



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 Dashboard	6
2.2 Logs	6
2.3 Sessions	6
2.3.1 KVM management	6
2.3.2 Serial management	12
2.4 Configuration	13
2.4.1 Registration	13
2.4.2 Network	14
2.4.3 Serial interfaces	14
2.4.4 User management	15
2.4.5 Services	16
2.4.6 Lightweight Directory Access Protocol (LDAP)	16
2.4.7 Date and time	17
2.4.8 System settings	17
2.4.9 Certificate	18
2.5 Firmware	18
2.5.1 Firmware management	18
2.5.2 Firmware inventory	19
2.6 Remote Media	20
Appendices	21
Appendix A: Technical Specifications	21

This page intentionally left blank

1 Getting Started

1.1 Product Overview

The demand for keyboard, video, and mouse (KVM) switches that support 4K video resolution is growing fast. The Vertiv™ Avocent® IPUHD 4K IP KVM device provides you with remote access to servers with 4K video resolution. It also integrates seamlessly with the Vertiv™ Avocent® RM1048P Rack Manager and the Vertiv™ Avocent® MP1000 Management Platform, enabling you to manage and control secure KVM usage at a holistic and granular level.

Figure 1.1 Avocent IPUHD 4K IP KVM Device Descriptions

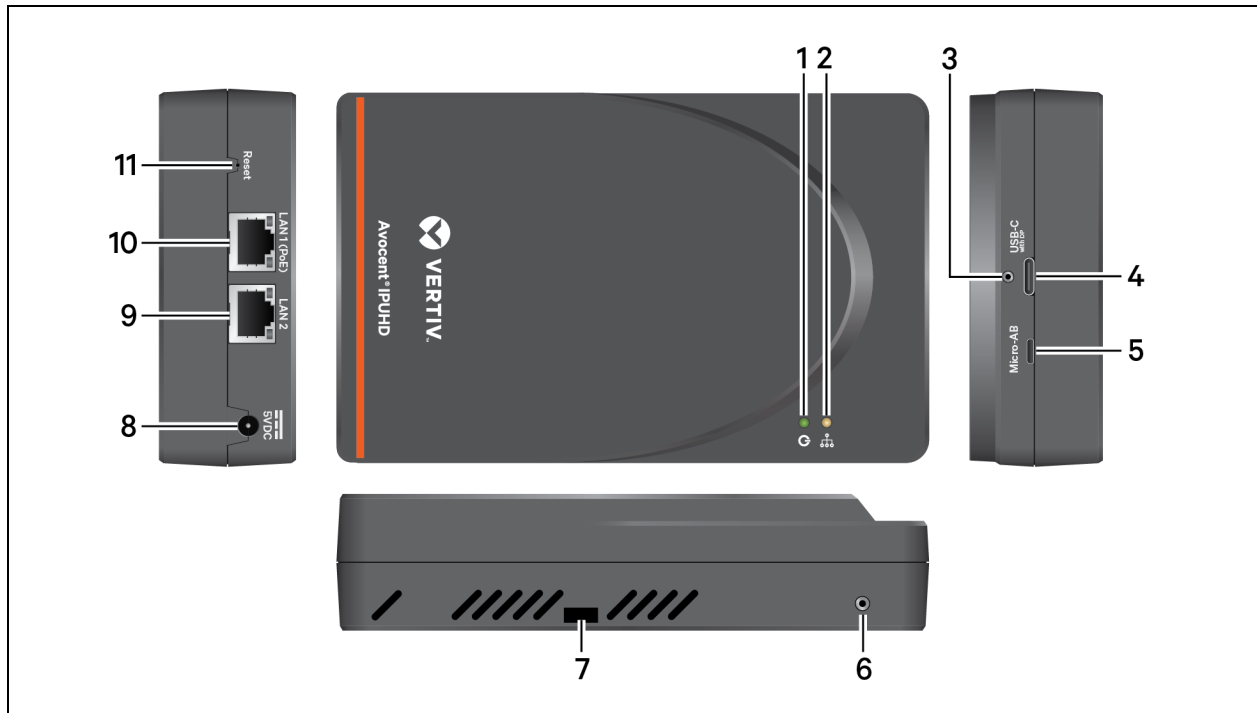



Table 1.1 Avocent IPUHD 4K IP KVM Device Descriptions

Item	Description	Item	Description
1	Power indicator	7	Hole to secure device
2	Activity indicator	8	Power input
3	Screw hole to tighten USB connector	9	LAN2 port
4	USB-C port	10	LAN1 (with PoE) port
5	Micro-AB port	11	Reset button
6	Screw hole to tighten USB (not currently in use)		

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	
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	
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 stand-alone 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 Avocent IPUHD 4K IP KVM device Quick Installation Guide provided with your Avocent IPUHD 4K IP KVM 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 the 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 with its web UI. The web UI provides direct access to the Avocent IPUHD 4K IP KVM device.

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.

Figure 2.1 Web UI Overview

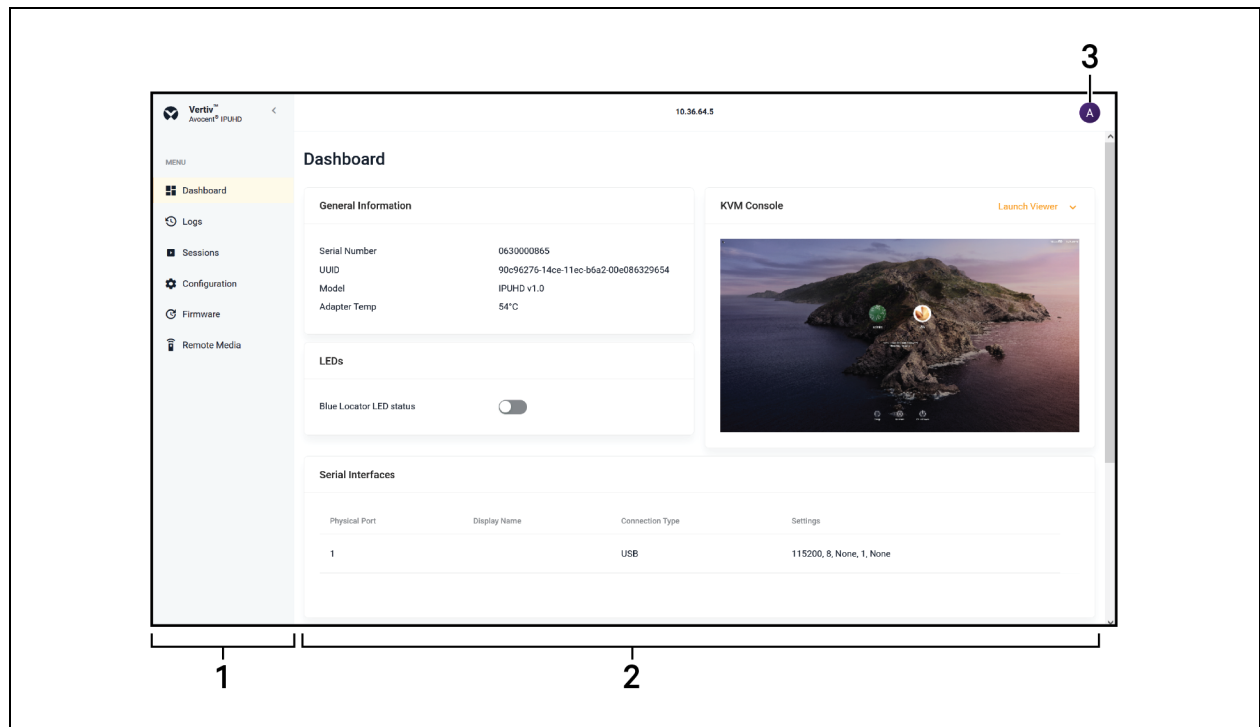


Table 2.1 Web UI Overview Descriptions

Item	Description
1	Sidebar
2	Content area
3	User preferences

NOTE: Avocent IPUHD 4K IP KVM device is automatically managed by a rack manager via its Managed mode. To configure the mode of the IP KVM device, please see [Registration](#) on page 13.

2.1 Dashboard

From the *Dashboard* screen, the following options are provided:

- Access to general information, including the UUID, model, and adapter temperature.
- Launch KVM sessions in a new tab or window via the KVM Console section.
- Configure the blue locator LEDs status using the slider button.
- View the serial interfaces associated with the Avocent IPUHD 4K IP KVM device.
- View the audited log of events for the IP KVM device.

2.2 Logs

When an event occurs, it is saved in the audit log that can be viewed from the Logs screen.

From the *Logs* screen, the following options are provided:

- Use the Search bar to search for a specific event.
- Use the drop-down menu to filter by name, resolution status, or severity.
- Use the arrows next to each column to sort each event.
- Click the appropriate icon in the upper right-hand corner to clear or refresh the logs.

2.3 Sessions

2.3.1 KVM management

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. KVM over IP gives you flexible target device management control and secure remote access from anywhere at anytime.

The KVM over IP functionality of the appliance provides enterprise customers with the following features and options:

- Keyboard, video, and mouse (KVM) capabilities, configurable for digital (remote) connectivity
- HTML5 KVM viewer
- Serial viewer
- Session management
- Session sharing
- Screen capture
- Screen recording
- Control over color depth and maximum target resolution
- Zoom
- Virtual keyboard
- Copy and paste
- Network bandwidth optimization
- Macros
- Virtual media

Table 2.2 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	✓	✓	✗	✗

Table 2.3 Feature Comparison for Avocent IPUHD 4K IP KVM Device and Vertiv™ Avocent® IPIQ IP KVM Device Viewer

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

HTML5 video viewer session

Using the web UI, you can connect to each target, access target server files, manage software updates, and execute operating system commands. Each target server has a device information panel that contains data about the device.

Prerequisites

Launching an HTML5 video viewer session requires the following:

- Must have assigned rights or belong to a user group with assigned rights.
- Must use the latest version of one of the following supported web browsers: Google Chrome, Microsoft Edge, Apple Safari, or Mozilla Firefox.
- May need to disable the browser's pop-up blockers to allow the session to launch.

To launch a video viewer session:

1. From the *Dashboard* screen, click *Launch Viewer* from the KVM Console tab.
2. Select whether to open the session in a new tab or window.

To close a video viewer session:

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

To configure access to a video viewer 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 select how you want the user to connect. The following options are available:

- Approve
- Reject
- Allow as read-only

Video viewer

The Avocent IPUHD 4K IP KVM device is used to conduct a KVM session with one or more target devices attached to one or more KVM switches. When you connect to a device using the Avocent IPUHD 4K IP KVM device, the target screen appears in a new window. The Avocent IPUHD 4K IP KVM device allows you to control the target server in person remotely. When 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. You can manage computer settings, access files, and launch virtual media sessions from the client.

You can use the menu located at the top of the window to access features such as screen capture, refresh, and virtual keyboard. Although you can use the virtual keyboard to enter text to the target server, you can use the Macros feature to send multi-key commands to make sure the command string is accurate. Depending on the operating system selected in the Macros settings, the command options will change. You can also configure the settings of the Avocent IPUHD 4K IP KVM device using the Settings icon.

Video viewer menu

The video viewer session can be configured with the settings described in this section.

File menu

Click *File* to copy and paste text into the target or open a server-side recording file.

View options

Click *View* to access and perform the following operations:

- Display options for the video viewer.
- Enable full-screen and single-cursor modes.
- View KVM statistics.
- Display or hide the status bar at the bottom of the screen.

Video options

Click *View - Video Options* to access and perform the following operations:

- Display more colors for the best fidelity, or fewer colors to reduce the volume of data transferred on the network. The choices range from Grayscale 16 Shades (maximum speed) to Color 24-bit (maximum video quality).
- Enable noise reduction for VGA or disable it for a digital video source.

To select a color depth for the video viewer:

1. From the toolbar, click *View*.
2. Click *Video Options*.
3. Use the slider to select the color depth.
4. Click the radio button to enable or disable noise reduction.

5. Click *Apply*.

Scaling

Click *Scaling* to adjust the appearance of the target's screen in the KVM Viewer by using the following options:

- Enable *Maintain Aspect Ratio* to maintain the aspect ratio of the Target screen.
- Select *Stretch to Window* to fit the Target screen to your display.
- Select *Zoom* and use drop-down menu to select the zoom percentage of the display.

Max resolution

Click *Max Resolution* to select the maximum target resolution for your KVM session. This setting affects all sessions and remains until changed again.

NOTE: This setting causes a change of the actual video resolution on your target system's OS.

Macros

Click *Macros* for the following options:

- View a list of supported operating systems that your target device may use. After you select the applicable operating system, you can access the list of command strings that are valid for the selected operating system.
- Send a string of commands with one click to the target computer. The options in the drop-down list are predetermined based on the macro set you select by accessing the Macros tab. If you are looking for a command string that does not appear in the list, be sure to verify that you have the correct operating system selected in the Macro Manage drop-down list.
- Define macros using the *Manage Macros* tab.

NOTE: To save time and eliminate error risk, it is recommended that you use the Macros feature to send a command string to a server. Using the macros feature when sending a command string, such as Ctrl-Alt-Delete, to a target device will not affect your client server.

To send a command to the target computer:

1. Click the Macros drop-down list at the top of the screen and select a command string from the Static Macros list.
2. Click *Send*.

Tools

Click *Tools* for the following options:

- Select the keyboard language.
- Capture a screenshot.
- Send an instant message.
- Select the mouse mode.
- Reset the keyboard and mouse.
- Enable a virtual keyboard.
- Optimize network bandwidth and choose when to reduce the update rate.

Virtual keyboard

When the virtual keyboard is enabled, the keyboard is displayed on the client's workstation and can be positioned anywhere inside the window. The up and down directional arrows in the top right corner of the virtual keyboard are used to increase or decrease the size of the keyboard, respectively.

Virtual media

Use the virtual media feature on the client workstation to map an .iso or .img file on the client machine as a virtual drive on a target device. You can also use the client workstation to add and map an .iso or .img file as a virtual drive on the target device.

Requirements

The virtual media feature has the following requirements:

- 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.
- If the target device does not support a portable USB memory device, you cannot map it on a client machine as a virtual media drive on the target device.
- The user (or user group to which the user belongs) must have permission to establish virtual media sessions and/or reserved virtual medial sessions to the target device.
- Only one virtual media session can be active on a target device at one time.

To map a virtual media drive:

NOTE: To map a virtual media drive, you must launch a video viewer session. See [To launch a video viewer session: on page 8](#).

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 check-box* in the Virtual Disk Management dialog box.

NOTE: If the virtual media session settings were previously configured so that all mapped drives must be read only, the *Read Only check-box* will already be enabled and cannot be changed. You might wish to enable the check-box 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*.

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

To unmap a virtual media drive:

1. From the Virtual Media menu, click the *mapped drive* to unmap that drive.
-or-
Click *Deactivate* to unmap all the drives.
2. At the prompt, click *Yes* to unmap the drive.

2.3.2 Serial management

The Avocent IPUHD 4K IP KVM device provides remote access to your serial devices. To modify your serial communication parameters, see [Serial interfaces on page 14](#).

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

1. Using a micro USB to USB-A OTG adapter and then 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 *Dashboard* screen, under Serial Interfaces, move your mouse over the device you want to access.
2. On the right side of the column, click the Launch Console icon.

-or-

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

To end a serial session:

Click the user icon in the upper right-hand corner and select *Exit Serial Viewer*.

2.4 Configuration

2.4.1 Registration

The Avocent IPUHD 4K IP KVM device can be operated completely standalone or can be managed by one of the management stations included in the Vertiv™ Avocent® DSView™ solution (Vertiv™ Avocent® RM1048P Rack Manager or Vertiv™ Avocent® MP1000 Management Platform).

Figure 2.2 Registration Overview

The screenshot displays the 'Registration' settings page in the Vertiv Avocent IPUHD web interface. The left sidebar shows the 'Configuration' menu with 'Registration' selected. The main content area is titled 'Registration' and 'Registration Settings'. It indicates the device is 'Registered successfully' and 'Config via DHCP Enabled' is turned on. The 'Registrar IP Address' is set to 10.36.64.21, and the 'Interval' is 170. The 'Mode' is set to 'Managed' (radio button selected). The 'Registrar Hostname' is *.RMx.interbox.vertiv.com, and the 'WSS Port' is 443. There are 'Discard' and 'Apply' buttons at the bottom right.

To configure the registration settings:

NOTE: The hostname configuration and registrar IP address are obtained from the DHCP server that assigned the IP address to the Avocent IPUHD 4K IP KVM device when Config via DHCP is enabled using the ON/OFF button and configuration items are identified in the DHCP data.

1. From the left-hand sidebar, click *Configuration - Registration*.
2. Click the radio button to select the Managed mode.

NOTE: When the Managed mode is selected, all web UI control features in the Configuration tab are disabled, except Registration and Serial Interfaces.

3. Enter the IP address of the managing appliance (Vertiv™ Avocent® RM1048P Rack Manager or Vertiv™ Avocent® MP1000 Management Platform) in the Registrar IP Address field that should manage the Avocent IPUHD 4K IP KVM device.
4. Enter the hostname in the Registrar Hostname field.

NOTE: Enter *.RMx.interbox.vertiv.com if the managing appliance is Vertiv™ Avocent® RM1048P Rack Manager, and *.MPx.interbox.vertiv.com if the managing appliance is Vertiv™ Avocent® MP1000 Management Platform, in the Registrar Hostname field.

5. Click *Apply*.

NOTE: When Config via DHCP is disabled, the Registrar IP Address and Registrar Hostname configuration information is disregarded.

NOTE: The values in the Interval and WSS Port fields are pre-defined and must not be changed. These values are used only in specific troubleshooting situations.

2.4.2 Network

From the *Configuration - Network* screen, you can view and configure network settings.

Ethernet interfaces

The Avocent IPUHD 4K IP KVM device has three physical network interfaces (USB0, eth0, and eth1). Network settings can only be changed for USB0 and ethbr0. The interfaces eth0 and eth1 reflect link status of the two LAN ports. The USB0 network settings are applicable when you connect a computer to the Avocent IPUHD 4K IP KVM device through the micro USB cable. Each interface has an individual MAC address and can be assigned an IP address via DHCP or statically.

To configure the ethernet interfaces:

1. From the left-hand sidebar, click *Configuration - Network*.
2. Navigate to the section for either the USB0 interface or the ethbr0 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 apply the changes.

To create a static IP address:

1. From the left-hand sidebar, click *Configuration - Network*.
2. Navigate to the section for either the USB0 interface or the ethbr0.
3. Use the slider button to enable the interface, if applicable

NOTE: Ensure the DHCP setting is disabled, if applicable.

4. Under the IPv4 Settings or IPv6 Settings heading, configure the existing IP address entry.

-or-

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

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

To create a static name server:

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

2.4.3 Serial interfaces

From the *Configuration - Serial Interfaces* screen, the serial communication parameters can be configured.

Figure 2.3 Serial Interfaces Overview

The screenshot shows the 'Serial Interfaces' configuration page in the Vertiv Avocent IPUHD 4K IP KVM Device Web User Interface. The left sidebar contains a 'MENU' with options: Dashboard, Logs, Sessions, Configuration, Registration, Network, Serial Interfaces (highlighted), User Management, Services, LDAP, Date/Time, System Settings, Certificate, Firmware, and Remote Media. The main content area is titled 'Serial Interfaces' and shows the configuration for 'Serial Interface ttyEcho-1'. Under 'Interface Settings', 'Interface Enabled' is a toggle switch that is turned on. 'SSH Enabled' is a toggle switch that is turned off. 'Signal Type' is set to 'RS232'. 'Bit Rate' is set to '115200'. 'Stop Bits' is set to '1'. 'Flow Control' is set to 'None'. On the right side, 'Display Name' is 'to IPSL RJ45 port 2', 'SSH Port' is '2200', 'Connection Type' is 'USB', 'Data Bits' is '8', and 'Parity' is 'None'. At the bottom right, there are 'Discard' and 'Apply' buttons.

To configure the serial interfaces:

1. From the left-hand sidebar, click *Configuration - Serial Interfaces*.
2. Ensure that the Interface Enabled option is enabled.

NOTE: Serial sessions cannot launch if this option is disabled.

NOTE: If the SSH Enabled option is enabled, you will be connected to the serial port that is configured as per SSH port 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 name in the Display Name field. You can give the name of the port to which it is connected. For example, to 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, use the refresh icon in the upper right-hand corner.

2.4.4 User management

Administrators can restrict port access through the permissions assigned to custom user groups. The default user for the Avocent IPUHD 4K IP KVM device is an administrator. The three pre-defined user groups are as follows:

- Administrator
- Operator
- Read only

From the **Configuration - User Management** screen, the following options are provided:

- Select the settings icon to configure the password policy and FIPS mode settings.
- Select the plus icon (+) to add a new user, then enter the required information.
- Select the refresh icon to reload the page.
- Select the vertical ellipses to the right of existing user entries to edit or delete the user.

2.4.5 Services

From the **Configuration - Services** screen, the following options are provided:

- View the settings for the web server.
- Configure the duration of the timeout, then click *Apply*.

2.4.6 Lightweight Directory Access Protocol (LDAP)

From the **Configuration - LDAP** screen, you can view a list of configured authentication providers. The Avocent IPUHD 4K IP KVM device authenticates users via Active Directory (AD) and LDAP. Additionally, remote group authorizations are supported by LDAP.

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

To configure an LDAP server:

1. From the left-hand sidebar, click *Configuration - LDAP*.
 2. Use the slider to enable LDAP.
 3. Enter the server address and server port in the appropriate fields. To add more than one server, click the plus icon (+).
 4. Under the Binding with LDAP service heading, select the binding method for the LDAP service. To use the login credentials associated with the IP KVM device, click the Use Login Credential radio button.
- or-
- To configure different credentials for the binding method, click the Use Configured Credential radio button, then enter the chosen credentials.
5. Under the Search Settings heading, enter the required information in the Base DN and UID Attribute fields.
 6. Scroll down and click *Apply*.

To configure additional parameters for the authentication method:

1. From the left-hand sidebar, click *Configuration - LDAP - Additional Parameters*.
2. From here, you can configure the following fields: Group Search Attribute, Group Filter, Login Permission Attribute.
3. Click *Apply*.

To delete an LDAP server:

Under the LDAP Server Info heading, click the Remove icon.

Active Directory (AD)

Role-based security can be enabled on the Avocent IPUHD 4K IP KVM device, to map your AD remote group to a role on the IP KVM device.

NOTE: When mapped to a local role with the related security enabled and configured, the AD remote group provides the appropriate permission after login.

To enable role mapping:

1. From the left-hand sidebar, click *Configuration - LDAP - Active Directory*.
2. Use the slider to enable role-based security. The Remote Role Mapping section appears.
3. Click the plus icon (+).
4. Enter the name of your AD remote group.
5. Use the drop-down menu to select the local role the remote group will be mapped with.
6. Click *Apply*.

To delete role mapping:

Under the Remote Role Mapping section, click the Remove icon next to the group you want to remove.

2.4.7 Date and time

From the *Configuration - Date/Time* screen, the following options are provided:

- Enable or disable Network Time Protocol.
- Set the timezone and date time for the serial device.

2.4.8 System settings

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

Password policy

The global password rules can be configured for all the user accounts, as well as account expiration settings. By default, password must have a minimum of eight characters and all other password expiration rules are set.

To configure global password rules:

1. From the *Configuration - System Settings* screen, under the Password Policy, use the slider to enable or disable password policy.
2. Under the Password Change Interval field, use the arrows to define an interval for password changes.
3. Use the slider to enable or disable password age check.
4. Use the arrows to define duration for checking password age under the Password Duration field.
5. Click *Apply*.

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

FIPS mode settings

The FIPS mode of operation can be enabled or disabled via the web UI and is executed after a reboot.

By default, the FIPS mode of operation is disabled and needs to be enabled to modify or update.

To enable or disable FIPS mode:

1. From the *Configuration - System Settings* screen, under the FIPS Mode Settings, use the slider to enable or disable FIPS mode.
2. Click *Apply*.
3. Perform a system reboot for the changes to take effect.

NOTE: The selected FIPS mode is enabled even after performing a factory reset.

Remote presence settings

From the *Configuration - System Settings - Remote Presence Settings* screen, the following options are provided:

- Enable an automatic lock for the host OS.

NOTE: This option is not applicable to the macOS.

- Enable a Keep Awake feature for the host OS.

2.4.9 Certificate

From the *Configuration - Certificate* screen, the following options are provided:

- View the general information for the currently uploaded certificate.
- Generate a Certificate Signing Request (CSR).
- Upload a certificate file.

To generate a CSR:

1. From the left-hand sidebar, click *Configuration - Certificate - Generate CSR*.
2. Enter the following required information: Common Name, State, Organization, Email, Country, City, and Organizational Unit.
3. Click *Generate*.

To upload a certificate:

1. From the left-hand sidebar, click *Configuration - Certificate - Upload Certificate*.
2. Click the *Upload PEM* button.
3. Browse to and select the appropriate file.

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

2.5 Firmware

2.5.1 Firmware management

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. Use the slider button to enable the Reset to Defaults on Firmware Update option.
6. When finished, click *Apply*.

2.5.2 Firmware inventory

From the left-hand sidebar, click *Firmware - Firmware Inventory*. Here you will find information regarding the main adapter firmware. This information includes the name, version, and status of the firmware.

NOTE: Ensure the Avocent IPUHD 4K IP KVM device is in Standalone mode.

To update 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*.

2.6 Remote Media

Figure 2.4 Remote Media Overview

The screenshot displays the 'Remote Media Drives' configuration page. On the left is a sidebar with navigation links: Dashboard, Logs, Sessions, Configuration, Firmware, and Remote Media (highlighted). The main content area is titled 'Remote Media Drives' and contains three sections:

- Virtual CD/DVD:** Shows 'Connected Status' as 'Not Connected'. It includes a 'Transfer Protocol' dropdown set to 'CIFS', a 'User Name' field, a 'Password' field, an 'Image File Path' field containing '///10.x.x.x/images/dvd.iso', and 'Discard' and 'Mount Image Path' buttons.
- Virtual Floppy:** Shows 'Connected Status' as 'Not Connected'. It includes a 'Transfer Protocol' dropdown set to 'CIFS', a 'User Name' field, a 'Password' field, an 'Image File Path' field containing '///10.x.x.x/images/floppy.img', and 'Discard' and 'Mount Image Path' buttons.
- Virtual Removable Disk:** Shows 'Connected Status' as 'Not Connected'. It includes a 'Transfer Protocol' dropdown set to 'CIFS', a 'User Name' field, a 'Password' field, an 'Image File Path' field containing '///10.x.x.x/images/disk.img', and 'Discard' and 'Mount Image Path' buttons.

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 Transfer Protocol either CIFS or NFS server.

NOTE: A Transfer Protocol is a CIFS server by default.

5. Enter the credentials (username and password).
6. Click on *Mount Image Path*.

NOTE: Once the physical drive or image is mapped, it can be used on the remote target device.

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 1920x1200, 1920x1080, 1024x768, 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
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 Power port
Power	
1 PoE port	802.3 @ Type 2 PoE+ PD
External Power Supply	+5V 25W
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 Tri color 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.twitter.com/Vertiv/>

