



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 result from use of this information or for any errors or omissions.

Refer to local regulations and building codes relating to the application, installation, and operation of this product. The consulting engineer, installer, and/or end user is responsible for compliance with all applicable laws and regulations relation to the application, installation, and operation of this product.

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

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	3
1.3 Installation and Initial Setup	3
2 Web User Interface (UI)	5
2.1 Dashboard	7
2.1.1 Serial management	7
2.2 User Profile	7
2.3 System Configuration	8
2.3.1 Registration	8
2.3.2 User management	9
2.3.3 Services	10
2.3.4 Date and time	10
2.3.5 System settings	10
2.3.6 Certificate	11
2.3.7 Troubleshooting	12
2.3.8 Remote syslog	12
2.3.9 Remote authentication	12
2.4 Interface Configuration	13
2.4.1 Network	13
2.4.2 Serial interfaces	14
2.5 Logs	15
2.6 Sessions	15
2.7 Firmware	15
2.7.1 Firmware management	15
2.7.2 Firmware inventory	16
2.8 Media	17
2.8.1 Remote media	17
2.8.2 Virtual media	17
3 Security Best Practices	19
3.1 Risk Assessment	19
3.2 Physical Security	20
3.3 Account Access	20
Appendices	21
Appendix A: Technical Specifications	21

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

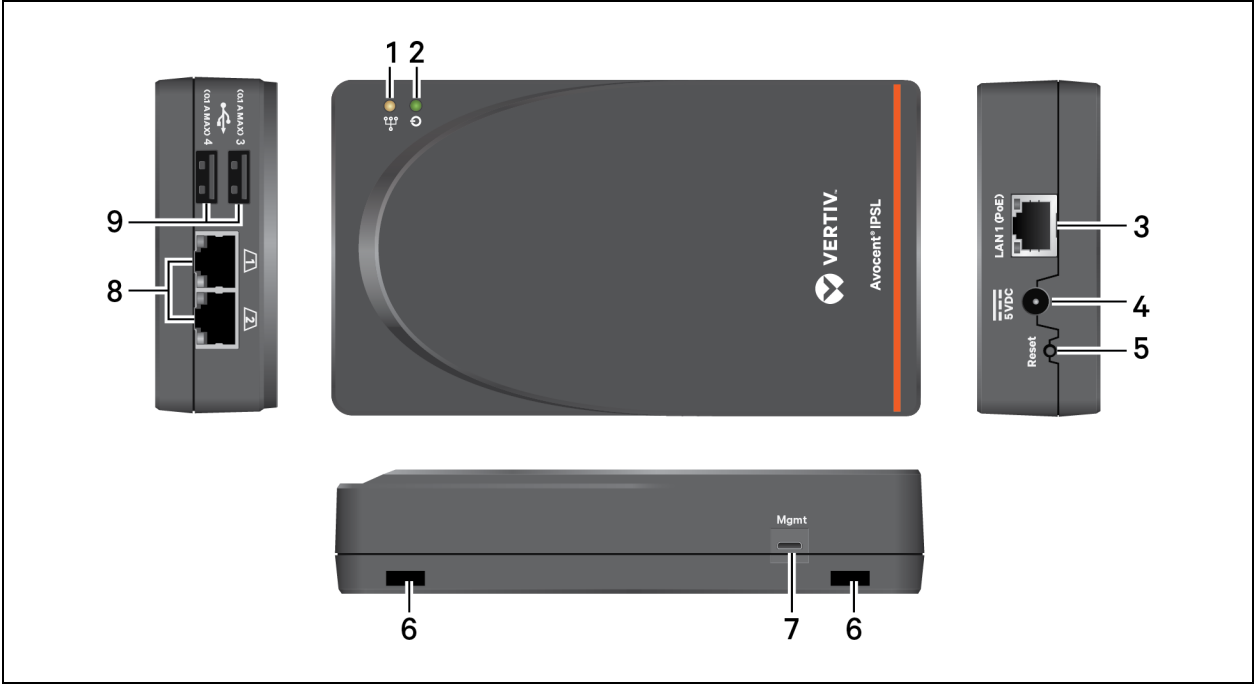


Table 1.1 Avocent IPSL IP Serial Device Descriptions

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 Vertiv 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 LED	
Blinking red	The serial device is booting.
Solid red	The device is fully booted and is now accessible.
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: 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 Vertiv 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 Vertiv Avocent IPSL IP serial device, refer to 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 Vertiv 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 Vertiv Avocent IPSL IP serial device via LED lights.
- Remote firmware updates of your IT devices.
- Standard management of your Vertiv Avocent IPSL IP serial device through compliance with the Redfish specification.

1.3 Installation and Initial Setup

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

This page intentionally left blank

2 Web User Interface (UI)

Once you have connected the Vertiv 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 and enter the IP address for the Vertiv Avocent IPSL IP serial device that you previously configured. The IP address should be entered in the following format:
https://<appliance.IP>
2. At the login screen, enter your username and password. The web UI opens into the Dashboard screen.

Figure 2.1 Dashboard Screen

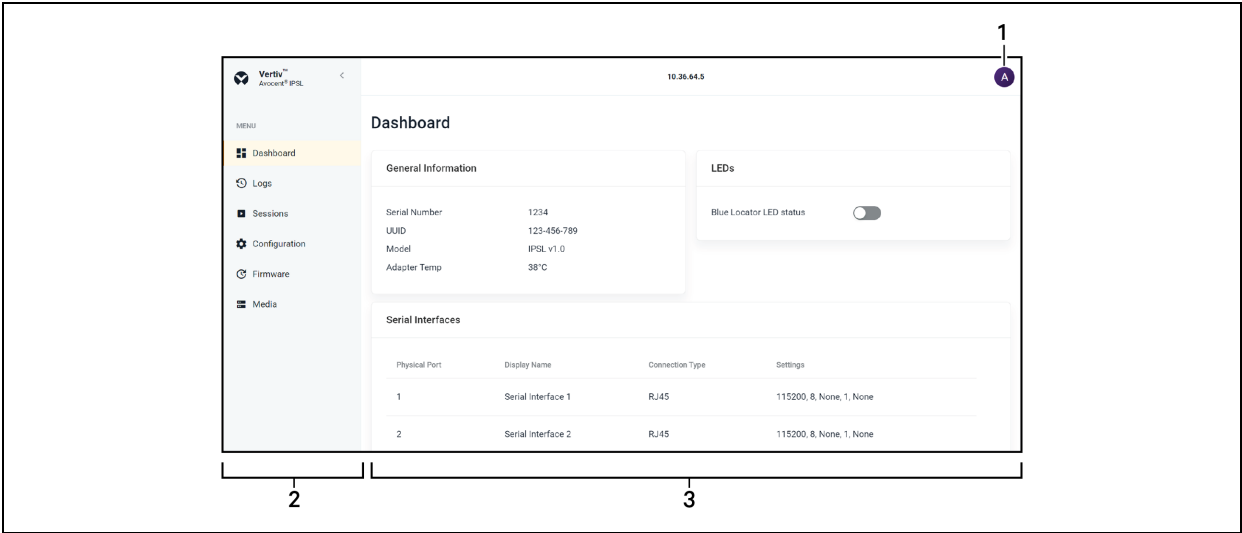


Table 2.1 Web UI Overview Descriptions

Item	Description
1	User profile
2	Sidebar
3	Content area

NOTE: By default, the serial device is set to Managed mode upon initial login. While in Managed mode, the serial device disables certain UI features under the Configuration tab. To configure the mode of the serial device, refer to [Registration](#).

2.1 Dashboard

From the Dashboard screen, you can perform the following functions:

- Access 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. For more information, refer to [Serial interfaces](#).
- View the serial interfaces associated with the serial device.
- View the audited log of events for the serial device.

2.1.1 Serial management

Prerequisites

Before launching an HTML5 serial session, ensure the following requirements have been met:

- 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 Vertiv Avocent IPSL IP serial device provides remote access to your serial devices. To modify your serial communication parameters, see [Serial interfaces](#).

To launch a serial session:

1. From the left-hand sidebar, click *Dashboard*.
2. Under Serial Interfaces, hover your mouse over the desired target and click the Launch Console icon.

-or-

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

To end a serial session:

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

2.2 User Profile

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

User Name

The name of the current user is displayed.

Help

This option redirects you to a digital copy of the Vertiv Avocent IPSL IP Serial Device Installer/User Guide.

Software Version

The current version number of the installed software is displayed.

Log Out

This option immediately logs you out of the web UI.

2.3 System Configuration

From the System Configuration tab, you can access nine sub-menu items - Registration, User Management, Services, Date and Time, System Settings, Certificates, Troubleshooting, Remote Syslog, and Remote Authentication - which allow you to configure the advanced settings for the IP serial device.

2.3.1 Registration

From the Registration screen, you can configure the operation mode of the Vertiv Avocent IPSL IP serial device.

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

To set the device to Managed mode:

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

NOTE: The values in the Interval fields should not be changed as they are pre-defined and used only in specific troubleshooting situations.

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

4. Click *Apply*.

2.3.2 User management

From the User Management screen, you can view and configure the user and group accounts. A single "admin" user with Administrator permissions is the only one that exists on the device in the factory default state.

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 permission groups.

Administrator

This user group has the maximum permission level, including the Operator level privilege plus the capacity to modify all system settings, execute firmware updates, provision network configuration, execute network troubleshooting actions, and replace certificates.

Operator

This user group permission level is limited to read-only access to view system configurations and operate the core device functionality, which is to configure access settings related to the connected serial targets and launch sessions to those targets.

Read-only

This user group has the lowest permission level and is only allowed to view system configuration settings.

This device is compliant with the required Roles defined by the Redfish specification, and the detailed information on the privileges defined for each role and what CRUD operations on each API endpoint require which privileges can be found by reviewing the Redfish specification document and querying the device REST API at `/redfish/v1/AccountService/Roles/{Role}` to view the role definitions and `/redfish/v1/Registries/VertivPrivilegeRegistry.<version>` to view the privileges required for each CRUD operation.

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 appears.
3. Select the appropriate radio button for the state of the user: Enabled or Disabled.
4. Enter the username 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 policy 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 Settings page, you can configure the password policy for users. See [System Settings](#) for more information.
4. Configure desired password settings.

5. Click *Apply*.

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.
 - a. To edit a user, click *Edit* and modify the information as needed, then click *OK*.
 - b. To delete a user, click *Delete*.

2.3.3 Services

From the Services screen, you can perform the following functions:

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

2.3.4 Date and time

From the Date/Time screen, you can perform the following functions:

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

2.3.5 System settings

From the System Settings screen, you can view and configure system settings for the Vertiv 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.

2.3.6 Certificate

From the Certificate screen, you can perform the following functions:

- 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*.

Select the key bit length or encryption curve ID that meets your security requirements for the chosen key algorithm.

NOTE: If you do not have specific security or compliance requirements, use the highest available key bit length or the strongest available encryption curve for the selected key algorithm. This configuration provides the highest level of cryptographic strength supported by the appliance and is the recommended default configuration.

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.

2.3.7 Troubleshooting

From the Troubleshooting screen, you can run a troubleshooting report on the serial device to identify certain issues.

To submit a troubleshooting report:

1. From the left-hand sidebar, click *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. Enter the port number.
5. 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.

6. Click *Submit*.

2.3.8 Remote syslog

From the Remote Syslog screen, you can add a remote syslog server for better management and monitoring of the serial device.

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*.

2.3.9 Remote authentication

From the Remote Authentication screen, you can implement authentication methods to ensure the security of your system and users. Providers can be authenticated via AD/LDAP, TACACS+, or RADIUS.

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

To set the priority order for authentication methods:

1. 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

2. Click *Apply*.

To add an LDAP authentication method:

1. From the *Configuration - Remote Authentication - LDAP* screen, 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 Vertiv Avocent IPSL IP serial device, to map your Active Directory remote group to a role on the Vertiv Avocent IPSL 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*.

To add a TACACS+ authentication method:

1. From the *Configuration - Remote Authentication - TACACS+* screen, 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*.

To add a RADIUS authentication method:

1. From the *Configuration - Remote Authentication - RADIUS* screen, 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*.

2.4 Interface Configuration

From the Interface Configuration tab, you can access two sub-menu items - Network and Serial Interfaces - which allow you to configure the advanced settings for the IP serial device.

2.4.1 Network

From the Network screen, you can view and configure the network settings for the serial device.

The Vertiv 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 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 information is provided:
 - Interface toggle.
 - Network speed.
 - Duplex mode status.
 - Auto Negotiation status.
4. Under the IPv4 Settings, the DHCP settings for the interface can be configured.
NOTE: IPv4 settings for the usb0 interface are read-only.
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*.

2.4.2 Serial interfaces

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

To configure the serial interfaces:

1. From the *Configuration - Serial Interfaces* screen, ensure that the Interface Enabled option is enabled. This setting must be enabled to launch serial sessions.

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.

2.5 Logs

From the Logs screen, you can view the log of events that have occurred on the serial device. On this screen, you can perform the following functions:

- 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.

2.6 Sessions

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

The Vertiv 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, refer to [Virtual media](#).
- Configure serial communication
- Parameters
- Data logging
- Manage up to 4 serial devices
- Serial over SSH

2.7 Firmware

From the Firmware tab, you can access two sub-menu items - Firmware Management and Firmware Inventory - which allow you to manage the firmware upgrades, factory settings, and reboot actions for the serial device.

2.7.1 Firmware management

From the Firmware Management screen, you can perform reboots and factory resets.

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*.

2.7.2 Firmware inventory

From the Firmware Inventory screen, you can access information about the primary firmware and failover firmware, including the name, version, and status of the firmware.

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

To update the primary firmware or failover firmware:

1. From the left-hand sidebar, click *Firmware - Firmware Inventory*.
2. Click the *Update* button under the respective firmware section.
3. Select one of the following image upload methods:
 - TFTP: Copy the TFTP file path and paste it into the TFTP Path field.
 - HTTP: Enter the HTTP URL of the firmware image in the appropriate field.
 - HTTPS: Enter the HTTPS URL of the firmware image in the appropriate field.
 - Image Upload (Drag and Drop): Drag and drop the firmware image file or folder into the upload area.
 - Browse: Select the firmware image file through a file explorer.
4. Click *Start Update*.

2.8 Media

From the Media tab, you can access two sub-menu items - Remote Media and Virtual Media - which allow you to configure the appropriate media options for file mapping with the serial device.

2.8.1 Remote media

From the Remote Media screen, you can add and configure a remote server location.

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.

2.8.2 Virtual media

From the Virtual Media screen, you can 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.

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 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 your use group) must have permission to establish virtual media sessions and/or reserved virtual medial sessions to the target device.

To map a Virtual Media drive:

1. From the left-hand sidebar, click *Media - Virtual Media*.
2. 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.

NOTE: Virtual Media control is disabled (Off mode) by default. Verify that another user is not using the Virtual Media feature on a different device or website if you are unable to enable Virtual Media control to On mode.

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 dialog 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.

3 Security Best Practices

The card is configured with secure default settings at deployment. To protect critical infrastructure equipment, review and configure all communication services according to your operational requirements. This section summarizes the available security settings.

Through the Vertiv™ SECURE product life cycle, Vertiv works to reduce cybersecurity risks in its products. Vertiv applies cybersecurity best practices throughout product design and development to provide secure, reliable solutions for customers.

Review the following cybersecurity recommendations during each phase of the product life cycle. These recommendations complement existing cybersecurity programs and do not provide a comprehensive cybersecurity guide. For additional cybersecurity guidance, refer to:

[CISA Cybersecurity Best Practices](#)

[Vertiv Security Support Center](#)

Table 3.1 lists security-related items to review. Assess and configure each item according to your operational requirements. Verify that each setting supports the required functionality while limiting unnecessary or unauthorized access to critical infrastructure. Refer to the section identified in the table for configuration instructions.

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

Item	Description	Comments
Accounts and Passwords	Change the default administrator password to immediately to prevent access through default credentials.	Enforced at first login
Remote Account Providers	Enable remote account providers (LDAP, TACACS+, or RADIUS) only when required.	See Remote Authentication
TLS Certificates	Installed TLS certificates from a trusted certificate authority (CA) or generate replacement self-signed certificates.	See Certificates

Table 3.2 lists the network ports used by this product. To improve security, configure local firewalls and network gateways to allow only the traffic required for operation. Disable unused ports on the device when supported. If the device does not support port disabling, block unused ports through external firewall rules.

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

Table 3.2 Network Ports Opened/Listened to by the Vertiv Avocent IPSL IP Serial Device

Network Service	Port Used	Default	Modification Possible by Admin	Comments
HTTPS	TCP 443	✓	✗	
mDNS	UDP 5353	✓	✗	See Finding the Assigned IP Address
SSH	TCP 2200-2203	✗	✓	See Serial interfaces

3.1 Risk Assessment

Vertiv recommends performing a risk assessment to identify and evaluate potential internal and external risks to security, availability, and integrity of the system and its operating environment. Conduct the assessment in accordance with applicable technical and regulatory frameworks, such as IEC 62443 and NERC CIP. Repeat the risk assessments periodically.

3.2 Physical Security

This product is designed for deployment and operation in a physically secure location. Vertiv recommends reviewing the physical security controls and operating environment of the unit. Because both external attackers and insider threats can cause significant disruption, following these best practices:

- Restrict access to areas, racks, and units by using encrypted RFID cards or badges, multi-factor authentication, mantraps, and biometric access controls.
- Employ trusted security personnel who have completed background checks. Maintain 24/7/365 on-site coverage and keep written logs to document and track physical access to the data center, building, and equipment racks.
- Limit physical access to telecommunications equipment and network cabling to help prevent interception or sabotage. Use metal conduits for network cabling that runs between equipment cabinets.
- Restrict access to all USB, RJ45, and other physical ports on the units.
- Do not connect removable media, such as USB devices, for operations such as firmware upgrades, configuration changes, or boot application changes unless the media source is known and trusted.

NOTE: Before you connect a portable device through a USB port, scan the device for malware and viruses.

3.3 Account Access

Manage account access privileges so that users have only the permissions required to perform their job responsibilities. Limit access to the web user interface (UI) to authorized users only. Vertiv recommends incorporating the following best practices into your organization's procedures for network and equipment access:

- Require users to create their own credentials during the first login.
- Prohibit account sharing. Assign each user a unique account and password. Audit logging functions rely on each account representing an individual user.
- Grant users only the access and privileges required for their job responsibilities.
- Restrict administrator-level privileges, such as firmware updates and protocol configuration, to approved administrators.
- Enforce password strength, complexity, and length requirements in accordance with company IT policies.
- Remove access immediately when an employee's employment is terminated. You can implement this control through an AAA or TACACS+ authentication process.
- Configure session timeouts to automatically end inactive sessions.
- Use a remote syslog facility to monitor system and network events, identify security threats, and troubleshoot device issues.

NOTE: A remote syslog facility may be required to support compliance with regulations or standards such as PCI DSS, SOX, or HIPAA.

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	2 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 Tricolor 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.x.com/Vertiv/>

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

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

590-2375-501D