each server connected to a managed appliance. For details, see the Mouse and Pointer Settings Technical Bulletin, which is available on http://www.Vertiv.com.

To align the mouse cursors:

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

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

4.8.7 Stats

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

4.9 Power Control

If opening a session from the Vertiv™ Avocent® DSView™ 4.5 management software or some Vertiv™ Avocent® Universal Management Gateway appliances, you can turn the host device on or off or power cycle it.

To manage power:

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

 Proprietary and Confidential ©2026 Vertiv Group Corp.

4.10 Smart Cards

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

To map a smart card:

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

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

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

4.11 Video Recording

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

4.11.1 Continuous recording

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

4.11.2 Persistent recording

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

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

To configure the recording capacity:

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

To control or view persistent video:

1. Select *Tools - Recorder/Playback Controls* from the KVM Video Viewer menu.

2. Use the controls as described in the following table.

Table 4.5 DVR Player Controls

Icon	Control	Description
	Open	Click this button to open the File dialog box to browse for and open a DVC file either created by the Record function on the KVM Video Viewer or downloaded from an appliance or service processor.
	Return To Start	When a persistent file is being played, click this button to move the playback position back to the start of the file. When a session is being recorded, clicking this button causes the continuous recording buffer to go to its oldest data and start playing back from that point.
	Skip Back	When a file or continuous recording is being played, click this button to shift the play position back one 30-second period at a time. Each time it is clicked, the play position moves back to the start of the previous period. If the playback mode was Play or Fast Forward when this button was clicked, the playback proceeds at a speed of 1X. If the playback mode was Paused when this button was clicked, the playback displays the first frame of the previous period. If the continuous recording buffer reaches the play position, then playback proceeds at a speed of 1X.
	Play	Click this button to play the recording.
	Pause	While a file is being played, the Play button becomes the Pause button. Click it to pause the playback. During a Live session, clicking the *Pause* button pauses the Live playback. Live mode changes to Continuous and the Play button is disabled.
	Recording Stop/Start	Click this button to open the Save dialog box. Use the drop-down menu to choose a location to save the recording. Once you have entered a filename and clicked *Save*, the recording begins. While recording, click the button again to stop the recording.
	Fast Forward	During playback, click this button to fast forward one 30-second period at a time. Each time this button is clicked, the playback rate increments by 10:1 until the fifth time it is clicked. The fifth time it is clicked, the playback rate returns back to 10X.
	Go To End	Click this button to go to the end of the file or continuous recording. When a file is not being played but a KVM session is in progress, clicking this button displays the live video from the connected KVM session.
	Live	Click this button to terminate the playback of a file or a continuous recording and to display the video from the connected KVM session. This button is disabled and grayed out when there is no connected KVM session, such as if a file was being played back without a connected KVM session or the KVM session had been terminated.
	Slider	Use the slider at the bottom of the screen to view and adjust the progress of the playback. The slider acts as a scrollbar, moving from left to right as the recording is played back. If the video is paused and you click or drag the slider, the playback moves to that position and remains paused. If the video is playing and you click or drag the slider, the playback moves to that position and continues playing.

4.11.3 Exporting video

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

To export video:

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

Proprietary and Confidential ©2026 Vertiv Group Corp.

4.12 KVM Session Optimization

To improve session performance:

1. From the KVM Video Viewer menu, click *Tools - Automatic Video Adjustment*to calibrate the A/D converter to the video signal coming from the server video card.
2. To identify a KVM session that is slow due to unclean video signals, click *Tools - Manual Video Adjustment*. A clean video signal will create 0 pkts/sec. on the performance monitor when there is not any activity on the target server.

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

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

If the above optimization options are ineffective at improving session speeds, the Video Noise Control setting can be enabled, which will increase session speed by ignoring small video changes. The only negative to this setting is that it can increase the appearance of video “blocks.” Also take note of the other settings that can be configured for KVM targets globally or individually.

The following information is an example of what is possible but not guaranteed since every target and every network is different. You will also note that some of the metrics are not entirely analogous (for example, FPS vs. pkts/sec.) Also, the bandwidth usage does not reflect the quality/fluidity of the session (the KVM session was much smoother and better than the vKVM).

Example: Appliance KVM session in a 100 Mbps LAN environment

The following metrics represent the KVM window resolution 1280x1024 @70 Hz (Windows Server):

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

The following metrics represent the KVM window resolution 1024x768 @70 Hz (Windows Server):

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

The following metrics represent the KVM window resolution 1024x768 @60 Hz (Ubuntu Desktop):

- Zero screen movement = 0 pkts/sec (avg. 1.3 Kbps download | 1.0 Kbps upload)
- Continuous mouse circles movement on screen = 30 pkts/sec (average 470 Kbps download | 245 Kbps upload)
- Rapidly opening and closing full-screen windows = 40-50 pkts/sec (average 750 Kbps download | 180 Kbps upload)

Appendices

Appendix A: Technical Specifications

Table A.1 Technical Specifications

Category	Value
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 CAT5 or CAT6, 45 meters maximum length
Dimensions	
Form Factor	1 U-rack, mountable
16 and 32-port models 4 and 8-port models	17.00 x 13.38 x 1.72 (Width x Depth x Height) 17.00 x 11.00 x 1.72 (Width x Depth x Height)
Weight (without cables)	MPU8032DAC: 8.6 lbs
SETUP Port	
Number	1
Type	RS232 serial
Connector	8-pin modular
Local Port(4 and 8 port)	

Proprietary and Confidential ©2026 Vertiv Group Corp.

Table A.1 Technical Specifications (continued)

Category	Value
Number/Type	1 VGA/4 USB
Local Port (16 and 32 port)	
Number/Type	1 VGA/5 USB
Network Connection	
Number	2
Type	10/100/1000 Ethernet
Connector	8-pin modular
USB Device Port	
Number	4 (4 and 8-port) or 5 (16 and 32-port)
Type	USB 2.0
MODEM Port	
Number	1
Type	RS232 serial
Connectors	8-pin modular
PDU Port	
Number	2
Type	RS232 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

 Proprietary and Confidential ©2026 Vertiv Group Corp.

Table A.1 Technical Specifications (continued)

Category	Value
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.	

Proprietary and Confidential ©2026 Vertiv Group Corp.

This page intentionally left blank

Appendix B: Terminal Operations

Each Vertiv Avocent 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 Vertiv™ Avocent® DSView™ 4.5 management software. See the Vertiv™ Avocent® DSView™ 4.5 Management Software Installer/User Guide for more information.

To connect a terminal to the Vertiv Avocent 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 switch. For Vertiv Avocent MergePoint Unity switch models that support an RJ45 port, an RJ45 to DB9 (female) adapter 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 switch. When the switch completes initialization, the Console menu will display the following message: *Press any key to continue*.

B.1 Console menu options

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

1. Network Configuration: Configure the IP address and other network settings.

2. Enable 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 Vertiv™ Technical Support. When you are finished viewing the messages, press any key to exit this mode.

3. Security Configuration: Enable/disable secure mode and Disassociate the unit from Vertiv™ Avocent® DSView™ 4.5 management software.

4. Enable LDAP Debug Messages: Turns on console status messages for LDAP. Because this can significantly reduce performance, you should only enable debug messages when instructed to do so by Vertiv™ Technical Support. When you are finished viewing the messages, press any key to exit this mode.

5. Reset Appliance: Reboots the appliance but also allows you to interrupt autoboot by pressing any key when prompted for the additional options below:

- **0.** Boot Current (continues boot with no changes)
- **1.** Boot Alternate (boot to previously loaded firmware)
- **2.** Configuration Reset (reset only configuration changes)
- **3.** Factory Reset (factory defaults the unit)

0. Exit: This menu selection returns you to the ready prompt. If the Console menu interface password is enabled, you must exit the Console main menu so the next user is prompted with the Username and Password login screen.

This page intentionally left blank

Proprietary and Confidential ©2026 Vertiv Group Corp.

Appendix C: Using Serial IQ Modules

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

C.1 Using DSRIQ-SRL modules

The DSRIQ-SRL module is a serial-to-VGA converter that allows VT100-capable devices to be viewed from the Vertiv Avocent MergePoint Unity switch local port, the OBWI, or by using the Vertiv™ Avocent® DSView™ 4.5 management 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 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.

C.2 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 Vertiv Avocent 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 Vertiv Avocent 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.

Proprietary and Confidential ©2026 Vertiv Group Corp.

C.3 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.

C.4 Using History mode

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

The 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.

C.5 DSRIQ-SRL module pinouts

The following table lists the pinouts for the DSRIQ-SRL module.

Table C.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

C.6 Using MPUIQ-SRL Modules

An administrator can choose between the Vertiv™ Avocent® ACS console server and Cisco pinouts for each MPUIQ-SRL serial port via the local user interface or the remote OBWI. The Vertiv™ Avocent® 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 Vertiv™ Avocent® ACS console server pinouts.

C.7 Vertiv™ Avocent® ACS console server port pinouts

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

Table C.2 Vertiv™ Avocent® ACS Console Server Serial Port Pinouts

Pin	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

Proprietary and Confidential ©2026 Vertiv Group Corp.

C.8 Cisco port pinouts

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

Table C.3 Cisco Serial Port Pinouts

Pin	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

This page intentionally left blank

Proprietary and Confidential ©2026 Vertiv Group Corp.

Appendix D: UTP Cabling

This appendix discusses various aspects of connection media. The performance of a Vertiv Avocent MergePoint Unity switch depends on high quality connections. Poor quality or poorly installed or maintained cabling can diminish switch performance. The Vertiv Avocent MergePoint Unity switches 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.

D.1 UTP copper cabling

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

- CAT5 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. CAT5 cable is generally used for networks running at 10 or 100 Mbps.
- CAT5E (enhanced) cable has the same characteristics as CAT5, but is manufactured to somewhat more stringent standards.
- CAT6 cable is manufactured to tighter requirements than CAT5E cable. CAT6 has higher measured frequency ranges and significantly better performance requirements than CAT5E cable at the same frequencies.

D.2 Wiring standards

There are two supported wiring standards for 8-conductor (4-pair) RJ45 terminated UTP cable: EIA/TIA 568A and B. These standards apply to installations utilizing CAT5, 5E and 6 cable specifications. The Vertiv Avocent MergePoint Unity switch supports either of these wiring standards. The following table describes the standards for each pin.

Table D.1 UTP Wiring Standards

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

D.3 Cabling installation, maintenance and safety tips

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

- Keep all UTP runs to a maximum of 30 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.

Proprietary and Confidential ©2026 Vertiv Group Corp.

Appendix E: Cable Pinout Information

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

Figure E.1 Modem Jack

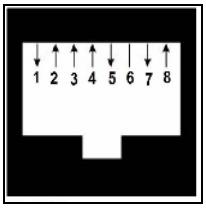


Table E.1 Modem Jack Descriptions

Pin Number	Description	Pin Number	Description
1	Request to Send (RTS)	5	Transmit Data (TXD)
2	Data Set Ready (Vertiv Avocent 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 E.2 Console/Setup Jack

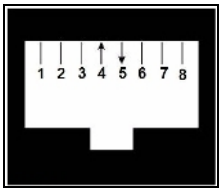


Table E.2 Console/Setup Jack Descriptions

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)

This page intentionally left blank

Proprietary and Confidential ©2026 Vertiv Group Corp.

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 below 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
Find	F9
Mute	keypad /
Vol.+	keypad +
Vol.-	keypad -
Command (left)[2]	F12
Command (left)[2]	Win (GUI) left[1]
Command (right)[2]	Win (GUI) right[1]
Endnotes: (1)Windows 95 104-key keyboard. (2)The Command key is the Sun Meta (diamond) key.	

F.1 Special considerations for Japanese Sun USB and Korean Sun USB keyboards (USBIQ 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 Vertiv Avocent MergePoint Unity switch using a VSN or WSN IQ module.

The following table 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
Hanja	0x91	N/A	N/A	N/A
Katakana/Hiragana	0x88	N/A	N/A	Han/Zen
Han/Zen	0x35	N/A	N/A	N/A

Proprietary and Confidential ©2026 Vertiv Group Corp.

Appendix G: Local UI Keyboard Shortcuts

The following table shows the available keyboard shortcuts for the local UI.

Table G.1 Keyboard Shortcuts

Desired Action	Shortcut
To open the local UI: -or- To switch between the local UI and an active session:	Print Screen
	Ctrl + Ctrl
	Shift + Shift
	Alt + Alt
To close the local UI:	Print Screen
	Esc

This page intentionally left blank

Proprietary and Confidential ©2026 Vertiv Group Corp.

Connect with Vertiv on Social Media

https://www.facebook.com/vertiv/

https://www.instagram.com/vertiv/

https://www.linkedin.com/company/vertiv/

https://www.twitter.com/Vertiv/

Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 USA

©2026 Vertiv Group Corp. All rights reserved. Vertiv™ and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions.

590-1548-501E