VERTIV™

Avocent® IPSL IP Serial 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.

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

This page intentionally left blank

1 Getting Started

1.1 Product Overview

In today's edge market, as the footprint of compute, network and storage devices continues to increase, there is a growing need for remote access to IT devices. The Vertiv™ Avocent® IPSL IP serial device provides an innovative serial IP solution for simplifying remote access and troubleshooting IT devices while seamlessly scaling from edge to enterprise.

Figure 1.1 Avocent IPSL IP Serial Device Descriptions

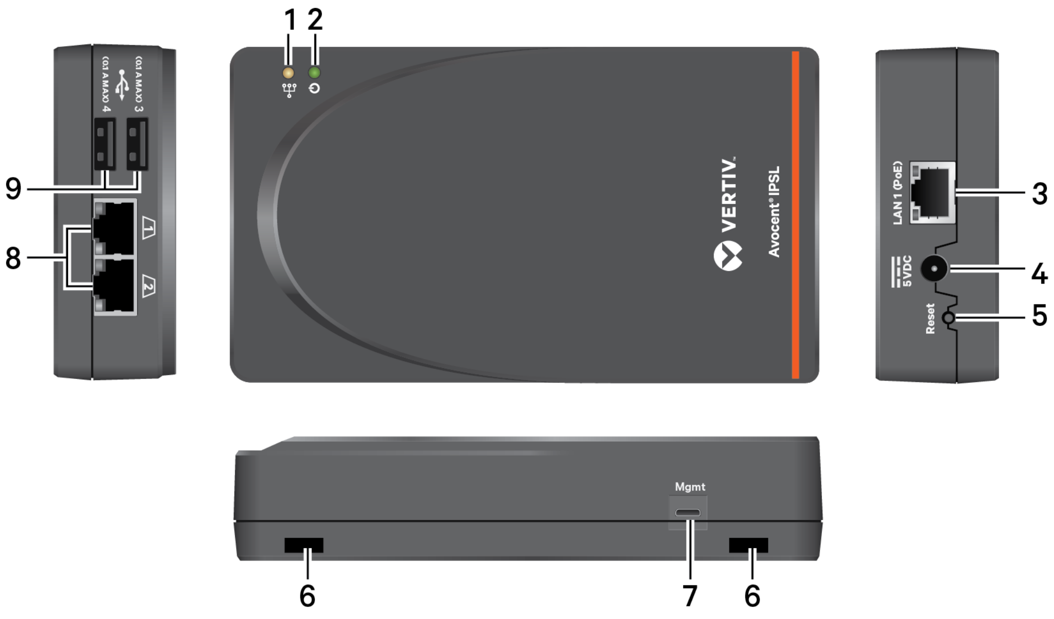


Table 1.1 Avocent IPSL IP Serial Device Descriptions

Item	Description	Item	Description
1	Activity indicator.	6	Holes to secure the device.
2	Power indicator.	7	Mgmt port for Micro USB.
3	LAN1 (PoE+) port.	8	RJ45 ports.
4	Power input.	9	USB Type A ports.
5	Reset button.		

The Avocent IPSL IP serial 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 serial device is booting.
Solid red	The device is fully booted and is now accessible.
Activity	
Off	No activity detected.
Solid green	Any session type is active.
Blinking blue	Locator function has been activated, either locally or remote.

⚠ **CAUTION: When performing a firmware update or factory reset for the serial device, both the power and activity LED's blink red. Do not remove the serial device during this time or else the firmware will become corrupted.**

The Avocent IPSL IP serial device also has a Reset button that enables you to reset the device or activate the device's locator function. Choose from the following options to utilize this button:

- To activate the locator mode, press and hold the Reset button for less than two seconds. Repeat this process to deactivate the locator mode.
- To reboot the device, press and hold the Reset button for two to eight seconds.
- To perform a factory reset, press and hold the Reset button for more than eight seconds. This erases all settings and configuration information on the IP serial device.

For more information about RJ-45 pin out of Avocent IPSL IP serial device, see the following table.

Table 1.3 RJ-45 Pin Out

RJ45 Pin	Avocent	Cisco
1	RTS	CTS
2	DTR	DCD/DSR
3	TXD	RXD
4	GND	GND
5	CTS	NC
6	RXD	TXD
7	DCD/DSR	DTR
8	NC	RTS

1.2 Features and Benefits

The Avocent IPSL IP serial device provides the following benefits for your data center:

- Secure remote serial access to IT devices to quickly troubleshoot problems without being physically present.
- Simultaneous management of up to four serial devices.
- Reduced power costs and simplified cabling by leveraging Power over Ethernet (PoE).
- Ability to work as a standalone serial device or as part of an integrated Vertiv™ Avocent® DSView™ solution.
- Centralization and protection for your expensive IT equipment on-site while permitting remote access.
- Quick location of your Avocent IPSL IP serial device via LED lights.
- Remote firmware updates of your IT devices.

1.3 Installation and Initial Setup

For installation and initial network configuration instructions, see the Avocent IPSL IP Serial Device Quick Installation Guide provided with your device. For any additional product documentation or product-related links, visit the product page at Vertiv Avocent IPSL Serial Device and select the *Documents & Downloads* tab.

This page intentionally left blank

2 Web User Interface (UI)

Once you have connected the Avocent IPSL IP serial device to a network and configured its IP address, you can directly access the serial device via its web UI.

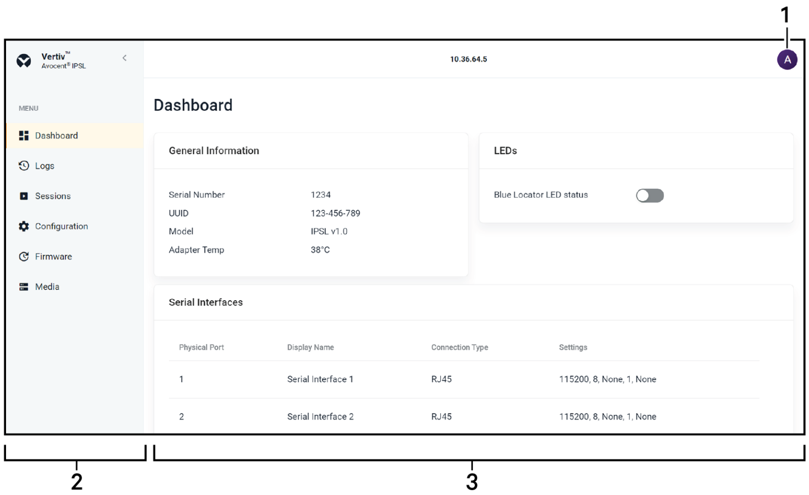
The web UI is compatible with the latest 32-bit and 64-bit versions of the following web browsers:

- 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 IPSL IP serial device.
2. At the login screen, enter your username and password.
3. Once you login, the dashboard screen appears.

Figure 2.1 Dashboard Screen



General Information

Serial Number 1234
UUID 123-456-789
Model IPSL v1.0
Adapter Temp 38°C

LEDs

Blue Locator LED status

Serial Interfaces

Physical Port	Display Name	Connection Type	Settings
1	Serial Interface 1	RJ45	115200, 8, None, 1, None
2	Serial Interface 2	RJ45	115200, 8, None, 1, None

Table 2.1 Web UI Overview Descriptions

Item	Description
1	User preferences
2	Sidebar
3	Content area

NOTE: By default, the serial device is set to Managed mode upon initial login. Certain features under the Configuration tab are disabled in this mode.

To configure the mode of the serial device, please see Registration on page 7

2.1 Dashboard

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

- Access to general information, including the serial number, UUID, model, and adapter temperature.
- Configure the blue locator LEDs status using the slider button.
- Launch serial sessions via the Serial Interfaces section.
- View the serial interfaces associated with the IPSL IP serial device.
- View the audited log of events for the IPSL IP serial 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, resolved, or severity.
- Use the arrows next to each column to sort each event.
- Click the icons in the upper right-hand corner to clear or refresh the logs.

2.3 Sessions

The Avocent IPSL IP serial device provides flexible, centralized control of data center servers and virtual media of remote branch offices where trained operators may be unavailable. This flexibility allows for target device management control and secure remote access from anywhere at anytime.

The target management functionality of the appliance provides enterprise customers with the following features and options:

- HTML5 serial viewer
- Virtual media. For more information, please see Virtual media on page 16 .
- Configure serial communication
- Parameters
- Data logging
- Manage up to 4 serial devices
- Serial over SSH

2.3.1 Serial management

Prerequisites

The following requirements must be met to launch an HTML5 serial session:

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

Launching a serial session

The Avocent IPSL IP serial device provides remote access to your serial devices. To modify your serial communication parameters, see Serial interfaces on page 9 .

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 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*.

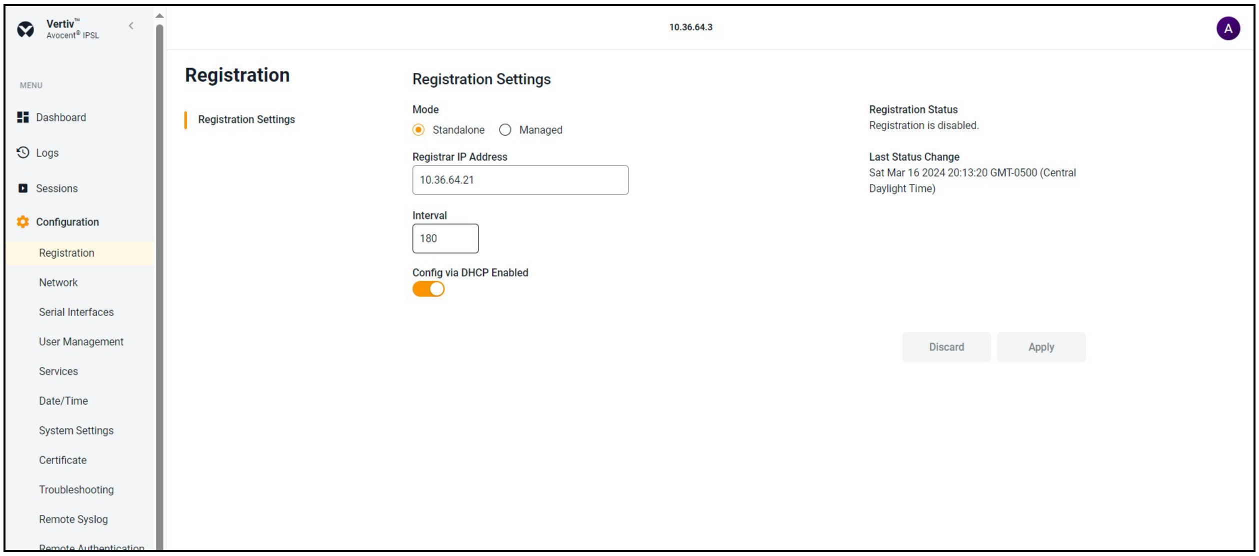
2.4 Configuration

This section includes procedures and information related to the configuration options for the IP serial device.

2.4.1 Registration

The Avocent IPSL IP serial device can be operated completely standalone or managed by a Vertiv™ Avocent® DSView™ solution managing appliance (Vertiv™ Avocent® RM1048P Rack Manager or Vertiv™ Avocent® MP1000 Management Platform).

Figure 2.2 Registration Overview



Registration Settings

Mode
● Standalone ○ Managed

Registrar IP Address
10.36.64.21

Interval
180

Config via DHCP Enabled

Registration Status
Registration is disabled.

Last Status Change
Sat Mar 16 2024 20:13:20 GMT-0500 (Central Daylight Time)

To set the device to Managed mode:

NOTE: If the Config via DHCP Enabled option is enabled and configuration items are identified in the DHCP date, the registrar IP address is obtained from the DHCP server that assigned the IP address to the Avocent IPSL IP serial device. If the option is disabled, the Registrar IP Address field is disregarded.

1. From the left-hand sidebar, click *Configuration - Registration*.

2. Click the Managed radio button.

NOTE: The Managed mode disables all web UI control features in the Configuration tab, except Registration and Serial Interfaces.

3. Enter the IP address of the appliance that will manage the serial device (rack manager or management platform) in the Registrar IP Address field.
4. Click *Apply*.

NOTE: The value in the Interval field is pre-defined and used only in specific troubleshooting situations. These values must not change.

2.4.2 Network

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

Ethernet interfaces

The Avocent IPSL IP serial device has two physical network interfaces (USB0 and eth0). Network settings can be changed for both interfaces. The eth0 interface reflects the link status of the one LAN ports. The USB0 network settings are applicable when you connect a computer to the Avocent IPSL IP serial device through the micro USB cable. Each interface has an individual MAC address and can be assigned an IP address via DHCP or statically.

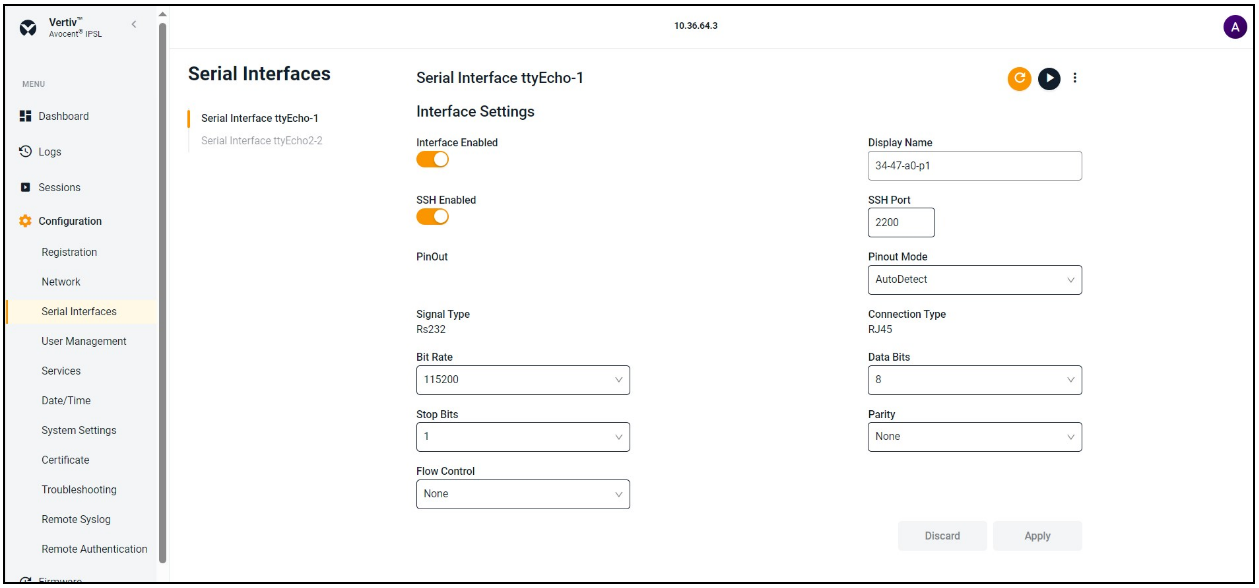
To configure the ethernet interface:

1. From the left-hand sidebar, click *Configuration - Network*.
2. From the Network menu, select either *Manager Ethernet Interface - eth0* or *Manager Ethernet Interface - usb0*.
3. Under the Interface Settings heading, the following options are provided:
   - Enable or disable the interface.
   - Set the network speed.
   - Enable or disable the Duplex mode.
   - Enable or disable Auto Negotiation.
4. Under the IPv4 Settings, the DHCP settings for the interface can be configured.
5. Under the IPv6 Settings heading, a static IP address can be configured by clicking the plus icon (+) to the right and entering the required information.
6. 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



Serial Interface ttyEcho-1

Interface Settings

Interface Enabled: on

Display Name: 34-47-a0-p1

SSH Enabled: on

SSH Port: 2200

PinOut

Pinout Mode: AutoDetect

Signal Type: Rs232

Connection Type: RJ45

Bit Rate: 115200

Data Bits: 8

Stop Bits: 1

Parity: None

Flow Control: None

To configure the serial interfaces:

1. From the *Configuration - Serial Interfaces* screen, ensure that the Interface Enabled option is enabled.

NOTE: If the Interface Enabled option is disabled, the serial sessions cannot be launched.

NOTE: If the SSH Enabled option is enabled, you will be connected to the serial port that is configured as per SSH port through SSH client.

2. Use the drop-down menu to select appropriate values for these fields:
    - Bit Rate
    - Stop Bits
    - Flow Control
    - Data Bits
    - Parity
3. Enter the name in the Display Name field. You can give the name of port to which it is connected. For example, serial interface 1.
4. Click *Apply*. Once the serial interface is configured, it appears 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 IPSL IP serial 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 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.

2.4.7 System settings

From the *Configuration - System Settings* screen, you can view and configure system settings for the Avocent IPSL IP serial 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.

2.4.8 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.

2.4.9 Troubleshooting

To submit a troubleshooting report:

1. Select the type of test action: *Ping*, *Traceroute*, or *TcpConnect*.
2. Enter the IP address.

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

3. Enter the port number.
4. Check the Force IPv6 option, if desired.

NOTE: FQDN addresses can be resolved to IPv6 using this field. IP addresses are automatically identified as IPv4 and IPv6.

5. Click *Submit*.

2.4.10 Remote syslog

To add a remote syslog:

1. From the left-hand sidebar, click *Configuration - Remote Syslog*.
2. Click the plus icon (+) in the top right-hand corner.
3. Enter the destination and certificate.
4. Using the drop-down menu, select the certificate type.
5. Click *OK*.

2.4.11 Remote authentication

From the *Configuration - Remote Authentication* screen, authentication methods can be implemented to ensure the security of your system and users.

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

Priority setting

From the *Configuration - Remote Authentication - Priority Setting* screen, use the drop-down menu to set the priority for the various authentication methods. The options include:

- Local - LDAP - TACACS+ - RADIUS
- Local - TACACS+ - LDAP - RADIUS

After selecting the desired option, click *Apply*.

LDAP

To add an LDAP authentication method:

1. Use the Service Enabled slider button to enable the LDAP service.
2. Enter the required information into the provided fields.
3. Click the plus icon (+) to add an LDAP service address.
4. Enter the server address and server port number.
5. Role-based security can be enabled on the AvocentIPSL IP serial device, to map your Active Directory remote group to a role on the AvocentIPSL IP serial device. Click the plus icon (+) 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.

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

TACACS+

To add a TACACS+ authentication method:

1. Use the Service Enabled slider button to enable the TACACS+ service.
2. Enter the required information into the provided fields.
3. Click the plus icon (+) to add a TACACS+ service address, then enter the IP address.

4. Click *Apply*.

RADIUS service

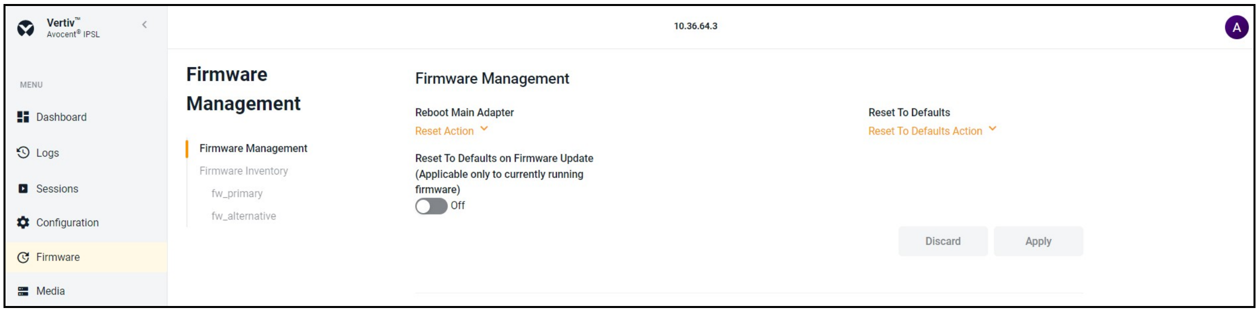
To add a RADIUS authentication method:

1. Use the Service Enabled slider button to enable the RADIUS service.
2. Enter the required information into the provided fields.
3. Click the plus icon (+) to add a RADIUS service address, then enter the IP address.
4. Click *Apply*.

2.5 Firmware

2.5.1 Firmware management

Figure 2.4 Firmware Management Overview



Reset To Defaults on Firmware Update (Applicable only to currently running firmware) Off

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 one of these options:
   - ForceRestart
   - Graceful reboot into primary firmware
   - Graceful reboot into failover firmware.
3. Click *OK*. The device reboots immediately.

To reset the currently running firmware settings to default values:

1. From the left-hand sidebar, click *Firmware - Firmware Management*.
2. Click on the drop-down arrow next to Reset To Defaults Action and select one of these options:
   - ResetAll
   - PreserveNetwork
   - PreserveNetworkAndUsers
3. Click *OK*. The device reboots immediately.

To reset to default values on firmware update:

By default, the currently running firmware update is set to Off. It must be enabled to reset the default values.

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

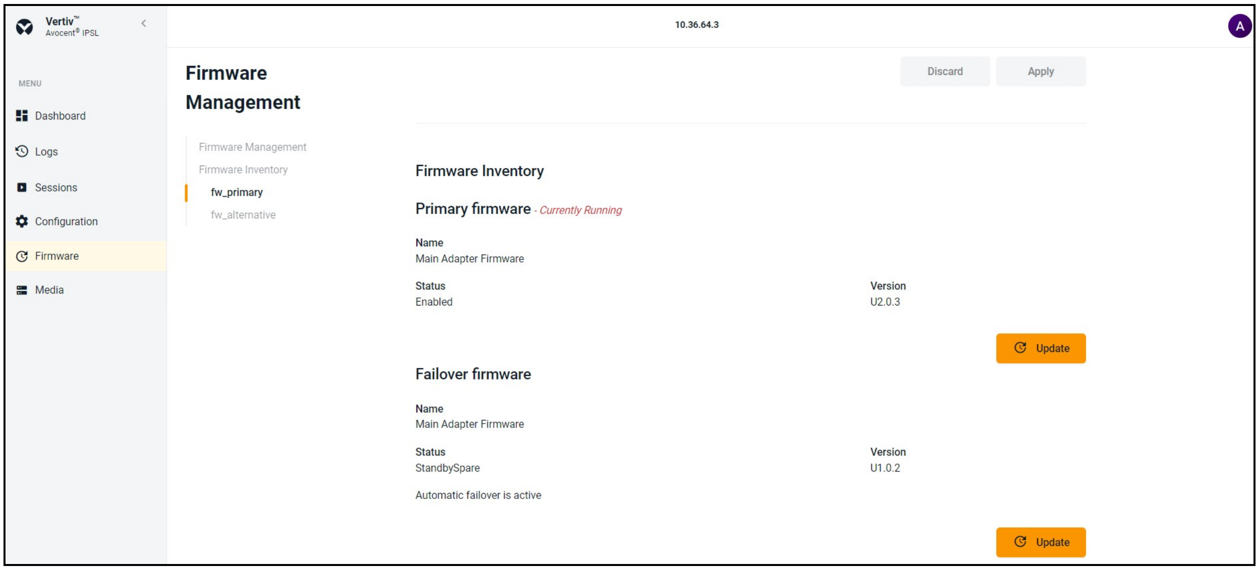
1. From the left-hand sidebar, click *Firmware - Firmware Management*.
2. Use the slider to enable or disable this option.
3. Click *Apply*.

2.5.2 Firmware inventory

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

NOTE: Ensure the Avocent IPSL IP serial device is in Standalone mode.

Figure 2.5 Firmware Management Overview



Firmware Inventory

Primary firmware - *Currently Running*

Name
Main Adapter Firmware

Status
Enabled

Version
U2.0.3

Failover firmware

Name
Main Adapter Firmware

Status
StandbySpare

Version
U1.0.2

Automatic failover is active

To update the primary firmware or failover firmware:

1. Click the *Update* button under the respective firmware section.
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-

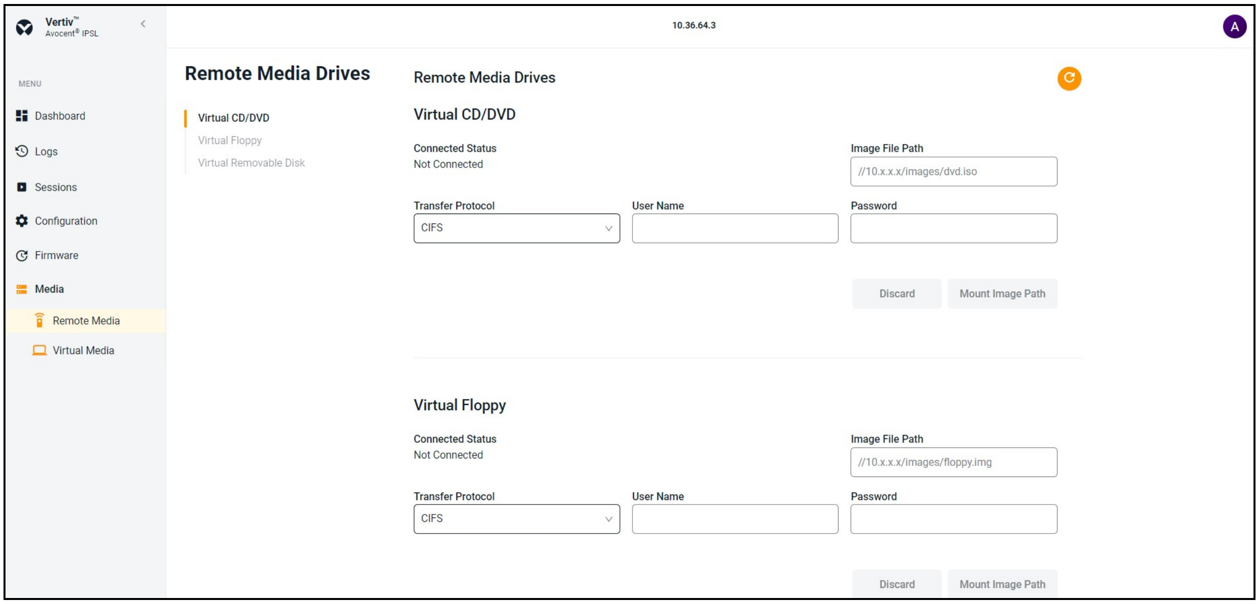
   Browse to and choose the file for updating firmware.
3. Click *Start Update*.

2.6 Media

This section includes procedures and information related the media options for the IP serial device. The device supports both remote and virtual media for file mapping.

2.6.1 Remote media

Figure 2.6 Remote Media Overview



Remote Media Drives

Remote Media Drives

Virtual CD/DVD

Connected Status
Not Connected

Image File Path
//10.x.x.x/images/dvd.iso

Transfer Protocol
CIFS

User Name

Password

Virtual Floppy

Connected Status
Not Connected

Image File Path
//10.x.x.x/images/floppy.img

Transfer Protocol
CIFS

User Name

Password

To configure a remote server location:

1. From the left-hand sidebar, click *Media - 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 either *CIFS* or *NFS* server for the Transfer Protocol.

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

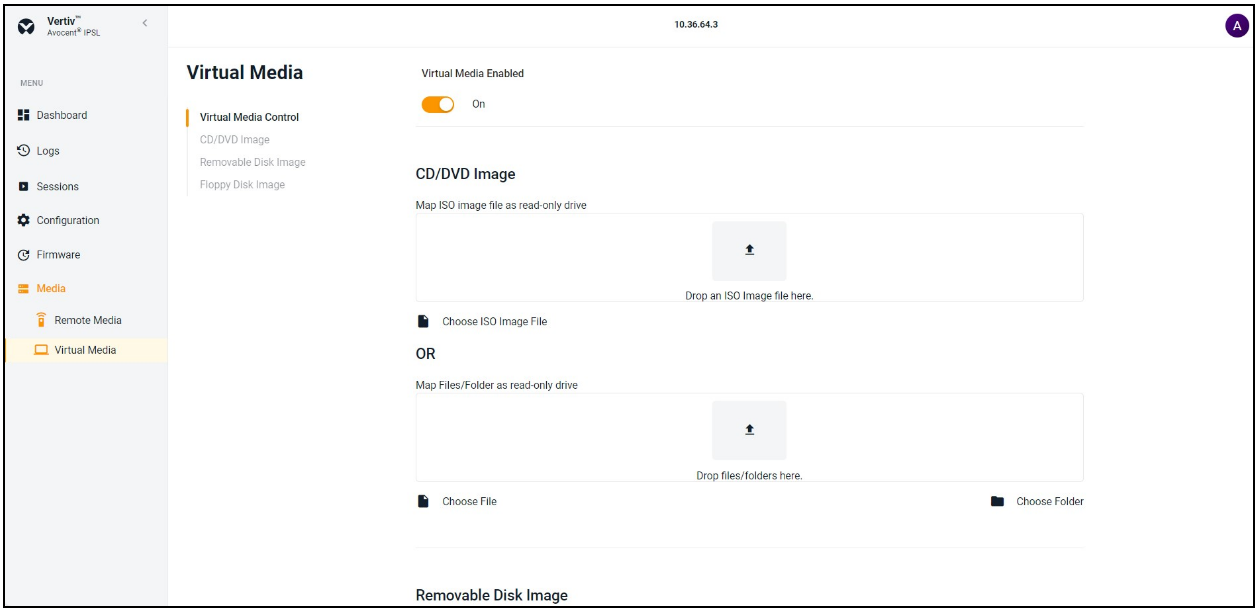
5. Enter the credentials (username and password).
6. Click *Mount Image Path*.

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

2.6.2 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.

Figure 2.7 Virtual Media Overview



Virtual Media Enabled

On

CD/DVD Image

Map ISO image file as read-only drive

Drop an ISO Image file here.

OR

Map Files/Folder as read-only drive

Drop files/folders here.

Removable Disk Image

Requirements

The virtual media feature has the following requirements:

- 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.

Map a virtual media drive:

Virtual media control is disabled (Off mode) by default.

NOTE: Verify that another user is not using the Virtual Media feature on a different device or website if you are unsuccessful to enable virtual media control to On mode.

To map a virtual media drive:

From the *Media - Virtual Media* screen, use the slider under Virtual Media Enabled to enable the On mode. This action shows the features of virtual media to map the .iso or .img files /folders.

To map an .iso image, files, or a folder:

1. From the left-hand sidebar, click *Media - Virtual Media - CD/DVD Image*.
2. Drag and drop an .iso image file.

-or-

click *Choose ISO Image File* to map single .iso image file.

-or-

Drag and drop files/folder .

-or-

Click *Choose File or Choose Folder* to map the file/folder which contains more than one .iso image files.

3. From the open dialogue box, navigate to the folder and select the .iso image, files or folder and click *Open* or *Upload*. This action maps an .iso image, files, or folder with read-only access as per selection in step 2.

To map an .img file:

1. From the left-hand sidebar, click *Media - Virtual Media* , then click either *Removable Disk Image* or *Floppy Disk Image* to map an .img file.
2. Drag and drop an .img file.

   -or-

   Click *Choose Image File.*

3. From the open dialogue box, navigate to the folder and select an .img file and click *Open*. This action maps an .img file with read-only access.

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, under the mapped drive click the *Unmap* button.
2. At the prompt, click *OK*. This action unmaps the drive from the target device.

This page intentionally left blank

Appendices

Appendix A: Technical Specifications

Table A.1 Avocent IPSL IP Serial Device Technical Specifications

Item	Value
Ports	
Network	2 x 1G LAN ports - 1 x PoE, 1 x Service Processor connectivity
Serial	1 x USB-A, 2 x RJ-45
Power	1 x Power port
Power	
1 PoE port	802.3 at 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 x Tri color lights
Dimensions	
Height x Width x Depth	1.6 inches x 4.1 inches x 6.6 inches (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/

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