



Avocent® IPUHD 4k IP KVM Device

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
1.1 Product Overview	1
1.2 Features and Benefits	2
1.3 Installation and Initial Setup	3
2 Web User Interface (UI)	5
2.1 Account Settings	6
2.2 Dashboard	6
2.3 System Configuration	6
2.3.1 Registration	6
2.3.2 User management	7
2.3.3 Services	8
2.3.4 Date and time	8
2.3.5 System settings	8
2.3.6 Certificate	9
2.3.7 Troubleshooting	10
2.3.8 Remote syslog	10
2.3.9 Remote authentication	10
2.4 Interface Configuration	12
2.4.1 Network	12
2.4.2 Serial interfaces	13
2.5 Logs	13
2.5.1 Audit	13
2.5.2 Diagnostics	14
2.6 Sessions	14
2.6.1 KVM sessions	14
2.6.2 Serial sessions	20
2.7 Firmware	20
2.7.1 Firmware management	20
2.7.2 Firmware inventory	21
2.8 Remote Media	21
3 Security Best Practices	23
3.1 Risk Assessment	24
3.2 Physical Security	24
3.3 Account Access	24
Appendices	25
Appendix A: Technical Specifications	25

This page intentionally left blank

1 Getting Started

1.1 Product Overview

The Avocent IPUHD 4K IP KVM device offers remote access to servers with up to 4K video resolution, increasing productivity and efficiency for users. The IP KVM device can be used as a standalone device with the Vertiv™ Avocent® IPPS Power Supply or can be seamlessly integrated with the Vertiv™ Avocent® RM1048P Rack Manager and the Vertiv™ Avocent® MP1000 Management Platform. This flexibility and scalability allows for KVM usage to be managed and controlled securely at a holistic and granular level.

Figure 1.1 Avocent IPUHD 4K IP KVM Device Descriptions

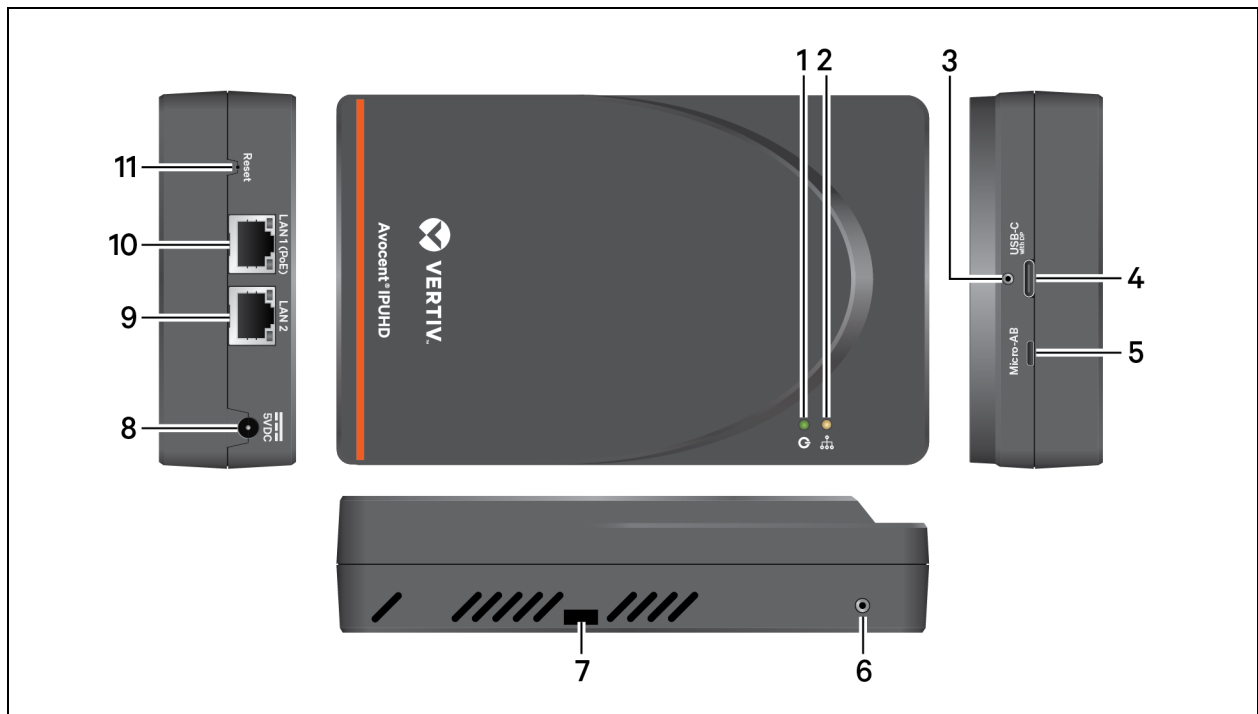



Table 1.1 Avocent IPUHD 4K IP KVM Device Descriptions

Item	Description	Item	Description
1	Power indicator	7	Tie-wrap mounting point
2	Activity indicator	8	Power input
3	USB-C cable retention point	9	LAN2 port
4	USB-C port	10	LAN1 (with PoE) port
5	Micro-AB port	11	Reset button
6	Future accessory attachment point		

The Avocent IPUHD 4K IP KVM device has LED indicators for both power and activity. The following table defines the indicators.

Table 1.2 LED Indicator Descriptions

Indicator	Description
Power LED	
Blinking red	The Avocent IPUHD 4K IP KVM device is booting up.
Solid red	Fully booted and is now accessible
Solid green	Video signal from a target is detected
Activity LED	
Off	No activity detected
Solid green	Any session type is active
Blinking blue	Locator function has been activated, either locally or remote
 CAUTION: During a firmware update or when the Avocent IPUHD 4K IP KVM device is being reset to factory defaults, both the power and activity LEDs blink red. During this time, you must not remove the Avocent IPUHD 4K IP KVM device, otherwise you may corrupt the firmware.	

The Avocent IPUHD 4K IP KVM device also has a Reset button that can be used to activate locator mode or reset the device as per the below conditions:

Press and hold the **Reset** button.

- For less than two seconds to activate locator mode.
- If locator mode is on, press and hold for less than two seconds to turn it off.
- For two to eight seconds to reboot the Avocent IPUHD 4K IP KVM device.
- For more than eight seconds to reset to factory default settings. This erases all configuration and settings on the Avocent IPUHD 4K IP KVM device.

1.2 Features and Benefits

The Avocent IPUHD 4K IP KVM device provides the following benefits for your data center:

- Improves productivity by leveraging fast, responsive high-resolution video to access resources remotely.
- Performs work seamlessly without video latency or resolution issues.
- Increases operational flexibility with the use of native USB-C sources without requiring additional adapters.
- Provides remote serial access to servers to quickly troubleshoot problems without being present in the data center.
- Leverages Power over Ethernet (PoE) to reduce power costs and simplify cabling.
- Works as a standalone 4K device or as part of an integrated Vertiv™ Avocent® DSView™ Solution.
- Provides secure remote access to protect your on-premise business applications.
- Supports any remote work use case where high-resolution video and audio are required.
- Centralizes and protects your expensive IT equipment on-site while permitting remote access.
- Uses LED lights to quickly identify the location of your Avocent IPUHD 4K IP KVM device.
- Scales to meet your needs.

1.3 Installation and Initial Setup

For installation and initial network configuration instructions, see the Vertiv™ Avocent® IPUHD 4K IP KVM Device Quick Installation Guide provided with your device. This document is also available on the Avocent IPUHD 4K IP KVM device product page.

To navigate to the product page:

1. Go to www.Vertiv.com.
2. On the Search bar, type **IPUHD** and press **Enter**.
3. Click on *Vertiv™ Avocent® IPUHD 4K IP KVM*.
4. Scroll down and click on the *Documents & Downloads* tab.
5. A list of manuals appears. Click on *Vertiv™ Avocent® IPUHD 4K IP KVM Device Quick Installation Guide*. The PDF file opens in a new tab.

To navigate to the Release Notes page for Vertiv™ Avocent® IPUHD 4K IP KVM Device:

1. Go to www.Vertiv.com.
2. On the Search bar, type **IPUHD** and press **Enter**.
3. Click on *Vertiv™ Avocent® IPUHD 4K IP KVM*.
4. Scroll down and click on the *Documents & Downloads* tab.
5. Scroll down and click on *Vertiv™ Avocent® IPUHD 4K IP KVM Software Downloads*.

This page intentionally left blank

2 Web User Interface (UI)

Once you have connected the Avocent IPUHD 4K IP KVM device to a network and configured its IP address, you can access the Avocent IPUHD 4K IP KVM device directly through its 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 to the address of the Avocent IPUHD 4K IP KVM device.
2. At the login screen, enter your username and password.
3. Once you login, the Dashboard screen appears.

NOTE: By default, the IP KVM device is set to Managed mode upon initial login. Certain features under the System Configuration and Interface Configuration tabs are disabled in this mode. To configure the mode of the IP KVM device, refer to [Registration](#) on the next page.

Figure 2.1 Web UI Overview

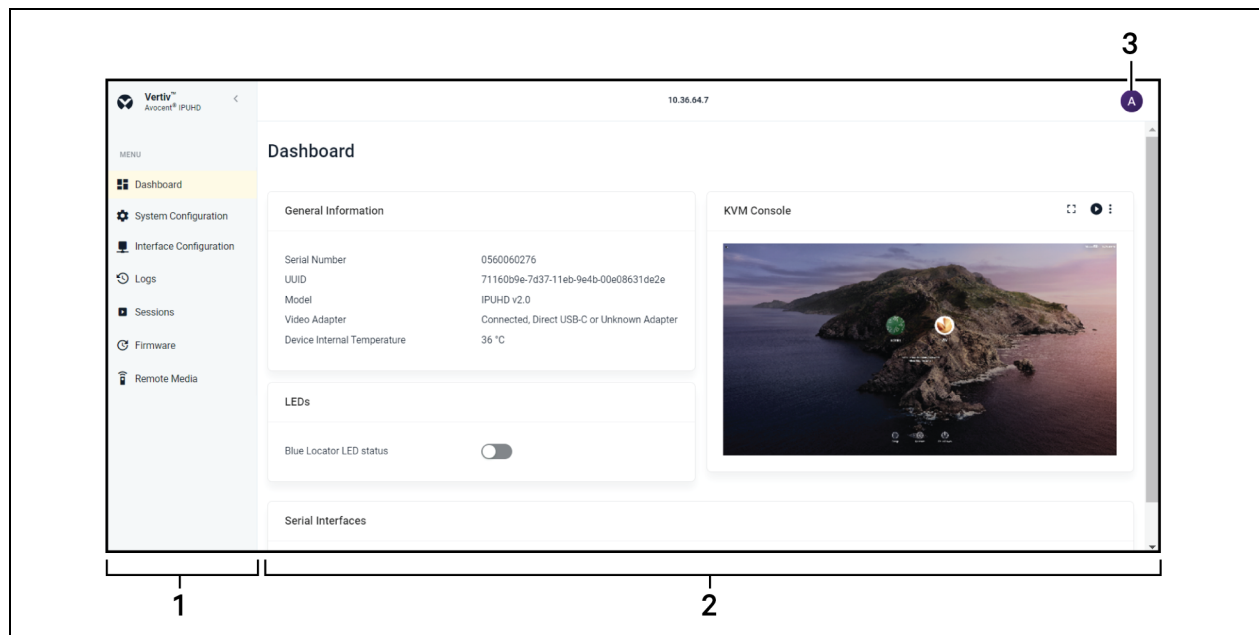


Table 2.1 Web UI Overview Descriptions

Item	Description
1	Sidebar
2	Content area
3	User preferences

2.1 Account Settings

You can view your account settings by clicking the profile icon in the top right corner of the web UI. The pop-up menu displays the name of the user currently logged in and the firmware version number of the device and allows you to choose from the Help and Log Out options.

Help

This option redirects you to a digital copy of the Vertiv™ Avocent® IPUHD 4K IP KVM Device Installer/User Guide.

Log Out

This option immediately logs you out of the web UI.

2.2 Dashboard

From the Dashboard screen, you can view general device information, including the serial number, UUID, model type, video adapter, and the internal device temperature. You can also view information related to the serial interfaces associated with the Avocent IPUHD 4K IP KVM device and an audited log of events for the device.

NOTE: If using an older version of the Vertiv™ Avocent® 4K IP KVM adapter or when the Avocent IPUHD 4K IP KVM device is connected directly to a USB-C target without an adapter, the Video Adapter information line will read "Direct USB-C or Unknown Adapter." If using the newest adapter, then the type of connected adapter (HDMI, DP) will be shown.

To navigate the Dashboard screen:

From the left-hand sidebar, click *Dashboard*. On this screen, you can perform the following functions:

- From the KVM Console section, launch a KVM session by clicking the Launch Viewer icon. Click the vertical ellipsis to launch the session in a new tab or window. Click the Full Screen icon to maximize the window.
- From the LEDs section, enable or disable the blue locator LED status by clicking the toggle button.
- From the Serial Interfaces section, launch a serial session by clicking the Launch Viewer icon on the right side of the column. Click the vertical ellipsis to launch the session in a new tab or window.

2.3 System Configuration

The System Configuration tab contains nine sub-menu items - Registration, User Management, Services, Date/Time, System Settings, Certificate, Troubleshooting, Remote Syslog and Remote Authentication - from which you can access the advanced settings to configure and manage the Avocent IPUHD 4K IP KVM device.

2.3.1 Registration

From the Registration screen, you can configure the operating mode of the Avocent IPUHD 4K IP KVM device. The device can be operated completely standalone or can be managed by one of the management appliances included in the Vertiv™ Avocent® DSView™ Solution (Vertiv™ Avocent® RM1048P Rack Manager or Vertiv™ Avocent® MP1000 Management Platform).

NOTE: When the device is in Managed mode, all web UI control features in the System Configuration and Interface Configuration tabs are disabled, except for Registration and Serial Interfaces.

To configure the operating mode:

1. From the left-hand sidebar, click *System Configuration - Registration*.
2. Click the Standalone radio button to set the device to Standalone mode.

-or-

Click the Managed radio button to set the device in Managed mode.
3. If you selected Managed mode, enter the IP address of the appliance that will managed the IP KVM device (the Vertiv™ Avocent® RM1048P Rack Manager or the Vertiv™ Avocent® MP1000 Management Platform).

NOTE: When the Config via DHCP Enabled setting is enabled and the configuration items have been identified in the DHCP data, the registrar IP address is obtained from the DHCP server that assigned the IP address to the Avocent IPUHD 4K IP KVM device. When the Config via DHCP Enabled setting is disabled, the Registrar IP Address field is disregarded.

NOTE: The value in the Interval field is pre-defined and must not be changed as it is used only in specific troubleshooting situations.

4. Click *Apply*.

2.3.2 User management

From the User Management screen, you can view and configure the user and group accounts.

Based on your assigned permissions, access to ports may be restricted by an administrator. By default, the user is admin and the following are the three pre-defined user groups:

- Administrator
- Operator
- Read-only

To add a new user:

1. From the left-hand sidebar, click *System Configuration - User Management*.
2. Click the Add icon (+) in the top right corner. An Add User dialogue box appears.
3. Select the appropriate radio button for the state of the user: Enabled or Disabled.
4. Enter the user's name and password, then re-enter the password.
5. Choose the desired user role from the User Role drop-down menu.
6. Click *OK*.

To configure the password policies for users:

1. From the left-hand sidebar, click *System Configuration - User Management*.
2. Click the Settings icon in the top right corner. You are redirected to the System Settings page.
3. From the System Setting page, you can configure the password policy for users. See [Password policy](#) on the next page.
4. When finished, click *Apply* to save your changes.

To edit or delete a user:

1. From the left-hand sidebar, click *System Configuration - User Management*.
2. On the left side of the row for the desired user, click the vertical ellipsis.

3. To edit a user, click *Edit* and modify the information as needed, then click *OK*.

-or-

To delete a user, click *Delete*.

2.3.3 Services

From the Services screen, you can view the web server settings, including HTTP, HTTPS, port numbers and timeout duration. The timeout duration setting can be configured.

NOTE: The Timeout field has a minimum value of 30 and a maximum value of 86,400.

2.3.4 Date and time

From the Date/Time screen, you can manually configure the date and time or use a Network Time Protocol (NTP) server to synchronize the date and time with the server.

To manually configure the date and time:

1. From the left-hand sidebar, click *System Configuration - Date/Time*.
2. Under the Timezone heading, select the desired timezone from the Timezone drop-down list.
3. Select a date and time from the Date Time field.
4. Click *Apply*.

To add an NTP server:

1. From the left-hand sidebar, click *System Configuration - Date/Time*.
2. Under the Network Time Protocol (NTP) Settings, click the Enable Network Time Protocol toggle button. An Add NTP Server icon appears to the right of the toggle button.
3. Click the Add NTP Server icon and enter the server information.
4. Click *Apply*.

2.3.5 System settings

From the System Settings screen, you can view and configure the system settings for the Avocent IPUHD 4K IP KVM device.

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

Password policy

You can configure the 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.

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

To configure global password rules:

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

FIPS mode settings

You can enhance the security of your IP KVM device, particularly for protecting sensitive data, by enabling FIPS mode. By default, the FIPS mode of operation is disabled and needs to be enabled to modify or update.

NOTE: Enabling FIPS mode requires the appliance to be rebooted.

To enable FIPS mode:

1. From the side of the System Settings screen, click *FIPS Mode Settings*.
2. Click the toggle button to enable FIPS mode.
3. Click *Apply*.
4. Reboot the device. Refer to [Firmware](#) on page 20. Upon reboot, FIPS mode is now enabled.

Remote presence settings

You can configure the general operating system (OS) settings, including the Auto-Lock, Keep Awake and Silently Accept Session Sharing features. When the Silently Accept Session Sharing feature is enabled, multiple KVM sessions can be launched to the same target without notifying the user of the sharing condition.

To enable the Remote Presence settings:

1. From the side of the System Settings screen, click *Remote Presence Settings*.
2. Click the appropriate toggle button, and then click *Apply*.

NOTE: The Auto-Lock feature is not available for the Apple macOS.

2.3.6 Certificate

From the Certificate screen, you can generate a new certificate signing request (CSR), as well as update or download the certificate currently installed on the appliance. You can either use this screen to generate a CSR to get this signed by an external CA of choice or provide your own signed certificate to be uploaded as a .pem file.

To download a copy of the certificate currently installed on the device:

1. From the left-hand sidebar, click *System Configuration - Certificate - Certificate Info*.
2. Click the Download Certificate icon in the top right corner. The CSR downloads as a .pem file to your local system.

To generate a new CSR:

1. From the left-hand sidebar, click *System Configuration - Certificate - Generate CSR*.
2. Enter the required information in the provided fields.
3. Click *Generate*. The CSR downloads as a .pem file and is now ready to be uploaded on the device.

To upload a certificate:

NOTE: If you are providing your own certificate, then the .pem file must contain the private key of the certificate.

NOTE: Uploading a new certificate replaces the current certificate and requires you to login to the appliance again.

1. From the left-hand sidebar, click *Configuration - Certificate - Upload Certificate*.
2. Click the *Upload PEM* button.
3. Browse to and select the .pem file to upload.
4. Click *Open*. The CSR file uploads to the device.

2.3.7 Troubleshooting

From the Troubleshooting screen, you can utilize various diagnostic tools to perform troubleshooting. The three available test actions are Ping, Traceroute and TcpConnect. These diagnostic tools are described in the following table.

Table 2.2 Test Actions

Use this:	To do this:
Ping	Test and verify if the specified IP address exists and can accept requests. This is helpful for testing network connectivity and measuring response time.
Traceroute	View a map of how data is traveling from the device to the specified IP address. This is helpful for understanding the routing hops the data must travel through, as well as response delays and points of failure.
TcpConnect	Create a test connection between the client and a remote TCP host using the specified IP address and port number. This is helpful for testing the connectivity to the application layer through TCP.

To run a troubleshooting test:

1. From the left-hand sidebar, click *System Configuration - Troubleshooting*.
2. Select the type of test action: *Ping*, *Traceroute*, or *TcpConnect*.
3. Enter the IP address.

NOTE: This field accepts both the FQDN and IP format.

4. Check the Force IPv6 box if you wish to force FQDN addresses to conduct the troubleshooting test action over IPv6 rather than IPv4.

NOTE: IP addresses are automatically identified as IPv4 or IPv6.

5. If you selected the TcpConnect option, enter the port number.
6. Click *Submit*.

2.3.8 Remote syslog

From the Remote Syslog screen, you can add a remote syslog, which allows you to route log messages centrally over a network connection.

To add a remote syslog:

1. From the left-hand sidebar, click *System Configuration - Remote Syslog*.
2. Click the Add icon (+) in the top right corner.
3. Enter the destination of the syslog server in the following format: **syslog://[destination]**
4. Enter the certificate of the syslog server.
5. Select the certificate type from the Certificate Type drop-down menu.
6. Click OK. Once added, click the Refresh icon in the top right corner to view the remote syslog on this screen.

2.3.9 Remote authentication

From the Remote Authentication screen, you can implement an authentication method to ensure the security of your system and users. Supported authentication methods include LDAP, TACACS+ and RADIUS.

NOTE: The authentication method configured for the Avocent IPUHD 4K IP KVM device is used for the authentication of any user who attempts to login through SSH or the web UI.

Priority setting

To configure the order of priority for authentication methods:

1. From the left-hand sidebar, click *System Configuration - Remote Authentication - Priority Setting*.
2. Set the priority order for the various authentication methods using the Priority Setting drop-down menu. The options include:
 - Local - LDAP - TACACS+ - RADIUS
 - Local - TACACS+ - LDAP - RADIUS
3. Click *Apply*.

LDAP

To add an LDAP authentication method:

1. From the left-hand sidebar, click *System Configuration - Remote Authentication - LDAP*.
2. Click the Service Enabled toggle button to enable the LDAP service.
3. Enter the required information into the provided fields.
4. Click the Add Service Addresses icon (+) in the lower right corner to add an LDAP service address.
5. Enter the server address and server port number.
6. Role-based security can be enabled to map your Active Directory remote group to a role on the Avocent IPUHD 4K IP KVM device. Click the Add Remote Role Mapping icon (+) in the lower right corner to perform remote role mapping.

NOTE: When you are mapped to any local role and the related security is enabled and configured, Active Directory remote group provides you the related permission after login.

7. Enter the remote group name and select the local role from the drop-down menu.
8. Click *Apply*.

TACACS+

To add a TACACS+ authentication method:

1. From the left-hand sidebar, click *System Configuration - Remote Authentication - TACACS+*.
2. Click the Service Enabled toggle button to enable the TACACS+ service.
3. Enter the required information into the provided fields.
4. Click the Add Service Addresses icon (+) in the lower right corner to add a TACACS+ service address, and then enter the IP address.
5. Click *Apply*.

RADIUS service

NOTE: Only one service address can be added to the system at a time.

To add a RADIUS authentication method:

1. From the left-hand sidebar, click *System Configuration - Remote Authentication - RADIUS Service*.

2. Click the Service Enabled toggle button to enable the RADIUS service.
3. Enter the required information into the provided fields.
4. Click the Add Service Addresses icon (+) in the lower right corner to add a RADIUS service address, and then enter the IP address.
5. Click *Apply*.

2.4 Interface Configuration

The Interface Configuration tab contains two sub-menu items - Network and Serial Interfaces - from which you can configure system network settings and serial communication parameters for the Avocent IPUHD 4K IP KVM device.

2.4.1 Network

From the Network screen, you can view and configure network settings for the four network interfaces (eth0, eth1, ethbr0 and usb0). Each interface has an individual MAC address and can be assigned an IP address via DHCP or statically. The network settings can only be modified for the usb0 and ethbr0 interfaces; the eth0 and eth1 interfaces only reflect the link status of the two LAN ports, while ethbr0 is the logical bridged interface built from eth0 and eth1. The usb0 network settings are applicable when you connect a computer to the Avocent IPUHD 4K IP KVM device through the micro USB cable.

To configure the network interfaces:

1. From the left-hand sidebar, click *Interface Configuration - Network*.
2. Navigate to the section for either the ethbr0 interface or the usb0 interface. The following sub-sections can be configured, if applicable: Interface Settings, IPv4 Settings, IPv6 Settings and Domain Name Servers.
3. When finished, click *Apply*.

To create a static IP address for the usb0 interface:

1. From the left-hand sidebar, click *Interface Configuration - Network*.
2. Navigate to the section for the usb0 interface.
3. Under the IPv4 Settings heading, ensure the DHCP Enabled toggle button is disabled (grayed out).
4. Under either the IPv4 Settings or IPv6 Settings heading, configure the existing IP address entry.

-or-

Click the Add icon (+) to add a new IP address entry.

5. Enter the required information in the provided fields.
6. Click *Apply*.

To create a static IP address for the ethbr0 interface:

1. From the left-hand sidebar, click *Interface Configuration - Network*.
2. Navigate to the section for the ethbr0 interface.
3. Click the Interface Enabled toggle button to enable the interface.
4. Under either the IPv4 Settings or IPv6 Settings heading, configure the existing IP address entry.

-or-

Click the Add icon (+) to add a new IP address entry.

5. Enter the required information in the provided fields.

6. Click *Apply*.

To configure one or more static name server addresses:

1. From the left-hand sidebar, click *Interface Configuration - Network*.
2. Navigate to the section for the ethbr0 interface.
3. Under the Domain Name Servers heading, click the Add Name Server icon (+) on the right-hand side, then enter the static IP address for the server.
4. Click *Apply*.

NOTE: If no static name servers are configured, the Avocent IPUHD 4K IP KVM device will automatically populate the static name servers list from the currently active name servers when disabling DHCP.

2.4.2 Serial interfaces

From the Serial Interfaces screen, you can configure the serial communication parameters.

To configure the serial interfaces:

1. From the left-hand sidebar, click *Interface Configuration - Serial Interfaces*.
2. Click the Interface Enabled toggle button to enable the serial interface.

NOTE: If Interface Enabled option is disabled, you cannot launch serial sessions.

NOTE: If the SSH Enabled option is enabled, you will be connected to the serial port specified in the SSH Port field through the SSH client.

3. Use the drop-down menu to select the appropriate values for these fields:
 - Bit Rate
 - Stop Bits
 - Flow Control
 - Data Bits
 - Parity
4. Enter the desired name for the interface in the Display Name field. You can use the name of the port to which the device is connected. For example: IPSL RJ45 port 2.
5. Click *Apply*. When finished, the serial interface entries appear on the Dashboard screen where you can launch sessions.

NOTE: To set the default values, click the Refresh icon in the top right corner.

2.5 Logs

From the Logs screen, you can view the audited log of events that occur and generate a diagnostic data log. You can navigate between the AuditLog tab and the DiagnosticDump tab.

2.5.1 Audit

To navigate the AuditLog screen:

From the left-hand sidebar, click *Logs*, then click the *AuditLog* tab. On this screen, you can perform the following functions:

- Search for a specific event using the Search bar.

- Filter the log by name, resolution status or severity using the drop-down menu.
- Delete the log by clicking the Clear Log icon in the top right corner.
- Export the log by clicking the Export Log icon in the top right corner.
- Refresh the page by clicking the Refresh icon in the top right corner.

2.5.2 Diagnostics

To navigate the DiagnosticDump screen:

From the left-hand sidebar, click *Logs*, then click the *DiagnosticDump* tab. On this screen, you can perform the following functions:

- Search for a specific diagnostic log using the Search bar.
- Filter the log by data size, data URI or name using the drop-down menu.
- Generate a diagnostic log by clicking the Generate Diagnostic Log icon in the top right corner. This may take up to 30 seconds.
- Delete the log by clicking the Clear Log icon in the top right corner.
- Refresh the page by clicking the Refresh icon in the top right corner.
- Initiate the creation of a new Diagnostics Dump package by clicking the + button, and then download this new diagnostics dump from the list.

2.6 Sessions

From the Sessions screen, you can view session information for past and current sessions.

2.6.1 KVM sessions

The Avocent IPUHD 4K IP KVM device provides flexible, centralized control of data center servers and virtual media of remote branch offices where trained operators may be unavailable. The Avocent IPUHD 4K IP KVM device allows you to conduct a KVM session with one or more target devices attached to one or more KVM switches. In addition to controlling each target device, you can access target server files, manager software updates and execute operating system commands. Each time you connect to the Avocent IPUHD 4K IP KVM device, your session can be confined to a window on your desktop or expanded to fit your entire desktop.

This section covers the following topics for KVM sessions:

- [Supported browsers and processors](#)
- [Launching KVM sessions](#)
- [Configuring KVM sessions](#)
- [Using virtual media](#)
- [Sharing KVM sessions](#)
- [Reconnecting to KVM sessions](#)

Supported browsers and processors

The HTML5 Video Viewer supports the latest version of the following web browsers:

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

The following table describes the compatibility of the Video Viewer capabilities for each supported browser.

Table 2.3 KVM Viewer Feature Compatibility

Feature	Menu	Google Chrome	Microsoft Edge (Chromium Based)	Mozilla Firefox	Apple Safari
Recording	Tools -> Start Recording	✓	✓	✓	✗
Create ISO image	Tools -> Create Image or drag and drop in canvas	✓	✓	✗	✗
Map files and folders as ISO image	Virtual Media -> Map ISO image or drag and drop in canvas	✓	✓	✗	✗
Map removable disk or floppy disk images by drag and drop	Virtual Media -> Map Removable Disk/ Floppy Disk image	✓	✓	✗	✗

Launching KVM sessions

NOTE: An Operator or Administrator user role is required to launch KVM sessions.

To launch a KVM session:

1. From the left-hand sidebar, click *Dashboard*.
2. From the KVM Console section, click the Launch Viewer icon in the top right corner.
3. Click the vertical ellipsis in the top right corner to choose whether to open the session in a new tab or window.

To close a KVM session:

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

Configuring KVM sessions

After launching a KVM session, you can use the menu located at the top of the window to access the tabs described in the following table. You can also configure the settings of the Avocent IPUHD 4K IP KVM device using the Settings icon. **Table 2.4** on the next page provides descriptions of the various KVM features. The availability of the KVM Video Viewer features varies by device type.

Table 2.4 Video Viewer Tab Descriptions

Feature	Description
File	
Open Server-side Recording File	Open a recording file from the server.
Paste Text From File	Copy and paste text to the target.
View	
Audio & Video Options	<p>NOTE: These settings apply to all users.</p> <ul style="list-style-type: none"> Audio Configuration - Configure the number of audio channels and audio quality level. Video Color Settings - Display more color options to optimize fidelity or less colors to reduce the volume of data transferred on the network. The maximum speed is Grayscale 16 Shades, and the maximum video quality is Color 24 bit. Video Noise Filter - Enable noise filter for VGA or disable it for a digital video source. Video Lane Settings - Configure USB-C lane speed and view the number of current video lanes.
Refresh	Refresh the session.
Full Screen	Enable Full Screen mode with or without single-cursor mode.
Scaling	Adjust the size of the ratios of the session screen by configuring or selecting the Fit to Window, Stretch to Window or Zoom setting.
Max Resolution	Select the maximum target resolution for your KVM session. This setting applies to all users and affects the actual video resolution of your target systems OS.
Single Cursor	Enable single-cursor mode.
Statistics	View KVM statistics.
User Information	View general user information.
Status Bar	Display or hide the status bar at the bottom of the screen.
Macros	
Static Macros	<p>After you select the applicable operating system, select <i>Static Macros</i> to access the list of command strings that are valid for the selected operating system. Send a string of commands by clicking the desired string from the Static Macros list and clicking <i>Send</i>. The options in the drop-down list are pre-determined based on the macro set you select. If you are looking for a command string that does not appear in the list, verify that you have selected the correct operating system in the Manage Macros window.</p> <p>NOTE: It is recommended to use the Macros tab to send a command string to a server. This saves time and eliminates the risk of errors. Your client server will not be affected.</p>
Manage	Define macros from the Manage Macros window.
Tools	
User Preferences	Select the keyboard language and configure the settings for pasting text, dragging and dropping files/folders and recording.
Instant Message	Send a message to all users currently logged in.
Capture Screen	Capture a screenshot of the session.
Mouse Modes	Select a mouse mode: Absolute, Relative (no acceleration) or Relative
Align Local Cursor	Align the cursor with the view orientation of the session.
Reset Keyboard/Mouse	If you begin experiencing issues with your keyboard or mouse, you can reset the device.

Table 2.4 Video Viewer Tab Descriptions (continued)

Feature	Description
USB	
Virtual Keyboard	When enabled, the keyboard displays on the client's workstation and can be positioned anywhere in the window. Use the up and down arrows in the top right to change the size of the keyboard.
Start Recording	Begin recording a video of the session.
Optimize Network Bandwidth	Optimize your network bandwidth for better session performance.
Remote Audio	Enable or disable remote audio.
Create ISO Image	Create an ISO image to store data from the target session.
Browse Disk Image	Browse to a saved disk image.
Virtual Media	
See Using virtual media on the next page.	

The following table compares the Video Viewer features available for the Avocent IPUHD 4K IP KVM device and the Vertiv™ Avocent® IPIQ IP KVM device with the features available for the managing appliances (the management platform and the rack manager).

Table 2.5 Feature Comparison for Avocent IPUHD 4K IP KVM Device and Vertiv™ Avocent® IPIQ IP KVM Device Viewer

Feature	Standalone Avocent IPUHD 4K IP KVM Device	Vertiv™ Avocent® MP1000 Management Platform / Vertiv™ Avocent® RM1048P Rack Manager (Avocent IPUHD 4K IP KVM device)	Vertiv™ Avocent® MP1000 Management Platform / Vertiv™ Avocent® RM1048P Rack Manager (Vertiv™ Avocent® IPIQ IP KVM Device)
Option to play server-side recorded file (File -> Open Server-side Recording File)	✓	✗	✗
Video Noise Filter (View -> Audio and Video Options)	✓	✓	✗
Video Lane Settings (View -> Audio and Video Options)	✓	✓	✗
Remote Audio Support (View -> Audio and Video Options) Tools -> Remote Audio)	✓	✓	✗
Remote Audio Support Max Resolution Settings (View -> Max Resolution)	✓	✓	✗
User Information (View -> User)	✓	✗	✗

Table 2.5 Feature Comparison for Avocent IPUHD 4K IP KVM Device and Vertiv™ Avocent® IPIQ IP KVM Device Viewer (continued)

Feature	Standalone Avocent IPUHD 4K IP KVM Device	Vertiv™ Avocent® MP1000 Management Platform / Vertiv™ Avocent® RM1048P Rack Manager (Avocent IPUHD 4K IP KVM device)	Vertiv™ Avocent® MP1000 Management Platform / Vertiv™ Avocent® RM1048P Rack Manager (Vertiv™ Avocent® IPIQ IP KVM Device)
Information)			
Instant Message (Tools -> Instant Message)	✓	✗	✗
Optimize Network Bandwidth (Tools -> Optimize Network Bandwidth)	✓	✓	✗

Using virtual media

The Virtual Media feature allows you to map a physical drive on the client machine as a virtual drive on a target device. Also, you can use the client workstation to add and map an .iso and .img file as a virtual drive on a target device.

NOTE: Only one Virtual Media session can be active on a target device at one time.

Prerequisites

Before using the Virtual Media feature, ensure the following prerequisites are met:

- The target device must be connected to a KVM switch that supports virtual media with an IQ module that supports virtual media.
- The target device must be able to use the types of USB2 compatible media that you virtually map.
- The target device must support a portable USB memory device to map it on a client machine as a Virtual Media drive on the target device.
- You (or user group to which you belong) must have permission to establish Virtual Media sessions and/or reserved Virtual Media sessions to the target device.

To map a virtual media drive:

NOTE: To map a virtual media drive, you must launch a Video Viewer session. See [Launching KVM sessions](#) on page 15.

1. In the Virtual Media section of the client navigational toolbar, click *Connect*.
2. After the virtual media session is activated, use the Virtual Media drop-down menu to select the type of file to map. Select *Map ISO image* to map an .iso file.

-or-

Select either *Map Removable Disk* or *Map Floppy Disk* to map an .img file.

3. Select a file from the Open dialog box with an .iso or .img file extension, depending on your selection in step 2, then click *Open*.

4. If you wish to limit the mapped drive to read-only access, click the Read Only checkbox in the Virtual Disk Management dialogue box.

NOTE: If the Virtual Media session settings were previously configured so that all mapped drives must be read only, the Read Only checkbox will already be enabled and cannot be changed. You might wish to enable the checkbox if the session settings enabled read and write access, but you wish to limit a particular drive's access to read only.

5. Click *Map Drive*, then click *Close*. Mapping is now complete, and the drive can be used on the target device.

To unmap a virtual media drive:

1. From the KVM Video Viewer session, click the *Virtual Media* tab, then click the mapped drive you wish to unmap.

-or-

Click *Disconnect* to unmap all the drives.

2. At the prompt, click *Yes*.

Sharing KVM sessions

When you connect to a target server that is currently being accessed by another user, the Video Viewer allows you to choose how to connect to the server. The following table describes the four different session sharing options.

Table 2.6 Session Sharing Options

Option	Description
Active Sharing	You, as well as other users, can interact with the target.
Passive Sharing	Access is granted to the target in read-only mode. The other user knows you are viewing the session.
Preempt	The previous user's session is interrupted and terminated.
Stealth	Access is granted to the target in viewer-only mode. The other user does not know you are viewing the session.

If you are currently connected to a target server and another user attempts to share the session with you, the Video Viewer allows you to choose if and how you want the user to connect. You can choose to Approve, Reject or Allow as read-only. You can disable the session sharing function from the System Settings page. When disabled, all connecting clients can silently join the currently running KVM session with full access. For more information, refer to [Remote presence settings](#) on page 9.

Reconnecting to KVM sessions

Viewer Reconnect is a session capability available for the Vertiv™ Avocent® RM1048P Rack Manager, the Vertiv™ Avocent® MP1000 Management Platform, and the Vertiv™ Avocent® MP1000 Management Platform Virtual Appliance. Supported target devices for Viewer Reconnect include the Vertiv™ Avocent® IPIQ IP KVM device and the Avocent IPUHD 4K IP KVM device.

When a KVM session disconnects from the target device but still maintains a connection to the managing appliance, the viewer will automatically attempt to re-establish a connection to the target device.

NOTE: Viewer Reconnect also works for standalone KVM sessions launched from the web UI of the Avocent IPUHD 4K IP KVM device.

2.6.2 Serial sessions

The Avocent IPUHD 4K IP KVM device provides remote access to your serial devices. To modify your serial communication parameters, refer to [Serial interfaces](#) on page 13.

To connect the Avocent IPUHD 4K IP KVM device to a serial device:

1. Using a micro USB to USB-A OTG adapter, connect it to the micro USB port on the Avocent IPUHD 4K IP KVM device.
2. Connect the USB-A end of the OTG adapter to a USB to serial adapter.
3. Connect the serial adapter to your serial device.

NOTE: The Avocent IPUHD 4K IP KVM device only supports Prolific and FTDI based serial cables.

To launch a serial session:

1. From the left-hand sidebar, click *Dashboard*.
2. Under Serial Interfaces section, hover your mouse over the desired serial device.
3. On the right-hand side of the column, click the Launch Viewer icon.

-or-

Click the vertical ellipsis and select whether to launch the serial session in a new tab or new window.

To end a serial session:

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

2.7 Firmware

The Firmware tab contains two sub-menu items - Firmware Management and Firmware Inventory - from which you can reboot or reset the device and upgrade the firmware.

2.7.1 Firmware management

From the Firmware Management screen, you can reboot the main adapter and perform a factory reset upon firmware update for the Avocent IPUHD 4K IP KVM device.

To reboot the main adapter:

NOTE: This action changes the currently running firmware. By default, currently running firmware is primary firmware.

1. From the left-hand sidebar, click *Firmware - Firmware Management*.
2. Click on the drop-down arrow next to Reset Action and select *GracefulRestart*.
3. Click OK. The device reboots immediately.

To reset to default values on firmware update:

NOTE: This option is only applicable to currently running firmware.

4. From the left-hand sidebar, click *Firmware - Firmware Management*.
5. Click the Reset to Defaults on Firmware Update toggle button to enable this setting.
6. When finished, click *Apply*.

2.7.2 Firmware inventory

From the Firmware Inventory screen, you can view information about the main adapter firmware, such as the name, version, and status of the firmware. You can also upgrade the firmware.

NOTE: Before upgrading the firmware, ensure the Avocent IPUHD 4K IP KVM device is in Standalone mode.

To upgrade the main adapter firmware:

1. From the *Firmware - Firmware Inventory* screen, click the *Update* button.
2. Copy the tftp file path and paste it in the TFTP Path field.

-or-

Click on *Image Upload* to drag and drop your file/folder.

-or-

Browse to and choose the file for updating firmware.
3. Click *Start Update*.

2.8 Remote Media

From the Remote Media screen, you can add and configure remote media drives to remotely store and manage digital media files for the Avocent IPUHD 4K IP KVM device. By default, this feature is disabled. To enable it, use the radio button at the top of the page. Once enabled, new drive letters will appear in the host operating system where the Avocent IPUHD 4K IP KVM device is connected. Additionally, you can attach one or more of the supported media types. The supported drive types are CDs/DVDs, floppy disks and removable disks.

To configure a remote server location:

1. From the left-hand sidebar, click *Remote Media*.
2. Select the type of file to map. Select *Virtual CD/DVD* to map an .iso file or select either *Virtual Floppy* or *Virtual Removable Disk* to map an .img file.
3. Copy the file path for the .iso file that is located on the CIFS server and paste it in the Image File Path field.
4. Use the drop-down menu to select the Transfer Protocol: *CIFS* or *NFS*

NOTE: By default, the Transfer Protocol is set to CIFS.

5. Enter the credentials (username and password).
6. Click on *Mount Image Path*. Once the physical drive or image is mapped, it can be used on the remote target device.

This page intentionally left blank

3 Security Best Practices

The default settings on the card are configured for security at the time of deployment. Ensuring the security of critical infrastructure equipment necessitates the proper configuration of all communication services. This section provides a summary of these settings.

Through our Vertiv SECURE product life cycle, Vertiv is dedicated to reducing cybersecurity risks in our products. We achieve this by applying cybersecurity best practices throughout the engineering design of our products and solutions, making them more secure, reliable, and competitive for our customers.

Below are some cybersecurity recommendations for various life cycle phases. These recommendations are intended to complement a customer's existing cybersecurity programs rather than serve as a comprehensive guide. For more information on general cybersecurity best practices and guidelines, you can visit the following sites:

<https://www.cisa.gov/topics/cybersecurity-best-practices>

<https://www.vertiv.com/en-us/support/security-support-center/>

Table 3.1 below provides a list of items to review. Each item should be assessed and configured according to the operational needs for managing the equipment. It is important to verify that the settings support the desired operational functionality without introducing unnecessary or unauthorized access to critical infrastructure. A reference to the appropriate section in this document is included for configuring each item.

Table 3.1 Settings to Review and Verify to Reduce the Risk of Unauthorized Access

Item	Description	Comments
Accounts and Passwords	Change the default admin user's password immediately to eliminate default credential access.	Enforced at first login
Remote Account Providers	Only enable Remote Account Providers (LDAP, TACACs, Radius) when needed	See Remote authentication on page 10.
TLS Certificates	Install your own TLS Certificates from a trusted certificate authority or generate alternative self-signed certificates.	See Certificate on page 9.

Table 3.2 below provides a list of ports used by this product. To enhance security, the local network firewall and gateway may be configured to permit only essential traffic on specific network ports.

NOTE: Some port settings may be modified by the administrator.

Table 3.2 Network Ports Open/Listened to by the Avocent IPUHD 4K IP KVM Device

Network Service	Port Used	Default	Modification Possible by Admin
HTTP	TCP 80	Y	N (redirect to 443)
HTTPS	TCP 443	Y	N
mDNS	UDP 5353	Y	N

3.1 Risk Assessment

Vertiv recommends performing a risk assessment to identify and evaluate potential internal and external risks to the security, availability, and integrity of the system and its environment. This assessment should be conducted in accordance with relevant technical and regulatory frameworks, such as IEC 62443 and NERC-CIP. Additionally, the risk assessment should be repeated periodically.

3.2 Physical Security

This product is designed to be deployed and operated in a physically secure location. Vertiv recommends reviewing the physical security and operating environment of the unit. Since both external attackers and insider threats can cause significant disruption, here are some best practice recommendations:

- Restrict access to areas, racks, and units through the use of encrypted RFID cards/badges, unique multi-factor passcode authentication, mantraps, and biometric scanners for physical access to the equipment.
- Employ trusted and background-checked security guards with a 24/7/365 presence, keeping written logs to document and track physical access to the data center, building, and racks.
- Limit physical access to telecommunications equipment and network cabling to protect against potential interception or sabotage. Best practices include using metal conduits for network cabling running between equipment cabinets.
- Restrict all USB, RJ45, and other physical ports on the units.
- Avoid connecting removable media (such as USB devices and SD cards) for any operations (like firmware upgrades, configuration changes, or boot application changes) unless the source of the media is known and trustworthy. Before connecting any portable device through a USB port or SD card slot, always scan the device for malware and viruses.

3.3 Account Access

The product's account access privileges should be managed to provide only the necessary functions that enable users to perform their job responsibilities. Access to the web UI should be limited to legitimate users. Organizations should adopt the following best practices in their written procedures for network and equipment access:

- The first login should require users to create their credentials.
- Account sharing is prohibited. Each user must have their own unique account and password. The audit logging functions expect every account to represent an individual, non-shared user.
- Administrators should restrict access and privileges to only what is required for each user's job responsibilities.
- Admin-level privileges, such as firmware updates and enabling or disabling protocols, should be limited to approved administrators.
- Enforce password strength, complexity, and length requirements at the highest level according to company IT policy.
- Ensure that terminated employees are immediately removed from accessing the product. This can be achieved using an AAA, TACACS+ user authentication process.
- Implement session timeouts after periods of inactivity.
- Utilize a remote syslog facility to monitor system and network events, security threats, and to troubleshoot device issues. This may also be required for compliance with PCI-DSS, SOX, or HIPAA regulations.

Appendices

Appendix A: Technical Specifications

Table A.1 Technical Specifications - Avocent IPUHD 4K IP KVM Device

Item	Value
Video	
Resolution	4K, 24-bit color up to 30Hz 1920 x 1200, 1920 x 1080, 1024 x 768, and lower resolutions up to 60HZ
Ports	
Network	2 x 1G LAN ports - 1 x PoE, 1 x Service Processor connectivity
Video In/Data	1 x USB-C with alt mode Display Port and Power Delivery
Audio	Delivered by target via HDMI or DP
Mono/Stereo	16-bit sampling width User selectable sample rate 9.6 – 48kHz
Serial	1 x Micro USB
Power	1 x DC Power port
Power	
1 PoE port	802.3 @ Type 2 PoE+ PD
External Power Supply	+5V 25W
Type-C Power Delivery	5V/3A
Environmental	
Storage	-20° C to 70° C (-4° F to 158° F)
Operating	0° C to 50° C (32° F to 122° F)
Indicators	
LED Lights	2 Tricolor lights
Dimensions	
Height x Width x Depth	1.6 in. x 4.1 in. x 6.6 in. (41 mm x 105 mm x 168 mm)
Weight	0.73 lbs (0.332 kg)

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

©2025 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.

590-2372-501D