Avocent® MergePoint Unity™ 2 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.

TABLE OF CONTENTS

1 Getting Started

1.1 Product Overview

The Avocent MergePoint Unity 2 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 Avocent MergePoint Unity 2 switch provides flexible target device management control and secure remote access from anywhere at anytime.

The following figure and table describe the various components of the Avocent MergePoint Unity 2 switch.

Figure 1.1 Avocent MergePoint Unity 2 Switch Description

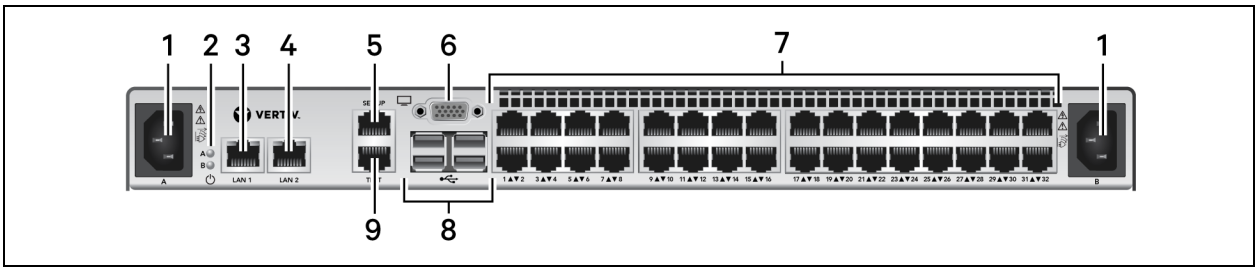

Table 1.1 Avocent MergePoint Unity 2 Switch Description

Number	Description	Number	Description
1	Redundant dual power supplies	6	VGA port
2	Power supply status indicators	7	Device ports
3	1G Uplink port	8	USB ports
4	1G Uplink port	9	Manufacturing test port (not for customer use)
5	Management port		

1.2 Features and Benefits

The Avocent MergePoint Unity 2 switch is designed to meet the evolving needs of modern IT environments, delivering advanced security, high-resolution remote access, and seamless integration for efficient server management. The key features and benefits are described in the following table.

Feature	Benefit
Remote System Management	Eliminate the need for on-site visits, saving time and reducing travel costs by managing systems remotely.
Efficient Troubleshooting	Quickly diagnose and resolve issues to minimize downtime and maintain business continuity.
Remote Firmware Updates	Update device firmware without requiring physical access, streamlining maintenance.
Centralized Management	Manage all servers from a single, unified interface for greater operational efficiency.
Streamlined Staff Training	Train IT staff on one comprehensive solution, reducing complexity and training time.
User Permissions	Assign different user roles and permissions to enhance security and control access.

Feature	Benefit
Remote UEFI and BIOS Access	Remotely access and configure UEFI and BIOS settings for critical system updates and hardware troubleshooting.
Virtual Media Support	Simplifies OS deployments, patch installations, and new application rollouts.
Smart Card and CAC Reader Support	Provides local support for smart card and CAC readers for secure authentication.
Local Hot Key Support	Enables faster navigation and task execution at the local console.
Serial Management	Serial modules support connections to serial devices for flexible management.
Browser-Based Interface	Both local and remote browser interfaces offer easy setup and use.
RESTful API	Supports automation and integration with third-party management tools.
Compact Design	When paired with the Vertiv™ Avocent® Rack Mount 18.5" LCD Console Tray, the switch fits within a single rack unit (1U).
Secure Boot & Signed Firmware	Only verified firmware and software are allowed to operate, protecting your systems.
FIPS 140-2 Compliance	Meets strict security requirements, ideal for high-security environments.
Authentication Protocols	Supports TACACS+, RADIUS, and LDAP for robust user authentication.
HTML5 Viewer	Provides secure, Java-free KVM access.
Updated Kernel	Enhanced security and performance through a modernized system kernel.
High-Quality Visuals	Supports video resolutions up to 1920 x 1080 with 24-bit color for detailed monitoring and troubleshooting.

2 Installation and Initial Setup

Installation and setup instructions related to rack mounting, device and accessory connections, power connections and initial network configurations can be found in the Vertiv™ Avocent® MergePoint Unity™ 2 Quick Installation Guide shipped with your product. The guide can also be found on the product page on www.Vertiv.com.

2.1 Physical Security

This product is designed and intended to be deployed and operated in a physically secure and network firewall-protected location. Vertiv recommends a review of the physical security and operating environment of the unit. Since an attacker or disgruntled user can cause serious disruption, below are some recommended best practices that include, but are not limited to:

- Restrict access to areas, racks, and units with encrypted card RFID/badges, unique multi-factor passcode authentication for access, man traps, and biometric scanners for physical access to the equipment.
- Have trusted and background-checked security guards with 24x7x365 physical presence and written logs to help document and note physical access to a data center, building, rack, and so on.
- Restrict physical access to telecommunications equipment and network cabling. Physical access to the telecommunications lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. Best practices include use of metal conduits for the network cabling running between equipment cabinets.
- All USB, RJ45, and/or any other physical ports should be restricted on the units.
- Do not connect removable media (such as USB devices, SD cards, and so on) for any operation (such as firmware upgrade, configuration change, or boot application change) unless the origin of media is known and trusted. Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.

2.2 Grounding Requirements

The Vertiv™ Avocent® MPUIQ KVM modules share a common ground with the target device. To successfully launch KVM sessions, use a power cable with a ground connector pin for the target device. This provides the necessary grounding for KVM functionality.

Alternatively, if the target device does not support a grounded cable, use a USB A-A or USB A-C cable to connect the switch's USB port to one of the USB ports on the target device. This USB connection establishes only a common ground connection; it does not provide any data function.

This page intentionally left blank

3 SSL Certificate Replacement

When you enter the switch's IP address into a web browser, you may receive an error message indicating that the SSL certificates are not recognized. If you wish to replace the SSL certificates, please visit the product page on www.Vertiv.com for a script and release notes for assistance with this process. If you need additional assistance, please contact your Vertiv Technical Support representative.

This page intentionally left blank

4 Local User Interface

The Avocent MergePoint Unity 2 switch includes a local port on the back panel to which you can connect a keyboard, monitor, and mouse directly to the switch and use the local UI for direct access. The local UI enables users to manage their sessions and devices directly from the interface.

To launch the local UI, connect your monitor, keyboard, and mouse cables to the Avocent MergePoint Unity 2 switch. This chapter will guide you through the various capabilities and operational procedures available within the local UI.

4.1 Main Dialog Box Functions

From the Main dialog box, you can perform several functions, including view and select ports and devices, view switch system status, select devices, soft switching, navigate the interface, and connect local virtual media.

4.1.1 View and select ports and devices

Use the Main dialog box to view and control devices in the switch system. View your devices by name, port, or by the unique EID number embedded in each IQ module.

Table 4.1 Main Dialog Box Functions

Button	Function
Name	Name of device
EID	Unique EID in a module
Type	Type of session: KVM or serial
Port	The port to which a device is connected
VMedia	Control virtual media connection
Hide Offline	Hide all offline IQ modules
Disconnect	Disconnect the session
Setup	Access the Setup dialog box and configure the local interface
CLI	Access the CLI dialog box.

4.1.2 View switch system status

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

Table 4.2 Local UI Status Symbols

Symbol	Description
	Device is connected and turned on, and the IQ module is online.
	Device is turned off or is not operating properly, and the IQ module is offline.
	A local session is active for this target.
	A remote session is active for this target. **NOTE: Connecting to the target via the local port will terminate the remote session.**
	A virtual media drive has been successfully mapped to the switch.

4.1.3 Select devices

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

To select a device:

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

To disconnect from a device:

Press Print Screen to return to the Main dialog box, and then click *Disconnect*.

4.1.4 Soft switching

Soft switching is the ability to switch devices using a hotkey sequence. You can select targets using the keyboard arrows and the Page Up and Page Down keys.

4.1.5 Navigate the interface

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

Table 4.3 Local UI Navigation Basics

Keystroke	Function
Print Screen, Ctrl+Ctrl, Shift+Shift, and/or Alt+Alt	Local UI activation sequence. By default, only Print Screen is enabled to invoke the local UI. You can update this via the Setup dialog box.
Alt	Opens dialog boxes, selects or checks options, and executes actions when using with underlined or other designated letters.
Single-click, Enter	In a text box, single-clicking an entry and pressing Enter selects the text for editing and enables left and right arrow keys to move the cursor. Press Enter again to quit the Edit mode.
Up/Down Arrows	Moves the cursor from line to line in lists.

Table 4.3 Local UI Navigation Basics (continued)

Keystroke	Function
Right/Left Arrows	Moves the cursor between columns. When editing a text box, these keys move the cursor within the column.
Page Up/Page Down	Pages up and down through names, ports, and Help pages.
Home/End	Moves the cursor to the top or bottom of a list.

4.1.6 Connect local virtual media

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

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

To start a local virtual media session:

1. Open the local UI. The Main dialog box appears.
2. Connect to the device with which you want to establish a virtual media session.
3. Use the arrow keys to highlight the device name and press Enter.
4. Press Print Screen to start the interface again. Click on the *Virtual Media* button to display the Virtual Media page.
5. Select one or more of the following checkboxes:
   - CD ROM - Select this checkbox to establish a virtual media CD connection to a device. Clear this checkbox to end the connection.
   - Mass Storage - Select this checkbox to establish a virtual media mass-storage connection to a device. Clear this checkbox to end the connection.
6. Click *OK*.

4.2 Setup Dialog Box Functions

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

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

Table 4.4 Setup Dialog Box Features

Feature	Purpose
Local Console Log Level	Set the log level of the local console. Local console logs are accessible from the CLI's Diagnostic Menu.
Timezone	Set the appliance's timezone. The timezone can also be set in the CLI and web UI.
Invoke Local Port UI	View additional keyboard strokes that will allow a user to return from an active session to the Main dialog box.
Reset Password	Reset the default admin user's password back to the default, 'admin.'
System Info	View additional appliance information which can be used for technical support.

4.3 CLI Dialog Box Functions

From the CLI dialog box, you can manage your switch system and perform various operations, which are described in the following table.

To access the CLI dialog box, click *CLI* on the Main dialog box.

Table 4.5 CLI Root Menu Descriptions

Root Menu Option	Purpose
0 - Exit the CLI	Terminate the CLI session.
1 - Show/Configure Network Settings	Configure the network settings for the switch's interfaces.
2 - Show Thermal and Power Data	Display sensor readings for the switch, including type, time, reading, units, voltage type, adapter, and channel ID.
3 - Show/Configure Chassis	View and modify key chassis-level metadata, including asset tag and location.
4 - Show/Configure Manager	Manage key system settings, including configuring date and time (with optional NTP sync), DNS search domains and name servers, uplink profiles, FIPS security mode, and CORS policies.
5 - Show/Configure Devices	View and configure the module device settings. The settings available varies by module type.
6 - Enrollment	Manage the switch's connection to a centralized management platform (Vertiv™ Avocent® MP1000 Management Platform). You can enable or disable enrollment status, update the manager address and port, or disconnect the switch from the management platform.
7 - Account Settings	Configure the password settings for the system.
8 - Update Firmware	Update the switch's firmware.
9 - Reset to Factory Defaults	Reset the system's settings to factory defaults. **NOTE: If you receive the error message, "*Oops! It seems like the server is taking a little too long to respond*." after attempting to perform a factory reset from the CLI, please allow the system additional time to complete the process and automatically reboot the appliance. Do not perform another factory reset at this time.**
10 - Shutdown	Shut down the switch system.
11 - Reboot	Reboot the switch system.
12 - Diagnostics	Provides tools for troubleshooting and system monitoring, including the ability to view and export logs to USB, manage services status and logging levels, test network connectivity (ping, trace route, TCP connect), verify NTP server connections, and display attached devices.

4.3.1 Configure the IP address

To configure the IP address for the switch:

1. Activate the interface and click *CLI*.
2. Enter the password for the switch.
3. Enter **1** for the Show/Configure Network Settings option.
4. Enter the number option for the network interface for which you wish to configure the IP address.
5. Enter the number option for configuring the IP address via DHCP or statically.
6. Enter the new IP address.

4.3.2 Upgrade firmware

To upgrade the firmware for the switch:

1. Activate the interface and click *CLI*.
2. Enter 8 for the Update Firmware option.
3. Enter the URL path for the upgrade.

NOTE: The time required to complete a firmware upgrade on the switch may vary depending on your network's bandwidth and overall speed. Environments with higher network activity may result in longer upgrade times.

NOTE: The switch reboots when the upgrade is complete.

This page intentionally left blank

5 Web User Interface

Once you have completed the initial setup and configuration activities as detailed in the Vertiv™ Avocent® MergePoint Unity™ 2 Quick Installation Guide, you can access the switch directly via the web UI.

The web UI is compatible with the latest 32-bit and 64-bit versions of the following web browsers:

- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox

To log into the web UI:

1. Open a web browser and enter the IP address for the Avocent MergePoint Unity 2 switch that you previously configured: **https://**<appliance.IP>
2. At the login screen, enter your username and password. The web UI opens into the Targets List screen.

Figure 5.1 Web UI Overview

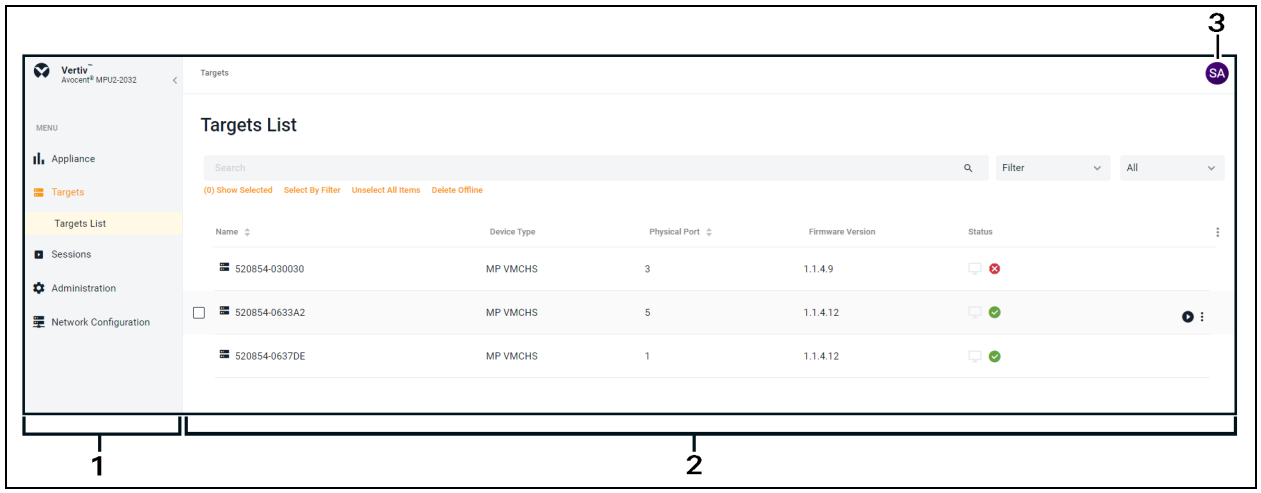

Table 5.1 Web UI Overview Description

Item	Description
1	Sidebar
2	Content area
3	Account settings

5.1 Account Settings

To open your account settings, click the profile icon in the top right corner of the web UI. The drop-down menu allows you to choose from User Preferences, Help, and Log Out.

User Preferences

This option provides you access to the following tabs: User Profile, Localization, and Color Theme. The following table describes the functions of these tabs.

Table 5.2 User Preferences

Tab	Description
User Profile	Configure the profile name, password and email address.
Localization	• Measuring System - Select either the Metric or Imperial radio button to determine the measuring system for the switch. • Time Zone - Select your time zone for alarms and notifications from the drop-down menu. • Time Number Separators - Select the digit grouping and decimal values from the respective drop-down menu. • Data Format - Select either the Day/Month/Year or Month/Day/Year radio button to determine the format for all dates in the web UI. • Time Format - Select either the 12-hours or 24-hour radio button to determine the format for all times in the web UI. • Language - Select the language to be used in the web UI from the drop-down menu.
Color Theme	Select the radio button for your desired color theme.

Help

This option redirects you to a digital copy of the Vertiv™ Avocent® MergePoint Unity™ 2 KVM over IP and Serial Console Switch Installer/User Guide.

Log Out

This option immediately logs you out of the web UI.

5.2 Appliance

The Appliance tab contains one sub-menu item - Overview - from which you can view and edit the properties of the switch and update the firmware.

5.2.1 Overview

From the Overview screen, you can view the serial number, model, and asset tag of the switch. The asset tag can be edited by clicking the pencil icon and entering the Device Name. You can also perform the following functions:

- Reboot or shut down the switch by clicking on the power icon in the upper right corner.
- Reset the switch the factory settings by clicking the vertical ellipsis in the upper right corner.
- Update the switch's firmware.

Update firmware

To update the switch's firmware:

1. From the left-hand sidebar, click *Appliance - Overview*.
2. Under the Firmware section, click *(Download Page)*. The Avocent MergePoint Unity 2 switch Software Downloads page opens in a new tab.
3. Download the latest firmware version for your switch.
4. Save the firmware to one of the following servers: local PC, TFTP, FTP, or HTTP.
5. Return to the Overview screen of the web UI and click the *Update Firmware* button.
6. Upload the firmware file.
    a. If you are uploading the file from your local PC, ensure that you are on the Upload File tab. Drag and drop your firmware file into the designated area, or click *Choose File* and browse to your firmware file.

    -or-

    b. If you are uploading the file from an TFTP, FTP, or HTTP ensure you are on the appropriate tab. Enter the file location and name, as well as the username and password, if required.
7. Click *Update*.

NOTE: The time required to complete a firmware upgrade on the switch may vary depending on your network's bandwidth and overall speed. Environments with higher network activity may result in longer upgrade times.

5.3 Targets

The Target tab contains one sub-menu item - Targets List - from which you can manage your target devices connected to the switch. The number of target devices permitted for a single Avocent MergePoint Unity 2 switch varies by model type. The Avocent MergePoint Unity 2 switch supports a variety of IQ modules, including:

- Vertiv™ Avocent® DSAVIQ-USB2
- Vertiv™ Avocent® DSAVIQ-PS2M
- Vertiv™ Avocent® MPUIQ-VMCHS
- Vertiv™ Avocent® MPUIQ-VMCHD
- Vertiv™ Avocent® MPUIQ-VMCDP
- Vertiv™ Avocent® MPUIQ-VMCDV
- Vertiv™ Avocent® MPUIQ-SRL
- Vertiv™ Avocent® SFIQ-VGA

NOTE: Non-administrator users can only see devices to which they have access.

5.3.1 Targets list

From the Targets List screen, you can view and manage the target devices connected to the switch. Target devices are organized within a table which displays their device type, physical port, firmware version, and status. You can perform the following functions from the Targets List screen:

- Modify device information
- Launch KVM sessions
- Launch serial sessions

- Decommission devices
- Delete devices

Modify device information

You can update certain device information from the device's side panel, such as the target's name. For serial IQ modules, you can also configure the interface settings, including the baud rate, data bits, parity, stop bits, flow control, DTR mode, and pinout.

To modify device information:

1. From the left-hand sidebar, click *Targets - Targets List*.
2. Click on the device row to open the device's side panel.
3. Click on the Edit icon (the pencil) to modify any editable information.

Launch KVM sessions

The HTML5 Viewer provides a secure, web-based interface for launching KVM sessions for one or more target devices on the Avocent MergePoint Unity 2 switch. The viewer supports the following browsers: Google Chrome, Microsoft Edge, Apple Safari, and Mozilla Firefox.

NOTE: To successfully launch a KVM session, ensure you have met the grounding requirements. For more information, refer to Grounding Requirements on page 3.

NOTE: You may need to disable your browser's pop-up blocker to launch a KVM session.

NOTE: You must have assigned rights or belong to a user group with assigned rights to launch a KVM session. For instructions on creating a user group with permissions for launching sessions, refer to the Vertiv™ Avocent® Creating User Groups Technical Note.

To launch a KVM session:

1. From the left-hand sidebar, click *Targets - Targets List*.
2. Hover the mouse over the desired target and click the Launch KVM Session icon (the play symbol) on the right side of the row. The KVM Viewer opens in a new tab.

To navigate a KVM session:

After launching a KVM session, you can navigate the session by using the menu located at the top of the Video Viewer window. You can also configure the settings for the Avocent MergePoint Unity 2 switch using the Settings icon. Depending on the target device type, the configuration options and settings may vary.

To close a KVM session:

From the KVM Viewer session, click the user icon in the upper right-hand corner and select *Exit Viewer*.

Launch serial sessions

The Avocent MergePoint Unity 2 switch supports the Vertiv™ Avocent® 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 Avocent MPUIQ-SRL module.

To launch a serial session:

1. From the left-hand sidebar, click *Targets - Appliance View*.

2. Hover the mouse over the device row and click the Launch Serial Session icon on the right side of the row. The Serial Viewer opens in a new tab.

To navigate a serial session:

After launching a serial session, you are presented with the CLI of the target serial device. You can use the menu located at the top of the Serial Viewer to perform a variety of functions.

NOTE: Depending on the target device type, the configuration options and settings may vary.

To end a serial session:

From the Serial Viewer menu, click the user icon in the upper right-hand corner and select *Exit Serial Viewer*.

Decommission devices

You can decommission an IQ module to remove stored data from the module in preparation for removing it from service on the Avocent MergePoint Unity 2 switch. The IQ module will remain operational on the appliance after decommission.

To decommission a device:

1. From the left-hand sidebar, click *Targets - Targets List*.
2. Hover over the device row, click on the vertical ellipsis on the right side, then click *Decommission*. A confirmation page appears.
3. Click *Decommission*.

Delete devices

You can delete a target device if it is offline and no longer needed. Deleting a device permanently removes the device, and all associated configurations, from the appliance.

To delete an individual offline device:

1. From the left-hand sidebar, click *Targets - Targets List*.
2. Hover over the device row, click on the vertical ellipsis on the right side, then click *Delete*. A confirmation page appears.
3. Click *Yes, Delete*.

To delete all offline devices:

1. From the left-hand sidebar, click *Targets - Targets List*.
2. Click *Delete Offline* above the list of target devices. All offline devices are cleared from the appliance.

5.4 Sessions

The Sessions tab contains one sub-menu item - Sessions List - from which you can view session information for active and closed sessions. The Avocent MergePoint Unity 2 switch allows you to launch multiple sessions simultaneously to access your target devices via the web UI.

5.4.1 Sessions List

From the Sessions List screen, you can view the log of active and closed sessions that have been launched from your switch. You can perform the following functions:

- View the session log based on status by clicking the *Active, Closed* and *All* tabs.

- Search for specific sessions using the search bar.
- View a device's information panel by clicking the target name.
- Sort the columns in ascending or descending order by clicking the arrows next to the column name. Columns can be sorted by target name, IP address, or start time.
- Refresh the web page by clicking the Refresh icon in the upper right corner.
- Export session data.

Export session data

You can easily export and share session data as a comma-separated values (CSV) file.

Prior to exporting the data, verify that the email address associated with your user account is correct in the web UI. To check your email address, click the profile icon and click *User Preferences*. Additionally, ensure that an email server has been configured on the System Settings - Email Server Configuration page. For setup instructions, refer to Email server configuration on page 33.

To export session data:

1. From the left-hand sidebar, click *Sessions – Sessions List*.
2. (Optional) Filter the list of sessions, as desired.
3. Click the Export icon to export the Active, Closed, or All page. The Export List to CSV dialog box appears.
4. Review the dialog box and verify the information is correct.
5. Click *Export*. The CSV file is sent to the specified email address.

The following table provides descriptions of the columns in the CSV file.

Table 5.3 CSV File Field Descriptions

Column Name	Description
Id	Unique identification of the session
Name	Name of the session
TargetId	SIP address of the session target
TargetName	Name of the session target
TargetIpAddress	IP address of the session target
DeviceId	Unique identification of the device
ParentId	Unique identification of the parent session ("NA" if not applicable)
MergedGroupId	Unique identification of the merged group
ConnectionPath	Connection path of the session ("NA" if not applicable)
StartTime	Start time of the session
EndTime	End time of the session
Status	Status of the session
SessionMode	Mode of the session
CreateTime	Creation time of the session

Table 5.3 CSV File Field Descriptions (continued)

Column Name	Description
UpdateTime	Last update time of the session
DeleteTime	Deletion time of the session ("NA" if not applicable)
UsersSessions	List of user session details associated with the session
Username	Username of the user associated with the session
Mode	Mode of the user session: • SM_UNDEFINED = session is not yet defined • SM_NORMAL = normal active session that maybe shared with other users • SM_SHARING_ACTIVE = active sharing session (multiple users control keyboard and mouse. This session got approved by the primary user.) • SM_SHARING_PASSIVE = passive sharing session (No keyboard/mouse interaction and no Virtual Media, video only. This session got approved by the primary user.) • SM_STANDALONE_PASSIVE = standalone passive session. (No keyboard/mouse interaction and no Virtual Media, video only.). Session will not be interrupted for any sharing request. • SM_STEALTH = shared session in stealth mode (No keyboard/mouse interaction and no Virtual Media, video only and the session will be hidden to other shared users. When primary user closes the session, this session will be closed automatically.) • SM_EXCLUSIVE = private session that does not allow sharing by other users. While setting session as exclusive session, if there are any shared sessions then those sessions will be closed automatically.) • SM_PREEMPT = preempt session. Existing session will be preempted and this session will become primary session. • SM_LOCAL_PORT = sessions involving the local port (may not be shared/stealthed/anything)
State	State of the user session: • SS_PENDING = session is defined but not yet connected • SS_INITIATED = session initiated in the process to be connected • SS_CONNECTED = session is connected • SS_TERMINATED = session was terminated by another user • SS_EXPIRED = session was terminated (based on session timeout interval) • SS_REJECTED = session request to share read-only or interactive was rejected, session was never connected • SS_RECONNECTING = session got interrupted by network. Session is in re-connecting state • SS_RECONNECTED = failed to reconnect the session

Type	Type of user session:
	• ST_UNSPECIFIED = 0; // the value has not been specified
	• ST_KVM = remote Keyboard/Video/Mouse session
	• ST_VIRTUAL_MEDIA = remote Virtual Media session
	• ST_SERIAL = remote serial (such as RS-232) session
	• ST_VIRTUAL_MACHINE = remote Virtual Machine session
	• ST_SSH = remote SSH session
	• ST_NATIVE_WEB = allows user to access device's web interface
	• ST_SSH_PASSTHROUGH = remote SSH passthrough session
	• ST_LOCAL_KVM = remote Keyboard/Video/Mouse session (using local port)
	• ST_LOCAL_VM = remote Virtual Media session (using local port)
	• ST_LOCAL_SERIAL = remote serial (such as RS-232) session (using local port)

Table 5.3 CSV File Field Descriptions (continued)

Column Name	Description
Client	IP address of the client
StartTime	Start time of the user session
EndTime	End time of the user session

5.5 Administration

The Administration tab contains ten sub-menu items - User Management, Roles & Permissions, Events, Authentication Providers, Firmware Updates, System Settings, and Registration - from which administrators can access the advanced settings to configure and manage the switch and its target devices.

5.5.1 User management

From the User Management screen, administrators can efficiently manage access and permissions for both individual users and groups. The User Management screen is divided into two main tabs: Users and Groups. Each tab provides tools for creating, configuring, and deleting users and groups, as well as assigning roles and permissions. For more information about these tabs, see Users below and User groups on the facing page.

Permissions and access

The Avocent MergePoint Unity 2 switch provides a flexible and secure user management framework that allows administrators to define granular access controls based on roles and permissions. By default, all newly created users are assigned to the default Users group, except for the default Systems Administrator user which is automatically assigned administrator privileges. Administrators have full visibility and control across all target devices and system settings. However, non-administrator users must be added to a user group, and an administrator must assign target devices and permissions to that user group for access. For detailed instructions on creating user groups and assigning devices, refer to User groups on the facing page.

Users

View and navigate users

From the left-hand sidebar, click *Administration - User Management*, then click *Users*. The Users tab displays all users and their specific information. You can configure which columns are shown in the user table via the Table Configuration option.

Create a new user

1. In the Users tab, click the Add (+) icon in the top right corner. The Add User dialog box appears.
2. Enter the following details:
   - Full name
   - User name
   - Temporary password (minimum eight characters)
3. Click *Add User*.

Configure user properties

1. In the Users tab, open a user's information panel by clicking on the user's name.
2. Expand the Properties menu and click the Edit (pencil) icon to update the user's name, email, or password expiration time.
3. To set password expiration:
    a. Enable the field using the slider.
    b. Select a date and time using the calendar feature.
    c. (Optional) Use the 24-hour clock format.
    d. Click *Done*, then *Save*.

Delete a user

1. In the Users tab, hover over the desired user and check the box on the left.
2. Click the Delete (trash can) icon above the user list.
3. Confirm deletion by clicking *Yes*.

User groups

A user group defines what the user can do within the web UI and CLI, regarding appliance settings and administration. Pre-defined user groups include:

- System-Administrators
- System-Maintainers
- User-Administrators
- Users

For a specific example of creating and configuring a user group with specific permissions, refer to the Vertiv™ Avocent® Creating User Groups Technical Note.

View and navigate groups

From the left-hand sidebar, click *Administration - User Management*, then click *Groups*. The Groups tab displays all users and their specific information.

Create a new user group

1. In the Groups tab, click the Add (+) icon in the top right corner. The Add New Group dialog box appears.
2. Enter the group name and select users to add to the group.
3. Click *Add Group*.

NOTE: By default, new groups have no permissions.

Configure user group properties

1. In the Groups tab, open a group's information panel by clicking on the group's name.
    - Expand the Group Properties menu to view and configure the group name, preemption level, and assigned system roles.
    - Expand the Users menu to view and configure the assigned users.

- Expand the Targets menu to view and configure the assigned target devices.
- Expand the External Groups to view and configure the assigned external groups.

Assign permissions to a group

1. After creating a group in the Groups tab, open its side panel and click the Edit (pencil) icon next to Group Properties.
2. Under System Roles, select the roles to assign permissions.
3. Click *Save Changes* to apply the changes.

Assign target devices to a group

Target devices can be assigned to non-administrative users for limited access, depending on the system roles of the user.

1. In the Groups tab, open the group's information panel and click the Edit (pencil) icon next to Targets.
2. Select the devices to add and click *Save Changes*.

Map local user groups

The Avocent MergePoint Unity 2 switch supports mapping local user groups to external authentication provider user groups, such as those from Active Directory (AD) or LDAP. This capability allows administrators to configure local user groups, assign system and target roles, and link resource groups, ensuring that users from external authentication provider groups inherit the same permissions as local users. The mapping process involves setting up the external provider, creating, and configuring local groups and roles, and then associating external groups with local ones. For detailed instructions, refer to the Vertiv™ Avocent® Mapping User Groups Technical Note.

Delete a user group

1. In the Groups tab, hover over the desired group and check the box on the left.
2. Click the Delete (trash can) icon above the group list.
3. Confirm deletion by clicking *Yes*.

5.5.2 Roles and permissions

A user permission authorizes a user to perform a specific operation on a target or system. A role is a collection of user permissions. There are four default system roles and two default target roles. From the Roles & Permissions screen, you can perform the following functions:

- Add a new role
- Configure an existing role
- Delete a role

For more information about the default roles, refer to System Roles below and Target Roles on the facing page.

System Roles

A system role is a collection of user permissions that can be applied to a system. These roles can be configured and applied to a user group to permit specific system operations. For example, a system administrator with a system role that includes the permission to change the user password is allowed to change user passwords from the web User Interface (UI). The following list highlights the four default roles and their associated user groups:

- System Administrator Role – System Administrators

- System Maintainer Role – System Maintainers
- User Administrator Role – User Administrators
- User Role – Users

User groups can be configured with one or more system roles. The system role permissions assigned to a user group are available for any user within the user group. For more information on user group configurations, refer to User groups on page 21.

Target Roles

A target role is a collection of user permissions that can be applied to a target device. These roles can be configured and applied to a user group to permit specific operations on a target device. For example, a user with a target role that includes the user permission to establish KVM sessions is allowed to launch KVM sessions to target devices from the web UI. The following list highlights the two default target roles:

- User Target Role
- System Maintainer Target Role

User groups can be associated with one or more target roles.

Table 5.4 below describes the user permissions allowed for each system and target role. A checkmark indicates the permission listed in the left-hand column is allowed for the role. An "x" indicates the permission is not allowed.

Table 5.4 Roles and Permissions

User Permission	System Roles				Target Roles	
	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
Boot order Control	✓	✓	✗	✗	✗	✓
Browse Virtual Media Disk Image	✓	✓	✓	✓	✓	✓
Change User Password	✓	✓	✓	✓	✗	✗
Configure Appliance Settings	✓	✓	✗	✗	✗	✓
Configure Data Points	✗	✗	✗	✗	✗	✗
Configure Devices	✓	✓	✓	✓	✗	✓
Configure Event Data Retention Policy	✓	✓	✗	✗	✗	✗
Configure External Authentication	✓	✗	✓	✗	✗	✗
Configure KVM Session	✗	✗	✗	✗	✗	✗
Configure Local User Accounts	✓	✗	✓	✗	✗	✗

Table 5.4 Roles and Permissions (continued)

User Permission	System Roles				Target Roles	
	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
Configure Notification Settings	✓	✓	✖	✖	✖	✖
Configure Permissions	✓	✖	✓	✖	✖	✖
Configure Preferences	✓	✓	✓	✓	✖	✖
Configure Scheduled Jobs	✓	✓	✖	✖	✖	✖
Configure Serial Session	✖	✖	✖	✖	✖	✖
Configure Shutdown profiles	✓	✓	✖	✖	✖	✖
Configure Sys Log	✓	✓	✖	✖	✖	✖
Configure User Policy	✓	✖	✓	✖	✖	✖
Configure User Profile	✓	✓	✓	✓	✖	✖
Create ISO image file in KVM session	✓	✓	✖	✖	✖	✖
Establish Exclusive Session	✓	✖	✖	✖	✖	✖
Establish KVM Session	✓	✓	✓	✓	✓	✓
Establish Serial Session	✓	✓	✓	✓	✓	✓
Establish SSH Session	✓	✓	✓	✓	✓	✓
Establish Stealth Session	✖	✖	✖	✖	✖	✖
Establish Virtual Media Session	✓	✓	✓	✓	✓	✓
Establish VKVM Session	✓	✓	✖	✓	✓	✓
Establish VNC Session	✓	✓	✖	✓	✓	✓
General Use	✓	✓	✓	✓	✖	✖

Table 5.4 Roles and Permissions (continued)

User Permission	System Roles				Target Roles	
	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
KVM Clipboard paste	✓	✓	✗	✗	✗	✓
KVM Paste text from file	✓	✓	✗	✗	✗	✓
KVM Remote Audio	✓	✓	✗	✗	✗	✓
KVM Screen capture	✓	✓	✗	✗	✗	✓
KVM Screen recording	✓	✓	✗	✗	✗	✓
Launch standalone passive KVM session	✓	✓	✓	✓	✓	✓
Led Control	✓	✓	✗	✗	✗	✓
Posts to Event Log	✓	✓	✗	✗	✗	✗
Power Control	✓	✓	✗	✗	✗	✓
Purge Event Log	✓	✗	✗	✗	✗	✗
Reboot Appliance	✓	✓	✗	✗	✗	✓
Reboot Server	✓	✗	✗	✗	✗	✗
Reset Appliance To Factory Defaults	✓	✓	✗	✗	✗	✓
Reset Control	✓	✓	✗	✗	✗	✓
Restart Control	✓	✓	✗	✗	✗	✓
Run Shutdown profiles	✓	✓	✗	✗	✗	✗
Shutdown Server	✓	✗	✗	✗	✗	✗
Stop active standalone KVM passive sessions	✗	✓	✓	✓	✓	✓
Terminate Target Session	✓	✗	✗	✗	✗	✗
Token for Web socket connections	✓	✓	✗	✓	✗	✗
Update Appliance SSL Certs	✗	✗	✗	✗	✗	✗

Table 5.4 Roles and Permissions (continued)

User Permission	System Roles				Target Roles	
	System Administrator Role	System Maintainer Role	User Administrator Role	User Role	User Target Role	System Maintainer Target Role
Upgrade Firmware	✓	✓	✖	✖	✖	✓
View Appliance Settings	✓	✓	✖	✖	✖	✓
View Appliance SSL Certs	✖	✖	✖	✖	✖	✖
View Devices	✓	✓	✓	✓	✓	✓
View Event Data Retention Policy	✓	✓	✖	✖	✖	✖
View Event Log	✓	✓	✖	✖	✖	✖
View External Authentication	✓	✖	✓	✖	✖	✖
View Local User Accounts	✓	✖	✓	✖	✖	✖
View Notification Settings	✓	✓	✖	✖	✖	✖
View Organizations	✓	✓	✓	✓	✓	✓
View Permissions	✓	✖	✓	✖	✖	✖
View Preferences	✓	✓	✓	✓	✖	✖
View Scheduled Jobs	✓	✓	✖	✖	✖	✖
View Shutdown profiles	✓	✓	✓	✓	✖	✖
View Sys Log	✓	✓	✖	✖	✖	✖
View System Logs	✓	✓	✖	✖	✖	✖
View Target Sessions	✓	✓	✓	✖	✖	✓
View User Policy	✓	✖	✓	✖	✖	✖
View User Sessions	✓	✖	✓	✖	✖	✖
Write to Virtual Media Disk Image	✓	✓	✓	✓	✓	✓

Add a new role

You can create a custom system or target role to which user permissions can be assigned.

To add a new role:

1. From the left-hand sidebar, click *Administration - Roles & Permissions*.
2. Select the *Target Roles* tab to create a target role.

   -or-

   Select the *System Roles* tab to create a system role.
3. Click the Add New Role icon (+) in the top right corner.
4. Enter a name and description for the role.
5. Check the desired box(es) to add permissions.

   -or-

   Check the Select All box to add all permissions.
6. Click *Add Role*.

Configure an existing role

NOTE: The default roles cannot be configured.

To configure an existing role:

1. From the left-hand sidebar, click *Administration - Roles & Permissions*.
2. Click a role to open its sidebar.
3. Expand *Properties* and click the Edit icon (pencil) to configure the description for the role.
4. Expand *Permissions* and click the Edit icon (pencil) to configure the permissions for the role.
5. Click *Save*.

Delete a role

NOTE: The default roles cannot be deleted.

To delete a role:

1. From the left-hand sidebar, click *Administration - Roles & Permissions*.
2. Hover the mouse over the desired target and check the box to the left.
3. Click the Delete icon (trash can).
4. At the confirmation screen, click *Yes* to delete.

5.5.3 Events

From the Events screen, you can view the saved log of events that have occurred and perform the following functions:

- Search for a specific event using the search bar.
- Filter events by severity (*All Severities, Info, Warning* or *Critical*) using the Filters drop-down menu.
- Sort events in ascending or descending order by clicking the arrows next to each column.
- View the information panel for each event by clicking on the desired event.

5.5.4 Authentication providers

From the Authentication Providers screen, you can view the list of configured authentication providers. You can also perform the following functions:

- Add a new provider
- Update the order of providers
- Delete an existing provider

For mapping local user groups to external authentication user groups, refer to User groups on page 21.

Add a new authentication provider

Providers can be authenticated locally or via AD/LDAP, TACACS+, or RADIUS. For the LDAP method, the Avocent MergePoint Unity 2 switch supports remote group authorizations.

NOTE: The authentication method chosen to configure the Avocent MergePoint Unity 2 switch is used for authenticating every user that attempts to log in through SSH or the web UI.

To add an authentication provider:

1. From the left-hand sidebar, click *Administration - Authentication Providers*.
2. Click the Add icon (+) in the top right corner.
3. Select *AD/LDAP, TACACS+* or *RADIUS* as the authentication type from the drop-down menu. A dialog box appears for the chosen authentication type.
4. Enter the required configuration information for your authentication server.
5. When finished, click *Add Provider*.

To enable an authentication provider:

1. From the left-hand sidebar, click *Administration - Authentication Providers*.
2. Click the vertical ellipsis next to the desired provider.
3. Click *Enable*.

Update the order of authentication providers

To ensure the most secure and preferred authentication methods are prioritized, you can adjust the order of authentication providers on the appliance. This helps in managing access control by determining which authentication provider is used first.

To update the providers order:

1. From the left-hand sidebar, click *Administration - Authentication Providers*.
2. Click the Add icon (+) in the top right corner.
3. Select *Update providers order* in the drop-down menu.
4. Use the right-hand drag icon to rearrange the providers as desired.
5. When finished, click *Update Order*.

Delete an authentication provider

To delete an authentication provider:

1. From the left-hand sidebar, click *Administration - Authentication Providers*.

2. Click the vertical ellipsis next to the desired provider.
3. Click the Delete icon (trash can).
4. At confirmation screen, click *Yes* to delete.

5.5.5 Firmware updates

From the Firmware Updates screen, you can perform the following functions:

- View the status of the firmware update by clicking the plus symbol (+) on the left side of the row.
- Refresh the page by clicking the Refresh icon in the top right corner.
- Configure the columns displayed in the table by clicking the vertical ellipsis in the right corner of the table and clicking *Table Configuration*.

For information on updating the firmware, refer to Overview on page 14.

5.5.6 System settings

From the System Settings screen, administrators can view and configure the system settings for the Avocent MergePoint Unity 2 switch. System settings include the following:

- Password policy
- Lockout policy
- Timeout
- Date and time
- Events retention
- Viewer settings
- Standalone KVM viewer settings
- KVM session settings
- FIPS module
- Syslog destination
- Email server configuration
- Notification configuration
- Certificate
- Reboot appliance
- Factory reset

NOTE: All configurations described in this section can be performed from the *Administration - System Settings* screen. Use the sidebar menu to navigate through the System Settings page.

Password policy

You can configure global password rules for all user accounts and configure expiration settings. By default, passwords must have a minimum of eight characters and all other password expiration rules are pre-defined. The maximum number of characters permitted is 64.

NOTE: When the global password policy is updated for enhanced security, all local user accounts will be flagged to change the password at the next login.

To configure the password policy:

1. From the sidebar of the System Settings screen, click *Password Policy*.
2. Use the toggle buttons and provided fields to configure the password settings.

Lockout policy

You can configure global lockout rules for all user accounts. By default, a user is locked out of the UI after three failed login attempts. After 20 minutes, the user's account is unlocked, and they may attempt to login again.

To configure the lockout policy:

1. From the sidebar of the System Settings screen, click *Lockout Policy*.
2. Click the Lockout toggle button to enable or disable lockout. If enabled, the user account will be locked out after a set number of failed login attempts.
3. In the Failed Login Attempts field, enter the number of failed login attempts a user is permitted before their account is locked.
4. Click the Login Retry Timeout toggle button to enable or disable a timeout that will force the user to wait before logging in after each failed attempt.
5. If you enabled the Login Retry Timeout button, enter the duration of the timeout in the Retry Timeout field.
6. Click the Automatically Unlock Account toggle button to unlock the account that was locked out after a set amount of time.
7. If you enabled the Automatically Unlock Account button, enter the duration of time before the account is automatically unlocked in the Automatic Unlock Time field.

Timeout

You can configure the global inactivity timeout for the application and the viewer. When the inactivity threshold is reached, the user session will be disconnected. By default, both the application and viewer timeout is enabled with a time limit of 30 minutes.

To configure the inactivity timeout settings:

1. From the sidebar of the System Settings screen, click *Timeout*.
2. Click the toggle button to enable or disable automatic log out of a user account after a set time of inactivity.
3. If enabled, enter the duration of time a user can be inactive before the viewer session times out and closes.
4. Click *Save*.

Date and time

You can view the current date and time, manually configure the date and time settings or use an Network Time Protocol (NTP) server.

To configure the date and time settings:

1. From the sidebar of the System Settings screen, click *Date and Time*.
2. Click the Configure Date and Time radio button to manually set the date and time.

   -or-

   Click the Use NTP Server radio button to synchronize the date and time with the server.

3. Click Save.

Events retention

You can determine the number of days (1-60) before events are automatically purged from the system.

To configure the events retention policy:

1. From the sidebar of the System Settings screen, click *Events Retention*.
2. In the Purge events section, use the slider to set the number of days before the events are purged.
3. In the Events Archiving section, click the Archive and delete radio button to archive the events before they are deleted.

   -or-

   Click the Delete radio button to delete the events after the set number of days for purging events passes.

   Click *Save*.

General viewer settings

You can configure the global inactivity timeout for the Video Viewer. When the inactivity threshold is reached, the viewer session will be disconnected. By default, the viewer timeout is enabled with a time limit of 30 minutes.

To configure the inactivity timeout settings for the Video Viewer:

1. From the sidebar of the System Settings screen, click *Viewer Settings*.
2. Click the toggle button to enable or disable automatic log out from a viewer session after a set time of inactivity.
3. If enabled, enter the duration of time a user can be inactive before the viewer session times out and closes.
4. Click *Save*.

Standalone KVM viewer settings

You can allow the system to launch standalone KVM sessions through the API, terminate standalone KVM sessions after a set time or inactivity, preempt standalone KVM sessions, and run standalone KVM sessions while running an exclusive KVM session.

To configure the standalone KVM viewer settings:

1. From the sidebar of the System Settings screen, click *Standalone KVM Viewer Settings*.
2. Click the Allow Standalone KVM Sessions toggle button to enable or disable the system to launch standalone KVM sessions through the API.
3. Click the Allow Preemption of Standalone KVM Sessions to enable or disable other users from interrupting active sessions.
4. Click the Standalone KVM Viewer Inactivity Timeout toggle button to enable or disable the system to terminate the session after a set time of inactivity.
5. If the Standalone KVM Viewer Inactivity Timeout button is enabled, enter the duration of time a user can be inactive before the viewer sessions times out and closes.
6. Click the Allow Exclusive Sessions with Standalone KVM sessions toggle button to enable or disable the system to run standalone KVM session while simultaneously running an exclusive KVM session.
7. Click *Save*.

KVM session settings

NOTE: This section applies only to IQ modules.

You can adjust the display settings for the KVM sessions launched from the switch.

To adjust the KVM session settings:

1. From the sidebar of the System Settings screen, click *KVM Session Settings*.
2. Choose the desired video resolution from the drop-down menu: *Standard - 1024 x 900 (4:3), Widescreen - 1440 x 900 (16:10), Widescreen - 1920 x 1080 (16:9)* or *Widescreen - 1366 x 768 (16:9)*
3. Omit display modes with a refresh rate higher than 60 Hz by clicking the toggle button to enable the setting.
4. Click *Save*.

FIPS module

You can enhance the security of your Avocent MergePoint Unity 2 switch, particularly for protecting sensitive data, by enabling FIPS mode. The Avocent MergePoint Unity 2 switch uses the OpenSSLv3 cryptographic module that is based on the FIPS 140-2 validated cryptographic module (certificate number 4282). The FIPS mode of operation can be enabled or disabled via the OBWI and is executed after a reboot. When the FIPS module is enabled, it will take longer for the switch to reboot because it must complete a FIPS mode integrity check.

NOTE: The FIPS mode of operation is initially disabled and must be enabled to operate. Restoring the switch to the factory default setting will disable the FIPS module.

To enable FIPS mode:

1. From the sidebar of the System Settings screen, click *FIPS Module*.
2. Click the toggle button to enable FIPS mode.
3. From the sidebar, click *Reboot Appliance*.
4. Click the *Reboot* button. Upon reboot of the appliance, the FIPS mode is now enabled.

Syslog destination

You can configure the application to send all the audit events to your syslog server. The syslog server acts as the aggregation point for various different applications.

NOTE: The Audit Events page logs all user activities.

To set up Syslog Destination:

1. From the sidebar of the System Settings page, click *Syslog Destination*.
2. Click the plus icon (+) in the top right corner. An Add Syslog Destination dialogue box appears.
3. Select the protocol from the Protocol drop-down menu.

NOTE: The recommended secure option for the Syslog Remote Destination setting is TCP with TLS support.

4. (Optional) If using the TCP - Secure protocol option, enter a valid TLS certificate in the Certificate field.
5. In the Destination IP field, enter the IP address of the syslog server.

NOTE: Port 514 is the standard port for the syslog server, and this field should not be edited.

6. (Optional) Add a name to the Tag field, if desired.
7. Select the appropriate syslog facility from the Facility drop-down menu.

8. Click *Test Connection*. If the IP Address is valid, a *Test Connection Successful* message pops up. If invalid, a *Test Connection Failed* message pops up.
9. Click *Add*.
10. Click the toggle button to enable the syslog connection.

Email server configuration

You can enter email server information for both a primary and secondary account. This information will be used for sending system notifications.

To configure email server information:

1. From the sidebar of the System Settings screen, click *Email Server Configuration*.
2. Click the Edit icon (pencil) to configure either the primary or secondary email server information.
3. (Optional) After entering all required information, you can send a test email by entering an email address in the Test Email Server Configuration field and clicking the *Send Test Email* button.
4. Click *Save*.

NOTE: After configuring the email server information, you must enable the Sending Email setting to receive email notifications. For instructions, refer to Notification configuration below.

Notification configuration

You can enable or disable the system to send email notifications to the email address specified on the Email Server Configuration tab.

To configure email notifications:

1. From the sidebar of the System Settings screen, click *Notification Configuration*.
2. Click the toggle button to enable or disable the system to send email notifications.
3. Click *Save*.

Certificate

You can generate and install new certificate signing requests (CSRs), as well as download the certificate currently installed on the appliance.

To generate a new CSR:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Generate Certificate icon in the right corner. The Generate Certificate Signing Request dialog box appears.
3. Enter the required information: Common Name, Country.
4. (Optional) Enter additional information: State, City, Organization, Organization Unit, and Email. You can also optionally add a Subject Alternative Name (SAN).
5. Click *Generate*. The CSR downloads as a .csr file and is now ready to be installed on the appliance.

To install a CA-signed certificate:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Install Certificate icon in the right corner.
3. Browse to and select the .pem file assigned by a CA (Certificate Authority) with base64 PEM.

4. Click *Upload*.

To download the certificate currently installed on the appliance:

1. From the sidebar of the System Settings screen, click *Certificate*.
2. Click the Download Certificate icon in the right corner. The certificate.pem file downloads to your local system.

Reboot appliance

You can reboot the appliance. Rebooting the appliance will log you out of the system.

To reboot the appliance:

1. From the sidebar of the System Settings screen, click *Reboot Appliance*.
2. Click the *Reboot* button.
3. A message appears, prompting you to confirm your reboot request. Click *Reboot*.

Factory reset

Resetting the switch can be useful in various scenarios, such as troubleshooting, re-purposing the device, or preparing it for a new user. You can reset your switch by one of three options: clearing the current firmware image, restoring the previous firmware image, or restoring factory settings. You can also choose to preserve the current network settings during the reset, if desired.

NOTE: When performing a factory reset, allow the system additional time to complete and automatically reboot the appliance. Do not perform another factory reset at this time.

To perform a factory reset:

1. From the sidebar of the System Settings screen, click on the *Factory Reset* tab.
2. Click the orange *Factory Reset* button. The Factory Reset dialog box appears.
3. If you wish to retain your current network settings, click the Preserve Network Settings radio button.

   -or-

   If you wish to delete all current configuration settings and files, click the Reset All radio button.
4. Under the Firmware Image heading, select the radio button for the firmware image that will be restored or retained.
   - Retain Current: If selected, this option clears all data on the current firmware image.
   - Restore Previous: If selected, this option restores the firmware image that was previously running on the appliance. If the firmware has not yet been updated to a new version, then this option will be grayed out.
   - Restore Factory: If selected, this option clears all data and restores the factory firmware image.
5. Click *Continue*. A confirmation page appears.
6. Review your selections and click *Yes, Reset*. The system will reboot, and your changes will be reflected.

5.5.7 Registration

From the Registration screen, you can configure the operating mode of the Avocent MergePoint Unity 2 switch. The device can be operated completely standalone or can be managed by the Vertiv™ Avocent® MP1000 Management Platform.

To enable Managed mode:

1. From the left-hand sidebar, click *Administration - Registration*.
2. Click the Enrollable toggle button to enable Managed mode.
3. In the Manager IP Address, enter the IP address of the management platform.
4. In the Manager Port field, enter the number for the HTTPS port used by the management platform.
5. Click *Apply*.

5.6 Network Configuration

The Network Configuration tab contains one sub-menu item - Settings - from which you can view and configure the network settings for the Avocent MergePoint Unity 2 switch, including the hostname, failover-bonded settings, failover-routed IPv4 routed trigger mode, and Ethernet interfaces.

NOTE: All configurations described in this section can be performed from the *Network Configuration - Settings* screen. You can use the sidebar menu to navigate through the Settings page.

5.6.1 Settings

From the Settings screen, you can configure the following:

- Network settings
- Protocol settings
- Normal/Failover-bonded settings
- Failover-routed IPv4 trigger mode
- Ethernet interfaces

5.6.2 Network settings

You can view and configure the hostname, primary DNS, secondary DNS and domain name.

To configure the general network settings:

1. From the sidebar of the Settings screen, click *Network Settings*.
2. Under the Network Settings heading, modify the hostname, primary and secondary DNS, and domain name as needed.

NOTE: The primary and secondary DNS and domain name can be modified only when the system is configured with a static IP address.

3. Click *Save*.

5.6.3 Protocol settings

You can configure the web server with HTTPS and enable or disable console access via SSH.

5.6.4 Normal/Failover-bonded settings

The Avocent MergePoint Unity 2 switchphysical network interface ports that can be configured for bonding and/or failover.

NOTE: The device must be rebooted for changes to take effect.

To configure failover for the network interface ports:

1. From the sidebar of the Settings screen, click *Normal/Failover-Bonded Settings*.
2. Using the Uplinks drop-down menu, select either *Ports not bonded, 1st and 2nd ports bonded* or *1st fails over to 2nd port*.
3. A message appears, prompting you to confirm your selection. Click *Yes, Update*. To determine when failover is initiated, refer to Failover-routed IPv4 trigger mode below.

5.6.5 Failover-routed IPv4 trigger mode

You can use the failover-routed IPv4 trigger mode to configure the trigger for initiating failover.

NOTE: The device must be rebooted for changes to take effect.

To configure the trigger mode for failover:

1. From the sidebar of the Settings screen, click *Failover-Routed IPv4 Trigger Mode*.
2. Under the Failover-Routed IPv4 Trigger Mode, select either the *Primary Interface Down,Unreachable Default Gateway* or *Unreachable IP* radio button. If you select *Unreachable IP*, then fill out the IP Address field.

5.6.6 Ethernet interfaces

The Avocent MergePoint Unity 2 switch has two physical network interfaces (eth0, eth1). Each interface has an individual MAC address and can be assigned an IP address via DHCP or statically. The Ethernet Interfaces tab allows you to configure the static IP address for the switch.

To configure a static IP address:

1. From the sidebar of the Settings screen, click *Ethernet Interfaces*.
2. Click the desired interface to open its information panel.
3. Expand *Network Configuration* to view the settings for the selected interface.
4. Click the Edit icon (pencil) to configure the selected interface.
5. For assigning a static IP, enter the IP address, prefix length and gateway address in the appropriate fields and click *Save*.

Appendices

Appendix A: Technical Support and Contacts

A.1 Technical Support/Service in the United States

Vertiv Avocent IT Management Software and Hardware Support Contacts

Phone: 1-888-793-8763

Website: https://www.vertiv.com/en-us/support/warranty/it-management-hardware-support-contacts/

Email: support.avocent@vertiv.com

A.2 Locations

United States

Vertiv Headquarters

505 N Cleveland Ave

Westerville, OH 43082

Europe

Via Leonardo Da Vinci 8 Zona Industriale Tognana

35028 Piove Di Sacco (PD) Italy

Asia

7/F, Dah Sing Financial Centre

3108 Gloucester Road, Wanchai

Hong Kong

This page intentionally left blank

Connect with Vertiv on Social Media

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

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

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

 https://www.x.com/Vertiv/

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

590-2387-501A